3GPP TR 23.799 V1.1.0 (2016-10)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on Architecture for Next Generation System
(Release 14)





The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Report is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631

Keywords
3GPP, Architecture, NextGen, Study

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2016, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 2 of 501

Contents

Foreword....18
1 Scope....19
2 References....19
3 Definitions and abbreviations....20
3.1 Definitions....20
3.2 Abbreviations....22
4 Architectural Requirements, Assumptions and Principles....22
4.1 High level Architectural Requirements....22
4.2 Architectural Assumptions....24
4.2.1 Initial High level architectural view....24
4.2.2 Reference points....25
4.3 Architectural Principles....25
5 Key Issues....25
5.1 Key issue 1: Support of network slicing....25
5.1.1 Description....25
5.1.2 Work Tasks....26
5.2 Key issue 2: QoS framework....26
5.2.1 Description....26
5.2.2 Work Tasks....27
5.3 Key Issue 3: Mobility management framework....29
5.3.1 Description....29
5.3.2 Work Tasks....30
5.4 Key issue 4: Session management....31
5.4.1 Description....31
5.4.2 Work Tasks....32
5.5 Void....33
5.6 Key issue 6: Support for session and service continuity and efficient user plane path....33
5.6.1 Description....33
5.6.2 Work Tasks....34
5.7 Key issue 7: Network function granularity and interactions between them....35
5.7.1 Description....35
5.7.2 Work Tasks....35
5.8 Key issue 8: Next Generation core and access - functional division and interface....36
5.8.1 Description....36
5.8.2 Work Tasks....36
5.9 Key Issue 9: 3GPP architecture impacts to support network capability exposure and context information awareness....37
5.9.1 Description....37
5.10 Key issue 10: Policy Framework....38
5.10.1 Description....38
5.10.2 Work Tasks....39
5.11 Key issue 11: Charging....40
5.11.1 Description....40
5.12 Key issue 12: Security framework....41
5.12.1 Description....41
5.12.2 Work Tasks....42
5.13 Key issue 13: Broadcast/Multicast Capabilities....42
5.13.1 Description....42
5.14 Key Issue 14: Support for Off-Network Communication....43
5.14.1 Description....43
5.15 Key Issue 15: NextGen core support for IMS....43
5.15.1 Description....43
5.16 Key Issue 16: 3GPP system aspects to support the connectivity of remote UEs via relay UEs....43
5.16.1 Description....43
5.17 Key Issue 17: 3GPP architecture impacts to support network discovery and selection....44

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 3 of 501

5.17.1 Description 44
5.17.2 Work Tasks 45
5.18 Key Issue 18: Interworking and Migration 45
5.18.1 Description 45
5.18.1.1 Interworking and migration principles 45
5.18.1.2 Assumptions on UE capabilities 46
5.18.1.3 Interworking and migration scenarios within an operator 46
5.18.1.4 Interworking scenarios on roaming 46
5.18.1.5 UE compatibility 46
5.18.2 Work Tasks 47
5.19 Key Issue 19: Architecture impacts when using virtual environments 47
5.19.1 Description 47
5.19.2 Issues to be addressed 48
5.19.2.1 Avoid UE interaction from NF Load Balancing, Scaling and Migration 48
5.20 Key issue 20: Traffic Steering, Switching and Splitting between 3GPP and non-3GPP Accesses 48
5.20.1 Description 48
5.20.2 Work Tasks 48
5.21 Key Issue 21: Minimal connectivity within extreme rural deployments 49
5.21.1 Description 49
5.22 Key Issue 22: Support of "5G connectivity via satellite" use case 49
5.22.1 Description 49
5.22.2 Work Tasks 50
5.x Key Issue x: Title 50
5.x.1 Description 50

6 Solutions 50
6.1 Solutions for Key Issue 1: Support of network slicing 51
6.1.1 Solution 1.1: Network Slicing without Slicing the radio 51
6.1.1.1 Architecture description 51
6.1.1.2 Function description 53
6.1.1.3 Solution evaluation 58
6.1.2 Solution 1.2: Network slice selection 58
6.1.2.1 Architecture description 60
6.1.2.1.1 Network Slice and Network Function selection 61
6.1.2.2 Function description 64
6.1.2.2.1 Functions 64
6.1.2.2.1 Reference points 64
6.1.2.2.1 High level operation description 64
6.1.2.2.2 Definitions used in the solution 65
6.1.2.2.3 Example procedures 66
6.1.2.2.3.1 Initial Access 66
6.1.2.2.3.3 Subsequent NAS signalling for PDU Session Modification 68
6.1.2.2.3.3 Reselection of a Network Slice after UE Registration 69
6.1.2.2.3.3.1 Network Triggered Reselection of a Network Slice 69
6.1.2.2.3.3.2 UE Triggered Reselection of a Network Slice 71
6.1.2.2.3.4 New Service Request and User Authentication by the 3rd Party 72
6.1.2.3 Solution evaluation 73
6.1.3 Solution 1.3: Support of multiple connections to multiple Network Slices 73
6.1.3.1 Architecture description 73
6.1.3.2 Function description 77
6.1.3.3 Solution evaluation 79
6.1.4 Solution 1.4: Void 79
6.1.5 Solution 1.5: Selection of a network slice instance 79
6.1.5.1 Terminology and modelling 79
6.1.5.2 Architecture description 80
6.1.5.2 Function description 81
6.1.5.3 Solution evaluation 83
6.1.6 Solution 1.6: Slice Instance ID based Network Slice Selection 83
6.1.6.1 Architecture description 84
6.1.6.2 Function description 84
6.1.6.2.1 Definitions and functions 84
6.1.6.2.2 Common Network Functions 85

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 4 of 501

6.1.6.2.3 The Attach procedure 85
6.1.6.2.4 Slice Instance ID update due to subscription change 87
6.1.6.3 Solution evaluation 87
6.1.7 Solution 1.7: Network Slice Selection based on Usage Class 87
6.1.7.1 Architecture description 87
6.1.7.2 Solution evaluation 89
6.1.8 Solution 1.8: Network slice instance reselection 89
6.1.8.1 Definition and categorization of slice reselection 89
6.1.8.2 Scenarios for slice reselection 90
6.1.8.3 Function description 91
6.1.8.3.1 Intra C-CPF Network Slice Change 91
6.1.8.3.2 Inter C-CPF Network Slice Change 92
6.1.8.4 Solution evaluation 92
6.1.9 Solution 1.9: Multiple Independent Slices per UE 92
6.1.9.1 Architecture description 92
6.1.9.2 Signalling Procedures 94
6.1.9.2.1 Attach Procedures 94
6.1.9.2.2 Routing Area Update Procedure 97
6.1.9.2.3 Detach Procedure 98
6.1.9.3 Solution evaluation 98
6.1.10 Solution 1.10: Roaming architecture for Network Slicing based on solution#2 98
6.1.10.1.1 Basic Non-roaming architecture 99
6.1.10.1.2 Home-routed roaming architecture 99
6.1.10.1.3 Local breakout roaming architecture supporting Home PLMN Application Function 100
6.1.10.1.4 Local breakout roaming architecture supporting Home PLMN Application Function 101
6.1.10.2 Solution evaluation 101
6.1.11 Solution 1.11: Network Slice Instance Selection and Association 101
6.1.11.1 Architecture description 101
6.1.11.2 Function description 102
6.1.11.2.1 Network slice instance selection and association procedure 102
6.1.11.3 Solution evaluation 104
6.2 Solutions for Key Issue 2: QoS framework 105
6.2.1 Solution 2.1: Per PDU Flow QoS Model 105
6.2.1.1 Architecture description 105
6.2.1.1.1 Relation between PDU Flow and Service Data Flow 107
6.2.1.1.2 Application requirements input 108
6.2.1.1.3 Network Authorized QoS parameters 109
6.2.1.1.3.1 Flow Priority 110
6.2.1.1.4.2 Network behaviour per flow 110
6.2.1.2 Function description 110
6.2.1.2.1 QoS Authorization at PDU session establishment 110
6.2.1.2.2 QoS Authorization based on application requirements 111
6.2.1.3 Solution evaluation 112
6.2.1.3.1 Solution comparison to the existing framework 112
6.2.2 Solution 2.2: Flow based QoS framework 113
6.2.2.1 Architecture description 113
6.2.2.2 Function description 116
6.2.2.3 Solution evaluation 119
6.2.3 Solution 2.3: Content Aware QoS Framework 119
6.2.3.1 Overview 119
6.2.3.2 Architecture description 120
6.2.3.3 QoS related information exchanged between network functions 122
6.2.3.4 Function description 125
6.2.3.5 Solution evaluation 126
6.2.4 Solution 2.4: QoS model for QoS Authorization and Request 126
6.2.4.1 Architecture description 126
6.2.4.1.1 Functional Architecture 126
6.2.4.2 Function description 126
6.2.4.2.1 QoS Pre-Authorization at PDU Session Establishment 126
6.2.4.2.2 QoS Establishment 126
6.2.5 Solution 2.5: QoS model for flexible traffic differentiation 128
6.2.5.1 Architecture description 128

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 5 of 501

6.2.5.1.1 Functional Architecture 128
6.2.5.1.2 Applications Requirements Input 128
6.2.5.1.3 Packet Markings for Traffic Differentiation 128
6.2.5.2 Function description 130
6.2.5.2.1 Dynamic QoS Modification 130
6.2.6 Solution 2.6: QoS ID solution 131
6.2.6.1 Architecture description 131
6.2.6.2 Function description 132
6.2.6.3 Solution evaluation 132
6.2.7 Solution 2.7: QoS framework for resource management for Mission Critical Group Communications 132
6.2.7.1 Architecture Description 132
6.2.7.2 Functional Description 133
6.2.7.3 Solution evaluation 134
6.2.8 Solution 2.8: Application-based uplink traffic identification 134
6.2.8.1 Solution Description 134
6.2.8.2 Function description 134
6.2.8.3 Solution evaluation 135
6.2.9 Solution 2.9: NextGen Bearer based QoS control model 135
6.2.9.1 Architecture description 135
6.2.9.1.1 NextGen Bearer level QoS parameters 136
6.2.9.2 Function description 138
6.2.9.2.1 NextGen Non-GBR Bearer established at PDU session establishment 138
6.2.9.2.2 NextGen GBR Bearer establishment based on the application server request 139
6.2.9.3 Solution evaluation 140
6.3 Solutions for Key Issue 3: Mobility framework 140
6.3.1 Solution 3.1: High-level functions of the mobility framework 140
6.3.1.1 Architecture description 140
6.3.1.2 Function description 141
6.3.1.3 Solution evaluation 142
6.3.2 Solution 3.2: Mobility state framework 142
6.3.2.1 Architecture description 142
6.3.2.2 Function description 143
6.3.2.3 Solution evaluation 143
6.3.3 Solution 3.3: Solution for mobility framework with RAN level tracking 143
6.3.3.1 Architecture description 144
6.3.3.2 Function description 145
6.3.3.3 Solution evaluation 145
6.3.4 Void 145
6.3.5 Solution 3.5: Stateless Context Management for Data Network Sessions 145
6.3.5.1 Architecture description 145
6.3.5.1.2 Support For Infrequent Small User Data Service 147
6.3.5.1.3 Support of CIoT User Plane Optimizations 147
6.3.5.2 Function description 147
6.3.5.2.1 Context Cookie Creation 147
6.3.5.2.3 Mobile Originated Small Data Service Transfer with Context Cookie-based context verification 149
6.3.5.2.4 Mobile Originated Small Data Transfer with Cookie-based context re-establishment 150
6.3.5.2.4 Connection Suspension and Cookie Generation for User Plane CIoT Optimisation 151
6.3.5.2.5 Connection Resume for User Plane CIoT Optimisation 152
6.3.5.2.6 Support of Scheduled Mobile Terminated Communications 152
6.3.5.2.7 Support of Unscheduled Mobile Terminated Communications 153
6.3.5.3 Solution evaluation 153
6.3.6 Solution 3.6: Mobility states for UE with power consumption optimization 153
6.3.6.1 Architecture description 153
6.3.6.2 Function description 153
6.3.6.3 Solution evaluation 154
6.3.7 Solution 3.7: NextGen State Model 154
6.3.7.1 General 154
6.3.7.2 Architecture description 154
6.3.7.2.1 NextGen Mobility Management (NMM) 154
6.3.7.2.2 Void 155
6.3.7.2.3 NextGen Radio Resource Control (RRC) 155

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 6 of 501

6.3.7.2.4 Overview of NMM, and RRC state models 156
6.3.7.3 Functional description 157
6.3.7.4 Solution evaluation 157
6.3.8 Solution 3.8: Simplified mobility states for stationary UE and MO data transmission only UE 157
6.3.8.1 Architecture description 157
6.3.8.2 Function description 158
6.3.8.2.1 Mobility states and corresponding transitions of stationary UE 158
6.3.8.2.2 Mobility states and corresponding transitions of MO data transmission only UE 159
6.3.8.3 Solution evaluation 159
6.3.9 Solution 3.9: Mobility levels using Mobility and Session classes 159
6.3.9.1 Architecture description 159
6.3.9.2 Function description 160
6.3.9.2.1 Mobility classes 160
6.3.9.2.2 Session classes 161
6.3.9.2.3 Assigning, controlling and enforcing Mobility and Session classes 161
6.3.9.2.4 Mobility aspects and how to handle roaming 162
6.3.9.3 Solution evaluation 163
6.3.10 Solution 3.10: RAN Specific paging for UE in CN connected mode 163
6.3.10.1 Architecture description 163
6.3.10.2 Function description 164
6.3.10.2.1 Downlink NG1 Signalling Triggered RAN Specific Paging. 164
6.3.10.2.2 Downlink NG3 data Triggered RAN Specific Paging 164
6.3.10.2.3 Core Network Assisted RAN Specific Paging Retry 165
6.3.10.3 Solution evaluation 167
6.3.11 Solution 3.11: Solution for dynamic mobility management 167
6.3.11.1 Mobility categories 167
6.3.11.2 Functional description 167
6.3.11.2.1 Dynamic mobility management in IDLE mode 167
6.3.11.2.2 Differences from existing solutions 168
6.3.11.3 Solution Evaluation 168
6.3.12 Solution 3.12: Solution for UE reachability in power saving state 168
6.3.12.1 Architecture description 168
6.3.12.2 Function description 169
6.3.12.3 Solution evaluation 170
6.3.13 Solution 3.13: Solution for mobility framework with split Location Tracking Function 170
6.3.13.1 Architecture description 170
6.3.13.2 Function description 170
6.3.14 Solution 3.14: Solution for determining UE mobility level 171
6.3.14.1 General description 172
6.3.14.2 Function description 172
6.3.14.3 Solution evaluation 173
6.3.15 Solution 3.15: Solution to support different levels of mobility 173
6.3.15.1 Mobility Levels Definition 173
6.3.15.2 Function description 176
6.3.15.3 Solution evaluation 177
6.3.16 Solution 3.16: Limited & Unlimited UE mobility level 177
6.3.16.1 Architecture description 178
6.3.16.2 Function description 178
6.3.16.3 Solution evaluation 180
6.3.17 Solution 3.17: Support for Idle Mode Mobility capabilities 180
6.3.17.1 Architecture Description 180
6.3.17.2 Function description 182
6.3.17.3 Solution Evaluation 182
6.3.18 Solution 3.18: Mobility procedure 182
6.3.18.1 Architecture description 182
6.3.18.2 Function description 182
6.3.18.2.1 Registration procedure 183
6.3.18.2.2 UE Status Update procedure 184
6.3.18.3 Solution evaluation 185
6.3.19 Solution 3.19: Solution to activate RRC inactive state 185
6.3.19.1 Architecture description 185
6.3.19.2 Function description 185

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 7 of 501

6.3.19.2.1 Service Activation Procedure 185
6.3.19.3 Solution evaluation 186
6.3.20 Solution 3.20: Solution for UE reachability for devices with only MO-communication 186
6.3.20.1 Architecture description 186
6.3.20.2 Function description 186
6.3.20.3 Solution evaluation 188
6.3.21 Solution 3.21: Solution for explicit signaling to limit idle mode procedures 188
6.3.21.1 General description 188
6.3.21.2 Functional description 188
6.3.21.2.1 Limited Reachability 188
6.3.21.2.2 Limited mobility tracking 188
6.3.21.2.3 Signalling Flows 189
6.3.21.3 Solution Evaluation 189
6.3.22 Solution 3.22: Applying customized NextGen mobility states 189
6.3.22.1 Architecture description 189
6.3.22.2 Function description 190
6.3.22.2.1 Procedure of enabling customized mobility states 191
6.3.22.3 Solution evaluation 191
6.3.23 Solution 3.23: Two layers Tracking Area handling 191
6.3.23.1 Architecture description 191
6.3.23.2 Function description 192
6.3.23.3 Solution evaluation 193
6.3.24 Solution 3.24: Mobility pattern based mobility management 193
6.3.24.1 General description 193
6.3.24.2 Function description 194
6.3.24.3 Solution evaluation 195
6.3.25 UE reachability management in Inactive mode 195
6.3.25.1 Architecture description 195
6.3.25.2 Function description 195
6.3.25.2.1 Common Functional Elements for all approaches 195
6.3.25.2.1.1 Transition to Inactive mode 196
6.3.25.2.1.2 Context Retrieval via Xn (based on Rel-13 X2 functions) 196
6.3.25.2.1.3 Context Retrieval via CN (within the same pool of CP CN nodes) 197
6.3.25.2.1.4 Context Retrieval failed (either on Xn or via NG2) 199
6.3.25.2.1.5 Xn Paging 199
6.3.25.2.2 Functional elements necessary if the RAN paging area is configured on NAS level (Tracking Area approach) 200
6.3.25.2.2.1 CN assisted RAN Paging 200
6.3.26 Solution 3.26: Intra-RAT HO procedure 201
6.3.26.1 Architecture Description 201
6.3.26.2 Function description 203
6.3.26.2.2 Inter-NextGen HO procedure 204
6.3.27 Solution 3.27: Multiple level Tracking Areas handling 205
6.3.27.1 Architecture description 205
6.3.27.2 Function description 206
6.3.27.2.1 Multiple level Tracking Area Allocation 206
6.3.27.2.2 Multiple level Tracking Area Update in the UE 207
6.3.27.2.3 Reachability Management for UE in IDLE state 207
6.3.27.3 Solution evaluation 207
6.4 Solutions for Key Issue 4: Session management 207
6.4.1 Solution 4.1: Session Management functions and relations 207
6.4.1.1 Architecture description 208
6.4.1.2 Function description 209
6.4.1.3 Solution evaluation 209
6.4.2 Solution 4.2: Session setup procedures 209
6.4.2.1 Architecture description 209
6.4.2.2 Function description 210
6.4.2.2.1 Session establishment procedure, non-roaming case 210
6.4.2.2.2 Session establishment procedure, home-routed roaming case 212
6.4.2.3 Solution evaluation 213
6.4.3 Solution 4.3: NextGen Session Management with Multiple PDU sessions to the same Data Network 213
6.4.3.1 Architecture description 213

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 8 of 501

6.4.3.1.1 NextGen Session Management Model and States 215
6.4.3.1.1.1 NSM-IDLE 215
6.4.3.1.1.2 NSM-CONNECTED 215
6.4.3.1.1.3 State transition and functions 216
6.4.3.1.2 NSM Context 216
6.4.3.2 Function Description 216
6.4.3.2.1 UE PDU Session Establishment Triggering 216
6.4.3.2.2 UP-GW Selection 217
6.4.3.2.3 Establishment of a PDU Session 218
6.4.3.3 Solution evaluation 219
6.4.4 Solution 4.4: Void 219
6.4.5 Solution 4.5: Network triggered on-demand SM setup procedure 219
6.4.5.1 Architecture description 219
6.4.5.2 Function description 219
6.4.5.3 Solution evaluation 220
6.4.6 Solution 4.6: Common interfaces towards UE, AN and SDM for both MM and SM related procedures 221
6.4.6.1 Description 221
6.4.7 Solution 4.7: Infrequent small data transfer 221
6.4.7.1 Architecture description 222
6.4.7.2 Function description 223
6.4.7.3 Solution evaluation 225
6.4.8 Solution 4.8: for Data transmission with ConnectionLess RAN-Core interface 226
6.4.8.1 Solution Overview 226
6.4.8.2 Call flows 229
6.4.8.2.1 Identities 229
6.4.8.2.1.1 UPGW CL SERVICE Id (UCLSI) 229
6.4.8.2.2 Assumptions 229
6.4.8.2.3 Procedures 229
6.4.8.2.3.1 Set-up of a PDU sessions with Connectionless mode data transfer on the RAN-Core interface 229
6.4.8.2.3.2 UE connectionless uplink data transfer 231
6.4.8.2.3.3 UE connectionless downlink data transfer 232
6.4.8.2.3.4 Paging for UE connectionless downlink data transfer 233
6.4.8.2.3.5 Mobility support 234
6.4.8.2.4.6 UPGW Triggered Release and Redirection During UE Connectionless Active Mode 235
6.4.9 Solution 4.9: UP protocol model - Per QoS class tunnel protocol 235
6.4.9.1 Architecture description 235
6.4.9.2 Function description 236
6.4.9.3 Solution evaluation 236
6.4.10 Solution 4.10: UP protocol model - Per PDU session tunnel protocol 236
6.4.10.1 Architecture description 236
6.4.10.2 Function description 237
6.4.10.3 Solution evaluation 237
6.4.11 Solution 4.11: UP protocol model - Per Node-level tunnel 237
6.4.11.1 Architecture description 237
6.4.11.2 Function description 238
6.4.11.3 Solution evaluation 239
6.4.12 Solution 4.12: UP protocol model - SDN-Based Approach 239
6.4.12.1 Architecture description 239
6.4.12.2 Function description 241
6.4.12.3 Solution evaluation 241
6.4.13 Solution 4.13: Session Management model for multiple parallel PDU Sessions and for multi-homed PDU Session 241
6.4.13.1 Architecture description 241
6.4.13.2 Function description 243
6.4.13.2.1 Session management procedure for multiple-homed PDU sessions 243
6.4.13.3 Solution evaluation 245
6.4.14 Solution 4.14: Session management with flexible multiple UP GW(s) assignment 245
6.4.14.1 Architecture Description 245
6.4.14.2 Session establishment with Edge GW and DN-GW selection and configuration 247
6.4.14.3 Edge GW relocation 247

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 9 of 501

6.4.15 Solution 4.15: Common interfaces towards UE, AN with MM and SM decoupled 248
6.4.15.1 Description 248
6.4.15.2 Procedure 249
6.4.16 Solution 4.16: the interaction between MM and SM 251
6.4.16.1 Architecture Description 251
6.4.16.1.1 Overview 251
6.4.16.1.2 Interactions between MMF and SMF 252
6.4.16.1.3 Subscription data 254
6.4.16.2 Function description 255
6.4.16.2.1 Set-up of a PDU session 255
6.4.16.2.2 The subscription on UE mobility 256
6.4.16.2.3 The notification on UE mobility 257
6.4.16.3 Solution evaluation 258
6.4.17 Solution 4.17: Void 258
6.4.18 Solution 4.18: Solution for Infrequent Small Data 259
6.4.18.1 Architecture description 259
6.4.18.2 Function description 259
6.4.18.2.1 Connection Establishment Flow 259
6.4.18.2.2 Uplink PDU Transfer Flow 260
6.4.18.2.3 Downlink PDU Transfer Flow 261
6.4.18.3 Solution evaluation 262
6.4.19 Solution 4.19: Infrequent small user data transfer via control plane 262
6.4.19.1 Architecture description 263
6.4.19.2 Function description 263
6.4.19.2.1 Mobile originated data transport via control plane 263
6.4.19.2.2 Mobile terminated data transport via control plane 264
6.4.19.3 Solution evaluation 265
6.4.20 Solution 4.20: Session Management on the PDU session(s) via different accesses 265
6.4.20.1 Architecture description 265
6.4.20.2 Function description 267
6.4.20.3 Solution evaluation 268
6.4.21 Solution 4.21: NG3 interface related procedures 268
6.4.21.1 Architecture description 268
6.4.21.2 Function description 269
6.4.21.2.1 NG3 Disconnection 269
6.4.21.2.2 Service Request 269
6.4.21.2.3 Paging 270
6.4.21.3 Solution evaluation 272
6.4.22 Solution 4.22: Session management per PDU session 272
6.4.22.1 Architecture Description 272
6.4.22.2 Function description 273
6.4.22.3 Solution evaluation 276
6.4.23 Solution 4.23: Asynchronous Session Management Model 276
6.4.23.1 Architecture description 276
6.4.23.2 Function description 276
6.4.23.2.1 Asynchronous session management procedure 277
6.4.23.3 Solution evaluation 278
6.4.24 Solution 4.24: Session Management with individual CP function per access network 278
6.4.24.1 Architecture description 278
6.4.24.2 Function description 279
6.4.24.3 Solution evaluation 280
6.4.25 Solution 4.25: Local Area Data Network 280
6.4.25.1 Architecture description 280
6.4.25.2 Function description 280
6.4.25.3 Solution evaluation 281
6.5 Solutions for Key Issue 5: Enabling (re)selection of efficient user plane paths 281
6.5.1 Solution 5.1: UP Functions selection 281
6.5.1.1 Architecture description 281
6.5.1.2 Function description 281
6.5.1.3 Solution evaluation 282
6.5.2 Solution 5.2: Solution to support Session continuity to enable (re)selection of efficient user plane paths 282

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 10 of 501

6.5.2.1 Architecture description 282
6.5.2.2 Function description 283
6.5.2.2.1 General 283
6.5.2.2.2 Mobility aspects 284
6.5.2.3 Solution evaluation 286
6.5.3 Solution 5.3: Re-selection of user-plane path based on UE traffic pattern 286
6.5.3.1 Architecture Description 286
6.5.3.2 Function description 287
6.5.3.3 Solution Evaluation 288
6.5.4 Solution 5.4: Multiple Tunnel based traffic offload 288
6.5.4.1 Architecture Description 288
6.5.4.2 Function description 289
6.5.4.3 Solution Evaluation 291
6.5.5 Solution 5.5: Application-aware UP Path (Re)selection 291
6.5.5.1 Architecture description 291
6.5.5.2 Function description 292
6.5.5.2.1 Co-ordination the Session and Service Continuity with the Application-aware UP Path (Re)selection 294
6.5.5.3 Solution evaluation 296
6.6 Solutions for Key Issue 6: Support for session and service continuity 296
6.6.1 Solution 6.1: Session and service continuity framework 296
6.6.1.1 Architecture description 296
6.6.1.1.1 Overview 296
6.6.1.1.2 Assumptions 296
6.6.1.1.3 Session and service continuity modes 296
6.6.1.1.4 Solution principles 297
6.6.1.1.4.1 Mode selection and network support 297
6.6.1.1.4.2 SSC mode 1 298
6.6.1.1.4.3 SSC mode 2 298
6.6.1.1.4.4 SSC mode 3 298
6.6.1.1.5 How the UE determines the required SSC mode 299
6.6.1.2 Function description 300
6.6.1.2.1 PDU session establishment/release triggered by handover procedure 300
6.6.1.2.2 Service continuity call flows 301
6.6.1.2.3 CN-provided trigger followed by UE-requested PDU Session (SSC mode 3) 301
6.6.1.2.4 CN-prepared PDU Session modification followed by notification to UE (SSC mode 3) 302
6.6.1.2.5 CN-provided trigger followed by UE-requested PDU Session establishment (SSC mode 2) 303
6.6.1.2.6 CN-prepared PDU Session modification followed by notification to UE (SSC mode 2) 303
6.6.1.3 Solution evaluation 304
6.6.2 Solution 6.2: Mobility on Demand using Mobility and Session classes 304
6.6.3 Solution 6.3: Multi-homing over multiple PDU sessions with network-provided routing rules 305
6.6.3.1 Architecture description 305
6.6.3.2 Function description 305
6.6.3.2.1 CN-provided trigger for new UE-requested PDU Session, no mobility case 305
6.6.3.2.2 CN-provided trigger for new UE-requested PDU Session, mobility case 306
6.6.3.3 Solution evaluation 306
6.7 Solutions for Key Issue 7: Network function granularity and interactions between them 306
6.7.1 Solution 7.1: Interconnection and Routing Function (IRF) based network function interconnection model 306
6.7.1.1 General (Assumptions and applicability) 306
6.7.1.2 Architectural description 307
6.7.1.2.1 Reference model 307
6.7.1.2.2 High level principles 308
6.7.1.3 Functional description 308
6.7.1.3.1 General 308
6.7.1.3.2 Functions of Interconnection & Routing Function (IRF) 308
6.7.1.3.3 Sample binding repository of IRF 309
6.7.1.4 Sample call flows 310
6.7.1.4.1 General 310
6.7.1.4.2 Basic routing of message between two NFs 310
6.7.1.4.3 Support for subscribe-notify type of mechanism 311
6.7.1.4.4 NF binding management at IRF 311

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 11 of 501

6.7.1.5 Solution evaluation 311
6.7.2 Solution 7.2: The interconnection of NFs and discovery of NFs via NF Repository Function 311
6.7.2.1 Architecture description 311
6.7.2.2 Function description 312
6.7.2.2.1 General model of Network Function 312
6.7.2.2.3 General model for the interconnection of CP NFs 312
6.7.2.2.4 NF Discovery 313
6.7.2.2.5 NF Monitor 315
6.7.2.3 Solution evaluation 316
6.7.3 Solution 7.3: Interconnection Function Solution 316
6.7.3.1 Architecture description 316
6.7.3.2 Function description 317
6.7.3.3 Solution evaluation 319
6.7.4 Solution 7.4: A Framework of Modular Network Functions 319
6.7.4.1 Reference Model 319
6.7.4.2 Functional Description 319
6.7.4.3 Composition of Network Function 319
6.7.5 Solution 7.5: Control Plane Interconnection model with a Data Layer 320
6.7.5.1 Architecture description 320
6.7.5.1 Reference model 320
6.7.5.2 Architecture principles 322
6.7.5.3 Function description 322
6.7.5.3.1 Data Layer (DL) 322
6.7.5.3.2 Core Control Plane Function (CCF) 323
6.7.5.4 Information exchange across different types of Network functions for capability exposure 324
6.7.5.4.1 Capability Exposure to PCF, CEF 324
6.7.5.5 Information exchange across same types of Network functions 324
6.7.5.5.1 Registration procedure 325
6.7.5.5.2 Handover Procedure 326
6.7.5.5.3 Service Request Procedure 327
6.7.5.5.4 MMF Failover 329
6.7.5.5.5 Context Clean-up scenario 329
6.7.5.5.6 Data Layer and Network slicing 330
6.7.5.6 Stateless Network Function 330
6.7.5.7 Solution evaluation 330
6.8 Solutions for Key Issue 8: Next Generation core and access - functional division and interface 331
6.8.1 Solution 8.1: Solution for Common Core support 331
6.8.1.1 Architecture description 331
6.8.1.2 Function description 332
6.8.1.3 Solution evaluation 332
6.8.2 Solution 8.2: Architecture for decoupling and independent evolution of CN and AN 332
6.8.2.1 Architecture description 332
6.8.2.2 Function description 335
6.8.2.2.1 General 335
6.8.2.2.2 EAP-over-EAPoL transport between UE and WLAN access point 336
6.8.2.2.3 IKEv2 transport between UE and N3ASF 338
6.8.2.2.4 PANA transport between UE and N3ASF 339
6.8.2.3 Solution evaluation 339
6.8.3 Solution 8.3: Alternative A for the interface between UE and Next Generation Core 340
6.8.3.1 Architecture description 340
6.8.3.2 Function description 340
6.8.3.3 Solution evaluation 341
6.8.4 Solution 8.4: Alternative B for the interface between UE and Next Generation Core 341
6.8.4.1 Architecture description 341
6.8.4.2 Function description 342
6.8.4.3 Solution evaluation 342
6.8.5 Solution 8.5: Alternative C for the interface between UE and Next Generation Core 343
6.8.5.1 Architecture description 343
6.8.5.2 Function description 343
6.8.5.3 Solution evaluation 344
6.8.6 Solution 8.6: Architecture for support of untrusted Non-3GPP Access 344
6.8.6.1 Architecture description 344

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 12 of 501

6.8.6.2 Function description 345
6.8.6.2.1 Initial attach procedure for Untrusted N3GPP Access 347
6.8.6.2.2 PDU session establishment via untrusted N3GPP access 350
6.8.6.3 Solution evaluation 351
6.8.7 Solution 8.7: Support standalone non-3GPP access via NG2/NG3 352
6.8.7.1 Architecture description 352
6.8.7.2 Function description 353
6.8.7.2.1 Overview 353
6.8.7.2.2 Protocol architecture for Trusted non-3GPP access 354
6.8.7.2.3 Protocol architecture for Untrusted non-3GPP access 356
6.8.7.2.4 Attach via Trusted Non-3GPP Access 357
6.8.7.2.5 PDU session setup via Trusted Non-3GPP Access 360
6.8.7.2.6 Attach via Untrusted Non-3GPP Access 361
6.8.7.2.7 PDU session setup via Untrusted Non-3GPP Access 363
6.8.7.3 Solution evaluation 363
6.8.8 Solution 8.8: Architecture for support of untrusted Non 3GPP access 363
6.8.8.0 Overview 363
6.8.8.1 Architecture description 364
6.8.8.2 Function description 365
6.8.8.2.1 Initial attach procedure for Untrusted N3GPP Access 368
6.8.8.2.2 PDU session establishment via untrusted N3GPP access 371
6.8.8.3 Solution evaluation 372
6.9 Void 372
6.10 Solutions for Key Issue 10: Policy Framework 372
6.10.1 Solution 10.1: Policy Framework alternative solution 1 372
6.10.1.1 Overall policy architecture 372
6.10.2 Solution 10.2: Analytics-based Policies 373
6.10.2.1 Architecture description 373
6.10.2.2 Functional Description 376
6.10.2.3 Solution evaluation 376
6.10.3 Solution 10.3: Policy function and framework for non-roaming case 376
6.10.3.1 Architecture description 376
6.10.3.2 Function description 378
6.10.3.2.1 Input for Policy Decision 378
6.10.3.3 Solution evaluation 379
6.10.4 Solution 10.4: Policy Reference Architecture 379
6.10.4.1 Overview 379
6.10.4.2 The Policy Function 381
6.10.4.3 The NG Control Plane input to the Policy Function 381
6.10.4.4 The Enforcement of Policy Decisions 381
6.10.4.5 Functions external to NG Control Plane 382
6.10.5 Solution 10.5: Policy function and framework for roaming cases 382
6.10.5.1 Architecture description 382
6.10.5.2 Function description 384
6.10.5.3 Solution evaluation 384
6.10.6 Solution 10.6: Encrypted traffic detection 384
6.10.6.1 General description of the solution 384
6.10.6.2 Procedures For Traffic Authorization and Validation at Flow Setup 384
6.10.6.3 Solution evaluation 385
6.10.7 Solution 10.7: Policy Architecture with CP functional split 385
6.10.7.1 Overview 385
6.10.8 Solution 10.8: Dual Level Policy framework 386
6.10.8.1 Acronyms/definitions 386
6.10.8.2 Architecture descriptions 387
6.10.8.3 Function description 389
6.10.8.4 Solution evaluation 389
6.11 Solutions for Key Issue 11: Charging 389
6.12 Solutions for Key issue 12: Authentication and security framework 390
6.12.1 Solutions 12.1: Authentication and security framework 390
6.12.1.1 Authentication and Security Framework description 390
6.12.1.1.1 Security Architecture 390
6.12.1.1.2 Authentication and Key Agreement 393

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 13 of 501

6.12.1.1.3 User Identity and ME Identity Confidentiality 394
6.12.1.1.4 System Signaling Protection 395
6.12.1.1.5 User Plane Protection 395
6.12.1.2 Solution evaluation 395
6.12.2 Solution 12.2: For security and authentication with Network Slice Support 395
6.13 Void 396
6.14 Void 396
6.15 Void 396
6.16 Void 396
6.17 Solutions for Key Issue 17: 3GPP architecture impacts to support network discovery and selection 396
6.17.1 Solution 17.1: Network discovery and selection in idle mode 396
6.17.1.1 Architecture description 396
6.17.1.2 Function description 398
6.17.1.3 Solution evaluation 398
6.18 Solution for Key Issue 18: Interworking and Migration 398
6.18.1 Solution 18.1 : interworking between NextGen core and EPC 398
6.18.1.1 functional description for interworking 398
6.18.1.2 Solution evaluation 399
6.18.2 Solution 18.2: Solution for interworking 399
6.18.2.1 Architecture description 400
6.18.2.1.1 Architecture for Scenario I1 400
6.18.2.1.2 Architecture for Scenario I2 401
6.18.2.1.2.1 Architecture for the non-roaming and roaming with local breakout scenarios 401
6.18.2.1.2.2 Architecture for the home-routed roaming scenario 402
6.18.2.1.2.3 Signalling flows 402
6.18.2.2 Function description 406
6.18.2.3 Solution evaluation 407
6.18.3 Solution 18.3: Solutions for migration from E-UTRAN/EPC including option 3 to option 2,4,5, or 7 ... 407
6.18.3.1 Architecture description 407
6.18.3.2 Function description 409
6.18.3.3 Solution evaluation 409
6.18.4 Solution 18.4: Solution for interworking and migration 410
6.18.4.1 Architecture description 410
6.18.4.2 Function description 412
6.18.4.3 Solution evaluation 413
6.18.5. Solution 18.5: Solution for full and partial migration scenarios from EPS to NG System 413
6.18.5.1 Architecture for full and partial migration scenarios from EPS to NG System 413
6.18.6 Solution 18.6: Migration solution with Evolved E-UTRAN to operate EPC and NextGen Core simultaneously 415
6.18.6.1 Architecture description 415
6.18.6.2 Function description 417
6.18.6.3 Solution evaluation 417
6.19 Solutions for key issue 19: Architecture impacts when using virtual environments 417
6.19.1 Solution 19.1: Avoiding UE interaction from NF Load Balancing, Scaling and Migration 417
6.20 Solutions for Key Issue 20: 3GPP architecture impacts to support access traffic steering and switching 418
6.20.1 Solution 20.1: Access traffic steering and switching 418
6.20.1.1 Architecture description 418
6.20.1.2 Function description 420
6.20.1.2.1 Steering of a new data flow by the UE 421
6.20.1.2.2 Steering of a DL data flow by the network for a dual radio-capable UE 422
6.20.1.2.3 Switching of an ongoing data flow by the UE 422
6.20.1.3 Solution evaluation 424
6.20.2 Solution 20.2: Solution based on ATSSS Function 424
6.20.2.1 Architecture Description 424
6.20.2.2 Functional Description 425
6.20.2.2.1 Operation Overview 425
6.20.2.2.2 Protocol Architecture 427
6.20.2.2.3 Signalling Flows 428
6.20.2.3 Solution evaluation 431
6.x Solution x - Title 431
6.x.1 Architecture description 431
6.x.2 Function description 431

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 14 of 501

6.x.3 Solution evaluation 431

7 Architecture(s) for the Next Generation System 431
7.1 Consolidated architecture option 1 431
7.1.1 General 431
7.1.2 High level architectural principles 431
7.1.3 Reference architecture 433
7.1.3.1 Non-roaming 433
7.1.3.2 Roaming 433
7.1.3.3 Reference points 434
7.1.4 High level functional description 435
7.2 Consolidated architecture option 2 436
7.2.1 General 436
7.2.2 Non-roaming reference architecture and reference points 436
7.2.3 Roaming reference architectures 438
7.3 Consolidated architecture option 3 439
7.3.1 General 439
7.3.2 Reference architecture 440
7.3.2 Applicable solutions 444
7.3.3 Evaluation 444
7.4 Consolidated architecture option 4 444
7.4.1 Non-roaming reference architecture and reference points 444
7.4.1.1 Communication between Network functions 446
7.4.1.2 Functional Description 447
7.4.2 Roaming architectures 448
7.5 Roaming interface functional distribution 448
7.5.1 Architecture description 448
7.5.1 Function description 450
7.5.1 Solution evaluation 450
7.6 Consolidated architecture option 6 451
7.6.1 General 451
7.6.2 Reference architecture 452
7.6.3 Network functions and reference points 456
7.6.4 Applicable solutions 458
7.6.5 Evaluation 458
7.7 Consolidated architecture option 7 459
7.7.1 General 459
7.7.2 High level principles 459
7.7.3 Reference architecture 460
7.7.4 Network functions and reference points 461
7.7.4.1 Network functions 461
7.7.4.2 Control Plane service interfaces 463
7.7.4.3 Other Reference points 463
7.7.5 Applicable solutions 464
7.7.6 Evaluation 464

8 Conclusions 464
8.1 Interim Agreements on Key Issue #1: Network slicing 464
8.2 Interim Agreements on Key Issue #2: QoS framework 465
8.3 Interim Agreements on Key Issue #3: Mobility management 468
8.4 Interim Agreements on Session management and Service Continuity (Key Issue #4, 5 and 6) 472
8.5 Void 475
8.6 Interim Agreements on Key Issue #6: Support for session and service continuity and efficient user plane path 475
8.7 Interim Agreements on Key Issue #7: Network function granularity and interactions between them 476
8.8 Interim Agreements on Key Issue #8: Next Generation core and access - functional division and interface 477
8.8.1 Interim Agreements on functional split between AN and CN 477
8.8.2 Interim Agreements on common AN-CN interface 479
8.9 Interim Agreements on Congestion and Overload Control 480
8.10 Interim Agreements on Key Issue #10: Policy Framework 480
8.11 Interim Agreements on Key Issue #18 480

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 15 of 501

8.11.1 Interim Agreements on EPC-NextGen Core interworking 480
8.11.2 Interim Agreements on option 3 to NG Core migration 481
8.12 Interim Agreements on the Overall Architecture 481
8.12.1 Architecture principles 481
8.12.2 Non-roaming reference architecture and reference points 481

Annex A: Key technical areas identified for investigation during the study 483

Annex B: Network slicing concept by NGMN 484

B.1 Network slicing concept 484

B.2 Definitions 484

Annex C: Work planning for NextGen Study Item on how to focus Rel-14 study 486

Annex D: Potential solution scenarios for support of multiple slices per UE 487

Annex E: Guidelines for specifying procedures, to allow its re-use 489

E.1 Specifying a procedure 489
E.1.1 As a service 489
E.1.2 Authorization 489

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 16 of 501

E.2 Procedure of a network function: independent, non-overlapping of each other 489
E.3 Procedure of the system: As a sequence of network function level procedures....489
Annex F: Minimizing access dependencies in the NextGen Core and AN - CN Interface....490
F.1 QoS....490
F.2 Authentication....490
F.3 Charging Framework....490
F.4 Policy Framework....490
F.5 Session Continuity....490
F.6 Session Management....490
F.7 Mobility Management....490
F.8 Minimization of Access dependencies and CP/UP functional split....491
F.9 Carrying of Access Specific information over AN-CN interface....491
Annex G: Reference point naming....492
Annex H: Support of edge computing....493
Annex I: Guidelines for defining network function granularity....494
I.1 General....494
Annex J: Deployment Scenarios....496
J.1 General....496
J.2 Deployment Option 2 - Standalone NR in NextGen System....496
J.3 Deployment Option 3 - Non-standalone NR in EPS....497
J.4 Deployment Option 4 - Non-standalone Evolved E-UTRA in NextGen System....497
J.5 Deployment Option 5 - Standalone Evolved E-UTRA in NextGen System....497
J.6 Deployment Option 7 - Non-standalone NR in NextGen System....498
Annex K: Change history....499

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 17 of 501

Foreword

This Technical Report 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.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 18 of 501

1 Scope

The objective is to design a system architecture for the next generation mobile networks. The new architecture shall support at least the new RAT(s), the Evolved E-UTRA, non-3GPP accesses and minimize access dependencies.

Proposals for the new architecture can be based on an evolution of the current architecture or based on a "clean slate" approach.

The study shall consider scenarios of migration to the new architecture.

The expected work will include:

- Investigation of high-level architectural requirements.
- Definition of the terminology to be used as common language for architecture discussions.
- Definition of the high-level system architecture as the collection of required capabilities, and high level functions with their interactions between each other.

The complete or partial conclusions of this study will form the basis for the normative work and/or for any further study.

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

[3] 3GPP TS 23.203: "Policy and charging control architecture".

[4] 3GPP TR 22.861: "Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things; Stage 1".

[5] 3GPP TR 22.862: "Feasibility Study on New Markets and Technology Enablers - Critical Communications; Stage 1".

[6] 3GPP TR 22.863: "Feasibility Study on New Services and Markets Technology Enablers - Enhanced Mobile Broadband; Stage 1".

[7] 3GPP TR 22.864: "Feasibility Study on New Services and Markets Technology Enablers - Network Operation; Stage 1".

[8] NGMN Alliance: "Description of Network Slicing Concept", Version 1.0, January 13, 2016 (http://www.ngmn.org/publications/technical.html).

[9] 3GPP TR 22.891: "Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)".

[10] 3GPP TR 38.913: "Study on Scenarios and Requirements for Next Generation Access Technologies".

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 19 of 501

[11] SP-160464/RP-161266, "5G Architecture Options- Full Set". Joint RAN/SA Meeting, Busan, S. Korea, June 2016.

[12] SP-160460/RP-161269, "Tasks", Joint RAN/SA Meeting, Busan, S. Korea, June 2016.

[13] 3GPP TR 38.801: "Study on New Radio Access Technology; Radio Access Architecture and Interfaces".

[14] IETF RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)".

[15] IETF RFC 5191, "Protocol for Carrying Authentication for Network Access (PANA)".

[16] 3GPP TR 33.899: "Study on the security aspects of the next generation system".

[17] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses; Stage 2".

[18] 3GPP TS 23.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 2".

[19] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[20] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[21] 3GPP TS 36.413: "Evolved Universal Terrestrial Access Network (E-UTRAN); S1 ApplicationProtocol (S1AP)".

3 Definitions 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].

Access Traffic Steering: The procedure that selects the "best" access network for a new data flow and transfers the traffic of this data flow over the selected "best" access network. The selection of the "best" access network is typically based on criteria such as the network load, the measured radio signal quality, the application associated with the data flow, etc. Access traffic steering is applicable between 3GPP and non-3GPP accesses.

Access Traffic Switching: The procedure that moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. Access traffic switching is applicable between 3GPP and non-3GPP accesses.

Access Traffic Splitting: The procedure that splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access. Access traffic splitting is applicable between 3GPP and non-3GPP accesses.

Evolved E-UTRA: RAT that refers to an evolution of the E-UTRA radio interface for operation in the NextGen system.

Network Capability: Is a network provided and 3GPP specified feature that typically is not used as a separate or standalone "end user service", but rather as a component that may be combined into a telecommunication service that is offered to an "end user".

NOTE 2: For example, the location service is typically not used by an "end user" to simply query the location of another UE. As a feature or network capability it might be used e.g. by a tracking application, which is then offering as the "end user service". Network capabilities may be used network internally and/or can be exposed to external users, which are also denoted a 3rd parties.

Network Function: In this TR, Network function is a 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 20 of 501

NOTE 3: A network function can be implemented either as a network element on a dedicated hardware, or as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

Network Slice Template (NST): is a logical representation of the Network Function(s) and corresponding resource requirements necessary to provide the required telecommunication services and network capabilities.

Network Slice Instance (NSI): is an instance created from a Network Slice Template (NST).

Network Slice: is a concept describing a system behaviour which is implemented via Network Slice Instance(s).

NextGen: Next generation used in the context of the present document.

NextGen Core Network: A core network specified in the present document that connects to a NextGen access network.

NextGen RAN (NG RAN): In the context of this document, it refers to a radio access network that supports one or more of the following options:

2) Standalone New Radio,

4) Standalone New Radio is the anchor with Evolved E-UTRA extensions,

5) Evolved E-UTRA,

7) Evolved E-UTRA is the anchor with New Radio extensions.

with the common characteristics that the RAN interfaces with the next generation core.

NOTE 6: NG RAN Options 2, 4, 5 and 7 are documented in the Annex J of this TR.

NextGen Access Network (NG AN): It refers to a NextGen RAN or a Non-3GPP access network and interfaces with the next generation core.

NextGen System (NG System): It refers to NextGen system including NextGen Access Network (NG AN)and NextGen Core.

NextGen UE: A UE connecting to a NextGen system.

Non Geostationary Satellites: (LEO and MEO) circle around the Earth with a period that varies between 1.5 hour and 10 hours. A constellation of NGSO satellite associated with handover mechanisms are necessary to ensure to service continuity.

PDU Connectivity Service: A service that provides exchange of PDUs between a UE and a data network .

PDU Session: Association between the UE and a data network that provides a PDU connectivity service. The type of the association includes IP type, Ethernet type and non-IP type.

PDU Session of IP Type: Association between the UE and an IP data network.

Service Continuity: The uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point changes.

Session Continuity: The continuity of a PDU session. For PDU session of IP type "session continuity" implies that the IP address is preserved for the lifetime of the PDU session.

Satellite: a platform integrating a transparent repeater or a telecommunication transmitter, placed into Low-Earth Orbit (LEO) typically at an altitude between 500 km to 2000 km, Medium-Earth Orbit (MEO) typically at an altitude between 8000 to 20000 km, or Geostationary-satellite Earth Orbit (GEO) at circa 35 786 km altitude.

UE Reachability Management: UE Reachability Management: It relates to reachability detection and tracking of UEs in idle mode state.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 21 of 501

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 term, if any, in TR 21.905 [1].

AF	Application Function
AS	Application Server
AS	Access Stratum
CIoT	Cellular Internet of Things
CP	Control Plane
CriC	Critical Communications
DRX	Discontinuous Reception
eMBB	Evolved Mobile Broadband
eMBMS	Evolved Multicast/Broadcast Service
FQDN	Fully Qualified Domain Name
GEO	Geostationary satellite Earth Orbit
IoT	Internet of Things
LEO	Low Earth Orbit
MBB	Mobile Broadband
MEO:	Medium Earth Orbit
mIoT	Massive IoT
MTC	Machine Type Communication
NF	Network Function
NG	NextGen
NGC	NextGen Core
NGS	NextGen System
NGSO	Non Geostationary Satellite Orbit
NG AN	NextGen Access Network
NG CN	NextGen Core Network
NG RAN	NextGen RAN
NG System	NextGen System
NG UE	NextGen User Equipment
NR	New Radio
NSA NR	Non-Standalone New Radio
NST	Network Slice Template
NSI	Network Slice Instance
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PGW	Packet Gateway
QoE	Quality of Experience
SA NR	Standalone New Radio
SDN	Software Defined Network
SDS	Small Data Service
SGW	Serving Gateway
UP	User Plane

4 Architectural Requirements, Assumptions and Principles

4.1 High level Architectural Requirements

Editor's note: This clause will document high-level architectural requirements that guide the architecture study.

The architecture of the NextGen System shall:

1 Support the new RAT(s), the Evolved E-UTRA, and non-3GPP access types. GERAN and UTRAN are not supported:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 22 of 501

a) As part of non- 3GPP access types, WLAN access (including "untrusted WLAN" according to the meaning defined in pre Rel. 14 for the term "untrusted") and Fixed access shall be supported. Support for satellite access is FFS.

b) Satellite radio access network (3GPP and non 3GPP defined) shall be supported (for phase 2)

c) The support of Satellite radio access network (3GPP defined) will be studied in conjunction with RAN activities.

2 Support unified authentication framework for different access systems.

3 Support multiple simultaneous connections of an UE via multiple access technologies.

4 Allow independent evolutions of core network and RAN, and minimize access dependencies.

5 Support a separation of Control plane and User plane functions.

6 Support transmission of IP packets, non-IP PDUs and Ethernet frames.

NOTE 1: This requirement assumes a point-to-point link between the UE and the data network.

7 Leverage techniques (e.g. Network Function Virtualization and Software Defined Networking) to reduce total cost of ownership, improve operational efficiency, energy efficiency, and simplicity and flexibility for offering new services.

8 Efficiently support different levels of UE mobility (including stationary UE(s)) / service continuity.

9 Support different levels of resilience for the services provided by the network.

10 Support different means for reducing UE power consumption while UE is in periods with data traffic as well as in periods without data traffic.

11 Support services that have different latency requirements between the UE and the Data Network.

12 Minimize the signalling (and delay) required to start the traffic exchange between the UE and the Data Network, i.e. signalling overhead and latency at transition from a period where UE has no data traffic to a period with data traffic.

13 Support access to applications (including 3rd party applications) with low latency requirements hosted close to the access network within the operator trust domain.

NOTE 2: The details of applications are beyond the scope of 3GPP.

NOTE 3: Details of hosting of applications is considered beyond scope in this release.

14 Support optimized mechanisms to control (includes avoiding) signalling congestion.

15 Efficient network support for a large number of UEs in periods without data traffic.

16 Support network sharing.

17 Support roaming:

a) As part of roaming, the architecture shall support both routing of user traffic entirely via the VPLMN and routing of the user traffic back to the HPLMN.

18 Support broadcast services.

19 Support network slicing.

20 Support Architecture enhancements for vertical applications.

21 Support dynamic scale-in /scale-out.

22 Minimize energy consumption in the overall network operation.

NOTE 4: Specific architecture work resulting from the previous requirement may have to be addressed by SA WG2, SA WG5, or both.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 23 of 501

23 Support critical communications, including mission-critical communications.

24 Support network capability exposure

25 Support efficient transmission of user data with characteristics required by Stage 1 requirements (e.g. low throughput short data bursts) including support of SMS.

26 Support regulatory requirements for Lawful Intercept.

27 Support a flexible information model with relationships between user related managed data, and with a level of abstraction sufficient to be independent of any specific protocols.

NOTE 5: The previous requirement may have to be addressed by SA WG2, SA WG5, or stage 3 working groups.

28 Support optimized distribution of the data and the location of the data repositories in the network (access and core network) for efficient management of user related data by network entities.

29 Support for location services as per the related service requirements and in alignment with NR RAN TR 38.913 [10].

30 Support regulatory requirements for Public Warning System (PWS), e.g. ETWS, CMAS, KPAS, etc.

4.2 Architectural Assumptions

Editor's note: This clause will document the identified common architecture assumptions during the study. The assumptions refer to items (e.g. architecture shall define RAN - core functional split) that must be fulfilled by the new architecture.

Editor's note: The terminology in this clause is reused from Architecture requirement 1 in clause 4.1. This terminology should be aligned throughout the TR once RAN terminology is defined by e.g. RAN WGs.

1 The functional split between NextGen core and access network shall be defined with support for the new RAT(s), the Evolved E-UTRA and non-3GPP access types.

2 A NextGen Core-NextGen RAN interface supporting new RAT(s) and the Evolved E-UTRA shall be specified.

3 The method how the NextGen UE interfaces with the NextGen Core - if any - is FFS. Regardless whether the UE is connected to either or both of the new RAT(s) and the Evolved E-UTRA, the number of NextGen UE - NextGen Core signalling association - if they exist in the final solution - is not impacted.

Editor's note: Whether the number of UE - NextGen Core signalling association is impacted when a UE is connected to multiple network slices (possibly involving multiple RATs), and/or non-3GPP access, is FFS.

4 It shall be possible to verify that the UE is allowed to access a specific network slice.

5 The life cycle management of network slice instances and network function instances are assumed to be within the scope of SA5.

6 When the UE is in CN_IDLE state, the UE location is known at the TA level granularity, as in EPC.

4.2.1 Initial High level architectural view

This clause shows the high level architecture that can be used as a reference model for this study. Figure 4.2.1-1 shows the NextGen UE, NextGen(R)AN, NextGen Core and their reference points.

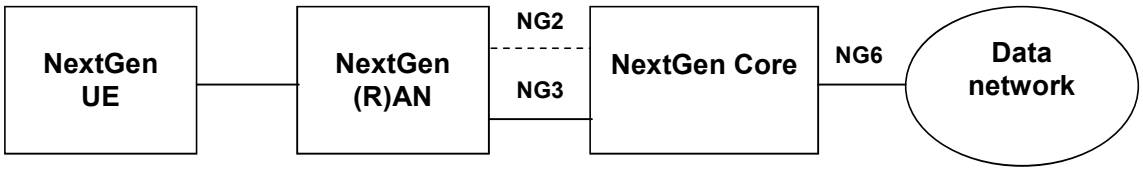


Figure 4.2.1-1: Initial High level architecture view for NextGen System

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 24 of 501

Editor's note: If, and possibly how, the NextGen UE interfaces with the NextGen Core is FFS.

4.2.2 Reference points

NG2: Reference point for the control plane between NextGen (R)AN and NextGen Core.

NG3: Reference point for the user plane between NextGen (R)AN and NextGen Core.

NG1: Reference point for the control plane between NextGen UE and NextGen Core.

NG6: It is the reference point between the NextGen Core and the data network. Data network may be an operator external public or private data network or an intra-operator data network, e.g. for provision of IMS services. This reference point corresponds to SGi for 3GPP accesses.

4.3 Architectural Principles

Editor's note: This clause will document the identified architecture principles during the study. This clause provides the guiding principles (e.g. establishing a session on demand for IoT devices, support for non-IP connectivity), key drivers for the architecture.

- The UE may be attached to the network without having an established session for data transmission.
- The number of reference points between the UE and the NextGen Core Network for the control plane over a single RAN should be minimized, independently of the functional composition of the control plane CN functionality.

5 Key Issues

NOTE: All the key issues are assumed to adhere to the list of architectural requirements, assumptions and principles in clause 4 and therefore these requirements, assumptions and principles are not repeated as part of the key issue descriptions.

5.1 Key issue 1: Support of network slicing

5.1.1 Description

Network slicing enables the operator to create networks customised to provide optimized solutions for different market scenarios which demands diverse requirements, e.g. in the areas of functionality, performance and isolation.

Solutions for this key issue will study:

- Functionality and capabilities within 3GPP scope that enables the next generation system to support the Network Slicing and Network Slicing Roaming requirements defined in TR 22.864 [7] and in normative stage 1 specifications (when available), including but not limited to:
  - How to achieve isolation/separation between network slice instances and which levels and types of isolation/separation will be required;
  - How and what type of resource and network function sharing can be used between network slice instances;

NOTE: Details of which resources are meant and how they relate to the 3GPP architecture is to be clarified as part of the solutions to the key issue.

- How to enable a UE to simultaneously obtain services from one or more specific network slice instances of one operator;
- What is within 3GPP scope with regards to Network Slicing (e.g. network slice creation/composition, modification, deletion);
- Which network functions may be included in a specific network slice instance, and which network functions are independent of network slices;
- The procedure(s) for selection of a particular Network Slice for a UE;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 25 of 501

- How to support Network Slicing Roaming scenarios; and
- How to enable operators to use the network slicing concept to efficiently support multiple 3rd parties (e.g. enterprises, service providers, content providers, etc.) that require similar network characteristics.

The required definitions and terminology will be agreed upon during the work, e.g. adopting any terminology and definitions from SA1, NGMN etc. Additional input from e.g. NGMN or other industry organisations on Network Slicing will be considered.

5.1.2 Work Tasks

Table 5.1.2-1: Work Tasks for Network Slicing

Work Task ID	Work Task(s)	Work Task Description
NS_WT_#1	Network Slice Instance Selection and Association	1) Initial network slice instance selection to support UE's service establishment and re-selection to support UE mobility and other scenarios that are TBD, Note: More scenarios beyond the mobility need to be identified that may trigger network slice instance re-selection. 2) Network slice instance identification, 3) authorization for UE association with network slice instance Network provided and UE provided assistance information support for network slice instance selection.
NS_WT_#2	Network Slicing Isolation	1) Security isolation 2) Resource isolation 3) OAM support isolation (e.g. Usage and Fault isolation etc.) Note: Whether all items listed here are within the scope of SA2 is FFS.
NS_WT_#3	Network Slicing Architecture	1) Identifying impacted network functions and interfaces to support one or more network slice instances on top of a shared RAN and a shared infrastructure. 2) Identifying the common functions (if any) that need to be available in the core network and/or RAN to enable network slicing Identifying the approach to enable UE to associate with multiple slices simultaneously.
NS_WT_#4	Network Slicing Roaming support	1) Determination what visiting and home Network Function(s) are required to support roaming.
NS_WT_#5	Network Slicing terminology & definitions	1) If Network Slice Instance is agreed to apply E2E system, then, we should consider new terminology for Access slice instance and Core slice instances.

5.2 Key issue 2: QoS framework

5.2.1 Description

This key issue should study the QoS framework for the system architecture i.e. the required functions (in both CP and UP) and a functional split between UE, Access Networks and CN, and any necessary QoS related signalling between those functions. The QoS framework should enable the operator to provide QoS for the wide range of use cases is expected to be fulfilled by the NextGen architecture.

The architecture should support QoS in such a manner that it fulfils the following principles:

- Solution for QoS framework should allow ease of reuse of Next Generation core for various access technologies (i.e. 3GPP access, non-3GPP access).
- Solution for QoS framework should allow independent evolution of core and access technologies (i.e. 3GPP access, non-3GPP access).
- Solution for QoS framework within NextGen core network is not access specific.
- Solution for QoS framework enables optimal service level quality as per application needs, optimizing network capacity utilization.

Editor's note: There may be interactions with key issue on network capability exposure (i.e. QoS for 3rd party applications).

- A QoS framework that can provide adequate QoS handling for:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 26 of 501

- Services whose characteristics have been explicitly provided to the 3GPP system (e.g. via Rx interface).
- Services/applications whose characteristics have been explicitly deduced by the 3GPP system.
- Services whose characteristics have been implicitly deduced by the 3GPP system (e.g. by subscription).
- Applications with non-deducible service data flows.

Solution for QoS framework should identify proper QoS granularities (e.g. per-UE, per-flow) and QoS parameters (e.g. maximum bit rate, guaranteed bit rate, priority level).

Editor's note: The need and the solutions for inter system change between NextGen and EPS are expected to be studied in other key issues, e.g. those on migration and coexistence with legacy systems. Depending on the outcome of interworking, QoS mapping between NextGen and EPS QoS framework should be specified.

- Solution for QoS framework should be able to support E2E QoS control (i.e. it should consider QoS control in RAN, CN, and transport network).

In terms of description the candidate solutions should clarify the following items:

- Functions: the required functions (including both CP and UP) and a functional split between UE, Access Networks and CN.
- Functional entities: indication of QoS control points, QoS enforcement points and the associated reference points.
- QoS model: how is QoS handled on each reference point (e.g. per packet, per flow, aggregation of flows etc.).
- QoS characteristics: the list of parameters (e.g. maximum bit rate, guaranteed bit rate, priority level) needed for the QoS framework.
- QoS related information exchange: how is QoS information conveyed to entities where it is enforced (e.g. to UE, to RAN, or to user plane gateways).
- Traffic identification: how is traffic identified (e.g. means beyond traffic identification based on L3/L4 information such as the IP-5-tuple for IP traffic) at the various QoS provisioning/enforcement points and at what level (e.g. per packet, per flow or as an aggregate of flow etc.) for both uplink and downlink direction? How is traffic identified at the UE for both uplink and downlink direction?
- Traffic separation: how is traffic separation achieved (in the core as well as on the CN-RAN interface) for QoS treatment; solutions shall also clarify the granularity of the traffic separation.

It should be noted that the items listed above are not exhaustive.

5.2.2 Work Tasks

Table 5.2.2-1: Work tasks for QoS framework

Work Task ID	Work Task(s)	Work Task Description
QoS_WT_#1	QoS parameters, i.e. how to describe the authorised treatment of the data traffic	1.1 Which QoS parameters may be used to describe the delivery of PDUs in the NextGen system and what is the traffic granularity on which these parameters apply (e.g. service data flow, PDU Session, UE, etc.)? NOTE 1: Clarify if GBR is part of the QoS parameters. NOTE 2: The QoS parameters describe the expected traffic handling provided by the NextGen system to a specific user data traffic flow in terms of priority, pre-emption, latency, error rate, etc.
QoS_WT_#2	How the application layer may request a specific treatment of the traffic	2.1 What are the parameters and procedures used to describe the application QoS requirements? NOTE 3: The term "application" here refers to the AF or to the application client in the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 27 of 501

QoS_WT_#3	How to distribute the QoS parameters describing the authorised treatment of the data traffic	3.1 Is QoS information signaled on each of the reference points in the architecture assumed for a given solution and how: - e.g. per Layer-3 aggregate (flow), per Layer-2 aggregate, per application, other? - which QoS parameters, and for which direction (UL, DL, both)? - for which type of traffic (e.g. traffic authorised via NG5, traffic authorised by subscription, etc.)? NOTE 4: If there is a need for multiple UP function(s) (thus multiple reference points from CP functions to multiple UP functions instances), clarify how many instances are needed in a non-roaming scenario and clarify the functional differences between them (if any). NOTE 5: There is no assumption that C-plane signaling is needed to support QoS of all types of traffic.
QoS_WT_#4	How to associate the authorised QoS treatment to User Plane data traffic	4.1 Is per-PDU marking used over RAN-CN interface and how? - What information is contained in the marking? - How is it determined by the sending side (CN or RAN)? - How is it used by the receiving side (RAN or CN)? (feel free to make assumptions about the QoS services provided by RAN) 4.2 How is a service data flow associated to a per-PDU marking? NOTE 6: there is no assumption that U-plane marking is needed to support QoS of all types of traffic.
QoS_WT_#5	Non-3GPP access	5.1 Describe how the QoS framework applies to non-3GPP access
QoS_WT_#6	Support for Non-IP PDU	6.1 Describe how QoS for non-IP PDUs is supported: - What is the granularity used for QoS differentiation? - How are non-IP PDUs identified for differentiated QoS (if any) within a PDU Session?
QoS_WT_#7	Roaming, interworking and migration	7.1 How is QoS supported in roaming, interworking and migration scenarios. Further details are FFS.
QoS_WT_#8	Alignment with Policy Framework and Charging	8.1 Check overall QoS solution compatibility with solutions studied in key issue #10 (Policy Framework) and key issue #11 (Charging)
QoS_WT_#9	GBR traffic	9.1 How is "GBR traffic" handled? NOTE 7: "GBR traffic" refers to traffic that is traditionally first subject to admission control, after which it is handled in a way that guarantees that no congestion-related packet drops will occur under any system load, as long as the offered traffic remains within its GBR envelop.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 28 of 501

5.3 Key Issue 3: Mobility management framework

5.3.1 Description

This key issue will look into proposing solutions for a Mobility Management (MM) framework that enables the operator to provide mobility support which, if needed, includes session continuity for all types of UEs that connect to the NextGen core via 3GPP accesses and/or non-3GPP accesses. The MM framework in the NextGen system will support mobility on demand concept (see TR 22.861 [4]). This key issue will attempt at developing a comprehensive MM framework for the NextGen system that is adaptive, flexible and intelligent, to cater for the disparate NextGen mobility requirements.

The solutions should define the level of mobility support for a UE (see TR 22.864 [7]), describe how and when the level of mobility is determined, and evaluate the benefits achieved as a result of the mobility on demand concept.

Solutions for this key issue will at least study:

- Mobility management signalling for:
  - UE/User registration to the network;
  - Support of reachability to enable mobile terminated communication;
  - Detection of UEs no longer reachable;
  - Assignment of CP and UP network functions (as needed); and
  - Mobility Restrictions, e.g. forbidding mobility at certain locations.

Editor's note: It is FFS whether aspects related to support of Geographical Location Services (e.g. to support stage 1 requirements for high positioning accuracy) is to be included in this key issue or in a separate key issue.

- Definition of mobility states and how to transition between the states.

NOTE: Defining the mobility states will be performed together with the RAN working groups.

- How to support mobility on demand for different mobility levels. Possible examples for support of different mobility levels support are:
  - Supported over a given area within a single RAN node (such as a cell of an eNodeB).
  - Supported within a single RAN node (such as an eNodeB).
  - Supported in a UE registration area (such as a TA in EPC).
  - Supported in the service area of a control plane or user plane CN entity (such as an MME pool area or a Serving GW service area in EPC).
  - Supported within a given RAT or combination of RATs integrated on the RAN level (such as LTE and 5G RAT).
  - Supported between two access technologies.

NOTE: Study on mobility limitations in RAN will be performed together with RAN working groups.

- How to determine the level of UE mobility support, e.g. by what characteristics/method, which criteria; and
- How to obtain the information (e.g. application's needs, device UE capabilities, used services) in order to determine the appropriate UE mobility level.
- How to enable operators to update the level of mobility support provided for UE, e.g. during session management procedures?
- Methods to limit the amount of mobility management signalling between NextGen core and the access, within the NextGen core as well as between the NextGen core and the UE;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 29 of 501

- How to efficiently control CP signalling for mobility management in case of congestion and/or overloaded situation, including:
  - studying with which granularity (e.g. per UE, per group, per network slice) CP signalling can be controlled; and
  - studying the interaction with access control functionality to prioritize the services by the operator's policy.
- Mobility support in interworking and network migration scenarios;
- How to support mobility between different access systems, including:
  - between 3GPP accesses (the level of interworking between 3GPP accesses i.e. seamless mobility or not is being defined by Stage 1 requirements);
  - between 3GPP accesses and non-3GPP accesses;
  - between non-3GPP accesses; and
  - studying the location of the mobility anchor point(s) (i.e. mobility anchor point includes UP network function and CP network function for mobility) and the use of mobility anchor point(s) for inter and intra access system(s) change due to user mobility (e.g. the study of buffering for idle mode UE, if applicable).
  - The impacts of other architectural features (e.g., separation of control and user planes, QoS concepts) on the mobility management.

5.3.2 Work Tasks

Table 5.3.2-1: Work tasks for Mobility Management

Work Task ID	Work Task(s)	Work Task Description
MM_WT_#1	Access control	1. Access control, when the UE registers with the network for obtaining services from the network, considering service, roaming, RAT restrictions. Access/RAT steering. UE and network capability handling. 2. Registration state model. NOTE: this WT may also be applicable for non-3GPP access.
MM_WT_#2	UE reachability management	1. Means for reaching the UE to enable mobile terminated communication, specifically during the various power saving means, like DRX or idle mode 2. Connection state model 3. Detection of UEs no longer reachable
MM_WT_#3	UE Mobility levels	1. What type of resources will be saved both on the network and the UE? 2. Define the different UE mobility levels (e.g. high, medium, low, or none) to be supported on the NextGen system. 3. How to determine the level of mobility support required e.g. by what characteristics/method, which criteria, and how to transition between different levels? 4. How to obtain the information in order to determine the appropriate UE mobility level? 5. What criteria will be used to transition between the different mobility levels? 6. How to save resources for UEs that do not require full mobility? 7. How to enable operators to update the level of mobility

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 30 of 501

		support provided for UE? NOTE: There may be interactions with the RAN working groups.
MM_WT_#4	Connected mode mobility and assignment of CP and UP network functions (as needed) and a related MM procedure	1.MM procedure should apply for the following scenarios: 1) for intra-RAT 2) for inter-RAT 3) Between 3GPP and non-3GPP access 2. What criteria will be used to determine mobility anchor point selection during the handover procedure? NOTE: This work task is intended to specify the solution for connected mode mobility procedure and also specify the selection criteria for mobility anchor. 3. The need for a user-plane mobility anchor separate from the terminating user-plane function (PDU session anchor) and the need to re-assign it during the handover procedure. NOTE: The need to re-assign UP functions during a handover also depends on the conclusions of key issues 4, 5 and 6).
MM_WT_#5	Mobility support in interworking and network migration scenarios	1. How and what level of mobility support be provided when UE moves to other networks? This work task is about interworking.
MM_WT_#6	Mobility between different access systems	1. What level of mobility interworking will be provided between 3GPP and non-3GPP accesses (i.e. seamless mobility or not)?
MM_WT_#7	Addressing and identifiers for MM	1. Addressing and identifiers necessary for MM. NOTE: This has dependency on other MM work tasks above.
MM_WT_#8	Non-3GPP access	1. Support for non-3GPP related MM.

5.4 Key issue 4: Session management

5.4.1 Description

The session management is responsible for the setup of the IP or non-IP traffic connectivity for the UE as well as managing the user plane for that connectivity. Scenarios and mechanism, which may not require the session to be established, e.g., to provide efficient support for infrequent small user data transmission, will also be investigated.

Solutions to this key issue will study the following aspects related to session management:

- Session management model, including:
  - describe UE related states and high-level procedures between the UE, AN and CN for session management, including establishing, maintaining and terminating both UE non-IP connectivity and IP connectivity in the NextGen system architecture.
  - how sessions are established on-demand instead of by default when attaching to the network.
  - session connection model, including identifying user plane functionality needed to provide IP and non-IP connectivity (e.g. IP anchor, tunnelling, etc.).
- How session management work for UEs connected via multiple accesses, multiple connectivity, and/or multiple transport paths, including providing multiple simultaneous traffic connectivity for the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 31 of 501

- How to control CP signalling for session management between the UE and CN with certain granularity, studying on which additional basis needs to be considered to control CP signalling for the various PDU session scenarios.
- Identify the correlation between session management and mobility management functionality, including:
  - studying whether separation of session management and mobility management is possible, and
  - identifying the interactions between session management and the mobility framework required to enable the various mobility scenarios (including those where efficient user plane path, as defined in TR 22.864 [7] clause 5.1.2.2, is used) while minimizing any negative impact on the user experience.
- Describe how the session management and mobility management can be decoupled for scenarios requiring it, if identified feasible as above.
- Investigate solutions to coordinate the relocation of user-plane flows with the relocation of applications (hosted close to the point of attachment of the UE) due to the mobility of users.

NOTE: The actual relocation of applications is considered beyond scope of 3GPP in this Release.

- Investigate solutions to optimally support intermittent connections due to unreliable links or energy saving strategies.

Solutions to this key issue will also study the following aspects related to transfer infrequent small user data with minimal signalling, including:

- How to efficiently transmit and receive infrequent small amounts of data and short data bursts through the Next Generation System, including studying whether sessions need to be established to enable such services.
- The solutions should allow for unidirectional transmission (i.e. uplink or downlink only transmission), efficient security mechanisms depending on user and/or operator needs, different options for addressing, charging, policing, inter-operator interworking.

5.4.2 Work Tasks

Table 5.4.2-1: Work tasks for Key Issue #4

Work Task ID	Work Task(s)	Work Task Description
SM_WT_#1	SM model	High-level functions definition and allocation (forwarding, address allocation, UP selection…)
		- PDU session type: support IP and non-IP connection - Identifier: for DN and PDU session (e.g., reconsider whether to use APN or not)
		Basic procedures: on-demand SM setup, roaming/non-roaming support; Session maintenance (release, deactivation…) and related UE state change; UP function selection
		UP protocol or model, e.g., - Identify UP functionalities needed to provide IP and non-IP PDU session (e.g. IP anchor, tunnelling, etc.) - Whether to simplify/remove tunnel if no mobility/session continuity support;
		Support multi-PDU sessions to the same DN and different DN
SM_WT_#2	Relation between SM and MM	SM and MM interactions, if any. (NOTE: refer to the KI# 4 for detailed description)
SM_WT_#3	Efficient infrequent small data transfer	Send and receive infrequent small amounts of data, including studying whether sessions need to be established to enable such services - Allow for unidirectional transmission (i.e. uplink or downlink only) - Efficient security mechanisms, different options for addressing, charging, policing, inter-operator interworking
SM_WT_#4	User plane flow relocation	Coordinate the relocation of user-plane flows with the relocation of applications (hosted close to the point of attachment of the UE) due to the mobility of users
SM_WT_#5	PDU sessions via different accesses	UE connected via multiple accesses, including non-3GPP Identify the architecture options for the following cases; - Multiple PDU sessions via different accesses - A single PDU session via different accesses (a.k.a. multi-access PDU session) (NOTE: the way to move IP flows between AN1 and AN2 depends on Key issue#20.)

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 32 of 501

5.5 Void

5.6 Key issue 6: Support for session and service continuity and efficient user plane path

Editor's note: This clause will identify key architectural issues and the corresponding candidate solutions during the design of the next generation system architecture.

5.6.1 Description

In order to address the specific needs of different applications and services, the next generation system architecture for mobile networks should support different levels of data session continuity based on the Mobility on demand concept of the Mobility framework defined in Key Issue 3 or service continuity. For example, the next generation system may do one of the following on per session basis for the same UE:

- support session continuity.
- not support session continuity.
- support service continuity when session continuity is not provided.

See Key Issue 3 for examples on the different levels of mobility support, where these levels also may apply to session continuity.

TR 22.864 [7] (SMARTER NEO) has several requirements for efficient user plane paths. These requirements apply to communication between UEs attached to the same network, between a UE and a host in the Internet, and between a UE and a service providing entity residing close to the network edge.

This key issue will study solutions for selection of anchor point to achieve efficient user plane path, as well as enablement of reselection of anchor point to achieve efficient user plane path with minimum service interruption. A possible cause for user-plane path reselection can be UE mobility causing the current user plane path to become inefficient.

The purpose of this key issue is to study additional aspects such as:

- The types of sessions to be considered in the context of session continuity;
- The level of session continuity to be supported depending on e.g. the type of service such as broadband, group communications, mission critical communications, etc.;
- Reducing the level of session continuity in some areas where QoE requirements are relaxed to meet deployment constraints, e.g. extreme rural deployments requiring maximal cost effectiveness and minimal energy consumption.
- How the next generation system determines the level of session continuity support for a new session;
- How it can be possible to apply one level of session continuity support for some sessions in a UE while, at the same time, apply a different level of session continuity for other sessions in the same UE; and
- How to provide service continuity when session continuity is not provided (e.g. when the user-plane anchor for a UE is relocated). This includes identifying whether upper-layer service continuity mechanisms (e.g. SIP, MPTCP, SCTP, Host ID, DASH, etc.) are applied for a session and how to leverage or interact with such mechanisms.
- How to identify traffic for which (re)selection of efficient user plane path is needed.
- When the previous path becomes inefficient or not able to meet the latency requirement of the UE's service, reselection of user-plane path(s) between a UE and the communication peer(s) which could be
  - other UE(s) attached to the same network.
  - outside of the mobile network (e.g. Internet hosts).
  - a service hosting entity residing close to the edge (including the radio access network).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 33 of 501

5.6.2 Work Tasks

The following list of work tasks has been identified for key issue 6.

Table 5.6.2-1 Work tasks for key issue 6 Session and Service Continuity and efficient user plane path

Work Task ID	Work Task(s)	Work Task Description
SSC_WT_#1	Identify the traffic and the types of session continuity	Identify the types of session continuity to be supported in NextGen Document assumptions/impact on how to convey continuity types as part of SM signaling. Identification of traffic needing efficient user plane path (re)selection
SSC _WT_#2	How the UE and the system determine the type of session continuity support for a new session	Clarify how for example session continuity types can be controlled by subscription (including based on UE request or solely based on subscription) Clarify how the UE determines the type of session continuity for a new session. Clarify how the network can reject or "downgrade"/"upgrade" requests for specific continuity modes
SSC _WT_#3	Selecting or reselecting an efficient user path	Criteria and trigger for efficient user plane path, considering the parameters influencing the selection of an user plane anchor point Related procedures to perform selection or reselection of an efficient user path .
SSC _WT_#4	Session continuity wrt UE mobility	Describe how session and service continuity is supported for different PDU Sessions in a UE that have different session continuity levels How it can be possible to apply one level of session continuity support for some sessions in a UE while, at the same time, apply a different level of session continuity for other sessions in the same UE Session and Service continuity solution should support the following mobility scenarios: intra-RAT, inter-RAT, 3GPP and non-3GPP. NOTE: Session continuity solution to support mobility between 3GPP and non-3GPP may need to be delayed till after overall architecture with non-3GPP is defined
SSC _WT_#5	Service continuity when session continuity is not provided	WT#5.1 Identify whether any relationship between NextGen system and upper-layer service continuity mechanisms is required WT#5.2 Define such interaction if required

NOTE: though some of the solution aspects are depending on other key issues (e.g. SM signaling), we should try to identify which functionalities are impacted and the type of information needs to be exchanged over the reference points NG1, NG2, etc. (for common reference wrt other discussion), including pre-requisites before such exchanges and results. This will later allow plugging in the solutions into other KI solutions.

NOTE: relation with per-flow traffic switching is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 34 of 501

5.7 Key issue 7: Network function granularity and interactions between them

5.7.1 Description

It is expected that network systems will consist of multiple physical and/or virtual network functions that may be deployed in the operator's network, and be able to support diverse service requirements.

To achieve flexibility, the next generation system architecture design should have the following capabilities:

- Support for network deployment with centralized or distributed control plane network functions including dynamic deployment of functions.
- High function re-usability in network deployments through architecture principles that allow flexible network function deployment, ease of interfacing, flexible chaining, co-location of network functions.

The solution for the functional granularity should cover:

- Criteria to determine the right level of granularity of next generation network functions, such as:
  - The level of inter-dependency between network functions
  - Need for independent scalability of individual network functions
  - Need for deployment of individual network functions within or across operator network (e.g. PLMN) boundaries
  - Need for supporting centralized or geographically distributed deployments
- Based on above, identification of the network functions for the next generation architecture and definition of the set of functionalities supported by each of them.

NOTE: The solution proposal for defining the right level of granularity of network functions will be based on the functionalities defined by the other key issues such as, session management, mobility management, QoS framework. As such it is expected that solutions addressing this aspect will be discussed after a degree of progress has been reached for other key issues.

For the control plane network functions, the solution should support flexible interconnection between them. For the user plane network functions, the solutions should support flexible chaining between them. The solution for the interconnection of the control plane network functions should allow:

- Network functions to be able to interact with each other, e.g. for new services and features, while avoiding functional and signalling impact to unrelated network functions for a given interaction.
- Mechanism for the exchange of information between network functions that results in agile/rapid deployment of new services, e.g. mechanism that allows reuse of procedures, wherever possible.
- Ability to deploy network functions in various network configurations.

5.7.2 Work Tasks

Following work tasks are defined for the interconnection of network function part of this key issue.

Table 5.7.2-1: Work tasks for interconnection of NF

Work Task ID	Work Task(s)	Work Task Description

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 35 of 501

INF_WT_#1	Network function interconnection reference model	1. State assumption and/or applicability of the proposed reference model 2. Depict how the network functions are connected using the proposed reference model 3. Identifying a mechanism for a NF instance to interconnect to its peer NFs instances (e.g. via provisioning, selection and discovery etc.)
INF_WT_#2	Sample call flow	1. Describe sample call flows, e.g. network function A sending a req/rsp to network function B

NOTE: The above work tasks may not be completely independent of each other, e.g. sample call flow in INF_WT_#2 may depend upon the proposed interconnection reference model in INF_WT_#1.

5.8 Key issue 8: Next Generation core and access - functional division and interface

5.8.1 Description

This key issue will address the following general aspects:

- analyze in detail the functionality for the Next Generation Core and for the interface between the access networks and the Next Generation Core to support the LTE radio access network, the new, expected 5G radio access network (depending on information available from RAN design and the SMARTER requirements), and for non-3GPP access networks, in order to identify the functional split between AN and Core Network, and to identify if a single AN-CN interface can be specified which can be used across many different access networks. In particular, the functionality should be decomposed between:
  - access-specific functionality: such functionality applies only to a specific (set of) AN(s)
  - access-independent functionality: such functionality applies to all ANs, though the set of information/parameters/policies used for the functionality may be dependent on the specific AN
- identify how the various functionality correlate to each other and identify interdependencies - i.e. impacting Next Generation Core, AN and UE
- identify how the functionality can be modularized for the definition of a modular Next Generation Core -ANs interface that minimizes access dependencies and applies to any access networks
- identify how to decouple the access network and the core network, and identify its effects and implications to the Next Generation Core. Such decoupling shall allow for parallel and independent design and evolution of access networks and core networks
- identify how the UE interfaces with the Next Generation Core in a manner that minimizes access dependencies and that is applied independent of the access network via which the UE is accessing the Next Generation Core

Solutions and agreements for 3GPP RAN specific aspects should be prioritized in order to facilitate cooperation with 3GPP RAN. Aspects to consider for such solutions include e.g. functions which have impact to both CN and RAN, desired NextGen Core - RAN functional split and interface. The new RAT(s) and the Evolved E-UTRA should be taken into considerations.

NOTE: This key issue has dependencies on the solutions specified for other key issues such as QoS framework, Mobility framework, Session Management.

5.8.2 Work Tasks

Table 5.8.2-1: Work tasks for AN and CN functional division and interface

Work Task ID	Work Task(s)	Work Task Description
FDI WT_#1	Identify the functional split between AN and Core Network	Capture the outcome of other key issues in Section 8.1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 36 of 501

FDI _WT_#2	Identify if a common AN-CN interface can be specified	Investigate the feasibility and solutions towards a common AN-CN interface can be defined. The AN includes the Evolved E-UTRA, new RAT(s) and non-3GPP. Identify how the UE interfaces with the Next Generation Core

NOTE: The above WTs cannot be progressed alone by themselves but accompany with the progress of other key issues such as QoS framework, Mobility framework, Session Management. The outcome of the WTs will impact RAN3.

5.9 Key Issue 9: 3GPP architecture impacts to support network capability exposure and context information awareness

5.9.1 Description

The next generation system is expected to accommodate various services and TR 22.861 [4], TR 22.862 [5] and TR 22.863 [6] will continue to define requirements for key service categories, i.e. massive IoT, critical communications, and enhanced mobile broadband, respectively. To allow the 3rd party， UE or Network Functions to access information regarding services provided by the network (e.g. connectivity information, QoS, mobility, etc.) and to dynamically customize the network capability for different diverse use cases within the limits set by the operator, the next generation system should provide suitable access/exchange of network/connectivity information (e.g. via APIs) to the 3rd party， UE and Network Functions.

Additionally, to enable service optimisations, the NextGen system should support the combination, collection and exposure of additional context information from/to Network Functions, UE and 3rd parties.

Solutions for this key issue will study the following aspects (non-exhaustive list):

- Define network capability and context information exposure framework.
- Identify information from the UE, external applications, Network Functions, and RAN that can be used, to create session/network context information.
- Identify the mechanisms and interfaces to expose network capabilities and context information to the 3rd party, UEs and Network Functions.
- Identify the network information and/or context information that can be provided to 3rd party ISPs/ICPs to the UE, and to Network Functions to enable more customized and efficient service provision:
  - For any identified information, how the operator network to acquire information and to allow the 3rd party, UE and the Network Functions to access these information.
- How to create the network slice based on the requirement of the 3rd party or customize network function on-demand.

Editor's note: Whether the above bullet involves possible work of SA2 is FFS.

- Support the existing network capability exposure within the next generation system architecture
- Support APIs for exposure of new network capabilities and context information within the next generation system

NOTE 1: Exposure of new system capabilities will be studied based on the exposure requirements captured in TR 22.861 [4], TR 22.862 [5], TR 22.863 [6] and TR 22.864 [7].

NOTE 2: APIs are not necessarily in the scope of 3GPP.

Solutions for this key issue will assume that the next generation system should be able to expose network capabilities to the 3rd party and the UE and enable exchange of information in a secured way.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 37 of 501

5.10 Key issue 10: Policy Framework

5.10.1 Description

In the EPC system, network functions are configurable via operator policies. This trend is expected to continue into the Next Generation System. These operator policies help shape a variety of network behaviours such as related to:

- QoS Enforcement.
- Charging Control.
- Gating.
- Traffic Routing.
- Congestion Management.
- Service Chaining.
- Network (e.g. PLMN) Selection.
- Access Type Selection.
- Roaming.
- Mobility.
- Policies related to group of users.
- Third party service handling.
- Enhanced sponsored data connectivity for a variety of data traffic types (e.g. including data traffic encrypted between the UE and an application server)
- RAT/Frequency selection priority index

The provisioning and enforcement of these policies can happen in:

- UE.
- Control Plane entities.
- User Plane entities.

This key issue will look into solutions for a policy framework for the Next Gen System that takes into consideration all these related aspects.

NOTE: Policies can be categorized further into different types e.g. subscription based policies, local operator policies, etc.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 38 of 501

5.10.2 Work Tasks

Table 5.10.2-1: Work tasks for Policy framework

Work Task ID	Work Task(s)	Work Task Description
Policy_WT_#1	Define overall non-roaming and roaming/interworking policy related framework for NextGen	1.1 Define entities which constitute the policy related architecture and interfaces between those entities. 1.2 Which information accounts for policy decisions and which entities provide it? 1.3 How policy provisioning performed? 1.4 Which entities enforce policy decisions? 1.5 Decide on policy interactions, referring to the granularity and type of information provided by the policy function to the policy requesters. NOTE 1: The granularity of the policy information may be for example per PDU session or for a group of PDU sessions. Policy information for all PDU sessions may also be possible without policy interactions. NOTE 2: The type of policy information may be QoS, charging, usage monitoring, etc, depending on the outcome of other key issues. The policy decision and provisioning depends on specific type of required functionality (e.g. charging, usage monitoring etc.), Policy information may be predefined in the enforcement point or may be dynamically provisioned by the policy function. NOTE 3: The purpose of the enforcement of the policy related information depends on the outcome of other key issues. NOTE 4: The policy architecture will use the solutions' outcome from other key issues in this TR. It may not be possible to fully progress but rather define a baseline framework to be enhanced as other key issues progress.
Policy_WT_#2	QoS information provided by the Policy Function	2.1 Define whether the defined QoS related actions (e.g. redirection, bandwidth limitation, gating, priority/ preemption, resource management, etc.) are sufficient or not and establish policy enhancements as needed. 2.2 Define whether providers and enforcers of those QoS related actions are the same as in the existing policy framework and establish policy enhancements as needed. NOTE 1: This Work Task covers the QoS information that the Policy function provides, the granularity, the QoS information enforcers and the information flows. This depends on QoS key issue outcome. If needed, reference QoS framework key issue outcomes for new QoS related actions and define the source/destination for those actions.
Policy_WT_#3	Information controlled over charging interfaces	3.1. Define which charging interfaces are applicable, what charging related information provided to/by Policy function over those interfaces and how it is used for credit management and reporting. NOTE: Some relation with the charging key issue and its solutions exists. An analysis of potential overlapping will be performed when the solution for charging key issue is stable.
Policy_WT_#4	Potential interactions with access network discovery and selection, if any	4.1 Describe if and how policy framework interacts with network discovery and selection functionality. NOTE: This depends on "3GPP architecture impacts to support network discovery and selection" key issue outcomes and will be handled once the corresponding solution is stable.
Policy_WT_#5	Policies controlling access traffic steering, switching and splitting, if any	5.1 Describe if and how policy framework interacts with access traffic steering, switching and splitting functionalities. NOTE: This depends on access traffic steering, switching and splitting key issue outcomes and will be handled once the corresponding solution is stable.
Policy_WT_#6	Flexible mobile service steering policy control	6.1. Define how policy framework supports dynamically flexible mobile service steering. 6.2 Which information accounts for Flexible mobile service steering

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 39 of 501

		policy decisions and which entities provide it?
Policy_WT_#7	User Plane Congestion management control	7.1 Define how policy framework supports User Plane congestion management control. NOTE: This may depend on QoS key issue outcomes.
Policy_WT_#8	Alignment with other key issues solutions	8.1 Address policy framework requirements/assumptions made by other key issues not explicitly mentioned by this table.
Policy_WT_#9	3rd party policy interactions	9.1 Define whether and how policy framework interacts with 3rd party supported services. NOTE: This depends on the outcome of the key issue#9 on network capability exposure. This will be handled once the corresponding solution is stable.
Policy_WT_#10	Session Management	10.1 Decide whether and how policy framework provides policies to control a PDU session, e.g. at establishment/modification/termination of a PDU session, including support for multiple PDU sessions for the same UE. 10.2 Define the session information that is relevant for policy decisions. NOTE: This depends on the outcome of the key issue#4 on session management. This will be handled once the corresponding solution is stable.
Policy_WT_#11	Mobility Management	11.1 Decide whether and how policy framework provides policies for mobility on demand within the Mobility Management key issue. NOTE: This depends on the outcome of the key issue#3 on mobility management. This will be handled once the corresponding solution is stable.
Policy_WT_#12	Slicing	12.1 Decide whether and how policy framework provides policies for slicing within the Slicing key issue. NOTE: This depends on the outcome of the key issue#1 on network slicing. This will be handled once the corresponding solution is stable.
Policy_WT_#13	Enhanced Sponsored Data Connectivity	13.1 Define a mechanism enabling sponsored data connectivity. This requires the detection and identification of encrypted traffic. NOTE: Depending on the solution, SA3 work may need to be involved in stage2/3.
Policy_WT_#14	RAT/Frequency Selection Priority index	14.1 Define how policy framework provides policies for RAT/Frequency selection priority index.

5.11 Key issue 11: Charging

5.11.1 Description

Mobile System Architecture cannot be considered complete without having appropriate charging support. While the charging requirements in Next Generation System are expected to be similar in nature to LTE/EPC, depending upon the Next Gen System Architecture how, where and when charging data gets collected and communicated can be different. This key Issue will look into the architectural aspects of collection of charging data.

The architecture shall support both Online and Offline charging. In addition it shall support various charging models including:

- Application based charging / Group of Applications based charging.
- Volume based charging.
- Time based charging.
- Volume and time based charging.
- Session based charging.
- Event based charging.
- Access specific charging.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 40 of 501

- No charging.
- Third party charging (sponsored data).

The solution should also investigate the charging for information exposed to applications hosted in the operator trust domain close to the UE's access point of attachment.

Only high level architectural aspects of charging are expected to be captured in SA WG2. Detailed charging architecture and solutions will be developed by SA WG5.

5.12 Key issue 12: Security framework

5.12.1 Description

The authentication function is responsible for the authentication of the identity (e.g. user identity) that is presented to the network, when a UE requests to receive service(s) from the next generation network.

Editor's note: Whether additional entities different from UE would be considered is FFS depending by consolidation of SMARTER requirements.

NOTE 1: The UE in the scope of this key issue are assumed to possess credential. How these credentials are provided is out of scope of this key issue.

This Key Issue focuses on identifying the high level architectural aspects of the security framework.

The NextGen core network shall efficiently and adequately support the following requirements relevant for the authentication functionality:

- Next Gen core network should be capable to support various subscriber identity types as defined by SMARTER TR 22.891 [9], TR 22.861 [4], TR 22.862 [5], TR 22.863 [6] and TR 22.864 [7], for example IMSI and other subscriber IDs such as URI e.g. for MTC UEs. In addition some UE may also be getting connected to the network via intermediate nodes.
- NextGen core network should be capable to support roaming scenario.

The solutions for this key issue will be developed in co-operation with RAN for the network functionalities residing in RAN and especially with SA WG3 responsible for the definition of solutions addressing security and threats including the security architecture and access security and security framework for the next generation system.

The solution for this key issue will study the following aspects:

- identify potential placement of authentication functionality within the NextGen core network.
- identify whether and how authentication function supports the different connectivity models defined based on other key issues, including solutions defined for small and infrequent data handling.
- identify how authentication solution efficiently and adequately supports (for example in terms of scalability of security signalling traffic, new types/formats of subscriber identities, etc.,) different kinds of scenarios and applications, for example, massive deployment mIoT with low activity, UE supporting MBB service, vertical services, etc.
- whether and how UEs are authenticated per network slice or for multiple slices.
- authentication in roaming scenario.
- how established security associations or contexts are transferred between Network Functions and (re)used, e.g. when the UE's serving Network Function(s) change due to mobility.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 41 of 501

5.12.2 Work Tasks

Table 5.12.2-1: Work tasks for Authentication Framework

Work Task ID	Work Task	Work Task Description
SEC_WT#0	Security Architecture Framework	- Provide overall security architecture. This allows SA3 to provide security framework and overall security architecture as per SA3 study item. - Minimize access dependencies. - Common aspects for WT#1 through WT#5 captured here. Flows in WT#1 through WT#5 can refer to this section. - Consider single network slice scenario only in WT#1 to WT#8 section.
SEC_WT#1	Authentication and Key Agreement	- Where are functions located, AN and/or CN and whether on some specific NF. - Provide details of transport aspects for security signaling.
SEC_WT#2	User and ME Identity Confidentiality	- Where are functions located, AN and/or CN and whether on some specific NF. - What identities (user and ME)are used/available that need confidentiality.
SEC_WT#3	ME Identity checking	- Where are functions located, AN and/or CN and whether on some specific NF. - Checking of ME Identity.
SEC_WT#4	System signaling protection (integrity/ciphering)	- Where are functions located, AN or CN and whether on some specific NF. - Consider if AN and CN signaling needs separate protection. - Are there signaling connection to multiple NFs from UE that need integrity/ciphering?
SEC_WT#5	User data protection (integrity/ciphering)	- Where are functions located, AN and/or CN and whether on some specific NF. - Consideration also case of CP/UP NF separation, as applicable.
SEC_WT#6	Non-3GPP Access	- For WT#1 to WT#5, capture any specifics/adaptation for Non-3GPP access based on architecture for integration of non-3gpp accesses. Minimize access dependency.
SEC_WT#7	Security handling at CN NF change, e.g due to mobility	- How established security associations or contexts are transferred between Network Functions and (re)used, e.g. when the UE's serving Network Function(s) change due to mobility. - Consider both 3GPP and non-3GPP access.
SEC_WT#8	Small Data Considerations	- Study security considerations related to small data traffic handling.
SEC_WT#9	Multiple slice aspects	- Consider multiple slice aspects of the above WTs in here. - Are there separate security contexts for different slices, and does UE have multiple of them?
SEC_WT#10	Provision 3GPP Credentials to UEs	- Support the remote provision of a UE that has not been pre-provisioned, with its 3GPP subscription credentials.

5.13 Key issue 13: Broadcast/Multicast Capabilities

5.13.1 Description

This key issue will address the need and possible solution aspects to support broadcast/multicast capabilities similar as provided currently like PWS, eMBMS and GCSE that are available for LTE/EPC networks, including support for features such as mission-critical applications.

Specific solutions proposed under this key issue include those needed to architecturally support:

- 1:many and 1:all communication involving 5G capabilities specified by RAN;
- Group handling (e.g. geographic scope of groups);
- Group communication (e.g. setup performance, services to the group member, group member requests of the system, priority and pre-emption of group communication, services provided during an ongoing group communication, and user perception of group communication);

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 42 of 501

- Functionality and performance needed to satisfy current and emerging 3GPP broadcast/multicast service requirements and application architecture requirements (e.g. MCPTT, MCVideo, MCData, CriC, and massive MTC);
- Functionality and performance needed to satisfy current mandated PWS requirements (e.g. ETWS, CPAS, KPAS, etc.);
- Consideration of related NextGen architecture key issues (e.g. session management, QoS framework).

5.14 Key Issue 14: Support for Off-Network Communication

5.14.1 Description

This key issue is to define support for off-network communication capabilities for in-coverage and out-of-coverage devices as specified by relevant Stage 1 requirements. For example, off-network group communication is needed to support current and emerging critical communications, including the individual- and group-based mission-critical voice, data, and video communications needed by public safety (e.g. see TR 22.862 [5]).

Specific solutions proposed under this key issue include those needed to architecturally support:

- Direct communication involving 5G capabilities specified by RAN (e.g. one-to-one, one-to-many, one-to-all);
- Functionality and performance needed to satisfy current and emerging 3GPP off-network service requirements and application architecture requirements (e.g. MCPTT, MCData, MCVideo, V2X, and MTC).
- Functionality to provide the required control by the MNO of off-network communication.

5.15 Key Issue 15: NextGen core support for IMS

5.15.1 Description

This key issue will study the system requirements and the solutions required in order to enable the next generation system to support IMS.

5.16 Key Issue 16: 3GPP system aspects to support the connectivity of remote UEs via relay UEs

5.16.1 Description

This key issue will study:

- Definition of a relay UE in the NextGen framework.
- Definition of remote UE in the Next Gen framework based on definitions in section 3.1 of TR 22.861 [4].
- The effects of a relay UE on the mobility framework as well as session management and session continuity.
- The support of remote UEs with different capabilities (e.g. UEs that are constraint in a way that they do not support the full set of NextGen UE functionality, e.g. mobility or UEs using a non-3GPP access for the indirect 3GPP connection, etc.)
- Which functions are further required/enhanced comparing to Rel-13 relay UE functionality, e.g. using a non-3GPP access for the connection to the core network .
- If there is need for selection criteria based on operator policy between the direct connectivity to the network and the connectivity via a relay UE to provide efficient service.
- Efficient session and/or service continuity mechanism between:
  - the direct connectivity to the network and the connectivity via a relay UE, and
  - the connectivity via a current relay UE and the connectivity via a new relay UE with minimizing the interrupt time for the service and signalling overhead.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 43 of 501

- How to enable flexible transport of traffic between the remote UE and the core network, e.g. switch between direct and indirect mode or transfer traffic between private network behind the relay UE via the core network e.g., to a 3rd party.

- The security and privacy aspects (e.g. how to establish the connectivity via a UE relay when there is no trusted relationship between the remote UE and the relay UE) , including authentication of remote UEs (with different types of credentials to allow for different deployment scenarios such as industrial factory automation);

Editor's note: Different types of credentials is still being studied in SA1and not yet normatively approved.

- Identification, discovery and management of the connection by the Next Gen framework of remote UEs

- Control by the MNO of the connectivity via a relay UE.

- Impact on QoS support for remote UEs

Additional inputs from SA WG1 will be considered for possible enhancement to a relay UE.

5.17 Key Issue 17: 3GPP architecture impacts to support network discovery and selection

5.17.1 Description

In EPS, a variety of solutions has been defined for network discovery and selection for 3GPP accesses and non-3GPP accesses. In order to enable integration of various 3GPP accesses and non-3GPP accesses and to cater for the architectural requirements and assumptions for the NextGen system, the introduction of a network discovery and selection mechanism will provide operators with a solution to flexibly control UE to select various accesses according to operator policy.

This key issue will address the following issues:

- Study how to support network discovery and selection mechanism for:

  - 3GPP and non-3GPP accesses.

  - non-roaming and roaming scenario.

  - idle and connected mode (for transition from a 3GPP access to a non-3GPP access or vice versa).

Editor's note: Access network selection in connected mode within 3GPP access is out of scope of this key issue.

- Study which information is required for the UE for network discovery and selection mechanism.

Editor's note: Actual policies provided to the UE for network discovery and selection, if any, will be defined under key issue on Policy Framework.

- Study which entity/functionality are involved in network discovery and selection mechanism and their interaction.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 44 of 501

5.17.2 Work Tasks

Table 5.17.2-1: Work tasks for Key Issue: Network Discovery and Selection Framework

Work Task ID	Work Task(s)	Work Task Description
NDS_WT_#1	Define overall architecture for network discovery and selection architecture in NextGen	1.1 Define entities which constitute the network discovery and selection architecture and interfaces between those entities. NOTE: A solution or a part of a solution may be specific to an access technology (e.g. to WLAN, Satellite Radio Access Technology) or a class of access technologies (e.g. to Non-3GPP Access Networks). 1.2 How is information provisioning performed? 1.3 Which entities enforce NDS decisions?
NDS_WT_#2	Network discovery and selection information provided by the NDS Function	2.1 Which information counts for network discovery and selection decisions and which entities provide it? 2.2 How to enable the operator to steer the UE to a particular service to enable in-network roaming (TR 22.864 [7], clause 5.6.1). 2.3 How to support PLMN selection based on operator policy including network supported services /slices, specific traffic type (from a specific application or service), multiple radio capability, level of trust and preferred partners (TR 22.864 [7], clause 5.6.2). 2.4 How to enable the UE to select multiple networks simultaneously so as to "obtain services from more than one network simultaneously on an on-demand basis (TR 22.864 [7] clause 5.1.2.5). 2.5 Identify the format of rules for network discovery and selection. 2.6 Identify the attribute types and metrics that may be present into network discovery and selection rules. 2.7 Decide on rules interactions based on type of information, source of information, etc. NOTE: It is FFS based on the progress of the work in the other KIs on how network discovery and selection relates to network slicing, in particular how to ensure the UE selects a network that provides the slices that the UE wants/needs.

5.18 Key Issue 18: Interworking and Migration

5.18.1 Description

This key issue focuses on migration and interworking scenarios.

5.18.1.1 Interworking and migration principles

- The deployment of NextGen System without interworking between EPC and NG-Core is the long-time final goal after migration (under the assumption the EPC may still last for a long time to provide legacy or roaming UE support).
- NextGen System's requirements therefore should not be compromised to improve interworking between EPC and NG-Core or to fit a specific migration path.
- Any interworking functionality between EPC and NG-Core shall be developed in a manner that
  - Minimizes impacts to EPC as well as to the NextGen core.
  - Does not create any permanent dependencies for NG-Core on interworking to EPC even after the migration is completed.
- Multiple architecture Options and UEs supporting different Architecture Options may coexist at the same time within one PLMN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 45 of 501

5.18.1.2 Assumptions on UE capabilities

To support backward compatibility with legacy LTE networks a UE that supports any NG RAN may also have LTE/EPC capability. UE support option 4 implies supporting option 2, and UE support Option 7 implies 5.

If NG NAS is supported by a UE, the UE can use the NG NAS on either New RAT or Evolved E-UTRA to access NG Core.Editor's note: Whether a UE supporting Option 4 (resp. Option 7) supports Option 7 (resp. Option 4) should be decided by RAN groups.

5.18.1.3 Interworking and migration scenarios within an operator

Any alternative combinations or sequence of deployment and/or transition flows involving options 3, 7, 2/4 would need to be specified. For example, two of the migration paths are illustrated as:

1) LTE/EPC -> Option 2/Option 4

2) LTE/EPC -> (Option 3) -> Option 7 -> Option 2/Option 4

NOTE 1: Option 7 and Option 3 can coexist in the same PLMN at the same time.

Gradual migration from EPS to EPS+NGS to NGS should be enabled by 3GPP specifications in Rel-15. From SA2 perspective the interworking scenario generated from the migration paths can be simplified as: LTE/EPC and NextGen System.

5.18.1.4 Interworking scenarios on roaming

A NextGen UE will get at least LTE/EPC service where LTE/EPC exists, if the UE supports backward compatibility with legacy LTE networks. On top of that, it may be able to use any NG RAN in the VPLMN that it supports and that the roaming agreement allows. The roaming scenarios can be categorized into the following Cases:

1) EPC in VPLMN, NG Core in HPLMN

2) NG Core in VPLMN, EPC in HPLMNNOTE: the solutions for above cases shall not create any permanent dependencies for NG-Core and EPC and compromise the design of NG Core.

5.18.1.5 UE compatibility

A UE supporting Option 3 may also support Option 7, and vice versa.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 46 of 501

5.18.2 Work Tasks

Table 5.18.2-1: Work tasks for Key Issue: Interworking and Migration

Work Task ID	Work Task(s)	Work Task Description
IWM_WT_#1	Interworking and migration Scenarios within an operator (non-roaming)	1.1 Identify and describe the interworking and migration scenarios wherein a PLMN/operator has deployed an NG system in parts of the PLMN area in addition to an existing legacy 3GPP RAN and where some interworking is required to maintain at least some level of service for UEs changing between NG RAN and legacy 3GPP RAN. NOTE: Level of service continuity offered during interworking may range from seamless service continuity to no service continuity, requiring re-attach. 1.2 For each of those scenarios, identify what level of service continuity, possibly specific per service, shall be maintained for UEs changing between NG RAN and legacy 3GPP RAN. 1.3 Identify the UE and CN requirements to support such aspects. NOTE: This WT considers all aspects that are in common for NG RANs corresponding to options 2, 4, 5, and 7.
IWM_WT_#2	Interworking and migration specifics related to the different NG RAN options	2.1 Identify any Interworking and migration aspects that are in addition to what is considered under WT1 and that are specific for any of the NG RAN options. For example, there might be some differences for UEs changing between LTE and Evolved E-UTRA (option 5 and 7) compared to changing between LTE and NR (option 2 and 4). 2.2 Identify the migration and interworking between option 2, 4, 5 and 7, if any is needed. 2.3 Identify the UE and CN requirements to support such aspects. NOTE: Solutions for WT#2 depend on the outcome of WT#1 and RAN WGs developing option 2, 4, 5 and 7.
IWM_WT_#3	Interworking and migration specifics related to option 3	Identify any interworking and migration aspects that are in addition to what is considered under WT1 and WT 2 caused by deployments that migrate first to option 3 and afterwards to other NG RAN options.
IWM_WT_#4	Roaming and Interworking Scenarios	4.1 Identify roaming scenarios between an operator that deploys an NG system and one that deploys only an EPS. For each of the identified scenarios determine what level of service is provided for the roaming users. 4.2 Identify roaming requirements for the UE and the network that solutions for other key issues (e.g. session management, mobility management, QoS, etc.) need to satisfy.

5.19 Key Issue 19: Architecture impacts when using virtual environments

5.19.1 Description

The NextGen system is expected to support deployments in virtualized environments. This key issue will determine the need for and architecture impacts due to load rebalancing and load migration in the context of:

- scaling of a network function instance, and
- dynamic addition or removal of a network function instance.

Editor's note: An appropriate definition of the various types of scaling will be discussed during the course of the work on this key issue.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 47 of 501

NOTE: Load rebalancing and load migration across network function instances assumes multiple active instances of a network function. Potential issues resulting from load rebalancing and load migration to be addressed may include:

- UE signalling overhead.

5.19.2 Issues to be addressed

5.19.2.1 Avoid UE interaction from NF Load Balancing, Scaling and Migration

When a Network Function is created, deleted, or moved, either within a data centre or between data centres, the IP address used by a remote entity (e.g. NG RAN node, MMF, SMF, UPF, SDM, etc.) to route signaling/data to that NF might (or might not) change.

If the IP address of such a Network Function does change, then it is very important that there is no need for UE interaction. The need to avoid UE interaction is to avoid radio interface signaling load, UE battery consumption and to handle cases where the UE is out of coverage or in Power Save Mode's/eDRX's deep sleep state.

5.20 Key issue 20: Traffic Steering, Switching and Splitting between 3GPP and non-3GPP Accesses

5.20.1 Description

For UEs that can be simultaneously connected to both 3GPP access and non-3GPP access, the NextGen system should be able to take advantage of these multiple accesses in a way that improves the user experience, optimizes the traffic distribution across various accesses, enables the provision of new high-data-rate services, etc. Towards this goal, this key issue will investigate the following aspects for UEs connected to both 3GPP and non-3GPP accesses:

- How the NextGen Core network and the NextGen UE can support access traffic steering (as defined in clause 3.1) between 3GPP and non-3GPP accesses.

- How the NextGen Core network and the NextGen UE can support access traffic switching (as defined in clause 3.1) between 3GPP and non-3GPP accesses. This includes the conditions that can trigger the switching of a data flow to a new access.

- How and if the NextGen Core network and the NextGen UE can support access traffic splitting (as defined in clause 3.1) between 3GPP and non-3GPP accesses. This includes the conditions that can trigger the splitting of a data flow across multiple accesses.

- How the access traffic steering, switching and splitting (ATSSS) can be taken into account by the charging framework (considered in Key Issue 11) in order e.g. to enable the network operator to differentiate charging for data traffic that is switched and/or split between 3GPP and non-3GPP accesses. It is clarified that this key issue will not address the charging framework but it will only consider what information needs to be provided to the charging framework in order to charge traffic that is switched and/or split between 3GPP and non-3GPP accesses.

Potential policies provided to the UE for access traffic steering, switching and splitting (ATSSS), if any, will be defined under the key issue on Policy Framework.

This key issue is restricted only to ATSSS procedures applied in the NextGen core network. Similar procedures that may be applied in the NextGen RAN are outside the scope of this key issue.

The procedures for access traffic steering, switching and splitting take place after the session management procedures are executed, i.e. after PDU sessions are established over 3GPP and non-3GPP accesses.

5.20.2 Work Tasks

All work tasks below apply when the UE can simultaneously connect to 3GPP and non-3GPP accesses and send data on both accesses.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 48 of 501

Table 5.20.2-1: Work Tasks for ATSSS

Work Task ID	Work Task(s)	Work Task Description
ATSSS_WT_#1	Access Traffic Steering & Switching	1) When a new data flow is initiated by the UE, the UE should decide to steer this data flow to 3GPP access or to non-3GPP access. How is this steering decision made? E.g. based on what criteria? 2) How does the network take steering decisions for new DL data flows (i.e. for flows not initiated by the UE)? 3) Which element can decide to switch (i.e. move) one or more data flows from 3GPP access to non-3GPP access and vice versa? The UE, the network or both? 4) Based on what criteria are the traffic steering & switching decisions made? 5) The network should be able to control the UE's steering & switching decisions. Should this be enabled by policy? If yes, how is this policy provisioned in the UE? How does this policy impact the policy framework? 6) When a data flow is switched between 3GPP and non-3GPP accesses, does the charging framework need to be informed? If yes, what information should be provided to the charging framework for enabling appropriate charging?
ATSSS_WT_#2	Access Traffic Splitting	1) In which scenarios is traffic splitting beneficial? 2) Which element can decide to split a data flow across 3GPP access and non-3GPP access? The UE, the network or both? 3) Based on what criteria it is decided if a certain data flow can be split or not? Based on policy? If yes, how is this policy provisioned in the UE? How does this policy impact the policy framework? 4) When a data flow is decided to be split, how is the traffic of this data flow scheduled on 3GPP access and on non-3GPP access? Based on what criteria? 5) What new functionality is required to enable traffic splitting and combining? 6) When a data flow is split across 3GPP and non-3GPP accesses, does the charging framework need to be informed? If yes, what information should be provided to the charging framework for enabling appropriate charging?

5.21 Key Issue 21: Minimal connectivity within extreme rural deployments

5.21.1 Description

In the context of "Markets requiring minimal service levels" described in TR 22.864 [7], "Extreme coverage in low density areas" described in TR 22.863 [6] and "Extreme rural for the Provision of Minimal Services over long distances" described in TR 38.913 [10]), this key issue will address the need and possible solutions to support minimal services in the context of extreme rural deployments, where territories are very large or resources are limited, e.g., limited electricity provided by alternative energy sources as there is no electricity grid, unreliable and costly backhaul, etc.

This key issue will study:

- mechanisms that finely control resource consumption in all the elements of the NextGen system architecture that are placed on the end-to-end path of sessions.

- optimized control of access network, backhaul, and core network resources while ensuring minimal connectivity over large territories for essential services with very limited bandwidth requirements (see TR 22.863 [6] clause 5.3.2.4).

- optimization of energy consumption of all the elements on the end-to-end path of sessions.

5.22 Key Issue 22: Support of "5G connectivity via satellite" use case

5.22.1 Description

This (Phase 2) key issue will address the possible SA2 architecture impact in relation to the "5G connectivity via satellite "use case. This can be achieved through satellite transport network or 3GPP/Non 3GPP defined satellite radio access networks.

This key issue will study:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 49 of 501

- Solutions (**in complement with key issue 6**) for dynamic reselection of efficient user plane path with minimum service interruption. A possible cause for user-plane path (re)selection can be NextGen (R)AN mobility requiring dynamic NG2/NG3 interface relocation for Next Gen service on board aircrafts, vessels or trains. When an existing path supporting the NG2/NG3 interface becomes unavailable, a new path shall be selected supporting the NG2/NG3 interface (NG2/NG3 interface relocation).

NOTE: NG2/NG3 interface relocation is needed when the IP address of the Next Gen (R)AN Node has to be changed (e.g. due a change of anchor satellite Earth station in the case of NetGen service on board moving platforms).

- Solutions (**in complement to key issue 6**) for (Re)Selection of efficient user-plane path(s) per UE session between a UE and the communication peer(s) upon context information such as network load and/or network latency associated to the possible anchor points or other criteria (e.g. Lawful intercept constraint for all or specific traffic type).

- Possible impacts on the SA2 architecture in the case of 3GPP or Non 3GPP defined satellite RAN based on GEO and NGSO satellites.

5.22.2 Work Tasks

The following list of work tasks has been identified for this key issue.

Table 5.22.2-1: Work Tasks for SAT

Work Task ID	Work Task(s)	Work Task Description
SAT _WT_#1	Dynamic Reselection of user path for a group of UEs	Simultaneous reselection of user path for the UEs served by a set of Next Gen (R)AN Nodes embarked on a moving platform (e.g. aircraft, vessel, train) to ensure service and session continuity; Identify specific information (e.g. Next Gen (R)AN Cell identity, Next Gen Core identity) that needs to be provided to trigger the reselection. Define related procedures to perform selection or reselection of the group UE user path, reusing whenever possible procedures defined under Key Issue 6.
SAT _WT_#2	Selecting or reselecting an efficient user path	Define criteria and trigger for efficient user plane path, considering the context information (e.g. cross border transport network supporting the NG2/NG3 interface) and other criteria influencing the selection of anchor point for the UE UP per session. Identify possible impact on the efficient user path (re)selection procedure defined under key issue 6.
SAT _WT_#3	Specifics of satellite RAN.	Identify possible impact on mobility management.(addressed in key issue 3): efficient tracking area design, adaptation of CN based paging procedures, Inter RAT (satellite and "terrestrial") cell reselection/Hand-over procedures. Identify possible SA2 architecture impact to support specific capabilities (e.g. UE to UE connectivity via satellite session management procedures, point-to-Multipoint service satellite capability).

5.x Key Issue x: Title

5.x.1 Description

Editor's note: This clause will identify key architectural issues to be solved during the architecture design.

6 Solutions

Editor's note: This clause describes the solutions to the key issues and solutions to architecture design.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 50 of 501

6.1 Solutions for Key Issue 1: Support of network slicing

6.1.1 Solution 1.1: Network Slicing without Slicing the radio

This solution applies to Key Issue 1 -Support of network slicing. The solution introduces the high-level solution for the network slicing without slicing the radio.

6.1.1.1 Architecture description

In this solution it is assumed that any slicing of a PLMN is not visible to the UEs at the radio interface. So in this case, a slice routing and selection function is needed to link the radio access bearer(s) of a UE with the appropriate core network instance. The solutions do not make any assumption on any potential RAN internal slicing. The main characteristics is that the RAN appears as one RAT+PLMN to the UE and any association with network instance is performed network internally, without the network slices being visible to the UE.

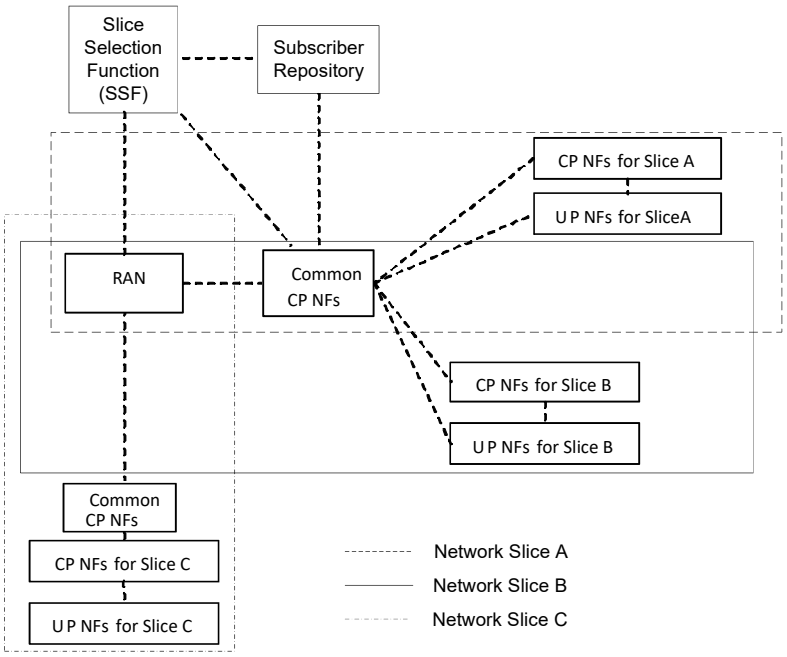


Figure 6.1.1.1-1: Control plane interfaces for network slicing with common and slice specific functions

This solution follows architecture principles for network slicing as below:

- Besides the Subscriber Repository function, the control plane of the NextGen Core is partitioned into three types of Network Functions (NFs).
  - Slice Selection Function (SSF): The SSF handles the UE's initial Attach Request and New Session establishment request by selecting an appropriate slice for the UE based on the UE's subscription information, UE usage type, service type and UE capabilities. The SSF is not specific to a particular network slice.
  - Common CP NF: The Common CP NF is the CP entry function, which at least includes the MM function, AU function, and NAS Proxy function. The Common CP is shared parts among different slices. When different types of Network Slice do the sharing, the required Common CP function can be different. One UE can only access one Common CP simultaneously.
  - Slice Specific CP NF: the NFs which are located on the non-shared Slice parts, e.g., SM NF.
    - No direct interface from RAN to the slice specific CP NFs.

Editor's note: It is FFS whether the slice specific CP NFs have a direct interface to the Subscriber Repository.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 51 of 501

- Each network slice instance associated with a network slice type ID (NeS-ID). The NeS-ID is used to identify the type of the slice. Both standardized and PLMN specific values for NeS-ID are possible. The NeS-ID can be separated into two parts:

  - Type of Common CP: When the different types of Network slice share the common network function, the Common CP need to accommodate the requirements from different slice, e.g. different MM requirement. Thus the required Common CP function can be different. The type of Common CP is introduced, which is to reflect the related requirement to the Common CP function from the sharing Network slices or individual Network slice.

NOTE 1 : The type of Common CP can be a numeric value which does not directly reflect the sharing network slices.

NOTE 2: The type of Common CP may reflect different purpose, e.g. same enterprise customer, or same combination terminal usage, etc.

  - Type of non-Shared Slice part, which identify the type of non-shard slice CN parts, e.g. eMBB non-Shared CN part.

- A Temporary ID can be assigned to the UE when the UE is successfully registered to the network. The UE Temporary ID is assigned by the Common CP NF. The UE Temporary ID consists of the routing information to the common CP NF of (similar as GUMMEI) and a UE specific identity (similar as M-TMSI). Even if UE can simultaneously access multiple network slices, the allocated Temporary ID shall be only one, which is linked to one Common CP NF in the network.

For roaming scenarios, there are two scenarios:

1. Home routed roaming case: The UE's traffics are transferred via the UP functions in both VPLMN and HPLMN. The NFs in the VPLMN cooperate with the NFs in the HPLMN to provide the end-to-end services for the roaming UE.

2. Local breakout roaming case: The UE's traffics are transferred via UP functions within VPLMN, and the HPLMN may provide policy control function for the roaming UE.

Figure 6.1.1.1-2 depicts the roaming reference architecture with support of network slicing in the home routed roaming scenario.

In this scenario, the end-to-end network slice is composed of HPLMN part and VPLMN part. The HPLMN and VPLMN parts of the network slice need to be selected to provide the end-to-end services for the roaming UE.

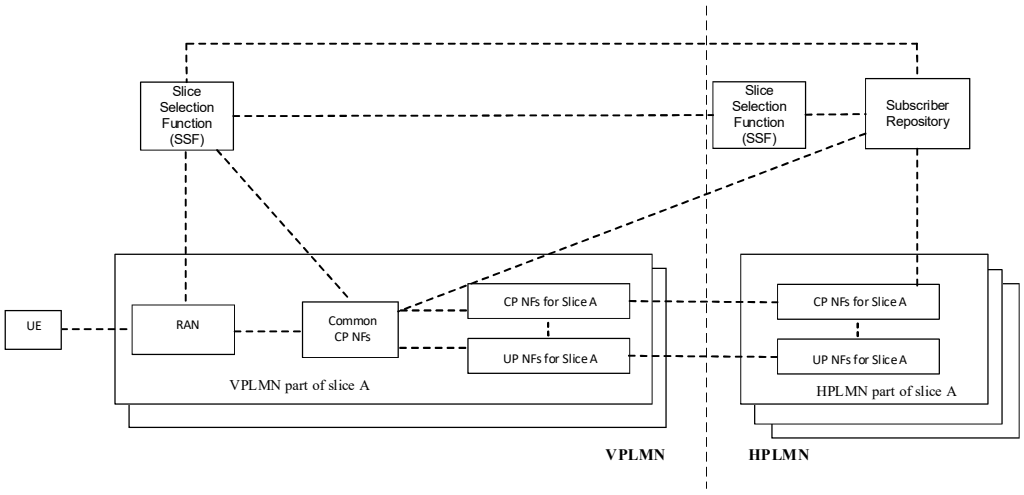


Figure 6.1.1.1-2: Roaming reference architecture with supporting slicing – home routed scenario

NOTE: The interface between SSFs in VPLMN and HPLMN is for selection of VPLMN part and HPLMN part of network slice. Other roaming interfaces are discussed in related KIs.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 52 of 501

Due to the potential complex relationship between HPLMN and VPLMN parts of the network slice, before selecting network function in HPLMN, the NeS-ID of HPLMN part should be determined firstly by network slice selection procedure. During this slice selection procedure, multiple factors, e.g. UE requested service type, user subscription, and roaming agreement can be considered to select the NeS-ID. After that, the network function selection can be simplified without considering these factors.

Editor's note: In roaming scenario, whether there are Common CP NFs for the HPLMN part of Network Slices is FFS. In figure 6.1.1.1-2, it is assumed that for the roaming UE there are no Common CP NFs existing in the HPLMN.

6.1.1.2 Function description

When the UE first time attach to the network and no valid NeS-ID (i.e. a standardized NeS-ID or PLMN specific NeS-ID), the RAN forward the request to the SSF. The slice selection function selects an appropriate slice for the UE based on UE provided and possible CN provided information. When the UE has a valid NeS-ID but the Temporarily ID is not valid, the RAN forward the request the Common CP NF based on the NeS-ID. When the UE has a valid Temporarily ID, the RAN forward the request to the Common CP NF based on the Temporarily ID.

As all network instances of the PLMN share radio access there is a need for separating any access barring and (over)load control per slice. That may be accomplished comparable to today's separated access barring and (over)load control that is provided per PLMN operator for network sharing.

With that solution there may be CN resources that cannot be fully separated, e.g. transport network resources. Any RAN internal slicing or managing of shared RAN resources is for RAN WGs.

The SSF handles the UE's initial Attach Request and New Session establishment request by selecting an appropriate slice for the UE based the UE's subscription information, UE usage type, service type and UE capability. During the attach procedure the SSF associates the UE to one default slices or a UE specified type slice. The initial Attach Request is then forwarded to the selected network slice and handled by the CP NFs in the selected network slice. During the attach process, the related NeS-ID and a Temporary ID for the UE are provided to the UE in Attach Accept message.

The SSF may also consider whether the UE is a roaming UE or not when perform slice selection. In the home routed roaming case, the roaming information, e..g. HPLMN ID, should be considered during VPLMN part of slice selection. The SSF in the HPLMN can select the HPLMN part of slice for the roaming UE by using the slice type of the VPLMN part as a reference.

After selecting the Network Slice, the SSF may perform the NNSF to select the CP NFs corresponding to the selected slice.

Editor's note: whether the Attach procedure described in this solution can be combined with the initial slice selection procedure described in clause 6.1.3 is FFS.

The UP connections for the UE can be established by the selected CP NF. This can be established during the attach procedure or it can be setup after the UE sends a New Session establishment request. If it is established during the attach procedure then a default or UE specified UP connection is setup. During the setup of UP connections, the NeS-ID may be sent to the RAN if the RAN need be slice aware.

After the attach procedure, a UE can be associated with multiple slices if the UE sends multiple new session establishment requests for services that are provided by different slices. The attach procedure is the same for the case where the UE can attach to one slice or multiple slices.

The SSF is involved in the following procedures:

- Attach procedure
  - The SSF selects a slice for the UE during the initial attach procedure based on the UE's subscription information, UE usage type, service type (if provided) and UE capability.

Editor's note: Details of the Service Type whether to use existing parameters or new parameters is FFS.

  - The SSF performs a UE identity check before a slice is selected. This function may be common to all slices.
  - The SSF may associate the UE with one default slices or a UE specified slice during the attach procedure.
  - The SSF perform the NNSF to select the CP NFs corresponding to the selected slice.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 53 of 501

- New session establishment request
  - The SSF may select additional slices for a UE after the initial attach request.
  - The new session establishment request may be forwarded to the SSF by the common CP NF selected from the initial attach procedure.

The UE attach procedure is illustrated in the following figure.

In scenario of Group B in Annex D, whether a CP NF should be common or not is decided based on whether the context it handled is common for multiple slices or not. With this criterion, the CP NFs fall into the following two categories:

a) The following CP NFs that handle UE common context information that is common for all of a UE's services or sessions shall be common for the multiple slices serving the UE

- The MM function. It is responsible for handling the MM context of the UE.
- The Access AU function. It deals with the security context of the UE.

NOTE 1: Slice specific authentication may be required when slices require different levels of security, which depends on discussion in security key issue.

- The UE specific policy control function (UE-PCF). It performs policy control based on per UE-related policy.

b) The following CP NFs that handle session level context or finer (e.g. flow level) context can be slice-specific

- The SM function. It is responsible for handling the session level SM context.
- The slice-specific policy control function (slice-PCF). It performs policy control based on session/flow level.

Editor's note: It's FFS the feasibility to the slice-specific policy control function which is dependent on the outcome of the KI#10 for NextGen policy framework.

The attach procedure applies to the following cases:

1. The MM, AU and SM are all slice specific NFs (e.g. Group A slice configuration).
2. The MM and AU are common NFs. The SM is a slice specific NF.

Editor's note: It is FFS whether common and slice specific authorization are both applied.

NOTE 2: How to ensure the appropriate security level is to be determined by SA WG3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 54 of 501

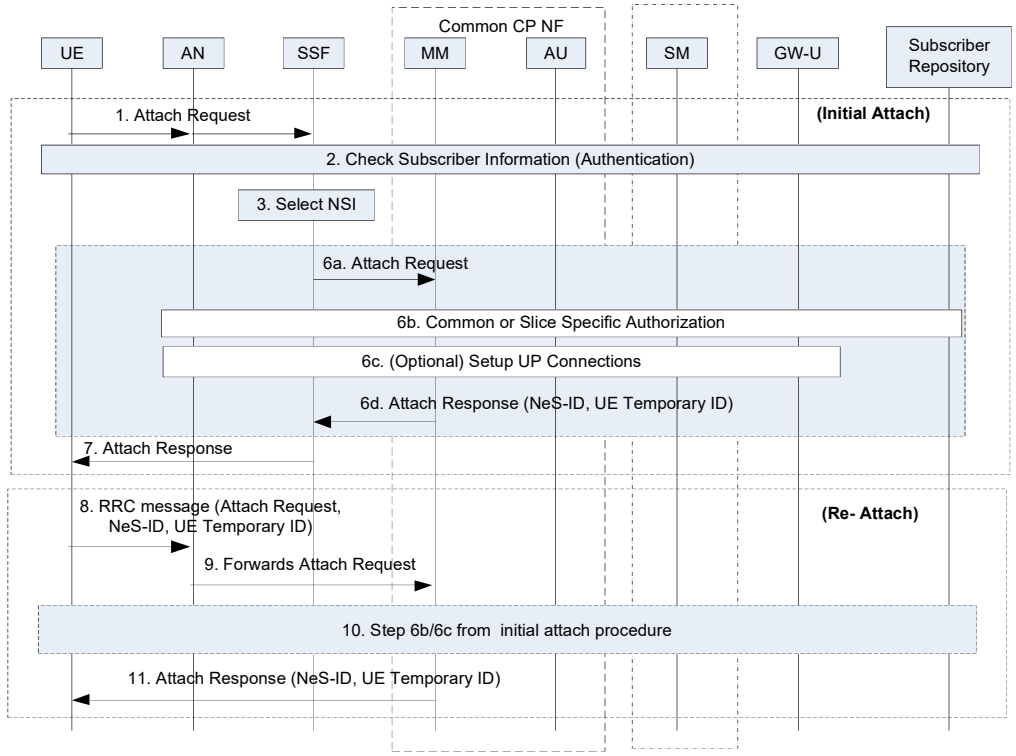


Figure 6.1.1.1-2: Initial attach procedure and re-attach procedure.

1. The UE sends an initial Attach Request to the AN including UE capability and requested service (optional). The AN forwards the Attach Request to the SSF.

2. The SSF determines which slice(s) the UE is selected by accessing the Subscriber Repository and authenticate the UE to check whether the UE is permitted to access the network.

3. The SSF selects the appropriate slice type as well as the related NeS-ID of the slice based on the information received from the UE in the Attach Request and profile information in the Subscriber Repository. The SSF further selects the slice instance according to the NeS-ID.

4. Void

5. Void

6. Common or Slice Specific Authorization:

   a. The SSF forwards the Attach Request to the MM NF which includes the NeS-ID information, and the MM communicates with the AU NF to handle the slice authorization. The AU NF is a common NF.

   b. The AU performs the authentication/ slice authorization procedure by checking the UE identity with the Subscriber Repository. The procedure determines whether the UE is authorized to access this slice. If the authentication is performed in step 2 and the received message is from SSF, the authentication can be skipped.

   c. (Optional) Setup of the UP connections for a default or UE specified type slice.

   d. The MM sends an Attach Response to the SSF. The Attach response includes the NeS-ID and the UE Temporary ID.

7. The SSF sends an Attach Response to the UE via AN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 55 of 501

When the UE get the NeS-ID and the Temporary ID, it can use those information to assist the network slice selection, e.g. when UE detach from the network and reattach to the network again.

8. If the UE re-attaches to the network after it got the NeS-ID and the UE Temporary ID, it can send an Attach Request to the AN with the NeS-ID and the UE Temporary ID. If the UE Temporary ID is valid, the AN can send the request directly to the Common CP NF, based on the UE temporary ID information. Otherwise, the AN selects Common CP NF based on the NeS-ID..
9. The AN can forward the Attach Request directly to the appropriate Common CP NF.
10. Steps 6 b/6c from the initial attach procedure can be performed.
11. After successfully attached, the Common CP NF sends an Attach Accept message, which includes, if necessary, a new NeS-ID (optional) and new UE Temporary ID to the UE.

If no UP connection is setup or if only a default UP connection is setup for the UE and the UE requests for a service that is provided by another slice then another UP connection for the UE is setup during the New Session establishment requestprocedure.

This procedure is illustrated in the example in Figure 6.1.1.1-3. In the example, the UE has a connection to common CP NF. The SM NF is assumed to be slice specific. If the UE has already been authenticated and the new slice uses the same authentication procedure then the AU function needs to only check whether the UE is authorized to use the slice.

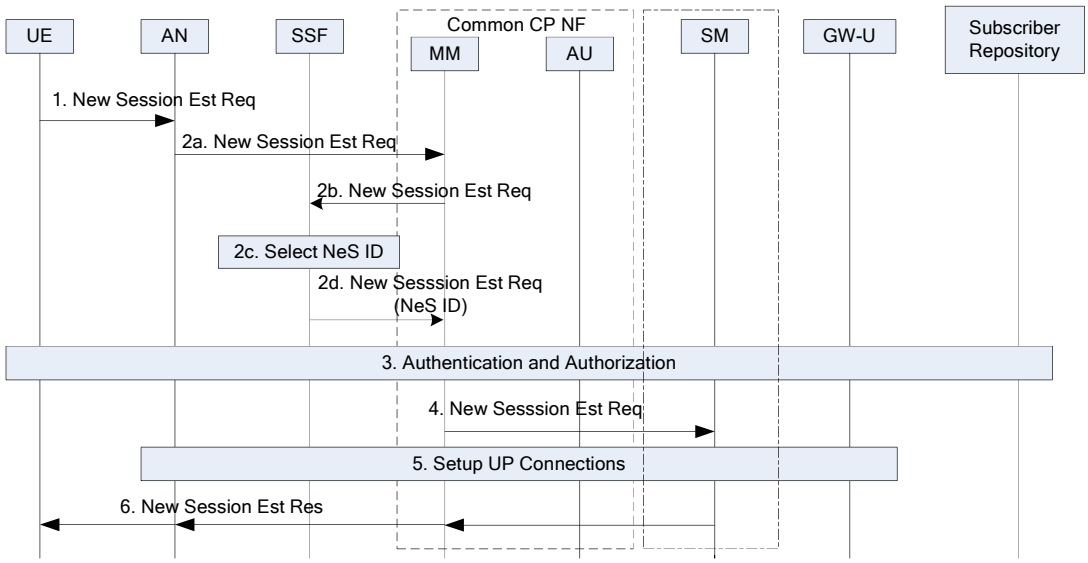


Figure 6.1.1.1-3: New session establishment request procedure after an initial attach request.

1. The UE sends a request for establishment of a new session.
2. Slice Selection Procedure for the new session establishment request:
   a. The New Session establishment request is forwarded by the AN to the common CP NF based on the UE temporary ID , which was allocated during the attach procedure
   b. If the Common CP NF does not know which non-Shared Slice CN part to handle this request, then the Common CP NF forwards the request to the SSF to determine which slice to select.
   c. The SSF selects the appropriate new NeS-ID. It is assumed the new NeS-ID shared the same type of Common CP, but with different type of non-Shared Slice CN part. Otherwise the reallocation of the Common CP NF is to be triggered.
   d. The SSF sends the New Session establishment request with the NeS ID to the Common CP NF.
3. Authentication and Authorization:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 56 of 501

a. If the UE has already been authenticated and the new slice requires the same authentication procedure then the AU NF only performs the authorization procedure.

b. If the AU NF is a common function for all slices then the authentication procedure is only performed for the first slice that is associated with the common MM and AU NFs.

4. The MM forwards the New Session establishment request to the corresponding SM.

5. The SM performs the session management procedure to setup the UP connection.

6. The SM sends a New Session establishment Response to the UE.

For roaming UE, the attachment procedure without PDU session establishment is similar with non-roaming case, except that the subscriber repository is located in HPLMN.

Figure 6.1.1.1-4 shows an example for new session establishment procedure after a successful attach procedure in home routed roaming scenario. In the example, the Common CP NFs in the VPLMN can be the MM functions, while the vSM NF and hSM are assumed to be NFs of non-Shared Slice CN part. It is assumed that for the roaming UE there are no Common CP NFs for the HPLMN part of network slice.

Editor's note: whether a network slice instance can span across HPLMN and VPLMN or if there are independant network slices in each PLMN is FFS.

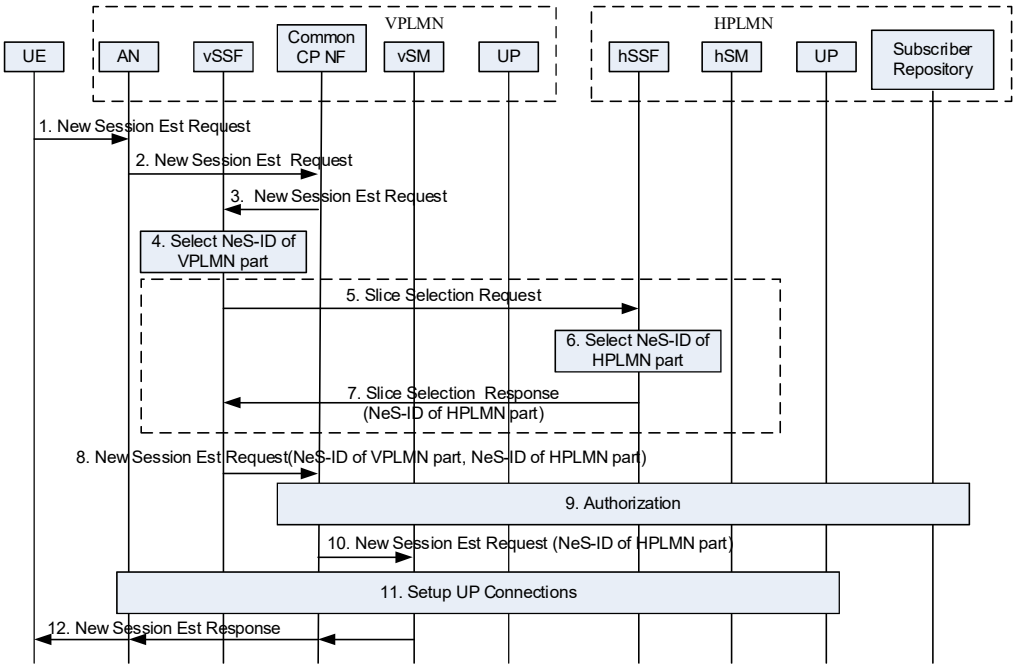


Figure 6.1.1.1-4: New session establishment request procedure in home routed roaming scenario.

1. The UE sends a request for establishment of a new session.

2. The new session establishment request is forwarded by the AN to the Common CP NF in the VPLMN based on the UE temporary ID, which was allocated during the attach procedure.

3. If the Common CP NF does not know which non-shared Slice CN part to handle this request in the VPLMN then the Common CP NF forwards the request to the vSSF (i.e. SSF in the VPLMN) to determine which VPLMN part of slice to select.

4. The vSSF selects the appropriate NeS-ID of VPLMN based on UE's subscription information, UE usage type, service type, UE capability, and the HPLMN ID.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 57 of 501

5. The vSSF sends a Network Slice selection request to the hSSF (i.e. SSF in the HPLMN), which includes the UE ID, service type, and the selected NeS-ID of the VPLMN part of slice.

NOTE 3: If the NeS-ID is standardized or can be understood by the HPLMN, the hSSF can select the HPLMN part of slice by using the NeS-ID of the VPLMN part as a reference.

NOTE 4: The vSSF can derive the IP address of the hSSF via mechanisms discussed in KI #7.

Editors' note: how vSSF decide whether it need to contact to hSSF is FFS.

6. The hSSF selects a NeS-ID of HPLMN part of slice based on the information included in the Network Slice selection request.

7. The hSSF sends a Network Slice selection response to the vSSF, including the selected NeS-ID of HPLMN part of slice, or IP address of the SM NF in the selected HPLMN part of network slice.

8. The vSSF sends the session establishment request to the Common CP NF with the selected NeS-ID of the VPLMN part of slice and the NeS-ID of the HPLMN part of slice or IP address of the hSM NF.

9. The authorization procedure is performed by Common CP NF and subscriber repository.

10. The Common CP NF forwards the session establishment request with the NeS-ID of the HPLMN part of slice or IP address of the hSM NF to the corresponding vSM.

NOTE 5: The Common CP NF determines the corresponding vSM NF based on the NeS-ID of the VPLMN part of slice.

11. If the IP address of the hSM NF is not included in the session establishment request, the vSM uses the NeS-ID of the HPLMN part of slice to select the hSM via mechanisms discussed in KI #7. Then the vSM and hSM perform session management procedure to setup the UP connection. The details should be discussed in Session management Key issue.

12. After the session establishment finished, the vSM sends a session establishment response to the UE via the Common CP NF.

NOTE 6: If both VPLMN and HPLMN have roaming agreement to use same NeS-ID for same service type, then only one NeS-ID is need in this call flow, and step 5-7 can be omitted.

6.1.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.2 Solution 1.2: Network slice selection

This is a solution for key issue 1 on support for network slicing. This solution is focused on supporting the Group-B type of network slicing as described in Annex-D. The UE related NG2 and NG1signalling are handled by a set of Common Control Network Functions (CCNFs) as shown in figures 6.1.2-1 and 6.1.2-2. Figure 6.1.2-1 depicts the non-roaming architectural concept of this solution to support the Core Network Slicing. In this architecture, the Core network part of the Network slice is sharing some network functions with other Core Network part of Network slices which serve the same UE, including the NG1 and NG2 terminations, in the CCNF. In the remainder of this Solution description we may refer to the Core Network part of a Network Slice as Core Network (or CN) Slice, and to the Radio Network part of a Network Slice as RAN Slice.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 58 of 501

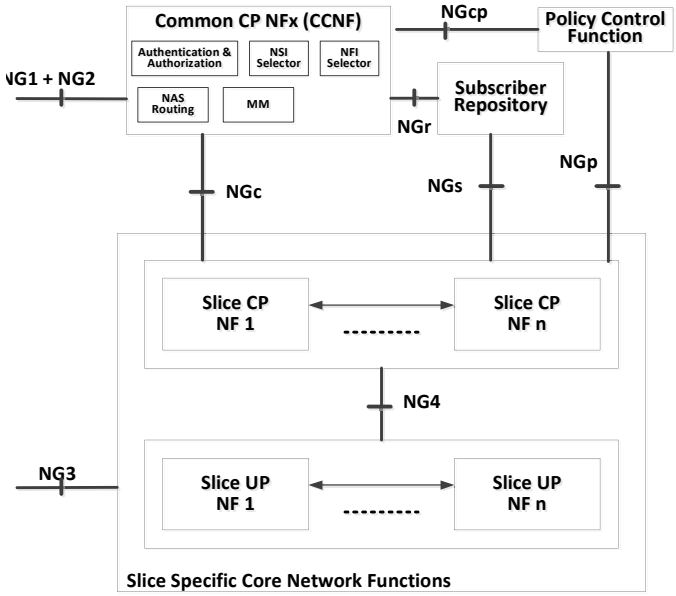


Figure 6.1.2-1: Core Part of Network Slicing concept (Non-roaming scenario)

In this architecture, once the UE is assigned to CCNFduring the attach procedure, as described below in subclause 6.1.2.2.3.1, the signalling connection between the UE and the CCNF is based on the UE Temporary ID, i.e. the RAN part of the network slice routes UE signalling to the CCNF based on the Temporary ID the UE provides in RRC signalling. The CCNF is logically part of all the Network Slice Instances (NSIs) that are being used for the UE. So when a new NSI is added or an existing NSI is removed to/from the set of slices used by a UE, a more optimal CCNF may have to be selected to serve the new set of NSIs used for the UE, thus triggering a CCNF redirection procedure. Figure 6.1.2-2 shows UE1 and UE3 with 3 slices accessing multiple core network slice instances (NSIs) and therefore multiple Slice-Specific Core network Functions (SCNF) (see section 6.1.2.1) via CCNF-1; UE2 is associated with 1 NSI and is assigned to different CCNF-2 after the UEs attach to has occurred. Note that, prior to the UE being assigned to a Serving CCNF during the attach procedure (e.g. due to the processing of the network policy or subscription policy), a UE signalling may be first routed by the RAN to a default CCNF based on RAN Routing policy, if the UE has no Temporary ID yet. Further details on the CCNF assignment are described in the later sections.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 59 of 501

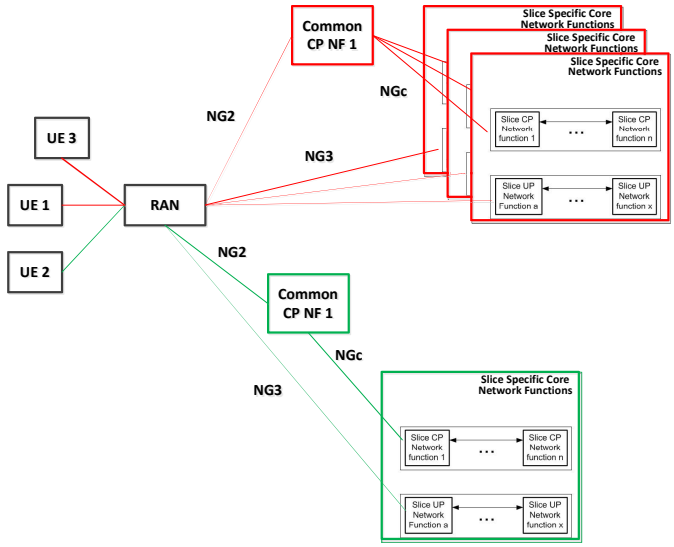


Figure 6.1.2-2: UEs assigned to Core part of NSI after Attach.

6.1.2.1 Architecture description

This solution is based on the following fundamental architecture principles for network slicing:

- In this proposed architecture, the control plane of the NextGen Core is partitioned into two types of Network Functions (NFs).
  - Common Control Plane Network Functions (CCNFs), and
  - Slice-specific Control Plane Network Functions (SCNFs)

  The CCNF is the set of fundamental control plane network functions to support basic functions operation common among the NSIs within a NextGen Core. The CCNF functions are: Subscriber Authenticator and Authorisator, Mobility Management, Network Slice Instance Selector (NSI Selector), Network Function Instance Selector (NFI Selector) and NAS Routing Function. In order to support the CCNF operation, CCNF uses the Subscriber Repository to support UE authentication and for UE subscription data retrieval (e.g. operator's policy towards the UE's requested service, QoS and security policy etc.)

- To support the selection of a particular NSI for a UE, this solution proposes that an MDD (Multi-Dimensional Descriptor) may be configured in the UE. The definition of the MDD is provided below in clause 6.1.2.1.1. The UE may providethe MDD in RRC and in the NG1 (NAS) signalling, during the UE attach. The RRC layer may route NAS signalling to a CCNF based on the assistance of MDD during the attach procedure, if the UE does not provide a valid Temporary ID for the PLMN if available. Once the CCNF is selected at attach time, a Temporary ID is provided to the UE for the subsequent UE's NAS messaging to its serving CCNF. This Temporary ID is included in the RRC signalling to enable such routing of NAS signalling.

- By leveraging also the UE's capability and subscriptions data from the subscriber repository in addition to the MDD, the UE is authorized at attach time to access certain NSIs that correspond to certain MDD values, and the target NSI(s) are selected by the NSI selector of the CCNF. This creates a context in the CCNF for the given UE which defines the binding between the MDD vectors and the corresponding NSIs. Any PDU session establishment in these NSIs may happen via subsequent SM signalling after attach, or related SM signalling containers could be embedded in the attach request.

  Note that, while NSIs are selected, it is possible the CCNF that was initially selected by the RAN (e.g. default CCNF) for the UE is not the most optimal based on operator policies, so a CCNF change may happen and the UE is redirected to an optimal Serving CCNF; otherwise, the default CCNF becomes the Serving CCNF if it is considered suitable based on operator policy. If the UE is not configured with an MDD, the

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 60 of 501

network may provide a default MDD at attach time based on UE subscription information and other criteria as discussed below.

Once the NSIs applicable to the UE are selected and with that the Serving CCNF, the Temporary ID and the Accepted MDD may be used by the UE for the subsequent NAS signalling as necessary for each individual NAS message.

- It should be possible for the UE or a PLMN to change the set of NSI(s) a UE is using depending on the type of application and service it requires, or depending on changes to UE's subscription or operator's policy etc. This may depend on factors such as UE capabilities, configuration and authorization.

Editor's note: It is FFS on how to perform the steering to a different NSI.

Editor's note: The non-3GPP access aspects are FFS.

6.1.2.1.1 Network Slice and Network Function selection

In order to perform NSI selection, the NSI selection principle should enable the selection of the appropriate set of network function to deliver a certain service and/or for a certain use case.

A network slice fulfils at least a couple of purposes for a UE:

1. It offers a UE particular system behaviours tailored to specific application needs, from the standpoint of specific control plane (e.g. a UE may not need MT procedures, or require optimal behaviour for massive MTC, or Critical communications, etc.) or user plane behaviours (e.g. the UE may need a slice supporting header compression)

2. It offers a UE access to resources allocated for a specific Service or Application domain, or a Tenant (e.g. minimum level of guaranteed resources or aggregate number of subscribers allowed to access the service at any point in time)

In summary, Tenant represents an organization, agency, application (or application class) or business entity which is entitled to access the service for the use of guaranteed network resources through a predefined Service Level Agreements and Policies with the network operator.

For example,a Tenant of PLMN resource e.g. is a wholesale customer of the PLMN(e.g. a big company, or an agency which requires a PLMN to provide at least access to a predefined set of resources, or some specific policies in handling its slices subscribers at times of congestion).A PLMN may apply tenant specific policies at times of overload. An example of a tenant may be some public safety agency. The tenancy concept may also be needed to meet application specific requirements. For instance let us consider an enterprise deployment: in the enterprise, we may have a factory floor set of devices and devices that are associated to non factory floor operations. The enterprise may have a policy to allocate at least 60% of resources (whether in the RAN or in the Core) to factory floor operation at times of congestion but not to segregate resources at all times. So the enterprise may set up a tenanted slice so that factory floor devices get at least 60% of resources at times of congestion.

Therefore at least two dimensions can identify a slice and these are the components of a Multi Dimensional Descriptor (MDD) vector:

- one identifying a tenant (identified by the Tenant ID component of an MDD vector)

- one identifying the network behaviours for the target network service identified by the Slice Type component of an MDD vector (e.g. eMBB service, CriC, mMTC or other behaviours which may also be operator specific).

An MDD vector can be PLMN specific or standardized. When a MDD vector is PLMN specific, the UE stores the PLMN ID of the PLMN that assigns the MDD vector. The UE shall not use this MDD vector outside the PLMN that assigns it as it identifies a PLMN specific slice, not available elsewhere. Standardized MDD vectors can be used in all PLMNs. Federations of PLMNs may agree on common values of MDD vectors and support the same slice types, but this outside the scope of 3GPP.This is to say, in summary, that the value of Tenant ID and Slice Type may be standard or operator specific.

The Tenant ID field may have a standard value that indicates to the network that it is to be ignored (so the MDD vector is effectively only based on one dimension, i.e. the Slice type field).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 61 of 501

Information such as UE's capability, UE's location (based on the UE's serving access) may also be used to support the UE authorization to access and to select a slice, and therefore to be authorised to use a certain MDD vector in the PLMN.

The MDD is a matrix that indicates in each of its rows a slice the UE may request to access or address. If the NSI to be accessed is only one, the MDD is just a single MDD vector. A row in the MDD is referred to as MDD vector.

For instance, UE1 in Figure 6.1.2.1.1-1 may indicate the following MDD at attach time to request the network to allow it to use slices from the same tenant in parallel.

Tenant ID=1	Service Descriptor/Slice type = 1
Tenant ID=1	Service Descriptor/Slice type = m

However, for example and illustrative purposes only, if the UEs just needed to access the first slice of the two in the MDDs above, to e.g. send UL data for that slice, they both may indicate to the network in the RRC signalling needed to establish the RRC connection the following MDD.

Tenant ID=1	Service Descriptor/Slice type = 1

A network may configure the RAN to use the whole MDD or part of it, if available in RRC signalling, to assist the routing of NAS Attach request messages in a RRC connection that was established without the indication of a valid UE temporary ID for the PLMN. This allows the Attach request to be routed to a more suitable CCNF which would otherwise be selected if the network would just apply a load balancing based policy without using the MDD.

For access control purposes, or overload control, and in general for the NextGen system slicing support, the RAN may be configured to act on the whole MDD or just a part of it.

The network may also refer to the MDD alongside other information (e.g. subscription, UE capabilities) available to the network to choose the appropriate Network Slice Instances and network functions which the UE can use. The Attach accept includes the MDD indicating the MDD vectors of the active NSIs the Ue has been authorised to use.

The UE may be provisioned with MDD values to be used or the UE may obtain these from the network during the attach procedure.

The UE uses the last accepted MDD vectors to address the active set of NSI.

For the case of PLMN-specific values of the MDD fields, they are always provisioned as a (PLMNID, Value) pair and the UE shall not use these when camping on PLMNs different than the one associated to the value, (e.g. if a Slice Type is applicable just to a certain PLMN, it shall be stored in the UE as (PLMN ID, Slice Type).

Figure 6.1.2.1.1-1 depicts the semantics intended by the MDD with UEs that can access a single tenant slices. The case of UEs accessing multiple tenant NSIs is also possible as long as these NSIs do not require their dedicated CCNFs.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 62 of 501

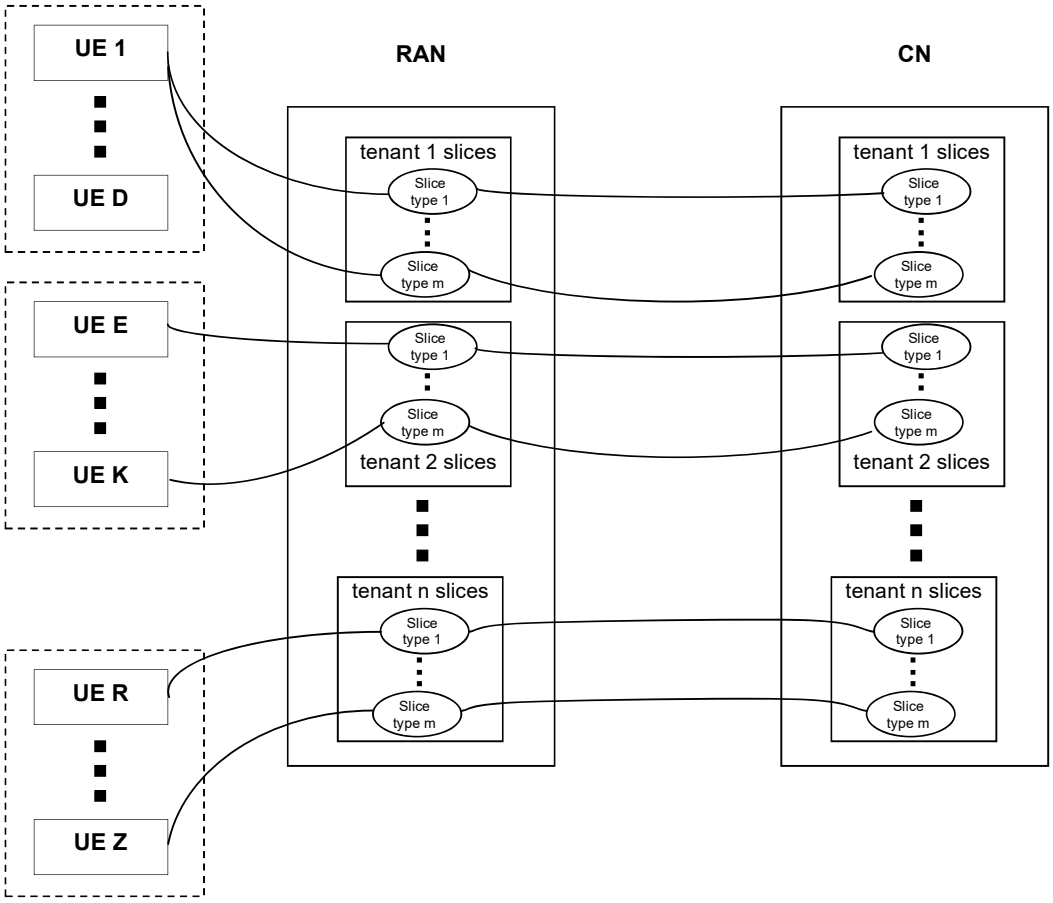


Figure 6.1.2.1.1-1: Network with n Tenants and m possible Slice Types (with UEs which can only access a single tenant slices)

In Figure 6.1.2.1.1-1, we have a network that is supporting n tenants and up to m network behaviours (slice types) in both the RAN and the core.

It is assumed to be possible for the RAN to dedicate resources to a slice.

Editor's note: How RAN implements this (RAN slicing or not) is FFS and shall be decided by RAN, including whether certain slice types require specific RATs.

The indication of the MDD (vectors)in the RRC layer during RRC connection establishment allows the RAN to apply Congestion management policies based on MDD (vectors), RAN WGs should decide which exact RRC messages shall include the MDD if available in the UE.

A CCNF that serves the PLMN can also serve multiple tenants as long as all these tenants are hosted by the same PLMN and these tenants do not request their dedicated CCNFs.

In the Core Network, receiving the MDD in NAS signalling (and maybe also in RAN-CN signalling) allows the core to handle incoming NAS signalling in accordance to policies specific to both the Tenant ID (from a resource isolation and congestion handling standpoint) and the Slice Type (from a dedicated network behaviour standpoint). It also may allow the core network to understand which NSI or a set of NSIs that a UE may request to be selected at attach time, out of a subscribed set of MDD vectors (if available) applicable to the PLMN.

In summary, NSI selection criteria should enable selection of a correct NSI for a certain application/tenant. This is a role of the NSI selector function in the CCNF.

When a PDU Session Request is sent by a UE for a certain NSI, the NFI selector will then trigger the corresponding set of control plane NFIs within the serving core NSI for the network function discovery and interconnection among themselves.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 63 of 501

Editor's note: Further details on NFIs discovery and interconnection are discussed in the separate work task related to KI#7.

6.1.2.2 Function description

6.1.2.2.1 Functions.

CCNF: the Common Control Network Functions is a group of functions that are shared across the slices concurrently supported for a UE

SSNF: Slice Specific Network Functions is the set of functions of a Network Slice that are not shared with other Network slices concurrently supported for a UE. It includes Slice CP Network functions and Slice UP network functions.

Slice CP Network functions: Control plane functions applicable to a SSNF

Slice UP network functions: User Plane functions applicable to a SSNF

PCF: the Policy Control Function, controls the Slicing Selection policies in CCNF and also Policies related to UE handling inside a SSNF

Subscriber Repository: Repository of subscription information

6.1.2.2.1 Reference points

NGc: Reference point between the CCNF and the Slice CP Network functions, used to exchange control information

NGr: it is used by the CCNF to access subscription data

NGcp: It is used by the CCNF to obtain e.g. UE Mobility polices.

NGs: It is used by the Slice CP Network functions to access subscription data

NGp: It is used by the Slice CP Network functions to obtain Policy decisions (e.g. related to QoS or charging aspects for a session PDU flows).

6.1.2.2.1 High level operation description

The binding of a UE to a set of Network Slice Instances happens when the network receives the Attach request. The set of these NSI's that are bound to a UE is known as "Active Set of NSIs". This is a high level description of the steps that are followed:

1. When a CCNF receives the attach request, it checks the UE has valid credentials and validates its IMSI (in the equivalent of an IMSI attach) or it binds the Temporary ID the UE provided to its IMSI (If the attach uses a Temporary ID). In the process, the network gains access to subscription data for the UE and a (new)Temporary ID may be assigned by the CCNF that has received the UE signalling.

   The functions of CCNFs are described as follows:

a) Subscriber Authenticator and Authorisator: is responsible to authenticate the UE for accessing the NextGen system as well as to maintain the context for UE's identity, capability and service subscription etc. to support Network Slice Instance selection.

b) Mobility Management is responsible for supporting the UE registration and MM status in the operator's network, keeping track of UE location, reachability, providing roaming support, and supporting mobility restriction

c) NSI Selector is responsible for selecting specific core network slice instance based on the MDD and other information provided by the UE (e.g. UE capabilities) and the subscriber information retrieved from the Subscriber Repository.

   - It is assumed that the NSI Selector is aware of the presence of the NSIs that were provisioned by the Network Management which is responsible to maintain the life cycle of the network slice instances. In addition, the NSI Selector is programmed with the intelligence to interpret the MDD, the UE capability, UE location and the subscriber information to select the appropriate core part of the NSI. When a specific NSI is selected based on a certain MDD vector value, the binding between NSI and the corresponding MDD vector is included in the UE's context in the CCNF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 64 of 501

d) NAS Routing function is responsible for relaying NAS message between the UE and the NSI Slice specific part, if applicable (e.g. SM messages)

e) NFI Selector is responsible for initiating the NextGen Core CP NFIs discovery among themselves as well as interconnecting with each other when the UE's serving NSI receives the PDU Session Request.

Editor's note: Further details on NFIs discovery and interconnection are discussed in the separate work task related to KI#7.

2. If the UE provides no MDD in the Attach Request, default policies in the PLMN apply which could be based e.g. on subscription information. In such case, the CCNF assigns the UE to Default set of Slice Instances and the related network selected MDD vectors are passed to the UE in the Attach Accept.

   If the UE provides an indication of initially requested MDD, then the NSI selector verifies the UE is allowed to access the corresponding NSI(s). Upon successful authentication and authorisation, the network returns the same MDD to the UE unless the operator policy has changed for the UE due to UE capabilities, UE's subscription and/or UE's serving RAN type and therefore the NSI selector is not allowing all or part of the MDD vectors to be associated to a NSI. If happens, the requested MDD will then be revised prior to be included in the Attach Accept sent to the UE for the subsequent use.

   The allowed NSI assignment to the UE can be based on the UE capabilities, assuming that the subscriber may use different types of UEs by swapping the UICC.

   In summary, it is the evaluation of the received combination of IMSI, IMEI-SV, requested MDD, UE capabilities, RAN type as well as the possible the UE's subscription which determines which Accepted MDD is returned to the UE in the Attach Accept message.

   In this step, the UE may be assigned to a different Serving CCNF different than the one the RAN had selected if the resulting set of NSIs is better served by another CCNF, or due to load considerations. In this case, the Temporary ID assigned to the UE in the Attach Accept Message is corresponding to this finally selected Serving CCNF.

3. The Accepted MDD is also included in the NG2protocol used to carry the Attach Accept message (and other DL NAS messages) to the UE so that the RAN is aware of the active set of slices for the UE.

   In general in all the cases where the RAN needs awareness of Active Slice set or applicable NSI for a transaction, the MDD or applicable MDD vector should be included in messages that the AS layer can interpret.

4. The UE, at NAS transactions subsequent to the successful attach, exiting from Idle state, will include the Temporary ID and the MDD in the RRC layer if these eventually result in slice specific resources to be required or other slice-specific outcomes.

5. The RAN handles RRC messages without a MDD in the RRC connection request using a default behaviour.

6. When a Temporary ID is present in RRC message, the Routing of NAS messages to the correct CCNF by the RAN is always based on the Temporary ID regardless MDD is present or not. If the Temporary ID is not present, then a default routing is used. This default routing of NAS messages could be assisted (and made more accurate) also if the UE includes the MDD in RRC messages.

7. If the NSI is tenanted by a third party, the third party may require an extra level of UE authentication on top of the NG system access authentication.

6.1.2.2.2 Definitions used in the solution

Temporary ID: Identifier, similar to a GUTI, which logically associates the UE to a CCNF for the UE in a PLMN on a temporary basis. It is composed of a Routing information (necessary for the RAN to route the NAS messages carried in the RRC layer to the right contact point for the selected Serving CCNF), and a value assigned by the CCNF which is used to uniquely identify the UE context it retains. If the Temporary ID is not indicated to the RAN, or it is not recognised in the RAN, the RAN applies a default routing behaviour.

Multi-Dimensional-Descriptor (MDD): The multi dimensional descriptor of a slice is typically composed of MDD vectors each comprised of a Tenant ID field that identifies an Application (e.g. a popular OTT service) or a tenant (e.g. a certain company that requires certain minimum resources in the network) and a Slice Type (which may be standard - e.g. eMBB, mMTC, criC - or operator specific). There may be default values for MDD. The MDD is used to support the

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 65 of 501

Slice Instance selection in the core and in the RAN. If an MDD vector is PLMN-specific, it is not used outside the PLMN that assigns it.

Tenant ID: Identifier of the Tenant which represents an organization, agency or business entity that is entitled to access the service for the use of guaranteed network resources through a predefined Service Level Agreements and Policies with the network operator.

Token: Temporary Identifier of UE which associates UE to both the 3rd Party Server and the network after 3rd Party authentication is conducted. When the UE uses the 3rd Party NSI and is successfully authenticated by the 3rd Party, the token is assigned by 3rd Party to both the UE and the network (CP NF). The UE sends the token included in service request to the network if it is valid.

6.1.2.2.3 Example procedures

6.1.2.2.3.1 Initial Access

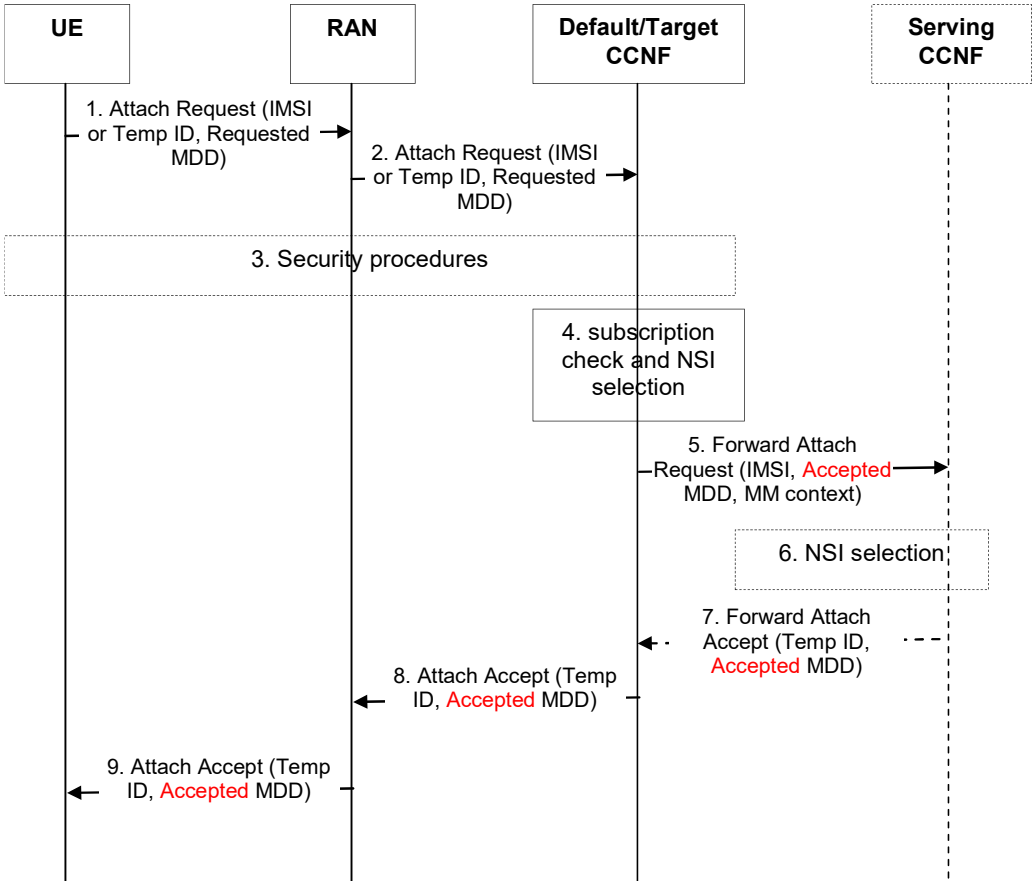


Figure 6.1.2.2.3.1-1: Initial Access

1. The UE sends and attach Request including the IMSI if a Temporary ID for the UE is not available.

   If the UE requests one or a set of NSIs to be bound to it initially, it can do so by including a Requested MDD in the Attach Request. The Requested MDD may also be included in the RRC layer to further enhance the routing to an initial default/target CCNF of the Attach Request message in the event when the Temporary ID is not available to the UE or the Temporary ID was not assigned by the same PLMN of the current network that serves the UE. The MDD in the RRC layer may also be included to enable the access to a suitable RAN resources. It is assumed the RAN maintains a MDD-based table in order to route/forward the attach request message to a proper CCNF when the Temp ID is missing.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 66 of 501

If the Temporary ID is available, the UE includes it in the RRC layer message used to establish the RRC connection, so that the RAN can route the message to the CCNF in the core which has generated it.

2. The RAN forwards the Attach Request to the Core based on the routing criteria outlined in step 1.

3. The CCNF proceeds with the procedures for 3GPP system authentication and authorization for the UE.

4. If the UE is successfully authenticated, its subscription data is checked and the allowed MDD vectors are decided (which will form the Accepted MDD which will be returned to the UE in the Attach Accept), alongside the compatibility of the CCNF with these MDD vectors. It the CCNF detects it is not an appropriate handler for the UE step 5 is executed immediately without binding of NSIs to MDD vectors occurring in this CCNF.

The CCNF decides the initial set of NSI(s) for the UE based on an evaluation of the Requested MDD, Subscribed MDD (if available), UE capabilities, UE's subscription policy, UE's serving RAN type etc. The following may apply:

- if the UE did not provide the Requested MDD, the network assigns the UE to the default NSI (s)
- if the UE did provide the Requested MDD, the network assigns the UE to the NSI(s) that the UE is authorized for.

  - if some Default NSI(s) was missing from the requested MDD, the UE is still assigned to these NSI(s) and the corresponding MDD vector(s) is added in the Accepted MDD

The Accepted MDD and is passed to the UE in the Attach Accept message.

If some DNNs are specific to some MDD vectors (e.g. based on subscription data), the mapping of these DNNs to MDD vectors is recorded in the UE context in the CCNF.

The procedure continues to step 8.

5. If the UE is not suitably handled by the (Default/Target) CCNF where the Attach Request was routed to, this CCNF may redirect the UE to a new Serving CCNF that is more optimal (or less loaded) for the selected slices. Then, the Default/Target CCNF forwards the attach request to the new Serving CCNF with an indication that it is a forwarded attach together with IMSI , the MM context including the NAS key and Accepted MDD (which was determined to evaluate CCNF compatibility in step 4) in order to indicate that the UE has been authenticated for NSI(s) Assignment as described in step 4.

6. The Selected Serving CCNF performs the NSI selection as described in step 4 above.

7. The Selected Serving CCNF binds the UE to the selected NSI(s) by creating the related context associating the Accepted MDD vectors to the NSI(s) for the UE and then sends back the Forwarded Attach Accept message with Temporary ID and the Accepted MDD for subsequent usage by the UE. If there are any DNNs that are specific to any MDD vectors, the mapping is passed to the UE also.

8. If the steps 5 to 7 were executed, the Serving CCNF sends to the RAN the Attach Accept in a NAS message including the content as described in the message in step 7 above. Otherwise, the Default/Target CCNF, which is now the Serving CCNF, binds the UE to the selected NSI(s) by creating the related context associating the Accepted MDD vectors to the NSI(s) and then sends Attach Accept message with Temporary ID the Accepted MDD for subsequent usage by the UE and any DNN to MDD vector mappings. The Serving CCNF includes the Accepted MDD in the NG2 transport.

9. The RAN forwards the Attach Accept received in step 7 or 8 to the UE

It is possible to include in the Attach Request an SM container so that the PDU sessions are established for all or a subset of the Active NSIs for the UE. Alternately a subsequent SM message exchange could be used to establish the PDU sessions for the NSIs that need these.

Editor's note: How the NSI matching a certain MDD is obtained in steps 4 and 6 is to be decided together with SA5.

6.1.2.2.3.2 Subsequent NAS signalling - PDU Session Request

The following procedure describes how a PDU session can be established with an existing NSI identified by a certain accepted MDD vector.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 67 of 501

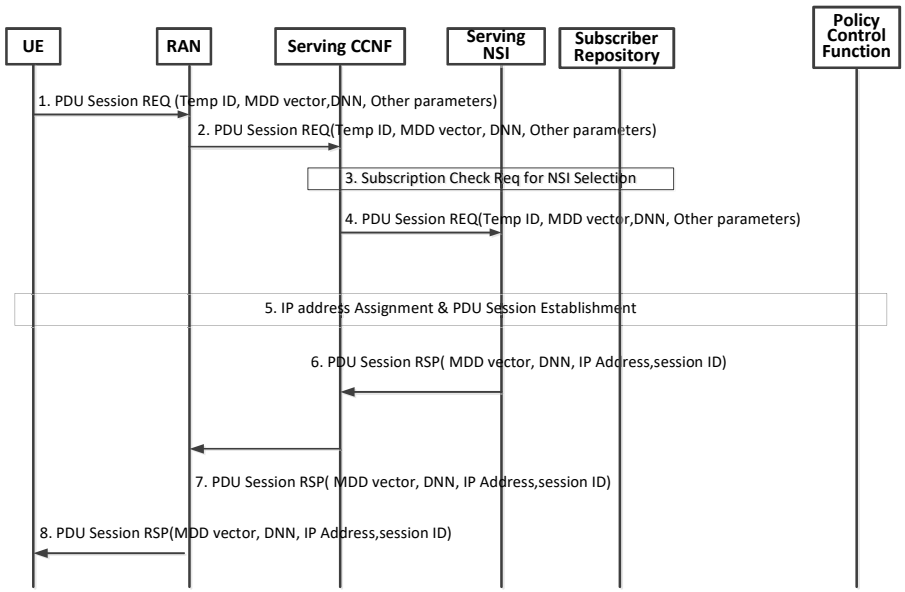


Figure 6.1.2.2.3.2-1: Subsequent PDU Session Request Slicing Procedures

1. The UE initiates the PDU Session Request message to request for the service by including the Temporary ID, the MDD vector of the NSI that the PDU session applies to, the DNN of the PDN connection and the related parameters (e.g. QoS). The UE includes the routing field of the Temporary ID in the RRC layer message for the RAN to route the NAS Message to the appropriate Serving CCNF. If the DNN is omitted a default or a set of default DNN connections in the NSI are established.

2. The RAN routes and forwards the NAS message to the proper Serving CCNF based on the information in step 1.

3-4. Serving CCNF verifies with Subscriber Repository if the requested DNN is subscribed- for the NSI that is identified by the MDD vector. If the DNN is allowed the NFI Selector forwards the PDU Session REQ to the target NSI.

5. SM function will then proceed with the PDU Session Establishment procedures accordingly and the operation details should refer to KI#4.

6-8. Once the step 6. above is complete, the serving NSI completes the PDU session establishment procedure by sending the PDU Session Response to the UE through RAN.

6.1.2.2.3.3 Subsequent NAS signalling for PDU Session Modification

This message flow represents a PDU session modification for a PDU session previously established in a certain NSI. Other parameters in the NAS message (e.g. the DNN in certain session management messages, or QoS parameterts etc.) beyond MDD vector and the Temporary ID related ones are not discussed here in this procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 68 of 501

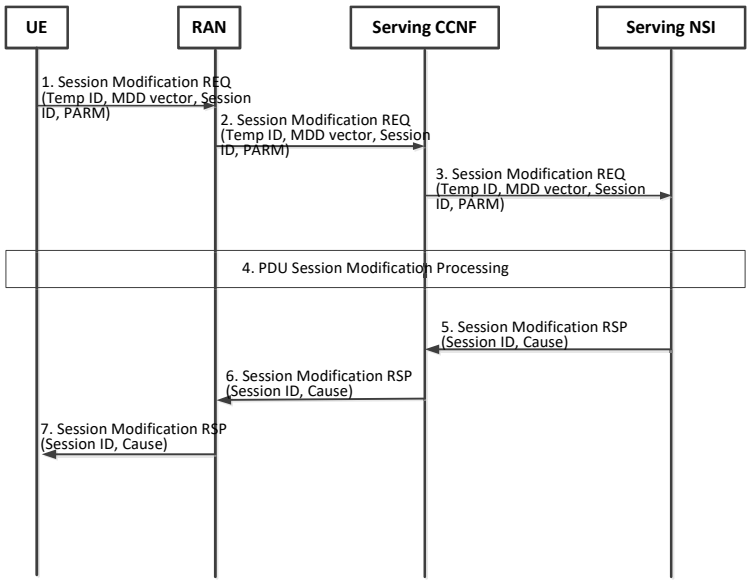


Figure 6.1.2.2.3.3-1: Subsequent Session Modification Request Slicing Procedures

1. The UE initiates Session Modification Request procedure after the PDU session was established in the target NSI, so it sends a Session Modification Request message including its Temporary ID, the MDD vector of the NSI and the Session ID and the related parameters (e.g QoS). The MDD vector is included since a specific NSI needs to be addressed by the NAS procedure. The UE includes at least the routing field of the Temporary ID in the RRC layer message for the RAN to route the NAS Message to the appropriate Serving CCNF.

2. The RAN routes and forwards the NAS message to the proper Serving CCNF based on the information in step 1.

3. The Serving CCNF forwards the Session Modification Request to the NSI indicated in the MDD vector

4. The PDU Session Modification REQ is processed. The operation status is captured in the cause to be responded to the UE.

5. The Serving NSI responds to the UE by sending to the RAN a Session Modification Response NAS message with the cause.

6-7. The CCNF and RAN forward the Session Modification Response message the CCNF has received in step 5 to the UE.

6.1.2.2.3.3 Reselection of a Network Slice after UE Registration

After the UE is registered with a CCNF, the network's local policies may change, or the UE subscription information may be updated, or an updated MDD may be sent by the UE. As these factors may determine the selection of a particular slice for a UE, the update may lead to a modification of the Active set of Network Slice Instances for the UE. This in turn may lead to the need to change the CCNF as the current CCNF may not be any longer suitable for the active set of slices. In general, the modification can be network triggered or UE triggered as described below.

6.1.2.2.3.3.1 Network Triggered Reselection of a Network Slice

Based on the network policies or updated subscription information, the network determines a new MDD that is allowed for the UE. With the new MDD. The Network slice Instance Selection Function is triggered to evaluate the applicable NSIs for the UE and the following procedure in figure 6.1.2.2.3.3.1-1:

Editor's note: whether a change of MDD can occur for a UE without a change of NSI or CCNF is FFS.

Editor's note: how a change of NSI or CCNF is done due to load balancing or other reasons not described above is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 69 of 501

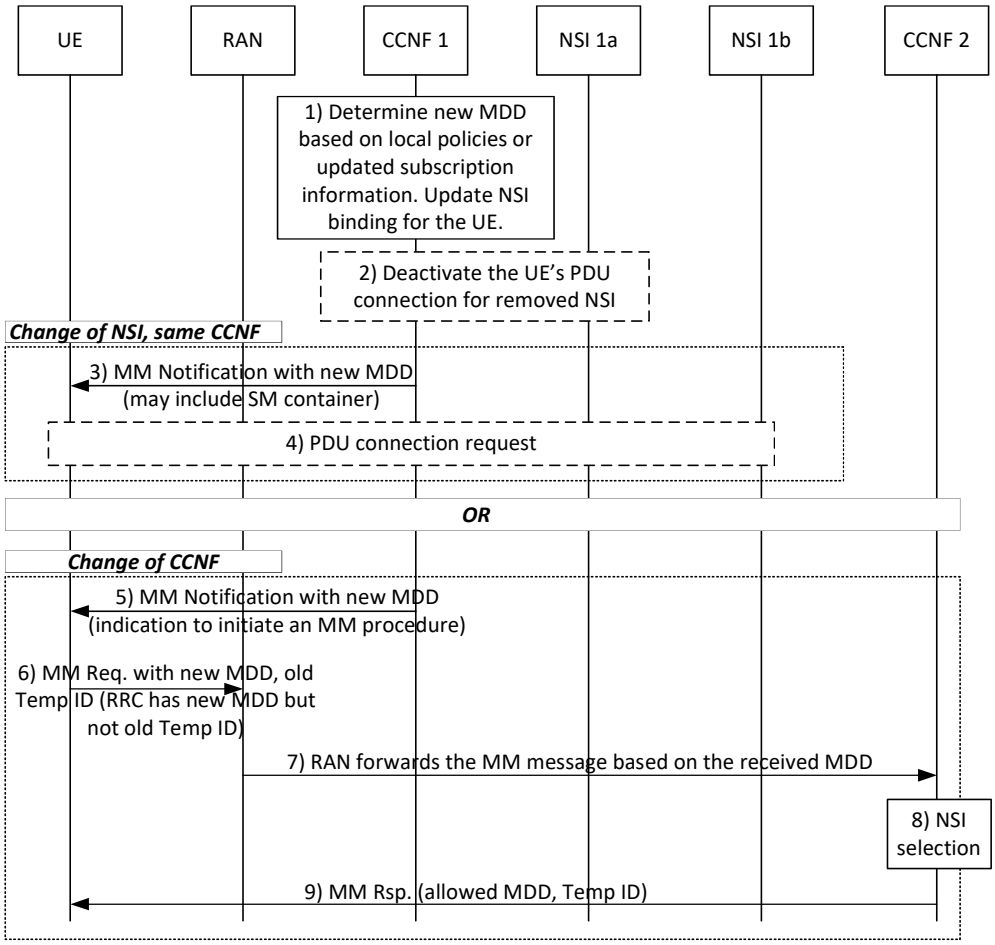


Figure 6.1.2.2.3.3.1-1: Network Triggered Reselection of the Network Slice

1. The network determines a new MDD for the UE be based on local policies or updates subscription information. The network updates the NSI binding for the UE.

2. The CCNF may deactivate a PDU session for the NSI that has been removed for this UE.

   If the same CCNF can serve the UE, the procedure continues with step 3. If the current CCNF needs to be reselected, then the procedure continues with step 5 directly.

3. The CCNF sends an MM Notification message to the UE and includes the new MDD. The MM message may also carry an SM message for any PDU connection that may have been deactivated.

4. If required, the UE may establish a new PDU session using the new MDD. For a change of NSI only within the same CCNF, the procedure ends here.

5. If the serving CCNF determines that the CCNF should be reselected for this UE, the CCNF sends an MM Notification message with the new MDD. The message also includes an indication for the UE to initiate an MM procedure. The UE updates its currently used MDD vectors set accordingly. The MM message may carry an SM container indicating in an SM message which PDN connections are released if applicable.

6. The UE sends an MM Request message including the new MDD and the old Temp ID that was provided by the first CCNF. The UE includes the new MDD in the RRC message but does not include the old Temp ID in the RRC message. The MM message may carry an SM container indicating in an SM message which PDN connections are to be established if applicable

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 70 of 501

7. The RAN forwards the NAS message to the appropriate CCNF that is determined based on the new MDD in the RRC message. The new CCNF may use the old Temp ID to fetch the UE's context from the previous CCNF.

8. The new CCNF performs NSI selection and binding for the UE.

9. The CCNF sends an MM Response message to the UE including the allowed MDD and a Temp ID that points to this CCNF. If required, the UE may subsequently request a new PDU session using the allowed MDD.

6.1.2.2.3.3.2 UE Triggered Reselection of a Network Slice

A UE may be configured with an MDD that has multiple vectors. The UE may be using at a given point in time a subset of the whole set of MDD Vectors it is configured with. If the UE requires to use a different set of MDD vectors, different from what is currently being used, e.g. due to a need for a new PDN connection or other local UE policies, the UE executes this procedure.

When the request is triggered by a need for a new PDN connection, the UE sends the updated MDD in the NAS MM message that also carries the SM message in a SM container. If the requested is triggered for other reasons e.g. local policies in the UE, then the UE sends an MM message with the updated MDD.

NOTE : the exact MM message to use for sending an updated MDD that is not triggered by a SM request is up to stage 3 working groups to define.

The overall procedure is described in the figure below.

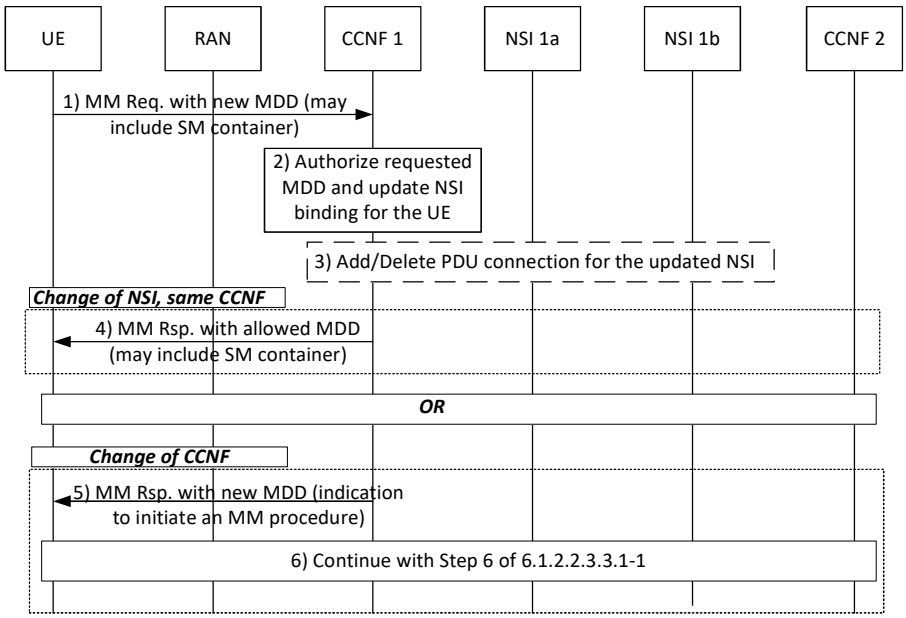


Figure 6.1.2.2.3.3.2-1 – UE Triggered Reselection of the Network Slice

1. The UE sends an MM Request message to the network with the new MDD. If the updated MDD is triggered by a SM request, the MM message will also carry an SM message in a SM container.

2. The network verifies if the updated MDD is allowed for this UE based on local policies and subscription information. The CCNF updates the NSI binding for this UE accordingly.

3. If the NAS message contained a SM request, the network processes the SM request if authorized. The CCNF may add or delete an NSI based on the authorized MDD update.

   If the CCNF determines that only the NSI should be changed for the same CCNF then the procedure continues with step 4. If the CCNF determines that a reselection of the CCNF is needed, then the procedure continues with step 5 directly.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 71 of 501

4. For a change of NSI only, the CCNF sends an MM Response message to the UE with the allowed MDD. The MM message may carry an SM container indicating in an SM message which PDN connections are released if applicable. If the updated MDD leads to a change of NSI only, the procedure ends here.

5. If the CCNF determines that a CCNF reselection is needed, the CCNF sends an MM response message with the allowed MDD and an indication for the UE to initiate an MM procedure.

6. The UE continues with step 6 of 6.1.2.2.3.3.1-1.

6.1.2.2.3.4 New Service Request and User Authentication by the 3rd Party

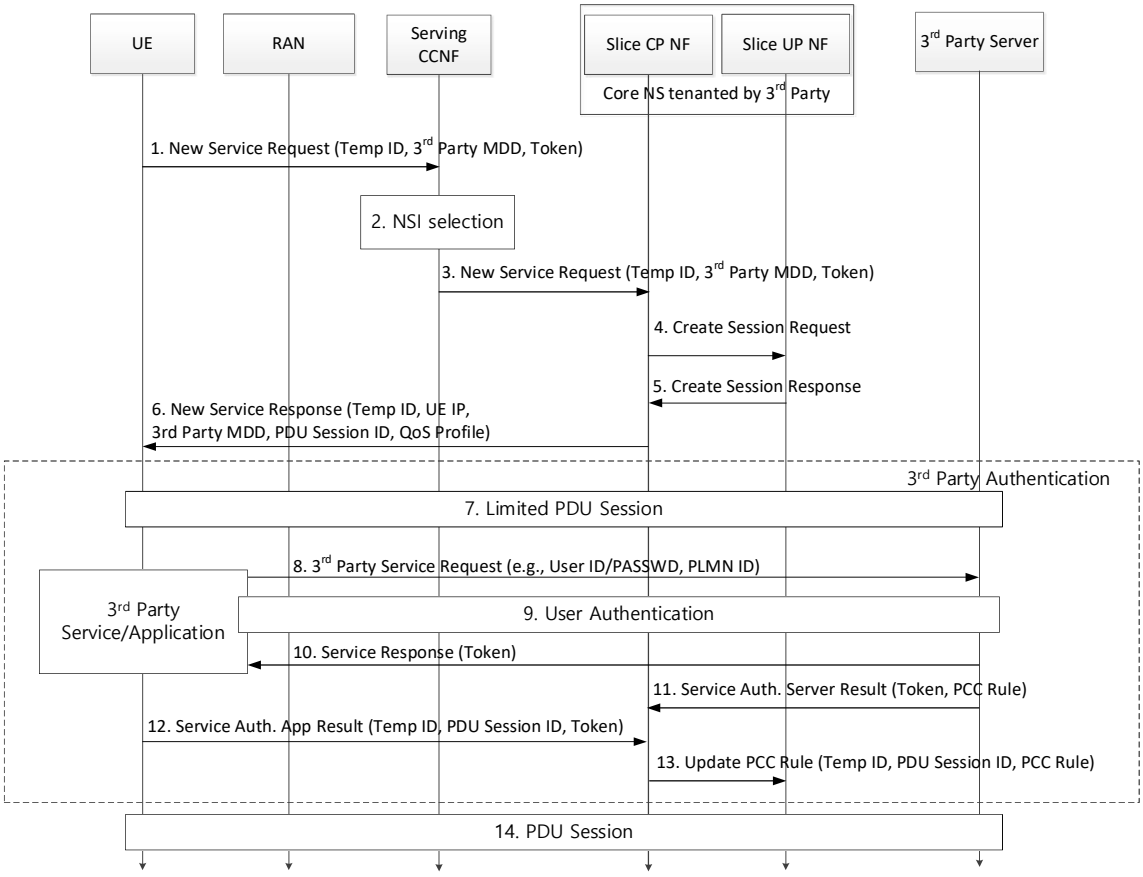


Figure 6.1.2.2.3.4-1

1. When the service/application associated with the 3rd Party MDD which is not sent at the Attachment starts, the UE sends a New Service Request message including its Temporary ID, a 3rd Party MDD, a token if available and related signature for the network validate the UE. If the service/application is not associated with any MDD, the UE may send a New Service Request message without the MDD.

Editor's note: Configuring the 3rd party MDD in the UE and identifying which MDD is associated with which service/application are FFS.

The RAN routes and forwards the New Service Request message to the proper Serving CCNF based on Temporary ID.

2. Serving CCNF selects the NSI for the UE based on an evaluation of the 3rd party MDD, UE capabilities, UE's subscription policy, UE's serving RAN type etc.

3. The Serving CCNF forwards the New Service Request message to the selected Core NS CP NF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 72 of 501

4. The CP NF assigns a PDU Session ID and sends the Create Session Request message including Temporary ID, PDU Session ID and PCC rule for the session. The CP NF provides the PCC rule for the session which is based on following:

   A. If the selected NSI doesn't belong to the 3rd Party, the PCC rule is retrieved from the subscription repository.

   B. If the selected NSI belong to the 3rd Party and the token is available, the PCC rule, which is previously received from the 3rd Party Server, is applied based on the Token.

   C. If the selected NSI belong to the 3rd Party and the token is not available or isn't provided by the UE, the pre-defined PCC rule which provides the limited access for authenticating the UE. Also, it has the HTTP redirection rule which makes all traffic generated by the UE forward to the 3rd Party Server.

5. The UP NF sends the Create Session Response message.

6. The CP NF sends the New Service Response message including Temporary ID, UE IP, 3rd Party MDD, PDU Session ID and QoS Profile.

7. If the UE doesn't need to be authenticated by the 3rd Party (e.g., the UE provided the valid token or the selected NSI doesn't belong to the 3rd Party), the 3rd Party Authentication procedure can be skipped. For UE authentication, the limited PDU Session is created between the UE and the UP NF. It has a limited bandwidth (e.g., 64Kbps) and HTTP redirection to redirect all the traffic from the UE to the 3rd Party Server.

8. The Service/Application in the UE sends the 3rd Party Service Request message for the User Authentication which is similar to login to the web site. This message includes the user authentication information (e.g., the user ID and the password) and PLMN ID. The 3rd Party may contract with multiple MNOs for renting NSI, so PLMN ID can be used for identifying which MNO the UE uses. This message is sent as the user data.

9. The User Authentication for using 3rd Party NSI between the Service/Application and the 3rd Party Server can be done with 3rd Party's proprietary method.

10. The 3rd Party Server sends the Service Response with a Token if the user is successfully authenticated. The Token is used to identify UE/User in the 3rd Party and the network. It has a timer, so it is valid before the timer expires.

11. The 3rd Party Servers sends the Service Authentication Server Result message to the CP NF including the Token and PCC rule. The token is the same as it sent the UE.

12. The UE sends the Service Authentication App Result message including Temporary ID, PDU Session ID and Token.

13. After the CP NF receives both Result messages from the UE and the 3rd Party Server, it verifies if the UE is appropriate to use the selected NSI. The CP NF sends the Update PCC Rule message in order to update the PDU session. It includes Temporary ID, PDU Session ID and PCC rule.

14. The PDU Session is created between the UE and the UP NF for sending/receiving PDN data.

6.1.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.3 Solution 1.3: Support of multiple connections to multiple Network Slices

This solution is to solve the key issue#1 on support of network slicing.

6.1.3.1 Architecture description

To enable a UE to simultaneously obtain services from multiple Network Slices of one network operator, the Core Network Instances can be set up as depicted in Figure 6.1.3.1-1. That is:

- A single set of C-Plane Functions that are in common among Core Network Instances is shared across multiple Core Network Instances;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 73 of 501

- U-plane Functions and other C-Plane Functions that are not in common reside in their respective Core Network Instances, and are not shared with other Core Network Instances.

Common C-Plane Functions to multiple Core Network Instances can be:

- Authentication function (AU): AU is responsible for authenticating and authorizing the UE to attach to the operator's network. It also provides security and integrity protection of NAS signaling.
- Mobility Management function (MM): MM is responsible for UE registration in the operator's network (e.g., storing of UE context) and UE mobility support (e.g., providing mobility function when UE is moving across base stations within the operator's network).

Dedicated C-Plane Functions for each Core Network Instances can be:

- Session Management function (SM): SM is responsible for PDU session establishment, PDU session modification and PDU session termination.

Editor's note: Whether there are more C-Plane functions to consider as a common C-Plane function for multiple Core Network Instances or a dedicated C-Plane function for each Core Network Instance is FFS.

As a deployment option all the C-Plane Functions can be deployed as part of a common C-Plane Function as described in figure 6.1.3.1-2.

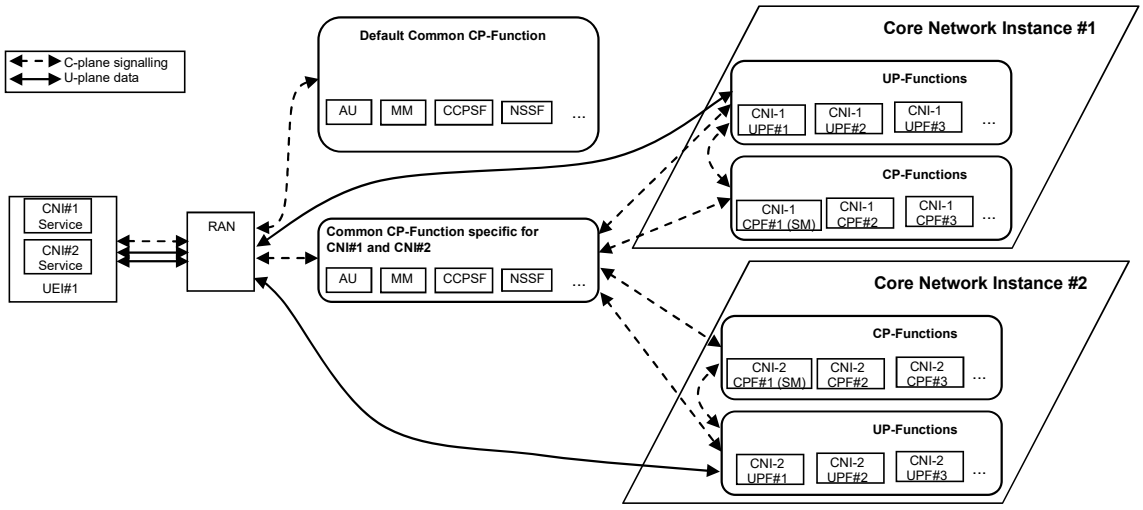


Figure 6.1.3.1-1 Sharing a set of common C-plane functions among multiples Core Network Instances

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 74 of 501

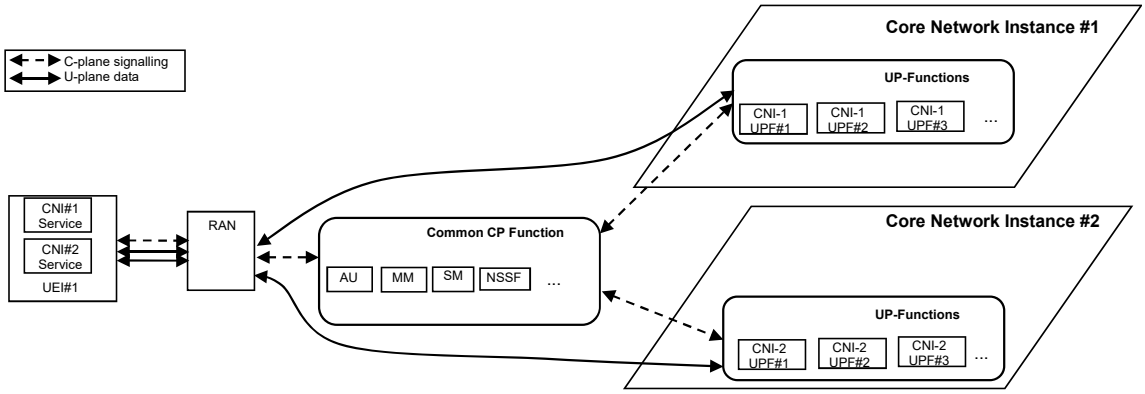


Figure 6.1.3.1-2 Sharing all the C-plane functions in a Common CP Function for all the Core Network Instances

The direct CP interface between RAN and CP-functions of CN instance is not needed, since the encrypted NAS signalling message has to be decrypted by a common C-Plane function, which has exchanged the encrypted key with the UE, for example, the AU function.

NOTE 1: In case of UE accessing a single Core Network Instance, RAN can have a direct CP interface to the specific CP function located within the Core Network Instance. In such case, those CP functions depicted as a part of common CP function are considered to be CP functions resided within the Core Network Instance, and hence, there is no common CP function.

The principles of the solution depicted in Figure 6.1.3-1 are described as following:

- A Core Network Instance consists of a single set of C-Plane Functions and a single set of U-Plane Functions.
- A Core Network Instance is dedicated to the UEs that are belonging to the same UE type. Identifying the UE type is done by using a specific parameter, e.g. the UE Usage Type, and/or an information from the UE's subscription.
- A set of C-Plane functions is responsible, for example, for supporting UE mobility if demanded or for admitting the UE into the network by performing authentication and subscription verification.
- All C-Plane Functions that are common to multiple Core Network Instances, are not necessary to be created multiple times.
- Other C-Plane Functions that are not in common with other Core Network Instances are only used by its own Core Network Instance.
- A set of U-Plane Functions in a Core Network Instance is responsible for providing a specific service to the UE and for transporting the U-Plane data of the specific service. For example, one set of U-Plane functions in Core Network Instance#1 provides an enhanced mobile broadband service to the UE, whereas another set of U-Plane functions in Core Network Instance#2 provides a critical communication service to the UE.
- Each UE can have multiple U-Plane connections to different sets of U-Plane Function that are available at different Core Network Instances simultaneously.
- The Network Slice Selection Function (NSSF) is responsible for selecting which Core Network Instance to accommodate the service/session request by the UE by taking into account the UE's subscription and the specific parameter, e.g. the UE Type, the Service Type or Domain Network Name (DNN) that can be mapped to represent the Service Type that the CNI supports.
- The RAN communicates with the common CP function or the common CP function specific for CNI via a single CP interface regardless of which CP function within the common CP that the RAN is communicating with. Hence, a common CP is considered as a black box.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 75 of 501

- The Common C-Plane Selection Function (CCPSF) is considered to be a part of common CP function, i.e. the CCPSF is assumed to be located in the common CP function. The CCPSF is responsible for determining which common C-Plane Function that the Base Station should communicate with. Determination of common C-Plane Function is done by checking with the UE's subscription profile. If the common C-Plane Function needs to be changed, CCPSF in the serving common C-Plane Function is responsible for reselecting target common C-Plane Function.

NOTE 2: The CCPSF is not a function to route the NAS signaling message to the right Common C-Plane Function. In this solution, it is assumed that the RAN has a function to route the NAS signalling message to a proper Common C-Plane Function by taking the information that is sent by the CCPSF in case of the first initial connection request or by the UE in case of any subsequent NAS messages.

- Both default common CP function and common CP function specific for CNI have the MM, AU, CCPSF and NSSF as depicted in the Figure 6.1.3.1-1. However, there can be different variants of MM and AU function. For instance, MM for MBB service might be different than the MM for MTC service. In case, the UE want to connect both the services, only one common CP function selected as explained in Figure 6.1.3-2.

- When the UE establishes PDU session, the PDU session is identified as follows:

  Option 1: Each Core Network Instance has instance identity which uniquely identifies Core Network Instance. This identity is transferred to UE and the UE includes Core Network Instance Identity in each session management message. The PDU session is identified by combining Core Network Instance Identity and PDU session identity assigned by SM function.

Editor's note: It is FFS which C-Plane function allocates Network Slice Instance Identity.

  Option 2: C-Plane Functions that are common to multiple Core Network Instances allocates PDU Session Identity when a UE requests new PDU session. The PDU session identity is transferred to the SM function.

Editor's note: It is FFS which C-Plane function allocates PDU Session Identity.

  Option 3: Operator configures different PDU session identity pool in each Core Network Instance.

  Option 4: The UE assigns PDU session identity and it is sent to the network during the PDU session establishment procedure.

Editor's note: Only one option will be selected after evaluating above options.

In this solution, the "UE Usage Type", "DCN-ID", "Service Type" and "DNN" are used for the purposes as described below:

- "UE Usage Type" is used for identifying the type of UE, e.g., Car UE Usage Type, Smartphone UE Usage Type. This is a parameter only available in the CN and the UE is not aware of it. Similar to Décor and eDecor, different PLMNs expect to apply the same set of values for standardized UE Usage Type.

- "DCN-ID" is used for identifying a Dedicated CN (DCN) that is specific for each UE Usage Type. In addition, an operator may consider to use the DCN-ID to identify a DCN that is specific for the enterprise of the same UE Usage Type or even for the different variants of dedicated CN. An example for the latter case could be to have different variants of dedicated CN for CIoT UEs, i.e. supporting different CIoT optimization features as specified in TS 23.401 [2]. In other words, DCN-ID is used to determine which common CP function that is specific for this UE Usage Type and (optionally) for a specific enterprise of this UE Usage Type. For instance, one could think of having a different DCN for different car enterprises, although UE from these enterprises belong to the same type of UE. This is the parameter that may be preconfigured at the UE or provided/updated by the CN during the initial Attach procedure. Similar to Décor and eDecor, this DCN-ID can be standardized value or PLMN specific. When the UE roams to a visited PLMN, the UE may provide this DCN-ID to the CN. If the Temporary UE identity for this visited PLMN is not provided by the UE, the RAN may use this DCN-ID to route the Attach request to the common CP function according to its RAN pre-configuration. In case this DCN-ID is not up-to-date for the visited PLMN, redirection to another dedicate common CP function that corresponds to the latest UE's subscription is hence needed.

- "Service Type" is used for identifying what type of service that the Core Network Instance (CNI) is supposed to support, e.g., the car UE may want to access multiple CNIs simultaneously that supports eMBB service and V2X service. There can be both standardized Service Type applicable to all PLMNs or PLMN specific Service Type. This Service Type will be stored at the UE and can be updated according to the operator's policy from the PLMN that the UE is roaming to.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 76 of 501

- "Domain Network Name (DNN)" is used for identifying the Packet Data Network (PDN) that a UE wants to communicate with for a certain service type, e.g., DNN#1 for Internet service that requires Mobile Broadband service.

- Temporary UE identity is a temporary identifier provided by the CN to the UE. This is similar to GUTI in EPS case. This temporary UE identity consists of two parts: 1) identifier of Common CP function, 2) UE specific identifier. The RAN routes the UE's NAS signalling message to the address of Common CP function as specified in the temporary UE identity.

Taking the above explanation into account, selecting a proper CNI for the service type that is requested by the UE can be done by using the DNN parameter.

6.1.3.2 Function description

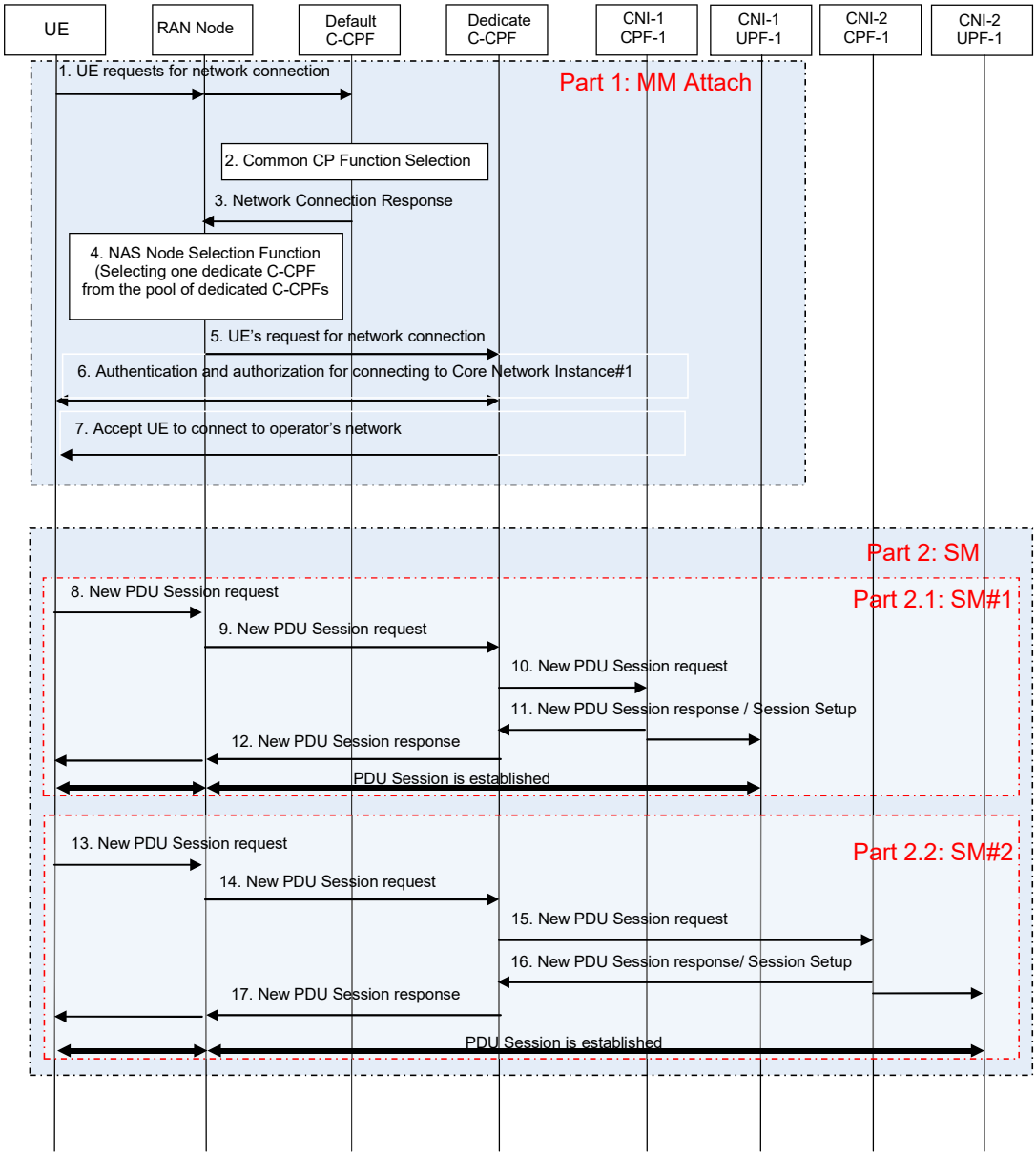


Figure 6.1.3-2 Signalling flow for supporting connections with multiple Core Network Instances

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 77 of 501

1. When a UE first connects to the operator's network or registers to the PLMN for the first time and there is no sufficient information for the RAN to route this network connection request to an appropriate Common C-Plane Function, the UE sends a network connection request to the RAN, which is then further forwarded to the default Common C-Plane Function. The flow continues in step 2.

If the UE provides the DCN-ID along with this network connection request, but does not provide a Temporary UE identity, the RAN uses this DCN-ID to determine an appropriate Common CP that supports this DCN-ID, and the flow continues in step 4. In addition, the UE may provide other information, e.g., Service Type and/or DNN along with this network connection request.

If the UE provides the Temporary UE identity, the RAN uses the Temporary UE identity to determine a Common CP function specific for CNI-1 and CNI-2 and, the flow continues in step 4. In addition, the UE may provide other information, e.g., DCN-ID, Service Type and/or DNN along with this network connection request.

NOTE 1: When the UE sends a request to connect to an operator's network, a UE may request to establish a session for a particular service by sending the DNN along with this network connection request. If this is the case, after the authentication and authorization in step 6 has been performed, the C-CPF specific for CNI-1 and CNI-2 will establish the session for the request service like similar to step 9, 10 and 11.

2. The CCPSF located in the default C-CPF determines which Common C-Plane function to be connected to by taking into account information in the network connection request from a UE in step#1. In addition, other information from the subscription database may be also considered. For example, the UE's subscription may indicate that for this UE, the operator should set up a session with the particular CNI. In this signalling flow example depicted in Figure 6.1.3-2, this is the Core Network Instance#1.

In case the default C-CPF determines that it will serve this UE's network connection request, it either continues with the authentication and admitting the UE to attach/connect to operator's network or reject this UE's network connection request and hence this procedure ends in this step. It is to note that this specific case is not depicted in Figure 6.1.3-2 for simplicity of the signalling flow.

Editor's note: It is FFS, if authentication of UE to access operator's network should occur before the NSSF/CPSF selects Core Network Instance.

3. The default C-CPF sends a response to the RAN node with the Common C-Plane function specific for CNI-1 and CNI-2, for which the UE to attach. Same content of UE's network connection request in step#1 and may also include e.g. DCN-ID from step#2 is also sent back to the RAN.

Editor's note: whether a default CCPF will communicate directly with the C-CPF specific for CNI-1 and CNI-2 is FFS, i.e. without redirecting the "network connection request" to the C-CPF specific for CNI-1 and CNI-2.

4. If the UE provides a Temporary UE identity, this means that the UE has been once registered at the PLMN, and the CN has provided the UE the DCN-ID, which the UE should be connected. Hence, the RAN uses only the Temporary UE identity to route the NAS message to the appropriate Common CP function.

In case there is a pool of Common C-Plane Functions that are dedicated for this UE Usage Type and/or for this DCN-ID provided by the UE or by the default Common C-Plane Function in step#3, the RAN node performs NAS Node Selection Function (NNSF) similar to what we have for the NNSF in eNB .

5. The RAN node routes the UE's network connection request to the Common C-Plane Function specific for CNI-1 and CNI-2 . Along with this request, it may contain other information like the DNN to enable the C-CPF specific for CNI-1 and CNI-2 to select a CNI that is specific for a certain Service Type. If the C-CPF specific for CNI-1 and CNI-2 rejects the UE's network connection request, the C-CPF specific for CNI-1 and CNI-2 sends a NAS reject message to the UE.

6. Authentication and admitting the UE to attach/connect to operator's network is performed.

NOTE 2: In this step, the key for decrypting NAS message between the UE and the Common CP function specific for CNI-1 and CNI-2 is also provided.Exact details of UE authentication and UE's subscription verification for step 7 are out of scope of this solution.

7. The Common CP function specific for CNI-1 and CNI-2 sends a network connection accept response to the UE. In this response, it contains the Temporary UE identity and the information, for which the UE is to be configured, e.g., which DCN-ID, its corresponding Service Type and/or corresponding DNN that the UE is

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 78 of 501

allowed to connect. In case, the DCN-ID newly provided does not match to the ones that the UE already has, the DCN-ID(s) will be configured at the UE.

8. UE requests for establishment of a session for a communication service (e.g. service#1 that is provided by the Core Network Instance#1) by sending an SM request for a new PDU session. In this PDU session request, the UE provides the DCN-ID and DNN.

9. The RAN forwards the PDU session request to an appropriate Common C-Plane function specific for CNI-1 and CNI-2by using the DCN-ID information sent by the UE.

10. The NSSF in the C-CPF specific for CNI-1 and CNI-2selects C-Plane Function of the Core Network Instance#1 by using the DNN information that can be mapped to represent the Service Type that the CNI supports in the PDU session request, and forwards the UE's PDU session request for the service#1 to the CPF-1 in Core Network Instance#1 (CNI-1 CPF-1), which is responsible for session management in CNI#1. Note that this forwarded PDU session request still contains the information that has been sent by the UE such as the UE Usage Type, DCN-ID and DNN.

11. The CPF-1 in Core Network Instance #1 sends the session setup message to the UPF-1 in Core Network Instance #1 for session establishment. After a successful session establishment, the CPF-1 in Core Network Instance#1 sends the session response back to the C-CPF specific for CNI-1 and CNI-2.

12. The C-CPF specific for CNI-1 and CNI-2sends a new service response back to the UE via the RAN. After this step, the UE is successfully connected to Core Network Instance #1 with an active PDU session.

13. UE requests for the establishment of another session for a new communication service that is of a different service type than the previous service. In this PDU session request, the UE provides the Temporary UE identity, UE Usage Type, DCN-ID, and Service Type and/or DNN.

14. The RAN determines the Common C-Plane Function specific for CNI-1 and CNI-2 by using the Temporary UE identity sent by the UE and forwards the PDU session request to the Common C-Plane Function specific for CNI-1 and CNI-2.

15. The C-CPF specific for CNI-1 and CNI-2 selects C-Plane Function of the Core Network Instance#2 by using the DNN information in the PDU session request, and forwards the UE's service request for the new service to the CPF-1 in Core Network Instance#2 (i.e. CNI-2 CPF-1), which is responsible for session management in CNI#2. Note that this forwarded PDU session request still contains the information that has been sent by the UE such as the UE Usage Type, DCN-ID, and Service Type and/or DNN.

16. The CPF-1 in Core Network Instance #2 sends the session setup message to the UPF-1 in Core Network Instance #2 for session establishment. After a successful session establishment, the CPF-1 in Core Network Instance#2 sends the session response back to the C-CPF specific for CNI-1 and CNI-2.

17. The C-CPF specific for CNI-1 and CNI-2 sends a new service response back to the UE via the RAN. After this step, the UE is successfully connected to Core Network Instance #2 with an active PDU session.

6.1.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.4 Solution 1.4: Void

6.1.5 Solution 1.5: Selection of a network slice instance

This solution applies to Key Issue 1 -Support of network slicing.

Editor's note: Further details on how multiple network slices per UE is supported e.g. in RAN, and whether additional information is needed to select network slices is FFS.

6.1.5.1 Terminology and modelling

A network slice is always "complete" in terms of some business objective to be served. The term network slice should thus not refer to some smaller aggregate of functions. The term "sub-CN instance" can be used to refer to such smaller aggregates. Such sub-Core Network Instances may be dedicated or shared across network slices.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 79 of 501

Selection of a "network slice", i.e. how a UE (and its traffic) is associated and steered into the resources/functions associated with a network slice is not a monolithic entity/procedure. It is rather a set of one or more procedures/functions that jointly provide these capabilities and create the desired flexibility of how to compose network slices and support the overall business needs.

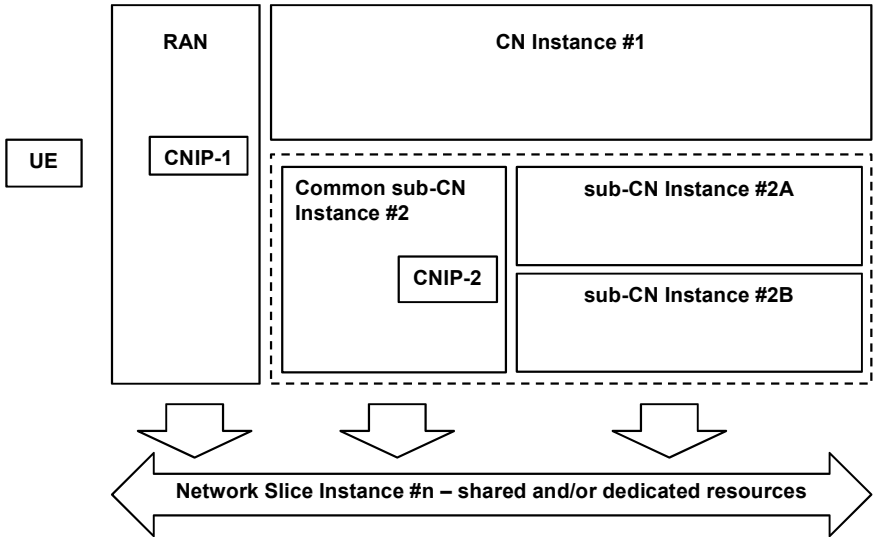


Figure 6.1.5.1-1 Network Slice modeling

Figure 6.1.5.1-1 models these capabilities. There may be "Core Network Instance Selection Procedures" in the RAN (referred to as CNIP-1) that allows steering of traffic into completely isolated core network instances (comprising CP as well as UP), shown as CN Instance #1 and CN Instance #2 in the figure. There may however also be a second layer of selection (CNIP-2) that for instance could allow different control and User Plane functions to be selected from, while sharing common set of Control plane functions (Common sub-CN instance).

Some network slices could potentially be "selected" in one step (e.g. CNIP-1), but it might also be so that the full selection is only possible through the combined procedures as indicated by the example above for CN Instance #2. In addition, the first selection procedure (CNIP-1) can also be used to apply relevant resource/function allocation in the RAN to support network slicing.

The following sections describe the first layer of selection (CNIP-1). It shall be noted that this does not exclude the use of the other layers as well, they can be combined and complement each other to serve the overall objectives of network slicing.

6.1.5.2 Architecture description

The solution provides the means to do a first level (not to exclude additional levels) of selection of Network Slice Instance by:

The UE provides:

If available, Network Slice Selection Assistance Information (NSSAI);

if available, NG Globally Unique Temporary Identity (NGUTI), which points to the NG CN NF in use, which is common for all CNIs the UE is allowed to use;

Selected PLMN;

UE identity (when NGUTI is not available); and

UE capabilities.

The RAN:

Selects an CNI based on the information from the UE and the configured information. RAN may take additional decisions related to RAN resources to support network slicing based on the information provided by the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 80 of 501

The Subscription:

The subscription may contain the subscribed Network Slice Type.

The NG CN:

The NG CN verifies and authorizes the UE access to Core Network Instance (CNI) or redirects the UE to a different CNI.

At attach (and subsequent mobility updates) the NG CN may provide the UE with (new) NSSAI .

Editor's note: Description of Network Slice selection at roaming and detailed CP and UP selection is FFS.

Editor's note: How an CNI is selected over non-3GPP access is FFS.

6.1.5.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

The following figure 6.1.5.2-1 depicts the signalling flow for Core Network Instance selection. The signalling may be combined with signalling related to other signalling procedures (e.g. initial attach).

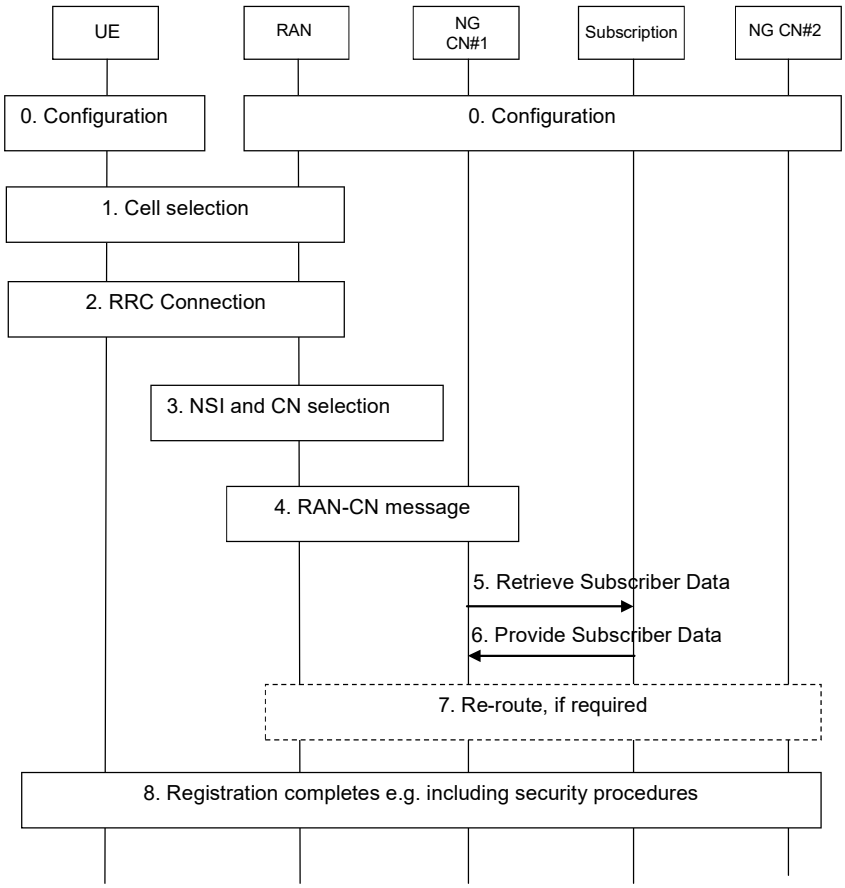


Figure 6.1.5.2-1 Core Network Instance selection

0. The NG system is configured:

UE: The UE may be pre-configured with Network Slice Selection Assistance Information (NSSAI). The NSSAI can be standardized and shared across PLMNs, or it can be specific per PLMN. The NSSAI is used as input to select an NG CN instance to serve the UE, which is a CN_CP function common for all CNIs the UE is enabled to access.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 81 of 501

RAN: The RAN is configured with the corresponding NSSAI of the connected NG CN Instances.

CN#x: Each CN#x is configured with the corresponding policies that enables the CN to verify a UE access to the /CNI.

Subscription: The Subscription may be configured with the subscribed Network Slice Type

1. The UE selects a RAN.
2. The UE initiates RRC connection providing PLMN information, UE identity (if NGUTI is not available), UE capabilities, NSSAI (if available), NGUTI (if available). The UE also initiates an NG Attach procedure (or equivalent mobility procedure).
3. The RAN may take decisions related to RAN resources by using the NSSAI (if provided by the UE) and the selected PLMN. The RAN then selects aCNI corresponding to the NSSAI (if provided by the UE) and the selected PLMN. If the UE did not provide any NSSAI, then RAN selects a default CNI for the selected PLMN.

NOTE: The default CNI can e.g. be a general purpose eMBB CNI.

If the UE provides an NGUTI, the CNI selection has already been made and the RAN uses only the NGUTI to route the NAS message.

4. The RAN forwards the NAS message to the selected NG CN Instance.
5. The NG CN Instance may interact with the Subscription to retrieve the e.g. subscribed Network Slice Type.
6. The Subscription provides the subscribed Network Slice Type along with other subscription information. The NG CN#1 Instance examines the NSSAI received from RAN, the Network Slice Type provided by the Subscription, other information available (e.g. UE capabilities, other subscription information, SLA information, local configuration), and verifies that the selected NG CN#1 Instance and Network Slice Instance is suitable to serve the UE. If the UE is authorized to access the Network Slice and the NG CN#1 Instance is suitable to serve the UE the flow continues at step 8.
7. If the Network Slice Instance is not suitable to serve the UE the NG CN#1 Instance initiates a re-route to an appropriate Network Slice /Core Network Instance by providing the target CNI to the RAN (and e.g. original RAN message) which invokes the appropriate NG CN instance (NG CN#2). The NG CN#2 verifies that the NG CN#2 is suitable to serve the UE based on received information during re-route procedure and information fetched from the Subscription.
8. The Attach procedure completes (including e.g. security procedures towards the UE). The selected NG CN Instance assigns an NSSAI and provides the NSSAI to the UE together with an NGUTI. If provided to the UE, the UE shall indicate the NSSAI and (when valid) the NGUTI always when connecting to the network in that PLMN.

When establishing a PDU session an APN (or equivalent) is used as input to select the appropriate CN_SM and CN_UP functions. The UE stores which APNs to use for each application.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 82 of 501

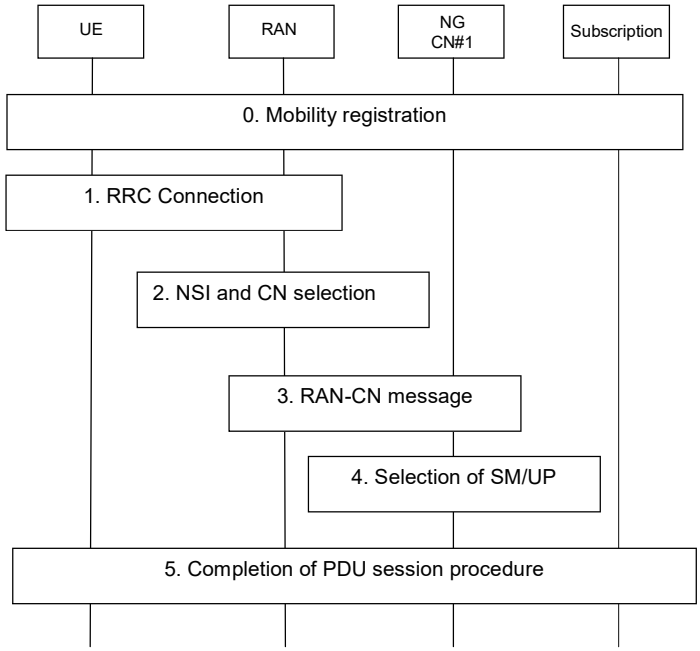


Figure 6.1.5.2-2 Network Slice Instance selection. PDU session

0. The UE has been mobility registered (attached) to the NG network (according to figure 6.1.5.2-1)
1. The UE initiates RRC connection providing NSSAI, NGUTI. The UE also initiates a PDU session related procedure and optionally provides APN.
2. The RAN routes the message to the NG CN NF corresponding to the NGUTI.
3. The RAN forwards the NAS message to the selected NG CN Instance. Along with the NAS message from the UE, the RAN includes the NSSAI from the UE, if provided by the UE.
4. The NG CN instance selects the appropriate NG_SM/NG UP functions using subscription information and UE provided information e.g. NGUTI, APN, if provided by the UE or default APN from the subscription in case the UE did not provide APN.
5. The PDU session related procedure is completed. The NG CN provides the APN in use for the PDU session to the UE. In subsequent PDU session messages related to the APN, the UE provides the received APN in use which points to the selected CN_SM/CN_UP function.

6.1.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.6 Solution 1.6: Slice Instance ID based Network Slice Selection

This solution is for key issue 1 WT#1 and mainly describes the mechanism for network slice selection by using Slice Instance ID. This solution supports the group A and group B in Annex D.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 83 of 501

6.1.6.1 Architecture description

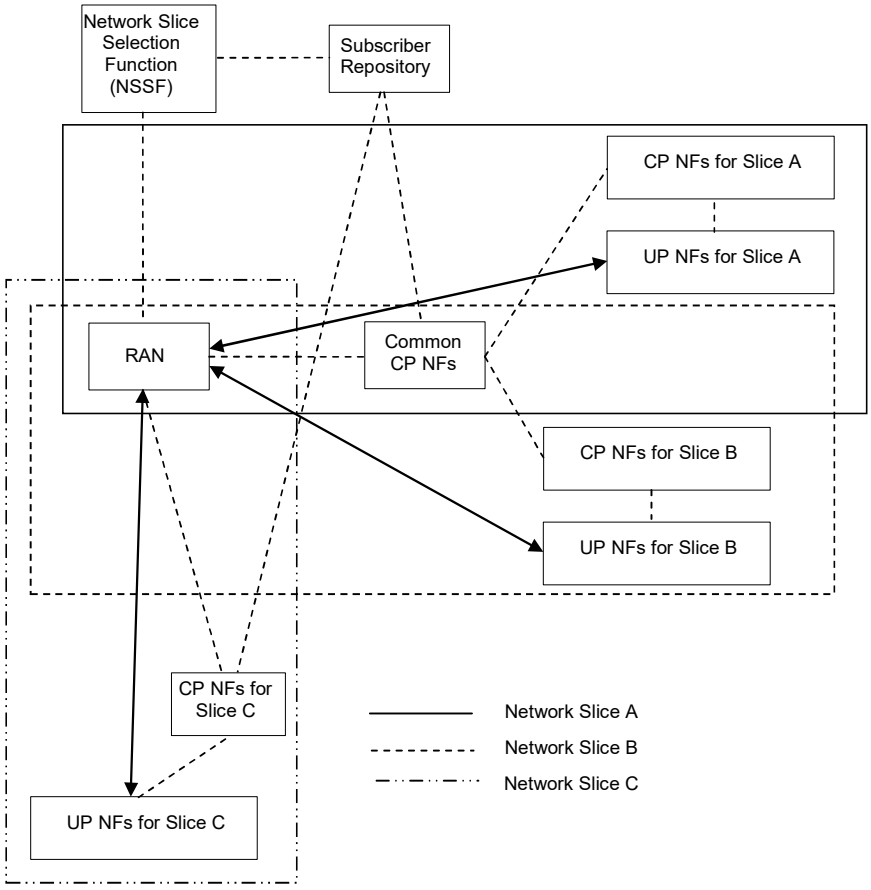


Figure 6.1.6.1-1: Network Slice architecture with two groups-common CP NFs and dedicated CP NFs

As the figure shown, the architecture includes two groups. One is the dedicated network slice (Group A in Annex D) and the other is the network slices have shared common CP NFs (Group B in Annex D).

Editor's note: The Non-3GPP access aspects of this solution is FFS.

Definitions in this solution:

- **Slice Instance ID:** identifier of a network slice instance. It is used as an indicator by the network to select the corresponding slice for a UE.
- CP-**NF ID:** identifier of a control plane network function instance.

For this solution, the NSSF (Network Slice Selection Function) is common to all network slices in the PLMN and can realize the slice selection function for both groups. The NSSF is located in the NextGen CN and has interconnection with subscriber repository.

The AN acts as a routing function to link the UE with the appropriate CN part of network slice .The AN stores the mapping between the Slice Instance ID and NF ID. CP-NF ID can be resolved to CP-NF address by DNS and the AN can transfer the data to specific CP-NF.

6.1.6.2 Function description

6.1.6.2.1 Definitions and functions

Slice Instance ID: identifier of a network slice instance. It is used as an indicator by the network to select the corresponding slice for a UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 84 of 501

Slice Instance ID is configured in UE by the operator or the user. As an identifier, it refers to the network slice instance provided by the operator. Therefore, similar as APN, the Slice Instance ID could be operator dependent. The value should be defined by Stage 3 but the content is operator specific.

Editor's note: The duration of validity of the Slice Instance ID within a UE, and any subsequent impacts due to it is FFS.

NSSF: Network Slice Selection Function. The NSSF stores the mapping information between Slice Instance ID and NF ID (or NF address). The NSSF has connection with the subscriber repository to get the UE's subscribed Slice Instance IDs corresponding to current PLMN. NSSF can also obtain network slice selection policy from policy function. CP-NF ID or address is determined by the NSSF based on Slice Instance ID, UE's subscribed information, and/ or network slice selection policy. NSSF can respond the specific CP-NF ID/address corresponding to the Slice Instance ID to the AN. The NSSF is located in the core network, which is benefit for the interaction and mapping update between the NSSF and subscriber repository, and this makes the management of the mapping between Slice Instance ID and NF ID/address in an efficient centralized way.

6.1.6.2.2 Common Network Functions

Common network functions across multiple slices. Such functions are those related with multiple slices in the network, e.g., UE subscription repository function. The NSSF is such a common function provide to all network slices in a PLMN.

Common CP network functions for multiple slices with UE simultaneously connected. A UE can access multiple network slices at the same time. In this case, there should have a minimum set of NFs which can be flexibly expanded with additional NFs per slice requirement. The minimum set of common CP NFs should include:

- Mobility Management: the signalling (e.g., between UE and MM function, and between new/target MM function and old MM function) can be reduced if mobility management (e.g. UE location update related management) is shared among different network slices when a UE simultaneously obtains services from different slices.

Editor's note: the connection mechanism between the common CP NFs and the dedicated NFs in specific core network slices is FFS.

6.1.6.2.3 The Attach procedure

Suppose a UE is slice-enabled, there are three cases for the attach procedure:

1) UE attaches without Slice Instance ID but may take some assistant parameters (e.g. service type) , or not. The AN forwards the attach request to NSSF. Then NSSF, may check with subscription data and network slice selection policy, response with a predefined/default Slice Instance ID to the UE. Then UE will update/store the selected Slice Instance ID and then re-attach the network with the assigned Slice Instance ID. The authentication for the UE is done by the NSSF which fetch the UE subscriber information from subscriber repository and check whether the UE can connect to the network.

2) UE attach es with a Slice Instance ID, but the AN does not know the corresponding slice. The AN forwards the UE request signalling to NSSF and NSSF would respond with specific CP-NF ID/address corresponding to the Slice Instance ID.Then the AN will route the attach request to the specific CP-NF. The authentication and authorization for UE is done in step 5 as the figure 6.1.6.2.3-1 shown.

3) UE attaches with Slice Instance ID, and the AN has the related mapping between the Slice Instance ID carried by UE and CP-NF ID. The attach request will be routed to the specific CP-NF in the core network. The authentication and authorization for UE is done in step 5 as the figure 6.1.6.2.3-1 shown.

Editor's note: how to handle the Slice Instance ID is FFS in the roaming scenario.

Editor's note: for group B, how to select the dedicated CP-NFs after common CP NFs have been selected is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 85 of 501

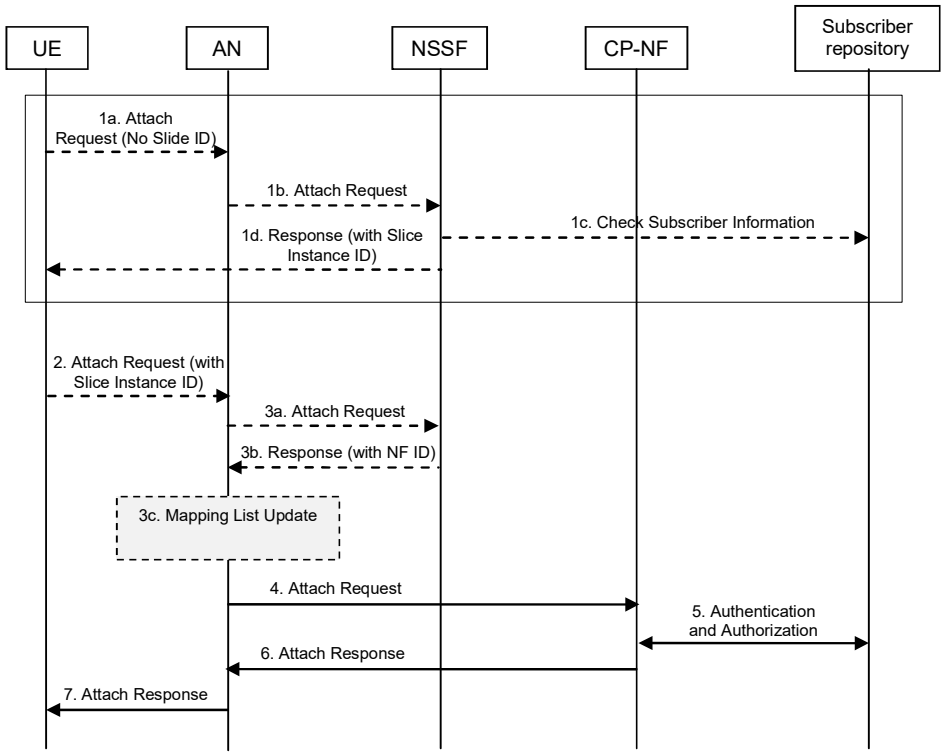


Figure 6.1.6.2.3-1: Attach procedure

1. A UE attach without Slice Instance ID will get Slice Instance ID configured.

   1a. A UE sends an Attach Request without Slice Instance ID to AN.

   1b. The AN find no Slice Instance ID in the attach message, then the AN forwards the attach request to NSSF.

   1c. The NSSF check with Subscriber Repository to get UE's subscription information. The authentication for the UE is done by the NSSF to check whether the UE can connect to the network.

   1d. The NSSF responds with a specific Slice Instance ID or a default Slice Instance ID to UE.

2. The UE sends an Attach Request with Slice Instance ID.

3. If the AN does not have the mapping between the Slice Instance ID UE carried and the corresponding CP-NF ID,

   3a. AN forwards the Attach Request to the NSSF

   3b. The NSSF finds the corresponding CP-NF ID/address for the Slice Instance ID, and responds to the AN. Some other information such as UE's subscription information, network slice selection policy may be needed for the NSSF to determine the network slice selection.

   3c. The AN get the mapping between Slice Instance ID and CP-NF ID/address from NSSF and update the mapping list. If CP-NF ID is returned, the AN could use CP-NF ID to resolve the CP-NF address by e.g., DNS.

4. The AN forwards the Attach Request to the CP-NF. The CP-NF could be a common CP NF or a dedicated CP-NF.

5. The CP-NF interacts with the Subscriber Repository to fetch the UE subscriber information and conduct the authentication and authorization per slice. The CP-NF determines whether the UE could access to the slice.

6. The CP-NF sends the Attach Response to AN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 86 of 501

7. The AN sends the Attach Response to UE.

Suppose a UE is not slice-enabled, the AN should recognize such case and a predefined/default slice will serve the UE. The corresponding procedures could be:1a→1b→1c→3b→4→5→6→7 .

Editor's note: how to support UE access another network slice instance when the UE has already accessed one network slice is FFS.

6.1.6.2.4 Slice Instance ID update due to subscription change

When the UE's subscribed slice instance ID in the Subscriber Repository is modified, the UE's slice instance ID configuration should be updated correspondingly.

The method is that the network trigger the UE to delete the its previous slice instance ID and attach the network without slice instance ID.

The procedure for UE's slice instance ID modification is shown as follows:

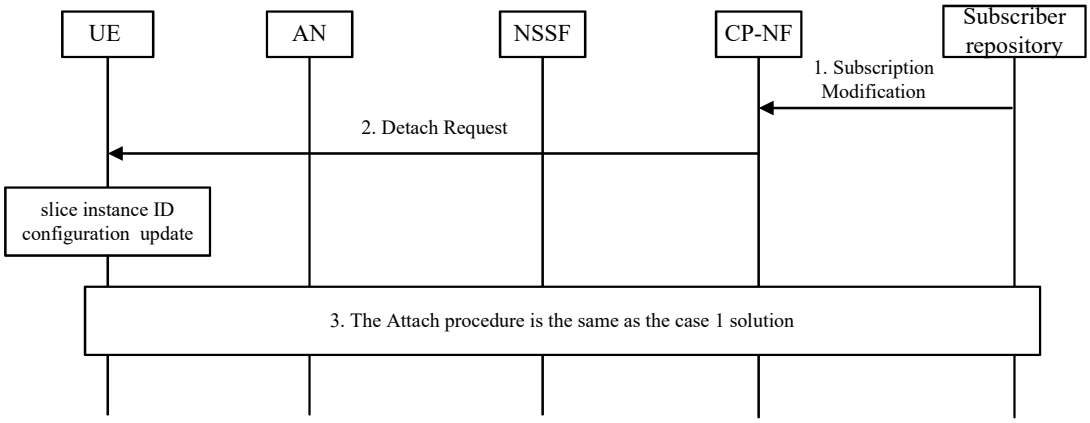


Figure 6.1.6.2.4-1: The procedure for UE's slice instance ID modification

1. When the UE's subscriber information is modified, the Subscriber Repository would send Subscriber Modification message to the CP-NF (e.g., MM) to trigger the UE's slice instance ID configuration update
2. The CP-NF sends Attach Reject to UE, with a reason cause showing the rejection is caused by the slice instance ID subscription modification. The UE would delete the previous slice instance ID.
3. The UE would send the Attach Request to the AN without slice instance ID. And the following procedures are the same as the case 1 in 6.1.6.2.3.

6.1.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.7 Solution 1.7: Network Slice Selection based on Usage Class

This solution addresses Key Issue 1 (Support of Network Slicing) and specifically it considers (a) how the UE derives network slice selection information and (b) how the UE can have multiple simultaneous PDU sessions each one associated with a different network slice.

6.1.7.1 Architecture description

The key aspects of the solution are illustrated in Fig. 6.1.7.1-1 and are further described below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 87 of 501

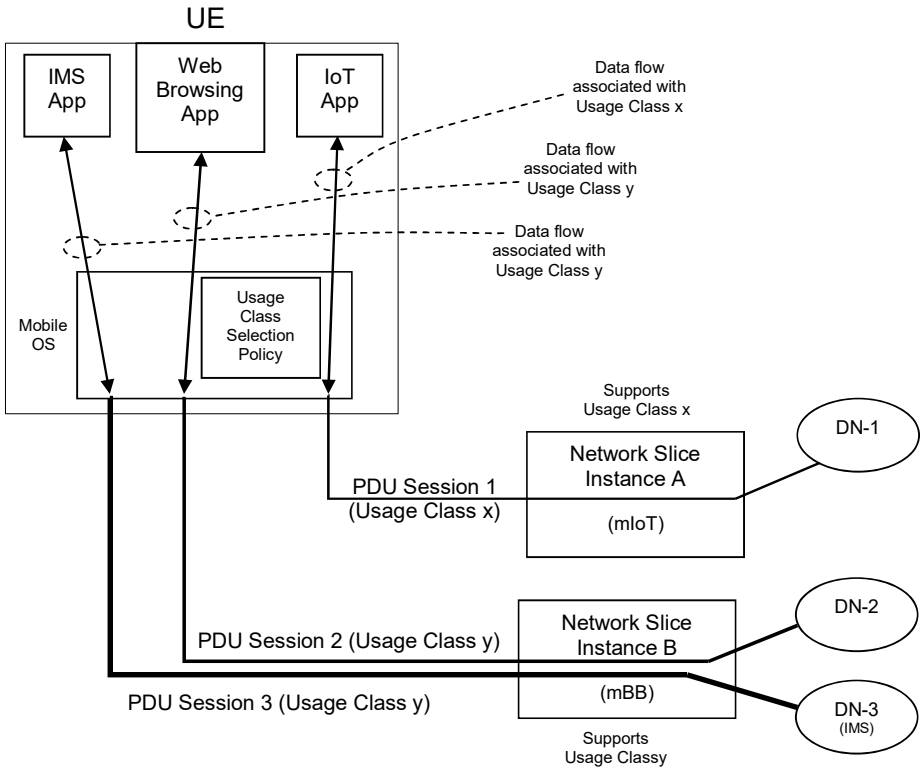


Figure 6.1.7.1-1

1. Every network slice instance supports one or more *Usage Classes*. For example, as shown in Fig. 6.1.7.1-1, a network slice instance optimized for massive IoT (mIoT) supports Usage Class x, while a network slice instance optimized for enhanced mobile broadband (MBB) supports Usage Class y. The Usage Class of a network slice indicates the use case that the network slice instance is configured to support, i.e. the type of the network slice instance.

2. The UE associates every data flow with a Usage Class (and thus with a type of network slice). This association is accomplished by using a Usage Class Selection Policy which is provisioned in the UE and contains a list of prioritized rules matching different data flows with different Usage Classes. For example, the Usage Class Selection Policy may contain the following rules:

   a. Rule 1, priority 1: App-id=com.example.app1, Usage Class=x

   b. Rule 2, priority 2: App-id=com.example.app2, Usage Class=y

   c. Default rule: Usage Class=z

The Usage Class Selection Policy may contain only the default rule in which case all UE data traffic is associated with the same Usage Class.

The Usage Class Selection Policy can be provided to UE by the HPLMN and by a VPLMN. In roaming scenarios, the UE applies the policy of the registered PLMN (RPLMN), if it exists.

NOTE 2: Since any PLMN can provide policy to UE that includes its own Usage Classes it might not be necessary to standardize Usage Class values that are common to all PLMNs. Each PLMN may use its own proprietary values.

In the example scenario shown in Fig. 6.1.7.1-1 the UE associates the data flow of the IoT app with Usage Class x and the data flows of the web browsing and IMS apps with Usage Class y.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 88 of 501

The Usage Class Selection Policy is provided to UE by the appropriate policy functionality that is defined as part of the NextGen policy framework (see clause 6.10). Details on how this policy is provided to UE are outside the scope of the present solution.

3. When the UE initiates a new data flow and this data flow is associated with Usage Class x, the UE routes the data flow via a suitable PDU session that matches this usage class (if it exists). In the example shown in Fig. 6.1.7.1-1 the data flow from the IoT app is associated with Usage Class x and it is therefore routed via the PDU session 1 that supports the Usage Class x.

   - If the UE has no suitable PDU session matching the Usage Class associated with a new data flow, then the UE requests the establishment of a new PDU session with the Usage Class associated with the data flow.

4. The UE provides the Usage Class as "assistance information" for network slice selection. It is used by the network to select a network slice that supports the requested Usage Class. The UE may provide multiple Usage Classes as "assistance information" in order to be connected to different network slices.

5. The UE may be simultaneously using multiple Usage Classes and it may have multiple PDU sessions, each one associated with a Usage Class. In the example scenario shown in Fig. 6.1.7.1-1 the UE is simultaneously using Usage Class x and Usage Class y and has established three different PDU sessions: one with Usage Class x which is routed via the network slice instance A and two with Usage Class y which are both routed via the network slice instance B.

6. When an app in the UE wants to establish a new PDU session, the app itself may indicate a Usage Class for the PDU session. If the app does not provide the Usage Class the UE uses the default Usage Class. The default Usage Class may be determined from the default rule of the Usage Class Selection Policy, as shown in bullet 2 above.

An example of UE procedures is provided below to better clarify the solution.

1. The UE powers up and provides the default Usage Class (determined from the default rule of the Usage Class Selection Policy) as "assistance information". The default Usage Class may depend on the type of UE (e.g. IoT device, smart phone, etc.) and is used by the network for selecting a network slice instance for the UE. The UE is informed that is it connected to a network slice instance that supports e.g. Usage Class x and Usage Class y.

2. A web browser is launched in the UE and initiates a new data flow. By using the Usage Class Selection Policy, the UE associates this data flow with Usage Class y. The UE requests the establishment of a PDU Session for Usage Class y (the PDU session request message includes the Usage Class y). After establishing the PDU Session the UE routes all data flows of the applications associated with Usage Class y (e.g. Internet traffic) within this PDU Session.

3. Later an IoT app is launched in the UE and initiates a new data flow that is associated with Usage Class z. Since the UE is not connected to a network slice that supports Usage Class z, the UE provides to the network the Usage Class z as "assistance information" to be connected to another network slice. The network connects the UE to another network slice instance that supports the Usage Class z (e.g. a network slice optimized for IoT). After that, the UE establishes a PDU Session for Usage Class z and routes all data flows of the applications associated with this Usage Class (e.g. all IoT traffic) within the PDU session.

6.1.7.2 Solution evaluation

Editor's note: The solution evaluation is FFS.

6.1.8 Solution 1.8: Network slice instance reselection

This is a solution for key issue 1 on support for network slicing. The NW slice architecture considered in this solution is based on solution 1.3. This solution identifies the scenarios and principles for network slice instance reselection.

Editor's note: Whether to capture this solution as part of solution 1.3 is FFS.

Editor's note: This solution can be applied on the top of existing solutions based on the group B architecture in Annex D.

6.1.8.1 Definition and categorization of slice reselection

Network Slice reselection: Once the UE is connected to a network slice, there may be some scenario for the UE or the network to change the network slice providing service to the UE. In this case, the network slice needs to be reselected

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 89 of 501

for receiving services from the network. Network slice reselection is categorized into Inter-C-CPF reselection and Intra-C-CPF reselection based on whether the serving C-CPF changes or not.

Intra C-CPF slice reselection: If the UE needs to change the network slice which the UE is connected within the serving C-CPF, only CNI is changed for the UE while the C-CPF remains the same. In this case, MM contexts may not change but SM contexts changes to different non-common CNI.

Inter C-CPF slice reselection: If the UE needs to change the network slice which the UE is connected with change of the serving C-CPF, the UE needs to change both C-CPF and CNI and reselect the network slice for receiving services. SSC may not be guaranteed with the inter-C-CPF reselection.

6.1.8.2 Scenarios for slice reselection

The network slice reselection/change scenarios can be grouped, but not limited to, as follow:

1. Slice reselection due to the mobility (UE location change)

This scenario can happen when the UE moves into different service area which has connections with different network slice set. This means that the serving AN is changed and the target AN doesn't support all deployed slices of the network. Mobility to different PLMN (e.g. roaming scenario) also causes slice reselection due to the mobility.

Editor's note: Whether an AN cannot support all deployed slices is FFS.

2. Slice reselection due to the network maintenance issue

A node consisting a network slice fails for some reason (e.g. node failure, network congestion) and the network needs to change the serving node for the UE. For example, if a serving C-CPF has network congestion, the network may trigger the network slice reselection for guaranteeing certain level of QoS.

Editor's note: Whether this scenario is relevant is FFS.

3. UE requested service change

The UE may request to change service that the UE is receiving, which may lead to the network slice reselection. This scenario can happen when the UE supports multiple services and the services cannot be served without change of network slice. For example, the UE using V2X services may need to receive CriC service which is provided in an isolated slice instance, which trigger an inter C-CPF reselection.

4. Network requested subscription/policy change

The network may request to change service that the UE is receiving, which may lead to the network slice reselection. The network initiated service change may be triggered by the change of UE subscription information or policy.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 90 of 501

6.1.8.3 Function description

6.1.8.3.1 Intra C-CPF Network Slice Change

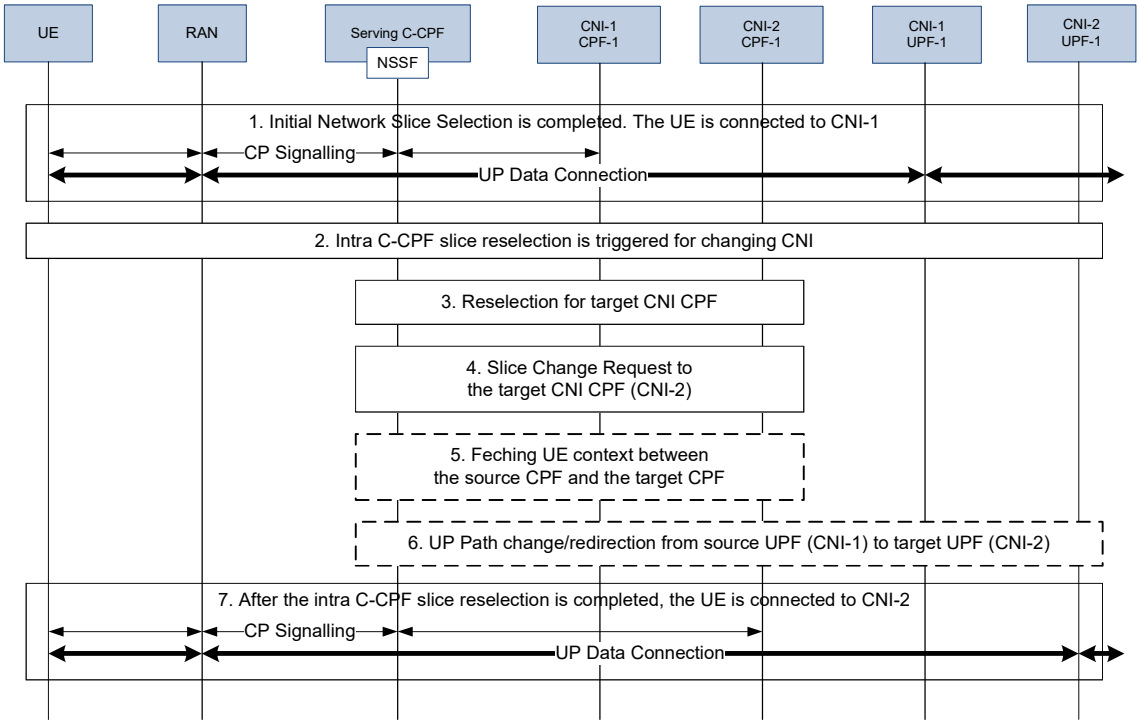


Figure 6.1.8.3.1-1: Intra C-CPF Network Slice reselection procedure

1. After the initial selection for network slice (e.g. initial attach, new service request), the UE is connected to CNI-1.

2. Due to some reason specified in 6.1.8.2, the UE or the network needs to change the network slice which the UE is connected, with only changing CNI, without changing C-CPF.

3. NSSF in C-CPF performs CNI reselection based on similar criteria for initial selection, e.g. DNN, Service Type.

4~6. After the target CNI is selected, reselection/redirection is performed. These steps may be conducted similar to PDN connection disconnect/Bearer resource deactivation with re-activation procedure in EPC according to TS 23.401 [2]. Note that step 5 and step 6 is optional depending upon the network's deployment.

7. After the intra C-CPF slice reselection procedure is completed, the UE is connected to CNI-2 without changing C-CPF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 91 of 501

6.1.8.3.2 Inter C-CPF Network Slice Change

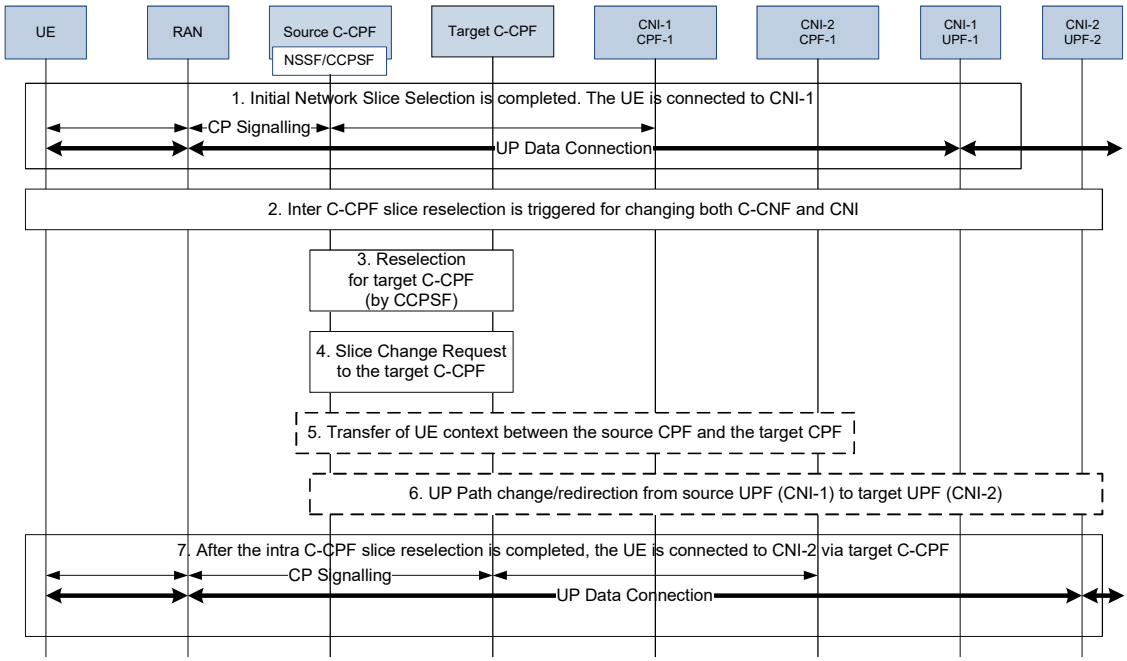


Figure 6.1.8.3.2-1: Intra C-CPF Network Slice reselection procedure

1. After the initial selection for network slice (e.g. initial attach, new service request), the UE is connected to CNI-1 via initially selected C-CPF.

2. Due to some reason specified in 6.1.8.2, the UE or the network needs to change the network slice which the UE is connected, with changing both C-CPF and/or CNI.

Editor's note: Whether a CNI can be shared between multiple C-CPF is FFS.

3. NSSF or CCPSF in the source C-CPF performs slice reselection based on similar criteria for initial selection, e.g. DCN ID, UE Usage Type, Service Type, DNN, etc..

4~6. After the target C-CPF is selected, reselection/redirection is performed. These steps may be conducted similar to the detach procedure with re-attach in EPC according to TS 23.401 [2]. Authentication and/or Authorization for the target C-CPF may be skipped upon the operator's policy and the slice change scenario. Note that step 5 and step 6 is optional depending upon the network's deployment.

7. After the inter C-CPF slice reselection procedure is completed, the UE is connected to new CNI via new C-CPF.

6.1.8.4 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.9 Solution 1.9: Multiple Independent Slices per UE

This solution addresses Key Issue 1 (Support of Network Slicing) and specifically considers (a) how a network slice instance is selected, (b) how the network slices can be independent (without sharing common network functions) and (c) how a UE can be simultaneously connected to multiple network slice instances.

6.1.9.1 Architecture description

The key aspects of the solution are illustrated in Fig. 6.1.9.1-1 and are further described below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 92 of 501

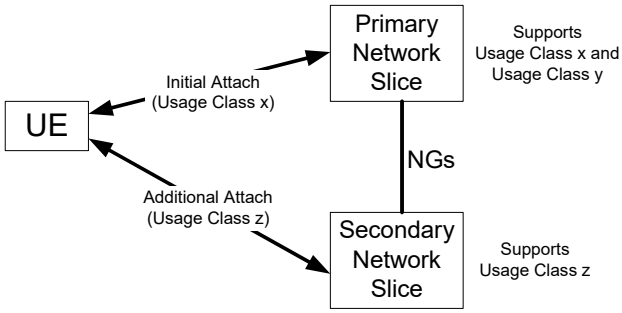


Figure 6.1.9.1-1

1. The network slice instances can be independent and they do not need to share any CP or UP functions. They may share however common databases such as the subscription database and/or policy databases.

2. Network slices instances can communicate via the NGs interface. Each network slice instance has a unique slice identity that can be resolved to an IP address for communication via NGs.

3. Each network slice instance supports one or more Usage Classes. For example, a network slice instance optimized for massive IoT can support Usage Class z, while a network slice optimized for enhanced mobile broadband can support Usage Class x. The Usage Class of a network slice indicates the use case that the network slice is configured/optimized to support and is discussed in more detail in clause 6.1.7.

4. A UE can be simultaneously attached to multiple network slice instances. One of these slices is the primary network slice for the UE and all the others are secondary network slices for the UE. The difference between primary and secondary network slices is further elaborated below.

5. The first attach performed by the UE is called Initial Attach and attaches the UE to the primary network slice.

6. A subsequent attach (i.e. after the initial attach) is called Additional Attach and attaches the UE to a secondary network slice. How the UE decides to initiate an additional attach is discussed in clause 6.1.9.2.1.

7. The UE sends all slice-independent signalling (i.e. signalling not associated with a specific network slice) only to the primary network slice. For instance, as shown in Fig. 6.1.9.1-2, all routing area update (RAU) requests are sent only to the primary network slice. The primary network slice forwards a RAU request to all secondary network slices via NGs and provides a consolidated RAU response back to the UE. Clause 6.1.9.2 below provides more details.

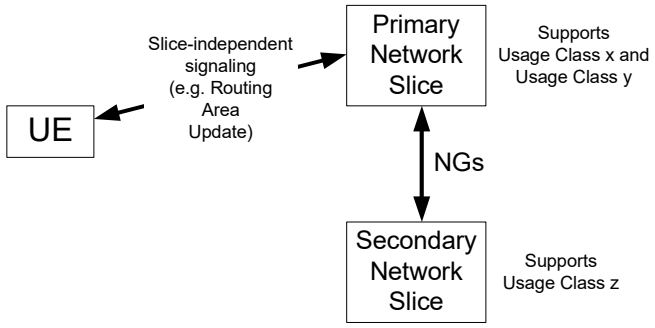


Figure 6.1.9.1-2

8. Every attach request (either initial attach or additional attach) includes a Usage Class, which is used as "assistance information" for network slice selection. For example, when the UE wants to attach for Usage Class x, the UE sends an Initial Attach request including the required Usage Class x. Later the UE may want to attach also for Usage Class z, in which case the UE sends an Additional Attach request including the Usage Class z as "assistance information".

NOTE 1: Although this solution is described by using the Usage Class as "assistance information", it can be applied with any other type of "assistance information" (e.g. with a DCN-id).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 93 of 501

9. Every time the UE attaches (e.g.) for Usage Class x, a PDU session for Usage Class x is also created. The PDU session is created either during the attach procedure or after the attach procedure.

10. The Usage Class associated with an attach procedure is provided to the RAN as "assistance information" and it is used for network slice selection.

As shown in the figure below, the UE maintains separate MM and SM context for each attached network slice and executes MM and SM procedures toward every attached network slice independently. The only exception is that the UE executes TAU/RAU procedures only towards the primary network slice. The UE maintains a separate NG1 signalling connection with the primary and the secondary network slices. However, TAU/RAU procedures are only executed via the NG1 connection towards the primary network slice.

Editor's note: If there is any RAN impact, it will be addressed by the RAN working groups.

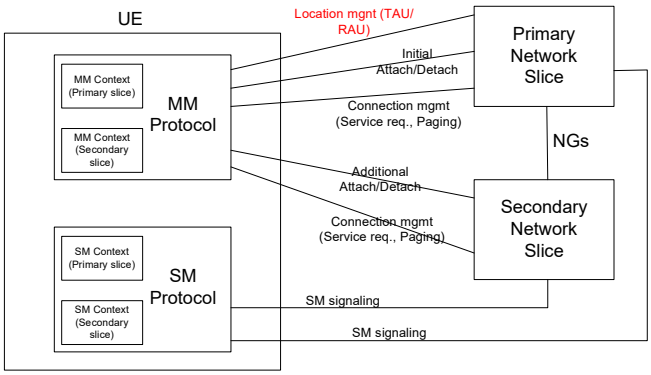


Figure 6.1.9.1-3

6.1.9.2 Signalling Procedures

6.1.9.2.1 Attach Procedures

This clause specifies the details of the initial attach and the additional attach procedures.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 94 of 501

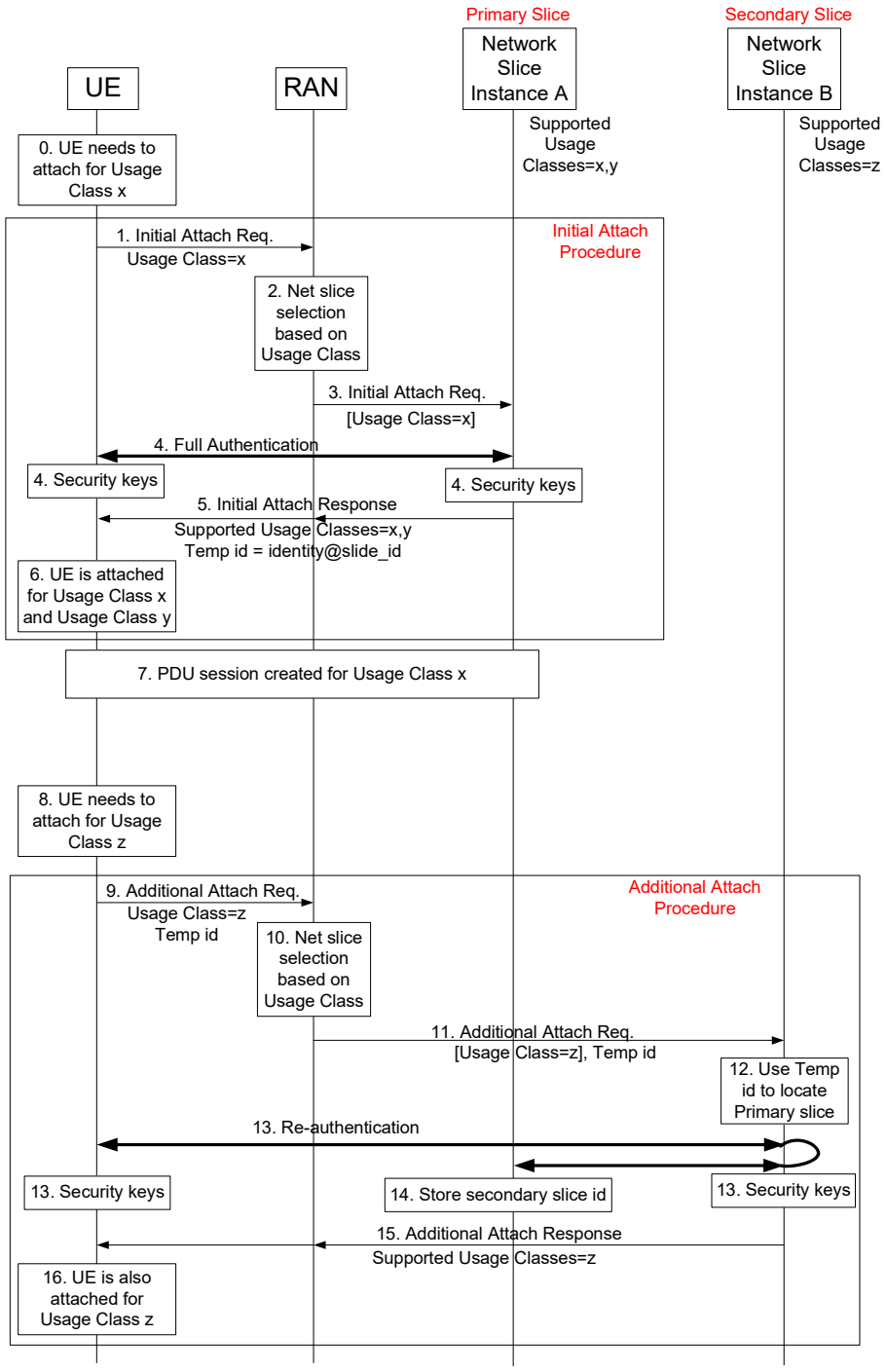


Figure 6.1.9.2.1-1

0. The UE determines it needs to attach (e.g.) for Usage Class x. For example, a web-browser application in the UE requests a new data session and the UE associates this data session with Usage Class x. How the UE associates an application (or data flow) with a Usage Class is specified in clause 6.1.7, "Solution 1.7: Network Slice Selection based on Usage Class".

1. Since the UE has not already performed an initial attach, the UE sends an Initial Attach request for Usage Class x. The Usage Class x is included as "assistance information".

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 95 of 501

2. The RAN uses Usage Class x as "assistance information" and selects a network slice instance that supports Usage Class x. This network slice instance becomes the primary network slice for the UE. The RAN is assumed to know the Usage Classes of all network slice instances.

3. The RAN forwards the Initial Attach request message to the selected network slice instance. The Usage Class x may also be included as part of the NAS message.

4. A mutual authentication takes place and security keys are generated in the UE and its primary network slice instance.

5. The primary network slice instance responds with an Initial Attach response message that includes the supported Usage Classes (x, y in this example) and the temporary identity assigned to UE. This temporary identity may be formatted as a NAI (e.g. temp_id@slice_id) and includes the slice identity of the primary network slice. The UE may also receive (not shown in the above figure) an identity for the Control Plane function in the primary network slice which was assigned to serve this UE.

6. The UE is now attached for Usage Class x and Usage Class y.

7. A PDU session for Usage Class x is also created with the primary network slice (either during or after the initial attach procedure). The UE forwards all user-plane traffic associated with Usage Class x within this PDU session.

8. The UE determines it needs to attach for Usage Class z. For example, an IoT application in the UE requests a new data session and the UE associates this data session with Usage Class z.

9. Since the UE has already performed the initial attach procedure, it sends an Additional Attach request that includes the Usage Class z and the temporary identity assigned to UE during the initial attach (in step 5). If the Additional Attach request is sent when the UE is in RRC Connected mode, then the "assistance information" is still included in the RRC message that carries the Additional Attach request.

10. The RAN uses Usage Class z as "assistance information" and selects a network slice instance that supports Usage Class z. This network slice instance becomes a secondary network slice for the UE.

11. The RAN forwards the Additional Attach request message to the selected network slice instance.

12. The secondary network slice uses the temporary identity of the UE to determine the primary network slice of the UE.

13. A mutual re-authentication takes place between the UE and the primary network slice instance via the secondary network slice instance. Security keys are created in the UE and the primary network slice instance. The primary network slice instance forwards these keys to the secondary network slice instance. Note that the secondary network slice instance behaves as a kind of AAA proxy in this case.

NOTE 1: The UE may provide its temporary identity to the secondary network slice instance during the re-authentication procedure (instead of providing this identity in message 9).

14. During the re-authentication the primary network slice instance is informed that the UE has attached to a secondary network slice instance and stores the slice identity of this secondary network slice instance. This identity can be passed from the secondary network slice instance to the primary network slice instance within the re-authentication signaling.

15. The secondary network slice instance responds with an Additional Attach response message that includes its supported Usage Classes and may also include a temporary identity assigned to UE by the secondary network slice instance. This message may also include an identity for a serving Control Plane function in the secondary network slice instance.

16. The UE is now attached also for Usage Class z. A PDU session for Usage Class z is created between the UE and its secondary network slice instance and all UE traffic associated with Usage Class z is transferred via this PDU session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 96 of 501

6.1.9.2.2 Routing Area Update Procedure

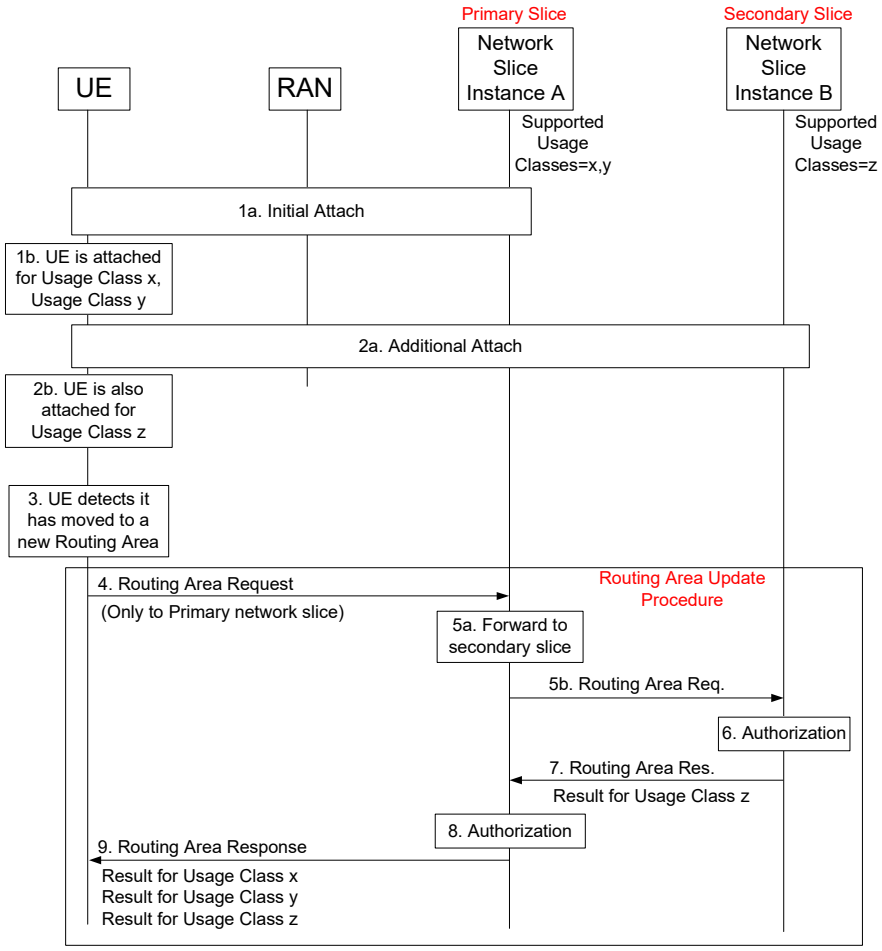


Figure 6.1.9.2.2-1

1-2. See clause 6.1.9.2.1.

3. The UE detects it has moved to a new routing area, or the UE needs to initiate a periodic routing area update.

4. The UE sends a Routing Area Update request message only to its primary network slice.

5. The primary network slice forwards the Routing Area Update request message to all secondary network slices of this UE. Note that the primary network slice is notified when the UE attaches to a secondary network slice (as specified in the previous clause) and stores the slice identities of all secondary network slices of the UE.

6. The secondary network slice determines if the UE is allowed to receive services from the secondary network slice in the new routing area.

7. The secondary network slice sends a Routing Area Update response which indicates if the routing area update is accepted or rejected for Usage Class z.

8. The primary network slice determines if the UE is allowed to receive services from the primary network slice in the new routing area.

9. The primary network slice sends a Routing Area Update response which indicates if the routing area update is accepted or rejected for each one of the Usage Classes supported by the primary and secondary network slices. After the step, the UE knows which Usage Classes are accepted in the new routing area.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 97 of 501

The above procedure can be applied for all slice-independent signaling, not only for routing area updates. So, all signaling messages not related to a specific Usage Class are sent by the UE only to its primary network slice.

6.1.9.2.3 Detach Procedure

When the UE wants to detach from (e.g.) Usage Class x, the UE sends a Detach Request message including the Usage Class x. This message is transferred to the network slice instance that the UE is attached to and supports Usage Class x. This may be either a secondary network slice or the primary network slice of the UE.

- When the UE detaches from a secondary network slice:
  - The secondary network slice notifies the primary network slice about the Detach and the primary network slice removes the slice identity of the secondary network slice from its list of secondary network slices.
- When the UE detaches from the primary network slice:
  - The primary network slice selects one of the secondary network slices (if any) to become the new primary network slice for the UE. The primary network slice transfers the stored slice context for this UE (including the list of secondary network slices) to the new primary network slice. The new primary network slice assigns a new temporary identity to UE which is included in the Detach response message.

    The Detach from primary network slice is schematically shown in the figure below. After receiving the Detach response (step 7), the UE knows that Usage Class z has become its new primary Usage Class and all slice-independent signalling should be sent to the new primary network slice (i.e. to the network slice associated with Usage Class z).

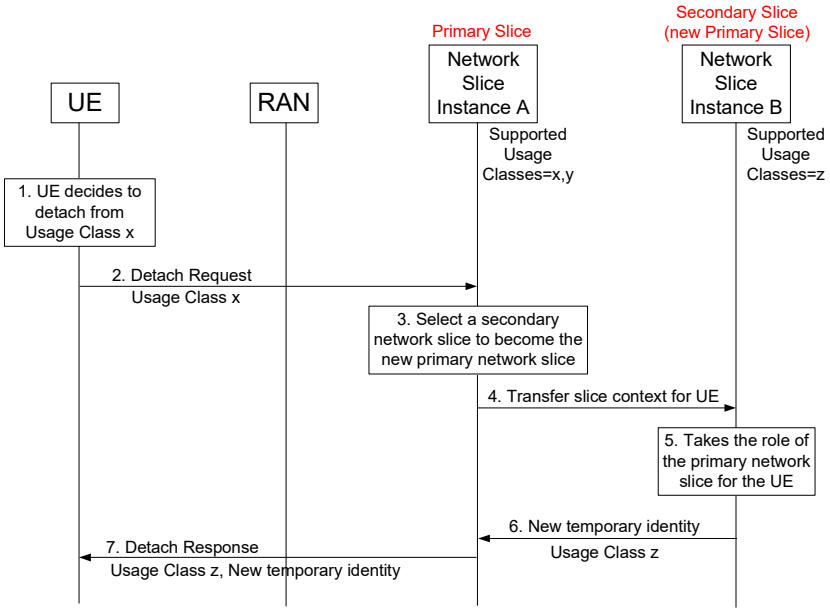


Figure 6.1.9.2.3-1: Detaching from the primary network slice.

Editor's note: Additional procedures that may be required in this solution are FFS. In particular, if there is need to coordinate paging and handovers across the different network slice instances is FFS.

6.1.9.3 Solution evaluation

Editor's note: The solution evaluation is FFS.

6.1.10 Solution 1.10: Roaming architecture for Network Slicing based on solution#2

Figure 6.1.10.1.1-1 depicts the non-roaming architectural concept based on solution#2 for the Core Network Slicing. Figures 6.1.10.1.2-1, 6.1.10.1.3-1 and 6.1.10.1.4-1 depict the roaming architecture scenarios. Among all these

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 98 of 501

architecture, the Core network slice is sharing some network functions with other slices for that serve the same UE, including the NG1 and NG2 terminations, at the CCNF.

6.1.10.1.1 Basic Non-roaming architecture

The following non-roaming scenario is based on network slicing solution#2 as captured in clause 6.1.2.

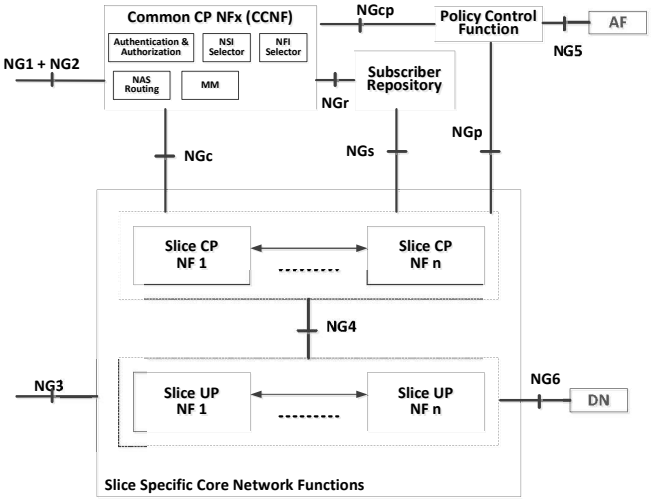


Figure 6.1.10.1.1-1: Core Part of Network Slicing concept (Non-roaming scenario)

Editor's note :The support of NGcp between the CCNF and the Policy Control Function (PCF) is dependent on the outcome of NextGen policy framework as documented as KI#10 in clause 6.8.10.

6.1.10.1.2 Home-routed roaming architecture

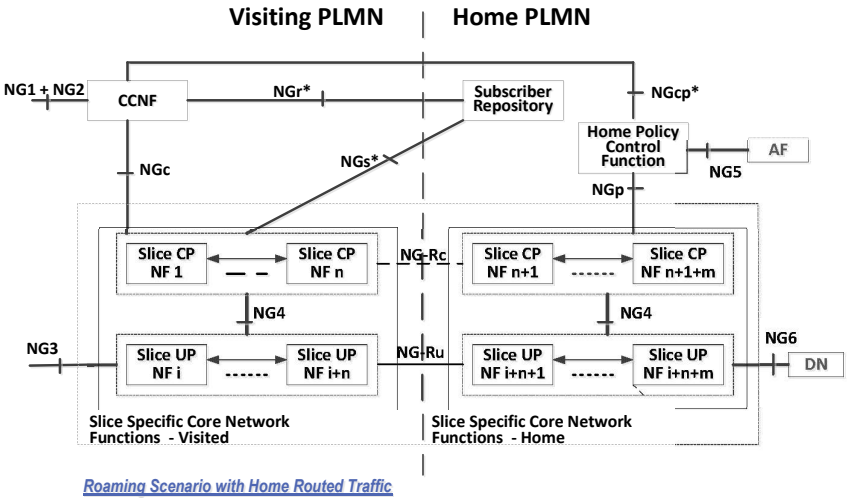


Figure 6.1.10.1.2-1: Core Part of Network Slicing concept (Home Routed roaming scenario)

In all roaming scenarios, it is possible that, the control plane and the user plane of the Core part of the NSI may be split between the visited and the home PLMNs (e.g. SM etc.). Such design consideration is very similar to today EPC roaming scenario.

The assignment of network function at the HPLMN corresponding to the requested slice type from the VPLMN is the decision of the HPLMN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 99 of 501

Based on the roaming agreement, during NSI selection, the serving CCNF uses the subscriber information it has obtained from the HPLMN Subscriber Repository, which includes the subscribed MDD, the subscribed DNN and possibly other information (e.g. to support the selection of the network function entities corresponding to the subscribed MDD and subscribed DNN in HPLMN) to bind the subscribed MDD with a MDD value in the VPLMN.

The serving CCNF replaces the serving PLMN MDD with the corresponding HPLMN subscribed MDD (which was bound to it in NSI selection phase) in signalling it routes to Slice Specific Network functions which may require the Slice Specific Network Functions in the VPLMN to interact with Slice Specific Network Functions in the HPLMN. The Routing of this signalling from VPLMN Slice Specific Network Functions to HPLMN Slice Specific takes into account the subscribed MDD.

If there is no roaming agreement to support Network slicing between a HPLMN and a VPLMN, the VPLMN assigns the UE to an inbound roaming slice and the selection of the HPLMN functions is based on the DNN only.

6.1.10.1.3 Local breakout roaming architecture supporting Home PLMN Application Function

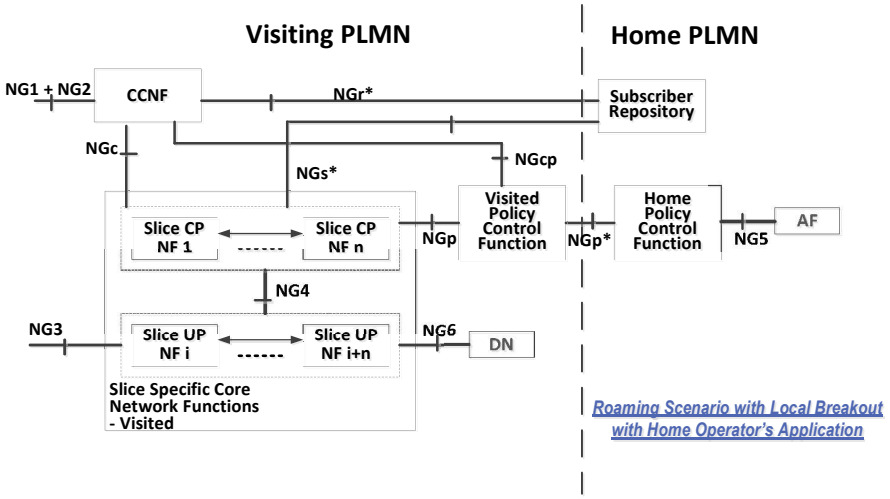


Figure 6.1.10.1.3-1: Core Part of Network Slicing concept (Local Breakout roaming scenario with Home Operator's Application Function)

In the above local breakout roaming scenario, the visited PLMN hosts the NSI to serve the UE's home PLMN's application function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 100 of 501

6.1.10.1.4 Local breakout roaming architecture supporting Home PLMN Application Function

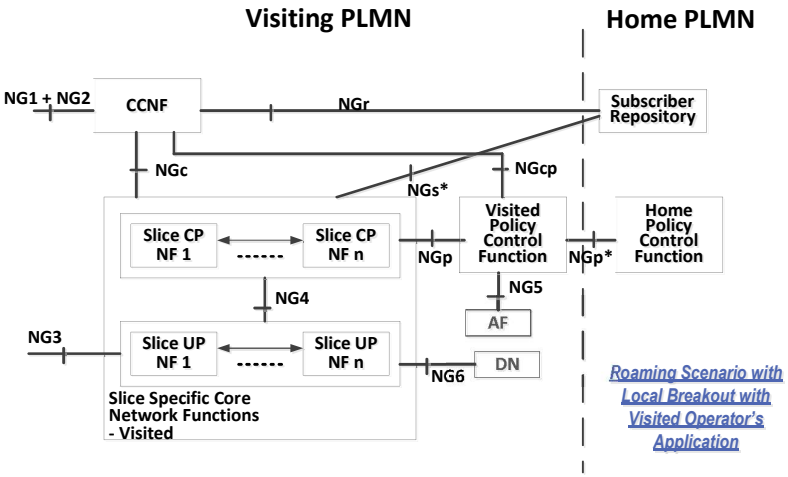


Figure 6.1.10.1.4-1: Core Part of Network Slicing concept (Local Breakout roaming scenario with Visited Operator's Application)

In the above local breakout roaming scenario, the visited PLMN hosts the NSI to serve for its local application function.

6.1.10.2 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.1.11 Solution 1.11: Network Slice Instance Selection and Association

Editor's note: Before this solution can be considered as one possible alternative, one must justify the architecture difference of this solution compared to other existing solutions that have been proposed in clause 6.1.

6.1.11.1 Architecture description

It is possible that a network slice instance is created with special designed network functions, which form a specific network function topology for this particular network slice instance, to provide particular kind of service. For example, a network slice instance that provides enhanced mobile broadband services may consist of an EAP-AKA based authentication function, a general mobility management function, a general session management function, a dynamic IP address allocation function, UP NF1 and UP NF5. While a network slice instance that provides mission critical services may consist of fast authentication function, a QoS management function, a static IP address allocation function, UP NF2, UP NF3 and UP NF4.

Editor's note: What is meant by "fast authentication" and the need for such concept is FFS.

Further more, the network slice instances may be comprised of VNFs generated by using a network slice template, with pre-defined network functions and interfaces. That means there is no need to select network function within a network slice instance.

Figure 6.1.11.1-1 shows an example of the network architecture of network slice instance selection and association.

Editor's note: The below figure needs to be replaced by an editable figure according to the 3GPP Drafting Rules.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 101 of 501

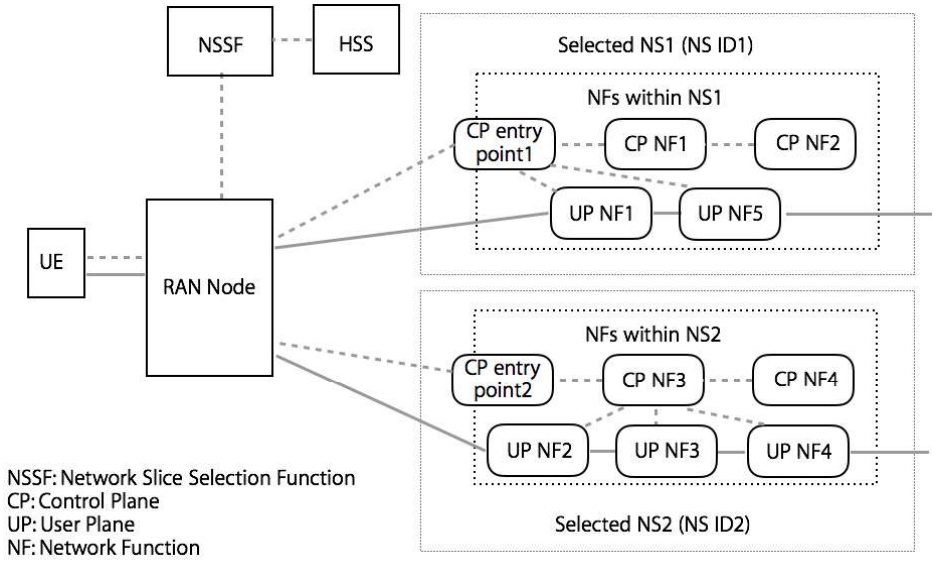


Figure 6.1.11.1-1 network slice instance selection and association architecture

Network Slice Selection Function (NSSF) is responsible for selecting a proper Network Slice ID for a particular UE connection upon the RAN node's request, based on user subscription from the HSS and operator's policies.

CP entry point is the CP network function that connects to the RAN node and is the first hop in core network for the control signaling.

Network Slice Identifier (NS ID) is unique within a PLMN.

Editor's note: it is FFS whether the NSSF is part of the AN or the CN.

6.1.11.2 Function description

6.1.11.2.1 Network slice instance selection and association procedure

Editor's note: How authentication and authorization are performed, and how the HSS is involved in these functions, need to be described.

Editor's note: The below figure needs to be replaced by an editable figure according to the 3GPP Drafting Rules.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 102 of 501

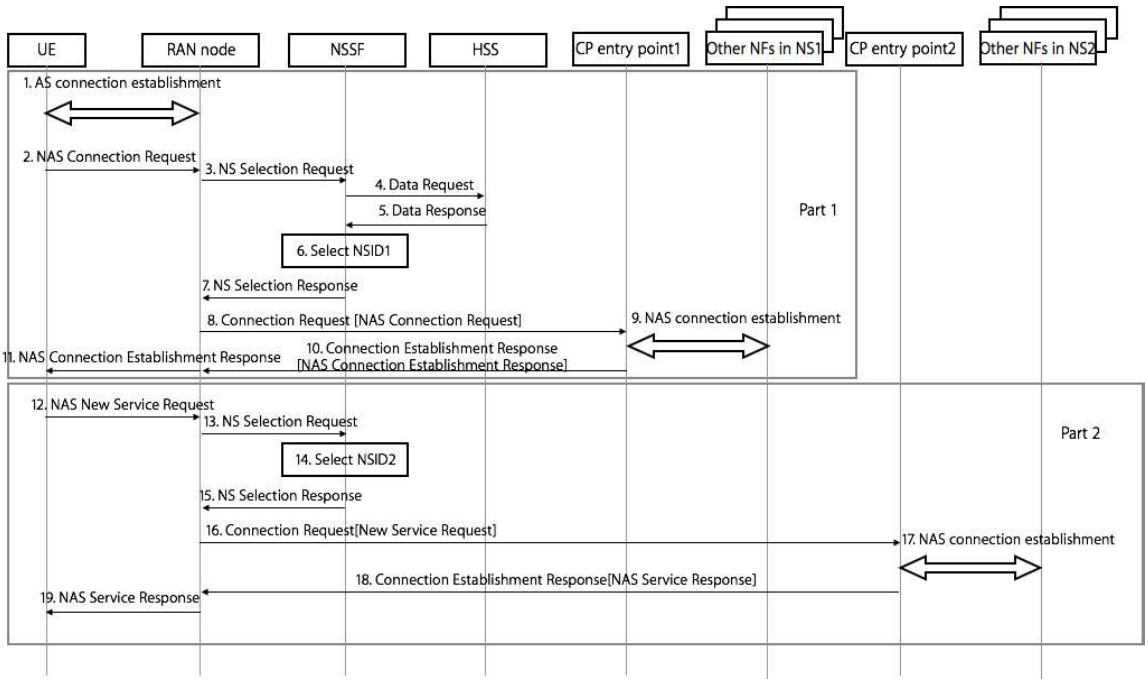


Figure 6.1.11.2.1-1 network slice selection and association procedure

1. RAN node may broadcast its supporting NSIDs in addition to the PLMN ID. After having performed PLMN selection, the UE may select the RAN node according to its supporting NSIDs. The UE and RAN node establish AS connection.

Editor's note: The requirement for the RAN node to broadcast NSID needs further study in RAN WGs.

Editor's note: It is FFS on how UE recognizes the broadcast NSID from different roaming partners of its HPLMN for the UE's target service(s).

2. The UE sends a NAS connection request message to the selected RAN node, with information e.g. UE ID, Service Type, Application ID, etc. Optionally, the UE may include a UE preferred NSID in the message.

3. The RAN node send NS selection request message to the Network Slice Selection Function (NSSF), containing the information got in step 2, e.g. UE ID, Service Type, Application ID, UE preferred NSID, and RAN node ID, etc.

4. The NSSF checks if it has valid subscription data or network slice selection related data for the UE. If not, the NSSF requests for the UE's subscription data or network slice selection related data from the subscription repository (e.g. HSS).

Editor's note: Mutual authentication and authorization of the UE to access the RAN needs to be described.

5. The HSS send requested data to the NSSF. The NSSF stores the data from the HSS and starts a timer for its validation.

6. Based on operator's network slice selection policies, the NSSF selects a NSID according to the information got in step 3 and step 5. If the UE preferred NSID is provided and matches the selection policy, it will have highest priority among all matching NSIDs. If the UE preferred NSID does not match the selection policy, the NSSF shall select the one with highest priority among all matching NSIDs. A Network Slice ID is associated with one CP entry point and a set of CP Network Functions and UP Network Functions

Editor's note: The architecture as shown in Figure 6.1.11.1-1 requires two level UE authentication. It is FFS whether the NSSF is co-located with a Common Control Network Functions (CCNF) in order to optimize UE authentication.

Editor's note: Authorization aspects to access the Network Slice are FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 103 of 501

7. The NSSF sends the NS selection result message to the RAN node, containing the selected NSID (in this case NSID1) and associated CP entry point (in this case CP entry point1) IP address information.

8. The RAN node sends a connection request message to the CP entry point1 carrying the NAS connection request message, with the selected NSID1 and RAN node ID. The RAN node establishes UE context with the selected NSID1 and CP entry point1 IP address.

9. The CP entry point1 starts the connection establishment procedure as pre-defined for the selected NSID1.

NOTE: The connection establishment procedure may be network slice specific, involving different network functions. The connection establishment procedure may include one or more of the following parts: authentication, temporary ID allocation, IP address allocation, session establishment, etc.

10. The CP entry point1 sends a connection establishment response message to the RAN node, carrying the NAS connection establishment response and UP NF1 IP address. The RAN node updates UE context adding routing information e.g. UP NF1 IP address, corresponding AS connection ID.

11. The RAN node sends the NAS connection establishment response to the UE containing information e.g. temporary UE ID, IP address allocated for the UE.

Editor's note: How cyphering and integrity protection at the AS and NAS are performed, and with which keys, are FFS.

12. The UE sends a New Service Request message to the RAN node in a new NAS connection, with information e.g. UE ID, Service Type, Application ID, etc. Optionally, the UE may include a UE preferred NSID in the message.

Editor' note: It is FFS whether the Service Request uses an existing or a new security association in order to reduce the number of NAS contexts the UE needs to maintain.

13. The RAN node sends NS selection request message to the Network Slice Selection Function (NSSF), containing the information got in step 12, e.g. UE ID, Service Type, Application ID, UE preferred NSID, and RAN node ID, etc.

14. The NSSF checks if it has valid subscription data or network slice selection related data for the UE. Based on operator's network slice selection policies, the NSSF selects a NSID (in this case NSID2) according to the above data and information got in step 13.

15. The NSSF sends the NS selection result message to the RAN node, containing the selected NSID (in this case NSID2) and associated CP entry point (in this case CP entry point2) IP address information.

16. The RAN node sends a connection request message to the CP entry point2 carrying the New Service Request message, with the selected NSID2 and RAN node ID. The RAN node updates UE context, adding NSID2 and CP entry point2 IP address.

17. The CP entry point2 executes the connection establishment procedure as pre-defined for the selected NSID2.

18. The CP entry point2 sends a connection establishment response message to the RAN node, carrying the NAS Service Response and UP node IP address. The RAN node updates UE context adding new routing information e.g. UP NF2 IP address, corresponding AS connection.

19. The RAN node sends the NAS service response to the UE.

Editor's note: it is FFS if and how the UE maintains separate NAS signaling connections and MM contexts with different CP entry points in the CN.

6.1.11.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 104 of 501

6.2 Solutions for Key Issue 2: QoS framework

6.2.1 Solution 2.1: Per PDU Flow QoS Model

6.2.1.1 Architecture description

This solution addresses the key issue 2 on a QoS framework.

The QoS functions of current 3GPP architecture are distributed between the UE, RAN and CN. This solution describes an overall QoS solution for the NextGen system, describing how the QoS functionality is distributed between the CN, the RAN and the UE, see Figure 6.2.1.1-1 for a high level view of such functional split.

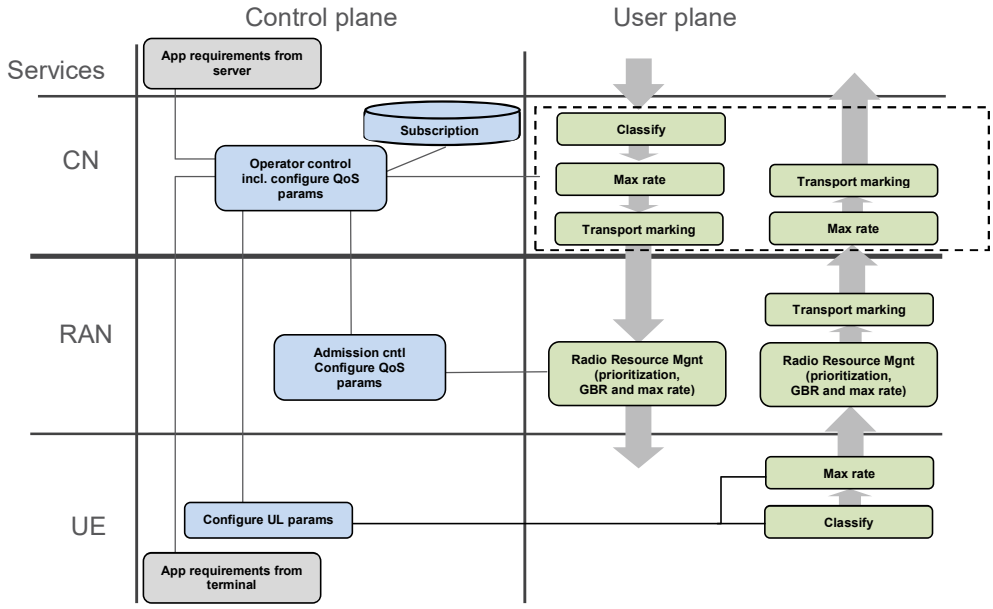


Figure 6.2.1.1-1: QoS functional split including 3GPP RAN

The table 6.2.1.1 below lists the QoS functional split corresponding to the Figure 6.2.1.1-1 above.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 105 of 501

Table 6.2.1.1: QoS functional split between UE, AN, CN and SL

Function	Distribution	Comment
Subscription(incl Default QoS Profile)	CN	
QoS Operator control	CN	
Access and Admission control	AN	Access and Admission to AN resources
Configuration of QoS parameters	UE, AN, CN	
Application requirements input	From CN/SL to CN From UE/SL to CN From UE/SL to CN/SL	The application requirements input may be sent from either the server or the client.
Classification:	CN (DL), UE (UL)	Provides classification of packets for QoS purposes
Max rate control	CN (DL, UL) AN (DL. UL) UE (UL)	
Transport marking	AN (UL), CN (UL, DL)	
Resource Mgmt	AN	Packet scheduling with regards to resource utilization and availability (RRM) Resource mgmt is also performed in the transport domain (not visible in figure 6.2.1.1-1

NOTE: This solution has dependency on RAN WGs. Decision to support QoS functionalities proposed for NextGen RAN is up to RAN WGs.

Subscription (incl Default QoS Profile): The subscription contains information about which QoS parameters that are included in the subscription terms. The subscription QoS is an input for the network when authorizing the QoS for a PDU session and a non-Service-specific PDU flow in the QoS Operator control function.

QoS Operator control: With the input from the subscription, operator policies and application requirements input from the service layer, the QoS parameters for PDU sessions and PDU flows are authorized in the QoS Operator control function. The QoS Operator control function is also responsible for distributing the authorized QoS parameters in the network. In case of PDU connectivity services provided in network sharing and/or roaming across, the QoS Operator Control allows also to limit the QoS offered by the network providing the access.

Access and Admission control (AN): The access control in the AN regulates the conditions on which the UE establish a request for connection in the random access channel based on the QoS parameters applied for the session and flows. The admission control function controls which PDU flows that shall be admitted in the access network when the resources are scarce based on the QoS parameters applied for the session and flows. The admission control also includes to sacrify already admitted flows to allow more prioritized flows.

Configuration of QoS parameters: Each network element in the end-to-end solution is configured with the expected behaviour with respect to QoS, i.e. how QoS parameters received from the QoS Operator control function shall be handled and applied to the PDUs.

Application requirements input: To know the requirements of the Service Data Flows transmitted through the network, the network may be informed from the service layer about the service behaviour and service requirements. The application requirement input is used by the QoS Operator control function when authorizing the QoS parameters for PDU session and PDU flows.

Classification: Indicates which Service Data Flow and PDU flow each packet belongs to. The classification is used to select which authorized QoS parameters to apply to each PDU in the CN-UP, AN-UP and UE-UP. Deducible SDFs may be classified based on TFT filters in DL and UL. Non-deducible SDFs may be classified in DL based on packet inspection. CN-CP may also provide application layer information (e.g. application identity) to UE for UL traffic classification.UE reflective QoS equivalent to what described in TS 24.139 for fixed broadband network and packet inspection in CN-UP may be used for classification of non-deducible IP or non IP flows in UL.

NOTE: UE reflective QoS cannot be used to unambiguously classify all types of Non-deducible SDFs e.g. aggregated traffic using HTTP/port 80.

Max rate control: Max rate control function ensures that the maximum bitrate in the Authorized QoS parameters are maintained.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 106 of 501

Transport marking: The transport marking function is indicating the expected treatment in IP networks as well as in non 3GPP accesses with a stateless QoS mechanisms, for example routers between the network elements. Each PDU is marked by the CN_UP (DL) or AN (UL) based on the QoS associated to the PDU flow.

Resource Mgmt: The resource management function is responsible for how the resources are distributed in the access network based on the Authorized QoS parameters from the QoS Operator control function and the monitoring of the fulfilment of the QoS targets. The resource management function can be different in 3GPP and non-3GPP ANs with regards to the possibilities to control resource utilization and availability. Resources mgmt is also done in the transport network.

Editor's note: It is FFS if all functions described above are needed for NextGen system.

NOTE: Functions related to policy control are not described in the solution above and will need to be addressed as solutions to the key issue on Policy Framework.

6.2.1.1.1 Relation between PDU Flow and Service Data Flow

The PDU flow is a logical packet transport of defined characteristics, i.e. corresponding to the finest granularity of packet forwarding/treatment differentiation a PDU session can offer to a service data unit flow (SDF). To a PDU Session may be associated a number of logical PDU flows realized in the UP layer. An application in the service layer may require one or multiple Service Data Flows that may be mapped into one or multiple PDU flows. PDU flows may be Service-specific and non-Service-specific PDU flows. The term non-Service-specific PDU flow refers to the PDUs within the PDU session to which there is no specific packet forwarding/treatment differentiation defined (i.e. the non-Service-specific PDU flow will be treated according to the default QoS profile).

In the Next Gen QoS framework a PDU Flow is identified by a PDU FlowId in the header encapsulating the service data unit. Additional identitiers in the header encapsulating the service data unit is dependent on the NG3 tunnel(s) used, e.g. if there is a tunnel per PDU session then in addition an identification of the PDU session is needed.

The PDU Flow ID is assigned to a PDU flow by the CN_CP and distributed to the CN_UP, the 3GPP access network and optionally the UE.

QoS parameters assigned to a PDU flows are distributed by the CN_CP to the CN_UP, the 3GPP access network and optionally the UE, and are enforced by the network functions (CN_UP, AN optionally UE).

Multiple SDFs, a single SDF or part of an SDF (e.g. the first packets of an SDF) may be aggregated through configuration and policy to a single PDU flow and by that be treated according to the QoS of the PDU flow.

Through configuration and policies, multiple SDFs may be aggregated to a single PDU flow or an SDF may be separated into one or more PDU flows and by that be treated according to the QoS of the PDU flow.

The classification of SDFs and binding to PDU flow Id is done based on TFT filters provided by the CN_CP to the CN_UP and to the UE. In case of reflective QoS function, the UE is requested to apply it explicitly based on an indication as part of the UL TFT (with highest precedence priority). The UE may also use application layer information provided by the CN_CP for UL traffic classification.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 107 of 501

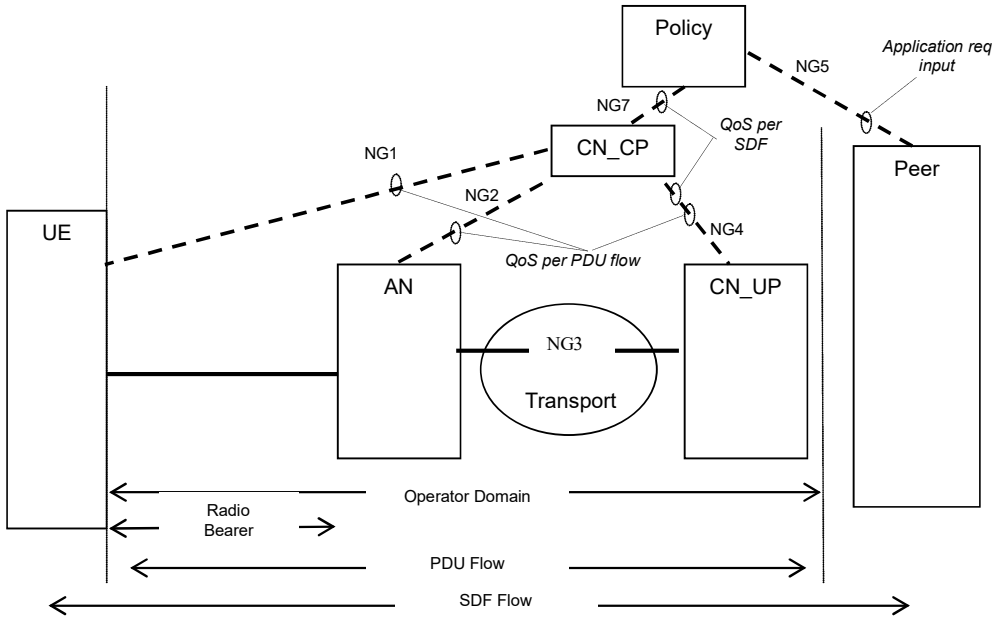


Figure 6.2.1.1.1-1: Relation between PDU flow and Service Data Flow

6.2.1.1.2 Application requirements input

Network needs to know the application requirements in order to apply the correct QoS parameters to the Application's Service Data Flows.

The application requirements information may be provided from the service layer (server or client side):

- Service identification:
  - How to identify the Service Data Flows associated with the application.

NOTE: The Service Data Flows may be of IP type or non-IP type depending on the PDU session type.

- Service Behaviour (the behaviour the network can expect from the application), such as:
  - Maximum bitrate per SDF: the Max bitrate that the service is expected to deliver.
- Service Requirements (the network delivery behaviour requested by the application), such as:
  - Minimum bitrate per SDF: the bitrate that is required for the service to be delivered with sufficient QoE.
- Delay requirements.
- Priority between different SDFs within the application.
  - Requested network behaviour with respect to Admission, Retention and Notification.
  - Requested Measurement Window Size, to indicate the condition when observing the service behaviour and requirements fulfilment.

Editor's note: It is FFS if the Measurement Window Size need to be adaptive or can be configured or specified.

Editor's note: The list of service behavior and service requirements is not exhaustive and it is FFS which application requirement input that shall be specified within the QoS framework e.g. which input that is determined to be useful.

In case of applications depending on the outcome of the request for a specific network treatment to be complete conclusively (yes/no) for all (or a specified set of) involved users within an allotted and relatively short amount of time, such as in case of Mission Critical Communication applications, a function in the application domain may interact with the AF that initiate the request towards the Policy Function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 108 of 501

NOTE 1: The above avoids the need for any "NextGen Resources & QoS Manager" as described in solution 2.7 (see clause 6.2.7).

NOTE 2: Further details on the interaction between the application domain and the Policy function are addressed in the Policy Key Issue.

6.2.1.1.3 Network Authorized QoS parameters

Based on the subscription, application requirements input from the service layer and QoS configuration as well as operator policies, the QoS parameters for the PDU session, for Service-specific and non-Service-specific PDU flows and for Service Data Flows are decided.

QoS parameters per PDU session:

- Aggregated maximum bitrate for the session for all PDU flows of a PDU session.

QoS related parameters per Service-specific and non-Service-specific PDU flows:

- PDU Flow Id: The marking in the tunnelling protocol encapsulation header that identify the PDU flow in the user plane
- Traffic Flow templates and filters (when applicable): classifying the service data flow that the QoS parameters applies to. The TFT filter is defined to classify IP and non-IP flows. For example Ethernet flows may be classified based on Ethernet p-bit.
- PDU Flow Priority: priority per PDU flow for admission to network resources, i.e. how the traffic associated with the flow shall be handled in the AN, at admission and resource mgmt and in CN_UP.
- Maximum bitrate per PDU flow: UL and DL authorized bitrate value for a single PDU flow. This applies to Service-specific and non-Service-specific PDU flows.
- Required bitrate per PDU flow: the bitrate that is required for the service to be delivered with sufficient QoE. This parameter is used by the AN and the AN tries to support the required bitrate. When the AN cannot satisfy the required bitrate, the AN drops packet(s) or provides a best effort service with or without any signalling to the core network based on Network behaviour per PDU flow.
- Delivery characteristic per PDU flow: for example packet delay budget, packet loss/late rate. The delivery characteristics may be expressed via a scalar value such as the QCI value, or explicitly indicated..
- Network behaviour per PDU flow: the expected treatment if the QoS targets represented by the authorized QoS parameters for the flow are not met by the network.

NOTE: Not all QoS related parameters per PDU flow needs to be provided to the enforcement nodes (CN_UP, AN and UE) for all PDU flows. Which QoS related parameters that shall be enforced per PDU flow is an operator choice.

QoS related parameters per Service Data Flow:

- Traffic templates classifying the service data flow that the QoS parameters apply to. The TFT filter is defined to classify IP and non-IP flows. For example Ethernet flows may be classified based on Ethernet p-bit.
- SDF Priority: priority per SDF for admission to network resources, i.e. how the traffic associated with the flow shall be handled in the network at admission and resource mgmt and in CN_UP.
- Maximum bitrate per SDF: UL and DL authorized bitrate value for a single SDF.
- Required bitrate per SDF: the bitrate (Minimum or Guaranteed bitrate per flow) that is required for the service to be delivered with sufficient QoE.
- Delivery characteristic per SDF: for example packet delay budget, packet loss/late rate. The delivery characteristics may be expressed via a scalar value such as the QCI value, or explicitly indicated.
- Network behaviour per Service Data flow: the expected treatment if the QoS targets represented by the authorized QoS parameters for the flow are not met by the network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 109 of 501

NOTE: Not all QoS related parameters per Service Data Flow needs to be provided from the Policy function for all service data flows. Which QoS related parameters that shall be enforced per Service Data flow is an operator choice.

6.2.1.1.3.1 Flow Priority

The Flow priority is a parameter indicating the relative priority of fulfilling the Required Bit Rate and delivery characteristics (delay budget, packet loss/late rate). It impacts both the SDF/PDU flow admission to resources in the network as well as the distribution of resources for packet forwarding treatment, allowing consistency in admission and resource distribution to fulfil the service requirements.

In addition, whenever available, the Flow Priority is used as an input in the AN and in the UE to regulate the access control mechanisms (such as Access Class Barring and similar mechanisms) and thus the UE behaviour when connecting to the AN.

6.2.1.1.4.2 Network behaviour per flow

Network behaviour per flow shall indicate the following behaviour

- Admission. If the flow shall be admitted in the network even if there are not enough network resources to fulfil the service requirements (required bitrate and/or delivery characteristics) associated with the flow cannot be met (Keep/Drop)
- Retention: If the flow can be discontinued to allow the network to admit a flow with higher priority (Retain/May be dropped)
- Notification. If a network element shall send a notification (to the policy function) if the service requirements associated with the flow cannot be met. (Yes/No**)**

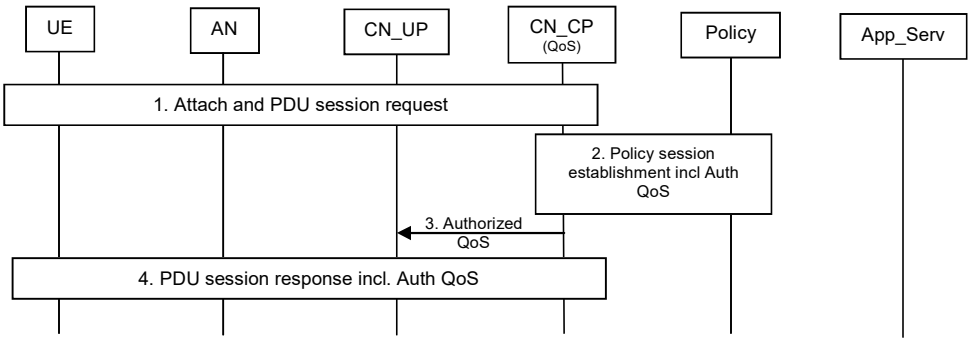
Editor's note: It is FFS how frequently the network elements indicate repeated failures to meet the service requirements.

The Network behaviour may apply to both the SDF/PDU flow.

6.2.1.2 Function description

6.2.1.2.1 QoS Authorization at PDU session establishment

During the PDU session establishment, the QoS for a generic treatment of service data flows in the network is decided and associated to a non-Service-specific PDU flow:



6.2.1.2.1-1: Sequence diagram for Authorized PDU Session QoS

1. The UE attach to the network and a PDU session between the UE and a data network is requested. The PDU session carries all traffic related to PDU connectivity service regardless of the characteristics of individual Service Data flows.
2. If deployed, the CN_CP (QOS) establish a session towards the Policy function and invoke to authorization of the PDU session including the Authorized QoS of the PDU session and for the PDU flow to be used for a generic treatment of service data flows in the network. Alternatively the CN_CP (QOS) may authorize the PDU session including the Authorized QoS of the PDU session and for the PDU flow to be used for a generic treatment of service flows in the network based on local policies.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 110 of 501

SDF QoS and Service specific PDU flows QoS may be authorized by the policy function or via local policy in this step.

3. The CN_CP (QOS) forward the Authorised QoS for the PDU session and the authorized QoS for the non service specific PDU flows (to be used for a generic treatment) to CN_UP. The CN_UP acknowledge the reception.

   Optionally, if service specific PDU flows have been authorized, the CN_CP (QOS) forward the Authorized QoS related parameters for those PDU flows to the CN_UP, well as the Authorized QoS per service data flows.

4. The CN_CP (QOS) complete the PDU session establishment and inform the network functions about the Authorized QoS of the PDU session (QoS parameters per PDU session and QoS related parameters for non-service specific PDU flows) as well as optionally QoS related parameters for service-specific PDU flows on which the QoS has to be enforced.

Editor's note: Details of step 4 in figure 6.2.1.2.1-1 is FFS.

6.2.1.2.2 QoS Authorization based on application requirements

An application server may require a specific treatment in the network of service data flow or flows. If so the Policy Function can authorize a QoS per SDF to be associated to a PDU flow and enforced by the network.

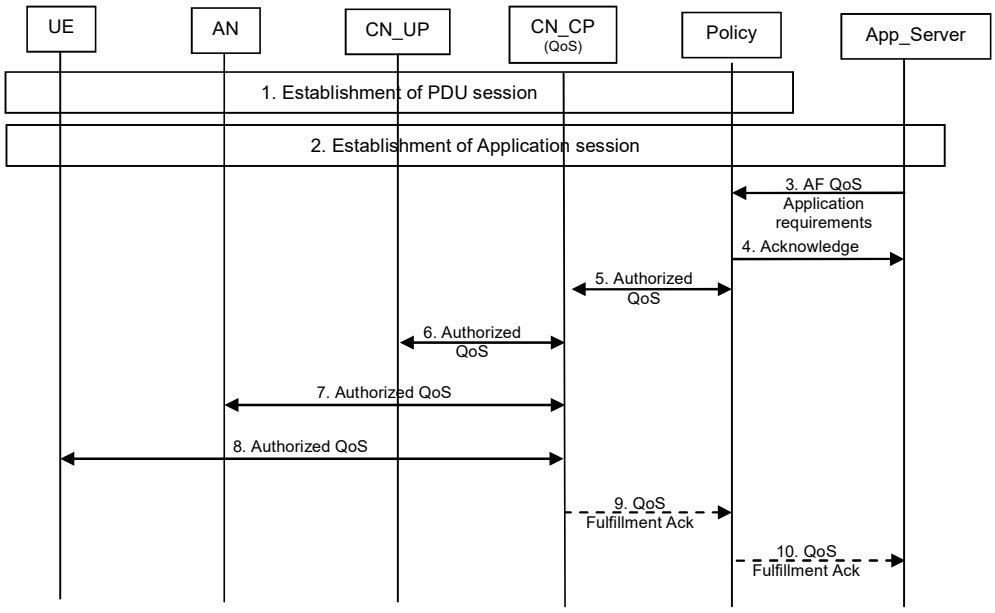


Figure 6.2.1.2.2-1: Sequence diagram for Authorized Flow QoS

1. A PDU session is established between the UE and a data network. The PDU session carries all traffic related to PDU connectivity service regardless of the characteristics of individual Service Data flows. The Policy function may be invoked to authorize the QoS characteristics of the PDU session as described in clause 6.2.1.2.1.

2. An Application Session consisting of one or multiple service data flows is established between the UE and the Application Server.

3. The App_Server (Service Layer) indicates the application QoS requirements as well as the necessary information to classify the application's service data flow(s). The request from the App_Server may be originating from the App_Server or from the UE through Service Layer communication.

4. Based on the operator policies, the Policy Function authorizes the QoS that the network will enforce on the application's service data flow(s) and acknowledge the Application layer.

5. The Policy Function sends the Authorised QoS per service data flow to CN_CP (QOS), as well as the necessary information to classify the application's service data flow(s). The Authorised QoS per service data flow represent the treatment that the network shall apply to the flow.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 111 of 501

6. The CN_CP (QOS) process the Authorised QoS per service data flow and forward the Authorised QoS related parameters per PDU flow to CN_UP as well as the Authorized QoS related parameters per service data flow. The CN_UP acknowledge the reception.

From this point the CN_UP may mark downlink packets matching the SDF with the PDU FlowID in the PDU encapsulation header.

From this point the CN_UP may mark downlink packets matching the SDF with a suitable marking in the outer header of the PDU derived from the Authorized QoS related parameters for the PDU flow.

7. The CN_CP (QOS) forward the Authorised QoS related parameters per PDU flow to AN. The AN acknowledges the reception and confirms that the Authorized QoS can be fulfilled to the CN CP.

The AN execute the differentiated treatement of the PDUs based on the Authorised QoS associated to the PDU Flow ID

NOTE: In case of transport networks and non-3GPP accesses, lacking the capability of receiving the authorized QoS for the PDU flow over the control plane, the execution of the differentiated treatment of the PDUs is based on the marking available in the outer header of the PDU.

8. The CN_CP (QoS) forward the Authorised QoS (TFT and filters, maximum bitrate) to the UE for classification and possible actions such as rate control. The UE acknowledge the reception.

9. The CN_CP (QOS) may confirm that the Authorized QoS can be fulfilled to the Policy Function.

10. The Policy Function may confirm that the Authorized QoS can be fulfilled to the App_Server.

6.2.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.2.1.3.1 Solution comparison to the existing framework

The solution follows the principles of the EPS QoS framework, retaining the Policy centric control of QoS authorization and leveraging on a per PDU flow QoS for service differentiation.

Improvements and enhancements are suggested to address the ability of fulfilling the requirements from new services foreseen for 5G, for example High Reliable communication services. High Reliable communication services are characterized by the service layer need of committed QoS targets and its possibility to act upon an expected change of the network fulfillment of the QoS targets.

The following enhancements are initially proposed (compared to the current EPS QoS framework):

- Improved Service-Network interaction allowing the service layer to request a specific network behaviour related to Admission, Retention and Notification. With this approach the network behaviour is extended beyond the currently available distinction between GBR (submitted to admission control) and nonGBR PDU Flows (no admission control and no network commitments), allowing the network (for any type of PDU flow):
  - to monitor the QoS targets fulfilment and
  - to notify the service layer in case the QoS targets cannot be fulfilled and the service layer has requested to be notified.
- Enhanced QoS parameters and alignment between application requirements parameters and authorized QoS parameters per PDU flow and SDF
  - Introduction of Required Bit Rate parameter for any kind PDU flow (regardless if "GBR" or "nonGBR" type).
  - A single priority parameter per PDU flow for admission and QoS targets (delay, bitrate etc.) fulfilment.
  - Decoupling of the PDU flow priority for QoS targets fulfilment from the delivery characteristics per flow
  - Option for explicit QoS targets (delay, bitrate etc.)

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 112 of 501

- Finer QoS granularity handling. PDU flow is the finest granularity for QoS handling. PDU Flow Id is added in the encapsulation header to identify the Authorised QoS of the PDU flow in the CN-UP, AN and optional UE. One SDF may be classified and bind to multiple PDU flows.

Those enhancements aim to simplify configuration, improve the predictability of the effects of QoS differentiation and limit the proliferation of standardised QCI values compared to the EPS QoS framework.

Editor's note: Additional differences with the EPS framework is FFS

6.2.2 Solution 2.2: Flow based QoS framework

This is a solution to Key issue 2: QoS framework.

6.2.2.1 Architecture description

The Figure 6.2.2.1-1 represents a flow based QoS non-roaming architecture that is used to describe the proposed QoS framework.

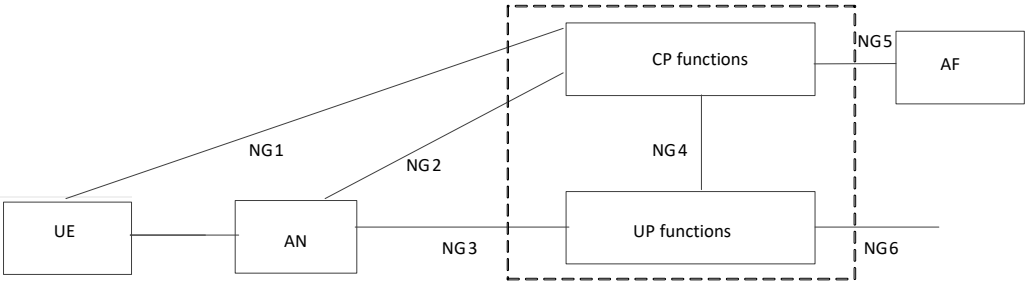


Figure 6.2.2.1-1: Flow based QoS non-roaming architecture

The Figure 6.2.2.1-2 represents a flow based QoS architecture for roaming, home routed traffic

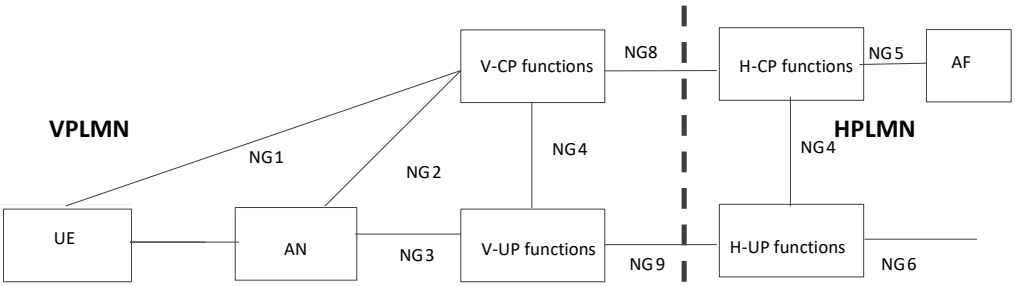


Figure 6.2.2.1-2: Flow based QoS architecture for roaming, home routed

The Figure 6.2.2.1-3 represents a flow based QoS architecture for roaming, local breakout

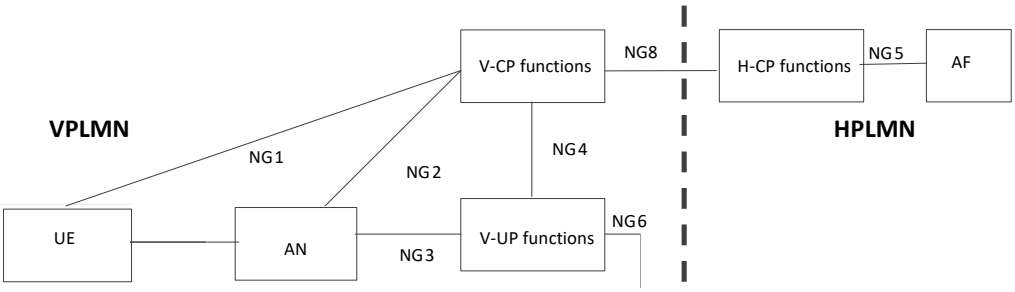


Figure 6.2.2.1-3: Flow based QoS architecture for roaming, local breakout

NOTE 1: These solutions do not assume a specific number of CP and UP functions, for illustrative purposes the CP and UP functions have been grouped.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 113 of 501

The QoS policy is stored and set-up at the CP functions in order to be:

- Enforced at UP functions.
- Transferred to AN and UE for QoS enforcement.

The following list of parameters is needed at this stage for QoS framework definition:

- Flow Priority Indicator (FPI): define priority per flow treatment at UP and AN functions. It corresponds to scheduling priority as well as priority handling in case of congestion. The FPI also indicates whether the flow requires guaranteed flow bitrate and/or maximum flow bitrate. The packet delay budget and packet error rate are implicitly covered by the FPI.

NOTE 2: The packet delay budget (PDB) associated with the FPI is a default parameter. The network can override the default PDB value with another value using C-plane signalling.

- Flow Descriptor: packet filters associated with that specific flow treatment. In uplink identification shall be done in the UE and AN but limited to layers 2 (e.g. for Ethernet PDU type) or 3 and 4 (for IP PDU Session type). In its request for uplink resources to RAN the UE specifies the FPI linked to the identified packets it intends to send.

Editor's note: This solution assumes that the RAN design of the radio interface supports transmission of FPI or class of FPI in request from the UE for uplink resources.

- Maximum Flow Bitrate (MFB): UL and DL bitrate value applicable for a single flow or aggregation of flows. It indicates maximum bitrate authorized for the data flow identified by a flow descriptor.
- Guaranteed Flow Bitrate (GFB): UL and DL bitrate value applicable for a single flow or aggregation of flows. It indicates guaranteed bitrate authorized for the data flow.

Application traffic detected by application detection function will be assigned a flow descriptor if deducible. That flow descriptor may be linked to a GFB which will then apply to the deducible flow. Otherwise a default flow descriptor will be assigned to the non-deducible flow and application of a GFB will not be possible on it.

NOTE 3: The MFB of a guaranteed flow shall be set larger than or equal to the GFB.

- Flow Priority Level (FPL): defines the flow relative importance to access to AN resource. In addition, the FPL indicates whether the access to AN non-prioritized resource should be pre-emptable and resources allocated should be protected from pre-emption.
- Session Bitrate: UL and DL bitrate value applicable for the established user session. It indicates maximum bitrate authorized for user session.
- Reflective QoS Indication (RQI): DL indication applicable for a single flow or aggregation of flows. When used as U-plane marking it is determined by the UP functions and is applied on per-packet basis for the lifetime of a flow.

Editor's note: It is FFS whether RQI need to be signaled in-band or whether UE shall apply reflective QoS for all flows that were initiated without explicit C-plane QoS signaling.

Editor's note: It is FFS whether RQI is needed in the uplink to allow the UE to indicate to the network to apply the same QoS for corresponding downlink flows.

Editor's note: It is FFS how the UP functions determines the lifetime of the flow and whether the FPI can change during the lifetime of a flow.

Editor's note: It is FFS whether UE bitrate value should be defined.

Two types of user plane per-packet marking information are introduced:

- Packet Priority Indicator (PPI): define scheduling priority per packet at UP and AN functions. Different PPIs are marked to the packets in the same flow by the NextGen UP functions and UE to identify the different scheduling priority for the packets e.g. with different content type.

Editor's note: It is assumed that either PPI or FPI is used as a user plan per-packet marking.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 114 of 501

Editor's note: How the UE supports different PPIs marking for the UL packets requiring different scheduling priority (e.g. with different content type) in the same flow is FFS.

- Packet Discard Priority Indicator (PDPI): defines the discard priority per packet in the NextGen system in case of congestion e.g. for differentiating content within the same flow. The PDPI marking in the downlink is set by the UP functions and is used by the AN.

Editor's note: Whether PDPI is used in the uplink and how is FFS.

Editor's note: The DL PPI and PDPI marking need per-packet inspection in the NextGen UP functions. How the NextGen UP functions decide the marking is FFS.

Editor's note: It is FFS whether a single parameter or multiple parameters carry the PPI and PDPI information.

QoS parameters are applicable at least in the following functions as summarized in the table below:

Table 6.2.2.1-1: QoS parameters

QoS parameters		UP functions	AN	UE
Flow Priority Indicator (FPI)		*	*	*
Flow Priority Level (FPL)			*	
Packet Priority Indicator (PPI)		*	*	*
Packet Discard Priority Indicator (PDPI)		*	*	*
Flow Descriptor	DL	*	*	
	UL	*	*	*
Maximum Flow Bitrate (MFB)	DL	*		
	UL		*	
Guarantee Flow Bitrate (GFB)	DL		*	
	UL		*	*(1)
Session Bitrate	DL	*		
	UL		*	
Reflective QoS Indication (RQI)	DL	*	*	*

Editor's note: It is FFS whether GFB is applicable in UP functions.

NOTE 4: Support of GFB in the UE depends on the QoS design of the radio interface.

The following reference points are assumed for the purpose of describing the QoS framework:

NG1: Reference point between the UE and the CP functions.

NG2: Reference point between the AN and CP functions.

NG3: Reference point between the AN and UP functions.

NG4: Reference point between the CP functions and UP functions.

NG5: Reference point between the CP functions and an Application Function (AF).

NG6: Reference point between the UP functions and a Data Network (DN).

NG8: Reference point between the V-CP and H-CP functions (roaming scenarios).

NG9: Reference point between the V-UP and H-UP functions (roaming scenarios).

All the parameters in the table above may be provided using C-plane signalling over NG4, NG2, NG1 or even at access stratum, depending on the RAN design for the radio interface.

FPI and RQI are used on NG3 and on the radio interface on per-packet basis for the lifetime of a flow:

- Upon uplink data reception the RAN performs verification whether the FPI corresponds to the set of pre-authorised FPIs and replicates it on the NG3 interface (e.g. in the NG3 encapsulation header, and/or as transport-layer marking). The uplink FPI is used further upstream by the UP functions to perform validation e.g. whether the FPI used by the UE corresponds to the (pre-)authorised QoS policies.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 115 of 501

- Upon downlink data reception the RAN uses the downlink FPI to determine the QoS treatment on the radio. It may also replicate the received downlink FPI and/or downlink RQI on the radio interface. Upon downlink data reception UE uses the downlink RQI to determine whether it shall apply reflective QoS on the corresponding (as determined by the UE) UL flows. The UE may use the downlink FPI to determine QoS for the corresponding uplink traffic in case of reflective QoS.

C-plane signalling over the radio interface should be used only when the information provided using U-plane markings (i.e. FPI and RQI) is not sufficient.

Editor's note: This solution assumes that the RAN design of the radio interface supports U-plane markings (e.g. FPI and/or RQI) on per-packet basis in both uplink and downlink.

Editor's note: This solution assumes that the RAN design of the radio interface supports in-band initiation of "radio bearers" (similar to the existing support on PC5 or GERAN) i.e. without any C-plane signaling between the UE and the network.

Editor's note: This solution assumes that the RAN design of the radio interface is able to map the uplink FPI to corresponding radio resource control.

6.2.2.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Depicted in Figure 6.2.2.2-1 is a call flow describing the C-plane QoS signalling.

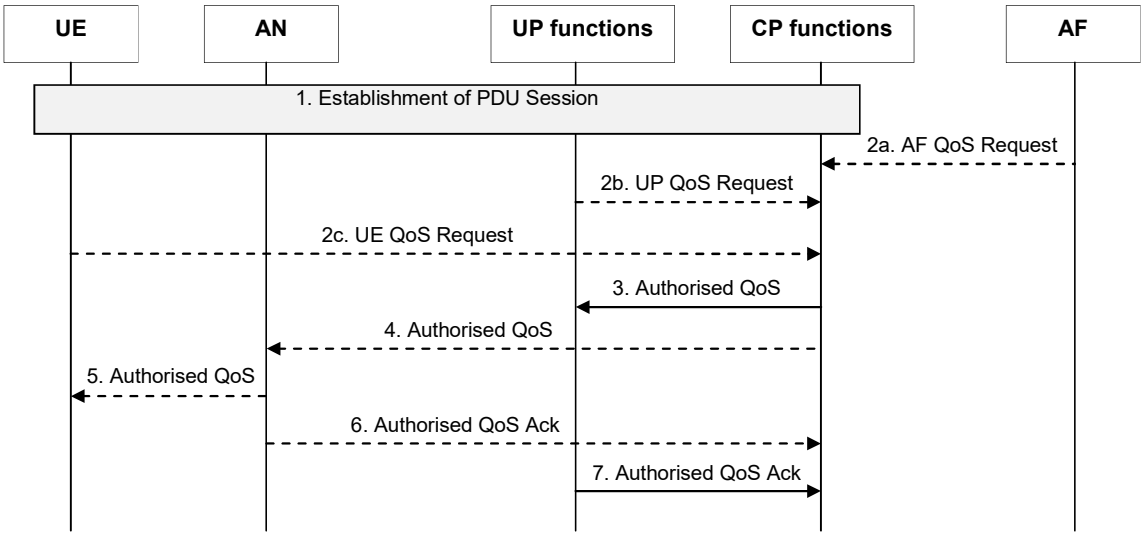


Figure 6.2.2.2-1: Flow based QoS architecture: Control plane signalling

1. A PDU Session is established between the UE and a data network. The PDU Session carries all traffic related to the PDU Session regardless of the QoS characteristics of individual traffic flows. QoS differentiation between several flows multiplexed on the same PDU Session can be provided by means of a QoS marking applied to each packet. As part of this step the UE is provided with a set of pre-authorised FPIs using AS signaling for which it can initiate UL packets without explicit signalling with the network.

2. A new QoS request is received by the CP functions from the Application Function (AF), from the UP functions, or from the UE, as described in steps 2a, 2b and 2c, respectively.

2a. The Application Function (AF) is an element offering packet flow that requires a specific QoS treatment. The AF sends [NG5] AF QoS request (Flow Descriptor, flow bitrate) to CP functions.

2b. The UP functions detect a new flow that requires specific QoS handling and sends a [NG4] UP QoS Request (Flow Descriptor, Application ID) to CP functions.

2c. The UE sends an explicit QoS request by sending a [NG1] UE QoS Request (Flow Descriptor, Requested QoS) to CP functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 116 of 501

3. The CP functions determines the authorised QoS for the QoS request received in step 2 based on operator requirements. The QoS policy is the list of parameters applicable to control QoS in relevant NextGen entities (CN, AN, UE).

   The CP functions sends a [NG4] Authorised QoS (UL and DL Flow Descriptor, Flow Priority Indicator, DL Max Flow Bitrate, DL Session Bitrate, RQI). The DL Flow Descriptor is used by the UP functions to identify user plane packets on which to perform packet classification and marking with the Flow Priority Indicator received within QoS policy. UL Flow Descriptor is used for validation of the FPI sent by the UE. In addition, the UP functions use DL Max Flow Bitrate and DL Session Bitrate to apply maximum bitrate control for downlink packets at the flow and PDU Session level.

   The Flow Priority Indicator refers to parameters which are preconfigured at AN node and which describe the packet treatment. RQI indicates whether UE shall apply reflective QoS for corresponding uplink flows. FPI and RQI are used by UP function for U-plane marking over NG3 in the downlink.

4. The CP functions may send [NG2] Authorised QoS (UL and DL Flow Descriptor, Flow Priority Indicator, FPL, UL Max Flow Bitrate, UL and DL GFB, UL Session Bitrate) message to the AN.

   The UL Flow Descriptor is used by the AN to identify user plane packets on which to perform policing action. The AN uses UL Max Flow Bitrate and UL Session Bitrate to enforce maximum bitrate control at PDU Session and flow levels for uplink user plane data packets based on received values.

NOTE: As part of this step the CP functions also provides information that allow the AN node to identify the PDU Session.

This message is optional. It is used only if AN needs to receive information that is not possible to receive using downlink user plane markings on NG3 or when the network needs to send Authorised QoS information to the UE. For instance, it is typically performed only for GFB flows or when a QoS modification is required for a non-GFB flow. If the UE requested explicit uplink QoS in step 2c, this message is mandatory to send Authorised QoS information to the UE.

5. The network may send Authorised QoS information (i.e. UL Flow Descriptor, Flow Priority Indicator, UL GFB) to the UE. It is assumed that the QoS information is signalled as AS information. The UL Flow Descriptor is used by the UE to identify user plane packets on which to perform packet classification and marking in the uplink with the Flow Priority Indicator received within the QoS policy.

This message is optional. It is typically triggered by step 4 and is used only if UE needs to receive information that is not possible to receive using user plane markings on the radio interface. For instance, it is typically performed only for GFB flows or when a QoS modification is required for a non-GFB flow.

NOTE: It is up to RAN groups to define QoS framework in radio access.

6. The AN acknowledges QoS enforcement operation to CP functions by sending a [NG2] Authorised QoS Ack message to CP functions. This message exists if step 4 was performed earlier.

7. The UP functions acknowledge QoS enforcement operation to CP functions by sending a [NG4] Authorised QoS Ack message to CP functions.

Depicted in Figure 6.2.2.2-2 is a call flow describing U-plane QoS aspects.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 117 of 501

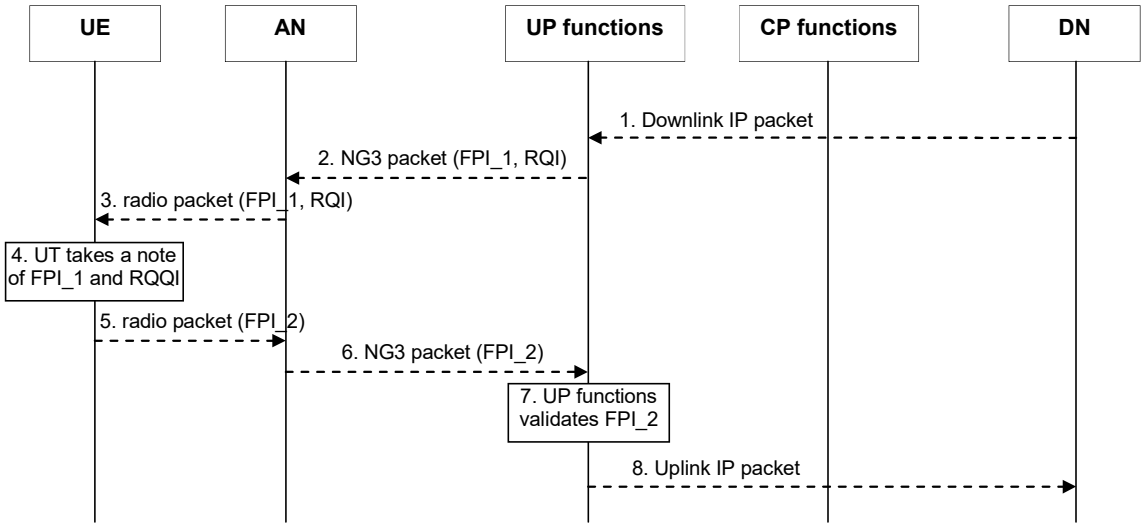


Figure 6.2.2.2-2: Flow based QoS architecture: User plane aspects

1. UP functions receive a downlink IP packet.

2. Based on the information configured using NG4 signalling as described in Figure 6.2.2.2-2, the UP functions determines the FPI (FPI_1 in the figure) to apply as packet marking over NG3. The packet marking is used in the NG3 encapsulation header, and possibly as transport-layer marking. If the UP functions determines that reflective QoS should be used for corresponding uplink traffic, it includes the RQI in the packet marking.

3. Upon reception of the NG3 packet the AN uses the FPI marking to determine the packet handling on the radio interface. If the UE has no corresponding "radio bearer" for FPI_1, the AN implicitly initiates a new "radio bearer" for FPI_1. If RQI was included in the NG3 packet, the AN replicates it in the radio header of the downlink radio packet. The AN also includes FPI_1 in the downlink radio packet e.g. to assist the UE in determining QoS for corresponding uplink traffic in case of reflective QoS or towards a Remote UE in case the UE acts as a Relay UE.

4. Upon reception of the radio packet UE take a note of the received information (FPI and/or RQI). If RQI was present in the downlink, it handles all corresponding uplink flows with the same FPI (i.e. FPI_1). Given that the QoS handling of this flow was initiated by the network, FPI_1 does not need to be part of the "pre-authorised FPI set".

5. An application client in the UE provides an uplink packet for transmission to the lower layers. Based on internal configuration the UE maps the uplink packet into one of the pre-authorised FPIs (FPI_2 in the figure) and proceeds with transmission in the uplink, as defined by RAN specifications. If the UE currently has no corresponding "radio bearer" for FPI_2, the UE initiates a new "radio bearer" for FPI_2 using in-band means. The UE includes the selected FPI (FPI_2) in the radio packet header.

6. Upon reception of the radio packet the RAN verifies whether FPI_2 is part of the "pre-authorised FPI set". In the affirmative case the RAN copies the received FPI in the NG3 encapsulation header, and possibly uses FPI_2 to determine any transport-layer marking over NG3. Otherwise the RAN discards the packet.

Editor's note: It is FFS whether in emergency situation UE should be allowed to initiate a flow with an FPI that is not part of the "pre-authorized FPI set" and how this is handled by the system.

7. Upon reception of the NG3 packet the UP functions performs validation of the FPI (FPI_2). If the UP functions determines that the flow initiated by the UE requires a different QoS than the one selected by the UE, the UP functions performs a QoS modification.

Editor's note: It is FFS whether the corrective action consists in silent packet discard or whether UP functions uses C-plane QoS signaling or U-plane markings to instruct the UE to switch to a different QoS.

8. UP functions forwards the uplink IP packet towards the data network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 118 of 501

6.2.2.3 Solution evaluation

The solution has the following properties:

- NG2 signalling is not needed to support initiation or termination of non-GFB flows. NG2 signalling can exceptionally be used for non-GFB flows e.g. when the network wants to perform QoS modification, or when the networks wants to override the default PDB associated with the FPI with an explicitly signalled PDB.
- NG1 signalling is not needed to support initiation or termination of non-GFB flows. AS signalling can exceptionally be used for non-GFB flows e.g. when the network wants to perform QoS modification.
- UE can initiate a new flow with one of the pre-authorised FPIs without using C-plane signalling.

Editor's note: The RAN dependencies in this evaluation need to be confirmed by the RAN groups.

6.2.3 Solution 2.3: Content Aware QoS Framework

6.2.3.1 Overview

This is a solution to Key issue 2: QoS framework.

NOTE: CN means Core Network; CP means Control Plane; UP means User Plane

The solution is based on following principles:

1. The CN (CP) is able to send to the RAN via CP signalling:

- Transport level rules (explicit QoS targets) associating a service data flow (e.g. IP flows in case of PDU sessions carrying IP traffic) with a set of transport level parameters (priority, delay, jitter, packet loss, etc.)
- but also more advanced rules containing higher level ("Quality of Experience" related) QoS parameters: "Intent level" QoS rules.

NOTE 1: The solution assumes that the AN is able to access to the header (e.g. IP & transport headers) of the PDU carried between the UE and NG-Gi.

NOTE 2: The transfer via signalling of QoS rules from the Core to the AN may not apply to all AN types.

2. No usage of bearers: bearers are used neither in the Core nor on the Core to AN interface.

NOTE 3: Whether bearers are used over the radio interface used for QoS differentiation is totally transparent for the solution and totally under the scope of RAN WG

3. DL packet marking in the User Plane from the Core to the RAN.
4. Different types of flows are envisioned. Flows (e.g. Guaranteed flow bit rate for Voice, strict packet delay budget requirement and strict enforcement based on such characteristics) that are associated with Transport level QoS policies from the Core (explicit QoS targets are applied). Other flows are associated with Intent level policies from the Core. Different Packet marking values set by the Core help differentiate the behaviors for the 2 types of flows.
5. QoS policies (transport level or explicit QoS targets, intent level QoS policies) are signalled to the RAN and UP function during PDU session establishment. No NG1, NG2, NG4 signaling expected on a per flow basis especially for non-GBR flows.
6. For services that require guaranteed bitrates, the CN-CP can request RAN for specific QoS treatment and it is subject to admission control in the RAN.
7. Network can signal the guaranteed bit rate information, maximum bit rate and per session bit rate information to the UE.
8. For operator offered services (e.g. IMS based services), it is assumed that multiple media type (voice, video, picture transfer, file transfer etc) running over IMS can be multiplexed within a single PDU session. QoS differentiation for various media types will be taken care of based on the principles mentioned above.

Editor's note: Applicability of this solution for non-3GPP AN is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 119 of 501

Principles 2 and 3 are common with the solution in sub-clause 6.2.2.

6.2.3.2 Architecture description

The Figure 6.2.3.2-1 represents a QoS architecture that is used to describe the proposed QoS framework.

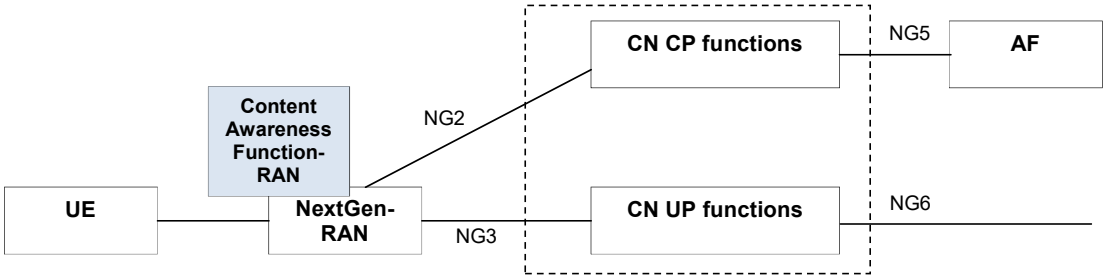


Figure 6.2.3.2-1: Content Aware QoS architecture

The architecture is mostly the same as in solution 2.2 with following differences:

1. NG2 may carry QoS rules (explicit QoS targets and Intent level QoS).
2. The NextGen-RAN contains a Content Awareness Function in the RAN (CAF-RAN). The role of the CAF-RAN is detailed below. CAF-RAN contains both CP and UP functions. The potential split between CAF-RAN CP and UP is considered out of scope of SA2

Editor's note: This solution has dependency on RAN WGs. Decision to support CAF-RAN within RAN belongs to RAN WGs.

3. No interface between the UE and the CN CP functions for the CN CP functions to configure QoS handling in the UE
4. The packet marking used in solution 2.3 does not carry itself information on the QoS to apply in the RAN. Information on the QoS policies to apply in the RAN is provided by the QoS rules provided by the CN CP to the RAN that refer to this packet marking.
5. The packet marking sent by the core may not map one to one to DRBs within the RAN. This is under the scope of RAN WGs. The following figure illustrates how the flows might map end to end when multiple DRBs are supported for QoS differentiation (e.g. for operator offered services):

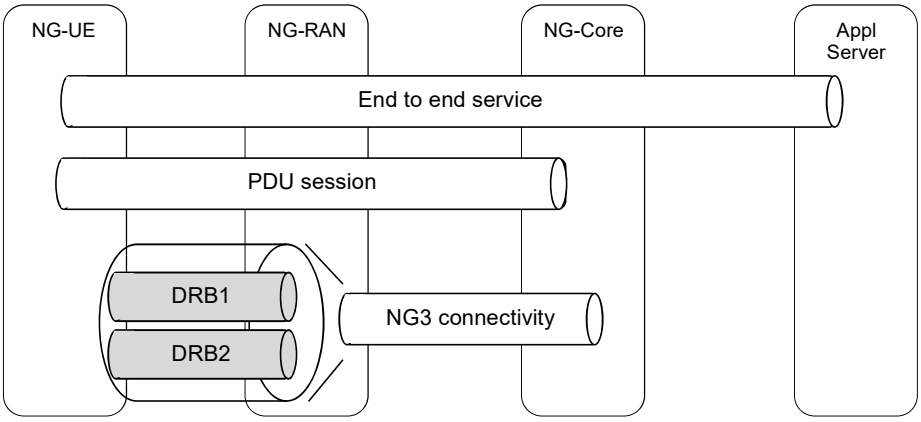


Figure 6.2.3.2-2: User plane connectivity for QoS framework

CN UP functions

As in solution 6.2.2, the CN UP functions are able to

- Receive QoS & charging rules from the CN CP. These rules target service data flows

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 120 of 501

- Detect applications
- Carry out charging actions (CDR, on-line charging) based on the rules received from the CN CP
- Mark DL UP traffic sent to the (CAF-)RAN based on rules received from the CN CP. This marking is called FII (Flow Identification Indicator). The FII marking is not meant to directly control the QoS behaviour in the RAN: the QoS behaviour in the RAN is controlled by QoS rules that may refer to FII and that are sent by the CN CP to the CAF-RAN.
- Enforce DL and UL per Session Bitrate i.e. it limits the aggregate bitrate that can be expected to be provided across all PDU sessions of the same APN (e.g. excess traffic may get discarded).
- enforce Maximum Flow Bit rate, Guaranteed Flow Bit rate. The Guaranteed flow bit rate denotes the bit rate that can be expected to be provided for a certain flow. The maximum flow bit rate limits the bit rate that can be expected to be provided by a flow (e.g. excess traffic may get discarded by a rate shaping function).
- the ARP can be used by the CN UP function to decide which flows to pre-empt during exceptional resource limitation within the CN (e.g. congestion situation).

RAN functions including Content Awareness function in the RAN (CAF-RAN):

- Enforce QoS guaranteed flow bitrate and maximum bitrate authorized for the session
- enforce per UE Maximum bit rate for the UL and DL.
- the ARP can be used by the RAN to decide which flows to drop during exceptional resource limitations within the RAN (e.g. at handover).

CAF-RAN:

- Receives QoS rules from the CN CP over NG2. These rules may target any combination of (FII (UP flow marking by CN UP), service data flows (PDU session flows))
- QoS rules sent to CAF-RAN use FII to identify the targeted traffic. This allows the CN CP to ensure coherency between charging decisions (and potential application detection) from the Core and QoS enforcement in the RAN
- QoS rules related with a flow descriptor may be sent to CAF-RAN while no corresponding traffic is currently exchanged between the UE and the network.
- Is made aware of the PDU session type (IP, Ethernet, Unstructured) by the CN CP.

NOTE: This is needed for the CAF-RAN to be able to filter traffic based on PDU session flows

- Transforms higher level QoS rules received from the CN CP into transport level QoS rules. This transformation is implementation-specific (i.e. will not be standardized) and may be dynamic and it takes into account the current radio load (in the cell(s) used to exchange UP traffic with the UE) and the radio quality for the UE
- This transformation may take into account the user plane traffic mix, simultaneous competing flows and network status and resource availability.
- Can Shape DL and UL traffic. DL traffic shaping helps controlling the flow of UL traffic.
- For services that require guaranteed bitrates for a certain flow, RAN performs admission control when CN-CP requests for specific QoS treatment,

Co-ordination between CN UP and CAF-RAN:

The CN UP provides packet marking (FII) based on the rules received from the CN CP. The traffic shaping and policy enforcement in the CAF-RAN is bound by Intent level -QoS rules received from the CN CP that may refer to this marking. The CN CP is responsible of ensuring the coherency between any application detection (and related charging data collection) in the CN UP and QoS rules sent to the CAF-RAN. This ensures that the CN UP and CAF - RAN are working in coordinated manner: the CAF-RAN is bound by the charging and detection performed in the core but is responsible of providing an appropriate QoS to the flows marked by the Core (FII). FII sent by the core may not map one to one with the radio bearers in the RAN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 121 of 501

CN CP function:

QoS rules are determined at the CN CP functions. They are transferred to the CAF-RAN and to the CN UP functions, at least at PDU session establishment. It can signal Maximum Flow Bit rate, Guaranteed Flow Bit rate, per Session Bit rate to the UE for enforcement of uplink flows.

Policy provisioning and enforcement:

Operator provisions subscriber and application specific QoS policies in the CN CP functions. The CN CP functions in the Core provide the rules to the CAF-RAN and CN UP functions.

Charging:

Traffic charging support (CDR, granted quota for on-line) is performed in the CN UP function based on the rules received from CN CP. When the CN UP function reports charging related information associated with traffic it provides the corresponding FII.,

NOTE: When charging requires precise knowledge of the exact QoS applied to some traffic, this traffic should only be associated with Transport QoS policies.

The following reference points are assumed for the purpose of describing the QoS framework:

NG2: Reference point between the RAN and CN CP functions.

NG5: Reference point between the CN CP functions and an Application Function (AF).

NG4: Reference point between the CN CP functions and CN UP functions.

NG3: Reference point between the RAN and CN UP functions.

NR-Uu: Reference point between the UE and the NextGen-RAN.

6.2.3.3 QoS related information exchanged between network functions

FII: Flow Identification Indicator: Traffic Mark set by the CN UP on DL UP traffic sent to the (CAF-)RAN. This marking is based on rules received from the CN CP and may e.g. identify traffic of applications detected by the CN UP function and/or traffic subject of a specific charging. The FII marking is not meant to directly control the QoS behaviour in the RAN: the QoS behaviour in the RAN is controlled by QoS rules that may refer to FII and that are sent by the CN CP to the CAF-RAN. The FII is used on NG3 on a per-packet basis. Traffic from 2 UE may be associated with the same FII.

NOTE1: Based on the output of application detection enforced in the CN UP functions, different PDU within the same flow (e.g. with the same 5 Tuple in case of a PDU session for IP traffic) may be associated by the CN UP with different FII values. This may not be possible in case of ciphered traffic. This assumes the transport protocol handles different streams for this kind of traffic.

The following table illustrates the classification for FII values:

Table 6.2.3.3-1: Packet marking value classification

Core – RAN User plane packet marking (FII) value	Semantics
1…m	Pointer to the explicit QoS targets signalled over NG2 or explicit QoS targets that are standardized.
m+1 …n	Pointer to the intent level QoS policies signalled over NG2.

Rules sent from CN CP to CAF-RAN:

A QoS rule sent by the CN CP to the CAF-RAN contains:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 122 of 501

- Flow descriptor: Information to identify the target UP flow (equivalent concept to SDF descriptor in PCC)
- A QoS precedence rule to determine which QoS rule to apply when a PDU would match multiple QoS rules. The precedence applies only within a PDU session i.e. traffic detection takes place within the flow of a PDU session.
- Target QoS information; this may correspond to a "explicitQoS targets " level or to a set of higher level rules ("Intent" level). A given QoS rule corresponds to one single level: either "explicit QoS targets" level or "higher" level.
  - Delivery Characteristics: Packet Delay Budget
  - Delivery Characteristics: Packet Error rate.
  - Priority Level: Refers to flow priority (i.e. between a class of applications).
  - QoE Level: Refers to priority within the same flow type (i.e. within the same class of application)
- Guaranteed Flow Bit rate: UL and DL bitrate value applicable for a single flow or aggregation of flows. It indicates guaranteed bitrate authorized for the data flow identified by a flow descriptor.
- Maximum Flow Bit rate: UL and DL bitrate value applicable for a single flow or aggregation of flows. It indicates maximum bitrate authorized for the data flow identified by a flow descriptor. for enforcement in the RAN
- Allocation and Retention Priority: The Allocation and Retention Priority for the service data flow consisting of priority level, pre-emption capability and pre-emption vulnerability.
- Per UE Maximum bit rate: This refers to the maximum bit rate that should be enforced for a certain UE in UL and DL.

NOTE: it is expected that the source for the QoS policies (e.g. for operator offered services) are defined as part of the policy framework Key Issue.

The target UP flow of a QoS rule sent to CAF-RAN may be identified by any combination of (including also wildcarding):

- FII (packet marking from CN UP)
- Flow descriptor (e.g. a 5 Tuple in case of a PDU session of IP PDU session type and this can apply to both UL and DL)

The CN CP may send following level of rules (different level of Target QoS information) to the CAF- RAN:

- Transport QoS level rules providing Explicit QoS targets (priority, packet delay budget, jitter, packet loss, etc.).
- Intent level QoS rules providing abstract QoS target.

When the CN CP function provides Intent level QoS policies for a certain FII, Explicit QoS targets are not provided. Similarly, when the CN CP function provides Explicit QoS targets for a certain FII, intent level QoS policies are not provided.

An Intent level rule associates a (Radio) Load and quality level with a QoE level.

- Load and Quality Levels may correspond to: "High", "medium", "low".
- Flow priority.
- QoE levels may correspond to:
- "High", "medium", "low" or to
- abstract rules . e.g. Voice type QoS, Smoothed Bit rate QoS (limit the bandwidth variation for the traffic), bulk traffic (traffic may be discarded when the radio conditions are bad or the cell too loaded), etc.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 123 of 501

QoE level may be applied for classification within a certain application (e.g. based on subscription level) and Flow priority may be applied for classification amongst different applications (i.e. applications that can be determined as different by the network). The intent level policies are translated by RAN to explicit QoS targets such as packet delay budget.

NOTE2: The translation from Intent QoS rules to explicit QoS targets (Transport QoS rules) in RAN is implementation specific , i.e. the translation from different vendors may not lead to exactly the same result. Thus when subscription requires precise knowledge of the exact QoS applied to some traffic (e.g. to ensure that the same transport QoS is applied across different RANs in multi RAN vendor deployments), this traffic should only be associated with explicit QoS targets (Transport QoS rules).

NOTE3: CAF-RAN applies Intent level rules for an UP flow only if the Core allows it:

- Intent level QoS rules sent to the RAN are associated with FII marks by CN CP plane (e.g. for certain FII values, CAF-RAN is not allowed to apply intent level rules)
- Thus CAF-RAN may apply Intent level QoS on a PDU session flow only when the CN UP has sent DL traffic of this PDU session flow with the corresponding FII marking.

CAF-RAN is responsible to locally map Intent level QoS rules into explicit QoS targets (Transport QoS level rules) based on

- Static information: local CAF-RAN policies and
- Dynamic information: local (radio) conditions (current context of the user plane traffic mix, simultaneous competing flows and network status and resource availability),
- bound by the upper limits of intent level QoS rules (QoE level).

The mapping from an Intent level rule to explicit QoS targets (Transport QoS level parameters) is implementation-specific and can be controlled by local operator policies.

At Hand-Over from source RAN to target RAN, the source RAN provides the target RAN with

- The QoS policies receivd from the CN CP i.e. transport QoS rules providing Explicit QoS targets and Intent QoS rules for the UE (information independent of the current PDU session flows of the UE)
- but also with the derived transport QoS rules currently applying to the PDU session flows of the UE (information sent only for the on-going PDU session flows of the UE)

In case of Home Routing type of roaming for a PDU session (where the PDU session anchor lies in the Home network), the CN CP QoS policies that target the CAF-RAN come from the CN CP entities of the Home network and are likely to contain only Transport level policies. They may nevertheless contain Intent level policies based on specific roaming agreements (e.g. between operators belonging having signed specific roaming agreements).

Rules sent from CN CP to CN UP:

A QoS & charging rule sent from CN CP to CN UP

- Targets a service data flow (Flow descriptor)
- Is associated with a precedence to determine which rule to apply when a PDU would match multiple rules. The precedence applies only within a PDU session i.e. traffic detection takes place within the flow of a PDU session.
- Identifies the charging related information (out of scope of this solution)
- Identifies the FII tagging to be used to send the corresponding traffic downstream. This is intended for the CAF-RAN
- Corresponds to a transport level QoS rule
- Transport QoS level rules providing Explicit QoS targets (priority, delay, jitter, packet loss, etc.)
- Per Session bit rate.
- Guaranteed flow bit rate,

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 124 of 501

- Maximum Flow Bit rate
- Allocation and Retention Priority

Support of UL QoS:

In order to support proper UL QoS,

this solution relies on support of reflective QoS (similar solution to the one described in 23.139) i.e. on in-band marking of the traffic called Flow Priority Level (FPL) and rules for mapping UL flows to a certain DRB.

If the Flow Priority Level (FPL) is sent to the UE, then it is determined by the RAN based on explicit QoS targets and based on the FII. RAN also determines how the different values (within the same or different flow) of FII values map to FPL values. When FII maps to intent level policies and RAN is congested, based on local policies, RAN may need to adjust the explicit QoS targets (Transport QoS level parameters) and this may also impact the FPL values (i.e. be different from the FPL values used prior to congestion) sent on in-band marking.

Editor's note: Whether Flow Priority Level (FPL) is sent to the UE and the FPL value sent to the UE is determined by RAN2.

FPL is different from the FII . The UE may use the downlink FPL to determine QoS for the corresponding uplink traffic, and the UE may also use it to determine the QoS on the link towards a Remote UE when the UE is acting as a UE-to-Network Relay.

In addition, network can provide UE with the default QoS policies (e.g. during PDU session establishment) that the UE can use to initiate new flows in the uplink. The default QoS policies may include rules for mapping UL flows to a certain DRB and/or default packet marking value (FPL) for UL flows identified by a certain flow descriptor (5-tuples) and this is provided by the RAN to the UE. This is subject to validation by the network (i.e. validation by RAN for FPL values and CN UP for FII values).

NOTE4: Reflective QoS allows to cope with OTT applications that make a heavy usage of short lived IP flows.

NOTE5: This FPL is similar to the bearer Priority sent by E-UTRAN to UE over RRC (that is different from QCI)

NOTE6: The final decision on this aspect is to be taken together with RAN groups.

6.2.3.4 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

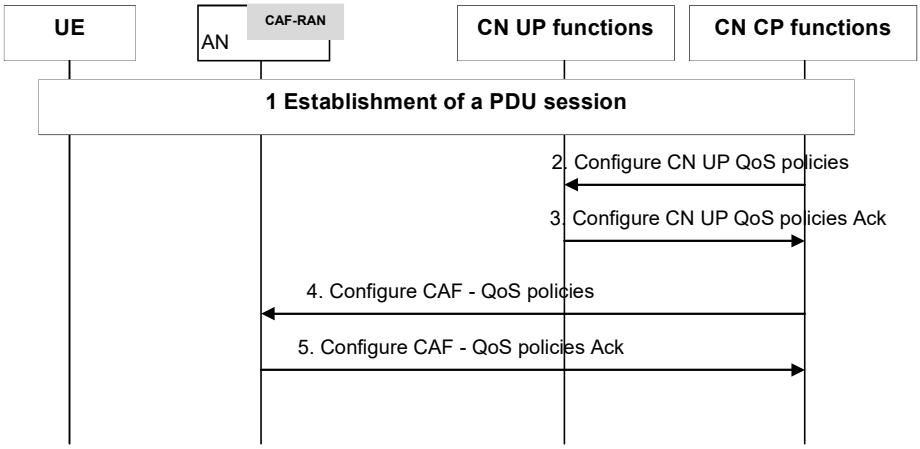


Figure 6.2.3.4-1

1. A PDU session for user plane traffic is established between the UE and a data network. The PDU session carries all user plane traffic regardless of the QoS characteristics of individual traffic flows.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 125 of 501

2,3. The CN CP functions signals QoS rules to the CN UP Functions. These rules are defined in § 6.2.3.3. They may refer to application detection and to FII marking to be set by the CN UP. The CN UP acknowledge (s) the rules received from the CN CP

4,5. The CN CP functions signals QoS rules to the CAF-RAN. These rules are defined in § 6.2.3.3. They may refer to FII marking received from the Core. The CAF-RAN acknowledges the rules received from the CN CP

NOTE 2: It is up to the RAN groups to define QoS framework in radio access.

CN CP functions may provide QoS policies for future use even when there are no current active flows associated with the Flow Descriptors of these QoS policies.

6.2.3.5 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.2.4 Solution 2.4: QoS model for QoS Authorization and Request

6.2.4.1 Architecture description

Editor's note: This clause will contain e.g., terminology, overview, architecture description of the solution.

6.2.4.1.1 Functional Architecture

The functional architecture of solution 2.2 is assumed.

6.2.4.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.2.4.2.1 QoS Pre-Authorization at PDU Session Establishment

Traditionally in EPC, and in solutions 2.1 and 2.2, data flows that require a specific QoS treatment have the QoS authorized by the network based on interaction with an AF.

In certain scenarios, when the UE establishes a PDU session towards a Data Network, the network may have policies associated to the UE subscription profile that indicate that certain data flows are pre-authorized to obtain a specific level of QoS. This may be based e.g. on specific applications in the UE.

This solution proposes that, when QoS is established (e.g. at PDU session establishment, as in the case of solution 2.1 in 6.2.1.2.1), the CP Function performing QoS decisions provides to the UP function (UP-GW(s)) and to the AN the Authorized QoS (per solution 2.1) or the QoS Policy (per solution 2.2) containing pre-authorized QoS information for specific IP flows. The same QoS information is also provided to the UE. Such pre-authorized QoS information applies to data flows for which no explicit QoS establishment is requested either by the AF or the UE.

When the UE establishes a data flow for which QoS and sends traffic over the AN, the UE uses best-effort transport over the AN. The AN, detecting that the UE is generating traffic corresponding to a data flow for which a specific level of QoS is pre-authorized performs AN specific actions to establish the resources required to provide such QoS and provides the UE with the information about the resources (e.g. radio bearers in case of a RAN with dedicated bearers). As an example, a RAN for which dedicated bearers are supported may establish a new dedicated bearer the data flow, or may re-use an existing dedicated bearer, inform the UE of what bearer should be used for the uplink traffic belonging to the flow, and use the dedicated resources to deliver corresponding downlink traffic.

If the UE receives from the AN QoS information for a data flow that do not match what the CN provided, the UE uses the information from the AN.

6.2.4.2.2 QoS Establishment

In addition to solutions 2.1 and 2.2, this solution proposes two additional alternatives for QoS authorization:

- Explicit UE requested QoS over NG1: the UE can trigger the establishment of QoS for data flows In reference to solution 2.1 in section 6.2.1.2.2, and solution 2.2 in section 6.2.2.2, instead of the AF triggering the establishment of QoS for data flows that require specific treatment in the network, the UE performs the triggering.When an application in the UE requires specific treatment of data flows, either the application requests

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 126 of 501

to the lower layer a specific level of QoS and provides the data flow descriptor, or the UE may be configured with policies (e.g. provided by the HPLMN or preconfigured in the UE) to associate the application request for transporting data with a specific QoS level. The UE then sends a request to the CP Functions containing the data flow descriptors and the level(s) of required QoS. The UE may send the QoS request before the establishment of the application session.

- Implicit QoS setup: the UE generates data flow(s) traffic for the application session and transmits the traffic using best-effort transport over the AN. The AN forwards the traffic toward the CN-UP function and uses best effort transport. The CN-UP function detects unclassified uplink data flow(s) and reports it to the CN-CP function providing the data flow(s) descriptor(s). To support such scenario, it is assumed that when the UE establishes a PDU session, the CP-CN function indicates to the UE whether implicit QoS setup is supported for the PDU session.

- Explicit UE requested QoS in user plane:

- Dynamic binding of QoS rule:For the pre-authorized QoS without traffic classifier, dynamic binding of downlink traffic to the pre-authorized QoS Flow can be performed by either by an NAS signalling (as described in the step 3a) or by uplink marking (as described in the step 3c) so that the network is able to perform accounting for the informed traffic classifier.

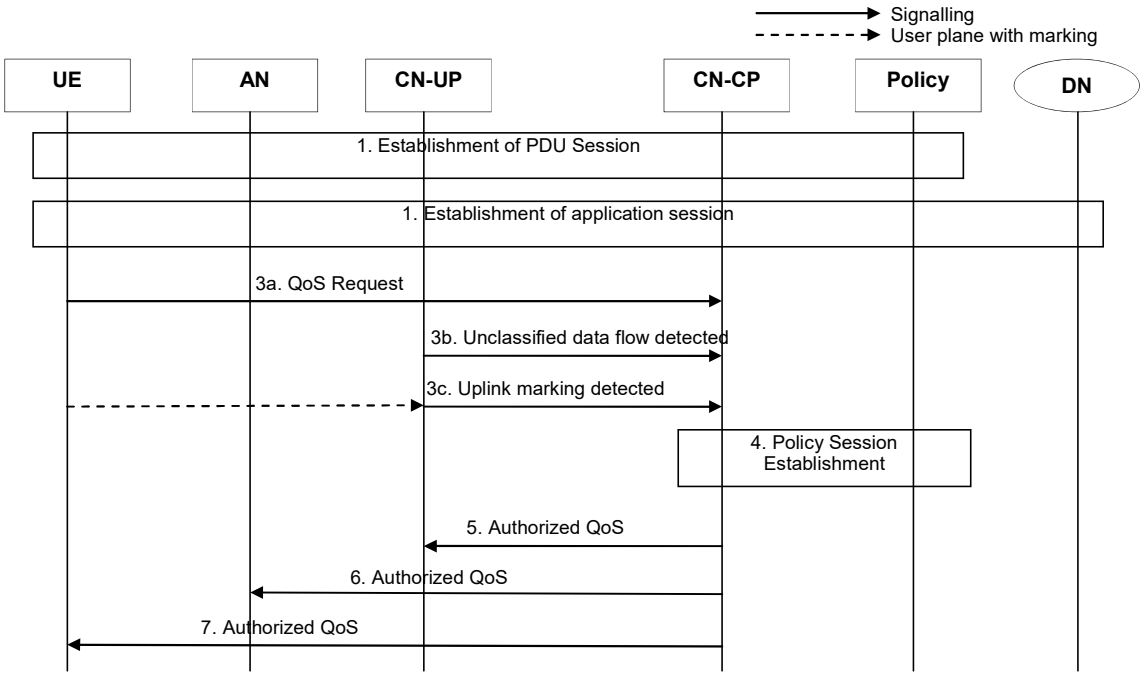


Figure 6.2.4.2.2-1: UE Requested QoS

1. The UE attaches to the network and a PDU session between the UE and a data network is requested.

2. The UE may establish an application session with a server in the Data Network. If the UE want to use the pre-authorized QoS which has been established without traffic classifier, it triggers the QoS establishment procedure explicitly to inform the network of the traffic classifier information so that the network is able to perform accounting for the informed traffic classifier.

NOTE: Step 2 may take place after step 3a.

3. Qos establishment is triggered. Either:

   3a. The UE determines that the data flow(s) for the application require QoS and the UE sends an explicit QoS Request to the CN-CP providing QoS requirements for a specific (set of) data flow(s); or

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 127 of 501

3b. Upon detecting unclassified uplink data flow(s) belonging to one of the rules provided by the policy function, the CN-UP function may report it to the CN-CP function providing the data flow(s) descriptor(s).

3c. The UE marks the uplink traffic with a specific indication to inform to the network that the traffic corresponds to a new flow. Only for uplink traffic marked by the UE the CN-UP reports the traffic to the CN-CP function. The CN-CP function provides the data flow(s) descriptor(s) for the uplink traffic and the corresponding downlink traffic if the traffic flow is authorized.

Editor's note: what mechanisms can be used to avoid excessive signalling between the CN-UP and the CN-CP due to unwarranted unclassified flow detections are FFS.

Editor's note: how the UE can mark the packets in step 3c and what type of marking is used (e.g. identify the type of flow or only indicate it is a new flow) is FFS.

4. The CN-CP function establishes a session towards the Policy function, invokes the authorization of QoS for the data flow(s), and receives the Authorized QoS for (each) data flow.

5. The CN-CP function forwards the Authorized QoS to CN-UP.

6. The CN-CP function may forward the Authorized QoS to AN. The AN acknowledges the reception and confirms that the Authorized QoS can be fulfilled to the CN-CP. The AN establishes the AN resources required to provide the QoS and may interact with the UE to establish the resources. As an example, a RAN for which dedicated bearers are supported may establish new dedicated bearer(s) for the data flow(s), or may re-use existing dedicated bearer(s), informs the UE of what dedicated resources should be used for the uplink traffic, and uses the dedicated resources to deliver corresponding downlink traffic.

7. The CN-CP function forwards the Authorized QoS to the UE for classification and for information and possible actions such as rate control. The UE stops the UL marking described in step 3c, if step 3c has been performed by the UE.

In addition or as alternative to step 7, if the UE has requested QoS establishment in user plane as in step 3c, the CN-CP function requests the CN-UP function to inform UE with explicit response signal in user plane. Upon receiving the corresponding downlink packets, the CN-UP marks some PDUs with a specific indication in PDUs' encapsulation header in order to reliably inform the UE that the UE's request has been received. When the downlink packet with the indication comes to the UE, it stops the UL marking described in step 3c.

6.2.5 Solution 2.5: QoS model for flexible traffic differentiation

6.2.5.1 Architecture description

Editor's note: This clause will contain e.g., terminology, overview, architecture description of the solution.

6.2.5.1.1 Functional Architecture

The functional architecture of other QoS solutions is assumed.

6.2.5.1.2 Applications Requirements Input

Other solutions for key issue #2 on QoS defines a set of application requirement inputs provided by an AF to the CP Function for QoS, and define how the QoS authorization based on application requirements takes place.

In addition to what is proposed already, this solution proposes that the AF provides to the CP Functions also an indication of whether different packets within a data flow require differentiated treatment. E.g., for a data flow, the AF may provide two levels of QoS requirements with respect to other solutions .

6.2.5.1.3 Packet Markings for Traffic Differentiation

A new packet marking that conveys in-band information related to the data flow features (including information describing packet characteristics above layer 4) is introduced in order to enable easier traffic differentiation when traffic cannot be easily detected (e.g. for encrypted traffic) and to enable differentiated treatment of different packets belonging to the same data flow (e.g. packets that have different characteristics at level 5 and above and that require different treatment).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 128 of 501

Editor's note: if packetization of data traffic in an application server includes e.g. high priority traffic and low priority traffic in the same packet, it is FFS whether it is possible to provide differentiated treatment for such traffic.

Editor's note: it is FFS to what media types the solution applies.

Upon definition of the QoS Policy or Authorized QoS in solutions 2.1 and 2.2 in collaboration with the AF (i.e. selection of QoS parameters defining the QoS for a data flow according to the QoS solution and the related parameters), the CP Function also generates a *Packet Marking Token* associated with the IP traffic.

The Packet Marking Token is proposed for media types where the traffic is encrypted and traffic differentiation information at L4 and above are not visible to the NextGen CN entities that perform traffic detection and classification. The proposed packet marking enables identification of the specific traffic in the packet by mapping the Packet Market Token directly to the QoS flow the data packet belongs to. The Packet Marking Token enables mapping a packet to:

- the corresponding QoS identifier (e.g. FPI, FII, QoS ID of other solutions) and a PDPI value, if a QoS flow is defined in terms of packets whose QoS treatment differ based on the PDPI
- the corresponding QoS identifiers (e.g. FPI, FII, QoS ID of other solutions) of the QoS flow, if an explicit PDPI value is not associated to a data flow but identified directly by the QoS identifier.

In addition, a *Packet Set Marking* is added by the entity sourcing the data traffic.

The solution is based on:

- The presence of an AF that supports this packet marking solution and that interacts with the NextGen CN over NG5 to establish the QoS and packet treatment for the traffic
- The AF marking packets with the proposed Packet Marking Token over the NG6 interface.

Editor's note: it is FFS how the Packet Marking Token and the Packet Set Marking are carried over NG6. E.g. for IPv6, extension headers can be used.

- The UP-GW that terminates NG6 receives the packet and, based on the Packet Marking Token, identifies the QoS flow the packet corresponds to and the associated QoS policy and packet treatment. The UP-GW marks the packet towards the AN with mechanisms defined in other solutions(e.g. a QoS identifier like an FII or QoS ID, and a PDPI value if supported) based on the associated QoS policy, and with the Packet Set Marking value received over NG6.
- The marking performed by the UP-GW is carried to the RAN which can enforce QoS as defined in other solutions.

The Packet Marking Token is defined and used as follows:

- Upon definition of the QoS Policy in other solutions in collaboration with the AF (QoS Policy then distributed to the UP function(s) over NG4 and to the AN over NG2), the CP Function also generates downlink Packet Marking Token(s) associated with the data traffic. This may include Packet Marking Tokens for potential future traffic exchanged by the UE and the AF.
- Each Packet Marking Token contains
- A Token ID, identifying the token and the corresponding QoS policy
- A Token Parameter Index (TPI) indicating which fields in a data flow header are used to compute the token hash
- A Token Hash, calculated using the fields in each packet of the data flow described by the TPI
- The Packet Marking Token is generated via a cryptographic hash with a key decided by the CP Function and provided to the entities that need to verify the token
- The Packet Marking Token is appended to each packet of a data flow over NG6. Verification of a Packet Marking Token appended to the packet enables the UP-GW enforcing QoS and performing traffic filtering to identify the QoS policy associated with the packet without the need for TFTs.

Editor's note: security aspects of this solution, e.g. how to securely generate, allocate, verify, and provision tokens to the UE will need to be studied by SA3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 129 of 501

- In the QoS Policy or Authorized QoS, the CP Function:

- for each data flow or specific set of packets in a data flow for which a downlink token has been generated, it provides to the UP-GW the Token ID, the information for token verification (e.g. the key used to generate the token), in addition to the remaining QoS information in the QoS policy.

- for each data flow or specific set of packets in a data flow for which a downlink token has been generated, it provides to the AF the downlink Packet Marking Token .

- Tokens are generated as follows:

- if for a data flow the AF provides a single requirement for packet treatment, e.g. flow descriptor/packet filter and the related QoS requirements, the CP Function generates a single downlink (DL) Packet Marking Token .

- if for a data flow the AF provides an indication that packets within the data flow require different QoS treatment, and the packets differentiation is at a layer above L3 and L4, and provides requirement for each required level of packet treatment, the CP Function generates a separate downlink Packet Marking Token for each different level of treatment. The CP Function indicates to the AF which Packet Marking Token shall be used for each different level of QoS treatment. When packets marked with the different Packet Marking Tokens corresponding to the different levels of treatment reach a the UP-GW, the correct QoS policy can be applied by verifying the token and using the token identifier to retrieve the QoS policy.

- For each packet received containing a Packet Marking Token, the UP-GW retrieves the information corresponding to the Token ID, and computes the hash of the fields in the packet identified by the TPI using the token verification key provided by the CP Function. If the token is verified, the UP-GW does not need to perform any further packet inspection and it applies the QoS policy associated with the token.

Editor's note: whether and how the solution works in the presence of middleboxes on NG6 is FFS and depends on how tokens are transported.

The *Packet Set Marking* is added in addition to the Packet Marking Token:

- in order to enable flexible and dynamic QoS for a block of packets in a data flows (e.g. a block of packets for a video streaming) or to enable dynamic modification of a block of packets within a data flow, each block of packets sourced at an application server is marked with Packet Set Marking that distinguishes a block of packets from the following one.

Editor's note: it is FFS if the Packet Set Marking is an additional marking wrt the Packet Marking Token, or if it is part of the Packet Marking Token, and depends on how the Packet Marking Token is encoded.

6.2.5.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.2.5.2.1 Dynamic QoS Modification

In order to enable the support of dynamic QoS modification for a data flow, e.g. temporarily, when the UE detects the need to modify dynamically the QoS treatment (e.g. priority) of a block of packets, the UE provides a request to the RAN indicating which data flow the request relates to, providing the Packet Set Marking to identify which specific packets the request relates to, and with an indication of the new requested priority. Though the specific of the indication shall be defined by RAN, from a NextGen system point of view if FPI is used as in solution 2.1, the UE requests an Override FPI value, whereas if FPI is not used as in solution 2.2 the UE may either provide the AN with the deadline for the delivery of the block of packets, or a value of downlink Packet Delay Budget (as defined in TS 23.203 [3] but applied to downlink).

Editor's note: how the UE indicates the modified priority is FFS and shall be defined by AN.

Editor's note: if the AN is in congested status, whether the UE can send this message to the AN is FFS.

In this solution it is also assumed that, when the CP Function provides the QoS Policy of the Authorized QoS to the AN, the CP Function also indicates based on the subscription profile, QoS request from the AF (and which AF is requiring the QoS), and local policies the data flows for which the UE is allowed to request a priority modification.

The AN, upon receiving the request to modify the priority, accepts or rejects such request based on local conditions and policies in addition to the information provided in the QoS Policy or Authorized QoS by the CP Function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 130 of 501

Editor's note: it is FFS if a similar mechanism should be defined for uplink traffic, e.g. when the UE acts as a streaming server.

6.2.6 Solution 2.6: QoS ID solution

6.2.6.1 Architecture description

Editor's note: This clause will contain e.g., terminology, overview, architecture description of the solution.

This solution addresses the working task #1,#2, #3 and #4 of key issue 2.

This solution is based on the following high-level principles.

1) A QoS ID is carried in encapsulation header of the data unit on NG3 and Uu to uniquely identify the QoS profile that this data unit is associated with. The QoS ID is not used to directly control the QoS behaviour in the RAN: the QoS behaviour in the RAN is controlled by QoS profile that is identified by the QoS ID and is sent by the CN CP to the RAN. The QoS ID can be set per flow or per aggregation of the flows. The QoS ID is allocated by CN CP and unique within the UE context. The usage of QoS ID is similar with the FII in solution 2.3.

2) No need TFT handling and packet detection in RAN.

3) The RAN provides the QoS ID and the radio link mapping rules to the UE via Uu.

4) For each QoS profile the CN CP provides the QoS ID and UL flow descriptor mapping rules or a reflective QoS indicator to the UE via NG1. The CN CP may provide a default QoS ID with wild card UL flow descriptor.

The following shows how this solution works in each working task of this key issue.

1. For WT#1: QoS parameters, i.e. how to describe the authorised treatment of the data traffic.

In this solution, it is assumed legacy QoS parameters/profile are used to describe the authorised treatment of the data traffic, such as QCI, ARP, GBR, UE/APN-AMBR, etc. However it is not excluded any new QoS parameter can be used.

2. For WT#2: How the application layer may request a specific treatment of the traffic

In this solution the applications in the UE or in the network can use the legacy mechanisms in EPS to request the change of the treatment of the traffic, for example the application in network can send the request message to the policy control function, the application in the UE can use NAS to send the request message to the network.

3. For WT#3: How to distribute the QoS parameters describing the authorised treatment of the data traffic

On NG1: QoS ID and the associated QoS profile may be sent to the UE. The QoS profile parameters include at least the UL flow descriptor or a reflective QoS indicator and at least the UL UE Max bit rate.

On NG2, QoS ID and the associated QoS profile are sent to RAN. It is RAN's decision how to associate this QoS ID with the radio link to the UE.

On NG4: QoS ID, associated QoS profile including the UL/DL flow descriptions are sent to the user plane function.

On the radio link: The mapping information between QoS ID and the associated radio link are sent to the UE.

4. For WT#4: How to associate the authorised QoS treatment to User Plane data traffic.

For UL traffic:

The UE maps the UL traffic to QoS ID according to the UL flow description or local configuration or reflective QoS mechanism and then further maps to radio link according the mapping information from RAN. The UE adds the QoS ID in encapsulation header of every UL PDU and sends the UL traffic over the associated radio link. The RAN performs UL traffic verification according to the radio link mapping information. As the QoS ID is unique in UE context the RAN finds the target PDU session according to the QoS ID and sends the UL traffic to the target User Plane function over NG3. The User Plane function in the Core may perform traffic verification according to the UL flow description.

For DL traffic:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 131 of 501

A PDU session level tunnel is used over NG3between the RAN and the User Plane function in the CN. The User Plane function adds the QoS ID in encapsulation header of every DL PDU according to the DL flow description and sends the DL traffic over NG3. The RAN finds the UE context and the associated QoS profile according to the PDU session level tunnel and the QoS ID in the DL PDU. The RAN sends the DL PDU over the radio link associated with the QoS ID to the UE.

NOTE 1: The impacts on RAN related interface should be studied in RAN group.

NOTE 2: The QoS profile referred by QoS ID may include GBR parameters. It is FFS whether there is need to support GBR.

6.2.6.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.2.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.2.7 Solution 2.7: QoS framework for resource management for Mission Critical Group Communications

6.2.7.1 Architecture Description

This solution addresses aspects of key issue 2 on a QoS framework with a partial solution for mission critical Group communication. It is intended to become part of the general NextGen solution for QoS handling. This solution is not presented as an alternative to other solutions but as a complement intended to work together with other solutions: e.g. no new QoS parameters are proposed, as the intention is to reuse of QoS parameters defined by solutions with which this solution will co-exist.

Figure 6.2.7.1-1 shows a general view of the architecture:

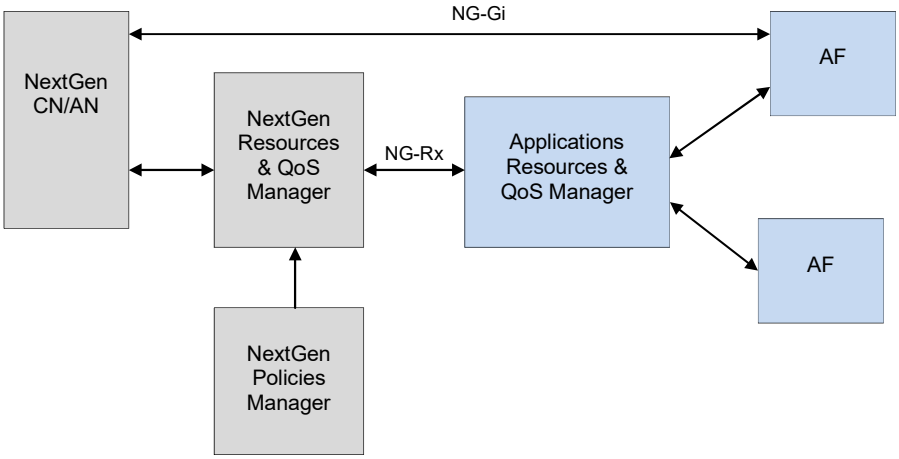


Figure 6.2.7.1-1: Flow based QoS architecture

NOTE: In this subclause, the Applications part is shown only for context and is not part of this NextGen proposed solution.

The following generic entities are defined:

- Application Function (AF) is located in the application domain. It communicates with the NextGen network directly via the NG-Gi interface (both CP and UP).
- Application Resources & QoS Manager (A-RQM)is located in the application domain and can handle all the AF, arbitrating their relative priority needs. It communicates with the NextGen system via NG-Rx interface which handles allocation requests

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 132 of 501

- NextGen Resources & QoS Manager (NG-RQM) is located in the NextGen system and can arbitrate between multiple ARQM, granting/revoking access to resources based on their availability (as reported by the NextGen CN/AN) and the operator's policy.
- NextGen Policy Manager stores and handles operator's policies with respect to access, QoS and possibly, charging.
- NextGen CN/AN is the actual traffic delivery network. This entity may provide periodic and on-demand snapshots of the current resource availability within the CN/AN to assist the NG-RQM with rapidly proceeding with allocations or deciding to reject request for resources.

6.2.7.2 Functional Description

Resources used in Group Communications for mission-critical services typically include network and radio bearers and associated QoS parameters and bandwidth. necessary for the setup and delivery of group calls. For example, a resource could be one of the GBR bearers that the network provides for a UE, and a request for resources will identify the UE/bearer combination the desired QoS (e.g. QCI) and bitrate. In case of group call, a set of bearers may have to be given to a set of UEs at the same time. The resources may be geographically distributed and potentially under the responsibility of different operators. The period of time needed to obtain the resources has to be bound and guaranteed, regardless of how many resources are being requested and where they are located. Multiple groups may be competing for the same resources at the same time, including at call setup and during the call, through dynamic call modification (e.g., emergency call, voice/video/data service modification) and in accordance with statically and dynamically configurable QoS/pre-emption/priority settings. The allocation requests for multiple resources to be used simultaneously need to fully succeed or fully fail, in which case no partial holding over of resources is acceptable. The ability for blocking/un-blocking (queuing) of resources is necessary, while enabling ways to recognize/resolve and/or prevent deadlock.

The resource management capabilities to be considered in the specification of architecture support for the Next Generation system include:

- Uniquely identify and bundle resources;
- Check the status of, reserve and release resources;
- Enqueue and dequeue requests for resources, respectful of priority order;
- Wait for resources to become available;
- Abort queued requests for resources (i.e. before they become available);
- Register and deregister interest of being notified when specific resources become available / busy;
- Transmit and receive notifications when specific resources become available / busy;
- Recognize, resolve and/or prevent deadlock when multiple resources are competed for by multiple parties.

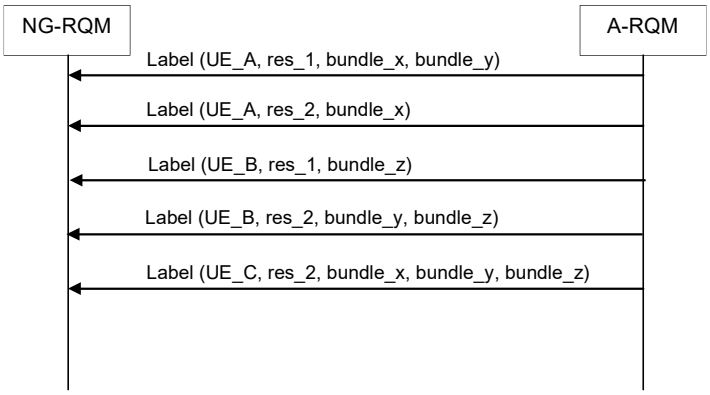


Figure 6.2.7.2-1: Example of resource bundling

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 133 of 501

In Figure 6.2.7.2-1, resources 1 and 2 of UE_A and resource_2 of UE_C are bundled together in bundle_x, resource_1 of UE_A, resource_2 of UE_B and resource_2 of UE_C are bundled in bundle_y and resource_1 and resource_2 of UE_B are bundled together with resource_2 of UE_C as part of bundle_z.

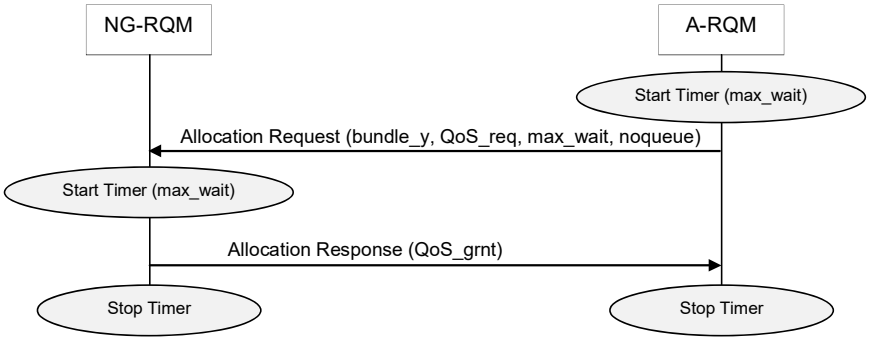


Figure 6.2.7.2-2: Example of successful multiple resource allocation

In Figure 6.2.7.2-2, all the resources associated with bundle_y are allocated with QoS_grnt within the allotted amount of time. QoS_grant can be different than QoS_req (if not satisfied, the A-RQM can release the entire bundle via a single message; not shown here).

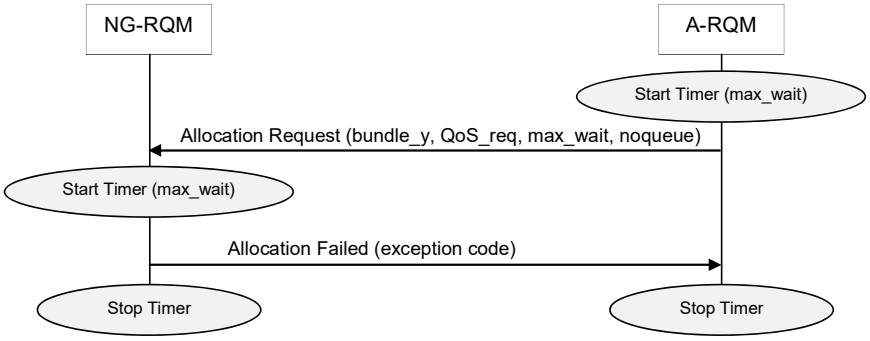


Figure 6.2.7.2-3: Example of successful multiple resource allocation

In Figure 6.2.7.2-3, none of the resources associated with bundle_y end up allocated via this request. The returned exception code provides the reason (e.g. at least one requested resource is busy/ not available).

6.2.7.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.2.8 Solution 2.8: Application-based uplink traffic identification

6.2.8.1 Solution Description

This solution addresses the working task#3 and #4 of key issue 2 on a QoS framework and is specific for the uplink traffic identification.

In this solution, the network may provide the UE the QoS policy together with application information when the PDU session is setup. The application information at least includes pair of OSId and OSAppId which can uniquely identify the application installed in the UE. For uplink traffic the UE identifies the application which generates the UL traffic and enforces the QoS Policy associated with the application information.

The User Plane Function in core network performs UL traffic verification by using application detection filters.

6.2.8.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 134 of 501

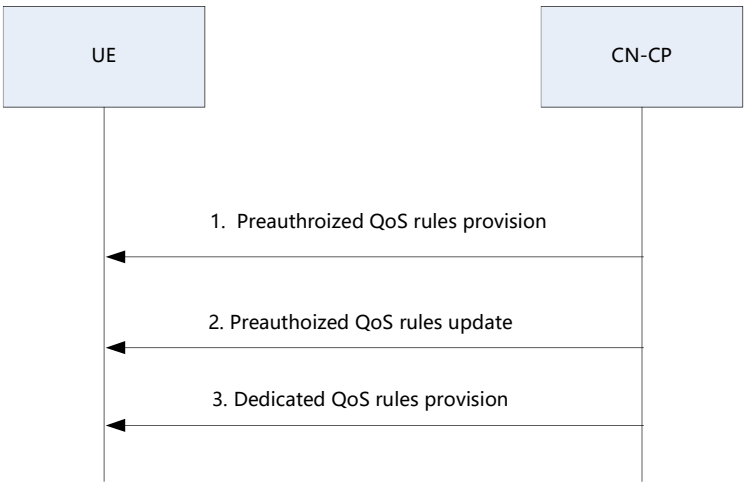


Figure 6.2.8.2-1 Application information provisioning

1. The CN-CP may provide the UE with the pre-authroized QoS rules. The pre-authorized rules include the application information and associated preauthorized QoS rules. The application information includes pairs of OSId and OSAppId which can uniquely identify the application installed in the UE. The UE uses this application information for UL traffic classification

2. The CN-CP may update the pre-authorized QoS rules in the UE.

3. The CN-CP may provide additional dedicated QoS rules including application information to the UE when the CN-UP detects an application which is subject with dedicated QoS control or the CN-CP receives dedicated QoS control request from application.

Editor's note : It is FFS whether the option in step 3 is needed or not.

Editor's note : How the CN-CP conveys the pre-authroized QoS rules to the UE is FFS. It could include e.g OMA-DM, or dedicated NAS signalling.

6.2.8.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.2.9 Solution 2.9: NextGen Bearer based QoS control model

This is a solution to Key issue 2: QoS framework.

6.2.9.1 Architecture description

The QoS control in the UP functions, AN and UE is based on the NextGen bearer (i.e. NextGen GBR bearer and NextGen Non-GBR bearer). See figure 6.2.9.1-1 for a high level view of such QoS control.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 135 of 501

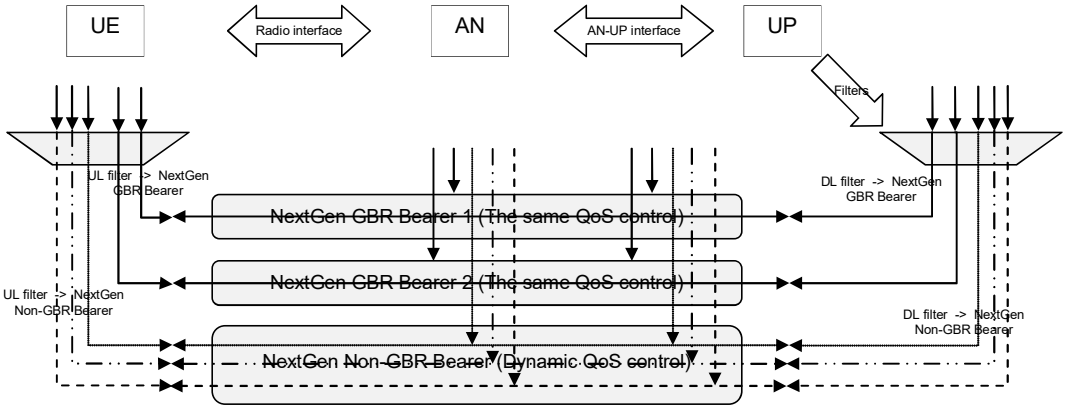


Figure 6.2.9.1-1 NextGen Bearer based QoS control

NextGen GBR bearer: an information transmission path of defined bit rate, scheduling priority, latency and reliability, etc. It is an end-to-end bearer between the UE and UP function Anchor. The QoS control of all service data flow binding to this bearer is the same.

For a PDU session, several NextGen GBR bearers may be established using the out band signalling. The service data can be transferred on the NextGen GBR bearer only after the information of NextGen GBR bearer successfully established is received. The CP Functions generate the QoS parameters (i.e. refer to the table 6.2.9.1.1-1) and forwarding them to the related UP functions, AN and UE. A NextGen Bearer ID is also allocated by the CP function which is used to index the QoS parameters in the UP functions, AN and UE, and the UP functions, AN and UE executes packer transmission control for the traffic binding to the NextGen GBR bearer using these QoS parameters of the NextGen GBR bearer.

NextGen Non-GBR bearer: a default transmission path for a PDU session, it is established when a PDU session is established. The QoS control of services mapped to this NextGen Non-GBR bearer is differentiated by the user plane marking of the user plane packet.

For a PDU session, only one NextGen Non-GBR bearer is maintained. During the PDU session establishment procedure, the CP functions provide the QoS rule (e.g. packet filter and the corresponding packet marking rules) to UP functions and UE using the out band signalling. This Non-GBR Bearer remains established throughout the lifetime of the PDU session.

6.2.9.1.1 NextGen Bearer level QoS parameters

The following list of QoS parameters is used in the NextGen Bearer QoS profile:

- NextGen QoS index: specifies characteristics describe the packet forwarding treatment that a service data flow aggregate receives edge-to-edge between the UE and the UP Anchor in terms of the following performance characteristics: Priority, Latency and Reliability. A standardized NextGen QoS index and corresponding characteristics is independent of the UE's current access (3GPP or Non-3GPP).

- Priority Level: define the service data flow's relative importance to access to AN resource. It is also used to decide whether a NextGen GBR bearer establishment request can be accepted or needs to be rejected due to resource limitation.

NOTE: Priority Level currently is only used for the NextGen GBR Bearer.

- Filter Descriptor: packet filters mapping the service data flow to the NextGen GBR bearer, or packet filters in the QoS rule to mark the NQI and PDPI for each packet of flows which is bind to the NextGen Non-GBR bearer.

For DL of NextGen Non-GBR bearer, NQI and PDPI are marked explicitly on packets by UP according to DL packet filter. AN can process the packets according to the marked NQI and PDPI. For UL, NQI should be marked on packets by UE according to UL packet filter.

- Maximum Bitrate: maximum UL and DL bitrate value applicable for a single flow or aggregation of flows mapped to the NextGen bearer.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 136 of 501

- Guarantee Bitrate: guaranteed UL and DL bitrate value applicable for a single flow or aggregation of flows mapped to the NextGen GBR bearer.

- Packet Discard Priority Indicator (PDPI): defines the discard priority per packet in the NextGen system in case of congestion e.g. for differentiating content type within the same flow. The PDPI marking in the downlink is set by the UP functions and is used by the AN. Each PDPI is associated with a filter descriptor and only applicable for the flows binding to the NextGen Non-GBR bearer.

In the case there is congestion in AN, the AN will discard some packets with high PDPI to free up resource for other packets with low PDPI.

A NextGen GBR bearer is realized by the following elements:

- In the UE, the UL filter descriptor maps traffic flows aggregate to a NextGen GBR bearer in the uplink direction;

- In the UP functions, the DL filter descriptor maps traffic flows aggregate to a NextGen GBR bearer in the downlink direction;

- AN implements admission control and traffic scheduling functions according NextGen GBR bearer QoS characteristics. For admission control, AN should ensure that sufficient resources are available to support a satisfied service before allowing the NextGen GBR bearer to be set up. For traffic scheduling, the QoS concepts of the NextGen GBR bearer is mapped to the QoS concepts of the underlying transport. AN is responsible for configuring the lower layer (layers 1 and 2) protocols between UE and AN in accordance to the QoS characteristics associated with the NextGen GBR bearer. This includes implementing packet forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.) and configuring the error-control protocols (modulation, coding, and link layer retransmissions) so that the QoS characteristics, such as capability, latency and reliability requirements are fulfilled. For a PDU session, each combination of NextGen QoS index and Priority Level is assumed to associate with a NextGen GBR bearer.

The QoS parameters in NextGen GBR Bearer QoS profile are applicable in the network elements as summarized in the follow table:

Table 6.2.9.1.1-1 NextGen GBR Bearer QoS Parameters

QoS parameters		UP functions	AN	UE
NextGen QoS index(NQI)		*	*	*
Priority Level (PL)			*	
Filter Descriptor	DL	*		
	UL	*		*
Maximum Bitrate (MBR)	DL	*	*	
	UL		*	*
Guarantee Bitrate (GBR)	DL	*	*	
	UL		*	*

A NextGen Non-GBR bearer is realized by the following elements:

- In the UE, the UL filter in the QoS rule maps a packet to of the NextGen Non-GBR bearer in the uplink direction. And the packet marking will be done to the traffic based on the QoS rule. Then the UE request the transmission scheduling from the AN based on the user traffic marking, and send the packet on the corresponding radio bearer.

- In the UP, the DL filter in the QoS rule maps a packet toof the NextGen Non-GBR bearer in the downlink direction, and the packet marking will be done to the traffic based on the QoS rule, then the packet is send on the NextGen Non-GBR bearer.

- In the AN, the packet is transmitted based on its packet marking, i.e. NQI and PDPI. The NQI decides the packet forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.) of corresponding radio bearer and the PDPI decides which packets should be discarded in priority in some special cases like congestion.

- The Figure 6.2.9.1.1-2 shows a high level view of packet transmission control based on the QoS rules of NextGen Non-GBR bearer.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 137 of 501

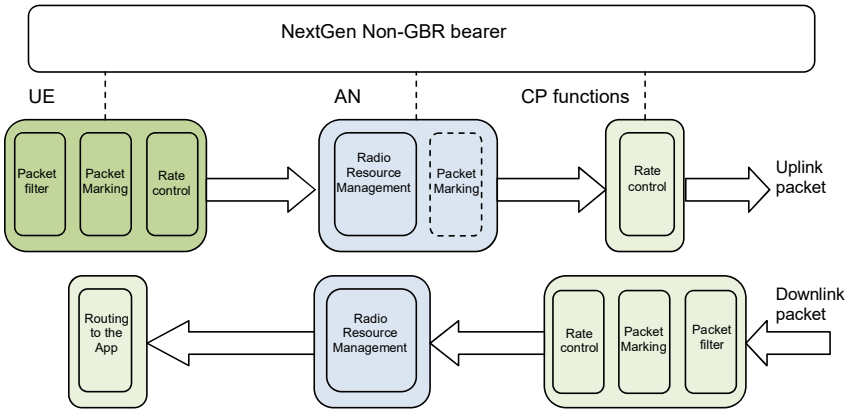


Figure 6.2.9.1.1-2 NextGen Non-GBR based QoS control

QoS rules included in the NextGen Non-GBR bearer QoS profile are applicable in the network elements as summarized in the follow table:

Table 6.2.9.1.1-2 NextGen Non-GBR Bearer QoS Parameters

QoS parameters		UP functions	AN	UE
NextGen QoS index(NQI)		*	*	*
Packet Discard Priority Indicator (PDPI)		*	*	*
Filter Descriptor	DL	*	*	
	UL		*	*
Session Maximum Bitrate (SMBR)	DL	*		
	UL		*	*

Reflective QoS:

- Reflective QoS is not used for the NextGen GBR flow.
- Reflective QoS is used for the NextGen Non-GBR flows without filter descriptor for the NQImarking.

6.2.9.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.2.9.2.1 NextGen Non-GBR Bearer established at PDU session establishment

During the PDU session establishment, the NextGen Non-GBR bearer for service data in the network is established.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 138 of 501

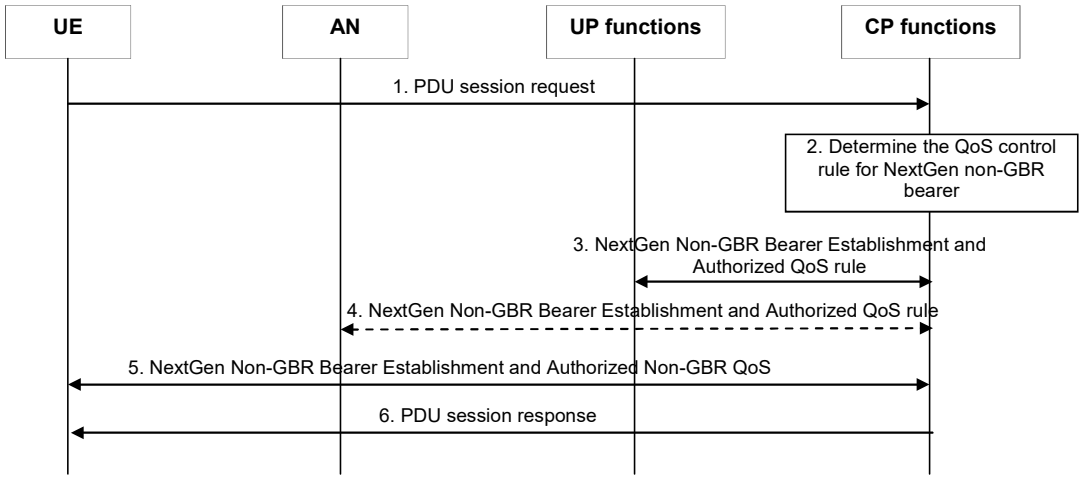


Figure 6.2.9.2.1-1: PDU session establishment with NextGen Non-GBR bearer

1. The UE determines to establish a PDU session and sends a PDU session request to CP functions.
2. The CP functions determine the QoS rulesof NextGen Non-GBR bearer. The QoS rules include default Qos rule (NextGen Bearer Id, default NQI, default PDPI , SMBR) and dedicated Qos rules(NextGen Bearer Id, filters, NQI , PDPI).
3. The CP functions forward the QoS rules of NextGen Non-GBR bearer to UP functions. The UP functions acknowledge the reception.
4. The CP functions forward the QoS rules of NextGen Non-GBR bearer to AN (NextGen Bearer ID, SMBR). The AN acknowledges the reception.

NOTE: For NextGen Non-GBR bearer, this step is optional.

5. The CP functions forward the QoS rules of NextGen Non-GBR bearer to UE. The UE acknowledges the reception.
6. The CP functions complete the PDU session establishment using the PDU session response and inform the UE about the QoS rules of NextGen Non-GBR bearer.

6.2.9.2.2 NextGen GBR Bearer establishment based on the application server request

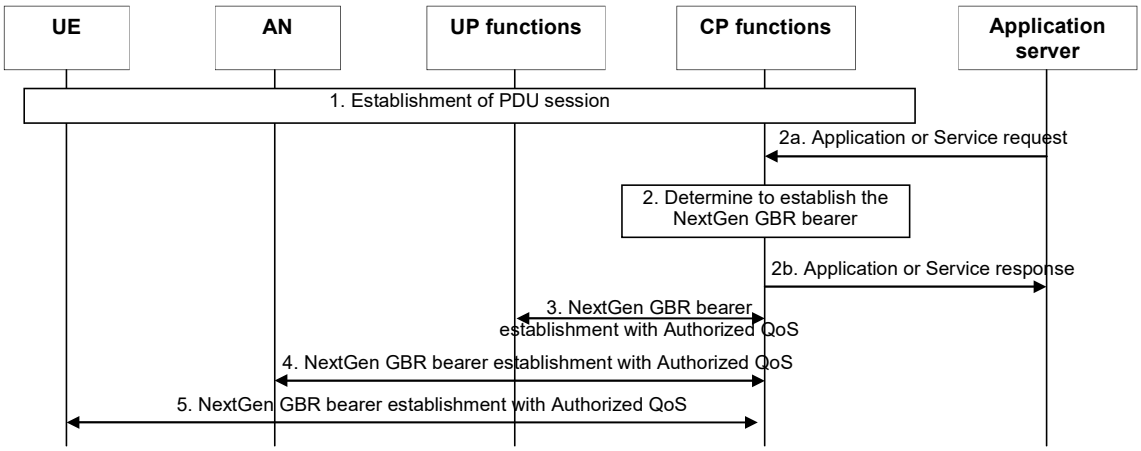


Figure 6.2.9.2.2 NextGen GBR bearer establishment based on the application server request

1. A PDU session between the UE and a data network is established and a NextGen Non-GBR bearer established.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 139 of 501

2a. An application server sends an application or service request with QoS requirement to CP functions.

2. CP functions determine to establish the NextGen GBR bearer.

2b. CP functions acknowledge the request with an application/service response to the application server.

3. The CP functions trigger the NextGen GBR bearer establishment with authorized QoS profile (NextGen Bearer Id, NQI, PL, Filters, GBR, and MBR) to UP functions. The UP functions acknowledge the establishment procedure.

4. The CP functions trigger the NextGen GBR bearer establishment with authorized QoS profile (NextGen Bearer Id, NQI, PL, Filters, GBR, MBR) to AN. The AN acknowledges the establishment procedure.

5. The CP functions forward the QoS profile (NextGen Bearer Id, NQI, PL, Filters, GBR, MBR) of NextGen GBR bearer to UE.

6.2.9.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3 Solutions for Key Issue 3: Mobility framework

6.3.1 Solution 3.1: High-level functions of the mobility framework

This solution applies to Key Issue 3 - Mobility Framework. The solution introduces the high-level functions for providing mobility support over the Evolved E-UTRA access and the new < 5G> RAT.

6.3.1.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

Figure 6.3.1.1-1 below shows the high-level functions used for the mobility framework. The interpretation of the high-level functions is elaborated below.

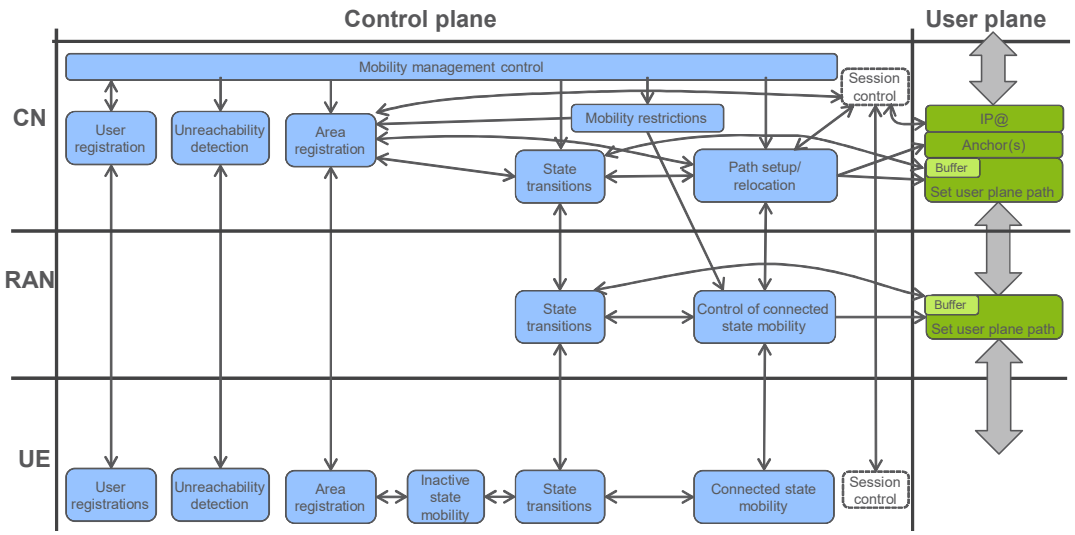


Figure 6.3.1.1-1: High-level functions of the mobility framework

The mapping of high-level functions to 3GPP NFs is FFS.

User registration. Initial setup of a signalling relation between the UE and the CN, authentication of the user, establishment of the user context in the network, exchange of basic parameters between the UE and the CN, and de-registration.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 140 of 501

Unreachability detection. Detects when a UE is no longer reachable, and clean up the necessary CN state as needed.

Editor's note: Details related to unreachability detection and the need for unreachability detection at the RAN is FFS.

Area registration. Allows the CN to be aware of the UE location on a configurable granularity, both in inactive and in connected state. This enables the operator to page the UE when necessary; perform relocation procedures as needed; and realize mobility restrictions on an area basis.

State transitions. State transitions to an inactive state help to reduce the network resource usage for UEs that are not currently sending or receiving data, and help minimizing the UE battery consumption. The mechanisms for state transitions may be optimized for reduced RAN and CN signalling and low latency. Paging is functionality to transition from inactive to connected state.

Editor's note: Details related to paging is FFS.

Connected state mobility. When the UE is connected to RAN, handovers are controlled by the RAN node. The CN sets up or updates the user plane path as needed.

Inactive state mobility. When the UE is in this state, cell selection is controlled by the UE.

Mobility restrictions. Operators may set certain areas of the network as forbidden for a specific group of UEs. Also, operators may set certain areas of the network accessible for a specific group of UEs. These restrictions may be derived from user subscription and operator configuration.

Mobility management control. Provides overall control and appropriate configuration of the mobility framework. The system may limit the level of mobility support for certain UEs in an effort to achieve cost reductions for the operator. The mobility management control functional block feeds the necessary parameters to other high-level functions to set the appropriate mobility limitations, which may be based on subscription data.

IP@. In the user plane, an entity with IP@ provides the point of presence in the IP network.

Editor's note: Further details of IP@ is FFS and depends on the session management key issue.

Anchor(s). One or more UP anchor points can be used which remain unchanged during UE mobility within the service area for the given anchor point.

Editor's note: Further details of UP anchor points is FFS.

Set user plane path. Below the anchor points, the user plane paths are updated upon UE mobility as needed, and the user plane path is set according to the UE's current location.

Buffering. Buffering is used for downlink packets for the period of time when the reachability towards the UE via the RAN has not yet been established.

Editor's note: It is FFS whether buffering can be done in RAN, CN or both.

Session control. Session control functionality is not elaborated in this solution, but it is assumed that mobility events may trigger session control so that sessions may be released or set up as needed.

6.3.1.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

After successfully registering with the network, UEs that are active sending or receiving data are connected to RAN where the handover decisions are under the control of RAN. The CN notifies the RAN about mobility restrictions which are taken into account in the handover decisions. Handovers within a RAN node may not lead to any CN signalling unless CN notification is requested. During handovers to a new RAN node, packet forwarding to the new RAN node helps to minimize the interruption time for the user. Once the handover to a new RAN node has taken place, the RAN informs the CN in the control plane. The CN control plane then updates the user plane path. In case the mobility management settings limit the mobility for a given user session, the session control functionality may be triggered to release the session and set up a new session if needed, which may utilize an user plane path optimized for the user's current location.

A state machine provides efficient system characteristics and low resource cost. An inactive UE utilizes a state which requires less resource utilization, and also minimizes the UE battery drain. The solution should be optimized so that

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 141 of 501

very fast and signalling-efficient transition can be achieved. The changes in the state machine imply the corresponding updates to the user plane path. A buffering mechanism is set up for downlink packets in the user plane. Initial downlink packets trigger the corresponding paging procedure and the subsequent setup of the downlink user plane path so that reachability for mobile terminated communications can be ensured. The state transition mechanisms are complemented by the unreachability detection function that can detect e.g. when a UE becomes unreachable due to lack of radio coverage, so that the release of the network resources can take place as needed.

Independent of the UE state, an area registration mechanism ensures that CN has knowledge about the current location of the UE at a granularity which is configurable for the operator. The area registration mechanism takes input from the mobility restrictions function and the mobility management control function so that it can limit mobility as required by the operator. Similarly as the connected state mobility function, the area registration mechanism can also trigger the session control function when necessary to set up or release a session as needed, so that an optimized user plane path can be achieved.

6.3.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.2 Solution 3.2: Mobility state framework

6.3.2.1 Architecture description

Next Generation (NG) core network should take into consideration the state machines envisioned for RRC protocol within new RAT. It is proposed that the mobility state machine for RRC should have an inactive connected state (in addition to an RRC Connected state and an RRC Idle state). The need for configurability of the RRC inactive connected state is motivated through several factors that require flexibility such as diverse requirements of the 5G use cases, future-proofness and quick time to market requirement for new services.

From the Next Generation core network perspective, UE is considered to be in the NG CM-CONNECTED state when UE is in RRC inactive connected state at the RRC layer. When the UE transitions between RRC connected state and RRC inactive connected state, it is not visible to the core network as no signalling towards the core network is expected due to this transition. Also, core network does not have to page the UE when the UE is in RRC inactive connected state as both control plane and user plane remains established between the RAN and core.

The characteristics of the RRC inactive connected state includes:

- UE is considered to be in the NG CM-CONNECTED state in UE and CN.
- Configurable to serve the service(s) requested by the UE. This implies that the RRC inactive connected state can be configured taking the characteristics and requirements of the application(s) running in the UE, subscription and UE activity into account. Core network shall provide that related information to RAN.
- UE based mobility inspired by cell reselection procedure with configuration from network , no network controlled handover is supported.
- UE performs Area registration to CN when the UE moves outside of the registered area(s).
- The Access Stratum (AS) context is stored in RAN and the UE.
- RRC inactive connected to RRC connected state transition inspired by the Suspend and Resume procedures defined for LTE in Rel-13. Furthermore, no signalling to the CN is needed to perform this transition. The AS Context may need to be transferred between the RAN nodes.
- U-plane and C-plane connections between RAN and core are kept established.
- UE reachability will be managed by the RAN, with assistance from core network.
- UE paging will be managed by the RAN.
- CN will transit to the NG-CM IDLE state upon RAN request.
- Distributed mobility management - Network follows UE on CN level.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 142 of 501

NOTE: Whether a RAN determined area where a UE can move without notifying the network is needed, is for the RAN WGs to determine.

- No Rx/Tx Data is performed in this state.
- To support LTE and NR deployments in an efficient way the solution for state transition shall avoid or minimize UE signalling when UE is toggling between NR and Evolved E-UTRA in Inactive state.

Following figure shows how the proposed RRC state machine fits within the NG CM/MM State machine model when using the RRC INACTIVE CONNECTED state:

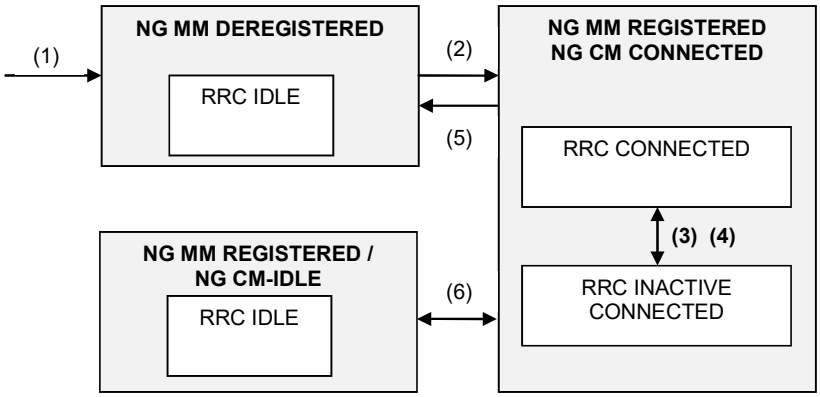


Figure 6.3.2.1-1: NG RRC/CM/MM with state transition illustrated

State Transitions illustrated:

(1) UE powers on, performs PLMN/cell selection and camps in a suitable cell.

(2) UE registers (attaches) with the network and performs connection setup. UE transmits and receives data in RRC connected.

(3) Inactivity results in transitions to RRC inactive connected.

(4) MT/MO trigger to transmit data results in transition to connected for Tx/Rx.

(5) Detach/Power off.

(6) Connection setup/release

NOTE: This solution has dependency on RAN as the RRC state design decision belongs to RAN WG2. RAN WG2 is expected to define the number of necessary states and their characteristics in order to achieve its requirements.

6.3.2.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.3.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.3 Solution 3.3: Solution for mobility framework with RAN level tracking

This solution addresses key issue #3, and in particular the following:

- Definition of mobility states.
- Support of reachability to enable mobile terminated communication.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 143 of 501

- Methods to limit the amount of mobility management signalling between NextGen core and the access, within the NextGen core as well as between the NextGen core and the UE.

6.3.3.1 Architecture description

This solution assumes the following:

- RAN-level UE tracking based on RAN Routing Areas (RRAs), the RRA being a collection of cells (similar to the URA in UTRAN).
- New battery-efficient RRC state (RRA_PCH; similar to URA_PCH in UTRAN) where the UE location within the RAN is known with the granularity of RRA and UE is not involved in data exchange with the network.
- Use of either NW-driven (i.e. handover) or UE-driven (i.e. cell reselection) mobility in RRC_CONNECTED state.
- From NextGen core perspective the UE is in permanent NextGen_Connected state i.e. the CN core - RAN interface is up and running regardless whether the UE is in RRA_PCH or RRC_CONNECTED mode.
- Use of a RAN-level anchor that minimises the need for relocation of the CN core - RAN interface in all RRC states.

Editor's note: It is FFS whether the RRAs are defined statically or whether they can be defined dynamically (e.g. centred around the current UE location, similar to how TAs are used). The definition of RRAs and new RRC mobility states need to be reviewed together with the RAN WGs.

Editor's note: It is up to RAN WGs to decide whether there is need to support both NW- and UE-driven mobility in RRC_CONNECTED.

Figure 6.3.3.1-1 illustrates that the RRA_PCH and RRC_CONNECTED states both correspond to a NextGen_Connected state in the NextGen core.

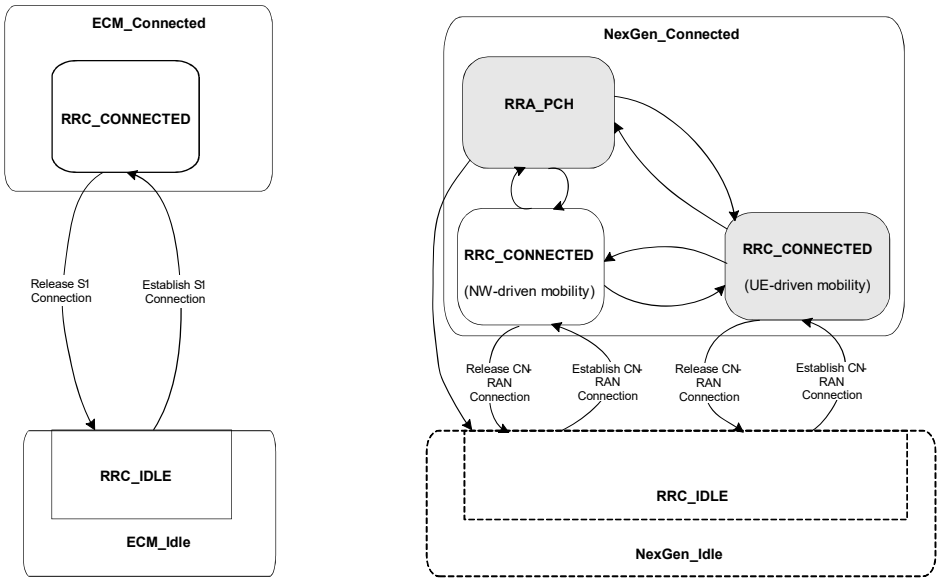


Figure 6.3.3.1-1: CN and RAN states for EPS/E-UTRAN (on the left) and NextGen/<5G RAN> (on the right)

Also depicted in Figure 6.3.3.1-1 is an RRC_IDLE state, corresponding to a NextGen_Idle state in the NextGen core. This state is needed if the concept of hierarchical tracking (similar to the one existing in UTRAN) is kept, as follows:

- When in NextGen_Idle state, the UE is tracked at Tracking Area (TA) level by the NextGen core.
- When in NextGen_Connected + RRA_PCH state, the UE is tracked at RRA level by the <5G> RAN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 144 of 501

Editor's note: The definition of the new states needs to be reviewed together with the RAN WGs.

Editor's note: The need for hierarchical tracking (i.e. the need for NextGen Idle / RRC_IDLE state) is FFS and needs to be reviewed together with the RAN groups.

6.3.3.2 Function description

6.3.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.4 Void

6.3.5 Solution 3.5: Stateless Context Management for Data Network Sessions

This solution applies to key issue 3 on Mobility management, but addresses also aspects of key issue 4 on session management.

6.3.5.1 Architecture description

The solution proposed in this document applies to both mobility management and session management.

The solution introduces the concept of a Context Cookie. The Context Cookie is assigned by the 5G system to the UE once the UE has successfully connected to the network (e.g. established a MM context, and optionally an SM context) and has been authenticated by the network. The Context Cookie is used by the UE, after a period of inactivity during which the network "releases" the UE context, to enable the 5G system to reconstruct the state when the UE connects (e.g. becomes connected and sends small data) without having to continuously maintain state in the network between instances of connectivity (or small data connectionless transactions).

The context cookie is applicable depending on the device type and/or service type the UE is connecting to, based on network policies.

The Context Cookie contains at a minimum the following information:

- A UE identifier, to enable the network to identify the UE.
- The UE security context in the AN (if any), to enable the network to e.g. either re-establish the UE context or decrypt the payload sent together with the Context Cookie.
- UE context information established during attachment and session setup (this may include an identity of the entity that generated the cookie).
- An expiration time set by the 5G system which limits the lifetime of the Cookie (i.e. prevents permanent reuse).

Editor's note: The exact content of the Context Cookie is FFS and depends on the specific scenario in which the Context Cookie is used.

The Context cookie contains a representation of the UE context sufficient so that the network does not to have to maintain a full copy of the UE context.

Editor's note: It is FFS how the cookie size can be minimized and/or optimized for different usage scenarios, e.g. transmission of single PDUs versus PDU bursts.

Editor's note: It is FFS whether it is possible to avoid maintaining any UE specific context information in the AN and CN.

With this solution, the UE can perform small data transfers (e.g. a single PDU) without requiring the UE to transition to connected mode and without any MM/SM signaling, and without requiring the network to maintain a full context for the UE. The UE can also use the Context Cookie to transition from idle to connected without requiring the network to maintain a full context for the UE. In such case, the UE uses the Context Cookie at the first time it transitions to connected state.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 145 of 501

It has to be noted that, in order to ensure correct behaviour of this solution, the Context Cookie needs to be secure.

Editor's note: The security aspects of this solution need to be studied by SA3. However, security requirements for the solution are described here.

Specifically, a secure Context Cookie must:

- protect the privacy of the context information.
- protect the integrity of context information.
- be bound to a device, i.e. not transferrable.
- be impossible to be modified and manipulated by a device.
- verifiable by the network when provided by the UE.
- enable the network (AN or CN) to identify the entity that created the cookie to enable cookie verification.

The Context Cookie operates on a similar principle to HTTP cookies, in that the network provides the UE with an encrypted context to use when connecting to the network.

The Context Cookie can be established and later verified by the network (AN or CN) based on security mechanisms that are not per-UE (e.g. per-AN keys), without the need for the network (AN or CN) to maintain any per-UE context. e.g. a secure Context Cookie is generated by a network function based on information maintained by the network function(e.g. security keys only known to the network function), and applied to all UEs for which the network function create a Context Cookie. No centralized entity is required for cookie creation and verification.

Editor's note: The mechanisms for Context Cookie creation for network sharing is FFS.

Editor's note: The interaction between roaming and the creation and usage of Context Cookies is FFS.

Editor's note: It is FFS whether the context information privacy can be achieved if the Context Cookie is protected using keys that are not per-UE. This should be established based on SA3 security analysis of the solution.

The use of the Context Cookie enables connectionless based services as defined in SMARTER TR 22.891 [9] (clause 5.40), since when the transfer of small amounts of data needs to take place, the Context Cookie enables the data transfer without requiring the establishment and teardown of connections, and enables the 5G system to accept data transmission from the UE without a lengthy and signalling intensive bearer establishment and authentication procedure since the UE context is verified and possibly re-established, depending on the functional description below, based on the Context Cookie. The Context Cookie can be generated as a:

- CN Context Cookie: the CN Context Cookie is allocated by the CN to the UE upon attachment and (possibly) session establishment with the network. It contains CN-specific context information.
- AN Context Cookie: the AN Context Cookie is allocated by the AN to the UE upon attachment and (possibly) session establishment with the network. It contains AN-specific context information (e.g. AS context).
- Single Context Cookie: the Single Context Cookie contains both AN and CN context information.

Editor's note: Whether the Single Context Cookie is a concatenation of the CN Context Cookie and the AN Context Cookie requiring two separate verifications (respectively in CN and AN), or a single piece of information with a single verification is FFS and depending on the design of MM and SM solutions.

Editor's note: Whether single CN Context Cookie is sufficient for different CN control plane functions or multiple CN Context Cookies are needed and its management, e.g. how to provide and update different CN Context Cookie, are FFS.

Editor's note: The solution described here assumes a single network slice in terms of AN Context Cookie and CN Context Cookie. How this applies to multiple slices is FFS and depends on the solution for network slicing.

A AN Context Cookie is applicable to mobile originated PDU transmissions.

A solution adopting solely the CN Context Cookie already enables the support of large numbers of devices that infrequently transmit Mobile Originated data by reducing the amount of context maintained in the CN for such devices

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 146 of 501

and by minimizing the amount of MM and SM signalling required to re-establish connectivity and transmitting data. When completed with a AN Cookie, this solution provides a complete solution for optimizing the management of a large number of devices that transmit Mobile Originated data infrequently, since no status in AN or CN needs to maintain when the devices are not active.

If a UE attempts to use a Context Cookie after the expiration of the cookie, or if the network has locally revoked the Context Cookie authorization, the UE request is rejected and the UE has to re-established connectivity as in the case of an initial attach.

The solution can build on the concepts developed for small data transmissions in EPC. As an example, an entity as the C-SGN (CIoT Serving Gateway Node) of the EPC architecture can be envisaged also for the NextGen architecture for CIoT deployments (e.g. a network slice dedicated to CIoT) to handle devices with small data transmissions. The solution based on Context Cookies is anyway orthogonal to the solutions for CIoT.

6.3.5.1.2 Support For Infrequent Small User Data Service

It is proposed to support infrequent Small Data Service (SDS) via the use of Context Cookies. In particular, the solution proposes that for UEs that require the support of SDS transfers, an AN Context Cookie is used to enable the transfer of SDS.

The solution is based on an initial authentication of the UE by the network during an attach procedure, in order to verify the validity of the UE to access the MNO resources for SDS transfer, and the creation of appropriate context cookie(s) as defined in 6.3.5.2.1 to enable the device to send infrequent SDS without requiring the establishment of any PDU Sessions. When the UE needs to send an SDS PDU, instead of re-attaching to the network or performing mobility management procedures, the UE provides the SDS PDU(s) to be transferred together with the Context Cookie to enable the network to verify that the UE is allowed to send such PDUs.

6.3.5.1.3 Support of CIoT User Plane Optimizations

In EPC, CIoT user plane optimizations have been defined. In such mechanism, when the UE goes to IDLE mode the eNB stores the Resume ID of the UE and the bearers and security context of the UE.

In this solution, it is assumed that similar optimizations will be adopted in the 5G NextGen system for the 3GPP RANs. It is proposed that if the UE is attached to the NextGen network and both the UE and the network support CIoT user plane optimization, when the UE goes to IDLE mode the AN stores only the Resume ID for the UE. The AN creates an AN Context Cookie for the UE containing the radio-related information and the security context of the UE, delivers the AN Context Cookie to the UE and release the UE context while maintaining the Resume ID.

6.3.5.2 Function description

Editor's note: The function description below considers the transfer of data on the user plane. However, as it was done for CIoT, control plane optimizations can also be consider to transfer small data over the control plane.

The following procedures define the establishment, delivery, and use of the Context Cookie.

Editor's note: The mechanisms for updating and/or generating new Context Cookies (e.g. after the UE re-establishes connectivity to send a small data burst and the UE has moved location within the network) are FFS.

6.3.5.2.1 Context Cookie Creation

The Context Cookie is generated by either the AN or the CN based on a set of information, including at least:

- Device Type
- Service Type

In particular, when deciding the type of Context Cookie to be provided to the UE, the AN and CN consider whether to provide an AN Context Cookie, a CN Context Cookie or a Single Context Cookie that includes both an AN Context Cookie and a CN Context Cookie based on such parameters. For example:

Context Cookie is generated by either the AN or the CN based on a set of information, including at least:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 147 of 501

- For services that require mobile terminated data delivery in addition to mobile originated data based on the UE having established PDU session(s), the network may decide to provide only an AN Context Cookie to the UE and maintain the CN context in the network when the UE becomes idle.

- For a device attached for SDS only without establishing any PDU sessions, only an AN Context Cookie is provided to the UE when the UE goes idle.

The Context Cookie is created as follows:

- AN Context Cookie: created and provided to the UE by the AN. Input from CN CP functions may be used. The AN Context Cookie is protected with an AN Cookie Security Context specific of the AN that generates the AN Cookie and that is not per-UE. When provided by the UE, the AN Context Cookie is verified by the AN.

- CN Context Cookie: created and provided to the UE by the CN CP functions. The CN Context Cookie is protected with a AN Cookie Security Context specific of the CN CP function that generates it, and that is not per-UE. When provided by the UE, the CN Context Cookie is verified by the AN.

- Single Context Cookie: created and provided to the UE by the AN in collaboration with the CN CP function. The Single Context Cookie is protected with an AN Cookie Security Context specific of the AN that generates it, and that is not per-UE. When provided by the UE, the Single Context Cookie is verified by the AN.

For SDS, the Context Cookie that enables the support of SDS may include the identity of a Small Data Serving Gateway Node (SD-SGN) allocated to support SDS for the UE (e.g. SCEF). The SD-SGN identity may be used when the SDS PDU is protected (e.g. ciphered, integrity protected, or both) between the UE and the SD-SGN in order to verify which SD-SGN can verify the SDS PDU.

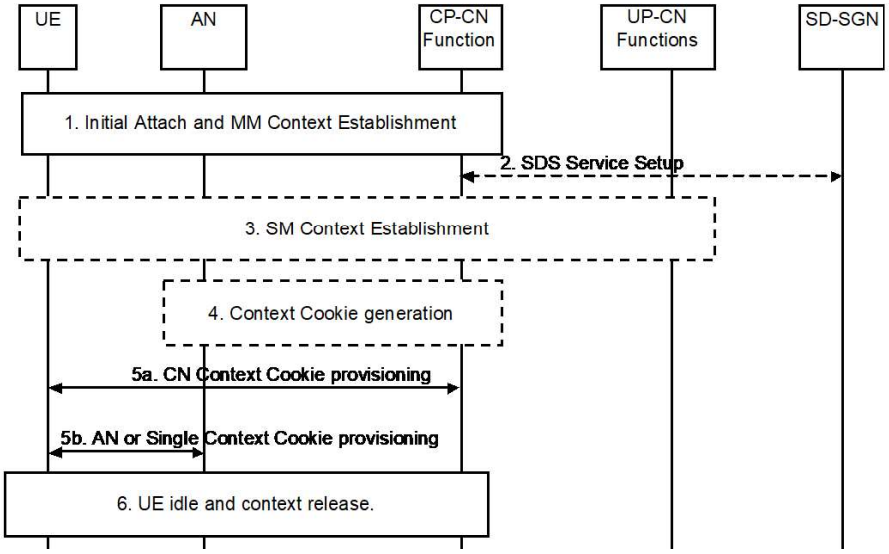


Figure 6.3.5.2.1-1 Connection Establishment using Context Cookies

1. The UE establishes a Mobility Management (MM) context via MM procedures with the CP-CN Function upon successful authentication.

Editor's note: For UEs that support only SDS, the CP-CN Function serving the UE can be a node similar to the C-SGN of the EPC architecture, i.e. a function that minimizes the number of physical entities by collocating entities in the control and user planes paths. Selection of the type of CP-CN function to serve a UE is FFS and may be based on assistance information provided by the UE upon initial attach (e.g. device type, service type).

2. If the UE supports SDS via control plane, the CP-CN function may establish the connectivity for SDS service by interacting with a Small Data Serving Gateway Node (SD-SGN) to serve the UE for the transfer of MO and MT SDS PDUs. The CP-CN function may interact with the SD-SGN to obtain a security context that enables the UE to protect (e.g. ciphering, integrity protection, or both) future MO SDS PDUs between the UE and the SD-SGN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 148 of 501

3. The UE may also establish one or more PDU sessions depending on the Data Network connectivity requirements.

4. Either during the MM context establishment or PDU session(s) establishment, or in a separate procedure, a context cookie is generated, including SDS specific information such as the SD-SGN identity:

- Single Context Cookie: the AN and the CP-CN interact to generate a Single Context Cookie using AN-specific and CN-specific information to create a secure Single Context Cookie. The Single Context Cookie is provided to the AN for securing the cookie and for delivering it to the UE.

- CN Context Cookie: the CP-CN generates a CN Context Cookie for the UE (containing MM context information and, if one was created, SM context information), using CN-specific information to create the Context Cookie.

- AN Context Cookie: a control plane functionality in the AN, which establishes and maintains the AN context for the UE, may interact with the CP-CN function and generates a RAN Cookie for the UE using AN-specific information to create a secure Context Cookie.

5a. The CP-CN Function delivers the CN Context Cookie to the UE.

5b. The AN delivers the Single Context Cookie or the AN Context Cookie to the UE, including the SD-SGN security context if provided for SDS.

6. The UE stores the CN CP-CN Cookie, and may become idle. The AN releases the UE context upon the UE becoming idle. Depending on the type of Context Cookie provided, the CN may release the UE context upon the UE becoming idle.

6.3.5.2.3 Mobile Originated Small Data Service Transfer with Context Cookie-based context verification

When a UE that has received Context Cookie(s) from the network needs to transfer small data, the UE uses the AN Context Cookie or the Single Context Cookie to re-establish connectivity necessary for the small data transfer.

Editor's note: support of mobile terminated SDS PDUs is FFS.

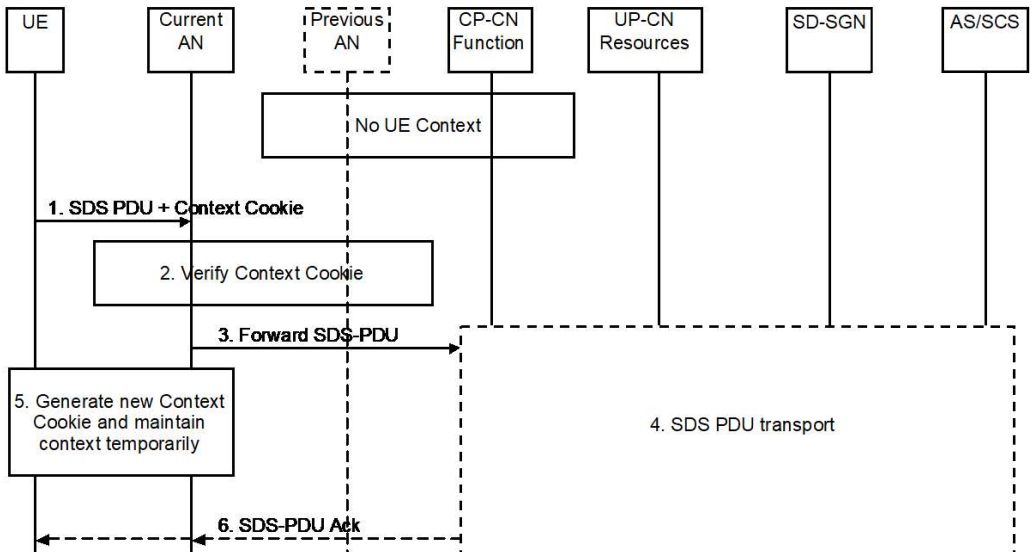


Figure 6.3.5.2.2-1 Small Data Transfer with Cookie-based context verification

After a certain period of UE inactivity, or e.g. after a small data transfer, the network maintains no context for the UE:

1. When the UE needs to send an uplink SDS PDU, e.g. for small data transfers or short bursts of data, the UE provides together with the SDS PDU to be transmitted also the AN Context Cookie or the Single Context Cookie to the network to enable the network to verify that the UE is allowed to transmit small data. In case of multiple

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 149 of 501

packet transmissions, the UE needs to provide the Cookie only one time, e.g. piggybacking them in the first PDU. The UE uses best effort transport (e.g. a default bearer) to transmit the PDUs.

2. In order to cater for scenarios where the UE may have moved from the original location where the Context Cookie was created, the AN verifies the Context Cookie if it is capable (e.g. the Context Cookie was generated by the functional entity that receives it). If not, it either requests the Context Cookie verification from the functional entity that generated it, or sends the PDU for verification to the functional entity that generated the Context Cookie.

3. Upon successful verification, the AN accepts the UE SDS PDU and forwards it to the CN for transfer according to the context information in the cookie without re-establishing the full context.

4. The CN transfers the SDS PDU towards the AS/SCS. This may happen via sending the SDS PDU to the SD-SGN (e.g. when the SD-SGN needs to verify the SDS-PDU before forwarding it), via user plane resources (e.g. in an existing PDU session), etc.

5. The network may create and deliver a new Context Cookie to the UE. This may happen e.g. due to the UE mobility (e.g. the UE may have moved between different areas of an AN or to a different AN). The network also maintains the UE context for a short time to assure that acknowledgement messages can be sent back to the UE.

6. If an acknowledgement is received from AS/SCS, the CN forwards it to the UE.

6.3.5.2.4 Mobile Originated Small Data Transfer with Cookie-based context re-establishment

In this example, it is assumed that the UE SM context is established before the UE becomes idle, and that it involves the establishment of a PDU Session connected to a data network via an UP-GW.

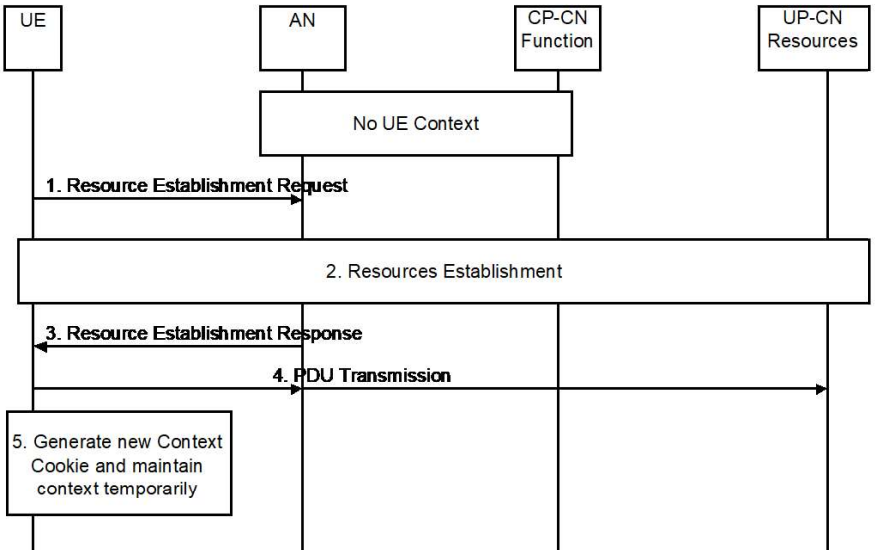


Figure 6.3.5.2.3-1 Small Data Transfer with Cookie-based context re-establishment

After a certain period of UE inactivity, or e.g. after a small data transfer, the network maintains no context for the UE:

1. When the UE needs to send uplink data for longer data transfers, the UE sends a Resource Establishment Request containing either the AN Single Context Cookie or both the AN and the CN Context Cookie.

2. Upon receiving the Context Cookie, and in order to cater for scenarios where the UE may have moved from the original location where the Context Cookie was created, the AN determines if it is capable of verifying the Context Cookie (e.g. the Context Cookie was generated by the functional entity that receives it). If not, it requests the Context Cookie verification from the functional entity that generated it, otherwise it directly verifies the Context Cookie. Upon successful verification, the AN re-establishes the UE context, selects a CP-CN Function for the UE, and forwards either the UE CN Context Cookie or the UE CN context contained in the

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 150 of 501

Single Context Cookie to the CP-CN function. This may include, for IP data transfers, re-establishing context in the AN, the CP-CN Function(s) (which may include selection a UP-GW)and in the serving UP-GW, including QoS based on the UE context contained in the cookie.

3. The AN confirms the re-establishment of the context to the UE.

4. The UE transmits the PDUs.

5. The network may create and deliver a new Context Cookie to the UE. This may happen e.g. due to the UE mobility (e.g. the UE may have moved between different areas of an AN or to a different AN) or expiration of the Context Cookie. When the UE becomes idle, the network then releases the context information again.

6.3.5.2.4 Connection Suspension and Cookie Generation for User Plane CIoT Optimisation

When the AN Context Cookie is applied to User Plane CIoT optimizations, the AN Context Cookie is generated and provided to the UE during the procedure to suspend the connection if the UE and the network support User Plane EPS Optimization.

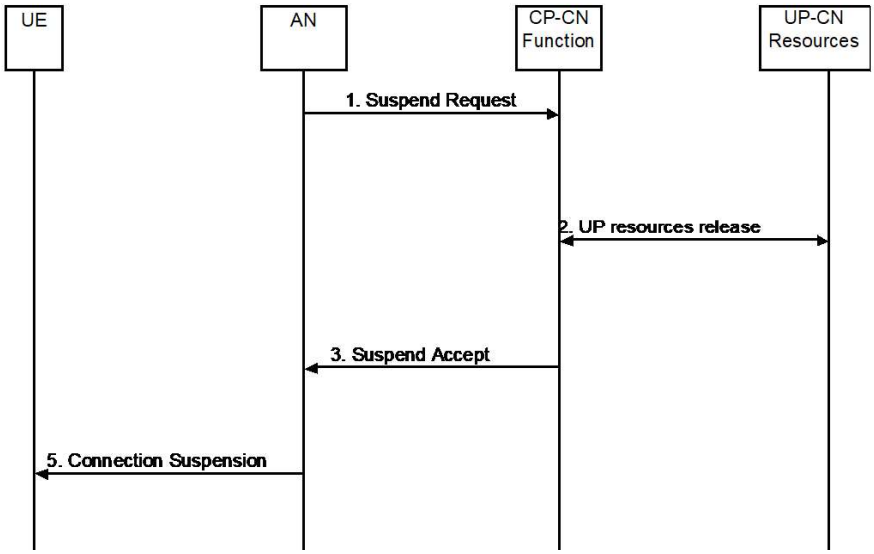


Figure 6.3.5.2.4-1: AN initiated Connection Suspend procedure with AN Context Cookie.

1. The AN initiates the Connection Suspend procedure to the CN-CP Function to indicate that the UE is suspending the connection. The AN may provide additional mobility management.

Editor's note: the exact information the AN provides to the CN-CP Function depends on the solution for mobility management.

2. The CP-CN Function may release some CN resources (e.g. user plane resources). The CP-CN Function does not release the UE context. User plane resources and related information necessary to reach the UE for mobile terminated traffic (e.g., for paging) are maintained.

Editor's note: the exact CP-CN behaviour in terms of managing user plane resources (e.g. tunnelling, packet forwarding, etc.) when the UE suspends a connection depends on the solution design for mobility management, session management and session connectivity in NextGen system.

3. The CP-CN Function informs the AN that the connection suspension can proceed.

4. The AN generates an AN Context Cookie and sends signalling to the UE to suspend connection, including the AN Context Cookie. The AN maintains the UE Suspend ID but releases the UE radio-related information (e.g. radio bearers) and security contexts.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 151 of 501

6.3.5.2.5 Connection Resume for User Plane CIoT Optimisation

This procedure is used by the UE to resume the connection if the UE and the network support User Plane Optimization.

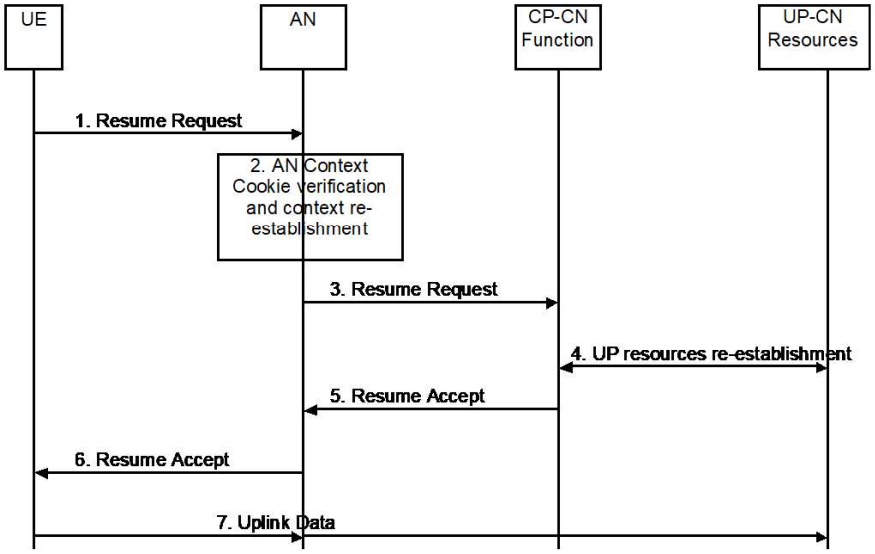


Figure 6.3.5.2.5-1: UE initiated Connection Resume procedure with AN Context Cookie.

1. The UE triggers the connection resume procedure with access stratum signalling and provides the Resume ID and the AN Context Cookie.
2. The AN verifies the AN Context Cookie and re-establishes the UE context based on the radio-related and security information in the AN Context Cookie.
3. The AN sends a Resume Request to the CP-CN Function to resume the connectivity.
4. The CP-CN Function re-establishes the resources for transferring data and confirms he resume to the AN.
5. The CP-CN Function confirms the resume to the AN.
6. The AN confirms the resume to the UE.
7. The uplink data from the UE can now be forwarded by the AN to the core network.

6.3.5.2.6 Support of Scheduled Mobile Terminated Communications

This solution applies to devices which only have scheduled mobile terminated communications (e.g., when the device is preconfigured to receive data at specific times).

NOTE: in scheduled mobile terminated communications a device may connect to the network even when no MT data needs to be transmitted.

In this scenario, the network generates an AN Context Cookie and a CN Context Cookie, or a Single Context Cookie, containing the whole UE context for the AN and the CN. When the UE goes into idle mode, from the point of view of the core network the UE is detached since no context is maintained in either AN or CN.

When mobile terminated communications are scheduled, the UE performs a context re-establishment procedure by providing the Context Cookie(s) provided by the network when the UE went idle. The context re-establishment includes e.g., selection of user plane functions (e.g. UP-GW) and IP address allocation.

Mobile originated communications take place as in the previous cases.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 152 of 501

6.3.5.2.7 Support of Unscheduled Mobile Terminated Communications

In order to enable delivery of unscheduled mobile terminated communications, the network maintains a minimum context in the core network sufficient to enable the delivery of (an) initial PDUs and trigger UE reachability procedures (e.g. paging in case of RAN).

Editor's note: the exact content of the context maintained in the network in terms of context information and user plane resources depends on the solutions for mobility management, session management, QoS and session continuity. e.g., some context in a user plane function and either SM or MM function are maintained to enable the delivery of (an) initial PDU.

The network generates an AN Context Cookie and a CN Context Cookie, or a Single Context Cookie, containing the AN context and the remaining CN context to enable the UE to provide information to allow the network to re-establish the full context.

6.3.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.6 Solution 3.6: Mobility states for UE with power consumption optimization

This solution addresses key issue #3, especially for the definition of mobility states and how to transition between the states. And a mobility state model of core network is proposed to meet the requirement for UE with power consumption optimization in the Next Generation Systems, e.g. wide area sensor monitoring and event driven alarms, Bio-connectivity devices and massive IoT devices.

6.3.6.1 Architecture description

A mobility state model of core network is proposed for UE with power consumption optimization, including the following states:

- NG_IDLE state: the UE is in NG_IDLE state when no signalling connection between UE and network exists. The UE performs cell selection/reselection and PLMN selection, monitors paging, and initiates mobile originating services or location update if necessary.
- NG_CONNECTED state: the UE establishes a signalling connection between the UE and the network, and performs location update and handover if necessary.
- NG_POWER-SAVING state: the UE deactivates its Access Stratum functions, and stops all idle mode procedures, but continues to run timers that may apply, e.g. the periodic timer for location update.

Editor's note: Whether the NG_POWER-SAVING state shall be considered as a substate of NG_IDLE state is FFS.

Editor's note: This solution focuses on the states assuming UE is registered to the network. States needed when the UE is deregistered is FFS.

Editor's note: The relation between RRC states, and the added "MM" states is FFS.

Editor's note: The relation to power saving mechanisms similar to extended DRX is FFS.

6.3.6.2 Function description

The mobility states and state transitions of core network for UE with power consumption optimization are modelled as shown below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 153 of 501

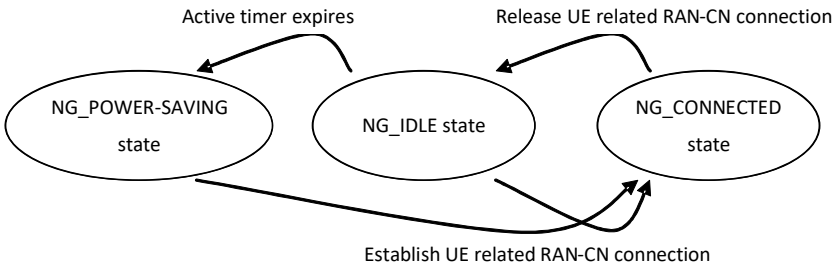


Figure 6.3.6.2-1: Mobility states and state transitions

If a UE is capable of adopting a NG_POWER-SAVING state and it wants to use the NG_POWER-SAVING state, it shall negotiate the related parameters with Control plane functions, e.g. MM function. And the parameters applied to NG_POWER-SAVING state maybe include the Active Time for entering NG_POWER-SAVING state and periodic timer for location update.

Editor's note: It is FFS how and when such parameters are negotiated.

When the UE-RAN connection is released, the state changes from connected state to NG_IDLE state, and the UE and the Control plane functions start the Active Timer with the Active Time value. When the Active Timer expires in the UE, the UE deactivates its Access Stratum function and enters the NG_POWER-SAVING state, only running the necessary timers. And if the Active Timer expires in the Control plane functions, the Control plane functions know that the UE entered NG_POWER-SAVING state and is not available for paging. When mobile originated events like data transfer or signalling happens, the UE can return from NG_POWER-SAVING state to NG_CONNECTED state after the CN-RAN connection is established.

6.3.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.7 Solution 3.7: NextGen State Model

6.3.7.1 General

This solution addresses Key Issue#3, Mobility Management framework, in particular related to work tasks #1 and #2.

6.3.7.2 Architecture description

6.3.7.2.1 NextGen Mobility Management (NMM)

Irrespective whether or not network slicing is used, there is at any point in time at most one NAS control-plane anchor per UE, operating a single NG Core/NMM instance for this UE.

Three states are defined.

- **NMM De-registered**: The UE is not attached to the network and is not reachable. The UE location is not known by the network (except possibly through the last registration if applicable).
- While NMM De-registered, the UE in lower layer (RRC) may be in Initial state, Low Energy state (transient) or High Performance state (transient), see sub-clause 6.3.7.2.3.
- NMM Registered: The UE is attached to and authenticated by the network. A NG1 connection is established. The UE is reachable by the network (subject to radio access reachability) though maybe not immediately (e.g. DRX). The UE location is maintained by the network at NAS CP Anchor Area level, NG RAN Node level and/or Cell level, possibly triggered by updates from the UE. Mobility is handled by means of cell reselection or handover depending on mobility requirements imposed, when applicable, by the QoS requirements of the ongoing service.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 154 of 501

- **NMM Registered Standby:** No NG2 or NG3 connections are established. Mobility is handled by the UE by means of cell reselection. The NG Core tracks the UE location at NAS CP Anchor Area Level. Paging is handled by NG Core, within the NAS CP Anchor Area. The lower layer (RRC) is in RRC Low Energy state maximizing battery efficiency, see sub-clause 6.3.7.2.3. The lower layer (RRC) may also be in RRC High Performance state to expedite transmission of NAS signalling.

- **NMM Registered Ready:** a NG2 connection is established. A NG3 connection is established upon data transmission, or if an RRC connection is established, for the duration of the RRC connection. Mobility is handled by means of cell reselection (no ongoing service or, with an ongoing service, if suitable according to the corresponding QoS requirements), or handover (when imposed by QoS requirements of the ongoing service). The NG Core tracks the UE location at NAS CP Anchor Area and NG RAN node levels. The NG RAN tracks the UE location at cell level. Paging is handled by NGRAN upon incoming data from NG Core. The lower layer (RRC) is either in RRC Low Energy state maximizing battery efficiency or in RRC High Performance state maximizing data efficiency, see sub-clause 6.3.7.2.3.

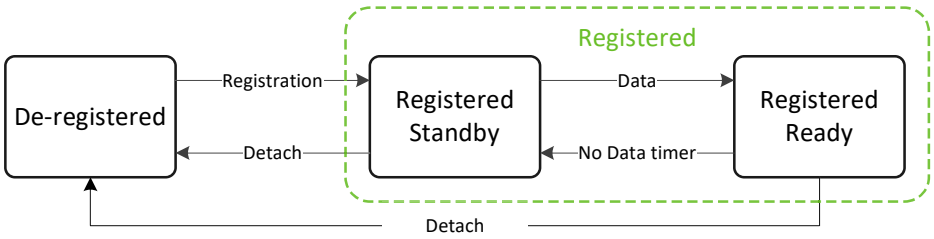


Figure 6.3.7.2.1-1 NMM State Model

Editor's note: state transitions will be detailed.

6.3.7.2.2 Void

6.3.7.2.3 NextGen Radio Resource Control (RRC)

Editor's note: decision on the RRC state model is under TSG RAN WG2 responsibility.

Three states control the operation and mobility of the UE in lower layers.

- **RRC Initial:** This state is supported by the UE only, to set-up operation. It is short-lived. NMM is NMM De-registered and no RRC connection is established. The UE performs initial cell and PLMN selection. Once a suitable or an acceptable cell is selected, the UE enters RRC Low Energy state. The UE stays in Initial state when no service can be had.

- **RRC Low Energy:** No RRC Connection is established between the UE and NGRAN. NMM may be NMM De-registered (transient), NMM Registered Standby or NMM Registered Ready. In this state, the UE battery consumption is optimized (deep sleep, DRX as applicable) and, when NMM Registered Ready, RRC connection-less (CP/UP) data transfer is possible.

  - If the UE is NMM De-registered, MT/MO transactions are not possible. This is expected to be transient only.

  - If the UE is NMM Registered, both MT and MO transactions are possible. RRC Connection-less data transfer is enabled if in NMM Registered Ready.

  - Mobility is handled by means of cell reselection, under UE control. Handover is neither needed nor supported. The UE location is known at cell level at least for the duration of data transfer while in NMM Registered Ready state, otherwise at NAS Control Plane anchor area level while in NMM Registered Standby State.

  - This state relies on pre-established centralized and distributed contexts e.g. for security and compression (centralized) and for radio communications (distributed) hence avoiding any further handshake for context set-up. It uses on-the-fly provision of additional information as needed e.g. UE capabilities (beyond a minimum set), QoS marking etc. In addition, UE context transfer is supported in the network for mobility.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 155 of 501

Editor's note: Whether the centralization of stateful network functionality (e.g. for UP security, compression) for RRC Low Energy lies in NG Core or in NGRAN is FFS and will be addressed in sub-clause 6.3.7.3.

- **RRC High Performance:** An RRC connection is established between the UE and NGRAN. The UE may be NMM De-registered (transient, e.g. performing registration) or NMM Registered Standby (transient e.g. requesting service) or NMM Registered Ready. In this state, data efficiency is optimized while the battery consumption is reduced in temporary periods of inactivity (DRX).

  - Both MT and MO transactions are possible.

  - Mobility is handled by means of handover, under network control. The UE location is known at cell level.

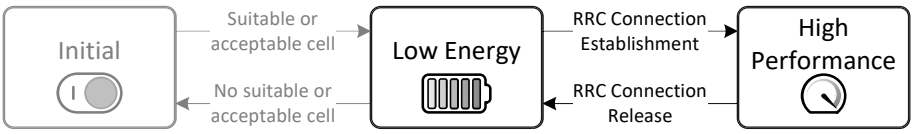


Figure 6.3.7.2.3-1 RRC State Model

NOTE: in this solution, an RRC Connection is assumed to be both logical and physical i.e. radio resources are assigned to the UE. RRC connection-less can be assumed as a logical connection exists.

6.3.7.2.4 Overview of NMM, and RRC state models

The following table summarizes the overall correspondence between NMM and RRC.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 156 of 501

Table 6.3.7.2.4-1 Overview of NMM, NCM and RRC State models

Correspondence RRC - NMM States

NMM / RRC	NMM De-Registered	NMM Registered	
		Standby	Ready
RRC Initial	Yes	No	No
RRC Low Energy	Transient	Yes	Yes
RRC High Performance	Transient	Transient	Yes

Mobility

NMM / RRC	NMM De-Registered	NMM Registered	
		Standby	Ready
RRC Initial	PLMN selection Cell (re)selection	n/a	n/a
RRC Low Energy	Cell reselection	Cell reselection	Cell reselection
RRC High Performance	n/a	n/a	Handover

UE Location tracking

NMM / RRC	NMM De-Registered	NMM Registered	
		Standby	Ready
RRC Initial	n/a	n/a	n/a
RRC Low Energy	n/a	NGCore: NAS CP Anchor Area NGRAN: n/a	NGCore: NAS CP Anchor Area, NGRAN node NGRAN: Cell
RRC High Performance	n/a	n/a	NGCore: NAS CP Anchor Area, NGRAN node NGRAN: Cell

Paging

NMM / RRC	NMM De-Registered	NMM Registered	
		Standby	Ready
RRC Initial	n/a	n/a	n/a
RRC Low Energy	n/a	NGCore	NGRAN
RRC High Performance	n/a	n/a	n/a

NGx connections

NMM / NGx connections	NMM De-Registered	NMM Registered	
		Standby	Ready
NG1 Connection	n/a	Yes	Yes
NG2 Connection	n/a	No	Yes
NG3 Connection	n/a	No	Yes and No

6.3.7.3 Functional description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.3.7.4 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.8 Solution 3.8: Simplified mobility states for stationary UE and MO data transmission only UE

This solution addresses some tasks of key issue #3, i.e. MM_WT_#2, 2.2 Registration state model and MM_WT_#3, 3.2 Connection state models.

6.3.8.1 Architecture description

For some low complexity UEs which are static or quasi-static, or support MO (mobile originated) data transmission only, their mobility states set can be simplified as followed:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 157 of 501

NG_NAS states:

- NG_NAS_REGISTERED state: the UE is attached/registered to the CN successfully, and establishes a signalling connection with the CN.

NOTE1: This state can be considered as the combination of EMM_REGISTERED and ECM_CONNECTED states.

- NG_NAS_DE-REGISTERED state: the UE is not attached/registered to CN (Core Network).

NOTE2: This state can be considered as the combination of EMM_DE-REGISTERED and ECM_IDLE states.

NG_RAN states:

- NG_RAN_CONNECTED state: the UE establishes signalling/data connection(s) with RAN (Radio Access Network).

- NG_RAN_INACTIVE state: the UE has no signalling/data connection(s) to RAN. In this state, the attached or registered UE can monitor RAN paging and/or initiate RRC connection establishment.

Editor's note: the specific state names may be updated further.

With such refined mobility states, the state transitions can also be simplified.

6.3.8.2 Function description

6.3.8.2.1 Mobility states and corresponding transitions of stationary UE

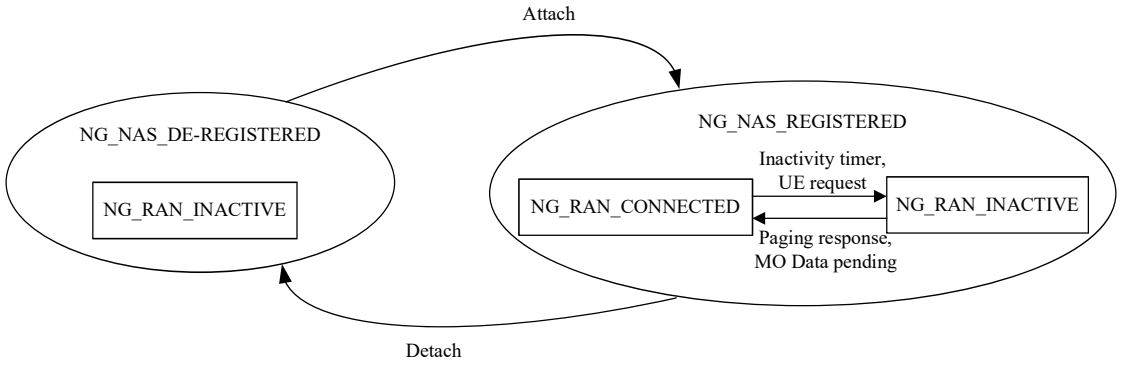


Figure 6.3.8.2.1-1: Mobility states and corresponding transitions for stationary UE

Before a UE is attached/registered to CN, it is in NG_NAS_DE-REGISTERED state and NG_RAN_INACTIVE state.

After the UE registered to the network, it enters NG_NAS_REGISTERED state which may be the combination of EMM_REGISTERED and ECM_CONNECTED states. In the NG_NAS_REGISTERED state, the UE always keep a signalling connection to the CN. Hence, from CN perspective, this UE is always CONNECTED.

During the registration procedure, the signalling connection between UE and RAN is established, as well as signalling connection between CN and RAN, and then the UE enters NG_RAN_CONNECTED. However, after the registration, the UE may enter NG_RAN_ INACTIVE state. The criteria used by RAN to move UE into NG_RAN_INACTIVE may include e.g. inactivity timer based mechanise, or upon UE requested radio link release, but this is left to RAN decision.

NOTE: Data path between the UE and the CN is established/released during the attach/detach procedure unless the data transmission between the UE and the CN is via connectionless signalling.

Once the UE enters NG_RAN_ INACTIVE state, no signalling connection and data path between the UE and RAN are existing. In this case, if there are downlink signalling/data arrival, it will be buffered in RAN node, and paging over the air interface is then triggered. Upon receipt of paging, the UE initiates procedure to re-establish signalling connection and/or data path between UE and RAN. Those re-established RAN connections would be connected with corresponding RAN-CN connections existed.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 158 of 501

6.3.8.2.2 Mobility states and corresponding transitions of MO data transmission only UE

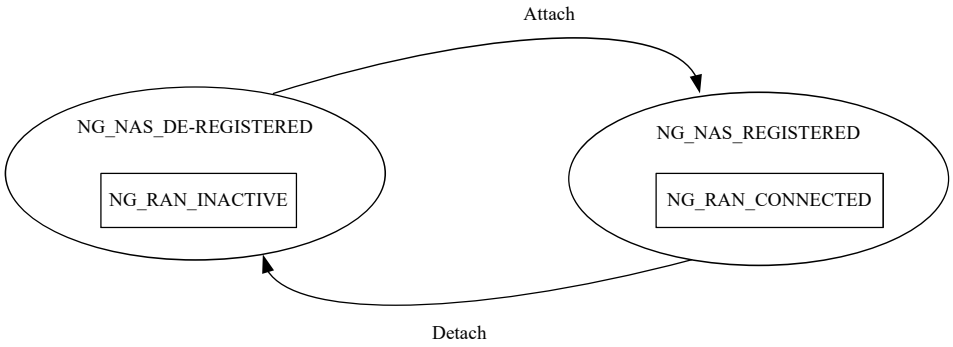


Figure 6.3.8.2.2-1: Mobility states and corresponding transitions for MO data only UE

For a UE only sending MO data, if it has data pending, it initiates attach/registration procedure and establishes signalling connection toward the CN. Then the UE enters NG_NAS_REGISTERED state. While the UE is attached/registered to the CN, the signalling connection between the UE and RAN is established, thus the UE enters NG_RAN_CONNECTED as well. The UE is always kept in NG_RAN_CONNECTED state until the transmission of MO data is completed.

NOTE 1: Data path between the UE and the CN is established/released during the attach/detach procedure unless the data transmission between the UE and the CN is via connectionless signalling.

NOTE 2: The UE in NG_NAS_REGISTERED state may receive downlink data via signalling connection or data path.

After completing the MO data transmission, the UE will detach from the network, release the signalling connections towards RAN and CN, and then enter NG_NAS_DE-REGISTERED state and NG_RAN_INACTIVE.

6.3.8.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.9 Solution 3.9: Mobility levels using Mobility and Session classes

This solution addresses the Mobility Levels part of 'Key Issue 3: Mobility Framework' and 'Key issue 6: Support for session and service continuity'. The solution introduces a mechanism for operator control of mobility support and session support over the evolved LTE access and the new 3GPP 5G RAT.

6.3.9.1 Architecture description

For mobility on demand, the NG Subscriber Data Management defines the subscribed base level(s) of mobility support for the UE and the NG Policy Control possibly adjust the subscribed level due to varying conditions e.g. geographical location, time and date. The NG Core Control Fcn NG CCF receives mobility level related subscription information from the NG Subscriber Data Management. The information is optionally (e.g. not for CIoT) sent to and adjusted by the NG Policy Control. It is the responsibility of the serving NG Core Control Fcn to enforce the mobility level(s) as received from the NG Policy Control.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 159 of 501

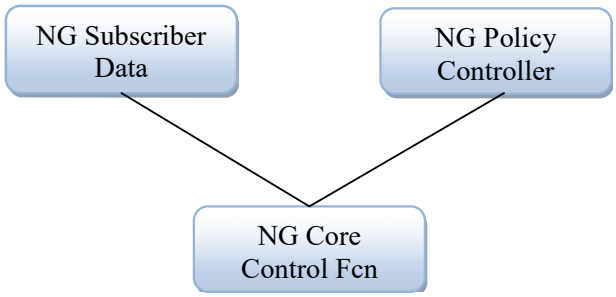


Figure 6.3.9.1-1: High-level architecture principles for operator controlled mobility levels

6.3.9.2 Function description

The most impact on a network due to a UE performing mobility is related to handling of PDU sessions and particularly for a UE being in connected mode. But even for a UE that is being registered without any PDU sessions mobility will induce load upon the network. The larger allowed area for a UE the more mobility and the higher probability of inter CN node mobility and thereby higher load upon the network. It is therefore proposed to have a separate mechanism for granting and controlling the allowed area of mobility support i.e. for this mechanism disregarding any impact from PDU session(s). Treating the mobility impact separately means that a separate mechanism is needed also for granting and controlling the level of mobility support related to a PDU session, thus allowing individual treating of different PDU sessions. It is proposed to introduce a Mobility class and a Session class:

- Mobility class
  Describes the level of mobility support for a UE. The Mobility class is purely related to impact from mobility for a UE as if the UE wouldn't have any PDU sessions, therefore one Mobility class per UE is needed.

- Session class
  Describes the level of mobility support for a UE's PDU sessions. The Session class is related to impact from mobility for a UE taking only the PDU session impacts into consideration. One Session class per PDU session is needed.

6.3.9.2.1 Mobility classes

By dividing the size of the allowed geographical area for the subscriber into a few sub-ranges it is possible to e.g. form the following Mobility classes:

A. Unlimited (or high) mobility
   No (or minor) restrictions upon the allowed geographical area e.g. used by MBB users.

B. Low mobility
   The allowed geographical area is limited e.g. used for stationary subscribers. The size could e.g. be limited to 5 TAs.

C. No mobility
   The allowed geographical area is limited e.g. used for users accessing the network only via a fixed point (having their own access network with possible mobility). The size could e.g. be limited to 1 TA.

NOTE 1: Additional Mobility classes can be added, if needed.

It is proposed that Tracking Area gives the granularity for the allowed area. Optionally all or parts of the allowed TAs may be configured in the Subscriber Data Management.

While the Mobility classes represents white lists (i.e. allowed areas) it shall still be possible to use black lists (e.g. roaming restrictions) and in case of overlapping the blacklisting taking precedence over the whitelisting.

The UE is expected to not communicate with the network when outside of the allowed geographical area, and the network is expected to e.g. reject a mobility TAU if sent outside of the allowed geographical area.

NOTE 2: Periodic tracking area updates can be allowed outside the allowed geographical area because this information at the network could be used for some kind of services, e.g. tracking of stolen devices or to push an update of Mobility class.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 160 of 501

6.3.9.2.2 Session classes

Based on the mobility procedures it is possible from a service point of view to have different types of establishment of the SM resources: Session pre-setup (i.e. Mobility with pre-setup), and Session post-setup (i.e. Mobility with post-setup). Pre-setup means that the SM resource(s) during a mobility procedure are established in advance in the target side (like handover in LTE) while at post-setup the SM resource(s) are established after the UE has moved to the target side (like setup after idle mode mobility in LTE). UEs that can and are allowed to benefit from (based on subscription and UE capability) SM resource establishment in advance of mobility belong to the Session pre-setup class and UEs that cannot or are not allowed to benefit from (based on subscription and UE capability) SM resource establishment in advance of mobility belong to Session post-setup or No PDU session classes. UEs that cannot use or are not allowed to use (based on subscription and UE capability) PDU sessions belong to the No PDU session class.

Using these terms it is possible to form three different Session classes:

A. Session pre-setup:
   Mobility with pre-setup of PDU session (SM resources established in advance in the target side i.e. equivalent to handover procedures).

B. Session post-setup:
   Mobility with post-setup of PDU session (SM resources established after the UE has moved to the target side i.e. equivalent to cell re-selection/idle mode mobility procedures).

C. No PDU session:
   No PDU session is allowed for the UE

NOTE: The Session classes can be applied independently from the Mobility classes.

6.3.9.2.3 Assigning, controlling and enforcing Mobility and Session classes

As individual UEs may have different levels of mobility support the subscribed base level(s) is defined in a subscriber database, NG Subscriber Data Management, and is possible to adjust (e.g. due to varying conditions such as UE's location, UE capabilities,application in use, time and date) by NG Policy Control.

First NG CCF, receives the level(s) of mobility subscription information from the NG Subscriber Data Management. The information is then optionally adjusted by the NG PC. The NG PC may raise the mobility level(s) above the level(s) given by subscription information. This could e.g. be useful at sponsored situations or at change between a local network and a macro network. It is the responsibility of the serving NG CCF to enforce the mobility level for the user as received from the NG PC. At initial registration the NG CCF provides the UE with the Mobility class i.e. the size of the allowed area and with any possibly configured allowed TAs as received from the NG Subscriber Data Management. Additional allowed TAs may optionally have been added by NG PC. While the UE is connected to the network, any registered and not yet allowed TA is added to the UE list of allowed TAs until the maximum allowed number of TAs is reached.

The NG PC, and NG SDM may trigger an update of the Mobility and Session classes at any time but the new classes are only provided to the UE when the CN anyway signals to the UE e.g. when connecting to the network. The UE shall not be paged solely due to change of Mobility or Session class.

Using different service levels for different PDU sessions means that all PDU sessions shall not necessarily be included in a pre-setup of resources at connected mode mobility (i.e. Handover in LTE). It is proposed that the NG CCF informs the RAN about the support (i.e. whether a PDU session at mobility shall be pre-setup or not).For a UE that is only allowed to access the network within a restricted part of the service area the NG CCF will inform the UE about the allowed TAs. And as a preventive measure the list of allowed TAs (in the form of a white or black list) may be sent to the UE already at registration of the UE in the NG CCF i.e. at Attach or TAU accept. In this way registration attempts in vain could be avoided.

For a UE in connected mode having only PDU sessions with service level Session post-setup, pre-setup of resources at mobility is not required. For such cases the NG CCF informs the RAN that pre-setup of resources is not allowed (thus not triggering e.g. handover). For 'No mobility' NG CCF informs the RAN that handover is only allowed within the TAI-list or TA area. A similar mechanism (i.e. informing RAN about allowed area) could also be used for Low mobility enforcement.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 161 of 501

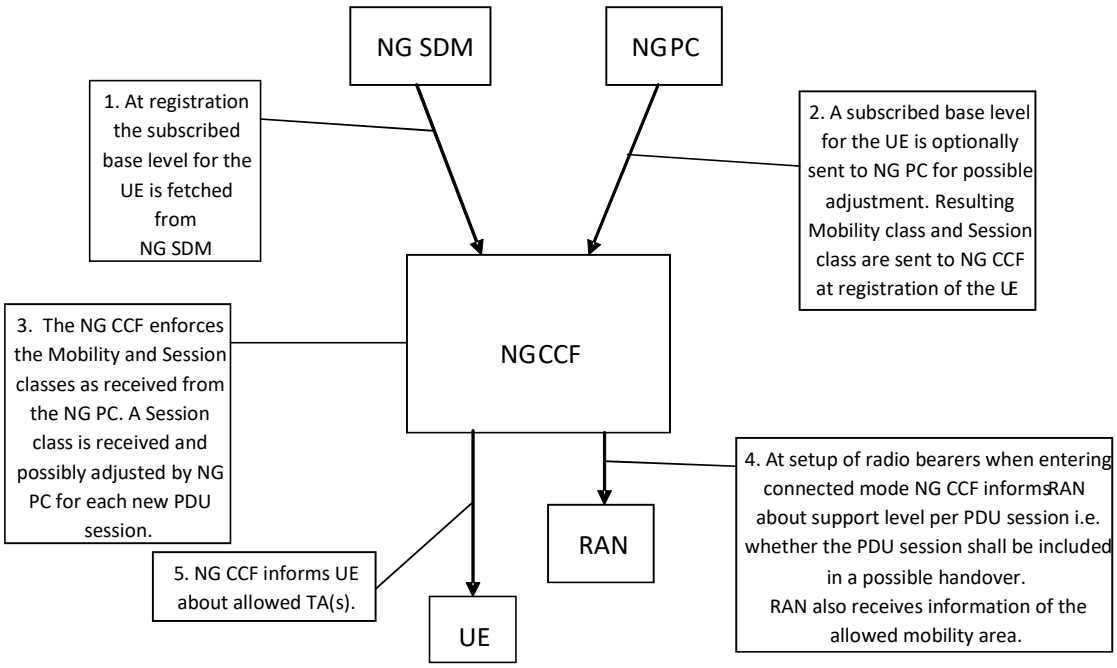


Figure 6.3.9.2.3-1: Assigning, controlling and enforcing Mobility and Session classes

6.3.9.2.4 Mobility aspects and how to handle roaming

When due to mobility a UE changes NG CCF, the list of allowed TAs, Mobility class and Session Class(es) may be transferred to the new serving NG CCF from the source NG CCF and optionally be adjusted by the serving NG PC.

In addition to the data transferred between the NG CCFs, when entering a visited network the subscribed Mobility and Session classes are transferred from the SDM via the serving NG CCF to the serving NG PC in the visited network but shall not put any constrains upon the selection of Mobility and Session classes in the visited network. For local breakout no load will be put on the nodes in the home network (except for fetching subscription data) and it is therefore anticipated that the model used for a UE in the home network is applicable also for that case. For home routed traffic it is expected that the visited network will still have a local NG User plane Fcn, NG UPF, for handling the user plane and that it is the local NG UPF that may change at mobility. The primary load will thus be put on the local NG CCF and local NG UPF and it is therefore proposed that handling of the SM classes in the visited network only needs to be performed by the local NG CCF and local NG UPF.

The SM classes will, as mentioned above, optionally be determined by the NG PC in the visited network and only based on the subscribed levels and local policies.

There will be no interaction between the NG PC in the visited network and the NG PC in the home network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 162 of 501

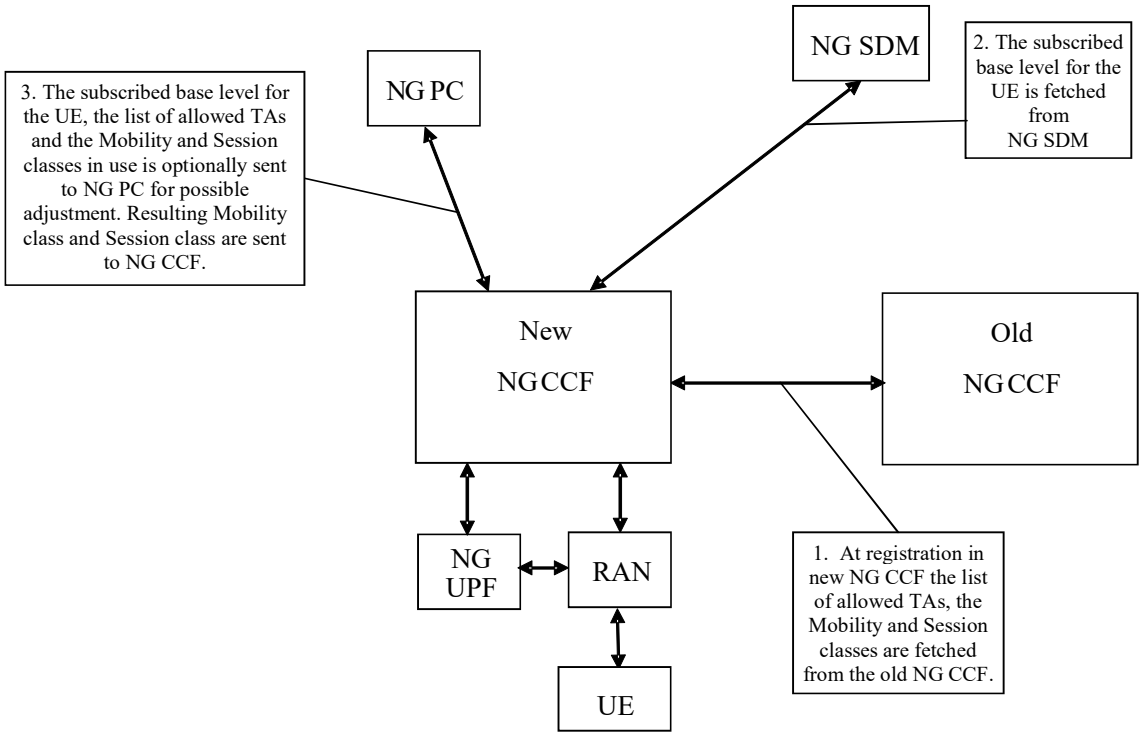


Figure 6.3.9.2.4-1: Mobility aspects and how to handle roaming

6.3.9.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.10 Solution 3.10: RAN Specific paging for UE in CN connected mode.

This solution addresses MM_WT_#2, UE reachability management, of Key Issue#3.

6.3.10.1 Architecture description

For UE in CN_CONNECTED state, the user plane path and signalling path for this UE has been established between the NexGen Core and the NexGen RAN. That is, the NG2 connection and NG3 connection for this UE always exist once this UE enters CN_ CONNECTED state, but the UE may be in RRC_INACTIVE state or RRC_IDLE state. Before actual data/signalling transfer, the UE should be brought back to RRC_CONNECTED. However, UP function and CP function of the NexGen Core are not aware of actual UE's RAN state.

DL data and MT signalling message could be sent directly to the NexGen RAN by the NexGen Core UP and CP function, and the RAN Specific Paging is triggered if the UE is in RRC-INACTIVE or RRC_IDLE state. In this case, DL data and MT signalling message is buffered in the NexGen RAN.

NOTE: When a UE in RRC_INACTIVE state or RRC_IDLE state moves into the area served by a new RAN node, if the coordination between the new RAN node and anchoring RAN node which has NG2 and NG3 connections for this UE is supported, then the anchoring RAN node receiving DL data or MT signalling message will cooperate with new RAN node for paging the UE. However, if the coordination between new RAN node and anchoring RAN node is not supported, the new RAN node needs to initiate the establishment of NG2 and NG3 connections.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 163 of 501

6.3.10.2 Function description

6.3.10.2.1 Downlink NG1 Signalling Triggered RAN Specific Paging.

If there is downlink signalling for a UE in CN_CONNECTED state, the NexGen Core sends the DL signalling message to the NexGen RAN via NG2. If the UE is in RRC-INACTIVE or RRC_IDLE state, the RAN Specific Paging is triggered, and the DL signalling message is buffered in RAN until UE come back to RRC_CONNECTED state.

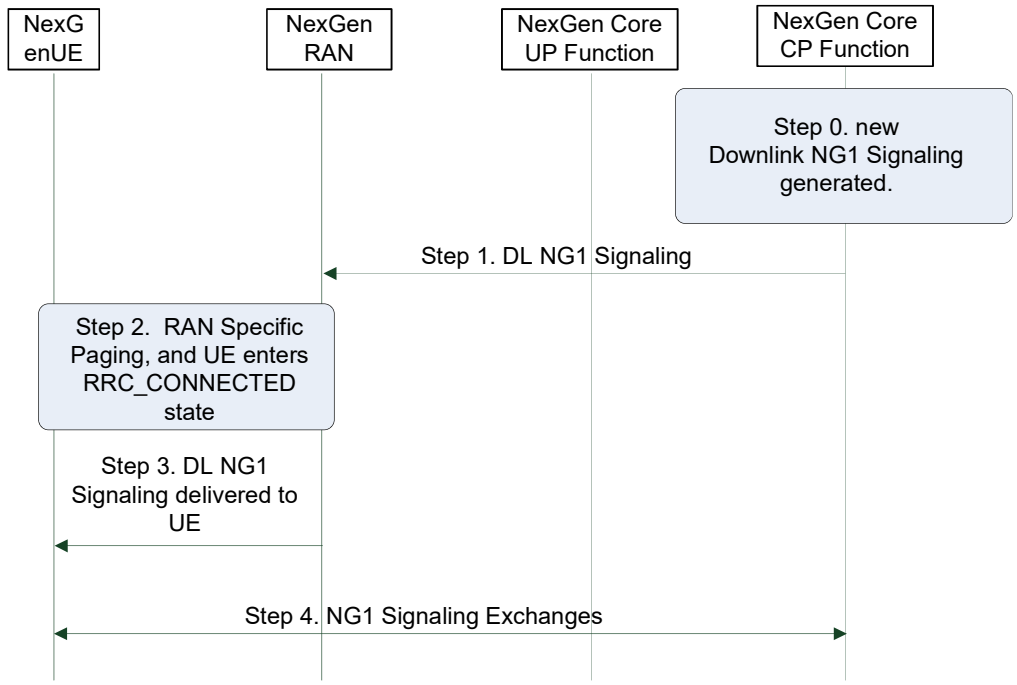


Figure 6.3.10.2-1: Downlink NG1 signalling transport

0. The NexGen Core CP function wants to send NG1 signalling to UE.
1. The NexGen Core CP function sends the DL NG1 signalling message to NexGen RAN via NG2.
2. If the UE is in RRC_INACTIVE or RRC_IDLE state, the NexGen RAN buffers the DL NG1 signalling message and then performs RAN Specific Paging. This procedure brings the UE back to RRC_CONNECTED state.

NOTE 1: The RAN Specific Paging procedure is defined by RAN WGs.

3. Once the UE is back to RRC_CONNECTED state, the buffered the DL NG1 signalling message would be delivered to UE.
4. The NexGen Core CP function and UE can then ex-change NG1 signalling.

6.3.10.2.2 Downlink NG3 data Triggered RAN Specific Paging

When there is downlink data arriving at the NexGen Core UP function, the NexGen Core UP function directly pass those data to NexGen RAN. The NexGen RAN will buffer DL data if the UE is in RRC_INACTIVE or RRC_IDLE state, and initiates RAN Specific Paging procedure to bring UE back to RRC_CONNECTED state. Once succeed, the NexGen RAN deliver buffered data to UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 164 of 501

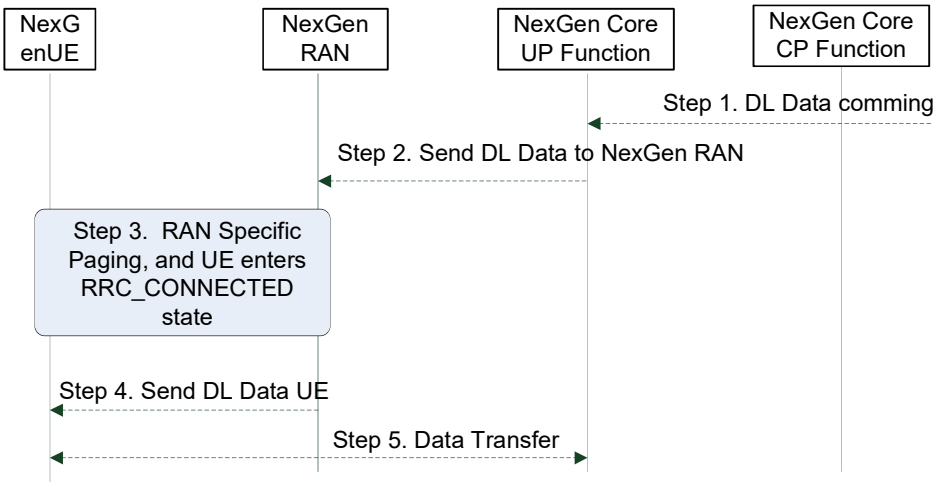


Figure 6.3.10.2-2: Downlink NG3 data transport

1. The DL Data arrives at the NexGen Core UP function, the NexGen Core UP function forward received data to NexGen RAN via existing NG3 tunnels.The DL Date is buffered at NexGen RAN.
2. The NexGen RAN checks the UE RAN state, if the UE is RRC_CONNECTED, then step 6 is preformed. Otherwise, step 3 is the next step.
3. The NexGen RAN performs RAN specific paging, and bring the UE back to RRC_CONNECTED state.
4. The NexGen RAN sends DL data to the UE.
5. The UE and the NexGen Core UP function start data transfer.

6.3.10.2.3 Core Network Assisted RAN Specific Paging Retry

Editor's note: This is a potential solution as it is expected that RAN WG will come up with specific RAN paging mechanisms. Details and final decision on this solution can be discussed together with RAN WG.

When RAN specific paging is applied, the signalling or data packet is buffered in NextGen RAN. If RAN paging cannot reach the target UE, e.g., due to unsuccessful paging coordination within RAN paging area or UE's movement without proper NG2/NG3 reestablishment, packet loss can happen. CN assisted paging retry procedures can be used to compensate the failure on RAN specific paging. RAN may transmit the paging request to the core network when the NextGen RAN node cannot reach the target UE by RAN specific paging, and CN initiates paging.

Figure 6.3.10.2-3 depicts the procedures for CN assisted paging retry after RAN specific paging fails.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 165 of 501

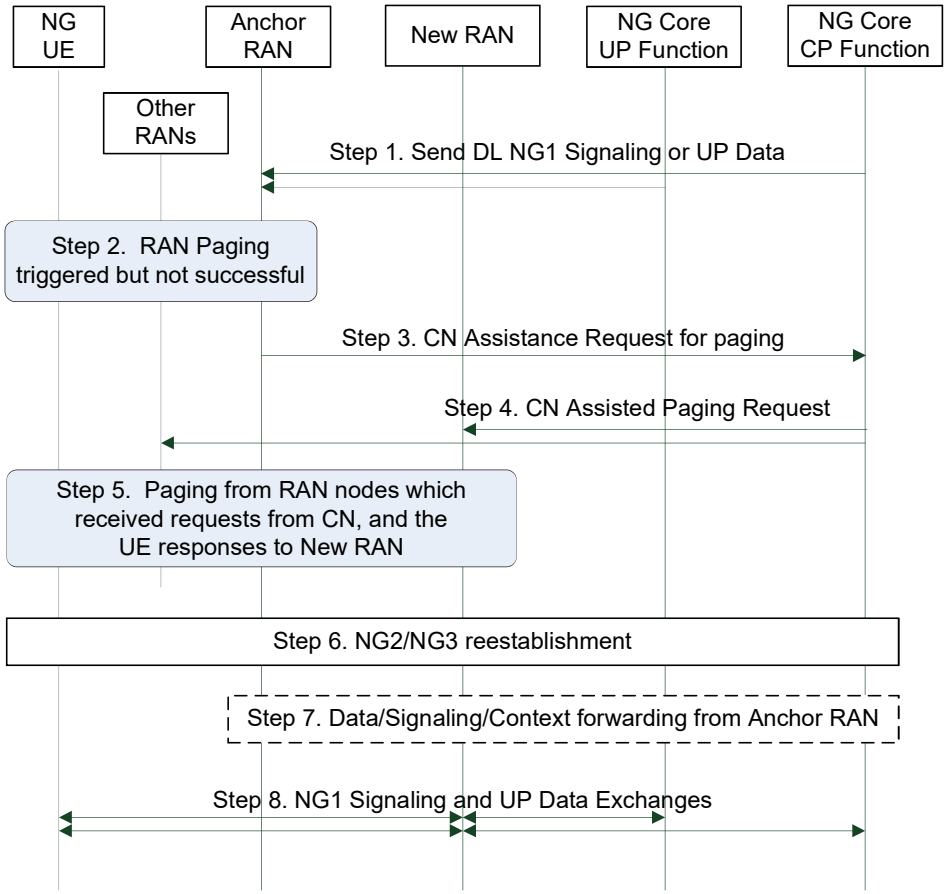


Figure 6.3.10.2-3: CN assisted paging after failure of RAN specific paging

1. NG1 signaling or UP data is generated and forwarded to the anchor NexGen RAN. The DL signaling messages or data packets are buffered at the anchor RAN.

2. Anchor RAN triggers RAN paging which may include the paging coordination between some RAN nodes, but the paging does not successfully reach the UE.

NOTE 2: The detailed coordination between RANs for RAN Specific Paging procedure is defined by RAN WGs.

3. The NexGen RAN request CN assistance for paging. The request message may include some additional information, e.g., RAN paging area information, last activated cell etc.

4. Based on the request from RAN, CN decides target paging area and sends CN Assisted Paging Request message to the RAN nodes within the target paging area.

5. RAN nodes which received the CN assisted RAN paging request perform paging. The target UE camping on the new RAN responses to the paging request, and this procedure brings the UE back to RRC_CONNECTED state.

Editor's note: CN may retrigger RAN specific paging based on RAN's control information provided in Step 3 or may reuse some parts of normal CN initiated paging used, but the detailed procedure is FFS.

6. NG2/NG3 connections for the UE can be re-established with new RAN and CN functions.

7. Forwarding of signaling and/or data packets and/or context information from Anchor RAN to New RAN may be performed.

Editor's note: How detailed recovery and forwarding mechanisms operate is FFS, e.g., reuse of handover procedure defined in NextGen.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 166 of 501

8. The UE and the NextGen CN functions continue data and signalling transfer.

6.3.10.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.11 Solution 3.11: Solution for dynamic mobility management

This is a solution to Key issue 3: Mobility framework, MM_WT_#3, in particular related to the issue "6. How to save resources for UEs that do not require full mobility?"

In this solution, both an approach that uses the traditional TAs and an approach that uses UE specific cell lists is described with the expectation that a choice will be made for the normative phase.

6.3.11.1 Mobility categories

The NextGen system should support the following mobility categories:

- **No mobility:** the UE is connected to the NextGen Core Network without need or ability for any change in point of attachment by means of a single cell ,a fixed line, a residential gateway or a WLAN hot spot with a wired or a wireless backhaul. The key point is that devices connected to the mentioned accesses are not capable or allowed to execute inter-access node or inter-system mobility procedures, i.e. they cannot or are not allowed to leave such accesses without losing connectivity with the NextGen Core Network.

- **Restricted mobility:** the allowed geographical area (e.g. defined by a set of tracking areas or a set of cells) is limited , specific to a UE, and known by the UE (by means of pre-configuration and/or signalling), i.e. the UE is permitted to move only within the allowed geographical area(i.e. assign a new TA list or cell list to the UE). At any time the network can update the UE with a new allowed geographical area. The UE is permitted to send signalling to the network only within the allowed geographical area, and the signalling received from the UE outside the allowed geographical area may be rejected by the network with an appropriate cause value.

NOTE: Periodic area updates can be allowed outside the allowed geographical area because they could be used e.g. for updating the UE with a new allowed geographical area or for tracking of stolen devices.

- **Unrestricted mobility:** no limitations upon the allowed geographical area are pre-set, i.e. the UE can move to any cell of the serving network.

NOTE: Whether the allowed geographical can contain cells belonging to roaming partners of the home network operator and/or non-3GPP access nodes – possibly within private or corporate ownership - is FFS.

6.3.11.2 Functional description

For "no mobility" mobility category the UE doesn't receive any list of tracking areas/cells when it connects to the network and the UE is not requested to perform regular updates: CN IDLE mode is not applicable to those UEs; implicit (e.g., the network knows the UE is connected using a fixed line or a certain cell) or explicit signalling from the UE is used by the network to identify this category.

When in CONNECTED mode UEs belonging both to the "unrestricted mobility" and the "restricted mobility" category are tracked by the network across their individually assignedareas, which may consist of many cells.

From the dynamic mobility management in IDLE mode perspective the "unrestricted mobility" and the "restricted mobility" categories behave the same way, as will be described in section 6.3.11.2.1: the only difference is in the need of an enforcement of the restrictions with respect to the allowed point(s) of attachment (e.g. the allowed cells) for the "restricted mobility" category.

6.3.11.2.1 Dynamic mobility management in IDLE mode

When the UE is in IDLE mode, the network assigns the list of tracking areas/cells and the timers for the periodic update of the list based on an algorithm that learns from the UE behaviour, i.e. the UE mobility pattern. As long as the UE stays within the same set of cells (as defined by the assigned TA list or cell list), the network progressively shrinks the list of tracking areas/cells assigned to the UE, i.e. where the UE can move without performing any update signalling; at the same time the network increases the time required for the next periodic tracking area/cell list update, i.e. the network progressively fine tunes the parameters in the algorithm to assign the list of tracking areas/cells and the timers for the

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 167 of 501

periodic updating. For example, if at a certain point in time the UE becomes almost stationary then the network updates the UE at each tracking area/cell list update with a list of tracking areas/cells that becomes smaller and smaller; if the UE becomes completely stationary the list could collapse to just one tracking area/cell or a small set of few neighbouring cells. Based on the same analysis of the mobility pattern, the network could provide the UE with periodic update timers that becomes longer and longer, until the need for the periodic update is completely suspended.

The savings are expected in terms of paging resources, UE power consumption, network signalling load and avoiding the complexity of having in the network different configurations to manage almost static, low mobility and high mobility devices, at the price of the computational effort to adapt the list of cells/tracking areas and the periodic cell list/ tracking area update timers to the UE behaviour.

When the UE in IDLE mode moves beyond the border of the assigned tracking area/cell (s), it shall perform a mobility tracking area /cell list update to continue to be reachable by the network: that update triggers the network to reset the parameters in the algorithm used to assign the list of tracking areas/cells and the timers for the periodic update to values corresponding to a full mobility pattern.

The above mentioned optimized algorithm can be a feature of the NG System, further developed and standardized in 3GPP– especially aiming at heterogeneous network access both regarding technology (e.g. 3GPP and non-3GPP) and access node features (e.g. temporary operation and moving nodes).

6.3.11.2.2 Differences from existing solutions

Firstly, three different mobility levels are defined for NextGen UEs that do not exist in this fashion in current networks.

For the TA based solution, it enables the network to provide adaptive management of TA list assignment and tracking area update timers per UE.

The cell list solution further enhances the TA based solution by allowing to assign individual cell lists per UE, whereas in the TA based solution, all UEs in the same TA use the same cell list. Thereby each UE can use its specific area - with a finer granularity than TAs - for paging and location updating. This also implies that the area boundary is different for each UE. Therefore, one particular advantage of the solution is that signalling storms of many UEs changing TA at the same time (e.g. train emerging from a tunnel) can be avoided.

With the cell list solution, it is not necessary to manage TAI on the RAN level, i.e. no TAI is broadcasted by the RAN nodes. The cell list is maintained in the CN for each UE, and transmitted to the UE (in place of a TA list) via NAS signalling.

Maintaining the TA list or cell list assignments can be handled by the MM function, or by an external repository such as the shared data layer or UDM, which the MM function can query if it needs to page the UE. Any processing algorithm that may be employed to dynamically fine tune the TA/cell list assignment can be implemented in the MM function or in an "external" network function.

The traditional TA approach can also be emulated with the cell list solution, by assigning predefined sets of cells to "areas" in the same way as TA planning is done today. In this case, the same cell list would be assigned to UEs that camp on the same cell rather than individual lists to each UE, thereby sacrificing some of the advantages of the solution for the sake of, at least initially, maintaining today's network planning approach. It can be envisaged that this approach would be the default, without or prior to applying any tuning algorithm that would subsequently make the cell list UE specific based e.g. on UE behavior analysis.

6.3.11.3 Solution Evaluation

Editor's note: This clause will contain evaluation on the system impacts.

6.3.12 Solution 3.12: Solution for UE reachability in power saving state

6.3.12.1 Architecture description

This solution addresses Key Issue #3, and in particular MM_WT_#2 (UE reachability management). It is similar to the ePSM solution described in TR 23.709 clause 5.8.

This solution can be equally applied to the "Connected Inactive" state (a.k.a. "RRA_PCH" in solution 2.3) or to the CN_Idle state (if supported), and is orthogonal to the discussion on whether CN_Idle state needs to be supported in the NextGen system.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 168 of 501

This solution proposes to define an enhanced Power Saving Mode (ePSM) as follows:

- Based on network configuration when in "Connected Inactive" or "CN_Idle" state the UE can alternate between successive Reachability interval (T_{Reach}) and Power Saving Mode (PSM) interval (T_{PSM}) that are repeated periodically.
- The period of the repetitive Reachability-cum-PSM cycle (further referred to as "RP cycle") is equal to the sum of a configured Reachability interval sojourn time (T_{Reach}) plus PSM sojourn time (T_{PSM}).
- The repetitive (T_{Reach} + T_{PSM}) pattern is made deterministic by locking it on an absolute clock reference (Tref), as illustrated in Figure 6.3.12.1-1. In other words, the combined (T_{Reach} + T_{PSM}) cycle starts at instants defined as t = Tref + N * (T_{Reach} + T_{PSM}), where N is a whole number. The absolute clock reference (Tref) can be based on Coordinated Universal Time (UTC).

Editor's note: This solution assumes that the RAN design of the radio interface supports periodic announcement of Tref in the system broadcast information. It is up to RAN to determine the periodicity.

- If UE needs to break the cycle for any reason (e.g. initiating MO communication, responding to paging, performing a mobility procedure, etc.), it returns to the (T_{Reach} + T_{PSM}) cycle as soon as it returns to "Connected Inactive" or "CN_Idle" state. Given that the (T_{Reach} + T_{PSM}) cycle is locked to an absolute clock reference, there may be an exceptional truncation or extension of the very first T_{Reach} or T_{PSM} interval, allowing the UE to lock the RP cycle on the absolute reference clock.
- The parameters defining the periodic RP cycle (Tref, T_{Reach}, T_{PSM}) may be provided to a 3rd party AS, by using a functionality similar to Service Capability Enablement Function (SCEF). Alternatively, the Tref can be pre-agreed between UE and AS, and then the UE requests the network to use the pre-agreed Tref.

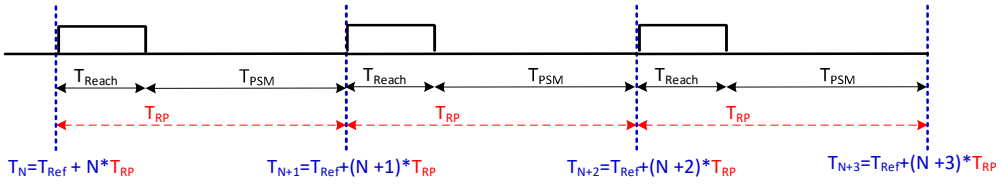


Figure 6.3.12.1-1 Clarifying how the RP cycle is locked to an absolute time reference (Tref)

When applied to "Connected Inactive" state the following applies:

- The RP cycle parameters (Tref, T_{Reach}, T_{PSM}) are determined by the RAN.
- The RAN may provide the RP Cycle parameters to the NG Core so that the latter can export them to 3rd party application servers; however, the NG Core typically does not make any other use of these parameters.
- Any MT data that may arrive while UE is in PSM cycle are buffered in the RAN. The RAN uses the RP Cycle parameters to determine when the UE becomes reachable and initiates paging.

When applied to "CN_Idle" state (if supported) the following applies:

- The RP cycle parameters (Tref, T_{Reach}, T_{PSM}) are determined by the NG Core.
- Any MT data that arrive while UE is in PSM cycle are buffered in the NG Core. The NG Core uses the RP Cycle parameters to determine when the UE becomes reachable and initiates paging.

Being informed of UE's RP Cycle, the 3rd party application server knows that it should initiate MT data transmission shortly ahead of the T_{Reach} interval, which clearly minimises the buffering delay.

NOTE: This scheme does not require tight synchronisation between UE, AN, CN and AS.

6.3.12.2 Function description

For more details refer to TR 23.709 clause 5.8.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 169 of 501

6.3.12.3 Solution evaluation

This is a solution for UE power saving functionality where Power Saving Mode period and idle mode period are regularly alternated while the UE is in CN_Idle mode or RAN Inactive mode. This solution addresses the minimizing of data buffering in NG CN side since the reachability period is synchronized with Application Server so the Application Server can avoid sending data while the UE is unreachable. Consequently, the solution reduces the delay for delivery of mobile terminated data to the UE. The solution requires that CN and RAN share a common clock based on UTC, but it does not require the use of any additional clock (cf. H-SFN in EPS) for synchronisation between CN and RAN, or within the RAN. Due to the coordination is required between AS and UE, exposure functionality is mandated for this solution. In other words, this solution isn't applicable for the AS which is connected directly to the operator network (i.e. Direct Model in TS 23.682).

6.3.13 Solution 3.13: Solution for mobility framework with split Location Tracking Function

This solution applies to key issue 3 on Mobility management, specifically on the UE reachability management.

6.3.13.1 Architecture description

Location Tracking (LT) functionality is separated into RAN LT function and CN LT function.

Besides the CN level UE location tracking, i.e. the location tracking via the NAS message, the CN LT function maintains RAN LT function ID, UE RAN anchor, and set the RAN Tracking policy (e.g., acceptable delays for DL reachability, etc.) as well as UE Location Update policy (e.g., RAN LR area, etc.).

The RAN LT function performs RAN level UE location tracking in its coverage area, e.g. calculate the UE location by processing the received radio signal. It reports UE location related information to the CN LT function when it is need. Triggers for the reports can be the changes of the UE RAN anchor point, UE moving out of coverage, etc.

The RAN UE anchors function is the user plane anchor point on the RAN side. It is responsible for routing the UE traffic to the right place, i.e. the UE for MT traffic or CN for the MO traffic.

Editor's note: It is FFS if the RAN LT function are not combined with the RAN anchor function.

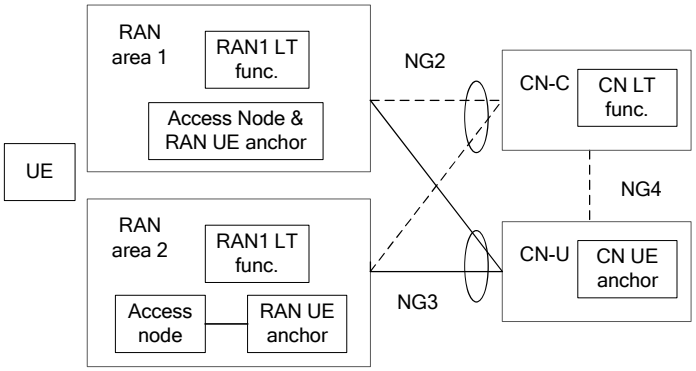


Figure 6.3.13.1-1: Split of LT functionality between RAN and CN

6.3.13.2 Function description

The CN LT function is responsible for:

1. Performing UE location tracking on the CN level, i.e. the location tracking via the NAS message.
2. Performing policy based location tracking management, (e.g., set the UE Location Update policy and report mechanism in the RAN, etc.)
3. Tracking/inquiring the UE RAN anchor and RAN LT changes.

The RAN LT function is responsible for:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 170 of 501

1. Performing UE location tracking in the RAN level according to the policy set by the Core LT function.
2. Reporting the change of UE RAN anchor, change of RAN LT to the CN LT function according the policy set the CN LT function.

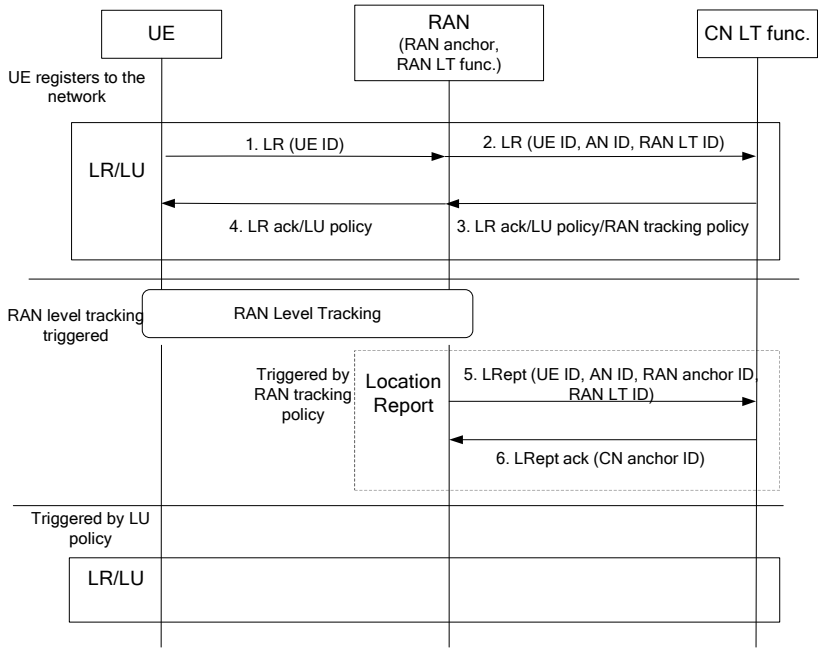


Figure 6.3.13.2-2: Location Registration and Location Update procedure

When UE first time attaches to the network, Location Registration (LR) is performed.

1. UE sends LR request via RAN to CN LT function.
2. RAN forwards the UE LR request (UE ID) to CN LT function with RAN LT ID and AN ID.

CN LT function triggers the authentication procedure and determines the tracking policy according to UE profile (e.g., UE usage type, mobility level).

3. CN LT function sends the LR Ack and LU policy to UE via RAN. In case RAN level tracking is appropriate, CN LT triggers RAN level tracking and sends the UE RAN tracking policy to the RAN LT function.
4. RAN LT function forwards the LR Ack and LU policy to the UE.

Based on the receiving LU policy, the UE suspend the CN level location update and trigger the RAN level location update. When trigged by the CN LT, RAN LT starts RAN level UE tracking according to the RAN Tracking policy defined by CN LT function.

When RAN anchor, RAN LT function changes, e.g. UE response the paging message via the different RAN Anchor function, RAN LT function reports UE location to CN LT (step 5, 6).

5. RAN LT sends LRept (UE ID(s), AN ID, RAN anchor ID, RAN LT func. ID) to the CN LT function.
6. CN LT function sends back the LRept acknowledgement, which could carry optional information on the tracking policy changes, CN anchor changes and/or stop signal for RAN level tracking.

According to the LU policy from CN LT (e.g., when UE moves out of certain CN area) Location Update (LU) procedure, can be trigged again at the UE. CN LT could use this procedure to stop/trigger/reset RAN level tracking policy in the RAN and resume the CN level location tracking procedure at UE.

6.3.14 Solution 3.14: Solution for determining UE mobility level

This solution aims to address some issues in work task #1 of on demand mobility support.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 171 of 501

6.3.14.1 General description

According to stage 1 requirements, mobility support in the next generation networks should take UE mobility patterns and service delivery requirements into count. Therefore, it is necessary to differentiate mobility support for UEs with different mobility and service/session continuity requirements.

NOTE 1: Service/session continuity requirements are handled by solutions for session management/session continuity.

This solution proposes to use "mobility level" to differentiate UE mobility in next generation networks, The mobility level here is a variable determined by the core network to describe how UE moves, i.e. UE mobility pattern. The specific UE mobility levels are defined as followed :

- No mobility: the UE is static or quasi-static and can only access the network via a fixed access point, which implies no TA change.
- Low mobility: the UE is expected to move within a designated/expected geographical area, e.g. a list of TAs for a campus.
- Full mobility: the UE moves across geographic areas randomly.

When UE at " low mobility" level moves out of the " designated/expected geographical area", it shall only send a tracking area update request. Depending on network policies, the network either rejects the request and indicates UE that no more requests are allowed outside the " designated/expected geographical area", or updates the mobility level for this UE.

For determining UE mobility level, the following information may need to be considered:

Subscribed UE mobility level(s): Subscribed UE mobility level(s) is stored in UE's subscription data, it indicates possible mobility level(s) that may be applied to the UE;

NOTE: The subscribed UE mobility level(s) may be inserted into UE subscription when the user signs a particular service contract, e.g. that for campus users, or when the network operator detects UE moving law from UE mobility history.

UE location: UE location change may lead to the change of mobility level, e.g. when an office worker move into office/company area, mobility level of their UE may need to be changed from " Full mobility" to " Low mobility";

Date and time: For accurately determining UE mobility levels, the network may need to take date and time into count, e.g. if an office worker moves into office/company area in the working time, mobility level of his UE may be changed from " Full mobility" to " Low mobility". However, if he moves into the office/company area in the nonworking time, the mobility level may not be changed;

UE capability: UE capability may be used by the network to determine UE mobility level.

The subscribed mobility level(s) of this UE is derived from UE type/capability and historical UE mobility information, e.g. a IoT device for environment monitoring may be with "no mobility"; a smart phone may have several mobility levels, i.e. different mobility levels in different date, time and/or places. The subscribed mobility level(s) of a UE is calculated on the application layer, e.g. by the operator's BSS/OSS system.

The subscribed mobility level(s) as well as the corresponding condition(s) of selecting each mobility level, e.g. date, time or UE location is stored in the UE profile, e.g. subscription data. The subscribed UE mobility level(s) may be updated if the operator discovers new UE moving laws based on its mobility history. With such mobility level(s) profile of a UE, when the network detects the condition(s) of selecting a particular mobility level is met, it will select the corresponding mobility level for this UE.

After determining the mobility level for the UE, the network may receive predictable UE mobility information, e.g. from application layer. In this case, the network may update UE mobility level based on the received information.

6.3.14.2 Function description

This solution relies on mobility level determination (MLD) function to determine the mobility level of a UE. The figure 6.3.14.2-1 shows the high level functions for determining UE mobility level.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 172 of 501

When a UE is accessing the network, the MLD function retrieves possible mobility level(s) and the corresponding conditions from UE subscription data. The MLD function may check whether the conditions of selecting a specific mobility level is met, e.g. whether the UE is within a particular area, if yes, the corresponding UE mobility level will be selected. The MLD may interrogate location management function for UE location information.

The policy control function may receive UE mobility information from application layer. UE mobility information can be predictable UE mobility behaviours, e.g. UE mobility pattern or possible UE mobility level(s). If UE mobility behaviours was indicated, the policy control function needs to interpret it to the possible UE mobility level(s). Based on the possible UE mobility level and current UE information, such as UE capabilities, UE location, date and time, the policy control function can determine current UE mobility level(s) , and send it to the MLD function, so that the MLD can update the UE mobility level if necessary.

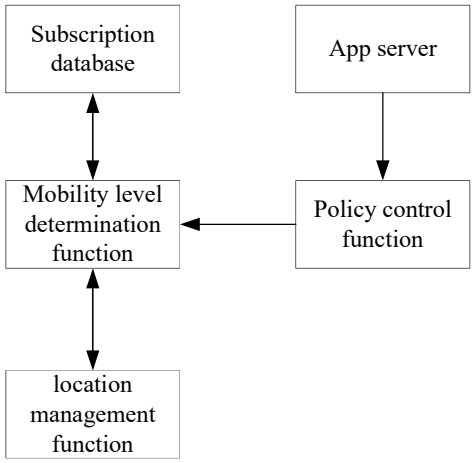


Figure 6.3.14.2-1: High level functions for determining UE mobility level

6.3.14.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.15 Solution 3.15: Solution to support different levels of mobility

The solution introduces mechanism to enable the support of different levels of mobility based on the following

1) The UE Capabilities of the UE that requests services from the Network e.g., device radio capability, (e.g., dual or single radio capable UEs, low-cost-devices, fixed terminals and full featured devices, terminals with battery constrains).

2) The requirements of services the UE wants to use are communicated by the UE, either during the initial registration or through a specific service request. E.g., the service requested by the UE can be characterized by providing an Application ID or even a mobility descriptor that can explicitly indicate mobility requirements for a particular service. E.g., Services that at a particular time only require mobile originating data transmission)

3) The services the UE subscribes to e.g., mobile originating connectivity services, mobile terminating connectivity services or both, Location-Based Services (i.e., UE can avail of services within a specific area only .e.g., Cell_Level), Roaming Services, Support for High Speed mobility.

4) Operator's policy the operator applies for a particular UE or groups of UEs, e.g., geographical scope of operation, UE speed, Roaming, Time based Network Access.

6.3.15.1 Mobility Levels Definition

Mobility Levels can be defined based on the area a UE is able to move before it needs to provide an area update (E.g., Tracking Area Update or Registration) and whether the UE requires Connectivity on Uplink, or both Uplink and Downlink. This can be referred to as Area Mobility Level and it can take any of the following levels.

a) Stationary (Uplink (UL)/Bidirectional (BD)): UE connectivity is provided through a fixed Access, where "fixed access" can be characterized as an access point which location never changes (regardless of whether the connection is

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 173 of 501

wireless or wired). When operating on this Mobility Level the UE is not allowed to connect from any other access point and therefore there is no need to perform location tracking. Furthermore if the connectivity mode is "UL" only or the UE has access to a constant power source, the UE is not expected to execute reachability update procedures. Note that the UE might be available for Mobile Terminating data transfer for a period of time right after a Mobile Originated procedures, such as Attachment and Service Request is executed, even if the connectivity mode is "UL" only. A UE operating under this Mobility Level (Stationary) and under this connectivity mode (UL) is permanently attached upon the successful completion of the Attach procedure.

If the connectivity mode is "BD" the UE is required to execute Area Update procedures to allow the Network to determine reachability status. A UE that fails to execute Area Update procedures when instructed by the Network to do so, it is considered implicitly Detached.

b) Limited (Uplink (UL)/Bidirectional (BD)): UE connectivity is provided on a limited area that can range from one to many access points (e.g., from a cell level to a collection of tracking areas). A UE operating under a Limited Mobility Level and under "UL" connectivity Mode, is not expected to execute reachability update procedures.

A UE operation under Limited Mobility Level and operation under "BD" connectivity mode, is expected to execute Area Update procedures within the boundaries of the limited area and in accordance to periodic Area Update reporting procedures. Furthermore a UE that leaves the Limited area is required to execute System Attach procedures before it can execute a Service Request procedure. A UE operating under the Limited Mobility Level and under "BD" connectivity mode is expected to execute reachability update procedures, depending on whether or not the Limited area is composed of smaller areas that need to be tracked.

c) Full (UL/Bidirectional) A UE operation under Full Mobility Level and under "UL" connectivity mode is not required to execute reachability update procedures and neither Area Update procedures as long as it remains within the boundaries of the PLMN. Note that Authentication and authorization procedures might be executed at any time, as configured by the operator, upon executing System Attach or Service Request procedures, as UEs operating in Full Mobility Level and "UL" mode can be permanently attached.

A UE operating in Full Mobility Level and "BD" connectivity mode is expected to execute full reachability and Area Update procedures

Table 6.3.15.1-1: UE and NW behaviour when operation under a specific Mobility Level and Connectivity Mode

MOBIITY LEVEL	CONNECTIVITY MODE	MAIN EXPECTED NW BEHAVIOUR	MAIN EXPECTED UE BEHAVIOR
Stationary	Mobile Originating Data Transfer (UL)	NW can keep UE permanently Attached, no need to keep Area Tracking or Reachability status NW can of course Authenticate the UE at any time the UE request connectivity services If the UE Capabilities allows it, the NW can keep the UE in Connected mode, immediately after a MO procedure to execute DL Data Transfer The NW does not Page the UE operating under Stationary Mobility Level with UL Connectivity Mode	The UE is not expected to execute Reachability update procedures (e.g., Periodic TAU) nor Area Update Procedures. Note that the UE might be available for Mobile Terminating data transfer for a period of time right after a Mobile Originated procedures, such as Attachment and Service Request is executed, even if operating under "UL" mode. The UE is permanently attached upon the successful completion of the Attach procedure, unless its Mobility Level is updated by the NW or upon successful execution of a new Attach procedure

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 174 of 501

			The UE can only execute a Service Request procedure, while Connected to a single Operator defined Access Point which Identity might be preconfigured in the UE
	Bidirectional Data Transfer (BD)	NW keeps track of the UE Reachability status using the Reachability reports from the UE. NW considers the UE implicitly Detached after failing to report Reachability status after a predefined time period NW only pages in the Service Area configured for the relevant UE	UE is required to execute Periodic Reachability Update Procedure but not Mobility based Area Update Procedures If the UE is not able to update its Reachability status after a predefined time which could be provided during the execution of the Attach procedure or preconfigured in the UE,, (e.g., the UE is outside the coverage of its dedicated Access Point) it should implicitly detach
Limited	Mobile Originating Data Transfer (UL)B	The NW handling for the UE in Limited Mobility Level and UL Connectivity Mode is similar to the Stationary Mobility Level only that The NW provides the UE with Area Information that defines the Service Area where the UE is allowed to avail of Data Connectivity services	The behaviour of the UE is similar to the Stationary Mobility Level only that that the UE can avail of connectivity services across the Service Area defined in the in Area Info provided to the UE upon Attachment
	Bidirectional Data Transfer (BD)	The NW handling for a UE in Limited Mobility Level and BD Connectivity Mode is similar to the Stationary Mobility Level only that: The NW provides the UE with Area Information that defines the Service Area where the UE is allowed to avail of Data Connectivity services The NW pages the UE in the Service Area configured for the relevant UE	The behaviour of the UE is similar to the Stationary Mobility Level only that: The UE can avail of connectivity services across the Service Area defined in the in Area Info provided to the UE upon Attachment The UE might report Area Update depending on the size and definition of the Area Info provided by the NW
Full	Mobile Originating Data Transfer (UL)	The NW handling for a UE in Full Mobility Level and UL Connectivity Mode is identical to the Limited Mobility Level	The behaviour of the UE is identical to the Limited Mobility Level

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 175 of 501

	Bidirectional Data Transfer (BD)	The NW handling for the UE in Full Mobility Level and BD Connectivity Mode is similar to the Limited Mobility Level only that: The NW manages the UE mobility across the service Area defined for the relevant UE spanning the entire PLMN (s), where the UE is allowed to avail of Data Connectivity services The NW might update the UE with new Area information as the UE moves across the entire Service Area of a PLMN	The behaviour of the UE is similar to the Limited Mobility Level only that: The UE might report Area Update when crossing the boundaries of an Area provided by the NW during the last Area update.

6.3.15.2 Function description

System Attach

The call flow in Figure 6.3.15.2-1 describes a possible Attach procedure where the UE provides information on the requirements of services that need to be supported and possibly its device capabilities. The Network uses configured operator policies and specific subscription information as well as the information provided by the UE to derive the level of mobility assigned to the UE.

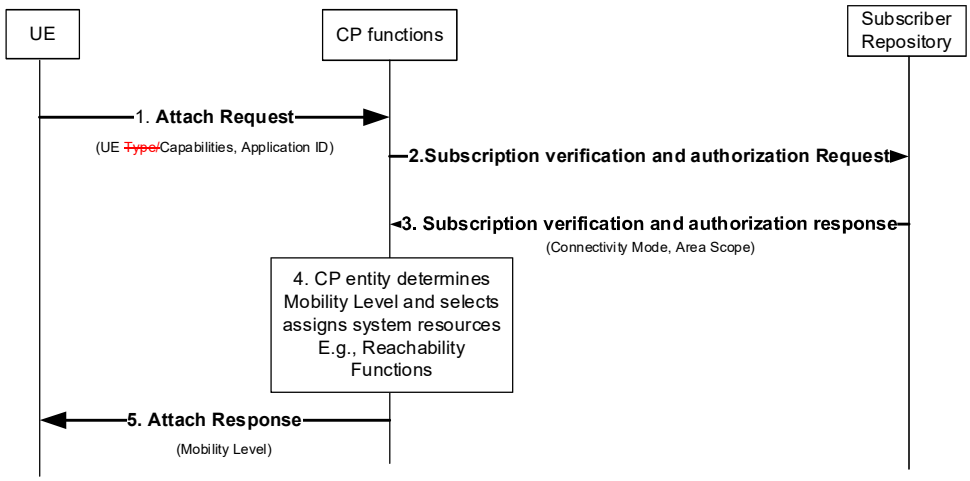


Figure 6.3.15.2-1

1. During the Attach procedure the UE provides specific requirements of the services that need to be supported. AUE may provide an Application ID or explicit Mobility Requirements in the form of a descriptor (similar to the multidimensional descriptor used for network slice selection) and/or UE Capabilities

2-3.During the Subscription authorization procedure, the Network may retrieve subscription information that can be used to determine the level of mobility the subscriber is entitled to

4. The CP entity uses the information provided by the UE, operator policies and subscription information to determine the mobility level that the UE can be assigned. The CP entity also determines Mobility Management resources that may be required to support the selected level of mobility, I.e., Stationary, Limited or Full).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 176 of 501

5. The determination of the mobility level (e.g., the Area the UE is allowed to send and or receive data, whether the UE is allowed to send data, receive data or both) is communicated to the UE to match the behaviour expected by the Network. Depending on the Mobility Level, the UE executes mobility procedures as specified in 6.3.15.1

New Service Request/Connectivity Request

The level of mobility might be modified either as a request from the UE to satisfy a different service or from the Network operator to modify the level of mobility currently provided.

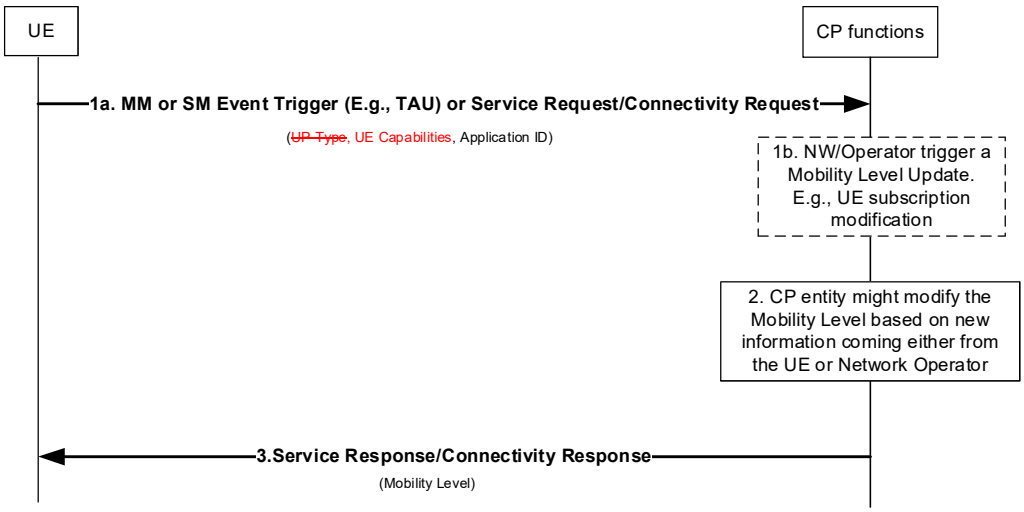


Figure 6.3.15.2-2

1a. During the execution of a mobility management or session management procedure (E.g., TAU or Service Request procedure or during the request for a PDU sessions) the UE may provide requirements of additional services that need to be supported. Similarly to the Attach procedure, the UE may provide an Application ID or explicit Mobility Requirements in the form of a descriptor (similar to the multidimensional descriptor used for network slice selection) and UE Capabilities.

1b. In addition, the operator or the Network may modify the level of mobility allocated to UE, e.g., triggered by a subscription changes, which can may cause an update of the existing mobility level allocation.

2. The CP entity uses the information provided by the UE, operator policies and subscription information to determine the mobility level that the UE can be assigned. The CP entity also determines Mobility Management resources that may be required to support the selected level of mobility, E.g., whether CP functions to support paging optimization are required.

3. The determination of new or modify mobility level or levels is communicated to the UE to match the behaviour expected by the Network. Depending on the Mobility Level, the UE executes mobility procedures as specified in 6.3.15.1

6.3.15.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE and CN

6.3.16 Solution 3.16: Limited & Unlimited UE mobility level

This solution is applicable to Key Issue 3 - Mobility Framework aiming to address WT#2 and WT#3. This solution proposes splitting TAU procedures into registration area update procedure and reachability update procedure reflecting its own purposes. Thus the handling of registration area update and reachability update procedure in regard to UE mobility area handling (i.e. limited mobility area, unlimited mobility area) and the necessity of mobile terminated service is described. Also, how to handle service request procedure if neither registration area update nor reachability update is executed for mobile originated only commination type.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 177 of 501

6.3.16.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

Splitting TAU procedure into Registration Area Update and Reachability Update:

It is proposed splitting TAU procedure into Registration Area Update and Reachability Update procedure based on its own purpose. Table 6.3.16.1-1 depicts which procedure is required depending on UE mobility Area and whether Mobile Terminated service is required or not.

NextGen system can configure whether a PDU session is designated for mobile originated only communication type during PDU session setup procedure. If all PDU session(s) which is allocated for a UE is mobile originated only communication type, then CP-MM treats the UE as no mobile terminated service required.

- Registration area update procedure: this is same as TAU procedure which is triggered when a UE detects it has entered a new TA that is not in the list of TAIs that the UE registered with the network.

- Reachability update procedure: this is same as periodic TAU procedure which is triggered when the P-TAU timer has expired.

Table 6.3.16.1-1: Required Idle mode behaviour regarding Mobility area handling and MT capability requirement

MT service / Mobility Area	MT required	MT is not required
Limited	- Reachability Update	Nothing
Unlimited	- Registration Area Update - Reachability Update	Nothing

To maximize resource efficiency both for UE and network, UE which does not require mobile terminated service shall not perform Registration Area Update and Reachability Update procedure including paging procedure. For UE which requires mobile terminated service but with limited mobility level, only Reachability Update procedure is required with paging procedure.

6.3.16.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Support of UE which does not required mobile terminated service:

For a UE which does not require mobile terminated service, neither Registration Area Update procedure nor Reachability Request procedure is required. However the NextGen CN (i.e. CP-MM) need to handle the registration validity. During Attach procedure, if a UE does not require mobile terminated service then CP-MM may include Attach valid Time to Attach Accept message depicted in Figure 6.3.16.2-1. If a UE receives Attach Valid Time during Attach procedure, the UE uses this Attach Valid Time to determine whether to perform Service Request or Attach procedure for the next mobile originated service request. If the Attach Valid Time is exceeded then UE considers this as implicit detach and the UE shall perform Attach procedure instead of Service Request procedure. If the Attach Valid Time is still valid then the UE still can perform service request procedure.

For a UE applies Limited mobility level, the Attach Valid Time is still applicable. For example, if a UE moves out of the allowed TA(s) then the UE shall not perform mobile originated procedure (i.e. Service request procedure for mobile originated service or attach procedure). However if the UE come back to the area of allowed TA(s) then the UE can perform mobile originated procedure again. In this case, if the Attach Valid Time is still valid then the UE can perform service request procedure instead of attach procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 178 of 501

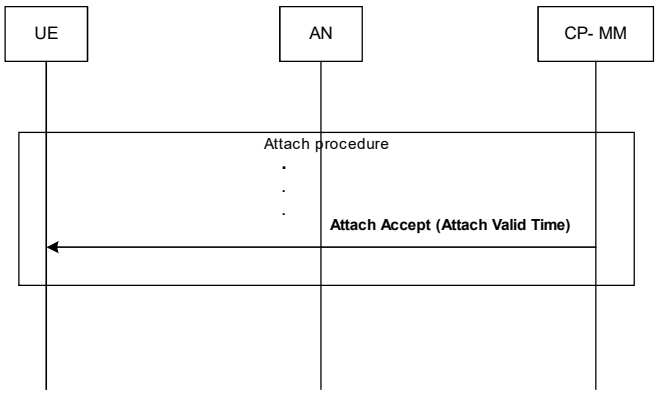


Figure 6.3.16.2-1: Attach procedure for MO only communication (No Mobile terminated service is required)

Since the UE does not perform Registration Area Update and Reachability Update procedure even in 'Unlimited mobility level', AN can fail to find serving CP-MM of the UE. Therefore UE should include CP-MM identification which is provided by serving CP-MM (e.g. GUMMEI) in RRC message which related to Service Request message as depicted in Figure 6.3.16.2-2. Accordingly AN can select serving CP-MM of the UE. If AN can't direct to UE's serving CP-MM new CP-MM can trigger relocation procedure conjunction with Service Request procedure.

MO procedure for UE with MO only communication

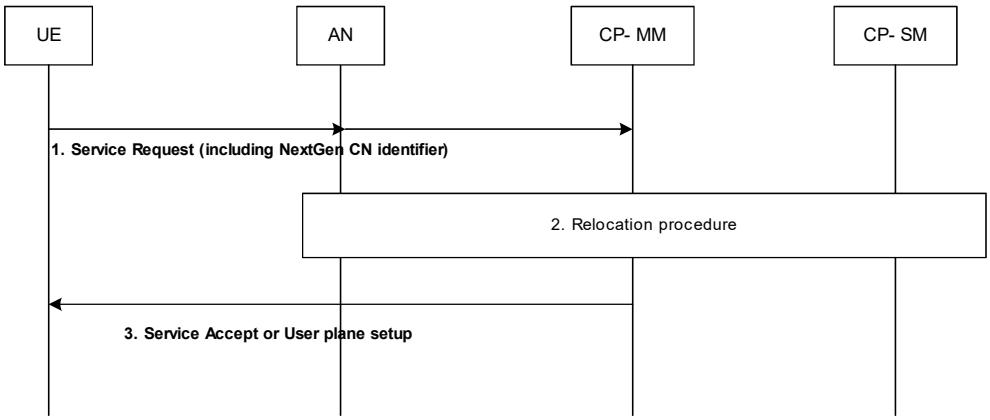


Figure 6.3.16.2-2: CN relocation procedure triggered by service request

The description of the steps is as follows:

1. If a UE wants to send data then the UE sends Service Request message. In this case, the UE shall include previously allocated NextGen CN identifier in RRC message.

2. If an AN can direct to the same NextGen CN which is indicated in RRC message, the AN sends the Service Request message to the indicated NextGen CN. If the AN can't connect to the indicated NextGen CN, then NextGen CN selection function should be performed to select appropriate NextGen CN. The detail procedure is out of scope of this solution.

3. Serving CP-MM returns Service Accept message to UE.Editor's note: Roaming case is FFS.

Support of Limited mobility level by providing Allowed TA(s):

Based on subscribed information, a CP-MM determines the UE mobility level is Limited then the CP-MM should include Allowed TA(s) for this UE in Attach Accept message as depicted in Figure 6.3.16.2-3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 179 of 501

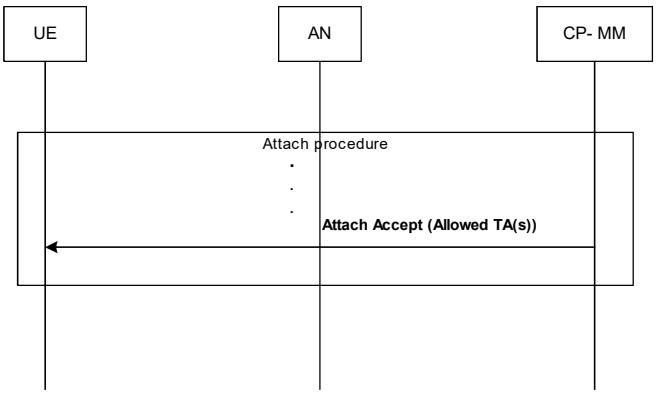


Figure 6.3.16.2-3 Attach procedure for limited mobility level

If a UE receives Allowed TA(s) during Attach procedure, then the UE shall not perform Registration Area Update procedure. If terminated service is required for this UE, the UE only performs Reachability Update procedure. If the UE moves out of allowed TA(s) the UE shall not request any service request procedure and also Reachability Update procedure. CP-MM consider the UE is implicitly detached when the UE does not perform Reachability Update procedure and/or the UE does not reply to paging request. When the UE comes back to area of allowed TA(s) again, UE may need attach again if the UE considers implicitly detached from the NextGen system.

6.3.16.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.17 Solution 3.17: Support for Idle Mode Mobility capabilities

This is a solution to Key issue 3: Mobility framework. This solution covers the problem identified for MM WT#3.

6.3.17.1 Architecture Description

To support the mobility on demand concept in the NextGen system, the following architectural concepts are proposed:

- Mobility levels are defined in order to support varying levels of UE mobility, ranging from no mobility, nomadic mobility to full mobility. Thus this solution proposes that the UE and the network may support a range of NextGen Idle Mode Mobility (IMM) capabilities, as follows:

  - Level 1 - Idle but not tracked- When UE is in level 1, it is neither tracked nor reachable by the Network, the UE is reachable only for a period after it awakens, enters the NG CM Connected State/RRC connected mode and engages in a transaction with the network. As long as UE is in connected mode, UE remains reachable. If the UE is not in NG CM connected/RRC connected mode, the UE is not reachable as the network does not page the UE until it engages in an MO transaction. Then, the UE becomes reachable again when it performs MO transaction.

  - Level 2 - Limited Idle Mode Mobility- When the UE is in level 2, UE is considered to be in a fixed tracking area (consisting of a list of cells, e.g. provisioned by network), hence it does not send TA Updates due to mobility (i.e. when it crosses boundaries). If the UE moves beyond the fixed Tracking Area, it cannot be reached as the network does not attempt to page in an area outside the fixed tracking area. Therefore, it can only be paged within the fixed tracking area. Level 2 is expected to be supported only for fixed and nomadic devices that is expected to be within a fixed tracking area assigned by the network.

  - Level 3 - Full Idle Mode Mobility - UE is tracked across tracking areas which may consist of many cells. If UE moves beyond the tracking area, it performs tracking area update to allow it to be reached by the network when paged.

Additional details about the different idle-mode mobility capabilities are as follows:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 180 of 501

IMM capability	Type	NW-UE data connection	UE performs TAU due to mobility	Network paging supported	Reachability
1	Idle but not tracked	Yes	No	No	Reachable when it engages in MO transaction and in NG CM/RRC connected mode.
2	Limited **Idle Mode Mobility**	Yes	No	Yes (in fixed tracking area)	Yes, in a fixed tracking area
3	Full **Idle Mode Mobility**	Yes	Yes	Yes (in multiple tracking areas)	Yes, in multiple TAs

NOTE: The IMM capabilities can be applied independent of the Mobility level for a UE.

- A UE may support more than one NextGen Idle capability.
- Mobility level(s) that can be assigned to the UE may be stored in the network subscription data for the UE.
- UE IMM capability is determined by negotiation between UE and core network based on UE subscription, UE capabilities, UE location, and operator policies.
- UE IMM capability can be changed, due to, e.g., subscription, location, or policy change. In addition, the UE and network can negotiate IMM capability change during a mobility management procedure.
- UE capabilities are provided by the UE in signalling towards the network.
- NextGen Idle Mode Mobility capability is an attribute of the UE.
  - At any given time, only one NextGen Idle Mobility Capability may be assigned for use on a UE
  - If a device supports more than one NextGen Idle Mobility capability, the currently assigned Idle Mobility mode may be changed without service disruption (idle mobility on demand)
  - The assigned NextGen Idle Mode Mobility is determined by signalling between the UE and the core network and is based on e.g. subscription information, UE capabilities or UE location change. Location from where

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 181 of 501

the UE performs TAU and the frequency for the TAUs performed could be considered as criteria for updating IMM capability for the UE.

- Following figure illustrates the transitions that are possible from one IMM capability to another IMM capability:

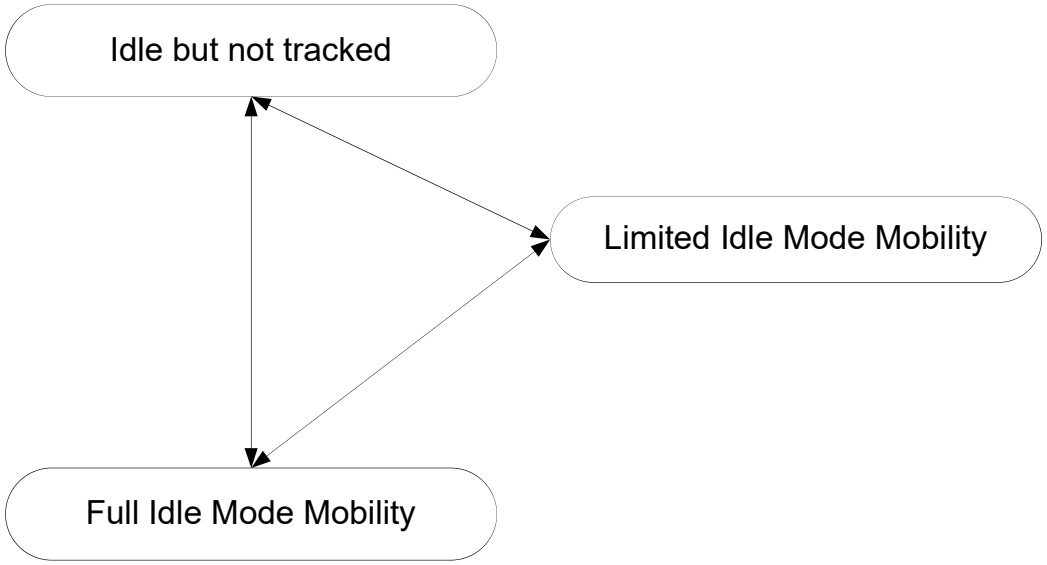


Figure 6.3.17.1-1: IMM capability transition

6.3.17.2 Function description

6.3.17.3 Solution Evaluation

Editor's note: This clause will contain evaluation on the system impacts.

6.3.18 Solution 3.18: Mobility procedure

This solution applies to Key Issue 3 - Mobility Framework. The solution introduces an idle mode mobility procedure for the NG UE registration to the network and NG UE mobility support.

6.3.18.1 Architecture description

The architecture is based on the architecture and terminology:

- NG UE
- NG RAN
- NG Core Control plane function: CCF
- NG Core UP function: UPF
- NG Subscriber Data Management: SDM
- NG Policy Control plane function: PCF

6.3.18.2 Function description

The main functionality of the solution is:

- The NG mobility procedure is including "attach and tracking area update functionality" within a single mobility procedure, the Registration procedure; and
- The NG UE status update procedure for exchange of protocol information between the UE and CCF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 182 of 501

The Registration procedure is used e.g. when the NG UE attach into the mobile network, upon mobility procedure when the NG UE changes to a new Tracking area (TA) in idle mode and when the NG UE performs a periodic update (due to a predefined time period of inactivity) etc.

The UE Status Update procedure is used by the NG UE to perform periodic updates or additional updates of UE capabilities and to re-negotiate UE parameters to synchronise bearer status and timer values with the CCF, if there is a need to change the values that were negotiated in the previous attach or TAU procedure.

Editor's note: It is for further study whether to include session management messages or not.

Editor's note: Additional functionality e.g. from TAU procedure e.g. providing UE capabilities, usage of active flag and synchronization of SM contexts is FFS.

6.3.18.2.1 Registration procedure

The Registration procedure is initiated by the UE to perform attach or mobility based update when entering new area.The registration procedure describes the high level principle; further details are FFS.

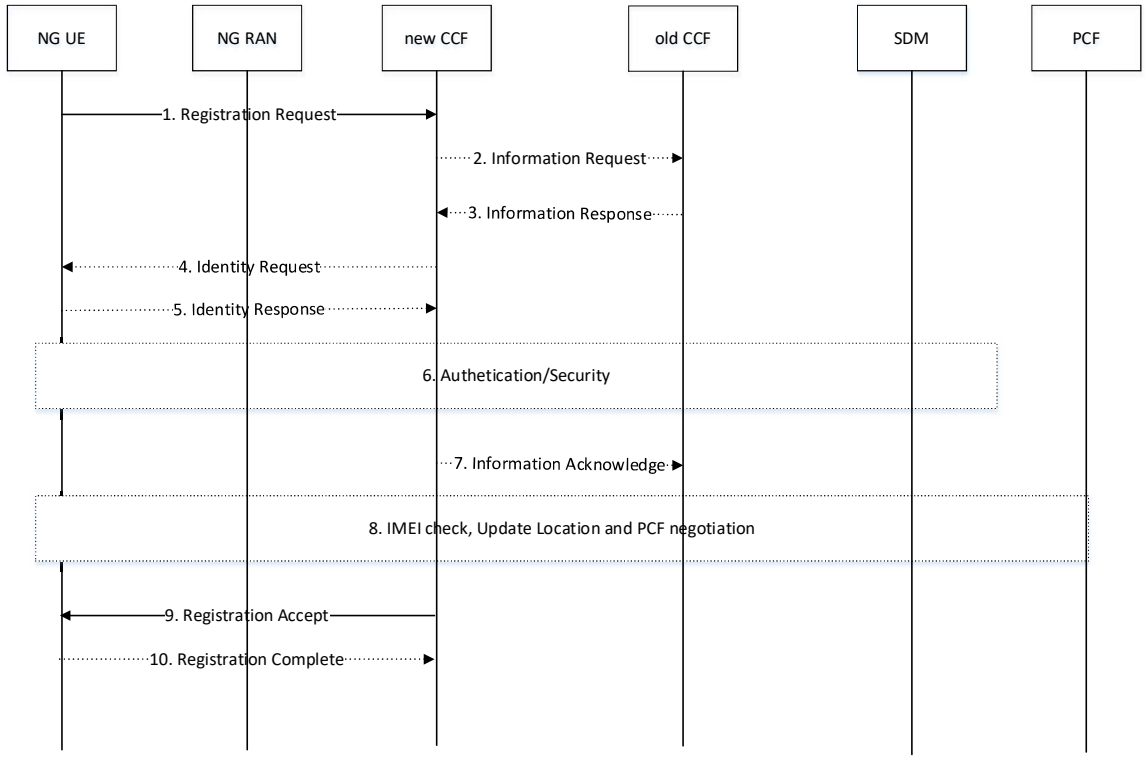


Figure 6.3.18.2.1-1: Registration procedure

Registration procedure

1. NG UE sends Registration Request message to (new) CCF including either a permanent ID (e.g. IMSI) or a unique temporary ID (similar as GUTI) and a Registration type. The Registration type indicates if the NG UE wants to perform an 'initial registration' (i.e. the NG UE is in non-registered state) or a 'normal registration' (i.e. the NG UE is in registered state). If 'initial registration' the message includes all necessary parameters for that (as in Attach in LTE). If 'normal registration' the message includes all necessary parameters for that (as in TAU in LTE). CCF checks the received message and if NG UE requested 'normal registration' but the new CCF was unable to retrieve information for the NG UE then 'initial registration' is performed instead.

2. New CCF may send Information Request to old CCF including e.g. complete Registration Request (including Registration flag) and CCF address.

3. Old CCF responds with Information Response to new CCF including e.g. a permanent ID (e.g. IMSI), MM Context and CCF address. If the Registration flag within the Complete Registration Request IE in the

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 183 of 501

Information Request message is set to 'normal registration' then e.g. session related data may also be included. If NG UE requested 'normal registration' but the new CCF was unable to retrieve information from old CCF then 'initial registration' is performed instead.

4. If permanent identity (e.g. IMSI) is not provided by the NG UE nor retrieved by new CCF then Identity Request is sent to the NG UE. This step is valid for both Registration type values.
5. The NG UE responds with Identity Response including a permanent ID (e.g. IMSI).
6. CCF initiates authentication of the NG UE if Registration Request was not sent integrity protected or integrity protection is indicated as failed in step 3/Information Response. NAS security functions is performed.
7. New CCF responds with Information Acknowledge if a successful Information Response is received. Old CCF marks the MM context as invalid.
8. IMEI check (optional procedure), Update Location procedure and optionally "PCF update and negotiation" are performed. If session data is received from old CCF then also session related procedures are invoked at this point.
9. CCF responds with Registration Accept to the NG UE indicating 'Registration result' with either 'initial registration' or 'normal registration'.
10. NG UE may respond with Registration Complete to (new) CCF.

6.3.18.2.2 UE Status Update procedure

The UE Status Update procedure is initiated by the UE to perform periodic update or update of parameters that are negotiated between UE and CCF. The UE Status Update procedure describes the high level principle; further details are FFS.

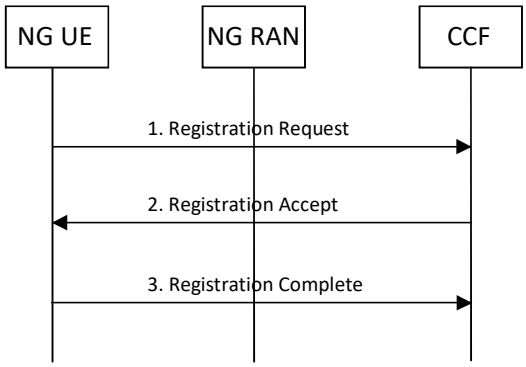


Figure 6.3.18.2.2-1: UE Status Update procedure

UE Status Update procedure

1. NG UE sends Registration Request message to serving CCF including either a permanent ID (e.g. IMSI) or a unique temporary ID (similar as GUTI). Additionally, the UE includes the negotiable parameters that it wants to update with the CCF.
2. CCF responds with Registration Accept to the NG UE, either echoing back the UE requested parameters, or negotiating them according to the UE capability, subscription and local policy. The CCF may include also additional information to synchronise the protocol status between the CCF and the UE.
3. NG UE may respond with Registration Complete to CCF.

NOTE: Identification, authentication and authorisation procedures are possible, but not shown.

Editor's note: Whether the UE Status Update procedure can re-use the same PDUs as attach and TAU is to be determined by CT1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 184 of 501

6.3.18.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.19 Solution 3.19: Solution to activate RRC inactive state

6.3.19.1 Architecture description

This solution enable to UE to enter RRC_inacive_state as described in clause 6.3.2.

When a UE activates user plane service, the UE may reports the list of cell IDs and/or TAs it desires to be served in while NG CM Connected and RRC inactive connected mode. This list (i.e. Intended Area in this solution) may help NG Core to limit the area to page the UE.

Editor's note: How the list is derived, maintained is FFS. Security and privacy aspects are FFS.

The NG Core determines whether the UE is allowed to use the RRC inactive connected mode based on the subscription and policy. The triggering of determination can be the request from a UE , or the NG Core itself according to the UE subscription. The Allowed Area is determined by NG RAN and then feedbacks to the UE. The Long Connected Allowed Area can be a list of Cell IDs or TAs.

When the UE is in RRC inactive mode and detects that it moves to a cell which is not in the Long Connected Allowed Area, the UE send a notification to the NG Core that the UE has left the Long Connected Allowed Area. The NG Core may update or delete the assigned Long Connected Allowed Area.

Editor's note: details of notification procedure are FFS.

6.3.19.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.3.19.2.1 Service Activation Procedure

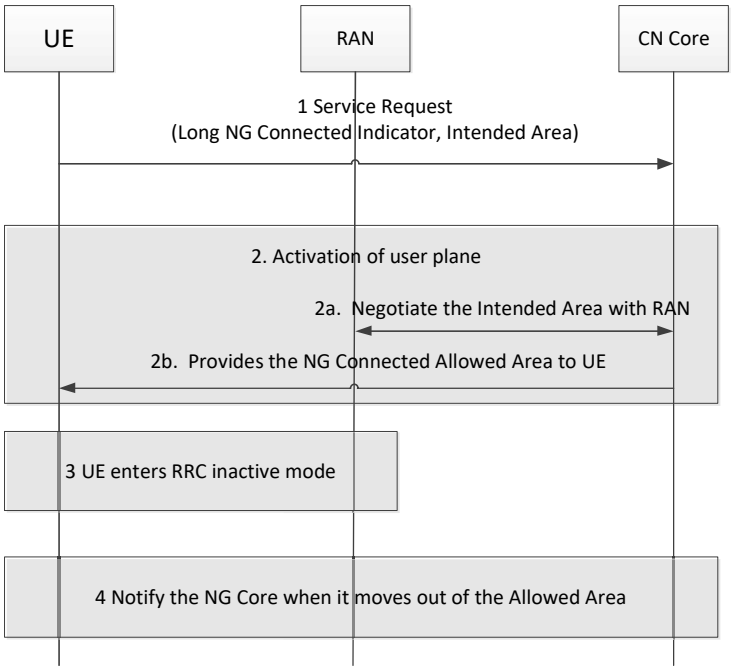


Figure 6.3.19.2.1-1 Service Activation Procedure

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 185 of 501

1. When the UE sends Service Activation Request, it optionally contains Long CM Connected indicator and the Intended Area. The Intended Area is the area that it desires to be served in NG CM Connected and RRC inactive connected mode.

Editor's note: It's FFS whether the Intended Area should be included or not.

2. NG Core performs the activation of the user plane. The NG Core determines whether the UE is allowed and appropriate to stay NG Connected for a long period. If yes:

2a. The NG Core indicates to RAN that the UE is considered long connected in the NG Core. The NG Core provides the Intended Area to RAN. The NG RAN generates the Long Connected Allowed Area taking the Intended Area into account.

Editor's note: It's FFS the relationship between the Intended Area and the Long Connected Allowed Area.2b. The Long Connected Allowed Area is sent to the UE.

Editor's note: Details of this step are FFS.

3. When NG RAN release the RRC connection (e.g. due to no data transmission over a certain time), the NG RAN and the UE enter RRC inactive connected state.

4. When the UE moves out of the Allowed Area, the UE notifies the CN Core.

Editor's note: details of notification procedure are FFS.

6.3.19.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.20 Solution 3.20: Solution for UE reachability for devices with only MO-communication

This solution addresses the Key Issue #3, in particular MM_WT_#2 (UE reachability management) and MM_WT_#3 (UE Mobility levels).

6.3.20.1 Architecture description

NG UEs are expected to have different characteristics and service needs that will influence the level of mobility management signaling required. Such characteristic and application service requirements can change over time for a given NG UE, and the change of the mobility management behavior can be needed.

An NG UE that relies on mobile originated communication (either no MT-service needed or MT-service limited to the time of UE initiated MO-communication) can either deregister from network after communication, or does not need to listen to paging during the periods between communications if it remains in IDLE mode. And the network does not need to track such NG UE.

Editor's note: The type of UE power saving mechanisms possible with this solution is FFS.

Further, mobility triggered location updates for such NG UE can also be omitted and will only be needed in conjunction with a trigger of mobile originated communication.

To control possible variations of the mobility management behavior, the NG CN and the NG UE need to coordinate the supported and applied functionality. Additionally, the MT-communication support preference during CONNECTED mode in the NG UE may also be negotiated between the network and the NG UE for the network to have a proper control of the MT-service.

6.3.20.2 Function description

An NG UE, especially when it relies on mobile originated communication, shall communicates its idle mode preference and paging preference to network during registration procedure. Additionally, the MT communication -service preference during CONNECTED mode may also be communicated to network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 186 of 501

The network shall apply proper mobility behavior based on preferences from NG UE, UE subscription and network configuration. The following tables describe the possible mobility behavior result matrix (table 1) and the detailed behavior of the NG CN and the NG UE (table 2)

Table 6.3.20.2-1: Preference, subscription/configuration based mobility management behavior control matrix

Parameters	NG UE	Subscription/Configuration	NG CN/NG UE behavior
IDLE mode	Preferred or not preferred	allowed or not allowed	applied or not applied (see table 2 for details)
Paging	Preferred or not preferred	allowed or not allowed	applied or not applied (see table 2 for details)
MT Communication	Preferred or not preferred	allowed or not allowed	applied or not applied (see table 2 for details)

Table 6.3.20.2-2: NG UE and NG CN detailed mobility behaviors based on negotiated parameters

Parameters in use (Note 3)	NG UE behavior	NG CN behavior
IDLE mode applied	IDLE mode at end of CONNECTED mode. See parameter Paging below for further behavior.	IDLE mode at end of CONNECTED mode. See parameter Paging below for further behavior
IDLE mode not applied	Deregistration at end of CONNECTED mode.	Supervise or trigger UE deregistration.
Paging Applied (Note 1)	Listen for paging in IDLE mode. Mobility triggered location update in IDLE mode. Periodic triggered location update in IDLE mode.	Paging request (i.e. signaling or traffic) when UE in IDLE mode.
Paging not applied	Periodic triggered location update in IDLE mode. Optional mobility triggered location update in IDLE mode.	Paging not allowed. Supervise CN-RAN interface release.
MT Communication applied (Note 2)	Supports MT-communication reception in CONNECTED mode See parameter IDLE mode above at the end of CONNECTED mode	Supports MT-communication delivery in CONNECTED mode. See parameter IDLE mode above at the end of CONNECTED mode
MT Communication not applied (Note 2)	No MT-communication support in CONNECTED mode. See parameter IDLE mode above for description of leaving	No MT-communication delivery in CONNECTED mode. See parameter IDLE mode above for description of leaving

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 187 of 501

	CONNECTED mode.	CONNECTED mode
Note 1: RAN handles UE as normal when NG UE is in CONNECTED mode (e.g. including the activation of the RRC inactive state). Note 2: MT Communication parameter is only applicable in CONNECTED mode. Note 3: The number of parameters reflects the functional options, but the parameters may be merged into fewer parameters in case some combinations are not needed.		

The network shall also inform the NG UE the conclusion of the UE preference.

Editor's note: It is FFS whether a solution without UE support is useful.

6.3.20.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.21 Solution 3.21: Solution for explicit signaling to limit idle mode procedures

This solution addresses task MM_WT_#2 (UE reachability management) of key issue #3. The solution introduces a mechanism for a UE to limit some idle mode procedures and avoid unnecessary signaling in the network.

6.3.21.1 General description

This contribution proposes a solution for reduce signaling in the network and power optimization in the UE when paging procedure will not be utilized or periodic TAU procedure is not needed.

To further optimize both UE power consumption as well as system resources in the network for IDLE UEs it may be desirable for those UEs that do not always require MT services to limit some of its idle mode procedures, such as sending TAU and/or listening to paging.

In addition to this it is also possible for the UE to utilize this mechanism during low battery condition to prioritize its operation over reachability.

The solution is to explicitly request stop sending TAU and stop listen for page whenever feasible.

NOTE 1: This is only applicable to some type of UEs e.g. that are not required to receive PWS (Public Warning System) information or required to always support MT services.

6.3.21.2 Functional description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.3.21.2.1 Limited Reachability

When a UE wants to limit its reachability (i.e. enter MO only mode), the UE may indicate to the MM function during the mobility management procedure that it will stop performing periodic tracking area update procedures and stop listen to page. The UE may update its reachability limitations using tracking area update procedure.

The network keeps track of the latest reachability limitations of the UE. When the UE has limited reachability then a) UE does not perform TAU procedures and b) does not listen to page and c) the network does not execute paging.

To revert back from limited reachability the UE performs normal TAU procedure without indicating the limited reachability.

6.3.21.2.2 Limited mobility tracking

Similar to section 6.3.21.2.1 the UE utilizes an MM procedure to request limited mobility tracking reporting i.e. the UE does not perform periodic TAU procedures. This request can be triggered e.g. when the UE enters a location where the UE will be for a long period of time.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 188 of 501

6.3.21.2.3 Signalling Flows

Figure 6.3.21.2.3-1.shows high level procedure description for the above solutions.

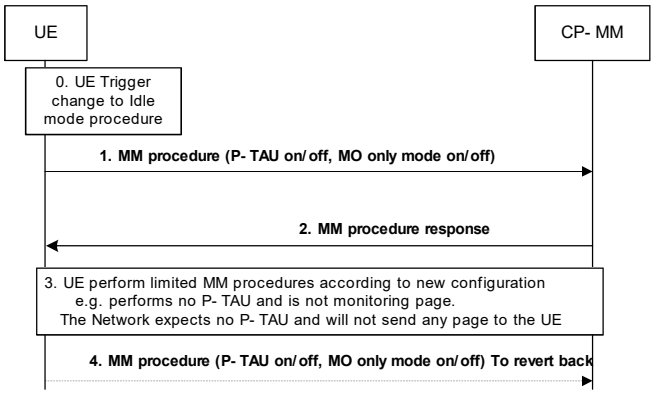


Figure 6.3.21.2.3-1: MM procedure for the UE to request reduced MM signaling in IDLE mode

1. The UE is attached to the network and detects that it prefers to optimize/limit the Idle mode procedures.
2. The UE uses an MM procedure to request a) "no P-TAU" within the same TA and/or b) "MO only mode"
3. The network acknowledged the request.
4. The UE adopts the agreed limited MM signaling, e.g. it no longer sends a P-TAU. In addition, if "MO only mode" then the UE is no longer reachable via a page and network is able to turn off the page signaling to the UE.

NOTE: Note that the UE might be available for Mobile Terminating data transfer for a period of time (e.g. defined by RAN Activity Timer) right after a Mobile Originated procedure. It is for FFS whether and how MT data should be buffered in the network.

5. The UE uses an MM procedure to revert back from limited MM signaling to normal idle mode behaviour.

6.3.21.3 Solution Evaluation

Editor's note: This clause will contain evaluation on the system impacts.

6.3.22 Solution 3.22: Applying customized NextGen mobility states

This solution addresses key issue #3, especially on mobility state aspect.

6.3.22.1 Architecture description

For efficient resource utilization, e.g. signalling saving or energy saving, UEs in different communication scenarios may require different mobility management, e.g. with different mobility states and state transitions as introduced in solution 6.3.8. Therefore, even only a general state model is defined, the NextGen network should be able to flexibly customize mobility states for this UE, and provide optimized mobility management adaptively.

While customizing mobility states and optimizing mobility management for a UE, the network has to take the following information into account:

- UE mobility level, e.g. "no mobility";
- UE preference on reachability, e.g., MO only, MT only, etc.
- Subscription/network configuration

Editor's note: The meaning of mobility level refers to solution 6.3.14.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 189 of 501

After determining the mobility states for a UE, the NG CN needs to inform the UE. Moreover, the NG CN may provide RAN node the assistance information for configuring RRC states, e.g. indication of whether RRC_connected_inactive can be activated for this UE.

6.3.22.2 Function description

The NG CN shall:

1. Determine the mobility states and mobility management behaviours for a UE;
2. Inform RAN node the assistance information for configuring RRC state machine if applicable;
3. Inform the NG UE the determined mobility states;
4. Enable the determined mobility management behaviours in CN.

UE needs to:

1. Communicate its preference, e.g. idle mode preference, to network if it wants;
2. Enable the mobility states received from the NG CN.

The following tables give an example of determining mobility states and mobility management behaviors:

Table 6.3.22.2-1: Parameters for determining mobility states and mobility management behavior

Mobility states or mobility management behaviours	NG UE preference	Subscription or Configuration	Mobility level	Network Decision
IDLE mode	Preferred or not	Allowed or not	No/low/full	Applied or not
Paging	Preferred or not	Allowed or not	No/low/full	Applied or not
RRC_connected_inactive	Preferred or not	-	No/low/full	Allowed or not

Table 6.3.22.2-2: Customized mobility states and mobility management behaviors

Mobility states or mobility management behaviours	Network Decision	NG UE behaviors	NG CN behaviors
IDLE mode	Applied	IDLE mode at end of CONNECTED mode.	IDLE mode at end of CONNECTED mode.
	Not applied	Deregistration at end of CONNECTED mode.	Deregistration at end of CONNECTED mode.
Paging	Applied	Listen for paging in IDLE mode	Triggering paging based on downlink signaling or data
	Not applied	Periodic location update or deregistration	Dropping/buffering downlink signaling or data
RRC_connected_inactive	Allowed	-	Providing the assistance information to RAN
	Not allowed	-	-

NOTE: More optimization on customizing mobility states and mobility management may be provided in other solutions, e.g. (section number of Ericsson solution for MO only case).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 190 of 501

6.3.22.2.1 Procedure of enabling customized mobility states

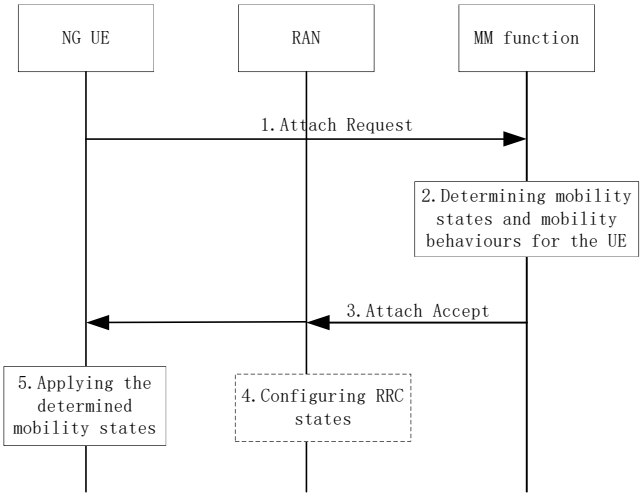


Figure 6.3.22.2.1-1 Procedure of enabling customized mobility states

1. When a NG UE is attached to the network, it may send its preferences, e.g. idle mode preference and paging preference, to the NG CN.
2. Based on preferences from NG UE, UE mobility level, UE subscription and network configuration and so on, the MM (mobility management) function in the NG CN determines the mobility states and mobility management behaviours for this UE. The MM function further applies the corresponding mobility states and mobility management behaviours in the CN side. The MM function may also determine the assistance information for configuring RRC states, e.g. when the UE is in "low mobility".
3. The MM function responses the UE with an Attach Accept, which informs the UE of the determined mobility states and/or behaviours. The NG CN may also provide RAN node the assistance information for configuring RRC state.
4. If the RAN node receives the assistance information from the NG CN, it may take such information into count while configuring RRC states for this UE.
5. The NG UE which received the determined mobility states from the network applies the mobility states and corresponding behaviours

6.3.22.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.23 Solution 3.23: Two layers Tracking Area handling

NextGen system is required to support efficient resource management with regard to different mobility characteristic such as no/low mobility and medium/high mobility. In this solution two layers Tracking Area concept for NextGen system is introduced.

6.3.23.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

Some of NextGen UE/application has static/quasi-static mobility characteristics. Therefore, in order to resolve the scare of paging resource issues, the tracking area should be managed relatively small size (e.g. one or small number of cells) compared with the legacy system. So the core network can trace the static UE in a small size of area thus the paging will be transmitted to restricted area. However, another verticals/applications requires wide range of mobility area.

If the tracking area is small (e.g. one or small number of cells), the scarce of paging resource issues can be resolved for the stationary UE. However the frequency of Tracking Area Update for the medium/high speed mobility UE is

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 191 of 501

increased so the power consumption/increasing of signalling interaction of these devices results in some inefficient situation. Therefore, if the NextGen system supports applications/services which have different mobility characteristics (i.e. no mobility and medium/high mobility type), applying different size of Tracking Area with this "Two layers tracking area handling" is beneficial.

The two layers tracking area handling allows efficient paging area management mechanism for both stationary device and normal mobility device. The concept of the two layers tracking area is that, a cell belongs to two different tracking areas. The first tracking area namely no/low mobility TA is relatively small (e.g. one cell or a few number of cells) and suitable for no/low mobility UE and the second tracking area 'Normal mobility TA" is relatively large and suitable for the medium/high mobility UE/application. In Figure 6.3.23.1-1, deployment example for two layers Tacking Area handling is depicted. There are 5 ANs and these 5 ANs belong to TAC 1 as a Normal Tracking Area but also belongs to TAC 100 to 104 as a No/Low mobility Tracking Area each one by one.

Editor's note: This solution has RAN2 impact so need to check with RAN2.

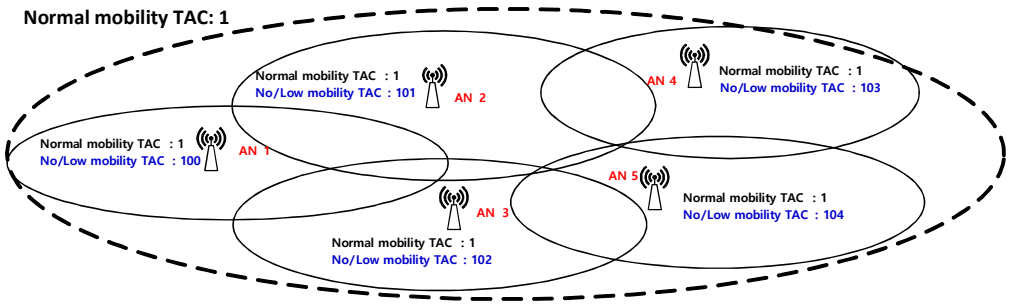


Figure 6.3.23.1-1 Concept of Two layers Tracking Area handling

UE which is configured with different Tracking Area type should act as below.

UEs configured with Normal mobility:

If the UE configured as Normal mobility then the UE should only refer the Normal mobility TAC which is broadcasted via System Information. So in Figure 6.3.23.1-1, this UE shall not trigger Tracking Area Update when the UE moves among AN1 to AN5

UEs configured with No/Low mobility:

If the UE configured as No/Low mobility then the UE should only refer the No/Low mobility TAC which is broadcasted via System Information. So in Figure 6.3.23.1-1, this UE should trigger Tracking Area Update whenever the UE moves to different ANs and the network can figure out the UE's location in each AN granularity. So the network pages UE restricted area.

6.3.23.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Procedure for configuring two layers tracking area handling:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 192 of 501

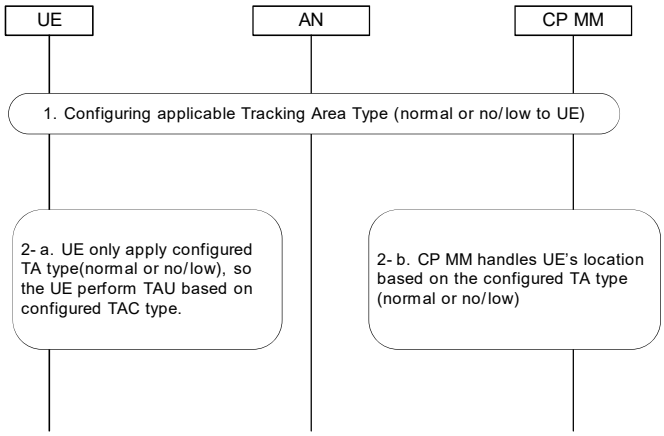


Figure 6.3.23.2-2 Procedure for configuring two layers tracking area handling

1. During Attach/TAU procedure, MME configures applicable Tracking Area type (normal or no/low) to the UE based on UE subscription information and also UE's mobility history. The MME provides Tracking Area list corresponding to the UE's Tracking Area layer (normal or no/low)

2-A. AN broadcast two TACs (one for Normal mobility, one for no/low mobility). A UE read system information and only applies configured Tracking Area type.

2-B. CP-MM maintains UE's location based on the configured Tracking Area type.

6.3.23.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.3.24 Solution 3.24: Mobility pattern based mobility management

This solution applies to Key Issue 3 - Mobility management framework. The solution introduces a solution for Optimised mobility management based on mobility pattern.

6.3.24.1 General description

For efficient resource utilization, e.g. signalling saving and energy saving, UEs in different communication scenarios may require different mobility management methods. The NextGen network should be able to flexibly customize the mobility states, state transitions, location tracking, paging area, reachability management…. and then adaptively apply them to the UEs and the network.

The UE and MM function negotiate the specific mobility pattern.

The mobility pattern could be based on below inputs:

- UE capability: the supported pattern from UE side, low end device, high end device, power (battery) sensitivity.
- UE mobility properties: whether trajectory has a regular pattern, location predictability;
- Mobility speed category: high, medium, low/no;
- Service characteristics: Communication duration time, communication period, uplink service only or not, etc.
- etc.

Both the UE and the network (MM function) can initiate the mobility pattern update which can be either decoupled or combined with the existing location update procedure. The MM function can obtain the UE mobility properties, mobility speed category, service characteristics and potential other information from UE, and/or subscription data, and/or from the Application through capability exposure functions to decide the final mobility pattern for the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 193 of 501

Based on the different mobility pattern, network perform corresponding mobility management optimizations, e.g. determine the UE states and provide necessary assistance information to RAN, limit the MM signalling interactions between UE and network, optimize the paging area, etc.

6.3.24.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

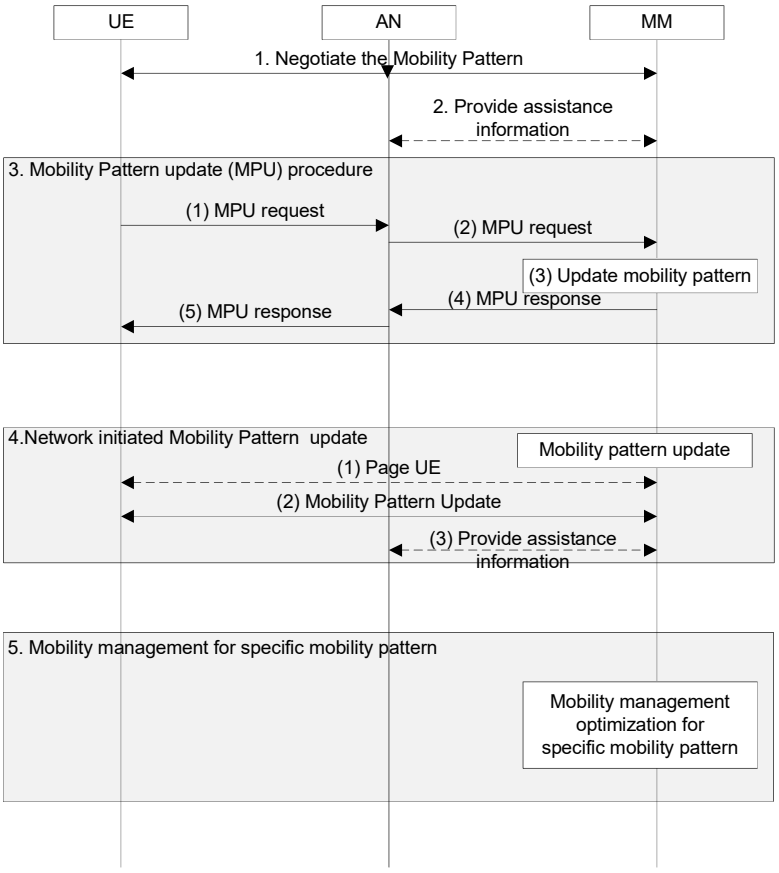


Figure 6.3.24.2-1: Procedure for Mobility mode based mobility management

Negotiate the mobility pattern:

1. During the attach procedure, UE and MM function negotiate the mobility pattern.

MM function obtains the UE mobility properties, mobility speed category, service characteristics and potential other information from UE and/or from the Application through capability exposure functions to decide the final mobility pattern for the UE. MM function sends the decided mobility pattern to the UE.

Editor's note: the mobility pattern may include the UE mobility properties, mobility speed category, and service characteristics information. Further details regarding mobility pattern is FFS.

2. If the mobility pattern has relationship with the RAN behaviour, MM function provides necessary assistance and configuration information to RAN, e.g. indication of whether RRC_connected_inactive needs to be activated for this UE.

Mobility pattern update from UE side:

3. The UE can initiate the mobility pattern update if the network decided mobility pattern is not aligned with the UE behaviour. Based on UE provided mobility pattern information, MM function decides the updated mobility pattern and provides feedback to UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 194 of 501

Network initiated mobility pattern update:

4. The MM function can initiate the mobility mode update, e.g. new session establishment, new trigger from the capability exposure functions, subscription data change. The MM function may first pages the UE and update the mobility mode information to UE. If the updated mobility mode has relationship with the RAN behaviour, MM function provides necessary assistance and configuration information to RAN.

Editor's note: the detailed triggers for the mobility pattern update initiated by UE or Network are FFS.

Editor's note: It is FFS whether the mobility pattern update could be combined with the normal location area update procedure.

Mobility management for specific mobility pattern:

For specific mobility pattern, MM function performs corresponding mobility management optimizations:

- Determine the UE states and provide necessary assistance information to RAN

And the MM function can also provide the necessary assistance information to RAN, e.g. the UE capability, mobility speed category and service characteristics. So the RAN can determine the RRC state based on the received assistance information.

- Based on the mobility speed and mobility properties, generate the mobility prediction information and allocate corresponding location areas for tracking area list management.

The MM function can allocate the location areas based on the mobility prediction information. Considering the UE mobility follows a regular pattern, e.g. when the UE is moving on a highway, its mobility trajectory may remain as a straight line for a period time. So the MM function can allocation the location areas along the highway.

- Based on the mobility speed and mobility properties, limit the paging area.

The mobility properties can further optimise the paging area, especially when the UE mobility trajectory has a regular pattern. The MM function can predict the UE mobility trajectory of UE, and predict the possible UE location in the TA list. So the paging area can be determined based on the TA list and the predicted UE mobility trajectory.

- Based on the communication duration and communication period, allocate different tracking area list for different time.

- For MO only service, minimize the location tracking and reachability management from network.

- ….

6.3.24.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.3.25 UE reachability management in Inactive mode

6.3.25.1 Architecture description

See solution in 6.3.2. The details regarding the procedures on the radio interface and such that affect procedures on the NG2 and Xn interface will be developed by RAN2 and RAN3, respectively.

Editor's note: Final decision on the solution will be taken together with RAN WGs once the solution on RAN Paging is developed.

6.3.25.2 Function description

6.3.25.2.1 Common Functional Elements for all approaches

The following sections describe functions required regardless of the details regardless the realization of the scope for RAN Paging.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 195 of 501

6.3.25.2.1.1 Transition to Inactive mode

This section provides a depiction and description of the procedure used at UE transition to Inactive mode.

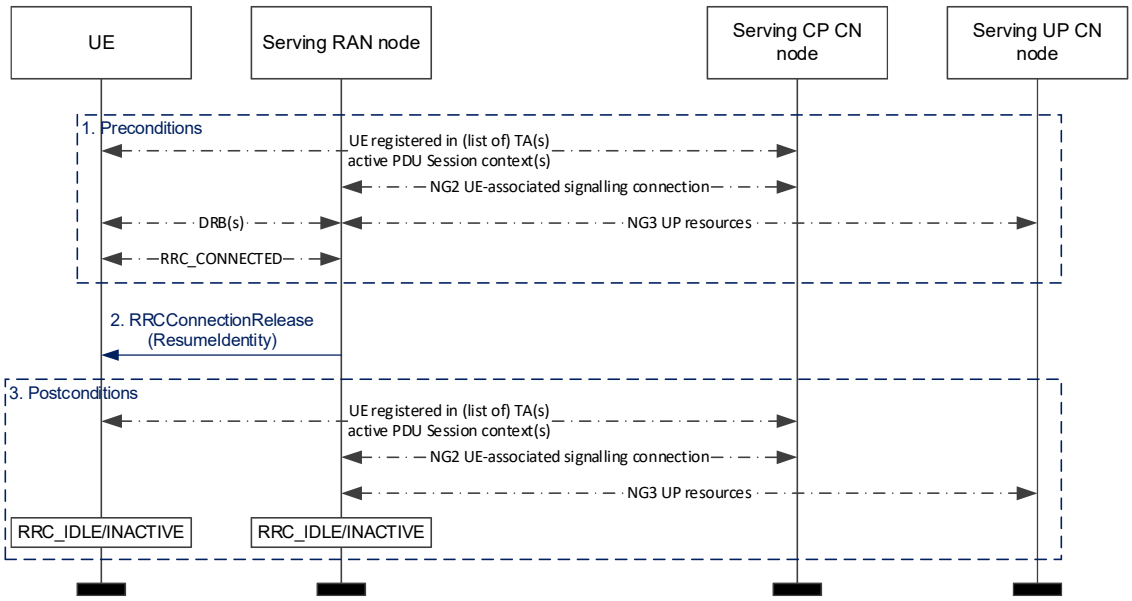


Figure 6.3.25.2.1.1-1: Moving UEs to Inactive Mode

1. Before the UE is moved to Inactive mode, the UE is in RRC_CONNECTED/CN-CONNECTED, i.e registered at the Serving CP CN node in a (list of) TA(s) with PDU Session contexts activated, a UE-associated signalling connection is established on NG2, and bearer contexts are established at the UE, the Serving RAN node and the Serving UP CN node.

2. The UE is moved to RRC_IDLE/INACTIVE (RRC state is FFS in RAN2). The Serving RAN node provides a UE Context identification (ResumeIdentity).

NOTE: Dependent on the chosen approach additional information may be provided in this message (e.g. a list of RAN Paging Area IDs, a list of Cell IDs) (FFS).

3. When the UE was successfully moved to Inactive mode, it is regarded by the CN as being in CN-CONNECTED, it has changed to RRC_IDLE/INACTIVE, it is still registered at the Serving CP CN node in a (list of) TA(s), the UE-associated signalling connection is established towards the Serving RAN node on NG2, NG3 UP resources are kept established but DRBs are released.

6.3.25.2.1.2 Context Retrieval via Xn (based on Rel-13 X2 functions)

This section outlines a stage-2 like description of Xn Context Retrieval. It shows Xn Context Retrieval in the context of RAN Paging, which is not detailed in this section. Further data forwarding and forwarding of NAS related signalling is described.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 196 of 501

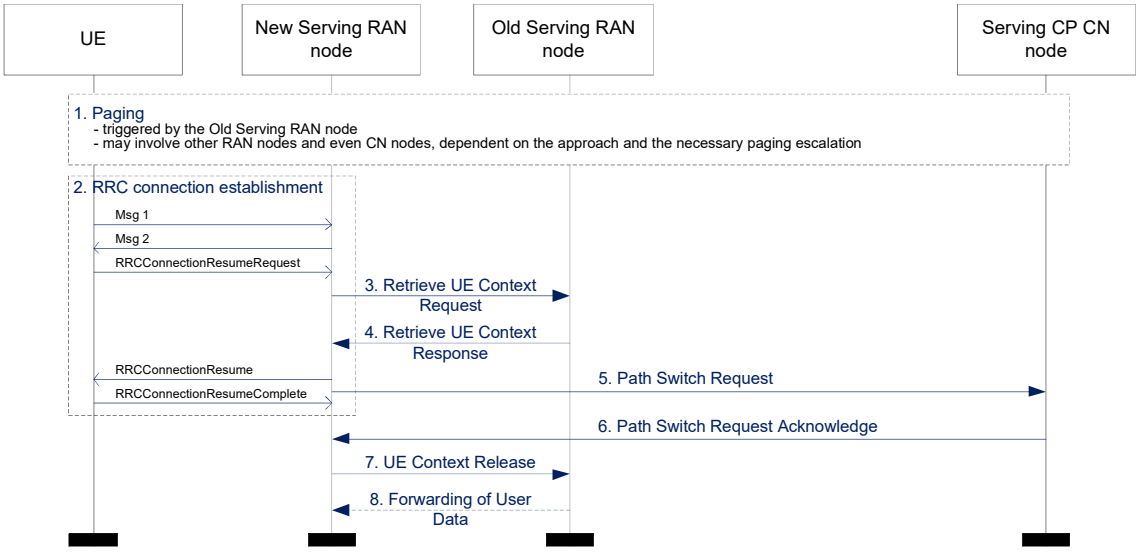


Figure 6.3.25.2.1.2-1: Context Retrieval via Xn

1. In case of a mobile terminating traffic, Paging is triggered by the Old Serving RAN node, which may involve, if necessary, other (neighbouring) RAN nodes and, probably dependent on the approach, the CN.

2. The UE performs the RRC connection establishment procedure. If it has received a Resume ID from the old serving RAN node it provides this ID in the RRCConnectionResumeRequest message. Figure 6.3.25.2.1.2-1 shows the case where the UE performs RRC connection establishment with a New Serving RAN node which is Xn connected to the Old Serving RAN node.

3. The New Serving RAN node attempts to retrieve the UE Context by triggering the Xn Retrieve UE Context procedure.

4. If the Old Serving RAN node is able to resolve the Resume ID it provides UE Context data to the New Serving RAN node.

NOTE: It is for further study whether it is necessary that the response message should also foresee means to forward NAS PDUs.

5.&6. The New Serving RAN node, after having performed admission control, triggers Path Switch Request towards the CN.

7. The New Serving RAN node requests the Old Serving RAN node to release the UE Context. This message may contain DL forwarding addresses.

8. Forwarding of pending DL user data is performed.

6.3.25.2.1.3 Context Retrieval via CN (within the same pool of CP CN nodes)

This section provides description on how a UE Context can be retrieved from the Old Serving RAN node via the CN, which becomes necessary if the New Serving RAN node realises that it has no Xn connection to the RAN node indicated in the Resume ID.

The main principle of this scheme would be to retrieve the UE Context via the same CN pool by means of connection less signalling, as the New Serving RAN node would not know which CP CN node in the pool actually holds the UE Context. Performing Context Retrieval in a connection oriented fashion would require to subsequently tear down the (short-lived) signalling connection unnecessarily and to keep a state-logic in a CP CN node that is not concerned with the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 197 of 501

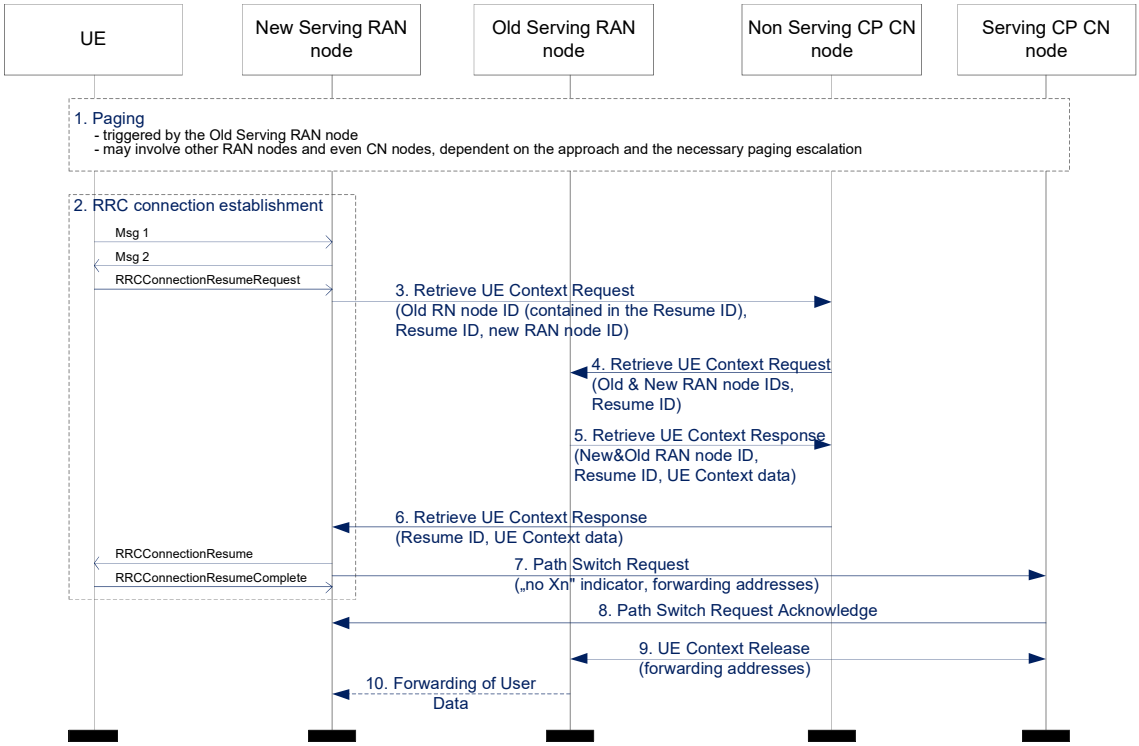


Figure 6.3.25.2.1.3-1-1: UE Context Retrieval via the CN

1. In case of a mobile terminating traffic, Paging is triggered by the Old Serving RAN node, which may involve, if necessary, other (neighbouring) RAN nodes and, probably dependent on the approach, the CN.

2. RRC connection is established, the UE provides the Resume ID in the RRCConnectionResumeRequest message.

3. The New Serving RAN node realises that it has no Xn connection to any RAN node with the identity indicated in the Resume ID and requests a CP CN node within a pool to which it is connected, to resolve the RAN node identity. This CP CN node doesn't necessarily need to be the CP CN node serving the UE. Respective signalling is performed in a connection-less and (for the CP CN node) stateless manner.

4. If the CP CN node is able to resolve the address of the indicated RAN node identity, it forwards the request to that node.

5. The Old Serving RAN node provides UE Context Data.

NOTE: It is for further study whether it is necessary that the response message should also foresee means to forward NAS PDUs.

6. The CP CN node forwards the information received in step 5 to the New Serving RAN node.

7. The New Serving RAN node triggers the path switch procedure (as if it would have received UE context data via Xn) and indicates that no Xn connection is available towards the Old Serving RAN node. The message also contains forwarding addresses.

8. The CP CN node response to the Path Switch Request.

9. The CP CN node triggers the UE Context Release procedure (as the New Serving RAN node is not able to trigger it via X2) and provides forwarding addresses.

10. If necessary, forwarding of user data takes place. Dependent on network configuration and deployment, either direct or indirect forwarding is applied.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 198 of 501

6.3.25.2.1.4 Context Retrieval failed (either on Xn or via NG2)

This section provides description of how a failed context retrieval is handled, also containing details of data forwarding of pending DL user data in the Old Serving RAN node.

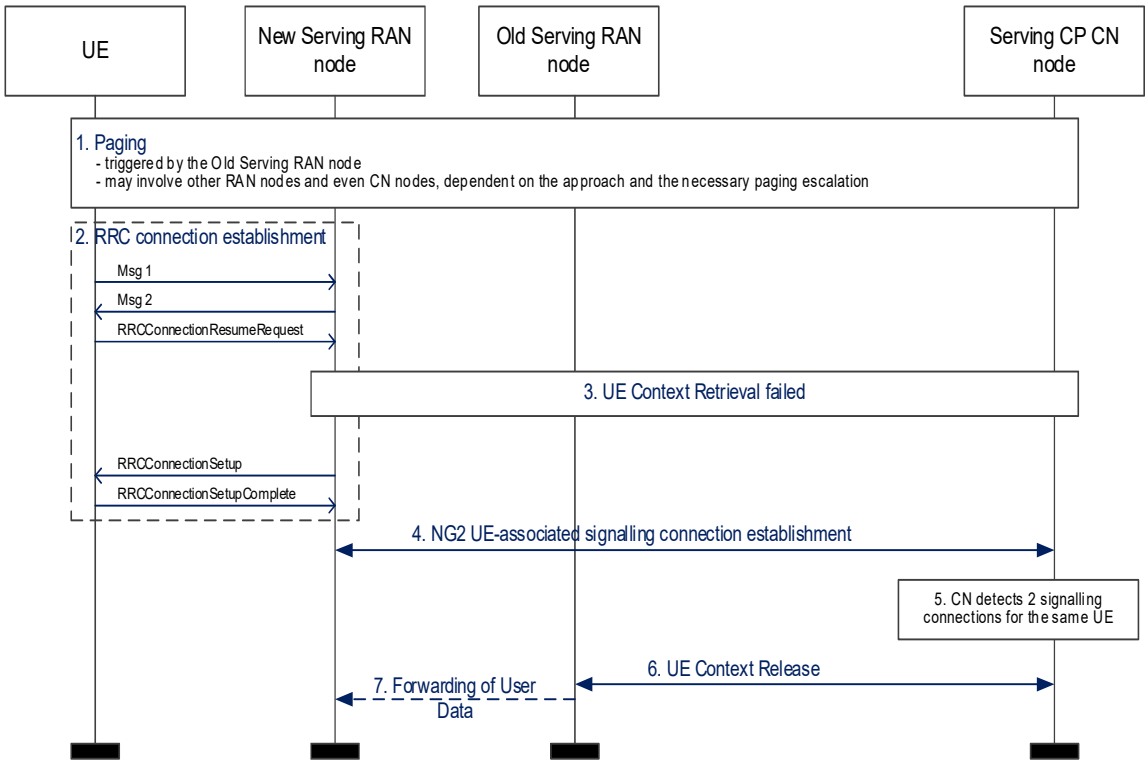


Figure 6.3.25.2.1.4-1: Failed Context retrieval.

1.&2: The UE is paged and establishes the RRC connection, first trying to provide the Resume ID.

3. Retrieving the UE Context, either by Xn or NG2 fails. The RRC connection establishment commences without the Resume ID.

4. The New Serving RAN node establishes an NG2 UE-associated signalling connection.

   If it is required to allow data forwarding also in this, the following scheme is proposed: In order to avoid lengthy additional signalling, the New Serving RAN node should provide forwarding addresses to the Old Serving RAN node in steps 4 and 6.

5. The CP CN node detects that 2 signalling connections exist for the same UE and releases the one towards the Old Serving RAN node.

6. Forwarding addresses are provided from the CN as received by the New Serving RAN node.

7. If necessary, forwarding of user data takes place. Dependent on network configuration and deployment, either direct or indirect forwarding is applied.

6.3.25.2.1.5 Xn Paging

This section outlines a stage-2 like description of the Xn Paging procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 199 of 501

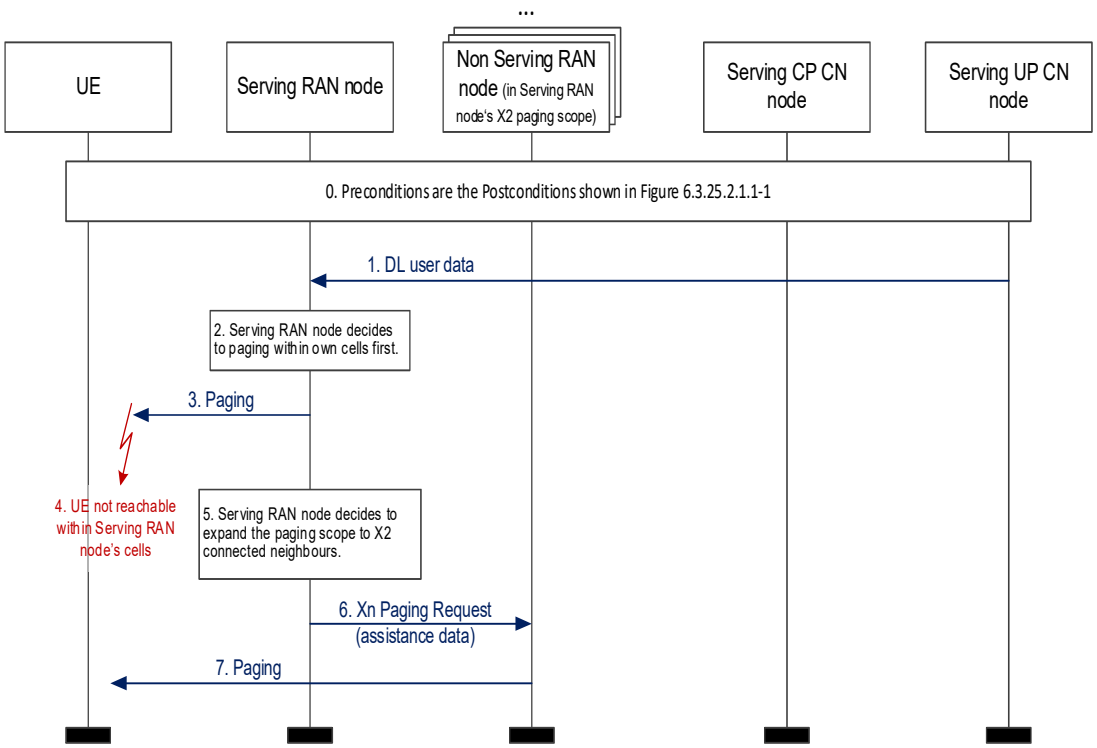


Figure 6.3.25.2.1.5-1: Xn Paging

0. The UE is in RRC_IDLE/INACTIVE and the Serving CP CN node regards the UE being in NG CM-CONNECTED, as described for the post conditions in section 6.3.25.2.2.1.

1. A DL user data packet arrives at the Serving RAN node

2. The Serving RAN node, based on available statistics, decides to page within its own cells first.

3.&4. The first paging attempt is not successful.

5. The Serving RAN node, based on available statistics, decides to expand the paging scope to its direct Xn neighbours.

6. The Serving RAN node sends a Paging Request to the selected Xn neighbours, including assistance data (Paging Attempt Count, Recommended Cell List, etc.)

7. The neighbour nodes page the UE.

6.3.25.2.2 Functional elements necessary if the RAN paging area is configured on NAS level (Tracking Area approach)

6.3.25.2.2.1 CN assisted RAN Paging

CN Assisted RAN Paging is needed if the Serving RAN node is not able to reach the UE by paging in its own and its Xn connected neighbour eNBs' cells.

A NG2 message is introduced for trigger the CN to distribute pages into an area indicate by the serving RAN node.

The RAN Paging Area and cell-list approaches heavily rely on Xn connectivity, which is not always given. If paging assistance data would indicate cells/nodes outside the RAN serving node's Xn connectivity, CN assisted RAN paging would need to be applied also for those approaches.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 200 of 501

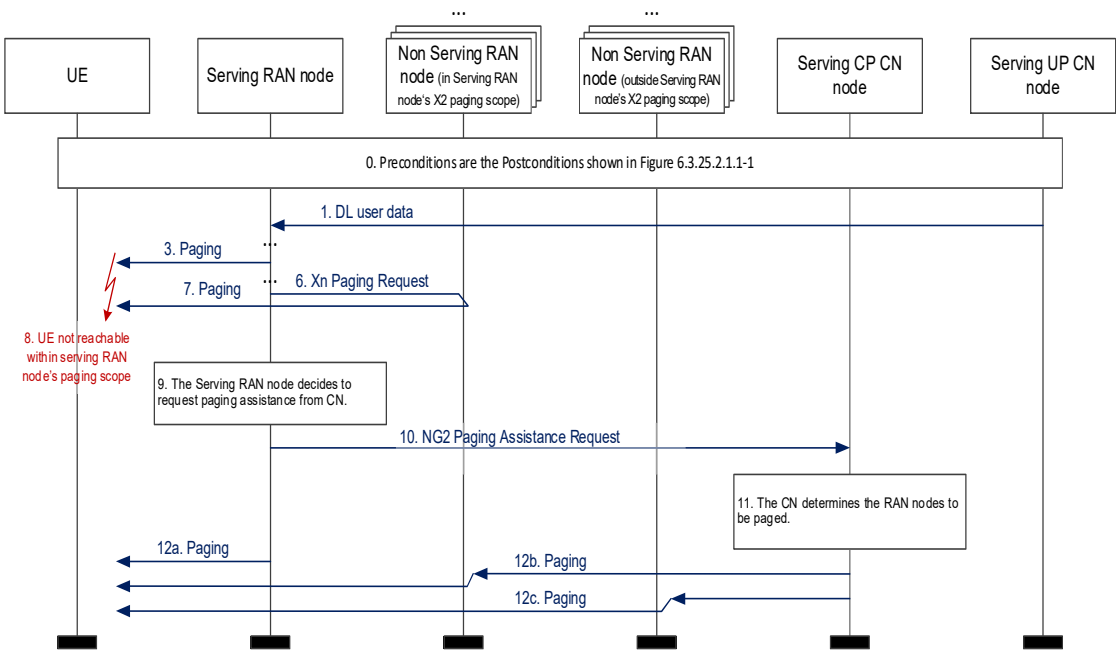


Figure 6.3.25.2.2.1-1: CN assisted paging

0.-7. These steps are described in section 6.3.25.2.1.5.

8. The UE hasn't been reachable the previous paging attempts in cells of the Serving RAN node and its Xn-connected neighbours.

9. The Serving RAN node decides to request assistance from the CN.

10. RAN sends a Paging Assistance Request to the CN.

11. CN determines the RAN nodes for paging. As the Serving RAN node is in charge of the overall paging process and the CN is only supposed to distribute S1 Paging messages to the RAN nodes within the paging scope, the Serving RAN node would need to be provided by the Serving CP CN node with respective paging parameters within NG2 Context Setup and Modification signalling. Examples for parameters are: (e)DRX related parameters, etc.

12a. The Serving CP CN node doesn't mirror back the Paging Assistance Request to the Serving RAN node which performs another paging attempt within its cells.

12b. Paging is distributed to RAN nodes that might have been previously requested via Xn to page the UE.

12c. Paging is distributed to RAN nodes that are out of Xn-reach for the Serving RAN node.

A paging response will be handled as described in sections 1.3 and 1.4 above.

6.3.26 Solution 3.26: Intra-RAT HO procedure

6.3.26.1 Architecture Description

This contribution proposes a solution for Key Issue 3, WT 4: intra-RAT mobility.

Intra MME and inter-MM HO procedure are supported in EPS system. The similar scenarios should be supported in NextGen system.

- Intra-NextGen CN handover: NextGen RAN is changed but NextGen CN is not changed.
- Inter-NextGen CN handover: NextGen RAN is changed and the NextGen CN is changed as well.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 201 of 501

Figure 1 is the architecture of intra-NextGen CN HO. X2 based HO is used to support intra-MME HO in EPS and the similar procedure is proposed to support intra-NextGen CN HO in NextGen system.

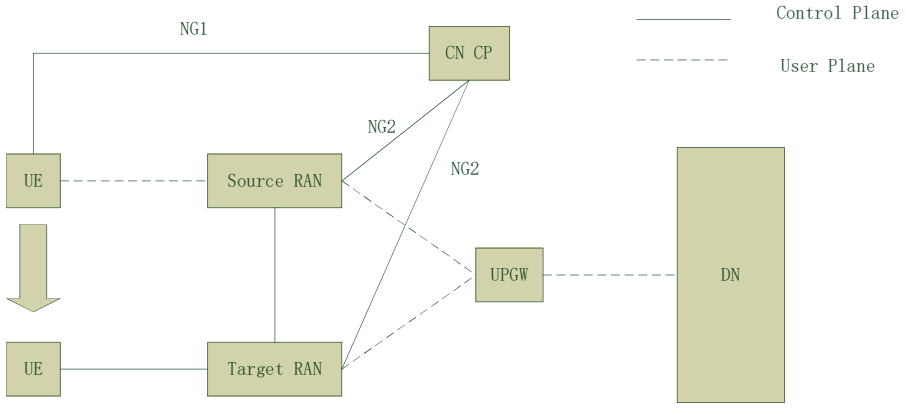


Figure 6.3.26.1-1: Architecture of Intra-NextGen CN HO

Figure 2 is the architecture of inter-NextGen CN HO. The NG2 based HO procedure which is similar to the S1 based HO procedure is proposed to support this scenario.

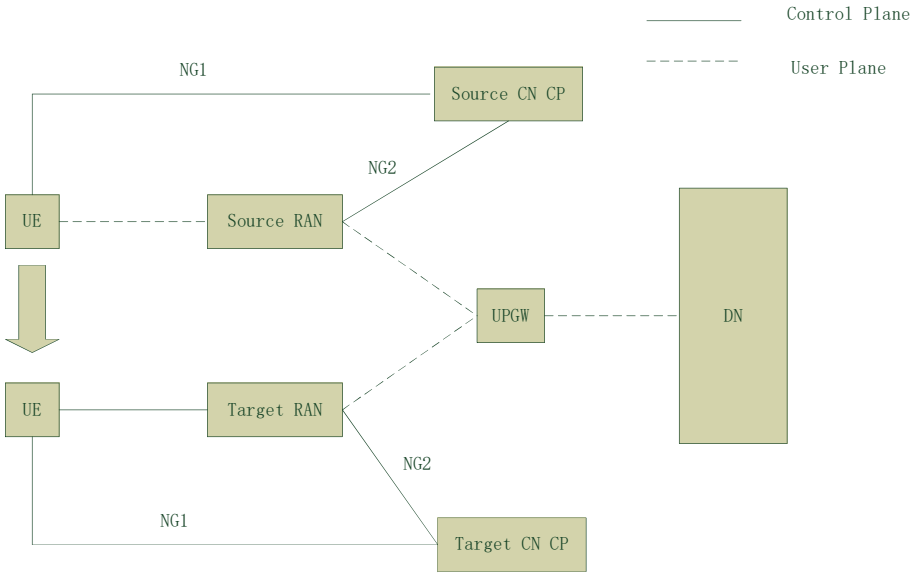


Figure 6.3.26.1-2: Architecture of Inter-NextGen CN HO

It is not impose the number of UP-GWs for a PDU session in the user plane. Considering the requirements that multiple PDU sessions are supported for the same data network, for these PDU sessions towards the same data network, there is the need of a convergence point to support the bitrate enforcement and charging. Therefore, if there is a convergence UP anchor for the PDU session, the convergence point may be relocated during the HO procedure.

The proposed solution of handover procedure assumes the following principles:

- The handover procedure is initiated by RAN.
- The target cell selection is performed by RAN, the target cell selection may consider the UE's restriction list, UE's mobility level, etc.
- Source MM selects the target MM if the NextGen MM will be changed during the HO procedure.
- Target MM selects the target SM if the NextGen SM will be changed during the HO procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 202 of 501

6.3.26.2 Function description

6.3.26.2.1 Intra-NextGen CN HO

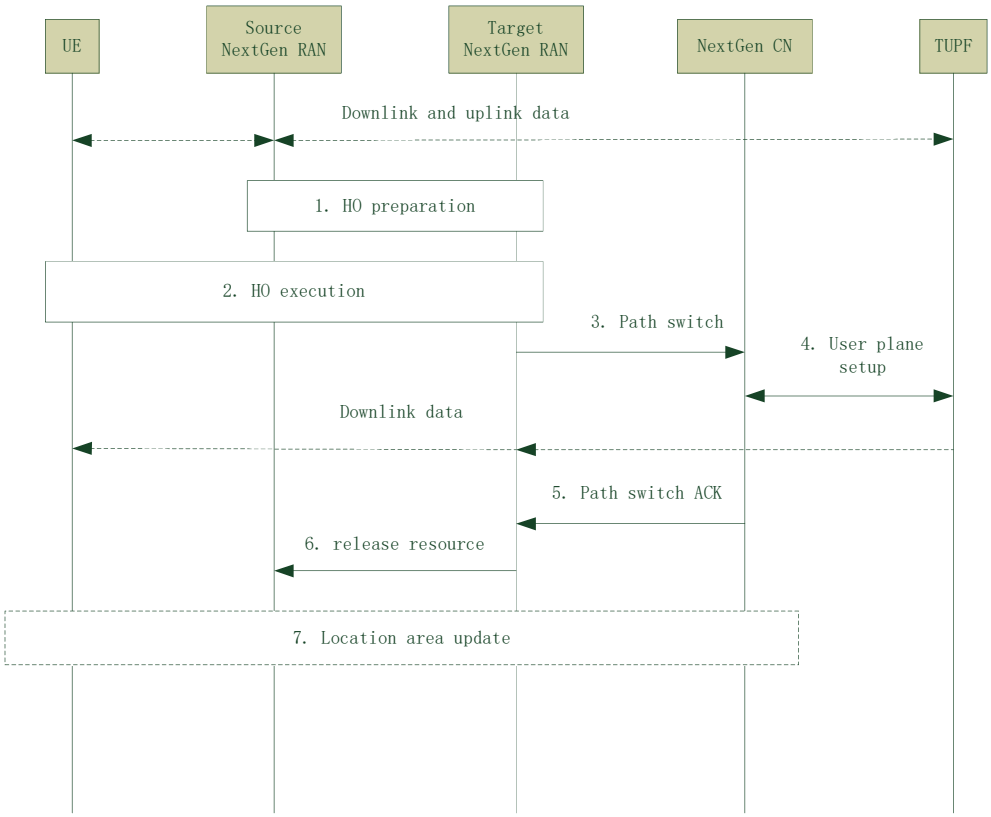


Figure 6.3.26.2.1-1: Intra NextGen CN HO procedure

1. Source NextGen RAN initiates the HO procedure. HO preparation procedure is performed between source NextGen RAN and target NextGen RAN. Target NextGen RAN performs the admission control for the PDU session connection which is sent from source NextGen RAN.

2. Source NextGen RAN informs UE HO command and UE accesses to the target cell.

Editor's note: The details of step 1 and step 2 are defined by RAN WG.

3. The target NextGen RAN sends a Path Switch message to NextGen CN to inform that the UE has changed cell, including the PDU session context to be switched. The DL tunnel ID and IP address for the PDU session is included in the PDU session context.

4. NextGen CN establishes the user plane path for the PDU session in the core network. The DL tunnel ID and IP address for the PDU session is sent to the TUPF.

5. NextGen CN sends the Path Switch ACK message to NextGen RAN.

6. The target NextGen RAN sends the resource release message to the source NextGen RAN.

7. UE initiates the location area update if it is necessary.

If there is a mobility anchor for a PDU session, the mobility anchor may be relocated by the NextGen core according to the target cell. The user plane setup in step 4 shall be used to establish the user plane path throug the new mobility anchor.

During the handover procedure, the user plane data path can be established between Source NextGen RAN to Target NextGen RAN to support data forwarding.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 203 of 501

Editor's note: The details of data forwarding mechanism are defined by RAN.

Editor's note: How to handle the SSC mode 2 / SSC mode 3 PDU session for the handover procedure is FFS.

6.3.26.2.2 Inter-NextGen HO procedure

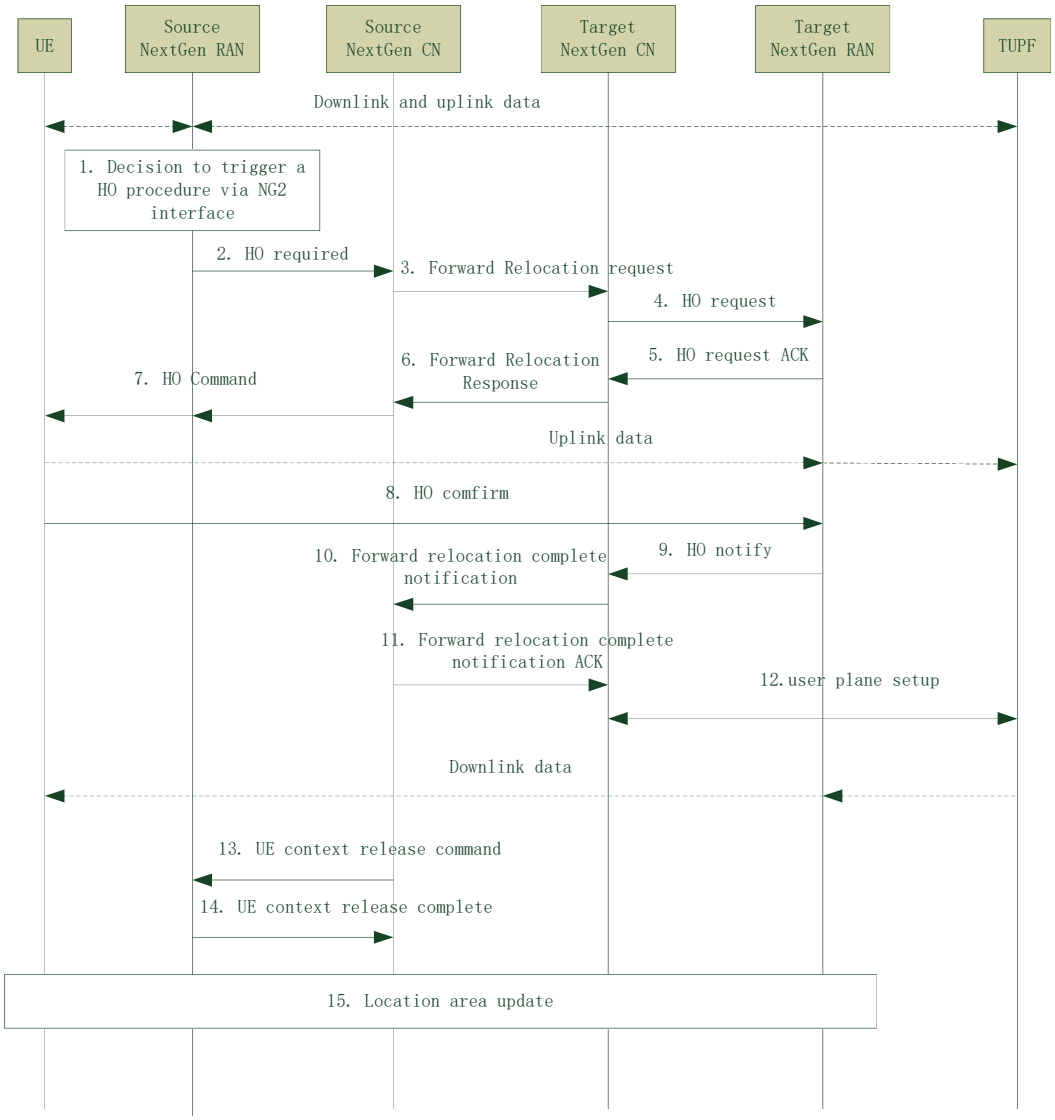


Figure 6.3.26.2.2-1: Inter NextGen CN HO procedure

Step 1: The source NextGen RAN decides to initiate an NG2-based HO to the target NextGen RAN.

Step 2: The source NextGen RAN sends HO required to the source NextGen CN.

Step 3: Source NextGen CN selects the target NextGen CN and sends a Forward Relocation Request message to the target NextGen CN. The UE context including MM context and SM context are included in the message.

Step 4: The Target NextGen CN sends Handover Request message to the target NextGen RAN. This message creates the UE context in the target NextGen RAN. Target NextGen CN allocates the UL tunnel identity and IP address for the activated PDU session and included in the PDU session information sent to the target NextGen RAN.

Step 5: The Target NextGen RAN sends a Handover Request Acknowledge message to the target NextGen CN, including the PDU session which is accepted by the target NextGen RAN. Target NextGen RAN allocates the DL

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 204 of 501

tunnel ID and IP address for the PDU session and included in the PDU session information sent to the target Target NextGen CN.

Step 6: The target NextGen CN sends a Forward Relocation Response message to the source NextGen CN.

Step 7: The HO command is send to UE to trigger to UE access to the target cell.

Step 8: After the UE has successfully synchronized to the target cell, it sends a Handover Confirm message to the target NextGen RAN.

Step 9: The target NextGen RAN sends a Handover Notify message to the target NextGen CN to inform UE which is HO success.

Step 10: The target NextGen CN sends a Forward Relocation Complete Notification to inform source NextGen CN that the HO is success.

Step 11: The source NextGen CN in response sends a Forward Relocation Complete Acknowledge message to the target NextGen CN.

Step 12: Target NextGen CN establishes the user plane data path for the PDU sessions.

Step 13: Source NextGen CN sends a UE Context Release Command message to source NextGen RAN to release its resources related to the UE.

Step 14: Source NextGen RAN sends the response message to the source NextGen CN.

Step 15: UE initiates the location area update if it is necessary.

If there is a mobility anchor for a PDU session, the mobility anchor may be relocated by the NextGen core according to the target cell. The user plane setup in step 12 shall be used to establish the user plane path throug the new mobility anchor.

During the handover procedure, the user plane data path can be established to support data forwarding.

Editor's note: The details of data forwarding mechanism are FFS.

Editor's note: How to handle the SSC mode 2 / SSC mode 3 PDU session for the handover procedure is FFS.

6.3.27 Solution 3.27: Multiple level Tracking Areas handling

In this solution, multiple level tracking areas are introduced for mobility management.

6.3.27.1 Architecture description

CP/MM allocates multiple level TAI lists, PT (i.e. Periodic Tracking Area Update timer value) and RT (i.e. UE Reachable Timer value) information for the UE during Attach/TAU/TAI relocation procedure. The relationship between different level TAI list, PT and RT are as follows:

- Level 1 TAI list> Level 2 TAI list> Level 3 TAI list>…>Level n TAI list (i.e. TAI list size: large to small)
- PT1< PT2< PT3<…<PTn (i.e. PT: small to large) (PTn: level n Periodic Tracking Area Update timer value)
- RT1< RT2< PT3<…<RTn (i.e. RT: small to large) (RTn: level n UE Reachable Timer value)

For ease of understanding, an example for two level TAI lists is described in the figure 6.3.27.1-1, for the level 2 TAI list, the tracking area can be discrete. The relationship between RT and PT values are depicted in figure 6.3.27.1-2.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 205 of 501

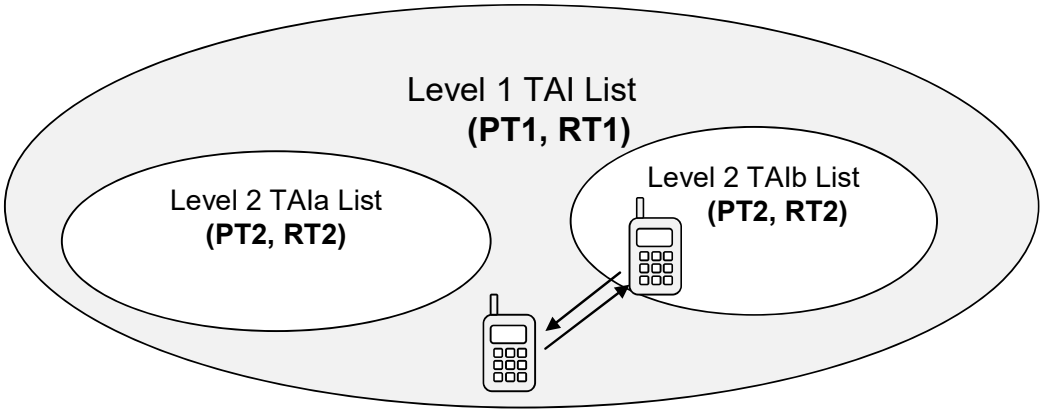


Figure 6.3.27.1-1: two level TA lists

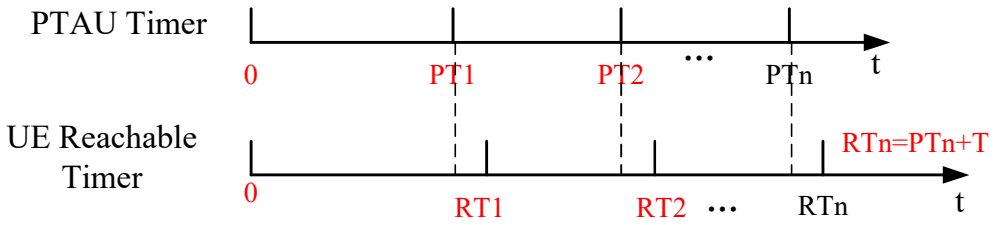


Figure 6.3.27.1-2: Relationship between the PT and RT

6.3.27.2 Function description

6.3.27.2.1 Multiple level Tracking Area Allocation

Normally, how the CPF determines and allocates a TAI List or multiple level TAI list to a UE is implement specific and will not be defined in the 3GPP TS for NextGen network. Two methods are introduced to provide some guidelines on multiple level Tracking Area Allocation:

Method 1: When the UE access to the network at first time, the core network can allocate a multiple level TAI list based on the UE current location as described in the initial allocation of figure 1, associated periodic update timer value for each level also be sent to the UE with the multiple level TAI lists together. The network can estimate the UE's track (i.e. the UE mobility pattern) based on the timer's status and UE's history track and shrinks the level 1 tracking areas assigned to the UE step by step. If the core network determines the UE always camps in level 3 TAI lists, the core network can reallocate a new multiple level TAI lists and sets the level 3 TAI lists as the new level 1 TAI list and the higher level TAI list (and more smaller Tracking Areas) are allocated accordingly, see the reallocation in the figure 6.3.27.2.1. According to this method the core network can achieve accurate UE tracking more quickly and can initiate the Paging at smaller tracking areas.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 206 of 501

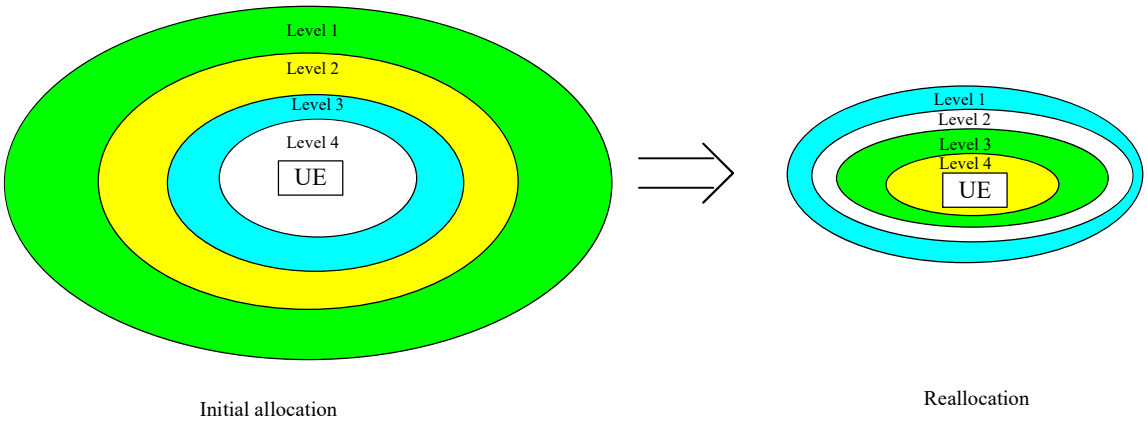


Figure 6.3.27.2.1-1: Multiple level tracking area allocation

Method 2: The core network can determine the TAI list using any available mechanism (e.g. solution 3.11, etc), based on this solution, the core network can set the determined TAI list as the Level 1 TAI list, and shrinks the higher level TAI lists level by level as descripted in initial allocation of figure 6.3.27.2.1. This solution can be used for any available TA management solution to determine the TAI list.

6.3.27.2.2 Multiple level Tracking Area Update in the UE

When the UE enters in IDLE state, the UE starts all levels periodic TAU timer from its initial value. The UE performs periodic Tracking Area Updates with the network based on the status of periodic TAU timer associated to the highest level TAI list the UE located. The detailed flows are depicted as below:

- UE identifies the highest level which it currently locates, e.g. level i;
- UE determines the status of PTAU timer is expired for the identified highest Level TAI list, the UE performs the PTAU procedure. If the UE locates in a higher level area, even the lower level PTAU timer expires, the UE does not perform the PTAU procedure.

When the UE move from one level to another level TAI list, UE performs the PTAU based on the target highest level PTAU timer status the UE locates.

If the UE enters to a new TA that is not in the allocated TAI lists, the UE initiates the Normal TAU procedure, and the CP/MM will performs a new multiple level TAI list allocation procedure.

6.3.27.2.3 Reachability Management for UE in IDLE state

When the UE enters in IDLE state, the CP/MM runs all level reachable timer. If all the timers expire in the CP/MM, the CP/MM can deduce that the UE is not reachable. If the CP/MM determines to page the IDLE state UE, to decrease the paging message overhead, the CP/MM should page the UE in the minimum TAI list UE locates. The paging area can be selected by CP/MM according to the RT timers' status as followed:

- The CP/MM checks that the level(1~x) RT timers are expired and level (x+1~n)RT timer does not expire;
- The CP/MM paging the UE based on the level (x+1) TAI list.

6.3.27.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4 Solutions for Key Issue 4: Session management

6.4.1 Solution 4.1: Session Management functions and relations

This solution applies to key issue 4 on session management.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 207 of 501

6.4.1.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

This solution describes PDU Session properties and functionality related to session management.

The PDU Connectivity Service is provided by a PDU Session.

Properties of a PDU Session:

- The NextGen systems will support connectivity towards different types of DN (e.g. Internet, IMS, corporate/private) and they need to be distinguished by some kind of identifier. The DN is identified by a DN name.
- Each PDU Session is associated with a PDU Session type that indicates what PDU type(s) are carried by the PDU Session. The PDU Session Type may be of IP Type, Ethernet Type or non-IP Type.

Editor's note: It is FFS whether non-IP PDU type should be renamed to something more descriptive.

The following functions are included as part of the solution for Session Management:

- Packet forwarding;
- Packet screening, i.e. the capability to check that the UE is using the exact IP address/prefix that was assigned to the UE;
- Session control, i.e. the overall functionality to handle SM signalling and managing PDU Sessions;
- Selection of user plane function.

NOTE: Functions related to e.g. QoS, charging, LI are not included here but are assumed to be described by solutions to other key issues.

Editor's note: The relation between user plane function selection and network slicing, e.g. in case the UE is connected to more than one slice, is FFS.

The Session Management functionality is used to provide PDU Connectivity Service for different PDU types, including IP, Ethernet and non-IP PDU types. Certain session management functionality is PDU type specific, such as e.g. IP address allocation for IP-based PDU types. However, to achieve a generic and re-usable NextGen system it is desirable that most functionality is common for all different PDU types. The following assumptions apply for the solution:

- The session management procedures (e.g. for establishing new PDU sessions and modifying/terminating established PDU sessions) are common to all PDU types. However, some information carried by the session management signalling may be PDU specific (e.g. IP addresses in case of IP-based PDU types).
- The solution does not require PDU-specific user-plane transport between AN and the core network.

For an IP-based Data Networks, also the following functions are part of the solution for Session Management:

- UE IP address allocation.

For an IP-based Data Network, the PDU Session can be identified by one or more allocated IP address(es)/prefix(es) and the DN identity.

Editor's note: Further details regarding sessions for non-IP DNs is FFS.

The allocation of Session Management functions to UE, AN and CN is shown in the Figure below. Note that the figure does not assume any specific grouping of these functions into logical Network Functions / Network Entities. This is instead assumed to be handled as part of work on the overall architecture.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 208 of 501

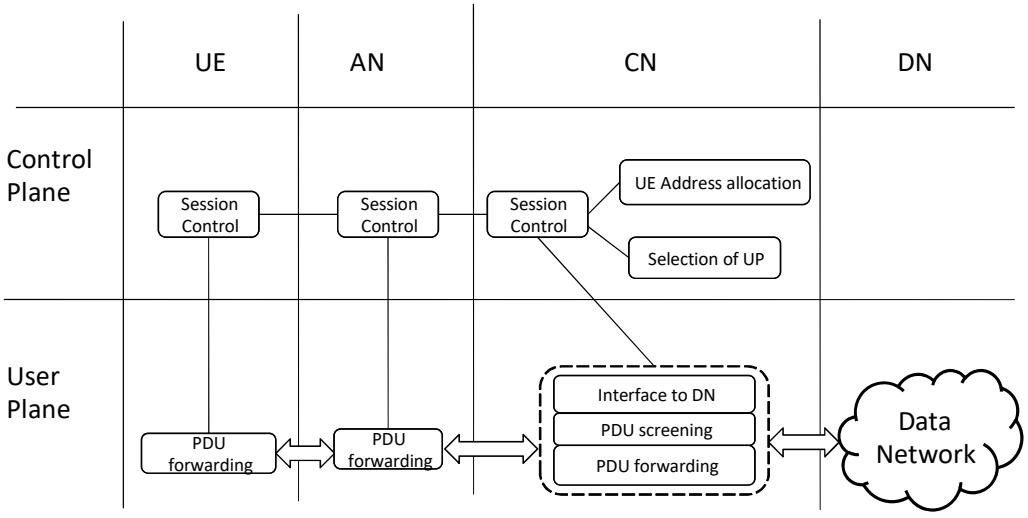


Figure 6.4.1-1: Session management functions

Editor's note: The figure above does not imply that the level of session control and session knowledge in the AN is the same as in the UE and CN, and does not detail how the AN is involved in signalling related to session handling. Further refinement of the AN functionality is FFS.

6.4.1.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.4.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.4.2 Solution 4.2: Session setup procedures

This solution addresses the Key Issue 4: Session management, specifically, on the session setup procedures.

6.4.2.1 Architecture description

Session management of next generation system may not be involved during the attach procedure. A UE may request session establishment procedure under the following states:

a) Unattached, session established with attach procedure (EPS-like session establishment).

b) Attached but no session established, the UE already attached to the network and would like to get IP/Non-IP connection for data transfer.

c) Already have session established, the UE already have session established over one or multiple DN(s), and would like to have another session.

Editor's note: It is FFS whether the same UP function is selected for all sessions to a single DN or whether separate UP functions may be selected is FFS.

Therefore, keeping at least one session is not mandatory but if needed for the desired service (e.g. eMBB service), it should be controlled as always-connected session.

Editor's note: It is FFS whether always-connected session is requested by UE or based on per subscription.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 209 of 501

The session management architecture could be depicted as Figure 6.4.2-1, where the SM is the function in control plane for session management handling.

The procedures below assume that a user plane tunnel is established between AN and the user plane functions in the core network.

Editor's note: The "User Data" in the figure below is the data repository of information related to session management and user subscription. Whether it is a standalone network function or collocated with some network function is FFS.

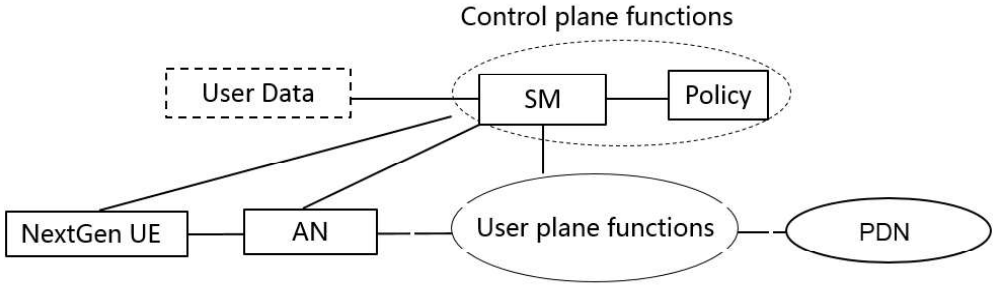


Figure 6.4.2.1-1: The non-roaming architecture for session management

The home-routed roaming architecture is shown in Figure 6.4.2-2.

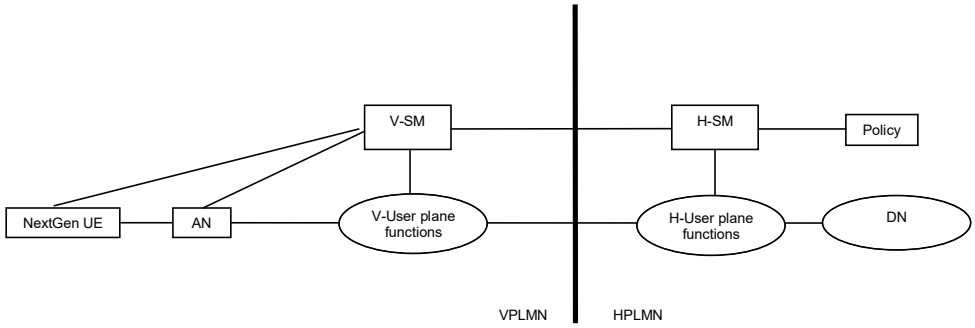


Figure 6.4.2.1-2: The home-routed roaming architecture for session management

Editor's note: The architecture figures above describe the logical relation between functionality for session management. Reference points used for session management for NextGen architecture and additional description of relation to other functionality in NextGen system such as mobility management functionality and is FFS.

Editor's note: Whether a "User Data" function needs to be added to the roaming architecture for session management is FFS.

Editor's note: Whether there is a need for a Policy control function in the VPLMN is FFS and also handled as part of the policy framework key issue.

6.4.2.2 Function description

6.4.2.2.1 Session establishment procedure, non-roaming case

A session can be established, released and modified and this clause shows how a session is established.

The procedures are depicted in the Figure 6.4.2.2.1-1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 210 of 501

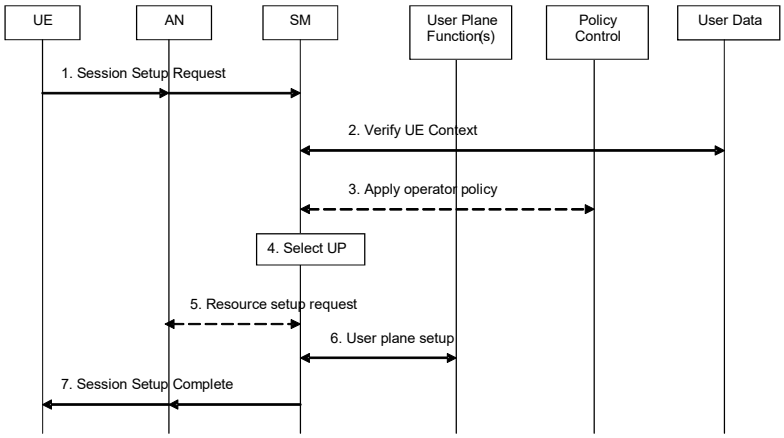


Figure 6.4.2.2.1-1: The procedure of session setup

Editor's note: Further details regarding UE IP address/prefix assignment is FFS.

Editor's note: It is FFS whether a procedure with two SM functions and two User Plane Function(s) as in the home routed roaming case applies also in the non-roaming case.

It is assumed for this procedure that the UE is attached to the network. As part of the attach procedure, subscription data is fetched from the Subscriber Data Management function.

1. The UE initiates a session setup request. The UE provides information indicating the PDU session type (e.g. Non-IP/IP). Indication of the DN network name may also be included. This step may be combined with the attach procedure in case the session is established with the attach procedure (EPS-like session establishment). It is assumed that this message is carried via an access/MM function and that this includes verification that the UE is attached and has an MM context.

Editor's note: It is FFS whether the DNN is identical to the APN.

2. The SM function fetches user data. Get related information from the UE context and may verify that the UE subscribed the service. If the authorization done as part of step 1, then this step 2 is not needed.

3. The SM function may interact with the Policy control function which determines the QoS property of the connection based on information such as UE request, and operator policy.

Editor's note: Based on the solutions developed for the QoS and Policy Framework Key Issues, it will determine how the QoS related property is set per operator policy.

4. The SM function selects the proper user plane function and, in case of connection type is IP, assigns IPv4 address/IPv6 prefix anchored in the User plane function.

5. The SM function may request the AN to setup resources for the session.

6. The SM function triggers the establishment of user-plane. The message includes the related QoS requirement for the connection to be established. Downlink tunnel information is also sent to the User plane functions (e.g. IP address of the AN node).

7. Uplink tunnel information is sent to the AN function (e.g. IP address of the User plane functions). This completes the PDU session setup procedure.

IPv6 stateless address auto-configuration or DHCPv4 may be used for IP address/prefix allocation after PDU session established. In this case, the DHCPv4 or RS/RA messages will be forwarded by the UP function between UE and the SM function.

Editor's note: In the case of Non-3GPP AN case, step 5 may not be needed. This is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 211 of 501

6.4.2.2.2 Session establishment procedure, home-routed roaming case

This clause shows how a session is established in a home-routed roaming case. The procedures are depicted in the Figure 6.4.2.2.2-1.

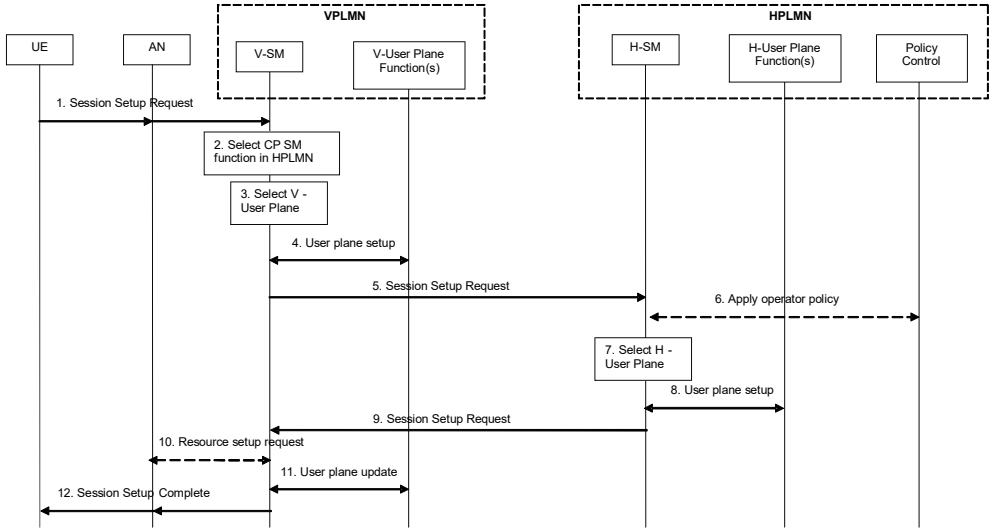


Figure 6.4.2.2.2-1: The procedure of session setup in a home-routed roaming case

It is assumed for this procedure that the UE is attached. As part of this, the attach procedure subscription data is fetched from a Subscriber Data Management located in the home network.

1. The UE initiates a Session Setup Request. The UE provides information indicating the PDU session type. Indication of the DN network name may also be included. This step may be combined with attach procedure in case the session is established with the attach procedure (EPS-like session establishment).

Editor's note: It is FFS whether the DNN is identical to the APN.

2. The SM Function in the VPLMN selects a SM Function in the home network.

3. The SM Function in the VPLMN selects proper user plane function(s) in VPLMN.

4. The SM function triggers the establishment of user-plane. The message includes the related QoS requirement for the connection to be established.

5. The SM Function in VPLMN sends a Session Setup Request to the SM Function in HPLMN. Downlink tunnel information (e.g. the IP address of the User Plane Function(s) in the VPLMN) is included in the request.

6. The SM Function in HPLMN may interact with the Policy Control function that determines the QoS property of the connection based on information such as UE request, and operator policy.

Editor's note: Based on the solutions developed for the QoS and Policy Framework Key Issues, it will determine how the QoS related property is set per operator policy.

7. The SM Function in HPLMN selects proper user plane function(s) and in case of session type IP, IPv4 address/IPv6 prefix assignment is performed as part of this step.

8. The SM function triggers the establishment of user-plane. The message includes the related QoS requirement for the connection to be established. Downlink tunnel information (e.g. the IP address of the User Plane Function(s) in the VPLMN) is sent to the user plane function(s).

9. Session setup is complete in the HPLMN and the SM Function in HPLMN sends a response to the SM Function in the VPLMN. Uplink tunnel information (e.g. the IP address of the User Plane Function(s)) is included in the message.

10. The SM Function in the VPLMN function may request the AN function to setup resources for the session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 212 of 501

11. The Control Plane Function in the VPLMN updates the user plane function(s) in the VPLMN with uplink tunnel information (e.g. the IP address of the User Plane Function(s)).

12. Uplink tunnel information is sent to the RAN function (e.g. the IP address of the user plane function(s) in the VPLMN). The UE is informed that session setup has succeeded.

IPv6 stateless address auto-configuration or DHCPv4 may be used for IP address/prefix allocation after PDU session established. In this case, the DHCPv4 or RS/RA messages will be forwarded by the V-UP/H-UP functions between UE and the H-SM function.

Editor's note: The verification of UE context (equivalent to step 2 of clause 6.4.2.2.1) is FFS.

6.4.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.4.3 Solution 4.3: NextGen Session Management with Multiple PDU sessions to the same Data Network

This solution applies to key issue 4 on session management, and parts of key issue 1 on network slicing. Specifically, the solution addresses the following work tasks:

- SM_WT_#1 SM Model
- SM_WT_#2 Relation between MM and SM
- SM_WT_#5 Multiple Accesses PDU Sessions

6.4.3.1 Architecture description

Editor's note: Non-IP session management is FFS.

In this solution for NextGen Session Management (NSM), a UE may establish multiple PDU Sessions to the same data network in order to satisfy different connectivity requirements of different applications (e.g. session continuity) that require connectivity to the same data network. In addition, different UP-GWs may be allocated for the different PDU Sessions to the same data network.

The solution is based on the following architecture:

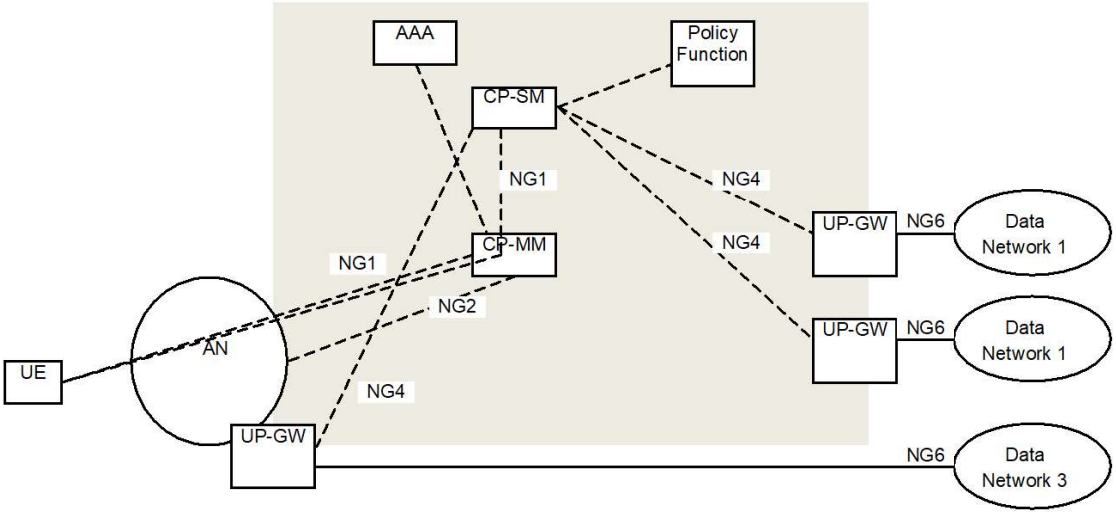


Figure 6.4.3.1-1: Session Management high level architecture.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 213 of 501

The functional entities in the architecture are defined as follows:

- CP-MM: the Control Plane Mobility Management function is in charge of establishing and maintaining the MM context for a device attaching to the NextGen network, including interacting with the. The CP-MM also implicitly interacts with CP-SM to validate the establishment of an NSM context for a UE that has securely established an MM context.

Editor's note: Whether one or multiple CP-MM instances are applied when the UE connects to multiple network instances/slices is FFS and depends on the definition for the architecture for network slices.

- CP-SM: the Control Plane Session Management function is responsible for establishing, maintaining and terminating PDU Sessions on-demand for the UE in the NextGen system architecture.

- AAA: NextGen CN profile repository and authentication server, stores the subscriber profile of the NextGen network operator, the subscriber credentials, and authentication algorithms. Authentication of the UE (e.g. at attach) is performed via the AAA.

Editor's note: it is FFS whether the CP-MM or the CP-SM interacts with the AAA to authenticate the UE based on the subscription profile, and depends on the solution for other key issues.

The solution is based on the following model:

- For a given network slice, the UE has a single MM context established with a CP-MM function.

Editor's note: This assumption is dependent on the solutions for the key issue on network slicing, and may need to be revisited when such solutions are defined.

- A UE can have a MM context established with the network without requiring the establishment of any PDU Sessions, but a PDU Session can be established simultaneously to an MM context.

- For each MM context, a UE can associate multiple SM contexts (i.e. PDU Sessions).

- The attempt to establish any PDU Sessions in relation to an MM context is authorized based on the UE previously having established an MM context.

- UP-GW selection and allocation is performed upon establishment of a PDU Session. UP-GW selection for a PDU Session is performed considering the connectivity requirements of the PDU Session to enable optimized establishment of the data path for each PDU Session.

- The UE can establish multiple PDU Sessions to the same data network. Different PDU Sessions connecting to the same data network may be served by different UP-GWs and, in the case of IP PDU Sessions, may have different IP addresses.

- A UE may be served by different CP-SM functions for different PDU Sessions (e.g. if specialized features need to be implemented by CP-SM for specific services).

In this solution, the establishment of a PDU Session may optionally be authorized/authenticated by the external DN via the session management functionality, similarly to how a PDN connection was authorized by an external data network:

- This enables the external data network to provide service-specific information for the data flows for the data network including QoS requirements, packet filtering information, e.g. for encrypted data, etc., to the CP-SM.

- The NextGen CN of the MNO uses such information as input for e.g. QoS establishment ,to perform packet filtering, and to select the UP-GW(s) for the PDU Session. Establishment and authorization of connectivity in an operator network is maintained under the control of the operator in the serving CP-SM, since the UE has a single active operator subscription being used with the operator network.

The following figure describes the functional allocation for this session management solution.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 214 of 501

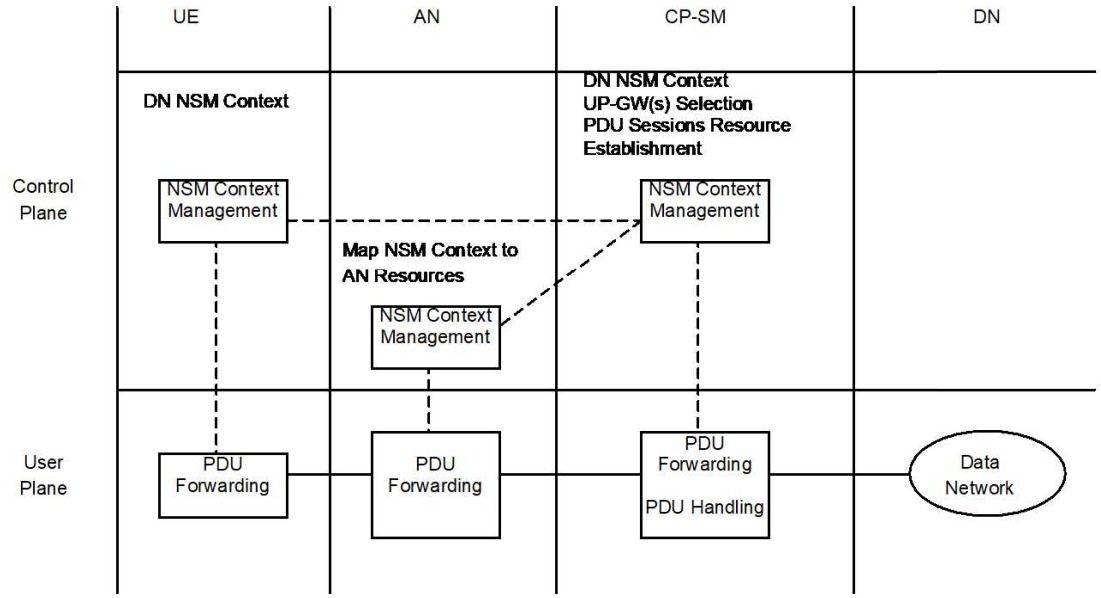


Figure 6.4.3.1-2: Functional Distribution for Session Management

6.4.3.1.1 NextGen Session Management Model and States

The NextGen Session Management (NSM) states describe the signalling connectivity between the UE and the NextGen CN. The NSM states are supported independently of the access network technology the UE is using, and therefore the relationship between the NSM states and the mobility management states is defined in such a way that the NSM states apply to any AN connected to the 5G NextGen, including scenarios in which the UE supports no mobility. This is proposed in order to have an NSM model that is independent of the specific access network mechanisms.

Editor's note: the exact relationship between the NSM states and the Mobility Management states is FFS and depends on the solutions for mobility management.

Editor's note: the states described below apply to the NSM state machine in the network.

Two NSM states are proposed for connectivity to a Data Network, independently on the number of PDU Sessions the UE has established to a given Data Network:

- NSM-IDLE.
- NSM-CONNECTED.

6.4.3.1.1.1 NSM-IDLE

A UE is in NSM-IDLE state when no PDU Sessions have been established for the UE. Any UE state in the AN, and the presence of an interface between the AN and the NextGen CN are based solely on the mobility management context.

Editor's note: the mobility management procedures that the UE perform when in NSM-IDLE are FFS and depend on the solutions on mobility management.

6.4.3.1.1.2 NSM-CONNECTED

The UE and the CP-SM enter the NSM-CONNECTED state for a specific Data Network when a PDU Session is established and the UE and the CP-SM have an NSM context.

The UE can be in NSM-CONNECTED state independently from the mobility management state, given that the UE is registered.

For a UE in the NSM-CONNECTED state, there exists a logical signalling connection between the UE and the CP-SM function. The logical signalling connection is transported over the AN with AN-specific mechanisms, and in the NextGen core network via the MM functions to the CP-SM function. While the UE is NSM-CONNECTED for a Data Network, the UE may add further PDU Sessions to the same Data Network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 215 of 501

Editor's note: the relationship between the state transitions and the establishment of AN and core network resources for QoS is FFS.

6.4.3.1.1.3 State transition and functions

The NSM model transitions from NSM-IDLE to NSM-CONNECTED for a Data Network when the first PDU Session to the Data Network for a UE is established.

The NSM model transitions from NSM-CONNECTED to NSM-IDLE for a Data Network when the last PDU Session to the Data Network for the UE is released.

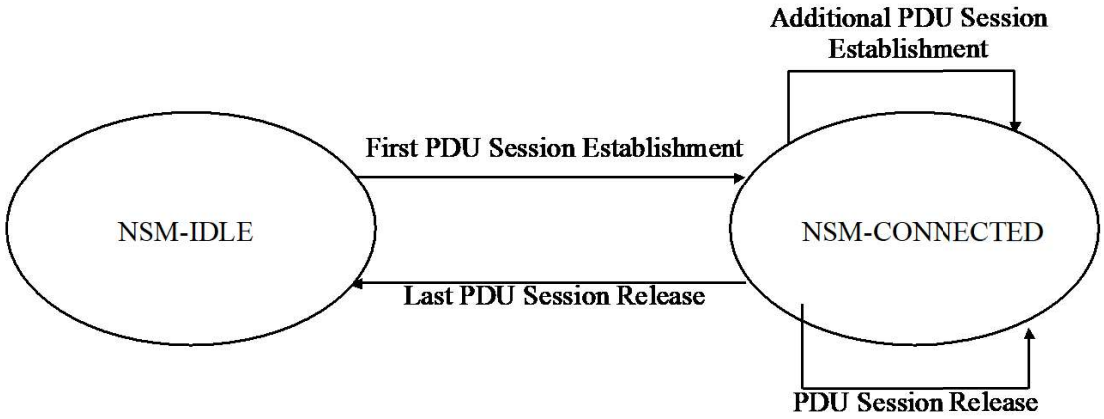


Figure 6.4.3.1.1.3-1: NSM state model.

6.4.3.1.2 NSM Context

An NSM context in the UE and the CP-SM function contain:

- A Data Network NSM context, containing all the PDU session contexts for each PDU session of the UE. This enables the CP-SM function to keep track of and correlate resources and status per-UE, independently of the number of PDU Sessions the UE has established towards a Data Network.
- For each PDU Session established, the connectivity information specific to the PDU Session.

In addition the CP-SM function maintains information about PDU session resources, including the allocated UP-GWs.

Editor's note: the details of the actual contexts parameters is FFS.

6.4.3.2 Function Description

Editor's note: The specific protocols for DN SM context establishment are FFS. It is expected that a subset of the current NAS functionality will be supported, independently of the protocol supported, depending on the solutions designed for other key issues (e.g. QoS, congestion control, etc.).

6.4.3.2.1 UE PDU Session Establishment Triggering

In this solution it is assumed that the UE is aware of the connectivity requirements for applications/services, including:

- The Data Network required for an application/service and the corresponding DN Name
- Specific connectivity requirements with respect to the transport, e.g. the type of session continuity for the data flow, etc.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 216 of 501

It is furthermore assumed that when applications require connectivity, they either provide specific connectivity requirements (e.g., regarding session continuity; type of connectivity in terms of local breakout, remote; etc.) or the UE is configured with information regarding connectivity requirements of specific applications.

Editor's note: The exact relationship between session management and session continuity requires further study and depends on the solutions developed for session continuity.

Editor's note: It is FFS whether and how the UE can be configured with such information, if applications cannot provide such requirements. e.g. in the same way that in EPC it was possible to define per-application ANDSF policies based on application ID, similarly per-application ID connectivity requirements could be provided in the UE.

Once a MM context has been established, the UE triggers the establishment of a new PDU session to a Data Network, even if the UE already has one or more PDU Sessions for the same Data Network when an application requires connectivity with specific requirements (e.g. session continuity) and no existing PDU Session satisfies such requirements. The UE determines whether one of the existing PDU Sessions to a Data Network satisfies the connectivity requirements of the application based on the connectivity requirements provided at the establishment for the previous PDU Sessions.

The UE provides in a PDU Session Request:

- The PDU Connectivity Requirements, which may contain one or more of:
  - Requirements for session continuity
  - A DN User Identity for the UE for the external Data Network, provided by the UE for connectivity to a specific Data Network when the UE requests the PDU session authorization via the external Data Network. The DN User Identity is specific to a Data Network.

Editor's note: it if FFS what additional PDU Connectivity Requirements the UE can provide.

- A Data Network Name, identifying the Data Network the UE requires connectivity to. The DN Name is optional and the network may decide how to provide the connectivity solely based on operator policies and the PDU Connectivity Requirement.

If the UE requests the establishment of a PDU Session for applications that require connectivity for services provided by an external Data Network and that require authorization and authentication via the external Data Network, the UE triggers the PDU Session authorization only for the first PDU Session to the external Data Network.

6.4.3.2.2 UP-GW Selection

During the establishment of a PDU Session, the network needs to select the UP-GW(s) serving the PDU Session.

The UP-GW selection is performed by the CP-SM based, when available, on:

- The DN Name if provided by the UE
- The UE subscription profile
- Network policies
- The PDU Connectivity Requirement.
- DN Service-specific Requirements provided by the external DN during the PDU Session authorization and authentication
- UE location
- Load conditions of candidate selected UP-GW

For the establishment of an additional PDU Session to a DN for which PDU Session(s) already exists, the CP-SM verifies if the existing UP-GW(s) can be used based on the PDU Connectivity Requirement provided by the UE, the subscription profile, etc. The CP-SM may select different UP-GW(s) to serve the new PDU Session and interacts with the UP-GW(s) for the establishment of the PDU Session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 217 of 501

The CP-SM may select one or multiple UP-GWs for the PDU session depending on the connectivity requirements, e.g. in roaming scenario a UP-GW in the VPLMN and a UP-GW in the HPLMN may be selected if traffic for the PDU Session need to be routed to the HPLMN.

6.4.3.2.3 Establishment of a PDU Session

Once a MM context has been established, if specific connectivity requirements arise in the UE for an application or service, the UE establishes a PDU Session.

The following procedure applies both to the establishment of a first PDU Session to a data network, and to the establishment of an additional PDU Session to the same data network.

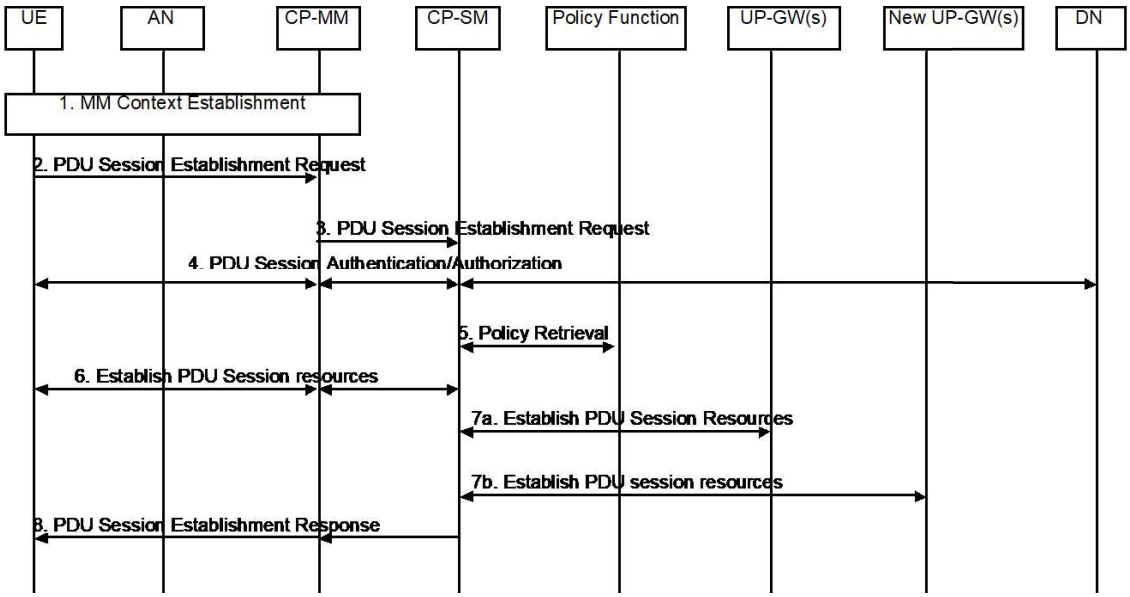


Figure 6.4.3.2.3-1: PDU Session Establishment

1. The UE has previously established a Mobility Management (MM) context via MM procedures with the CP-MM, including authentication.

Editor's note: The details of the establishment of the MM context are defined in the solutions for MM key issue.

2. The UE sends a PDU Session Establishment Request to the CP-MM, includes the PDU Connectivity Requirements, may include a DN Name, and a DN User Identity.

3. The CP-MM selects the CP-SM function to serve the UE based on the DN Name and the PDU connectivity requirements, and forwards the request to the selected CP-SM. The CP-MM may e.g. select a CP-SM in the VPLMN for Data Networks and services to be provided by the VPLMN, and a CP-SM in the HPLMN for Data Networks and services to be provided by the HPLMN and for home routed traffic.

4. The CP-SM verifies the UE request for the PDU Session based on the information provided by the UE with respect to the UE profile, and whether there are already existing PDU Sessions for the same data network. If the UE has provided a DN User Identity,the CP-SM triggers the authentication and authorization of the PDU Session Establishment Request with the external data network based on the DN User Identity provided by the UE. During the authentication procedure, the data network may provide a connectivity profile to the CP-SM containing DN Service -specific Requirements (e.g. QoS, connectivity type, etc.) which override the connectivity requirements provided by the UE. If the UE already has PDU Sessions to the same data network, the CP-SM verifies if additional PDU Sessions are allowed and if an additional PDU Session is required based on the PDU Connectivity Requirements provided by the UE.

5. The CP-SM may interact with the policing function to determine the policies to be applied to the PDU Session, and, if received from the external data network, provides the DN Service-specific Requirements.

6. The CP-SM interacts with the AN for the establishment of the resources required for the PDU Session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 218 of 501

7. The CP-SM:

   7a. If a PDU Session to the same Data Network exists and if the existing UP-GW(s) can be re-used, interacts with the UP-GW(s) for the establishment of the PDU Session (e.g. IP address allocation for PDU Session for IP traffic).

   7b. If it selects new UP-GW(s) to serve an additional PDU Session to the same Data Network, the CP-SM interacts with the new UP-GW(s) for the establishment of the PDU Session (e.g. IP address allocation for PDU Session for IP traffic).

8. The CP-SM confirms to the UE the establishment of the PDU Session and includes information related to the PDU Session contexts (e.g. IP addresses, etc.).

For roaming scenarios, when PDU Session traffic is home routed, the CP-SM may be located in the HPLMN, or there may be a CP-SM in the VPLMN and a CP-SM in the HPLMN. If two CP-SM functions are involved, in steps 7a and 7b the CP-SM in the VPLMN interacts with the CP-SM in the HPLMN for the UP-GW selection. Control of the PDU Session establishment may be in VPLMN or HPLMN (i.e. CP-SM in HPLMN may just perform UP-GW selection)

6.4.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.4 Solution 4.4: Void

6.4.5 Solution 4.5: Network triggered on-demand SM setup procedure

6.4.5.1 Architecture description

This solution applies to Key Issue 4: Session management, specifically on network triggered on-demand SM setup procedure.

On demand SM setup has been agreed as one of the architectural principles. It is possible that when UE has attached to the Network, no PDU session is established. The PDU session can be activated when the UE want to transfer the data. It should also be possible that PDU session can be activated when MT traffic is to be transferred.

It is proposed to introduce a mechanism that the network can trigger the UE to establish the PDN connectivity when it is need. This mechanism applies to all PDU type. The principle of this mechanism is that:

- The network sends a session activation trigger message to the UE.
- When the UE receives the session activation trigger message, it activates the PDN connection as requested.

6.4.5.2 Function description

Editor's note: The detail parameters at each step the flows are FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 219 of 501

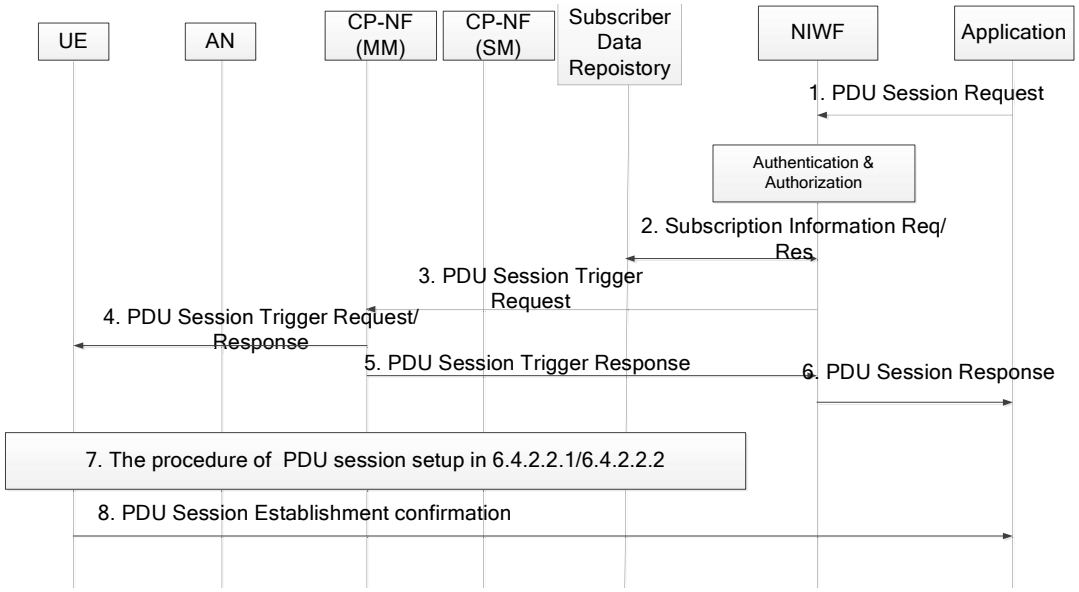


Figure 6.4.5.2-1: Network Triggered PDU Session Setup

1. The Application Server need send the data to UE and the PDU session has not been established between the UE and Application Server. The Application Server sends a PDU Session Request (External Identifier or MSISDN, Application Identifier, validity period, Application Port ID) message to the NIWF (Network Inter Work Function). The Application Port ID is to address a triggering function within the UE. The validity period indicates for how long the PDN Session Request message is valid. So if the trigger message does not reach the UE first time, the trigger message may still be send again if it is still valid.

   The NIWF checks whether the Application is authorised to send the PDU Session Request based on the Application Identifier. The NIWF also check whether the Application server has exceeded its quota or rate of trigger submission.

2. The NIWF sends a Subscriber Information Request (External Identifier or MSISDN and Application Identifier) message to the Subscriber Data Repository to determine the NF which serves the UE, i.e. the CP-NF(MM).

3. The NIWF send the PDU Session Trigger Request (DN name, Application Port ID, Application Identifier) to the determined CP-NF (MM). The DN name indicates which Data Network the PDU session is to be established. It is determined based on the Application Identifier and local configuration.

4. The CP-NF (MM) sends the PDU Session Trigger Request (DN name, Application Identifier, Application Port ID) to the UE. If the UE is not connected, the network pages the UE and delivers the message to the UE. Based on the Application Port ID, the related Application client on the UE is selected. The corresponding response message is send back to the CP-NF (MM) to confirm the receiving the request message.

5. The CP-NF (MM) sends the PDU Session Trigger Response to the NIWF to confirm the Request message has been received by the UE.

6. The NIWF sends the PDU Session Trigger Response to the Application Server.

7. The UE triggers the PDU session setup procedure as described in section 6.4.2.2.1/6.4.2.2.2. The Data Network to be connected is the DN name received at step 4.

8. After the PDU session to the determined DN is activated, the UE send the PDU Session Establishment confirmation message to the determined Application Server as the indicated Application Identifier received at step 4.

6.4.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 220 of 501

6.4.6 Solution 4.6: Common interfaces towards UE, AN and SDM for both MM and SM related procedures

6.4.6.1 Description

This contribution proposes a solution for Key Issue 4, WT 2 (relation between MM and SM).

As seen from the UE, there is a single CP termination point in the core network for the NG1 reference point, used for both MM and SM-related messages and procedures for a UE. The single CP termination point is located in MM.

NOTE: This does not imply that the MM and SM messages and procedures are coupled. How the UE communicates over this reference point for MM and SM is determined by solutions to e.g. MM and SM key issues.

As seen from the AN, there is a single CP termination point in the core network for the NG2 reference point, shared for MM and SM-related messages and procedures for a UE.

As seen from the Subscriber Data Management (SDM) system, there is a single CP termination point in the control plane used for retrieving both MM and SM-related subscription data for a UE from the SDM system. In the figure below this corresponds to the termination for the NG7 reference point between the SDM system and the CP function.

Editor's note: It is FFS whether UE credentials are handled over the same or a separate reference point as other subscription data.

NOTE: The use of a single termination point in the core network for interfaces towards does not imply that a single function in the core network handles both MM and SM functionality. The common CP termination points are shared by MM, SM and potentially the authentication functions.

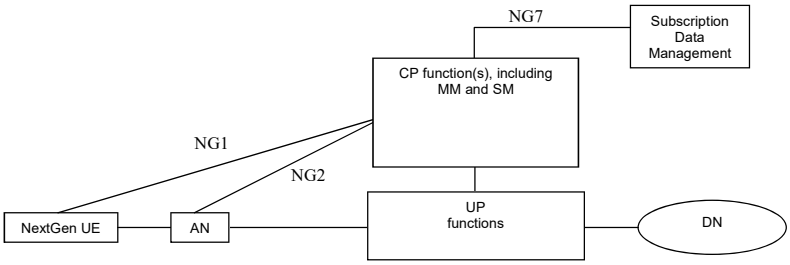


Figure 6.4.6.1-1: Common interfaces towards UE, AN and SDM for both MM and SM related procedures

NOTE: The figure above does not show all CP related functionality e.g. related to policy control.

Editor's note: How the above proposals relate to non-3GPP access is FFS and depends e.g. on how MM functionality is defined for non-3GPP accesses and how the overall architecture with non-3GPP is defined.

Editor's note: How the solution above is related to solutions for a UE connecting to multiple slices is FFS.

Editor's note: Whether and how the solution above is related to support of multiple connectivity is FFS.

6.4.7 Solution 4.7: Infrequent small data transfer

This solution applies to Key Issue 4: Session management, specifically on efficient infrequent small data transfer, which is not required the session to be established.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 221 of 501

6.4.7.1 Architecture description

For carrying infrequent small amount of data units in an efficient way which can reduce the allocation of the network resources, the connection-less small data service (SDS) that does not require a session set up is introduced. The SDS is a service that transfers messages between a UE and Service Provider (SP) or 3rd party. The SDS-PDU is self contained with all required information to deliver it to its destination. The source and destination IDs in SDS-PDU are assumed in the form of URIs.

Figure 6.4.7.1-1 shows the entities that are involved in mobile originated (MO) and mobile terminating (MT) SDS message handling for transfers between a UE and an application server or a Service Capability Server (SCS) in non-roaming scenarios. For the connection-less SDS the system functions called Small Data Handling Functions (SDHF) are introduced in the network to process the address information (the source and destination IDs) in the small data messages and verify and route the messages based on this information. The SDHF does not need to keep context information related to users and no UE attachment and UE authentication is performed.

The integrity of small data messages has to be verified, for example by a SDHF. To verify the integrity of a message the SDHF can get the required security material from the Credential Repository. For instance, the Repository may hold certificates that contain credential data. That is, integrity protection can be done without context information stored in the network, e.g., in the form of a signature that would allow any entity on the path (e.g. Serving SDHF) to check the authenticity of the SDS-PDU once this entity has access to the data (e.g. credentials in the Repository) necessary for validating the integrity protection, which is for SA3 to define, e.g. using a public key infrastructure. Thus, each SDS-PDU is e2e integrity protected.

NOTE 1: 3GPP specifies only integrity protecting the SDS-PDU between the UE and Gateway SDHF. The mechanisms for this protecting are to be determined by SA3. The external entities in the delivery chain (e.g. the SCS/AS) may also verify the SDS-PDU integrity, e.g. using a public key infrastructure, but the mechanisms for this are outside of the 3GPP scope.

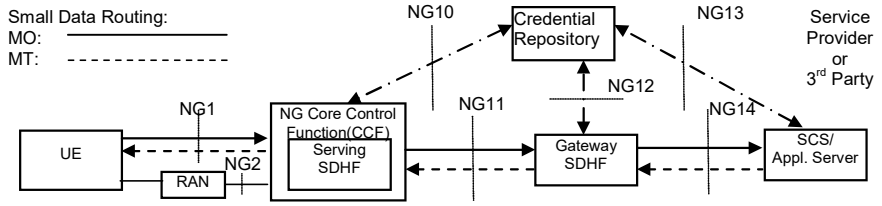


Figure 6.4.7.1-1 Architecture model for the Small Data Service - non-roaming case

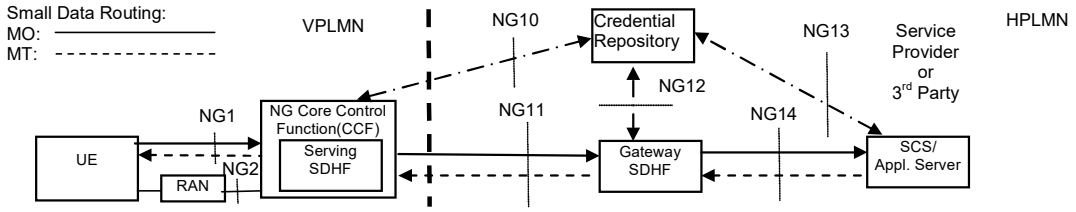


Figure 6.4.7.1-2 Architecture model for the Small Data Service –roaming case

NG1: Reference point between the UE and the NG Core Control plane function.

NG2: Reference point between the RAN and the NG Core Control plane function.

NG10: Reference point between the NG Core Control plane function and the Credential Repository function.

NG11: Reference point between the NG Core Control plane function and the Gateway SDHF function.

NG12: Reference point between the Gateway SDHF function and the Credential Repository function.

NG13: Reference point between the Credential Repository function and the SCS/Application Function.

NG14: Reference point between the Gateway SDHF function and the SCS/Application Function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 222 of 501

On receiving the MO SDS-PDU, the network establishes a short lived association with the UE, i.e. a temporary UE context, on the Serving SDHF to assure that acknowledge/reject messages or a potential user data response can be sent back to the UE. The RAN is assumed to provide an efficient radio transport means for the SDS PDU and maintains the short lived association with the UE, i.e. a temporary UE context, so that the UE remains reachable for receiving the incoming response information after sending the MO SDS-PDU. The association is established at the time when the uplink SDS-PDU is received.

Since the network can process address information (e.g. the source ID) in the small data messages it can set up SDS-PDU counters to control transmission frequency and restrict overload caused by those UEs that send small data too frequent or retry to obtain service (send data) although it was not accepted or allowed by the network. The Serving SDHFs may keep counters/contexts for a while after releasing the association, i.e. the valid time of temporary UE context is expired,to detect these UEs. A counter on the G-SDHF may also be used to count the total number of message transmitted by the UE. This is to restrict the total number UE transmitted SDS-PDUs via different S-SDHFs.

To deal with temporary surges in SDS traffic volume from massive UEs that may temporarily deplete resources available to non-SDS traffic a network operator can put a restriction per cell/resource that may be used by SDS. The upper bound per cell/resource can also limit the possible damages caused in case of some misbehaving UEs.

6.4.7.2 Function description

The uplink transmission procedure for a scenario where the MO SDS-PDU is forwarded to a SCS/AS is illustrated in Figure 6.4.7.4.2-1.

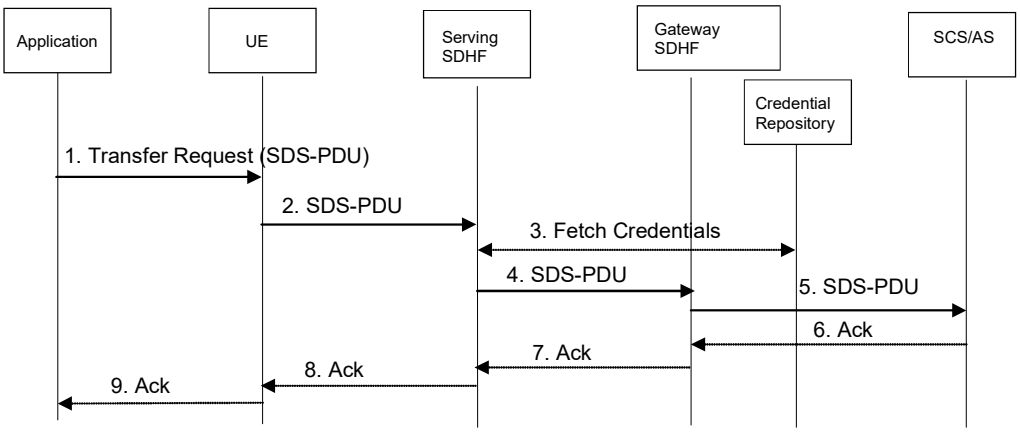


Figure 6.4.7.2-1 Uplink small data transmission procedure

1. The application of the UE requests the transfer of the SDS-PDU.

2. The UE transmits the SDS-PDU to a Serving SDHF. Since there is no need for the serving SDHF to keep any UE or MM context (i.e. no UE attachment and authentication is performed), normally it is not required to forward the SDS PDU to a specific Serving SDHF. However if the transmission frequency of small data is to be controlled, the SDS-PDUs from one UE is expected to be forwarded to the same Serving SDHF. The mechanism is implementation specific, e.g. based on the source ID address. When transferring between the UE and the Serving SDHF, the RAN is assumed to provide an efficient radio transport means for the SDS PDU and the RAN also maintains a short lived association with the UE so that the UE remains reachable for receiving DL traffic for a certain short time period (i.e. the reachability period).

3. The serving SDHF needs to verify the integrity of the SDS-PDU. The Serving SDHF checks whether it stores credentials for the sender of the SDS-PDU, i.e. source ID. If not, the Serving SDHF fetches the credential information for that sender from the Credential Repository. If the credential for the sender is not ok, the Serving SDHF sends a Reject to the UE with an appropriate cause code.

4. The Serving SDHF determines a Gateway SDHF from address information of the SDS-PDU header and forwards the SDS-PDU to the Gateway SDHF.

5. The Gateway SDHF determines the SCS/AS address from the destination ID in the SDS-PDU and forwards the SDS-PDU to the SCS/AS. The Gateway SDHF keeps the Serving SDHF identifier for possible DL traffic

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 223 of 501

delivery within the UE reachability period. The Gateway SDHF may verify the SDS-PDU integrity before forwarding it.

6. On receiving the SDS-PDU the SCS/AS may verify the SDS-PDU integrity if it has access to the Credential Repository. The SCS/AS returns an acknowledgement to the Gateway SDHF to confirm the SDS-PDU transfer if an acknowledgement is requested.

7. If an acknowledgement is requested, the Gateway SDHF sends it to the Serving SDHF.

8. The Serving SDHF forwards the acknowledgement to the UE.

9. The UE confirms the SDS-PDU transfer to the application.

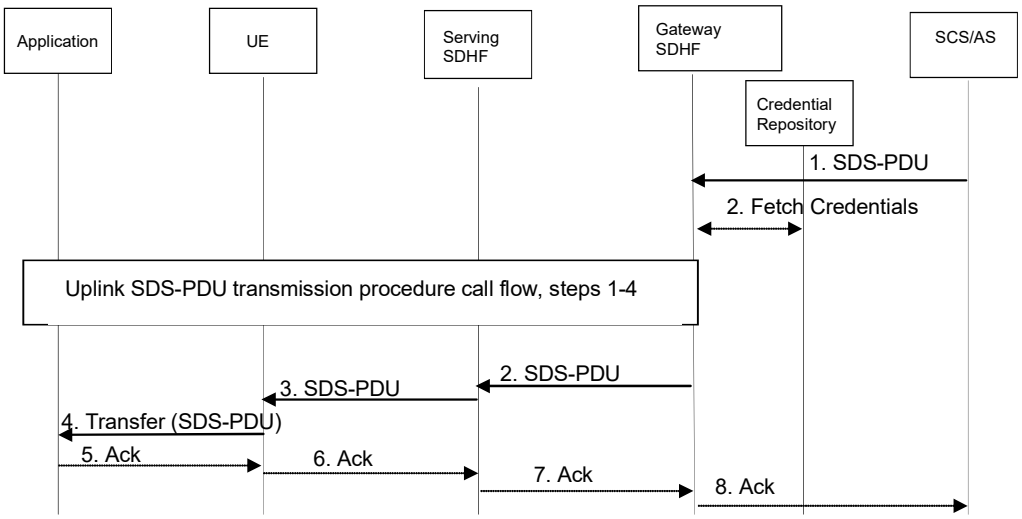


Figure 6.4.7.4.2-2 Downlink small data transmission procedure

The downlink transmission procedure for a scenario where the MT SDS-PDU is delivered towards the UE is illustrated in Figure 6.4.7.4.2-2 and has the following steps:

1. The SCS/AS sends a downlink small data to the Gateway SDHF indicating whether a delivery confirmation is required and possibly the SDS-PDU lifetime. The Gateway SDHF selected by the SCS/AS is same as the Gateway SDHF, which is configured on the UE for MO SDU transmission.

The Gateway SDHF may verify the integrity of the incoming SDS-PDU. In this case it checks whether it stores credentials for the originator of the MT SDS-PDU. If not, the Gateway SDHF fetches the credential information from the Credential Repository verifying the SDS-PDU integrity before accepting it for further delivery. If it is not ok, the Gateway SDHF sends a Reject to the SCS/AS with an appropriate cause code.

On receiving downlink small data SDS-PDU from the SCS/AS the Gateway SDHF checks whether the UE is still reachable after sending the MO SDS-PDU.

- If the UE reachability period is valid the SDS-PDU can be sent to the Serving SDHF immediately.

- If the UE reachability period is expired the Gateway SDHF stores the SDS-PDU in accordance with the permitted SDS-PDU lifetime, until the UE becomes reachable again. A trigger being informed when the UE becomes active is the received uplink small data as illustrated in Figure 6.4.7.4.2-2. The Gateway SDHF checks whether it stores any valid MT SDS-PDU(s) for the sender address of the received MO SDS-PDU. If it is a case the stored SDS-PDU(s) can be sent to the Serving SDHF. In case downlink transmissions dominate or for only downlink transmission scenarios a polling of the Gateway SDHF can be initiated when the UE sends an empty MO SDS-PDU to inform that it is available to receive downlink small data stored by the Gateway SDHF.

2. The Gateway SDHF sends the MT SDS-PDU(s) to the Serving SDHF together with an indication whether a delivery confirmation is needed.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 224 of 501

3. On receiving the MT SDS-PDU(s) the Serving SDHF forwards it towards the UE. The Serving SDHF may verify the MT SDS-PDU integrity before forwarding it.
4. The UE transfers the SDS-PDU to the application. The UE may verify the MT SDS-PDU integrity before transferring it to the application.
5. The application confirms its transfer to the UE, if confirmation is required.
6. The UE sends an acknowledgement to the Serving SDHF.
7. The Serving SDHF forwards the acknowledgement to the Gateway SDHF.
8. The Gateway SDHF confirms the MT SDS-PDU transfer to the SCS/AS.

6.4.7.3 Solution evaluation

The original targets of WT are fulfilled by this solution.

The solution is targeting an efficient transfer of infrequent small data units to allow interacting directly with external networks without the need to involve session management to establish connections when small amounts of data traffic have to be transferred. The solution does not require any SM and MM context and handles the small user data avoiding procedures related to registering and tracking a massive number of UEs. Also the introduction of the counters and message integrity checking can prevent the abuse of this mechanism.

NOTE: No authentication is performed before the data is sent to the CN, the Security impact is to be evaluated by SA3.

This mechanism is applicable for those UEs that do not use other data services than that Small Data Service. Other UEs may use SDS in addition/parallel to other data services and may have related context information due to these services (e.g. through NAS signaling).

The solution may enhance the SMS service that stems from the CS services domain era and has related restrictions, like using an MSISDN for addressing or having no means for preventing fraud as the integrity of the messages and addresses cannot be verified.

The solution assume when the UE sends the MO data it will be available for a short time period. During that time period if there are MT data stored on the Gateway SDHF, the MT data will be sent to the UE. As the UE does not need monitor the paging message, the eDRX or PSM mode are not need. As UE can be switched off after the MO data has been sent, the power efficiency can be achieved.

In particular, the solution has the following benefits and drawbacks.

Benefits:

- The solution is based on connectionless communication that does not require involvement of session management for sending infrequent small data units. In particular, there is no attach procedure. What is normally the attach message in this approach is the user data message. As a result, there is no need to establish and release sessions/connections when small amounts of data need to be sent, avoiding signalling delay and wasting of network resources related to signalling overhead in the core network and radio interface. It also can bring some benefits in terms of UE power efficiency.
- The solution does not require SM and MM context information. In addition network resource efficiency benefits from avoiding cases such as when for a single small data unit transfer there is effort to construct and store context information that is not used again afterwards.
- Integrity protection of SDS-PDUs can be done, e.g., in the form of a signature that would allow any entity on the path to check the authenticity of the SDS-PDU once this entity has access to the data (e.g. keys) necessary for validating the signature. The integrity protection is for SA3 to define, e.g. using a public key infrastructure.
- Every MO small data unit can be routed via a different serving SDHF if available, i.e. it is not required that a specific serving SDHF handles the SDS-PDU, hence a RAN node can select the serving SDHF freely and forward MO small data units.
- The solution can support unidirectional transmission.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 225 of 501

- The solution can work without paging to support minimum energy consumption for UEs. That is, the UE may be mobile, but if the acknowledgement is not delivered because the UE has moved that would have to be handled by retrial rather than by mobility management, i.e. the retrial is triggered when next time the MO data is received.

- Power efficiency can be achieved without the eDRX or PSM mode mechanism.

- The source and destination IDs in SDS-PDU are assumed in the form of URIs, which allows high flexibility in ID assignment. This solution provides uplink and downlink small data routing without the need for allocation of an MSISDN

Drawbacks:

- The solution is for delay-tolerant small data services and does not provide any QoS support.

- The solution provides only limited mobility support.

- If needed to control transmission frequency and restrict overload the network should set up SDS-PDU counters that adds some complexity. However, this applies for all message transferring mechanism.

6.4.8 Solution 4.8: for Data transmission with ConnectionLess RAN-Core interface

6.4.8.1 Solution Overview

The solution aims to cover at least following use cases:

- (Massive) IoT UE that may move and need to send sporadic (potentially small amount) data: in this case the UE sends data to the NextGen Core via the user plane path without requiring more signalling in the network (RAN and Core) than the amount of user data to be transferred.

Editor's note: It is FFS whether the solution applies to other use cases such as Smartphone issuing a regular check / polling for notifications of incoming messages / events.

In such situations, the following architectural concepts are proposed in order to support a fast switch from IDLE state to a CL-data state where data transfer occurs:

- The RAN-Core interface works in ConnectionLess (CL) mode for UP (User Plane) delivery: once the PDU session has been set-up, in order for the UE to be able to send or to receive data no connection dedicated with an UE needs to be set-up on NG2 or NG3.

- The service itself is not connectionless:

  - the UE needs to attach, set-up PDU sessions, etc.

  - When the UE exchanges MM or SM related signalling with the network a NG2 connection is set-up. Once the MM or SM transaction(s) are over the NG2 connection for the UE is released

- The MM procedures (e.g. ATTACH, authentication, , "Tracking Area" update,…) are independent from whether the UE will activate a PDU session used in ConnectionLess (CL) mode on the interface between RAN and Core. Thus an UE needs to ATTACH to the network before being able to activate a PDU session to be used in ConnectionLess (CL) mode on the interface between RAN and Core

- The UE is tracked at "Tracking Area" level and issues "Tracking Area" updates.

- The UE uses the same SM procedures to manage (set-up, release, etc.) a PDU session regardless of whether this PDU session is to be used in a Connection Oriented (CO) or in a ConnectionLess (CL) mode on the interface between RAN and Core.

  - During the PDU session set-up procedure some parameters specific to the CL data transfer are nevertheless exchanged between the UE and the network.

Editor's note: It is FFS whether the same PDU session may alternatively be used in a Connection Oriented (CO) or in a ConnectionLess (CL) mode on the interface between RAN and Core.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 226 of 501

- The support of the ConnectionLess (CL) mode on the interface between RAN and Core is independent from the nature of the data being carried in a PDU session (IPv4, IPv6, non IP).
- When the UE needs to send data (assuming the UE is already attached to the network and has established a PDU session):
  - There is no NG2 signalling exchange dedicated to the UE between the RAN and the Core.
  - There is no NG3 data plane connection dedicated to the UE between the RAN and the Core.
  - As there is no signalling exchange dedicated to the UE between the RAN and the Core, the RAN gets no security material dedicated to the UE. Thus the security and the header (de)compression of the user plane traffic are handled in the NextGen Core (in the UPGW part of the NextGen Core). The corresponding parameters (e.g. security algorithms, compression algorithms, etc.) are negotiated between the UE and the CN CP at PDU session set-up.

Editor's note: Any potential security impacts on signalling exchanges between the RAN and the UE is to be studied by SA WG3 in conjunction with RAN groups.

  - As the Core network User plane GW (UPGW) needs to decipher data received from a UE via the RAN, the UL (uplink) data are sent by the UE together with a non ciphered PDU session identifier allowing the UPGW to retrieve the deciphering context of the PDU session.
  - As the RAN needs to route Uplink (UL) traffic from the UE towards the UPGW, the UE needs to put packet forwarding information in its UL traffic allowing the RAN to determine the relevant UPGW.
  - The NextGen Core provides via NAS signalling UPGW CL Service information (UCLSI) to the UE: UE identifier and the packet forwarding information allowing the RAN to determine the UPGW. This information is provided on a per PDU session basis.
    - The NextGen Core provides UCLSI information to the UE at least upon UE request for a PDU session set-up. This information needs also to be provided to the UE when the UPGW that supports the PDU session of the UE has been changed.
  - When the UPGW receives UL traffic with a PDU session identifier for which it has no corresponding context, the UPGW fetches the corresponding information from the CN CP.
  - The UPGW keeps track of the RAN from which it last received UL traffic from a UE and associates this information with a UE location freshness timer. As long as the UE location freshness timer has not elapsed, the UPGW sends DL (Downlink) traffic for an UE towards the RAN from which it last received UL traffic from this UE. The DL data sent are sent by the UPGW towards the RAN together with a non ciphered UE identifier. If the RAN can't deliver the PDU (the UE may have moved in the mean time) the RAN deletes the PDU and notifies the UPGW that removes the relationship between the UE and the RAN.

Editor's note: DL data delivery requires further clarifications.

  - When the UPGW needs to send DL data towards an UE, and the UE location freshness timer has elapsed, the UPGW request the CN CP to page the UE. The CN CP pages the UE in the (set of) "Tracking Area" where it is registered.
  - The value of the UE location freshness timer is determined by the network taking into account the UE subscription.
- The UE mobility relies on cell reselection, not on network controlled Hand-Overs.

Editor's note: MM states are FFS.

Editor's note: The security aspects related with this solution need to be studied by SA WG3.

The architecture for Data transmission with ConnectionLess RAN-Core interface consists of the following network elements (fig 6.4.8.1-1):

- User equipment (UE).
- Radio Access Network (RAN).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 227 of 501

- User plane Gateway (UPGW).
- Core control plane (Core CP).

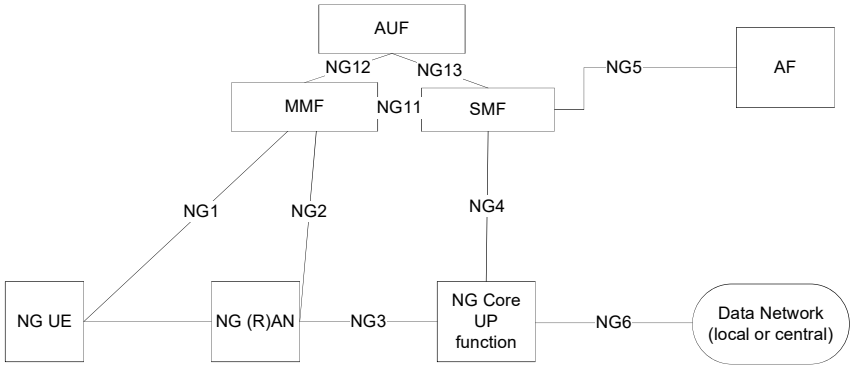


Figure 6.4.8.1-1: Architecture to support PDU sessions with Connectionless mode transfer on the RAN-Core interface

The User plane protocol stack is derived from the baseline connection oriented protocol stack with the UE-RAN layer NG-PDCP slit between lower and upper parts:

- (NG-)PDCP Upper: This layer, placed between IP and access stratum, links UE and UPGW, provides encryption and integrity protection between the UE and the network. The (NG-)PDCP Upper UP layer takes care to avoid packets duplication (Sequence Numbering).

Editor's note: It is FFS whether the (NG-)PDCP CLS Upper layer is identical to the upper part of the (NG-)PDCP / Network convergence sub-layer that is responsible for radio interface user plane security.

- (NG-)PDCP Lower: This layer, placed between the UE and RAN, provides PDU session identification at RAN level.
- Core CLS Relay: This layer, placed between the RAN and UPGW, provides relay of the PDU session identification and multiplexing of multiple PDU sessions over a NG3 link between an UPGW and an AN Node.

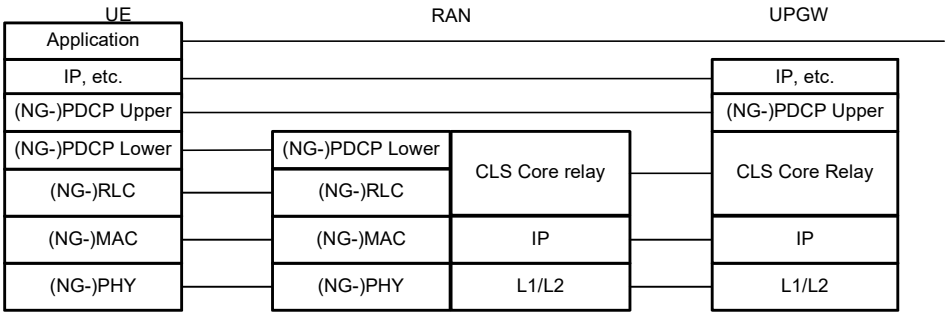


Figure 6.4.8.1-2: User Plane Protocol stack for Connectionless mode transfer on the RAN-Core interface

Following layers are to be defined by RAN groups

- (NG-)PDCP Lower
- (NG-)RLC: Radio control sublayer (responsible for segmentation and ARQ).
- (NG-)MAC: Media Access control (responsible for connectionless access and HARQ).
- (NG-)PHY: Physical Access.

Editor's note: The protocol stacks over NG3 is to be defined together with RAN groups.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 228 of 501

6.4.8.2 Call flows

6.4.8.2.1 Identities

6.4.8.2.1.1 UPGW CL SERVICE Id (UCLSI)

UCLSI is used by UE, RAN and UPGW to identify a PDU session with Connectionless mode data transfer on the RAN-Core interface. This identifier contains an Identifier of the UPGW serving the PDU session and a local identifier for a specific connectionless PDU session for a specific UE. RAN uses UCLSI to derive the UPGW that should handle Data exchanged with the UE. A UE may be allocated one or more UCLSI on one or more UPGW.

6.4.8.2.2 Assumptions

- The CN CP (SM) has to select an UPGW that supports PDU sessions with Connectionless mode data transfer on the RAN-Core interface. The UPGW selection procedure takes also into account the specific parameters (e.g. security algorithms, compression algorithms,...) proposed by the UE at PDU session set-up
- The UPGW manages a state per UCLSI
  - REACHABLE: The UCLSI is marked as REACHABLE when the UPGW knows the identity of the RAN serving that UCLSI as the last correctly received UL PDU from the UE has been received by the UPGW via this RAN. The UCLSI REACHABLE state is controlled by a freshness timer at the expiry of which the state becomes IDLE. The Timer is (re)started at the reception of each UL PDU correctly received from the UE on that UCLSI
  - IDLE: The UPGW does not know the identity of the RAN serving that UCLSI. Paging is required to send DL PDU for this UCLSI
- The RAN is assumed to also run a freshness timer for UCLSI. The Timer in the UPGW is assumed to be shorter than the timer in RAN

Editor's note: It is FFS How to ensure proper co-ordination of the freshness timers in RAN and in Core

6.4.8.2.3 Procedures

6.4.8.2.3.1 Set-up of a PDU sessions with Connectionless mode data transfer on the RAN-Core interface

This procedure is used to establish PDU sessions with Connectionless mode data transfer on the RAN-Core interface

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 229 of 501

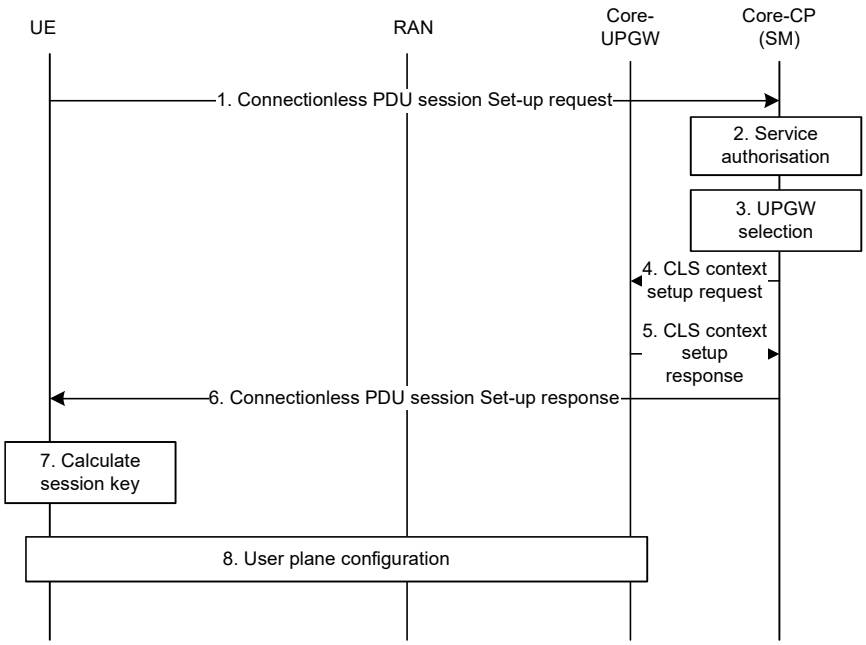


Figure 6.4.8.2.3.1-1: UE initiated setup of a PDU session with Connectionless mode data transfer on the RAN-Core interface

Pre-conditions

- UE has previously attached to network, authenticated and obtained master security key.

1 UE uses NAS to request the set-up of a PDU session with Connectionless mode data transfer on the RAN-Core interface. The UE provides the same parameters than for a PDU session working in full Connection Oriented mode but also , includes the supported header compression scheme (if any) and Data ciphering algorithms.

2 The Core control Plane (SM) authorizes PDU session set-up based on subscription information

3 The Core control plane (SM) selects an UPGW taking into account the header compression scheme (if any) and Data ciphering algorithms supported by the UE. The Core control plane (SM) chooses a UPGW CL SERVICE Id (UCLSI) that identifies the PDU session and the UPGW and gets from the AUC the keys to be used on the user plane link between the UPGW and the UE

Editor's note: The derivation of the keys to be used between UE and UPGW is to be defined at SA3; It should consider the master Key output of the last authentication as well as the UCLSI and the Direction of the traffic.

4. The Core control plane (SM) requests the establishment of user-plane for the PDU session in the UPGW. The request includes the related QoS requirement for the PDU session to be established as well as the header compression scheme (if any) and Data ciphering algorithms supported by the UE. Initial Downlink tunnel information is also sent to the User plane functions (e.g. address of the AN node).

5 The UPGW establishes the user-plane for the PDU session and replies to the Core control plane (SM). The reply contains the finally selected header compression scheme (if any) and Data ciphering algorithms to be used on the PDU session

6 The Core control plane (SM) sends a PDU session set-up response to the UE. The response contains the UCLSI and the finally selected header compression scheme (if any) and Data ciphering algorithms to be used on the PDU session

7 The UE calculates the key for the security association with UPGW based on the same algorithm and on the same input parameters than used by the Core control plane (SM) in step 3

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 230 of 501

8 UE may use the connectionless service to complete the user plane configuration (e.g. Router solicitation / IP address assignment, header compression initiation (if any), etc.)

6.4.8.2.3.2 UE connectionless uplink data transfer

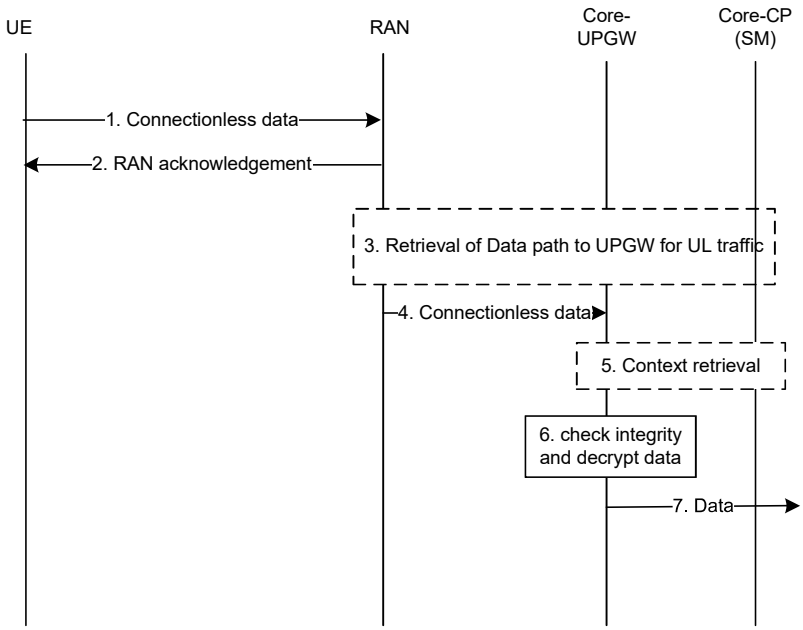


Figure 6.4.8.2.3.2-1: UE triggered uplink connectionless transfer

Pre-conditions

- The UE has uplink connectionless data (a PDU) to send on one of its already established PDU sessions with Connectionless mode data transfer on the RAN-Core interface.

1 The UE ciphers the PDU to transmit. The UE then puts the previously assigned UCLSI in the CLS UP data header and adds an integrity check signature.

UE access stratum may replace the UCLSI with a shorter identifier if available from RAN and UE RAN freshness timer has not expired. The UE sends uplink connectionless data transfer to the RAN.

NOTE1: The integrity check signature is to prevent another UE from injecting traffic on the PDU session. It is calculated on the UCLSI, not on any shorter RAN identifier possibly used instead the UCLSI on the air interface

2 RAN sends ack to the UE.

RAN resets UE location freshness timer for UCLSI.

The UE resets the UE UCLSI freshness timer.

3 If UPGW indicated by UCLSI is not known by RAN then RAN sends a request to control plane and the control plane responds with the forwarding information to the UPGW indicated in the UCLSI.

NOTE2: This step takes place only for the first user served by the RAN that is handled by a new UPGW.

4 Based on the received UCLSI, the RAN forwards all complete data PDUs with header including UCLSI to UPGW over appropriate transport interface.

5 Using the UCLSI, the UPGW retrieves the context of the PDU Session. If such context is not available the UPGW may send a query to the Core control plane (SM).

6 Using stored key UPGW verifies the integrity check signature and decrypts incoming uplink data.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 231 of 501

If the Integrity check is negative the UPGW silently discards the data. Otherwise,

(when needed) The UPGW decompresses the PDU header.

The UPGW learns that UE is available on a given RAN (the UCLSI is REACHABLE): the UPGW (re)starts UE location freshness timer for the UCLSI and stores the UCLSI to RAN transport interface mapping.

7 The UPGW forwards the PDU towards its destination

6.4.8.2.3.3 UE connectionless downlink data transfer

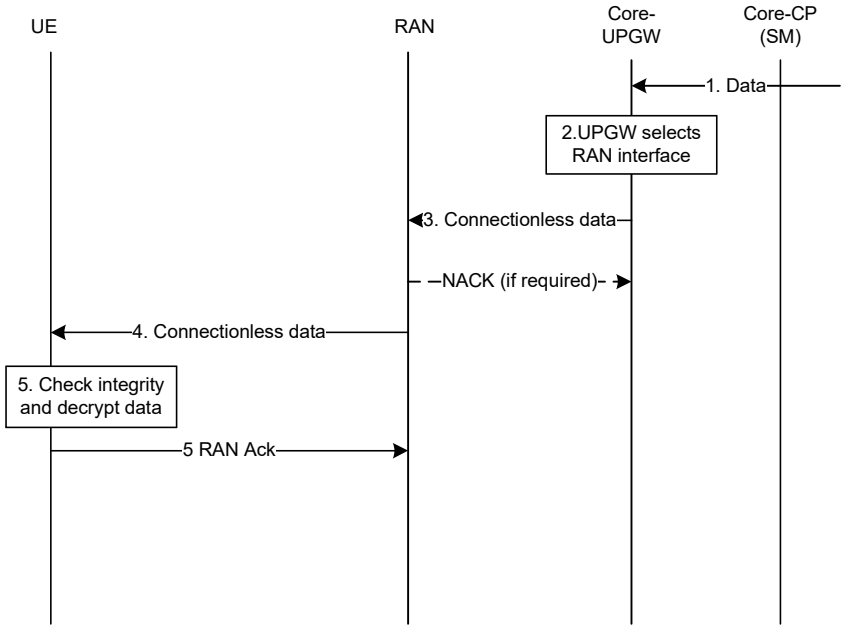


Figure 6.4.8.2.3.3-1: Downlink connectionless transfer

Pre-conditions

- the UE has previously established a PDU session with Connectionless mode data transfer on the RAN-Core interface

1. The UPGW receives downlink incoming data (a PDU)
2. The UPGW retrieves the corresponding UCLSI:
   - if the UCLSI is marked as "REACHABLE", the UPGW uses the last known RAN serving this UCLSI
     - The UPGW compresses the IP header (when needed), encrypts the data and forwards the data and UCLSI over the appropriate downlink RAN transport interface for the UCLSI.
     - The UPGW restarts UE location freshness timer for UCLSI
   - if UCLSI is marked "IDLE" then the UPGW may either drop packet or initiate network page. This behaviour is controlled by a policy received from Core control plane (SM) itself possibly depending on subscription.
     - The UPGW sends a paging request for the UCLSI to Core CP , buffers the data and starts a paging timer. Core CP triggers the corresponding paging by the RAN. If the page response from UE arrives before the paging timer times out, then the UPGW learns current RAN serving the UE and forwards the data via this RAN. This is further detailed in sub-clause 6.4.8.2.3.4

Editor's note: It is FFS whether the UPGW checks the UCLSI state of other PDU sessions of the same UE

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 232 of 501

3. (assuming UCLSI is marked REACHABLE) the UPGW forwards the data and UCLSI over the appropriate downlink RAN transport interface for the UCLSI. For any downlink incoming data, RAN matches downlink UCLSI:

   - if UCLSI is known to RAN then RAN transmits the data to UE

     - if UE transfer is successful, RAN restarts UE location freshness timer for UCLSI

     - if UE transfer fails, RAN drops packet, sends NACK to UPGW and deletes its context for theUCLSI

   - if UCLSI is not known to RAN (e.g. RAN previously had UE transfer fail) then RAN drops the data and sends NACK to UPGW

   - if UPGW receives NACK from RAN (e.g. the UCLSI was known but transfer failed or UCLSI was not known) then UPGW clears UPGW UE freshness timer and so marks UCLSI as "IDLE" (the UCLSI is no more associated with any RAN Node).

4 The RAN transmits the data to UE

5 When UE receives connectionless data, it processes the data (re-assembles, decrypts etc.), delivers the data to the application and sends uplink acknowledgement. UE resets UCLSI freshness timer.

6 If UPGW UE freshness timer for UCLSI expires, UPGW marks UCLSI as "idle"

7 If RAN UE freshness timer for UCLSI expires, RAN deletes UCLSI

8 If UE freshness timer for UCLSI expires or UE reselects a new cell, UE returns to connectionless idle state and stops monitoring downlink channels for data reception.

6.4.8.2.3.4 Paging for UE connectionless downlink data transfer

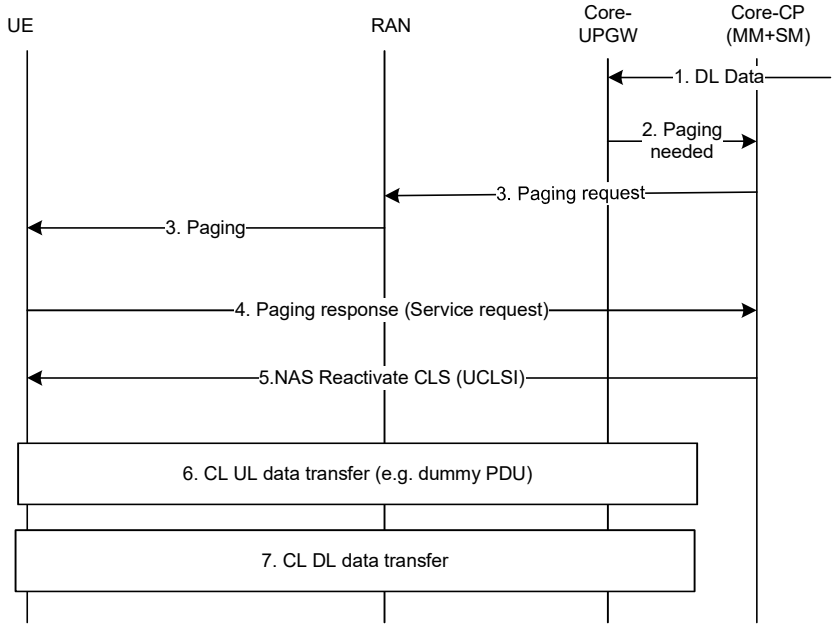


Figure 6.4.8.2.3.4-1: Paging for UE connectionless downlink data transfer

1. The UPGW receives DL data but the corresponding UCLSI context is marked "IDLE" and the policy received from Core CP is to page the UE in that case (step 2 of 6.4.8.2.3.3)

2. The UPGW notifies the SM that it has no RAN context for DL data related with an UCLSI. SM requests (Permanent User Id; UCLSI) MM to Page the UE corresponding to the permanent UE identifier (IMSI) associated with the UCLSI. The MM retrieves the corresponding UE NAS identifier (GUTI like) for paging.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 233 of 501

3. The MM requests the RAN to page the UE and the RAN pages the UE
4. The UE issues a NAS Page response to the Core CP (MM)
5. The Core CP sends a NAS Reactivate CLS (UCLSI) to request the UE to reactivate the UCLSI
6. The UE issues an UL Data request on the UCLSI (per clause 6.4.8.2.3.2). The request contains in the UL CLS data Header the UCLSI as well as an indication that the data is dummy (if the UE has no data to send and chooses to send a dummy PDU). The UPGW drops the data (if it indicated as a dummy data) and updates the UCLSI context: The UPGW starts UE location freshness timer for UCLSI and stores the UCLSI to RAN transport interface mapping
7. The UPGW restarts the DL data transmission per Figure 6.4.8.2.3.3-1

6.4.8.2.3.5 Mobility support

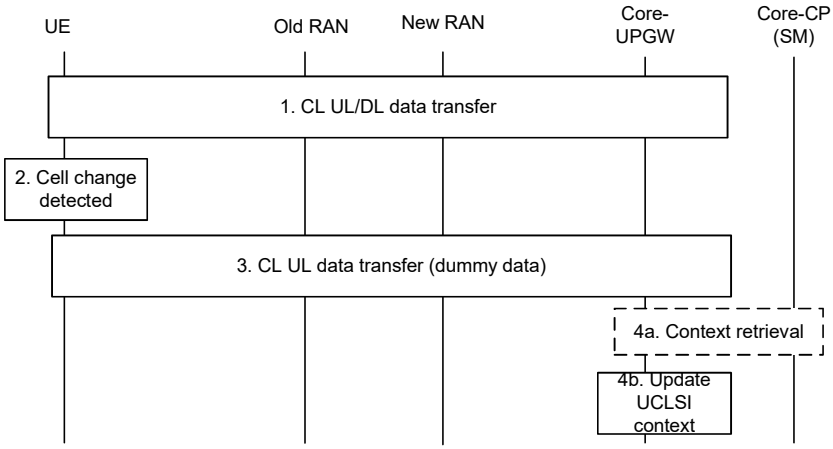


Figure 6.4.8.2.3.5-1: Mobility support

1. The UE and UPGW exchange UL and DL connectionless data
2. The UE detects cell change while UCLSI remains valid
3. The UE issues an UL Data request on the UCLSI (per clause 6.4.8.2.3.2). The request contains in the UL CLS data Header the UCLSI as well as an indication that the data is dummy (if the UE has no data to send and chooses to send a dummy PDU).
4. Using the UCLSI, the UPGW retrieves the context of the PDU Session.

   4a. If such context is not available the UPGW may send a query to the Core control plane (SM).

   4b. The UPGW drops the data (if it was indicated as a dummy data) and updates the UCLSI context: the UPGW restarts UE location freshness timer for UCLSI and stores the UCLSI to RAN transport interface mapping

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 234 of 501

6.4.8.2.4.6 UPGW Triggered Release and Redirection During UE Connectionless Active Mode

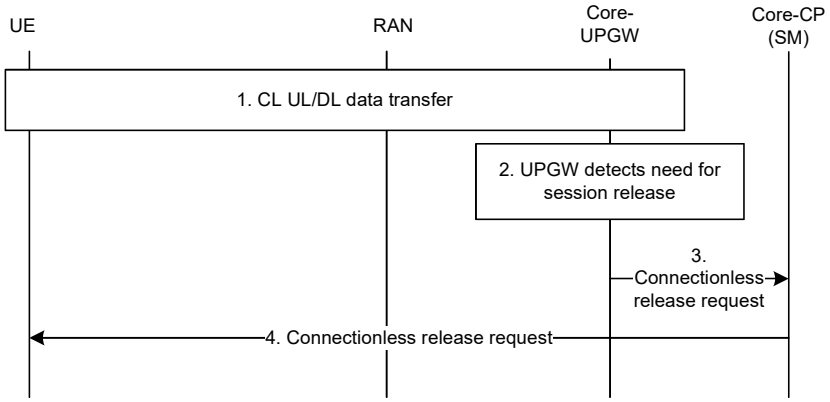


Figure 6.4.8.2.4.6-1: UPGW Initiated Release and Redirection

1. The UE and UPGW exchange UL and DL connectionless data
2. The UPGW detects need for session release (security violation, UE traffic profile violation, gateway overload protection, etc.)
3. The UPGW sends connectionless release request to the Core-CP (SM) with session identifier UCLSI. The UPGW provides a release cause indication
4. The Core-CP (SM) sends connectionless release request to the UE with session identifier UCLSI. The Core-CP (SM) provides information on the release cause indication and whether or not the network requires that UE request re-establishment of the PDU session

6.4.9 Solution 4.9: UP protocol model - Per QoS class tunnel protocol

6.4.9.1 Architecture description

This solution addresses the "UP protocol model" of the SM_WT_#1 SM Model.

In this option there is one tunnel per QoS class and PDU Session between a pair of NFs, e.g. between a RAN node and a UP function in the CN or between two UP functions in the CN. This option is similar to how it works for EPC where each QoS class (bearer) can have separate outer IP headers and separate encapsulation (GTP-U) headers.

This solution has the following additional properties:

- The receiving endpoint can use the outer IP header in combination with encapsulation header fields to determine the PDU Session and QoS class of the packet.
- New tunnel parameters need to be established for each QoS class.
- At mobility, signalling of tunnelling info per QoS class (although several QoS tunnels can be handled in the same message)
- Overlapping UE IPv4 addresses supported
- Different PDU types (IP, Ethernet, non-IP) supported
- End-user payload "layer" decoupled from the transport layer, allowing different technologies in the transport layer.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 235 of 501

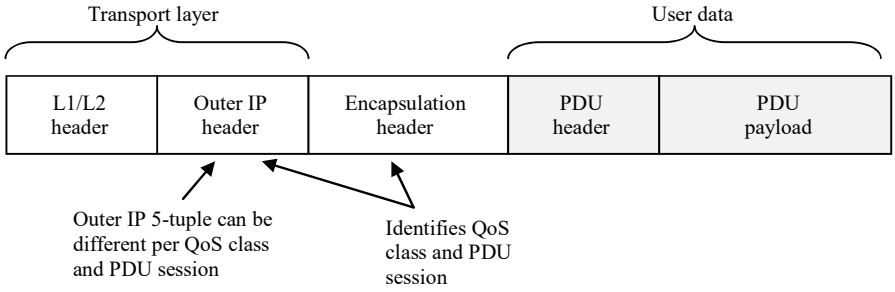


Figure 6.4.9.1-1: Per QoS class tunnel protocol

6.4.9.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.4.9.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.10 Solution 4.10: UP protocol model - Per PDU session tunnel protocol

6.4.10.1 Architecture description

This solution addresses the "UP protocol model" of the SM_WT_#1 SM Model.

In this option there is one tunnel per PDU Session between a pair of NFs e.g. between a RAN node and a UP function in the CN and between two UP functions in the CN. All QoS classes of a session share the same outer IP header, but the encapsulation header may carry QoS markings.

This solution has the following additional properties:

- The receiving endpoint uses an identifier in the encapsulation header, possibly in combination with outer IP header, to determine what session the tunneled PDU belongs to.
- Common signaling for all QoS classes in mobility
- Overlapping UE IPv4 addresses supported
- Different PDU types (IP, Ethernet, non-IP) supported
- End-user payload "layer" decoupled from the transport layer, allowing different technologies in the transport layer.

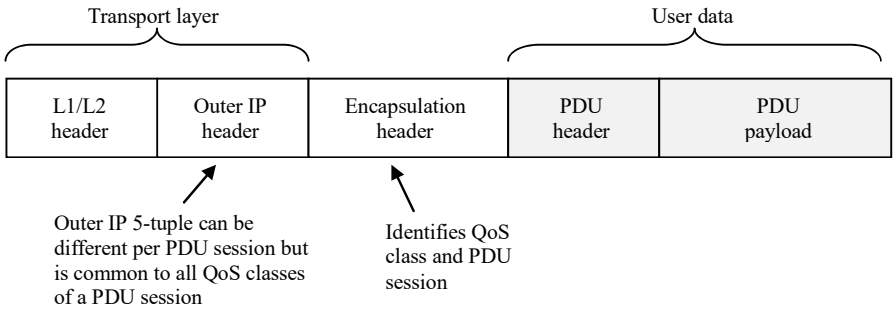


Figure 6.4.10.1-1: Per PDU session tunnel protocol

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 236 of 501

6.4.10.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.4.10.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.11 Solution 4.11: UP protocol model - Per Node-level tunnel

6.4.11.1 Architecture description

This solution addresses the "UP protocol model" of the SM_WT_#1 SM Model.

In this option there is a common tunnel for all traffic between each pair of NFs e.g. between a RAN node and a UP function in the CN or between two UP functions in the CN.

This solution has the following additional properties:

- There is no identification of the PDU Session within the outer IP header or the encapsulation header. Instead the endpoint needs to use information in the end-user PDU to identify the session, e.g. the UE IP address in case of PDU type IP.
- In case one AN connects with one UP accessing multiple DNs, there should be per-Node-per-DN tunnels between the AN and the UP function.
- For PDU type IP, the PDU session traffic is identified based on UE IP address. This requires that UE IP addresses are unique in one DN to allow unambiguous traffic identification.
- For Ethernet type PDU, a unique ID to identify session at UP function and RAN node is required, which is created per PDU type. The ID is located in PDU header like UE IP address for IP type PDU.

Editor's note: how to define the ID for session identification is FFS.

Editor's note: how to identify the session in case of a non-IP type PDU is FFS

Editor's note: It is FFS how UP-GW and data network exchange Ethernet type PDU and non-IP type PDU via SGi interface.

- The encapsulation header may or may not be needed, e.g. to carry an identifier for QoS purposes.
- In case a node/function supports multiple IP addresses there may be a need to signal the tunnel endpoint addresses in order to direct the traffic to the right IP address of the node/function due to e.g. load balancing.

Editor's note: It is FFS if multiple IP addresses per node/function need to be supported in certain use cases like fixed deployments.

End-user payload "layer" decoupled from the transport layer, allowing different technologies in the transport layer.

Editor's notes: It is FFS whether Ethernet and non-IP PDU types would need to be supported for certain use cases like fixed deployments.

Editor's note: The detailed QoS mechanism is per the progress of Key Issue#3: QoS framework.

For one AN node, there may be multiple tunnels connecting to different User Plane GWs. The node-level tunnel applies to UEs that are stationary and hence do not move. Therefore, the operator can ensure via configuration the assignment of non-overlapping IP addresses within one DN to the UEs belonging to the same Node-level tunnel.

Editor's note: The need for signaling to support mobility from one access node to another, for scenarios where UE mobility is needed, is FFS. It is FFS is this is applicable to Fixed Wireless Access deployments.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 237 of 501

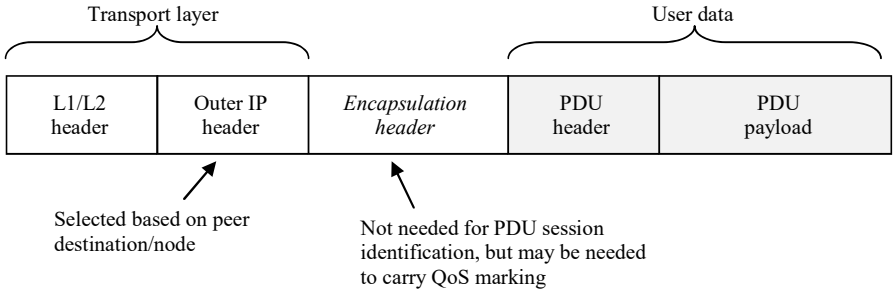


Figure 6.4.11.1-1: One tunnel per destination

A scenario where this solution may apply is when "a fixed wireless terminal" connects to the network, e.g., a IoT UE, or a CPE UE providing fixed-network comparable bandwidth as the access service for the "last one mile". Such fixed wireless terminals need almost no movement or may also not be allowed (e.g., per-subscription) to move.

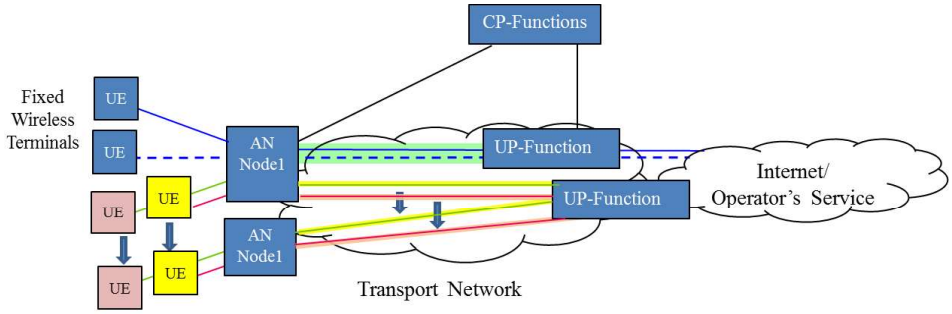


Figure 6.4.11.1-2: Scenario with fixed wireless and mobile terminals.

The fixed-UE scenarios are characterized by the large number of connections (e.g., IOT case) and the heavy UP traffics (e.g., CPE case). To simplify the tunnel, an "aggregated" node-level tunnel between the NextGen Access node and the UP Functions could be used.

6.4.11.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

When a UE attaches to the network or sets up a PDU session to one DN, the CP-AU authorizes the UE type (e.g., a type of fixed wireless UE) and identify whether AN node level tunnel applies. If so, the CP will determine the corresponding tunnel for the PDU session based on information such as DN name, the tunnel end point information (e.g., UP IP addresses) or the AN node ID provided by the AN.

Editor's note: the other parameters which could be used as UE type is FFS.

The UEs using the same AN node-level tunnel should be connected to the same CP SM.The AN node can identify the UE's traffic through the tunnel information (e.g., outer IP header) and the UE's IP address.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 238 of 501

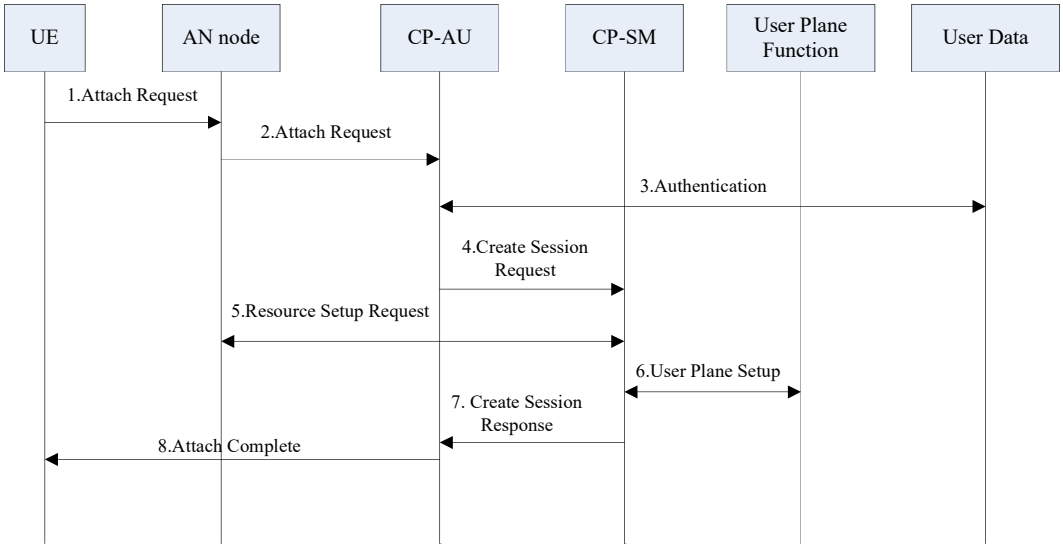


Figure 6.4.11.2-1 Illustration of a UE attach to the network by an AN node-level tunnel

1. The UE sends Attach Request to the AN node.The UE type is included in the signalling (similar as RRC message) associated with the attach request.
2. The AN node may recognize the UE type and incorporate the node-level tunnel selection assistance information (i.e., tunnel end point IP addresses, AN node ID) together with the Attach Request message send to CP-AU.
3. The CP-AU verifies the PDU type and User subscription data such as UE type to authenticate the UE.
4. The CP-AU sends Create Session Request message to the CP-SM.
5. The CP-SM select the UP function based on the information such as the DN Name, tunnel selection assistance information provided by AN. CP-SM assigns UE IP address corresponding to the UP function. CP-SM then request the AN to setup resources for the session.
6. The CP-SM function setup the user plane with the UP function, i.e., notifies the assigned UE IP address, indicate the tunnel used to the AN and the corresponding traffic handling policy for this Session.

Editor's note: how the solutions works in the IPv6 case is FFS.

7. The CP-SM sends Create Session Response to CP-AU. The message will contains the UE IP address.
8. The CP-AU send Attach complete to the UE.

6.4.11.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.12 Solution 4.12: UP protocol model - SDN-Based Approach

6.4.12.1 Architecture description

This solution addresses the "UP protocol model" of the SM_WT_#1 SM Model.

In this option there is no outer IP header or encapsulation header between each pair of NFs e.g. between a RAN node and a UP function in the CN or between two UP functions in the CN. Instead it is assumes that routers and/or switches on the path between the endpoints (e.g. RAN and CN UP function) are configured with forwarding/routing rules that ensures that the packet is carried to the correct destination. SDN-like technology is used to control the UP forwarding path.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 239 of 501

During the procedures of session establishment, the CP function performs as SDN controllers' role towards the routers/switches. The CP function, using SDi reference points, as shown in the Figure below, updates the forwarding table of the switches in the path between the NextGen AN node and the UP-Function. The forwarding rules in the table are based on the UE IP address, i.e., route traffic properly per source IP address for the uplink and per destination IP address for the downlink.

In case the switch in the path cannot determine the next hop of the IP packet, the packet will be forwarded to the controller to get the instructions on the next hop switch.

Editor's note: detailed procedures for using SDN setup the DN session is FFS.

The IP address of the UEs should avoid overlapping, e.g., using IPv6, or assign distinct public/private IPv4 address within the same transport IP network domain.

When UE moves to another NextGen AN node, the CP-Function determines which switch need to be updated and do the forwarding table update accordingly.

Editor's note: How to interact with other CP-functions when a UE moves out of the domain of the CP-Functions is FFS. This also includes how to support roaming scenarios

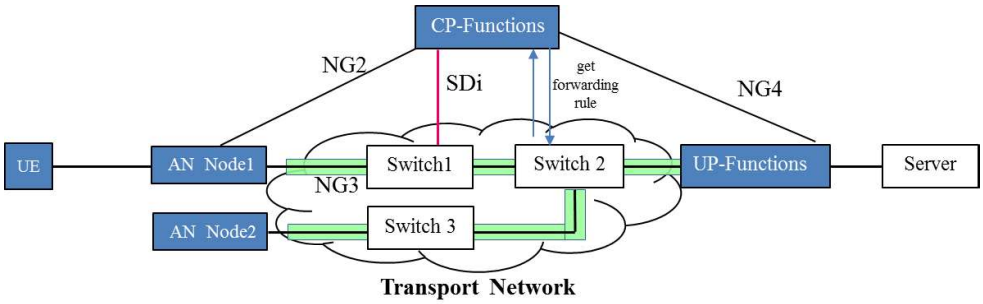


Figure 6.4.12.1-1: Illustration of SDN based approach.

This solution has the following additional properties:

- Different PDU types would require PDU-specific support in the transport layer
- Updates to intermediate switches/routers done to move the UP path at UE mobility.
- Overlapping IPv4 addresses not supported
- QoS control need to be forwarded via control signaling to intermediate routers/switches and RAN, or alternatively the UE payload header could be used to carry e.g. DSCP

Editor's note: It is FFS if Ethernet and non-IP PDU types can be supported using this solution and how the PDU Session can be identified in that case. The traffic transport rule (as compared with the forwarding table in the IP packet case) would need to be updated based on other forwarding information, e.g., layer 2 indication. This is FFS.

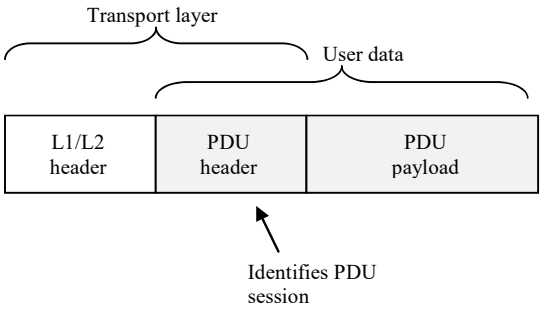


Figure 6.4.12.1-1: No tunnel

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 240 of 501

6.4.12.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.4.12.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.13 Solution 4.13: Session Management model for multiple parallel PDU Sessions and for multi-homed PDU Session

This solution addresses WT#1 (SM model) and WT#2 (relation between SM and MM).

6.4.13.1 Architecture description

This clause describes a session management model focusing on the following two cases:

- Multiple parallel PDU Sessions of IPv4, IPv6, IPv4/IPv6 (if this type is supported in NextGen) or non-IP type;
- Multi-homed PDU Session.

Editor's note: Support of multi-homed sessions for IPv4 are FFS

Editor's note: roaming case is FFS

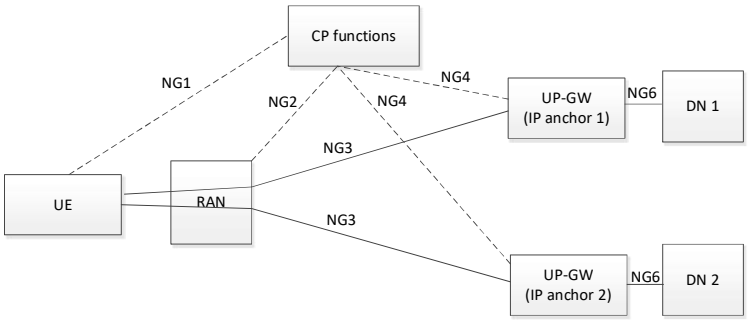


Figure 6.4.13.1-1: Session management model with multiple parallel PDU Sessions

The proposed solution assumes the following session management model principles:

- A PDU Session establishment and release is performed using NG1 signalling as in solution 4.2 and 4.3.
- A PDU Session is identified with a Data Network Name (DNN).

Editor's note: It is FFS whether the DNN is identical to the APN.

- CP functions in the NextGen core configure the user plane path for the PDU Session.
- The user plane path in the NextGen core consists of user plane gateways (UP-GWs). The number of UP-GWs for a PDU Session is not imposed by the specification.
- For UE with multiple PDU sessions towards different DN there is no need for mandatory "convergence point" similar to the SGW. In other words, going out of the RAN the user plane paths of PDU Sessions belonging to the same UE may be completely disjoint. This also implies that for idle mode UEs (if NextGen_Idle state is supported) there can be a distinct buffering node per PDU Session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 241 of 501

NOTE1: In case session bitrate limitation across all PDU sessions to the same data network is required (to be determined by the QoS key issue), then for UE with multiple PDU sessions towards the same DN there is the need of a Core Network User plane "convergence point" to support across session bitrate enforcement and charging. Across-session bitrate enforcement has to be run in a unique entity that handles all the DL traffic from the same DN. DL traffic Charging is to be performed after potential packet discard by across-session bitrate enforcement.

- A user plane path is materialised as a tunnel. There is one tunnel per PDU Session on between two entities . The tunnel carries all traffic of a PDU Session, regardless of the QoS requirements of individual traffic flows. The tunnel encapsulation header needs to be able to carry per-packet QoS markings and possibly other information.

- The network may decide to reconfigure the user plane path of a PDU Session outside of any UE mobility event.

- Multiple PDU Sessions to the same Data Network are supported as described in Solution 4.3 (clause 6.4.3) or by using a multi-homed PDU Session described below.

- a PDU Session may be associated with one or multiple IPv6 prefixes or IPV4 addresses. The latter case is referred to as multi-homed PDU Session and is described in Figure 6.4.13.1-2 and Figure 6.4.4.1-3. In this case the PDU Session provides access to the Data Network via two separate IP anchors. The two user plane paths leading to the IP anchors branch out of a "common" UP-GW referred to as "branching point". The branching point is a logical functionality which may be co-located with other entities (e.g., a UP-GW for one of the IP anchors). The branching point functionality ensures that uplink packets take the appropriate path based on the UE's source address or other header fields The branching point is a Core functionality as it has to enforce APN AMBR and charging. It enforces split of UL traffic from the UE (forwarding the traffic towards the different IP anchors) and merge of DL traffic to the UE (merging the traffic from the different IP anchors towards the link towards the UE)

NOTE 2: In case session bitrate limitation across all PDU sessions to the same data network is required (to be determined by the QoS key issue) then NOTE 1 applies also in this case.

- The use of multiple IPv6 prefixes in a PDU session could be based on

  - the "branching point" is configured as a mobility anchor that spreads the UL traffic between the IP anchors based on the Source Prefix of the PDU (selected by the UE based on policies received from the network). This corresponds to Scenario 1 defined in IETF RFC 7157 "IPv6 Multihoming without Network Address Translation". This allows to make the "Common UP-GW" unaware of the routing tables in the Data Network and to keep the first hop router function in the IP anchors.

Editor's note: In case of IPv4 multi-homed PDU session, it is FFS how the network can influence UE decisions on which source address to use

  - The multi-homed PDU Session may be used to support make-before-break service continuity as described in Solution 6.1 (SSC mode 3 in clause 6.6.1) illustrated in Figure 6.4.13.1-2. The multi-homed PDU session may also be used to support cases where UE needs to access both a local service (e.g. Mobile Edge Computing server) and the Internet, illustrated in Figure 6.4.4.1-3. Access to local services may also be realized using the same address/prefix as for other services, as described in Solution 5.2 in more detail. In this case, the branching point may use filtering criteria other than the source IP address for uplink traffic.

  - A branching point for a given session may be inserted or removed by the control plane on demand. For example, when a session is first created initially with a single address/prefix, no branching point is needed. When a new address/prefix is added to the session, a branching point may be inserted. After the release of the additional addresses/prefixed, the branching point may be removed by the control plane when there is only a single address/prefix for the session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 242 of 501

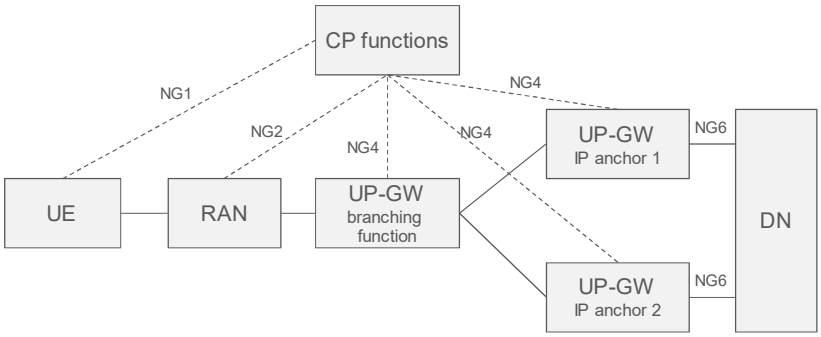


Figure 6.4.13.1-2: Multi-homed PDU Session: service continuity case

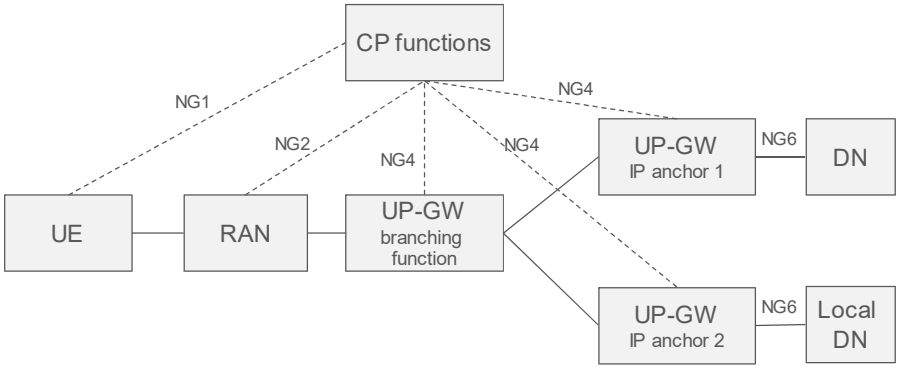


Figure 6.4.13.1-3: Multi-homed PDU Session: access to local DN

6.4.13.2 Function description

6.4.13.2.1 Session management procedure for multiple-homed PDU sessions

While the UPGW provides the mobility and IP anchoring functionality, the BP (Branching Point UP-GW) enables traffic from the UE to be split via multiple paths through multiple UPGWs in the UL direction. Similarly in the DL, the traffic from the AS, routed via multiple UPGWs, is merged at the BP prior to transmitting to the UE. The BP is generally located close to the AN in order to support multi-path/multi-homing transmission capability.

There are two scenarios to consider corresponding to figures 6.4.13.1-2 and 6.4.13.1-3. The session request procedure for both scenarios is illustrated in the following figure.

This case applies to where a UE has an ongoing PDU session using UPGW-1 without a BP and makes a request for a new path of the PDU session which requires a new UPGW (UPGW-2) and, as a result, a BP may be selected. Additionally, this also applies to the case where the UE has no ongoing session and makes a request for a PDU session which requires a BP and multiple UPGWs to meet the session performance requirements.

NOTE: When the PDU session is established, the BP function is not necessarily included in the path.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 243 of 501

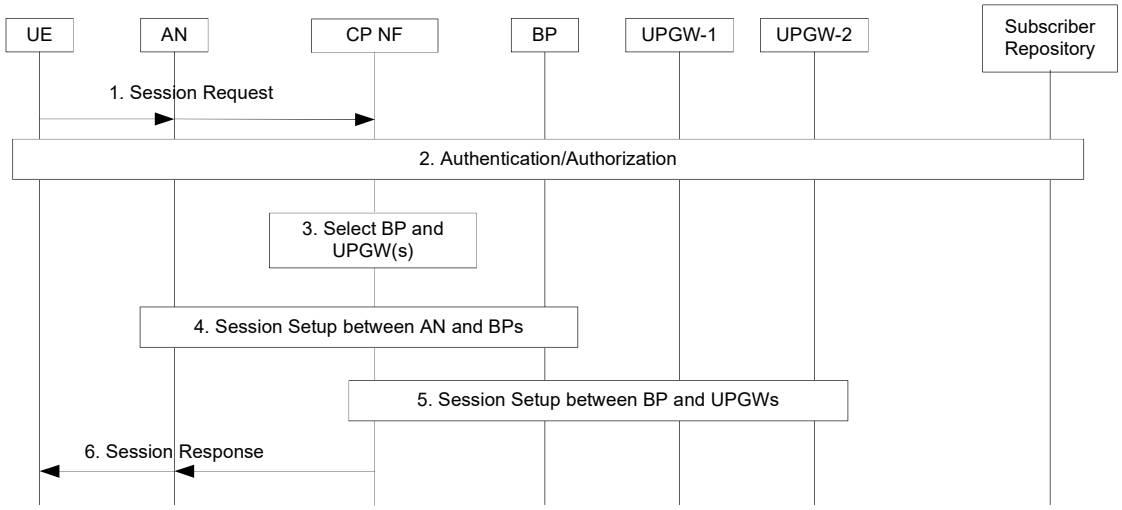


Figure 6.4.13.2.1-1: Session establishment procedure

1. The UE sends a Session Request to the CP NF via AN. The request may include QoS requirements such as latency and bandwidth requirements.
2. The CP NF initiates the authentication/authorization procedure by checking with the subscriber repository. Policy related procedure may be involved in this step.
3. If the authentication/authorization in step 2 is successful, the CP NF may select one or more UPGWs for the UE. The UPGWs are selected to satisfy the latency and other performance requirements. The CP NF may also select a BP serving the UE. The BP may be configured with criteria for forwarding packets using techniques other than the source IP address.
4. The CP NF establishes the UP paths between the serving AN and the selected BP.
5. The CP NF establishes the UP paths between the BP and the UPGWs.
6. The CP NF sends Session Response to the serving AN node. The serving AN node forwards the response to the UE.

After the session is setup, the UE can send UL data to the AN node using the appropriate source address for the given PDU session. The AN node forwards the UL data to the BP, which then forwards the traffic to the appropriate UPGW.

The UL and DL data transmission using the BP for a multi-homing PDU session is illustrated in the following figure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 244 of 501

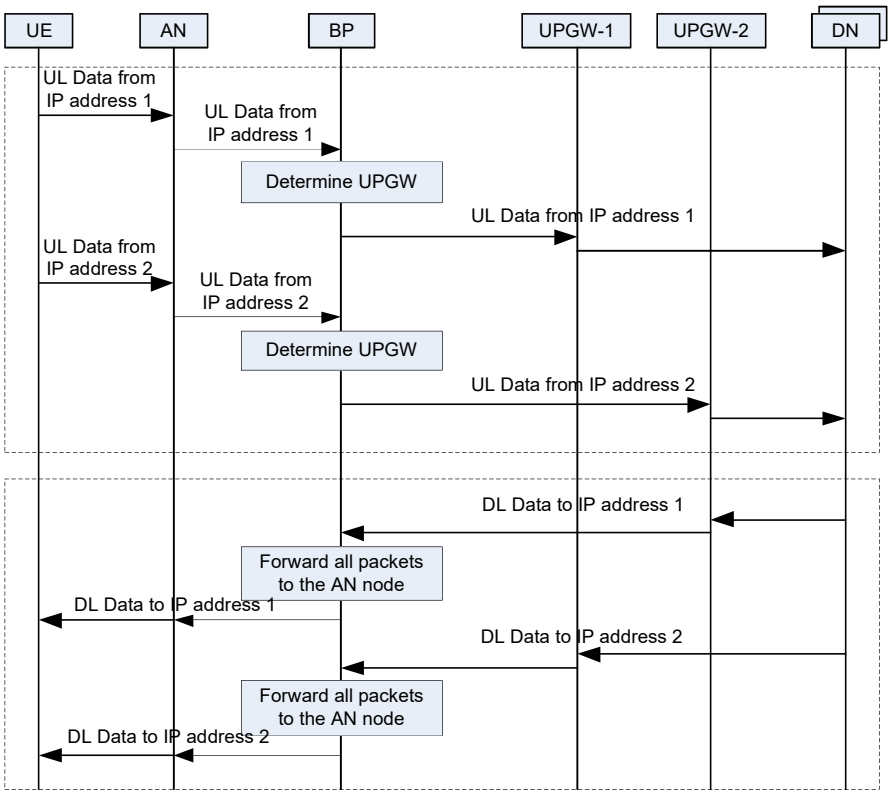


Figure 6.4.13.2.1-2: Data transmission using a branching function

When the UE moves toward the coverage area of other AN nodes that are connected to a different UPGW, the CP NF may select another BP and/or UPGW and setup the UP path between the AN and the new BP (if selected). If the UE moves out of coverage of the AN nodes that are associated with a given BP/UPGW then the corresponding paths can be removed.

The selection of the BP and UPGW and the BP to UPGW path establishment are done based on the PDU session requirements. For example, to satisfy low latency requirements, the BPs along with the UPGWs, can be co-located with the AN such that the application servers, which may also be located in a local DN, can be accessed with minimal RTT.

The session update procedure triggered by a handover is illustrated in Figure 6.6.1.2.1-1. During this procedure, a BP and/or UPGW may be added or removed. The CP NF updates the session between the AN and the BP and the path between the BP and the UPGWs. If a new UPGW is selected or removed, the network updates the IP addresses/prefixes to the UE.

6.4.13.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.14 Solution 4.14: Session management with flexible multiple UP GW(s) assignment

6.4.14.1 Architecture Description

This solution applies to key issue 4 on session management and key issue 5 on efficient user plane paths. The solution addresses the following work tasks:

- KI#4: SM_WT#1 (SM model);
- KI#4: SM_WT#2 (relation between SM and MM);

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 245 of 501

- KI#5: Eff_WT#3 (Selecting or reselecting an efficient user path); and
- KI#5: Eff_WT#4 (Interaction with SM, session continuity and/or MM).

NOTE 1: Some aspects of this solution are a variant of the multi-homed PDU Session as per subclause 6.4.4 and the (re)selection of efficient user plane paths as per subclause 6.5.2. The main differences in this solution are the session setup and support of Edge GW relocation based on SDN transport in the CN-UP.

NOTE 2: The characteristics of SDN user plane forwarding are described in solution in subclause 6.4.12.

The proposed solution is based on the following principles:

- The UE may establish a PDU session with multiple PDU flows to the same distributed data network (DN).
- An IP anchor GW (called Edge GW) is located close to the Access Network for optimal data path. The Edge GW serves as default router and possibly as IP anchor point for the UE (in case of traffic offload). In the DL, the Edge GW enforces associated policies (QoS for AN, gating for offloaded traffic, charging) of the UE's data traffic.
- A data network GW (called DN-GW) can be located more centrally (e.g. services hosted by an operator's own data centre or connectivity via specific Internet Exchange Point). The DN-GW serves as IP anchor for particular IP/PDU flow(s) within the PDU session. DN-GW can be selected and configured either 1) during the establishment of the PDU session, or 2) at the time when data traffic to particular service starts. The DN-GW can provides enforcement of QoS (which can be different from the QoS for the PDU flow anchored at Edge GW).
- In case the Edge GW needs to be relocated (e.g. due to UE mobility, load etc.) and IP address continuity has be configured for the PDU session, several options are possible based on the type of transport forwarding in the CN-UP:
  - if the forwarding in the CN-UP is done based on packet tagging/marking (e.g. MPLS, VLAN ID), a new traffic forwarding rule is enforced at the DN-GW to enable data traffic forwarding to the new Edge GW over the transport network;
  - if the forwarding in the CN-UP is done based on unmodified IP header, the forwarding rules in one or more intermediate SDN routers/switches needs to be modified.

The QoS marking from DN-GW towards the Edge GW can be carried in various ways, e.g. as DSCP marking in IP header or other SDN-based transport technology marking.

The SDN-based transport can be applied over NG6 interface.

Editor's note: The southbound interface (SBI) between the control plane and the SDN routers/switches used for the configuration of the forwarding rules at the SDN routers/switches is FFS.

Editor's note: It is FFS whether the SBI interface between the CP and the SDN routers/switches is in the scope of 3GPP.

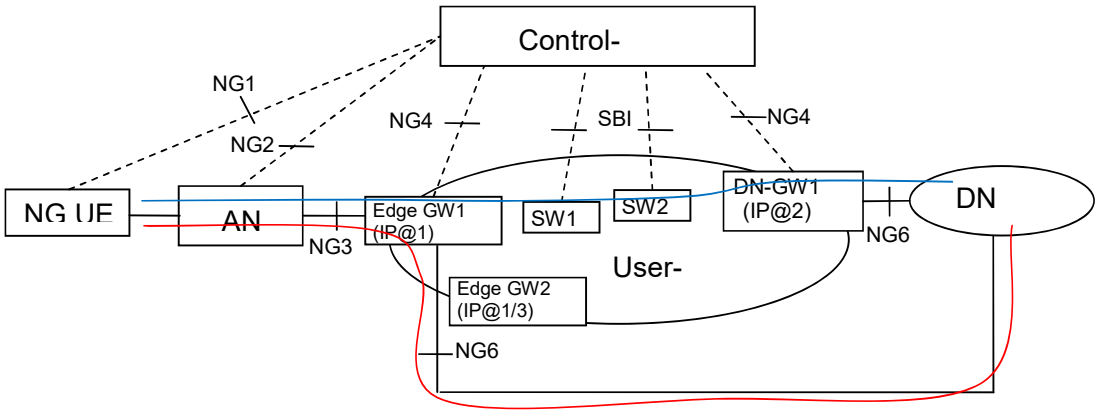


Figure 6.4.14.1-1: Reference Architecture with Edge GW close to the UE's AN and DN-GW in central location and SDN-based forwarding

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 246 of 501

6.4.14.2 Session establishment with Edge GW and DN-GW selection and configuration

The following Figure 6.4.14.2-1 shows the signalling flow diagram for the establishment of a new PDU session with local Edge GW anchoring IP@1 address and DN-GW anchoring IP@2 aaddress.

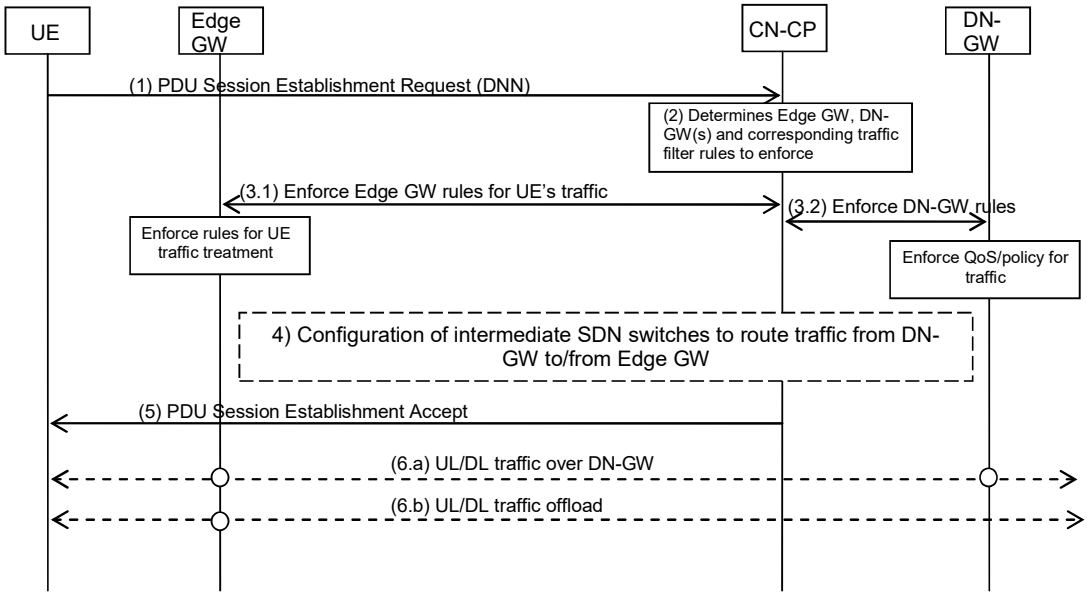


Figure 6.4.14.2-1: Session setup with Edge GW and DN-GW selection

The description of the steps is as follows:

1. The UE sends a PDU Session Establishment Request (Data Network Name (DNN)) message to CN-CP.

2. The CN-CP selects an Edge GW considering the location of the UE, the subscription parameters for the corresponding DDN and UE's context information (if available) like the mobility characteristics, or the user's preferred communication profile. The CN-CP can optionally select a DN-GW specific to a subscribed service (part of the same DNN).

3. The CN-CP provides forwarding and traffic treatment rules to the selected Edge GW and to the DN-GW. The downlink QoS parameters at DN-GW can be different from the default QoS parameters enforced at the Edge GW. At the Edge GW, the rules for uplink traffic can be aggregated, e.g. based on the UE's source IP address for forwarding towards the DN-GW and the destination IP addresses for offloading.

4. The intermediate SDN switches (SW1, SW2) are configured to forward traffic in the UL towards the DN-GW (e.g. based on source IP@2 address), and in the DL towards the Edge GW (e.g. based on destination IP@2 address).

5. The CN-CP sends a PDU Session Establishment Accept message to the UE, specifying the IP prefix/address that shall be used by the UE.

NOTE 1: In case of stateless address auto-configuration, the UE utilizes the information provided in this message to build an IP address.

6. The uplink (UL) and downlink (DL) traffic between the UE and the DN transits via Edge GW, whereas some IP flows can be offloaded and other IP flows are forwarded to a selected DN-GW1.

6.4.14.3 Edge GW relocation

Due to user mobility or other circumstances, e.g. load at the UE's Edge GW, the UE's Edge GW may be relocated, whereas the UE's current IP address may not match the new Edge GW's network. This is shown in Figure 6.4.14.1-1 as Edge GW1 and Edge GW2. If IP address continuity is required, the UE's IP address from Edge

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 247 of 501

GW1 can be imported and anchored at the UE's new Edge GW2. The CN-CP instructs the SDN SW to perform indirection of the UE's data traffic towards the UE's new Edge GW.

Editor's note: How the CN-CP configures different session and service continuity modes (SSC) for the same PDU session is FFS and may be covered in subclause 6.6. This refers to steps 1-3 below where decision is taken whether to advertise to the UE a new topologically correct IP prefix from Edge GW2.

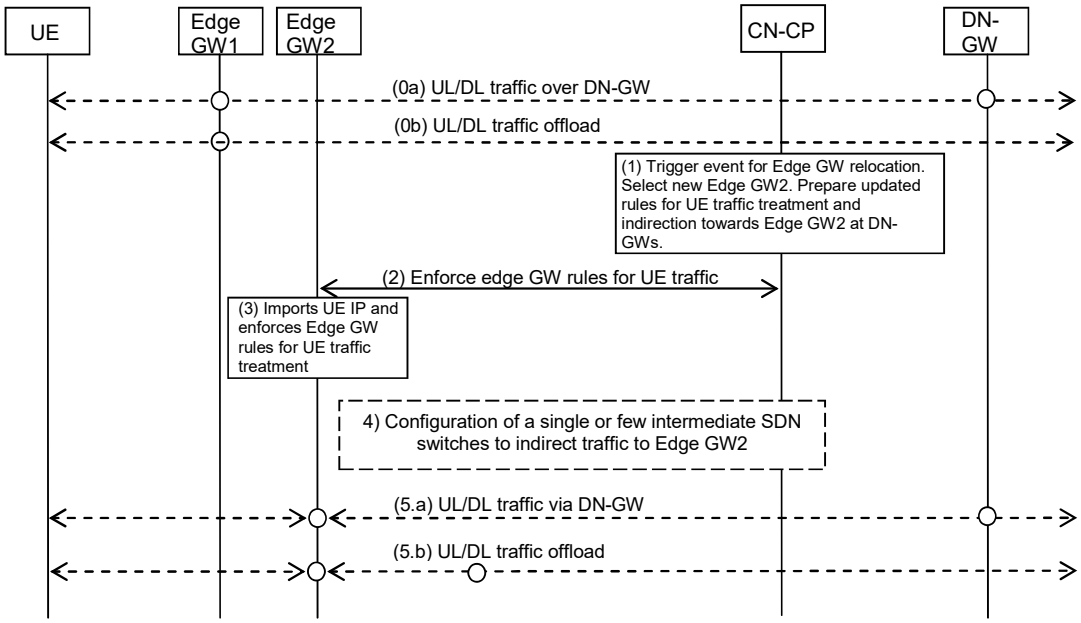


Figure 6.4.14.3-1: Edge GW relocation and intermediate SDN SW update.

The description of the steps is as follows:

0. The uplink (UL) and downlink (DL) traffic between the UE and the DN transits via Edge GW and DN GW.

1. An Edge GW relocation event occurs due to UE mobility (or other event) and the decision is taken at CN-CP. The CN-CP selects a new Edge GW2 as the UE's Edge GW and enforces rules for the UE traffic ad that edge policy enforcement.

2. The CN-CP enforces rules for the UE's data traffic at the new Edge GW2.

3. The traffic rules are enforced at the new Edge GW2. The Edge GW2 imports the UE's IP address (IP@1) as traffic selector and associated traffic treatment rules. The Edge GW2 may also advertise a topologically correct IP prefix (e.g. IP@3) to the UE.

4. The CN-CP updates rules in the one or multiple intermediate SDN switches close to Edge GW2 in order to assure that traffic targeted to IP@1 and IP@2 is forwarded to Edge GW2 in the DL. In the UL, traffic sourced from IP@2 should be forwarded to DN-GW.

5. Uplink and downlink traffic traverses the new Edge GW2 and the DN-GW.

Editor's note: Whether the selection of proper SDN switches and the enforcement of updated forwarding rules is in the scope of 3GPP is FFS.

6.4.15 Solution 4.15: Common interfaces towards UE, AN with MM and SM decoupled

6.4.15.1 Description

This contribution proposes a solution for Key Issue 4, WT 2 (relation between MM and SM).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 248 of 501

There is a single CP entry function in the core network for the NG1 reference point, used for both MM and SM-related messages and procedures for a UE.

To decouple the MM function with SM function, the following should be as the basis:

- The NAS entry function (assuming provided by NG MM) is used as a message entry point between UE and NG-CN. One single NAS connection is established for transmitting both SM and MM NAS message.

- MM messages and SM messages and the procedures should be decoupled. Next-Gen MM is not expected to maintain session context or be aware of the content of SM NAS message except SM message routing. SM NAS message should be processed by Next-Gen SM. The NAS entry point inside NG MM will know if one NAS message should be routed to NG-SM, or just having a localized routing to NG-MM.

Editor's note：It is FFS how to work in detail to not maintain session context of SM in MM.

- The NAS entry function for the NG1 reference point will work as a NAS proxy and should route the NAS message to the correlated NAS handling network function (NG-SM or NG-MM).

Editor's note：The detail to decouple the MM NAS message and SM NAS message is FFS.

- The information about the correlated NAS handling network function(e.g., Next-Gen SM identity of the UE) should be included if the correlated NAS handling network function has been selected during the prior procedures, and thus the related NAS message is intended to be sent to the same NAS handling network function.

User database could be local with receiving and storing the subscription data from the SDM. The stored information is made available to both MM and SM. The standalone authentication function provides authentication and security mechanisms to both MM and SM.

Editor's note: It is FFS how to implement the UE authentication with MM and SM decoupled, e.g. separate authentication for MM and SM.

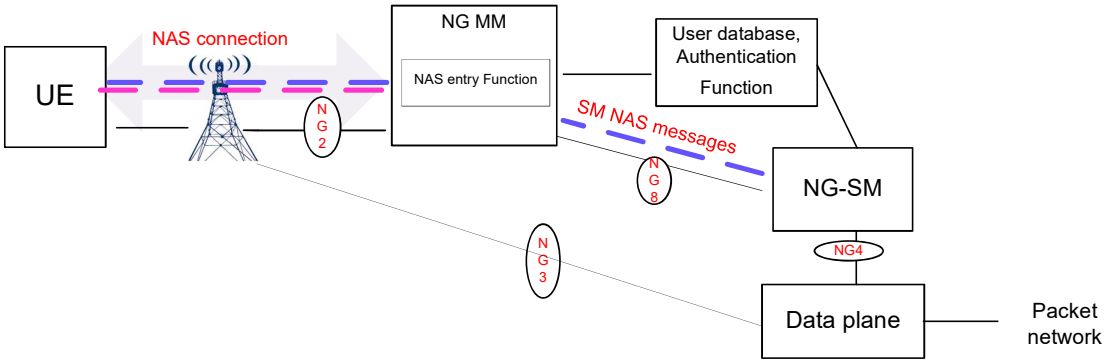


Figure 6.4.15.1-1: Common interfaces towards UE, AN with MM and SM decoupled

NOTE: The figure above does not show all CP related functionality e.g. related to policy control.

Editor's note: How the above proposals relate to non-3GPP access is FFS and depends e.g. on how MM and SM functionality is defined for non-3GPP accesses and how the overall architecture with non-3GPP is defined.

Editor's note: Whether and how the solution above is related to support of multiple connectivity is FFS.

6.4.15.2 Procedure

The procedure in figure 6.4.15.2-1 gives a general procedure about the NAS message routing and processing.

Editor's note: It is FFS for the detailed interactions between MM and SM due to mobility, state changes, paging, etc.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 249 of 501

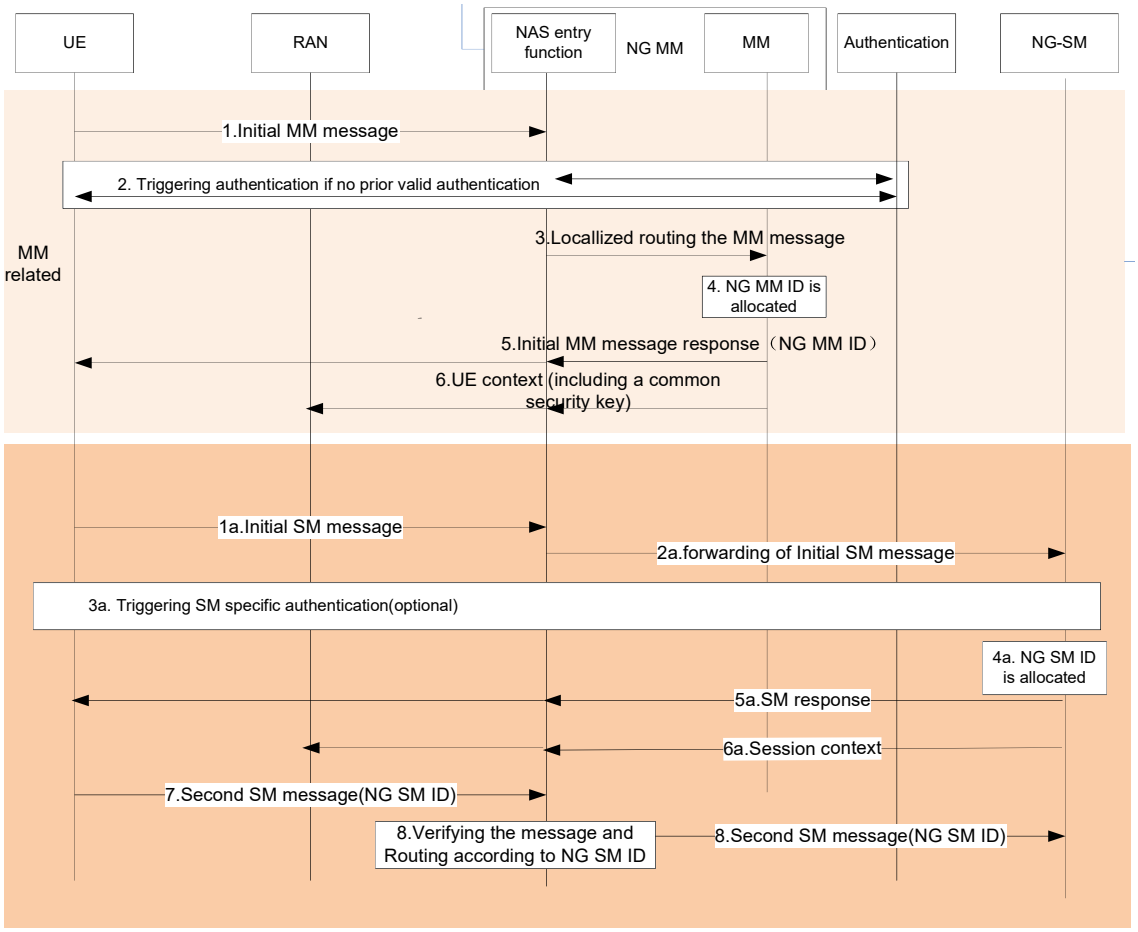


Figure 6.4.15.2-1: Example procedure about the NAS message routing and processing with MM and SM decoupled

1. UE sends an initial MM message to the NG-CN (e.g. attach, TAU). The NAS proxy is used as an entry point of NAS signalling messages.
2. If there is prior valid authentication between UE and NG-CN, an authentication shall be triggered between UE and the Authentication Function. A common NAS security is established between UE and NAS entry function.
3. NAS entry function inside NG MM determines the initial MM message (e.g according to the indication in NAS header) should be localized routed to MM model inside the NG MM.
4. MM allocates a NG MM ID for the UE. The NG MM ID is expected to be used to route the MM signalling thereafter.
5. MM replies an initial MM message response message to UE, which includes the NG MM ID.
6. MM forwards the UE context to RAN. Security context for AN may be included.

1a. UE sends an initial SM message to the NG-CN (e.g. PDN connectivity request).

NOTE: This message may be protected by the common NAS security if exists.

2a. NAS entry function inside NG MM forwards it to the corresponding SM entity.

NOTE: This message may be protected by the common NAS security if exists. How the SM entity is selected is up to the discussion of slices/network function selection. The SM NAS message may be verified and deciphered by the NAS entry function if the common NAS security is implemented there

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 250 of 501

3a. Optionally, based on slice policy, if a slice specific security is required, then a SM specific authentication need to be triggered between UE and SM.

Editor's note: Whether this slice specific authentication is required or not may depend on the security level and service's security requirement from Service Provider. And what is the slice specific authentication and how it works are FFS

4a. SM allocates a NG SM ID for the UE. The NG SM ID may be used to route the SM signalling thereafter.

Editor's note: The detail of NG SM Selection, NG SM ID and how to route the SM signalling is FFS.

5a. SM answers an initial SM message response message to UE, which includes the NG SM ID.

6a. SM sends the session context to RAN.

7. UE sends a second SM signalling message containing NG SM ID to SM.

8. NAS entry function inside NG MM determines (e.g according to NG SM ID) to route the SM message to the SM function.

6.4.16 Solution 4.16: the interaction between MM and SM

This solution is to address Work task 2 "the relation between SM and MM".

6.4.16.1 Architecture Description

6.4.16.1.1 Overview

The function architecture with MM and SM separation in Core network control plane functions is depicted in the following figure where MM and SM are in 2 different functional entities with a standard NG11 interface in-between:

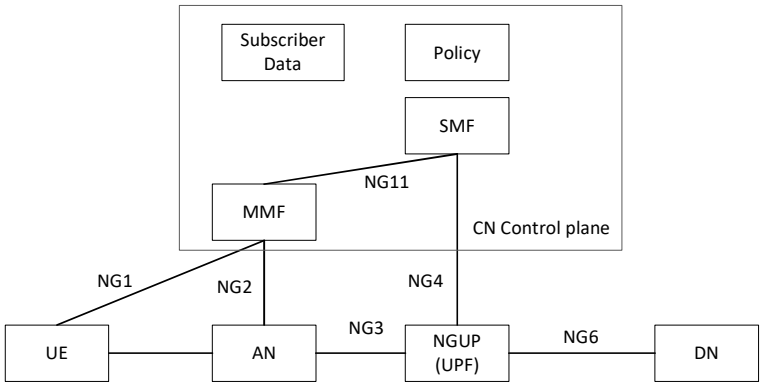


Figure 6.4.16.1-1: The reference architecture with MM and SM separation

The architecture includes the following functions and principles:

- The MMF Network Function supports the UE management functions per UE level, including: UE registration/de-registration, UE location reachability;
  - There is an unique MMF serving an UE. In case of roaming, MMF is always located in the serving PLMN
- The SMF Network Function supports the end-to-end control functions on PDU sessions and the SM control signalling towards/from UE is transferred via MM NF;

NOTE 2: Different SMF entities may manage different PDU Sessions of the UE without conflicting each others.

  - The context related with a PDU session in a NGUP (User Plane) is controlled by the SMF: NG4 terminates in the SMF

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 251 of 501

  - In case of roaming there is a SMF entity handling the SM signalling of the UE in the serving PLMN. In case of Home Routed roaming, there is another SMF entity in the HPLMN that controls the UPGW/UPF that terminates the NG6 interface with the Data Network.

- The MMF and SMF are separate NFs, with a standard NG11 interface.

- In case the UE is served by multiple slices the MMF belongs to the Common Core Functions (shared sub-CN instance).

  - In case of "group B" slicing architecture the SMF and the UPGW belong to a dedicated sub-CN instance.

  - In case of "group C" slicing architecture only the UPGW belongs to a dedicated sub-CN instance,

  - In case of an UE served by multiple slices there are multiple instances of SMF that serve the UE.

- The UE and the Core Network exchange NAS signalling via the common NAS Font-End that is located in the MMF. There is a unique NAS Front-End per UE handling all NAS related signalling from the UE. The NAS Font-End in MMF terminates NAS security for all NAS signalling and for NAS signalling that corresponds to SM acts as a relay between the UE and the different SMF instances. Nevertheless from the UE perspective there is an unique NAS termination in the network

  - MMF stores the identification of serving SM function(s) of UE and SM stores the identification of serving MM function of UE. Beyond this, the MMF is not expected to maintain session context or be aware of the content of SM NAS messages. SM NAS message are processed by SMF. Accordingly Session contexts should only be stored at SMF.

  - NAS MM messages and NAS SM messages and the corresponding procedures should be decoupled, so that the NAS Front End inside MMF can easily know if one NAS message should be routed to a SMF, or locally processed in the MMF.

NOTE 3: This simplifies the procedures related with NAS security (avoiding that each SM has to manage NAS security and the necessary re-Authentication that may be needed to refresh the NAS security keys)

- NG2 signalling related with UE is terminated in the MMF i.e. there is an unique NG2 termination for a given UE regardless of the number of PDU sessions (possibly zero) of this UE.

NOTE 4: This ensures that the RAN needs only to consider one single termination in the Core for the NAS signalling that it relays and this independently of the internal structure of the Core:.

  - To ensure a better decoupling of MMF and SMF, Mobility Management and Session Management related information shall be decoupled within NG2 signalling: the definition of the NG2 allows the NG2 termination in MMF to be able to transparently relay SM related information (like QoS control towards the AN, or the negotiation of NG3 transport information between the RAN and the UPGW) between the RAN and the SMF.

  - Some NG2 signalling (such as Hand-Over related signalling) may require both MMF and SMF interactions. MMF is responsible to ensure the coordination between MMF and SMF interactions.

Editor's note: The support in case on Non 3GPP AN is FFS. In that case a few features at the interface between MMF and SMF may not be needed such as the MMF-SMF interactions related with the transfer of SM related information to the AN via NG2. This point is assumed to be dealt with as part of KI 8.

6.4.16.1.2 Interactions between MMF and SMF

The interactions between MMF and SMF include:

- MMF maintains the UE MM context including UE location, the status of UE Control Plane Connection (NG1), SMF identities and SMF maintains the session context including the status of the UE session.

- There may be multiple SMF in CN CP to control the different types of PDU sessions on the UE. The MMF selects the SMF functions based on the assistance information in the NAS signalling. The UE is not aware whether a single SMF or different SMFs are handling the PDU Sessions of the UE.

- For one UE, the SMF NF store the MM NF that serves the UE in UE SM context in order to be able to use the NG1 / NG2 termination capability of the MMF.

- When UE mobility events occurs, the MMF NF notifies the related SMF NF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 252 of 501

- Some Mobility related events or state transitions have an impact on the PDU sessions and may require action on the NGUP (the User Plane entities in the Core) i.e. on NG4. Likewise some Session related actions are required towards the AN (on NG2)

    1. At the set-up / modification of a PDU session: the SMF needs to interact with MMF in order to send to the AN Data handling control information (e.g. indication of where to send UL traffic from the UE, rules related with the QoS associated with data flows) and needs to receive from the AN DL Data forwarding address information (User Plane address of the AN) in order to control DL data forwarding in the NGUP(s). This corresponds to NG2 impacts of SM events.

    2. At the release of a PDU session: the SMF needs to interact with MMF in order to remove the corresponding Data handling policies in the AN. This corresponds to NG2 impacts of SMF events

    3. At the transition from IDLE to CONNECTED: the SMF needs to interact with MMF in order to send to the RAN Data handling control information (e.g. indication of where to send UL traffic from the UE, rules related with the QoS associated with data flows) and needs to receive from the AN DL Data forwarding address information (User Plane address of the AN) in order to control DL data forwarding in the NGUP(s). This corresponds to the handling of a MM event requiring the exchange of session related information on NG2

    4. During a Hand-Over : the SMF needs to interact with MMF in order to receive from the RAN the DL Data forwarding address information (User Plane address of the RAN) from the RAN in order to control DL data forwarding in the NGUP(s). This corresponds to the handling of a MM event requiring the exchange of session related information on NG4

NOTE: The interaction information between MMF and SMF in Handover procedure depends on the detail handover solution discussed in mobility management key issue.

    5. When the UE becomes IDLE, MMF notifies the SMF in order for SMF to modify the settings for DL data forwarding in the NGUP(s). This corresponds to the handling of a MM event requiring the exchange of session related information on NG4

    6. When it has been made aware by the NGUP that some DL data has arrived for an UE in IDLE mode (and the UE is not known to be in a power saving state), the SMF has to be able to interact with MMF in order to trigger UE paging from the RAN. This corresponds to MM impacts (including NG2 impacts) of SMF events

    7. The SMF may need to interact with MMF in order to be able to control the NGUP(s) based on the power saving state of the UE

    8. When UE sends (non periodic) TAU request to MMF, the MMF may need to notify the SMF so that the SMF can determine whether TUPF relocation is required or not (based on SSC mode and on the new user location).

Editor's note: It is FFS whether or not MMF may need to notify the SMF of the transition of UE's idle mode mobility level. This can be added after decision on the Support for Idle Mode Mobility capabilities.

Management of the relationship between MMF and SMF

Some functionalities are needed in the MMF to deal with the multiple SMF that serve the UE: These functionalities are aware of the SMF that serve the UE and Route NAS SM signaling to SMF

- MMF store the identification of serving SMF(s) of UE

    - The relationship between MMF and a SMF entity is created at the first PDU session for the UE that is handled by a SMF instance and released when the last PDU session for the UE is deactivated in SMF.

- SMF stores the identification of serving MMF of UE.

Further considerations

- The SMF needs to receive an indication of the permanent user identity of the UE having sent a NAS SM message. This is needed for Policy, charging and LI interactions.

- When SMF needs to send NAS SM signalling to an UE, it provides the permanent user identity of this UE, in order for the NAS Front-End in MMF to retrieve the corresponding NAS signalling security context.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 253 of 501

6.4.16.1.3 Subscription data

It is needed to Control whether NAS SM requests from the UE comply with the user subscription. SMF enforces such control based on SM related subscription data.

To allow such control following alternatives are possible

- Alternative A: the MMF provides SMF with all SM related subscription data for the UE. Furthermore MMF notifies all SMF instances each time it receives a notification from SDM that such data has been modified .
- Alternative B: the MMF puts in a 'Service data Layer" Database located in the Serving PLMN the subscription information it has received from the Subscriber Data Base (in HPLMN). This information is made available by MMF to SMF. SMF subscribes towards the 'Service data Layer" Database to changes of the SM related subscription data of an UE (actually to changes on the DNN/APN related subscription data) .
- Alternative C: Each SMF contacts the SDM (in HPLMN) to fetch the SM related subscription data for the UE and subscribes onto the SDM (in HPLMN) for any modification of these data. This means that SDM has to manage subscriptions to subscriber data modification coming not only from MMF but also from each SMF that serves the UE
- Alternative D: Like alternative A but SMF explicitly subscribes to MNF to only receive a subset of the change of SM related subscription data

Editor's note: Only one alternative will be selective for the normative phase. These alternatives may require further clarifications

Editor's note: The interaction between the MM and SM besides the above mobility event procedure are FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 254 of 501

6.4.16.2 Function description

6.4.16.2.1 Set-up of a PDU session

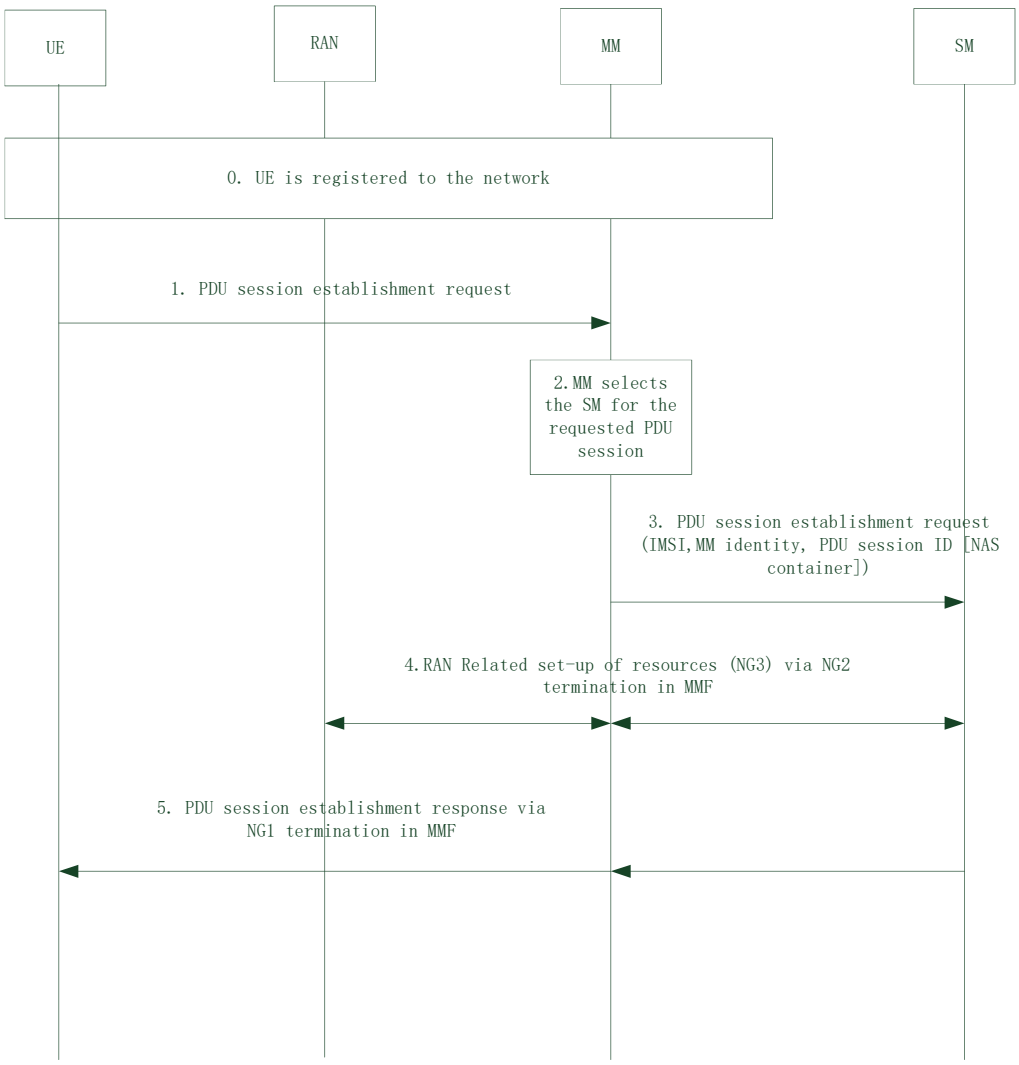


Figure 6.4.16.2.1-1: The PDU session establishment with NGm connection establishment

Step 0: UE is registered in the MMF.

Step 1: UE sends a NAS SM message to request a PDU session establishment.

Step 2: MMF selects a SMF function for the requested PDU session. SMF selection may be based on the requested DN name, UE's location information and slice related information. MMF stores the identity of selected SMF.

Step 3: MMF sends the PDU session establishment request message to the SMF. This message includes UE's IMSI, MMF identity and PDU session Identity and a NAS container. The NAS container includes the SM related NAS message transferred from UE to MMF. The MMF may also include other information such as UE location information,

Step 4: SMF initiates session establishment including set-up of NG3 with RAN via NG2 termination in MMF. The NG2 information from SMF is provided in NG2 containers between MMF and SMF and forwarded over NG2 by MMF towards RAN. In NG2 messages from RAN, the MMF identifies the SM NG2 information and provides it in NG2 containers over NG11 to SMF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 255 of 501

Step 5: SMF sends a message with a NAS container to the MMF. The NAS container includes the SM related NAS PDU Session establishment response that is to be forwarded to UE byMMF. The message also includes an indication to MMF that the session establishment is successful.

Allocation of the PDU session Identity:

It is needed to allocate a PDU session identity that is unique per PDU session of the UE and used at NAS layer between the SM entities in the UE and the SMF. The PDU session Identity is relative to an UE i.e. 2 UE may have sessions with the same PDU session Identity. It is used by the MMF to detect a new session and to direct SM related NAS signalling to the relevant SMF.

The PDU session Identity is allocated by the MMF: when it starts a new PDU session, the UE uses a default dummy PDU session Identity and upon reception of the corresponding SM signalling, the MMF allocates the PDU session Identity for that PDU session

Then

- when MMF detects NAS SM signalling with a new PDU session Identity, it allocates a SMF for this new PDU session and stores the association between the SMF Id and the PDU session Id
- when MMF detects NAS SM signalling with a known PDU session Identity, it forwards this SM signalling to the corresponding SMF.
- When the PDU session is torn down, SMF indicates to MMF the release of the PDU session Identity. The MMF removes the association between the SMF Id and the PDU session Id

As described in sub-clause 6.4.16.1.2, the SMF needs to be invoked based on some mobility events (e.g. IDLE – CONNECTED transitions, Hand-Over) thus there is a need for the MMF to know whether it needs to notify SMF about these mobility events.

There are 2 alternatives:

- alternative 1: Implicit subscription: when MMF allocates a SMF for a session, it implicitly knows that it needs to notify that SMF with session events (implicitly subscribes SMF to mobility events)
- alternative 2: SMF has to explicitly subscribe. This is documented in sub-clause 6.4.16.2.2

Editor's note: Only one of these alternatives will be selected for the normative phase

6.4.16.2.2 The subscription on UE mobility

NOTE: This corresponds to alternative 2 of 6.4.16.2.1

Editor's note: It is FFS whether this alternative will be selected for the normative phase

The subscription on UE mobility is depicted in the following figure:

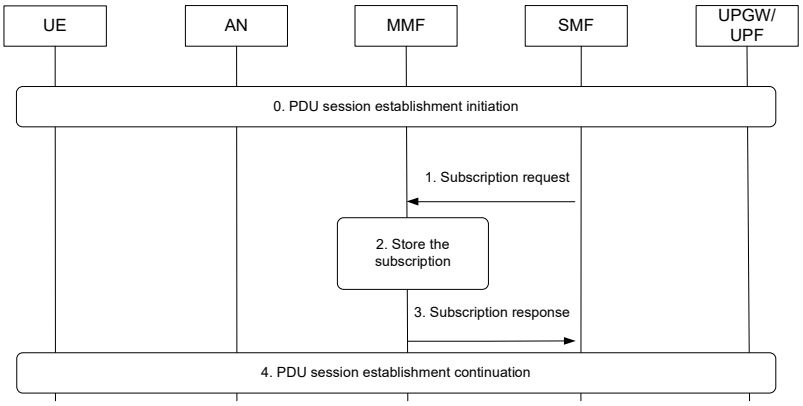


Figure 6.4.16.2.1-1: The subscription on UE mobility

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 256 of 501

0. During PDU session establishment, the MMF selects a SMF to handle NAS SM signalling indicating a new PDU session. The MMF transfers the SM NAS signalling between UE and SMF. The permanent User Identity is added to the NAS SM Signalling exchanged between MMF and SMF.

1. When the SMF considers the PDU session set-up request as valid, the SMF registers onto MMF for this UE and PDU session. This registration request includes the UE Identity, the PDU session Identity and the SMF identity. It may contain a Subscription Request on UE mobility in order for the SMF to be notified when an UE mobility event occurs(e.g. change between IDLE and CONNECTED, change of AN Node).

   The PDU session Identity is used by the MMF to know towards which SMF it needs to send uplink NAS SM signalling received from the UE

Editor's note: in case one SMF supports multiple PDU sessions for an UE it is FFS whether the SMF issues one subscription per PDU session or per UE

2. The MMF stores the ID of the SMF instance which serves the UE for that PDU session and the event notification request.

3. The MMF sends the Registration and Subscription Response to SMF to confirm the registration and subscription request is accepted.

4. The set-up of the session goes on: the SMF determines NG3 addressing information at the UPGW/UPF and QoS policies related with the PDU session and has via MMF NG2 signalling related with the PDU session exchanged with the AN. This NG2 signalling contains:

   - From SMF to AN: NG3 addressing information (at the UPGW/UPF) and QoS policies related with the PDU session

   - From AN to SMF: NG3 addressing information (at the AN) related with the PDU session

NOTE: It is up to stage 3 to determine whether or not step 4 takes place simultaneously with steps 1, 2 and 3

6.4.16.2.3 The notification on UE mobility

The notification on UE mobility is depicted in the following figure:

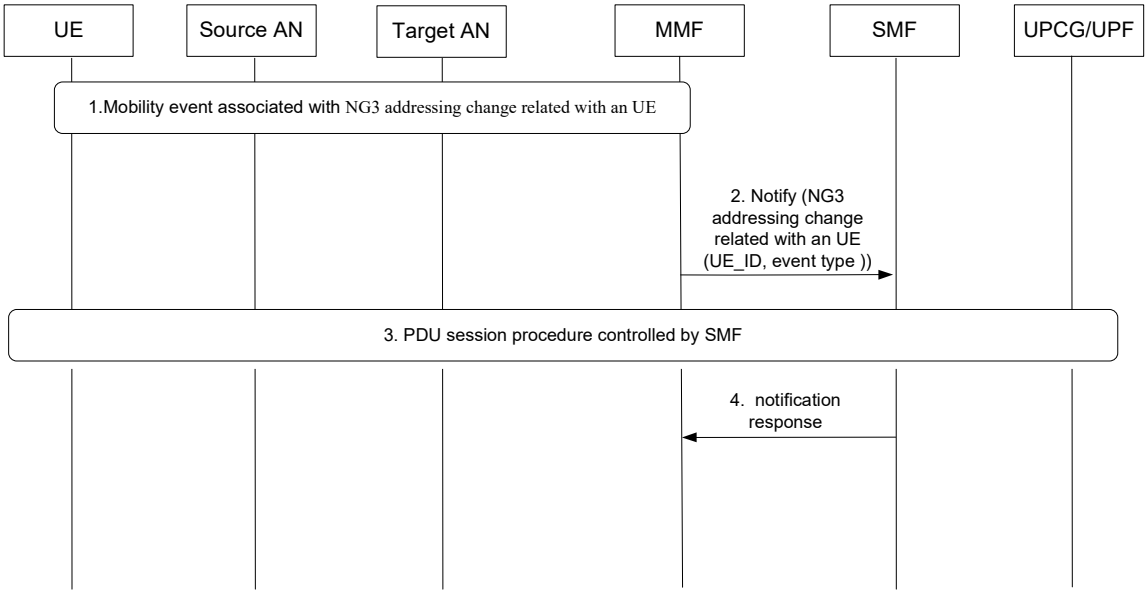


Figure 6.4.16.2.3-1: the notification on UE mobility

1. A Mobility event occurs that induces the need to notify SMF(s)

2. The MMF identifies which NFs shall be notified, and the MMF sends UE Mobility Notification message to the corresponding SMF. The notification includes UE ID event type and PDU session Id.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 257 of 501

3. The SMF perform the related session update, the detail session update procedure is determined by the session management solution;

   This may induce the transfer via MMF of NG2 signalling exchanged with the AN and related with the PDU session. This signalling contains:

   - From SMF to AN: NG3 addressing information (at the UPGW/UPF) and QoS policies related with the PDU session

   - From AN to SMF: NG3 addressing information (at the AN) related with the PDU session

4. The SMF sends UE Mobility Notification Response to the MM NF to confirm its operation on the NG3 addressing change related with an UE is completed;

NOTE: It is up to stage 3 to determine whether or not step 4 takes place simultaneously with steps 2 and 3

6.4.16.3 Solution evaluation

Subscription data transfer to SMFs

Two cases need to be considered:

- Initial subscription data transfer (providing subscription information to SMFs during session establishment)

- Subscription update (inform SMFs when the subscription data in the SDM is updated

NOTE: Subscription updates are very rare events.

Evaluation of the options for SMF to get subscription data:

- Alternative A/D (via NG11): From SDM's perspective, there is a single NG8 terminating point for a UE, so no interface between SDM and SMF is required. The signalling path for both initial subscription data transfer and subscription updates involves

  - MMF and SMF,

  - (in case of home-routed roaming) MMF, SMF in VPLMN and SMF in HPLMN.

  For initial subscription data transfer the subscription information can be sent together with session establishment signalling to SMF (i.e. no additional signalling is needed). Notification of SM subscription data change would use a common interface from SDM to MMF for both MM and SM related subscription data updates. The SM-related subscription data, would require forwarding from MMF, via SMF in VPLMN to SMF in HPLMN in case of home-routed roaming

  NOTE: This forwarding means involving MMF and SMF in VPLMN for SM subscription data change that may be used only by SMF in the HPLMN (use of SM subscription data by V-SMF is FFS).

  There is less load on SDM as each SMF does not need to request subscription data from SDM.

- Alternative B: From SDM's perspective, there is a single NG8 terminating point for a UE, but additional interfaces (MMF-Data layer to write the subscription data, Data layer-SMF to read the SM subscription data) are needed. For notifications related with SM subscription data change, MMF is involved by forwarding the updated subscription data to Data Layer that distributes it to the active SMFs. Solution is only applicable in non-roaming case and roaming LBO cases, a different solution is needed in case of home-routed roaming.

- Alternative C: From SDM's perspective, there are multiple NG8 terminating point for a UE (MMF + the SMF that serve the UE). The direct fetch of SM related subscription data for a UE by SMF does not involve the VPLMN. MMF is not involved for notifications related with SM subscription data change, so there is less load in MMF. Updates to subscription data needs to be pushed to the active MMF and SMFs and it needs to be ensured that potential race conditions due to simultaneous update towards MMF and SMFs are resolved.

6.4.17 Solution 4.17: Void

void

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 258 of 501

6.4.18 Solution 4.18: Solution for Infrequent Small Data

6.4.18.1 Architecture description

With the 5G architecture of the Core Network (CN) there are a number of basic assumptions made for Infrequent Small Data delivery:

- The PDU may be IP based or non-IP based.
- The method is based on using the methods in RAN developed for 5G, specifically the "RRC Inactive Connected/Active Connected" states and potential optimizations thereof. The solution thus assumes that the AN does not release the UE context. In case the AN releases the UE context, the solution falls back to regular CN IDLE state handling.
- CN CP UE contexts are established at attach or session setup.
- CN CP preserves UE PDU Session contexts as long as PDU session is maintained.
- CN UP can refrain from preserving UE state information during inactive periods for the UE. In this case CN UP context and connectivity is established when UE originated or terminated packets need be forwarded in the UP. After a packet is forwarded to/from the UE, a UE context is held for a short time in the CN UP to facilitate the server to send e.g. ACKs to/from the UE. Removing UE context from CN UP during inactivity periods and maintaining UE state only for a small fraction of the time allows the CN UP to multiplex its resources over a larger number of UEs.

6.4.18.2 Function description

6.4.18.2.1 Connection Establishment Flow

This clause shows how a PDU session is established for a UE device that sends data infrequently.

The procedures are depicted in the Figure 6.4.18.2.1-1.

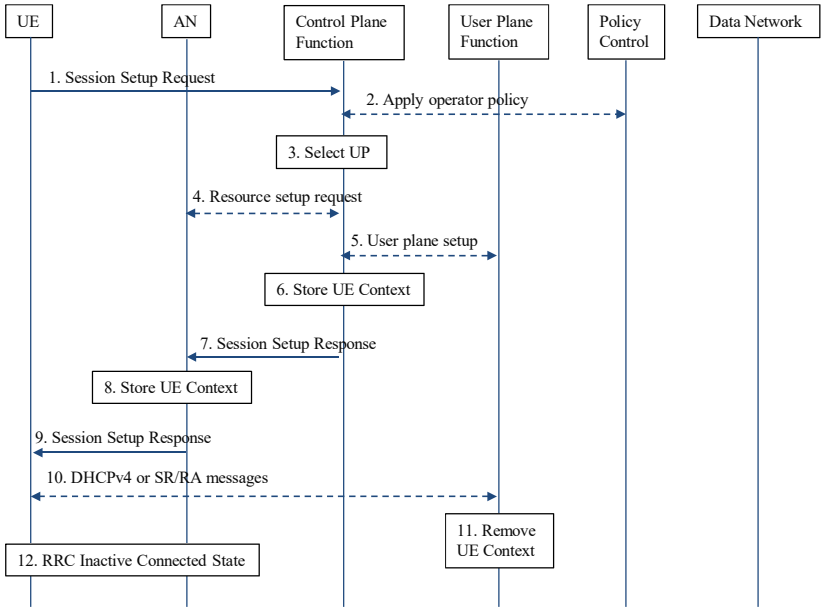


Figure 6.4.18.2.1-1: The procedure of session setup for infrequent data

It is assumed for this procedure that the UE is attached to the network. As part of the attach procedure, subscription data is fetched from the Subscriber Data Management function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 259 of 501

1. The UE initiates a session setup request. The UE provides information indicating the PDU session type (e.g. Non-IP/IP). Indication of the DN network name may also be included.

2. The SM function may interact with the Policy control function which determines the QoS property of the connection based on information such as UE request, and operator policy.

Editor's note: how the QoS related property is set per operator policy is per the solutions developed for the QoS and Policy Framework Key Issues.

3. The SM function selects user plane function and a tunnel identifier associated with the UE. In case of IP-based PDU type, the SM function assigns UE IPv4 address/IPv6 prefix anchored in the User plane function.

4. The SM function may request the AN to setup resources for the session.

5. In case of IP-based PDU type, the SM function triggers the establishment of user-plane session if to enable IPv6 stateless address auto-configuration or DHCPv4 options for IP address/prefix allocation after PDU session established. In this case, the DHCPv4 or RS/RA messages will be forwarded by the UP function between UE and the Control Plane functions.

This step is not needed if IP configuration is performed in the protocol over the control plane between the UE and the Control Plane Functions, or in case PDU address is not assigned to the UE at all.

6. The SM function stores the UE context with all necessary UE and PDU session data.

7. The SM function completes the establishment in CP and optionally in UP and provides the AN function with Uplink tunnel information.

Editor's note: It is up to solutions to other Key Issues if other information is transferred such as QoS, max bit rates etc

8. The AN function stores the UE context.

9. Session setup is complete.

10. In case IP, IPv6 stateless address auto-configuration or DHCPv4 procedure may be triggered between UE and the SM function over the user plane and the control plane between SM and User Plane Functions.

11. In case of IP-based PDU type, after the IPv6 stateless address auto-configuration or DHCPv4 allocation procedure is finished the UP Plane function may delete the UE context to release resources during a possibly long UE inactivity period. This may be triggered due to UE inactivity during a time period.

12. Due to e.g. user inactivity during a time period the AN function moves the UE to RRC Inactive Connected State.

6.4.18.2.2 Uplink PDU Transfer Flow

This clause shows how a Uplink PDU is transfer from a UE device that sends data infrequently.

The procedure is depicted in the Figure 6.3.18.2.2-1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 260 of 501

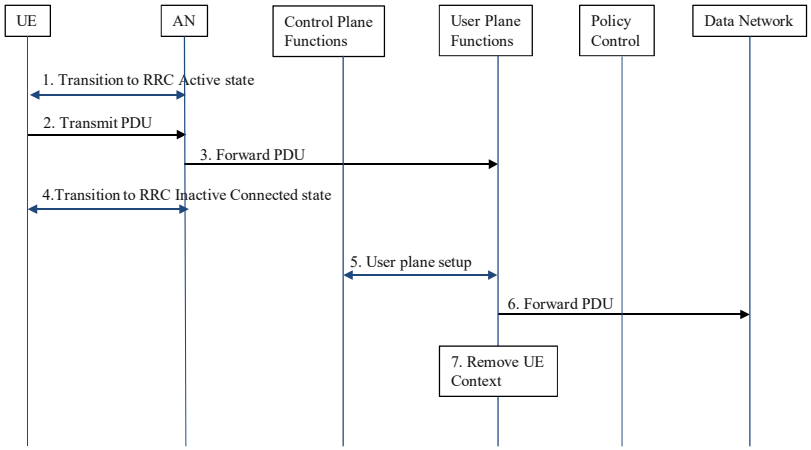


Figure 6.4.18.2.2-1: Uplink PDU transfer

It is assumed for this procedure that the UE is attached to the network and that a PDU session is established, the UE is in RCC Inactive Connected State and no UE context is currently established in the CN UP.

1. The UE and AN transitions to RRC connected state.
2. The UE transmits the PDU to AN and in case the UE knows that this is the last PDU to be transmitted for this occasion the UE may indicate it together with the last PDU.
3. The AN encapsulates the PDU into a tunnel protocol header and forwards the PDU to the User Plane function indicated by the tunnel identifier part of the UE Context.
4. After the AN has forward the PDU, the AN initiates transition to RRC inactive state triggered by last PDU marking or due to UE inactivity during a time period. The UE is moved to RRC Inactive Connected State.
5. The User Plane function receives the uplink PDU and as the UE Context does not exist the User Plane function requests the Control Plane function for the UE context. The User Plane function may select the Control Plane function based on the user plane tunnel identifier in the received PDU.

   In case that a UE Context already exists in the User Plane functions this step is omitted.
6. The User Plane function forwards the PDU to the Data Network. The User Plan function may enforce e.g. QoS marking, charging etc.
7. The User Plane function may remove the UE context according to e.g. a last PDU marking or e.g. due to inactivity.

Only up-link UP packets that are authorized based on the UE context in the AN are forwarded to the CN UP in step 3. This reduces the risk of DoS attacks causing overload in step 5.

6.4.18.2.3 Downlink PDU Transfer Flow

This clause shows how a Downlink PDU is transferred from a Data Network to a UE device that sends data infrequently.

The procedure is depicted in the Figure 6.4.18.2.3-1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 261 of 501

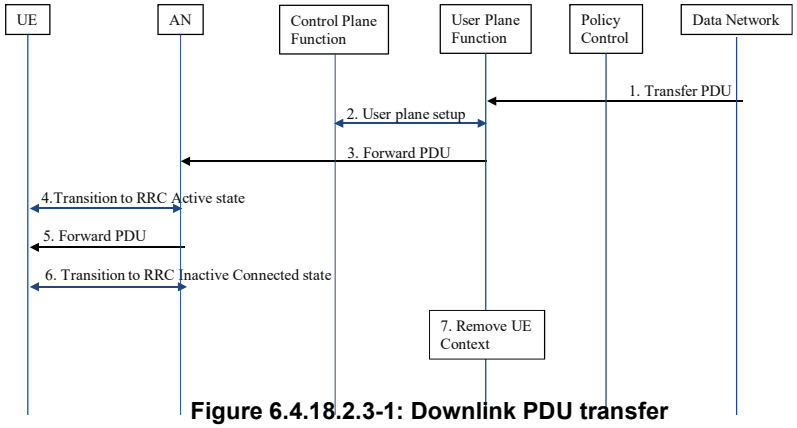


Figure 6.4.18.2.3-1: Downlink PDU transfer

It is assumed for this procedure that the UE is attached to the network and that a PDU session is established, the UE is in RCC Inactive Connected State and no UE context is currently established in the User Plane functions.

1. The application server in the Data Network transfers a mobile terminated PDU towards the User Plane Functions. In case of IP the destination address is the IP address of the UE device.

Editor's note: How Non-IP PDU is handled is FFS.

2. The User Plane functions receives the downlink PDU and as the UE Context doesn't exists the User Plane functions requests the proper Control Plane functions for the UE context. In case of IP the IP address is used to derive the proper SM function.

In case that a UE Context already exists in the User Plane functions this step is omitted.

3. The User Plane function encapsulates the PDU into a tunnel protocol header and forwards the PDU to the AN identified by he AN tunnel identifier part of the UE context. The User Plan function may enforce e.g. QoS marking, rate limiting, charging etc.

4. When the AN receives the PDU the procedure the UE and AN transition to RRC active state.

5. The AN forwards the PDU to the UE.

6. After the AN has forward the PDU, AN initiates the transition to RRC inactive statewith the UE e.g. due to UE inactivity during a time period. The UE is moved to RRC Inactive Connected State.

7. The User Plane function may remove the UE context due to e.g. inactivity.

In case the UP function is accessible from the Internet, the UE context may need to be kept in the UP function for longer times to avoid unnecessary signalling between UP and CP in step 2 (e.g. due to DoS attacks). In this case the CP function can instruct the UP function to not release UE context or instruct the UP function to use a longer inactivity timer.

6.4.18.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.4.19 Solution 4.19: Infrequent small user data transfer via control plane

This contribution proposes a solution that applies for key issue 4 on WT 3 "Efficient infrequent small data transfer" of the session management.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 262 of 501

6.4.19.1 Architecture description

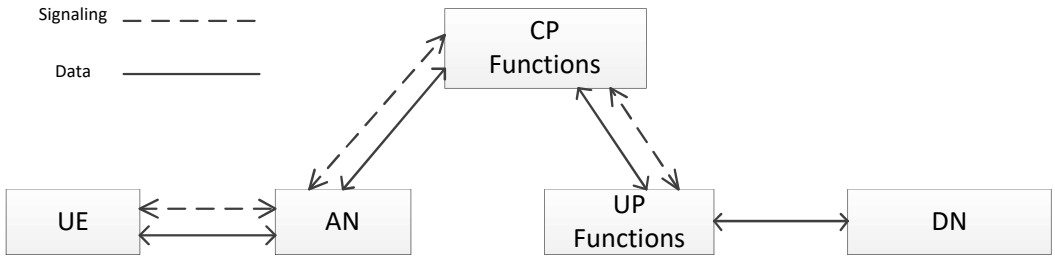


Figure 6.4.19.1-1: Architecture model for small data transfer in control plane - non-roaming case

In this solution, after UE attaches to the network, the CP NF may set up UE SM context by PDU session establishment procedure initiated by UE via NAS signalling, or the CP NF may set up UE SM context when it receives the non-IP PDU packet originated from UE. The CP then tracks the UE on tracking area granularity as UE is in idle mode.

When a MO PDU data needs to be transferred, the UE sends the data to the CP function via NAS PDU message. After integrity check and decryption, if corresponding session context does not exist in CP function, the CP function performs PDU session establishment and sets up SM context. The CP sends the PDU data to the UP function and then the UP function forwards the PDU data to the DN. For MT PDU data, the CP can initiate a paging procedure to find the AN node that the UE camps on, and sends the PDU data to the AN node then to the UE.

Editor's note: How to support roaming scenario is FFS.

6.4.19.2 Function description

6.4.19.2.1 Mobile originated data transport via control plane

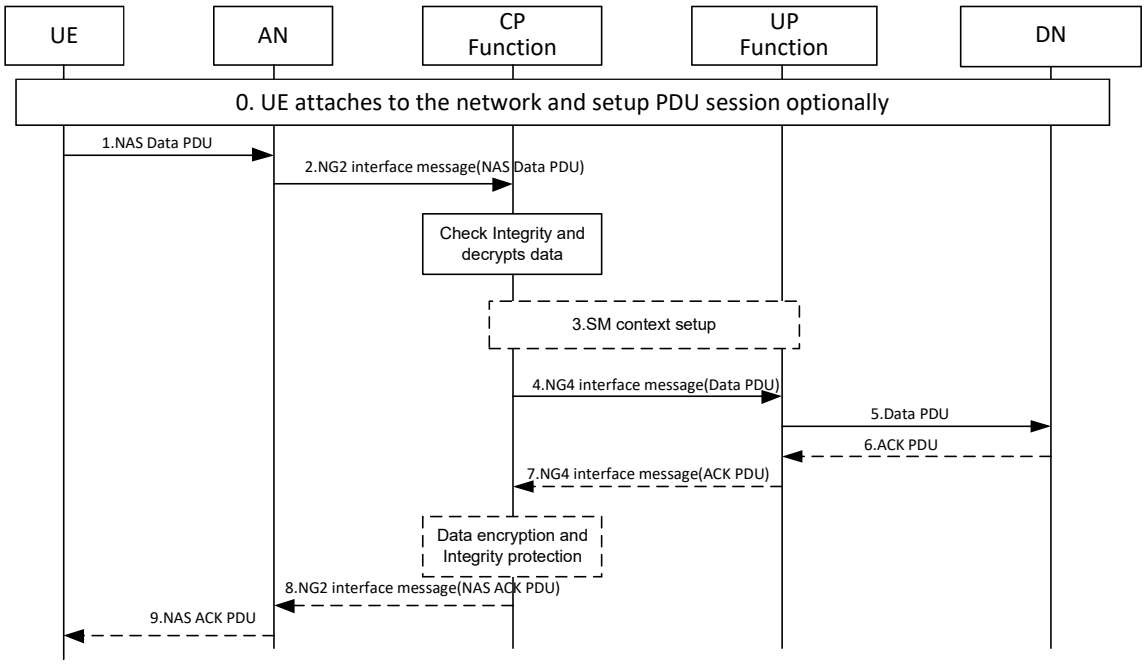


Figure 6.4.19.2.1-1: MO data transport in NAS PDU– non-roaming case

0. The UE attaches to the network. The CP may setup PDU session and perform the IP address allocation according to UE's request, capability or subscription.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 263 of 501

1. The UE sends an integrity protected NAS PDU to the AN node. The NAS PDU carries the encrypted uplink PDU data. The detail of this step should be decided in RAN WG.

2. The NAS PDU is relayed to the CP function by the AN node using a NG2 interface message.

3. The CP Function checks the integrity of the incoming NAS PDU and decrypts the PDU data.

In case the PDU data is non-IP packet, the CP check if there is a corresponding session context exists for the NAS PDU. If no, the CP function setups session context by performing UP selection and allocate IP address for the UE. The CP function may select the UP function based on the service type indication carried in the NAS PDU. The UE need not be involved in the procedure.

4. The CP function sends the PDU data to the UP function according stored UE context using a NG4 interface message. The CP function maintains a short lived association of the RAN node with the UE to assure the acknowledge message can be sent back to the UE.

5. The UP function forwards the PDU data to the DN.

In case the PDU data is non-IP packet, the UP shall encapsulate the PDU data into an IP packet. The source IP address should be set as the IP address of the UE.

6. The AS in the DN may return a DL PDU data, e.g. acknowledgement packet to the UP function.

7. The UP function forwards the DL PDU data to the CP function using a NG4 interface message. For non-IP type PDU session, the UP removes the IP header of the DL IP packet. In case UE context does not exist in the UP, the UP drops the DL PDU data.

8. The CP function encrypts and integrity protects the PDU data. Then the PDU data are encapsulated in a NAS PDU and sent to the AN node in a NG2 interface Message.

9. The AN node sends the PDU data encapsulated in NAS PDU to the UE.

6.4.19.2.2 Mobile terminated data transport via control plane

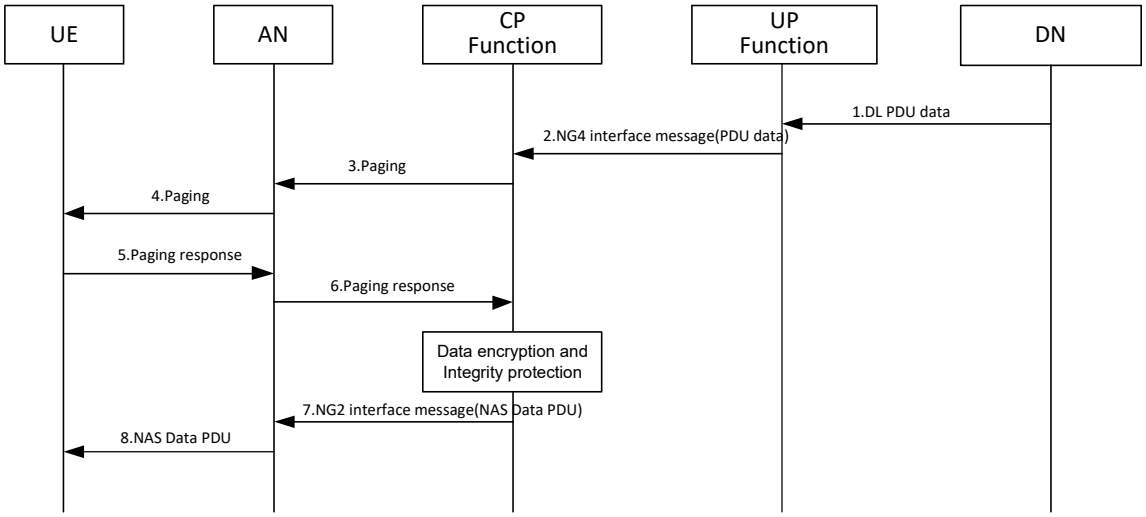


Figure 6.4.19.2.2-2: MT Data transport in NAS PDU– non-roaming case

1. The UP receives a downlink PDU data from the DN. In case the UE context does not exist in the UP, the UP drops the downlink PDU data.

2. The UP function finds the CP function according to context and sends PDU data to the CP function using a NG4 interface message.

3. If the CP function has no association on which RAN node that the UE camps on, the CP function will buffer the downlink data and sends paging message to AN nodes.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 264 of 501

4. The UE is paged by the AN nodes.

5-6. Upon reception of paging indication, the UE responses to the CP function via AN node.

7. The CP function performs integrity protection and encryption to the DL PDU data and sends it to the AN node using a NAS PDU carried by a NG2 interface message.

8. The NAS PDU with DL PDU data is delivered to the UE by the AN node.

6.4.19.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.20 Solution 4.20: Session Management on the PDU session(s) via different accesses

This solution applies to key issue 4 on session management. Specifically, the solution addresses the following work tasks:

- SM_WT_#5: PDU session(s) via different accesses

6.4.20.1 Architecture description

This clause describes a session management architecture focusing on the following three cases:

- Multiple PDU sessions via different accesses to the different data networks
- Multiple PDU sessions via different accesses to the same data network
- A PDU session via different accesses to the same data network (a.k.a. multi-access PDU session)

The proposed solution assumes the following session management model principles:

- A UE can have multiple PDU sessions via simultaneous multiple accesses to the different data networks or same data networks (as showed in the figure 6.4.20.1-1 and figure 6.4.20.1-2)
- A UE can have multiple PDU sessions via NG RAN and non-3GPP access network
- The establishment and release for the PDU Session via NG RAN (NR or Evolved E-UTRA) is performed using NG1 signalling.
- The establishment and release for the PDU Session via non-3GPP access may be performed using NG1 signalling.
- The SM context of NextGen core network should keep the access network types for multiple PDU sessions.
- A UE can have a PDU session via different accesses to the same data network (a.k.a. multi-access PDU session) (as showed in the figure 6.4.20.1-3)
- This solution defines « a multi-access PDU session » as follows;
  - A PDU session whose traffic can be routed over either a NG RAN or a non-3GPP access or both.

Editor's note: The definition of « a multi-access PDU session » is needed to be refined. It will be handled in phase 2 in detail.

- The SM context of NextGen core network should keep the access network types for a multi-access PDU session.
- There is one common MM CP function to manage multiple sessions via different accesses with individual NG1 connections as depicted in the following high level architecture. The ways to route over multiple accesses to the same CP function are
  1) Option 1: The information identifying the serving CP function is sent to the UE, and UE uses it when attaching via additional access. The access network directs the UE to the same CP function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 265 of 501

2) Option 2: The information identifying the serving CP function is stored to the CP management function (e.g. HSS). The CP function may be re-allocated when attaching via additional access.

- The SM message from a UE via NG1 is terminated to the serving MM CP function which is decided by MM attach procedure first. The MM CP function forwards the session setup request to the proper SM CP function (e,g. decided based on the requested DN Name)

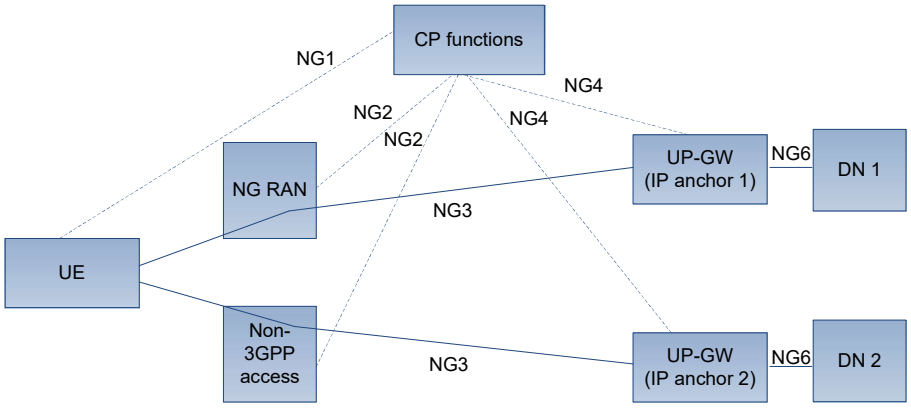


Figure 6.4.20.1-1: Multiple PDU sessions via different accesses to the different data networks

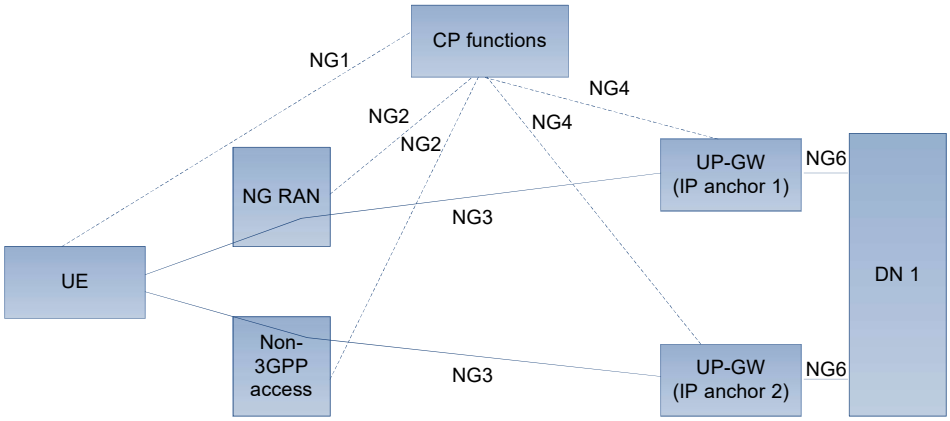


Figure 6.4.20.1-2: Multiple PDU sessions via different accesses to the same network

Editor's note: In case session bitrate limitation across all PDU sessions to the same data network is required (to be determined by the QoS key issue), then for UE with multiple PDU sessions towards the same DN there is the need of a Core Network User plane "convergence point" to support across session bitrate enforcement and charging. Across-session bitrate enforcement has to be run in a unique entity that handles all the DL traffic from the same DN. DL traffic Charging is to be performed after potential packet discard by across-session bitrate enforcement.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 266 of 501

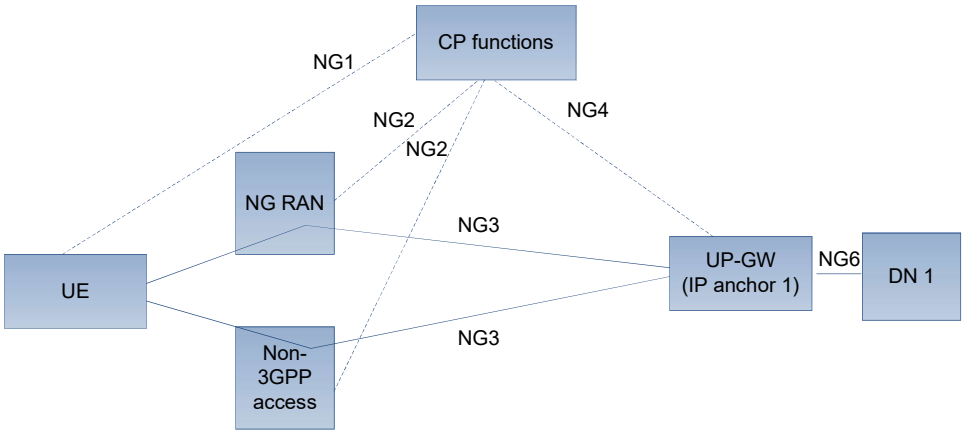


Figure 6.4.20.1-3: Multi-access PDU session to the same network

6.4.20.2 Function description

The multiple PDU session establishment procedure via different accesses are depicted in Figure 6.4.20.2-1 (for non-roaming case).

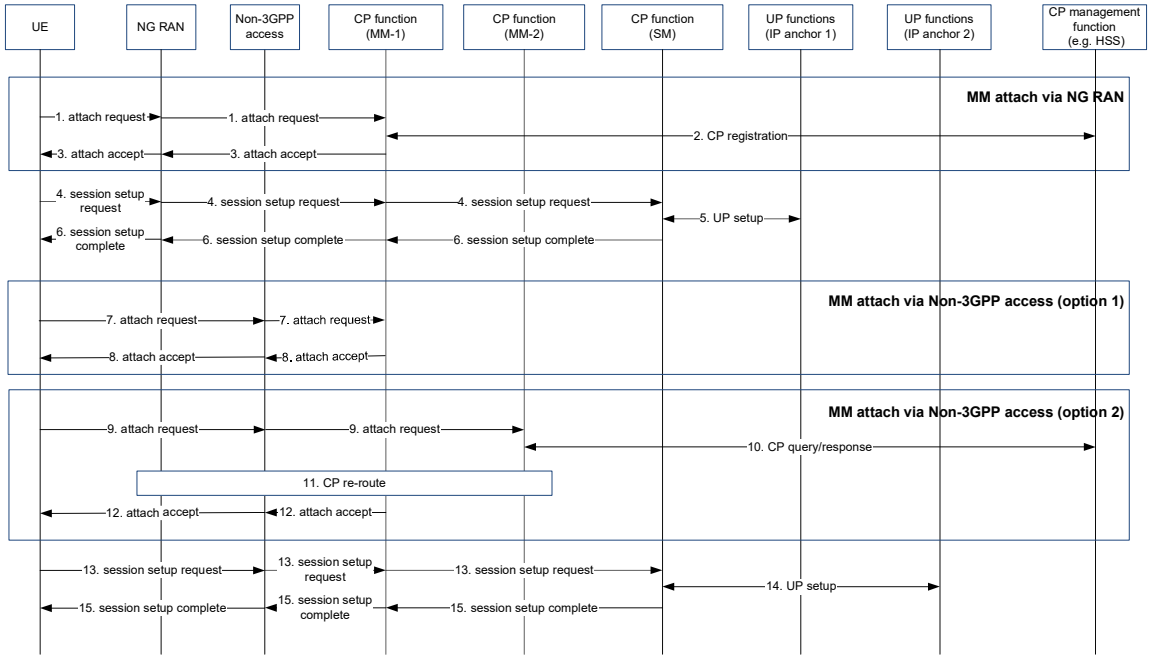


Figure 6.4.20.2-1: Multi-access PDU session setup procedure

NOTE: For the simplification, some network functions like the policy function are not showed in the procedure.

Editor's note: Further details regarding UE IP address/prefix assignment is FFS.

1. A UE initiates an attach request via NG RAN. The details depends on the solutions related to MM.
2. Before sending attach accept to the UE, the CP function may register the serving CP function to the CP management function (e.g. HSS or User Data).
3. The CP function sends attach accept to the UE via NG RAN. The information identifying the current serving CP function may be included in attach accept message.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 267 of 501

4. A UE initiates a session setup request via NG RAN. The CP function terminating NG1 is the serving CP function decided by MM attach procedure (e.g. MM-1 in the figure 6.4.20.2-1). The MM CP function forwards the session setup request to the proper the SM CP function (e,g, decided based on the requested DN Name).
5. The SM CP function selects the proper user plane function and triggers the establishment of user-plane.
6. The establishment of user-plane is completed.
7. The UE initiates an attach request via Non-3GPP access network. In case, the indication on additional attach may be included in the attach request message. If the UE gets the information identifying the serving CP function in the step 3, the UE sends it to the non-3GPP access using Non-3GPP access specific mechanisms together with attach request. Non-3GPP access network determines this information, then directs the UE to the same CP function. Further details depends on the solutions related to MM.
8. The CP function terminating NG1 may be confirmed.
9. The UE initiates an attach request via Non-3GPP access network. The indication on additional attach may be included in the attach request message.
10. If the CP function receives the attach request without the current serving CP related information from the UE, the CP function may perform the query about it to the CP management function. This query may be done together during the authentication procedure.
11. If needed, the CP re-allocation procedure is performed.
12. The CP function terminating NG1 may be confirmed.
13. A UE initiates a session setup request via Non-3GPP access network. The CP function terminating NG1 is the serving CP function decided by MM attach procedure (e.g. MM-1 in the figure 6.4.20.2-1). The MM CP function forwards the session setup request to the proper the proper SM CP function (e,g, decided based on the requested DN Name). It may be different to SM CP function decided in step 4.
14. The SM CP function selects the proper user plane function and triggers the establishment of user-plane.
15. The establishment of user-plane is completed.

6.4.20.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.21 Solution 4.21: NG3 interface related procedures

6.4.21.1 Architecture description

In group B based network slicing architecture, the common control network function (CCNF) terminating the NG1 interface is shared between different slices, the SM function is distributed into the isolated slices. The network architecture is shown in Figure 6.4.21.1-1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 268 of 501

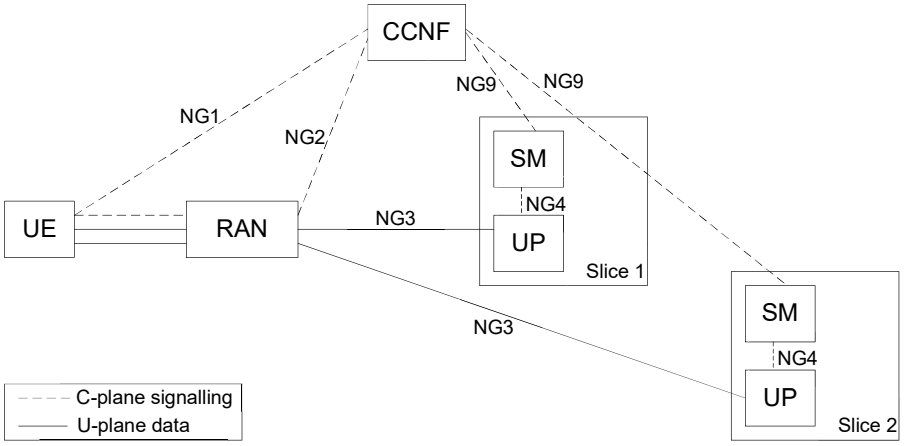


Figure 6.4.21.1-1: Network architecture

In this solution, the states of the PDU sessions of the UE are isolated. E.g. the setup and release of the NG3 connection and radio connection of a PDU session will not impact other PDU sessions of the same UE. Based on this assumption, the procedures related to NG3 interface are described.

6.4.21.2 Function description

6.4.21.2.1 NG3 Disconnection

This procedure is used by the RAN to release the NG3 connection and radio connection of a PDU session when e.g. the inactivity of the PDU session is detected.

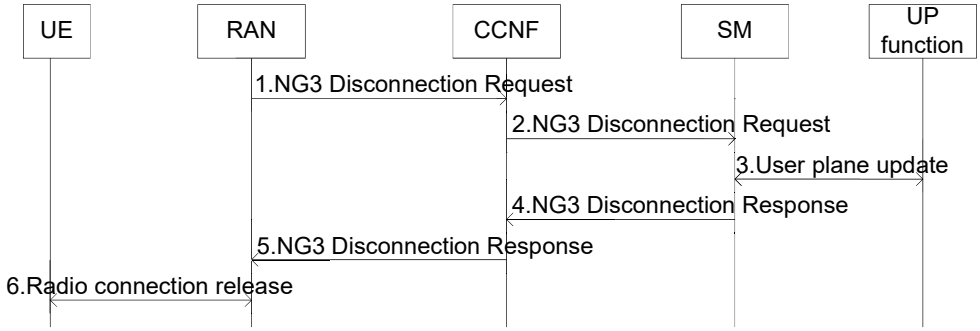


Figure 6.4.21.2.1-1: NG3 Disconnection procedure

1. RAN decides to release the NG3 connection and radio connection of a PDU session, it sends the NG3 Disconnection Request message to the CCNF.
2. The CCNF sends the NG3 Disconnection Request message to the SM.
3. The SM updates the user plane of the PDU session to delete the NG3 connection endpoint of the RAN.
4. The SM sends the NG3 Disconnection Response message to the CCNF.
5. The CCNF sends the NG3 Disconnection Response message to the RAN.
6. The RAN releases the radio connection of the PDU session and deletes the information of the PDU session from the UE context.

6.4.21.2.2 Service Request

The procedure is initiated by the UE to establish the NG3 connection and radio connection of a PDU session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 269 of 501

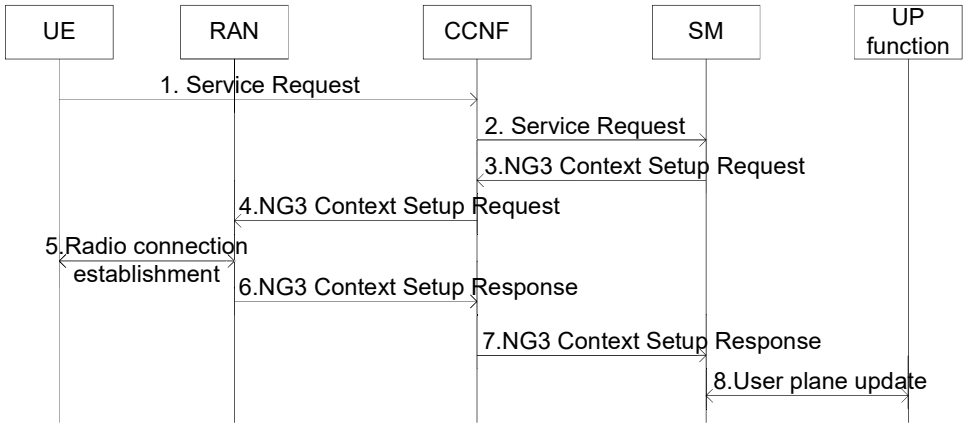


Figure 6.4.21.2.2-1: Service Request procedure

1. The UE sends the Service Request message to the CCNF. The message includes the information of the PDU session (e.g. identifier) that the UE wants to establish the NG3 connection and radio connection.

Editor's note: It's FFS how the identifier identifies a PDU session.

2. The CCNF sends the Service Request to the SM to request to activate the PDU session of the UE.
3. The SM sends the NG3 Context Setup Request to the CCNF to active the UP connection of the PDU session. The message includes the identifier of the PDU session, the NG3 connection endpoint of the UP function and the QoS of the PDU session.
4. The CCNF sends the NG3 Context Setup Request to the RAN.
5. The RAN establishes the radio connection for the PDU session.
6. The RAN allocates the NG3 connection endpoint for the PDU session and sends the NG3 Context Setup Response message to the CCNF. The message includes the NG3 connection endpoint of the RAN.
7. The CCNF sends the NG3 Context Setup Response to the SM.
8. The SM updates the user plane path of the PDU session. During the step, the SM notifies the NG3 connection endpoint of the RAN to the UP function.

6.4.21.2.3 Paging

When downlink data is received by UP function in a slice, if there is no NG3 connection endpoint of the RAN for the PDU session, the UP function sends the Downlink Data Notification to the SM to trigger the paging procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 270 of 501

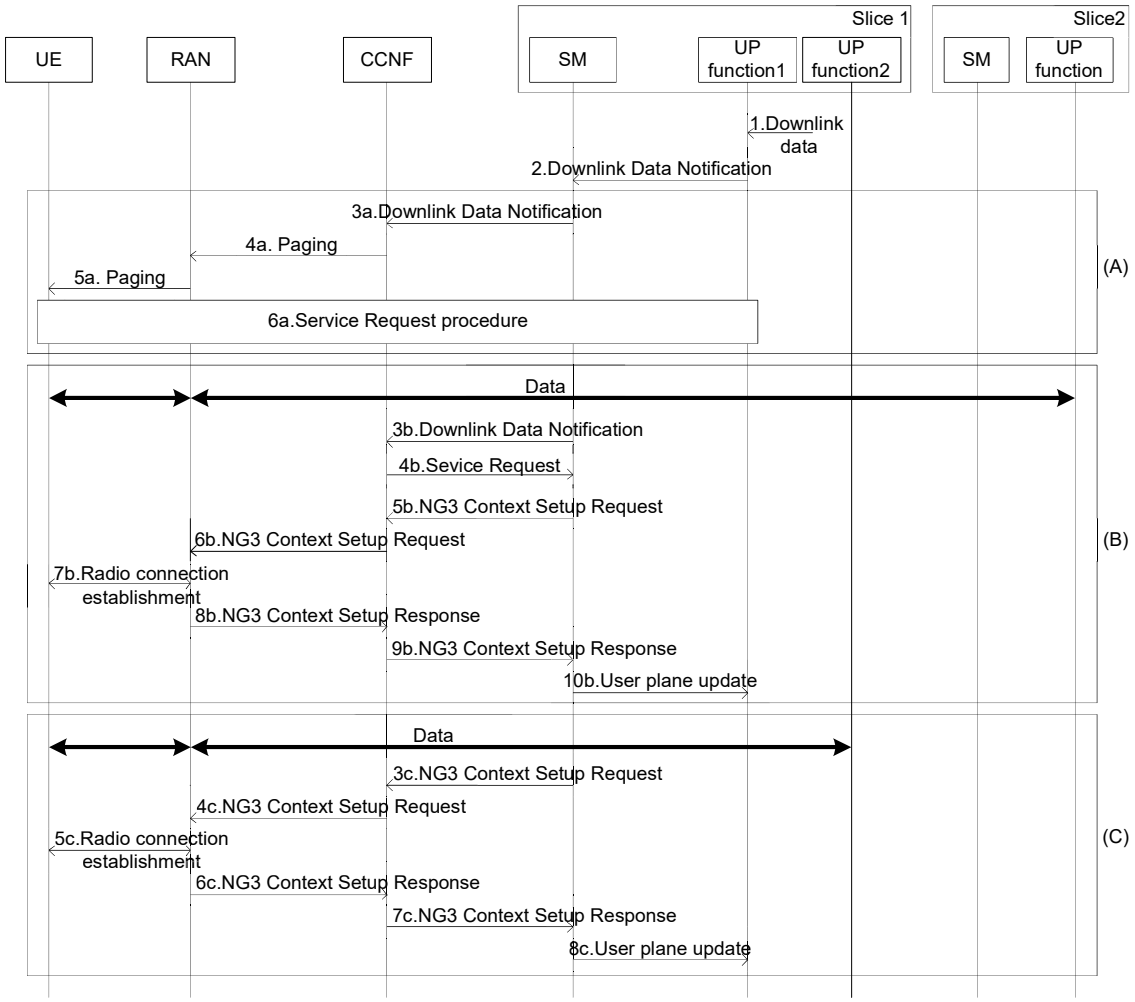


Figure 6.4.21.2.3-1: Paging procedure

1. The UP function receives a downlink data packet of a PDU session without NG3 connection endpoint of the RAN in the context of the PDU session , it buffers the downlink data packet.

2. The UP function sends a Downlink Data Notification (DDN) message to the SM.

After the step 2, based on the state of the NG3 connections (i.e. released or not) of the PDU sessions established by the UE, different step is performed. When the DDN message is received, if the SM finds RAN information of at least one PDU session of the UE, it initiates the NG3 connection establishment for the PDU session with downlink data pending, i.e. the step (C) is performed. Otherwise it sends the DDN message to the CCNF. When the message is received by the CCNF, if CCNF determines the UE is in IDLE mode, it pages the UE, i.e. the step (A) is performed. Otherwise the step (B) is performed. Step (A) includes the following steps:

3a. The SM sends the Downlink Data Notification message to the CCNF. The message includes the identifier of the PDU session which has downlink data pending.

4a. The CCNF sends the Paging message to the RAN. The Paging message includes the identifier of the PDU session which has downlink data pending.

5a. RAN pages the UE.

6a. The UE initiates the Service Request procedure. The Service Request message includes the identifier in the Paging message.

Step (B) includes the following steps:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 271 of 501

3b. The SM sends the Downlink Data Notification to the CCNF. The message includes the identifier of the PDU session having downlink data pending.

4b. If CCNF determines the UE has PDU sessions with NG3 connection setup in other slices, the CCNF knows the UE is connected to RAN. The CCNF sends the Service Request to request to activate UP connection, which including the current UE location.

5b. The SM sends the NG3 Context Setup Request to the CCNF to activate the UP connection of the PDU session. The message includes the identifier of the PDU session having downlink data pending, the NG3 connection endpoint of the UP function and the QoS of the PDU session.

6b. The CCNF sends the NG3 Context Setup Request to the RAN.

7b. The RAN performs the radio connection establishment procedure.

8b. The RAN sends the NG3 Context Setup Response to the CCNF. The message includes the NG3 connection endpoint of the RAN.

9b. The CCNF sends the NG3 Context Setup Response to the SM.

10b. The SM updates the user plane of the PDU session to notify the UP function the NG3 connection endpoint of the RAN.

Step (C) includes the following steps:

3c - 8c. Same as steps 5b – 10b.

6.4.21.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.4.22 Solution 4.22: Session management per PDU session

6.4.22.1 Architecture Description

This solution applies to key issue 4 on session management and key issue 5 on efficient user plane paths. The solution addresses the following work tasks:

- KI#4: SM_WT#1 (SM model);
- KI#4: SM_WT#2 (relation between SM and MM);

The proposed solution is based on the following principles:

- The session management function (SMF) and mobility management function (MMF) are split in different network functions. In the particular case of UE registered with multiple network slice instances, the UE would be served by multiple SMFs, i.e. multiple PDU session are established.
- The session management function (SMF) and mobility management function (MMF) are split in different network functions. In the particular case of UE registered with multiple network slice instances, the UE would be served by multiple SMFs, i.e. multiple PDU session are established.
- Multiple PDU sessions (to the same or to different network slices) are established for a given UE. A PDU session can be in Idle state or Active state.
- A UP connection (including data radio connection and NG3 tunnel establishing) can be activated for a single PDU session. UP connections for other PDU sessions (to the same or to other network slices) can be activated/deactivated independently.
- The procedures for PDU session activation and deactivation are proposed, meaning:
  - PDU session activation is the transition to "Active" session state in the SMF and the UP connection is established;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 272 of 501

- PDU session deactivation is the transition to "Idle" session state in SMF and the UP connection is released/deactivated.

- Similar to the existing SM in GPRS and EPS, this solution does not preclude to perform SM (i.e. Active/Idle transition management) for all existing PDU sessions together. Whether to perform activation of all PDU sessions or activation of individual PDU session can be based on subscription and UE capability.

NOTE: A PDU session establishment procedure is the initial establishment of a PDU session where UE context is installed in the corresponding SMFs and UPFs. The PDU session activation procedure is the activation/establishment of UP connection (e.g. radio data connection and NG3 tunnel).

The reference architecture is shown in the following figure. The common control plane network functions (CCNF) may include mobility management function or AAA functions as described in solution 1.2. The dedicated control plane network functions (Ded. CP NF) may include the session management function (SMF) and optionally the policy control function (PCF).

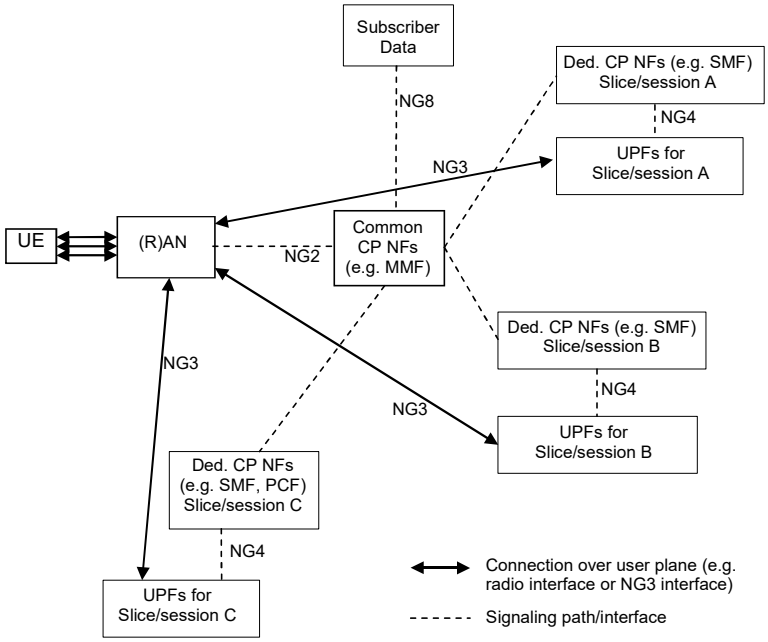


Figure 6.4.22.1-1: Reference Architecture with 3 PDU sessions to different network slices with independent session management functions (SMF)

6.4.22.2 Function description

Figure6.4.22.2-1 shows independent session state machines per existing session (i.e. per network slice, or PDU session). The session (SM) state machine can be maintained in the SMF as part of the UE's SM context in the SMF. The SM state machine is also maintained in the MMF.

The CCNF (e.g. MMF) knows the session state (Idle or Active) in SMFs for all the established PDU sessions. With this, in addition to the mobility (MM) context, the MMF maintains also state information for all established PDU sessions.

For example, if a PDU session is deactivated (i.e. the UP connection is released but context is kept in UE, SMF/UPF) the MMF knows that the corresponding SMF should not be updated when the UE moves and changes RAN node. In contrary, if a PDU session is activated, the MMF knows that the corresponding SMF should be updated with the new (R)AN node details (e.g. IP address, tunnel identifier, transport port ID, or other parameters) each time when a (R)AN node changes due to UE mobility.

NOTE 1: The details about the MM states are in the scope of KI#2 Mobility Management, and thus, can be different from the MM states shown in Figure 6.4.22.2-1

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 273 of 501

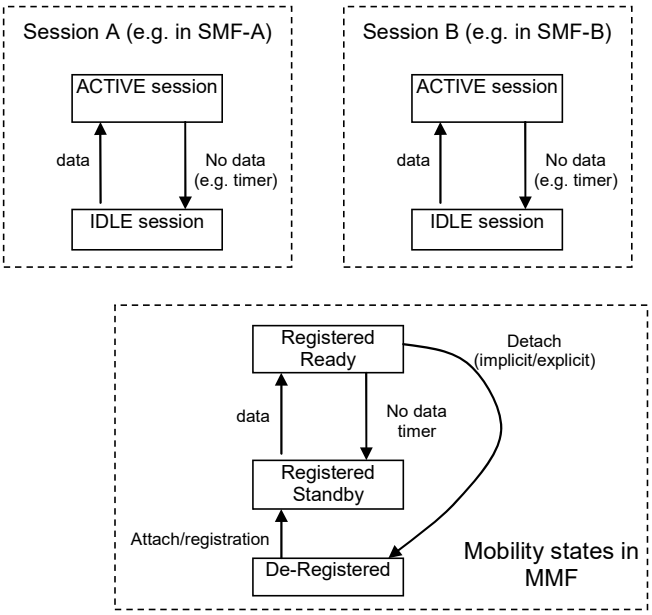


Figure 6.4.22.2-1: Multiple session state machines (one per established session) and a single mobility state machine

Figure 6.4.22.2-2 shows an example of the signalling flow for session activation triggered by DL data arrival which is independent from other PDU sessions.

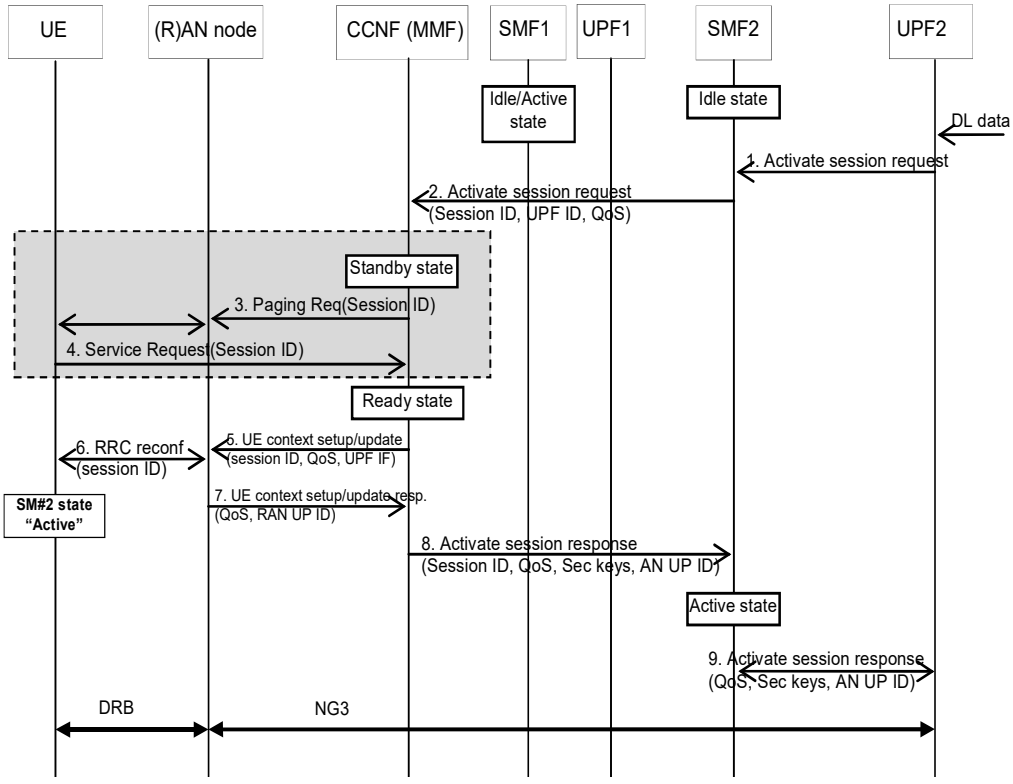


Figure 6.4.22.2-2: Signalling flow for session activation in MT case

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 274 of 501

The steps for session activation due to DL data transmission are described as follows:

1. The UPF2 initiates Activate session request procedure for the establishment of UP connection.

2. The SMF2 initiates Activate session request procedure towards the CCNF (e.g. MMF). SMF2 includes session ID, QoS parameters, paging priority and UPF ID (needed for NG3 tunnel establishment, e.g. IP address, tunnelling endpoint ID and/or transport layer port ID). If the CCSF has another Activate session request procedure in progress with other SMF (e.g. SMF1) and the Activate session request message from the SMF2 has equal or less paging priority than the one in progress., the CCSF does not initiates new paging procedure to the UE.

3-4. If the MMF is in Standby state, the MMF initiates the paging procedure to the UE. The Paging message includes the session ID that corresponding to the DL packets arrived to the UPF2. If the MMF is in Ready state i.e. there is an active session on going with UPF1, the CCNF sends service notification message to the UE over the NG1 interface instead of performing paging procedure.

4. UE sends the Service Request message to the CCNF. The Service Request message includes the session ID if it was present in step 3.

5-7. The CCNF (e.g. MMF) performs UE context setup procedure towards the RAN node. The SM state in the UE for this PDU session changes to "Active" and the UE is able to receive/send data.

8. MMF responds to step 2 towards SMF2 including the RAN node UP information for NG3 tunnel establishment. If the CCNF has Activate session request messages received from multiple SMFs, then multiple Activate session response messages are responded to corresponding SMFs.

9. SMF2 updates UPF2 with the information needed for NG3 tunnel establishment.

Figure 6.4.22.2-3 shows an example of the signalling flow for session activation triggered by UL data transmission which is independent from other activation of other PDU sessions.

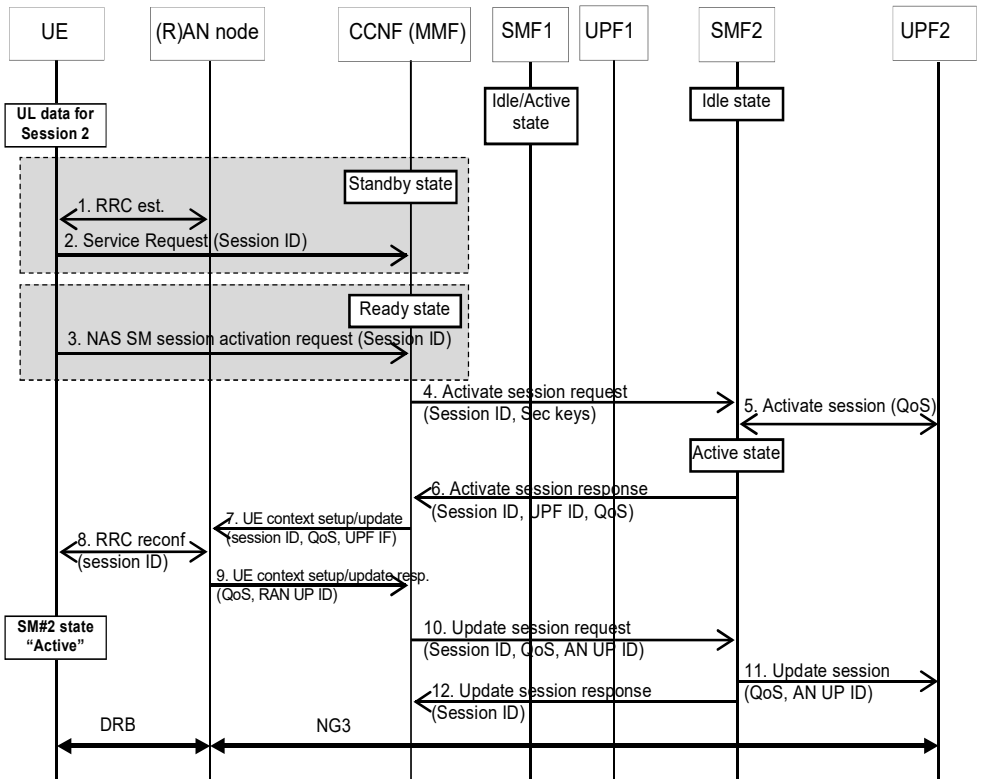


Figure 6.4.22.2-3: Signalling flow for session activation in MO case

The steps for session activation due to DL data transmission are described as follows:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 275 of 501

1. Due to UL data for PDU session 2, the UE initiates RRC connection establishment with RAN node to transmit an initial NAS message. If UE has active session (MM in Ready state), the UE skips this step and performs step 3.

2. If UE does not have any active sessions, UE sends the Service Request message to the CCNF. The Service Request message includes the session ID that UE wants to activate.

3. If UE has an active session (MM in Ready state), the UE sends NAS SM session activation message which includes the session ID that UE wants to activate.

4-6. The CCNF (e.g. MMF) performs Activate session procedure with the SMF2. SMF2 updates the UPF2, if needed, and replies to MMF with the corresponding stored QoS parameters and UPF ID.

7-9. The CCNF (e.g. MMF) performs UE context setup procedure to the RAN node. The SM state in the UE for this PDU session changes to "Active" and the UE is able to receive/send data for this PDU session.

10-12. MMF performs Update session procedure to towards the associated SMF2 to inform SMF2 and UPF2 about the RAN node UP information for NG3 tunnel establishment.

The procedure for session deactivation includes the release of the UP connection (data radio connection and NG3 connection/tunnel), whereas the UE's context in the SMF and the NAS SM context in the UE are kept, however the state is "Idle". The session deactivation procedure can be initiated by the RAN node.

6.4.22.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.23 Solution 4.23: Asynchronous Session Management Model

This is a solution to Key issue 4: Session Management.

6.4.23.1 Architecture description

This solution proposes an asynchronous session management model by using the session management model indication received from the Policy Function.

- Asynchronous Session Management: when the PF detects the PDU session need to be modified, firstly, it determines whether the modification could be updated in UE/AN later or immediately, then indicates to the CP the selected session management mode (i.e. Asynchronous session management or synchronized session management). If the CP receives PDU session management mode with asynchronization indication and the UE is in IDLE state, the CP marks the PDU session management request as pending state without paging UE. And the CP update the session context in the UE/AN after the UE enters CONNECTED state triggered by other conditions, e.g. location update procedure or service request procedure after some time later; Otherwise, when there is synchronization indication mode in the session management procedure and the UE is in the IDLE state, the CP initiates paging procedure and updates the session in the UE/AN immediately.

The asynchronous session management model can reduce the signalling overhead especially for the case when there is no data needed to be transmitted immediately after the signalling procedure or the network signalling load is serious with massive M2M/IoT devices.

6.4.23.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 276 of 501

6.4.23.2.1 Asynchronous session management procedure

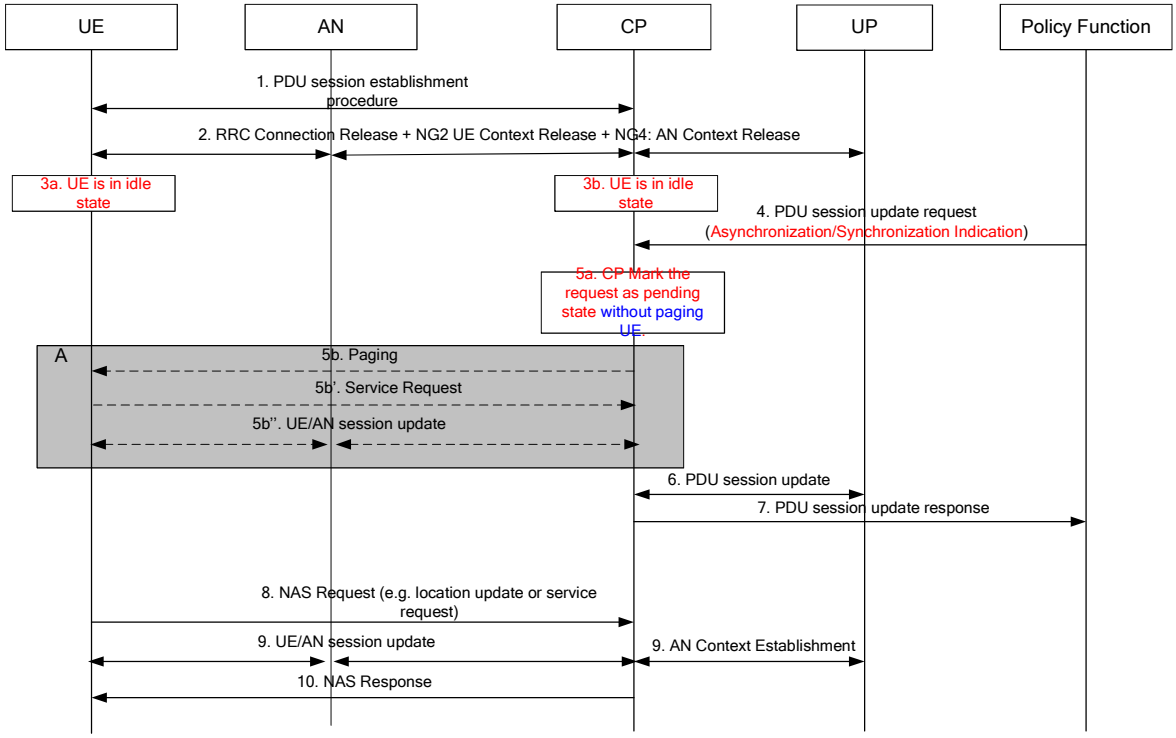


Figure 6.4.23.2.1-1 Asynchronous Session management procedure

1. The UE attaches to the network and a PDU session between the UE and the network is established.
2. When the AN/MME determines that the RRC connection should be release, AN/MME triggers the RRC context release, then the CP releases the NG2 UE context and the UP releases the AN context.
3. The UE enters IDLE state.
4. Policy Function (PF) detects the PDU session context is updated (e.g. new QoS is required due to a new service request or subscribed QoS is modified or an event is reported to PF) and it further determines the session management asynchronous/synchronized mode (e.g. use asynchronous mode if the network load is heavy or there no data need to be transferred in a short time). Then the PF sends PDU session update request with the asynchronization/synchronization indication.
5. The UE is in IDLE state, if the CP determines the session management mode is asynchronous mode based on the received asynchronization indication, the CP marks the PDU session update request as pending state without paging UE (i.e. step 5a). The updated PDU session context will not be sent to UE and/or AN immediately and step 6 and 7 are immediately performed. When the UE enters connected mode later based on the procedure step (8~10), the CP implements the session update in UE/AN.

   If the CP determines the session management is synchronized mode, the CP pages the UE and implements the session update in UE/AN immediately based on the procedure step (5b~5b") and step 8,9,10 are skipped after step 6 and 7 are performed.
6. The CP updates the PDU session context in the UP.
7. The CP sends a PDU session update response to the PF.
8. When the UE intends to enter CONNECTED state due to location update or service request or some other reason, the UE sends NAS request to CP.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 277 of 501

9. When the CP receives a NAS request from the UE and determines the session context is available in the UE, the CP triggers the session context update in UE and AN. When session update is completed in the UE and AN, the CP initiates the AN context establishment with UP.

10. The CP sends the NAS response to the UE.

6.4.23.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.4.24 Solution 4.24: Session Management with individual CP function per access network

This solution applies to key issue 4 on session management. Specifically, the solution addresses the following work tasks:

- SM_WT_#5: PDU session(s) via different accesses

6.4.24.1 Architecture description

This clause describes a session management architecture focusing on the following cases:

- Multiple PDU sessions via different accesses to the different data networks
- Multiple PDU sessions via different accesses to the same data network

The proposed solution assumes the following session management model principles:

- A UE can have multiple PDU sessions via simultaneous multiple accesses to the different data networks or same data networks (as showed in the figure 6.4.24.1-1 and figure 6.4.24.1-2)
- A UE can have multiple PDU sessions via NG RAN and non-3GPP access network
- The establishment and release for the PDU Session via NG RAN (NR or Evolved E-UTRA) is performed using NG1 signalling.
- The establishment and release for the PDU Session via non-3GPP access may be performed using NG1 signalling.
- The SM context of NextGen core network should keep the access network types for multiple PDU sessions.
- Individual MM CP function is operated per access networks, then the CP function terminating NG1 is different respectively.
- The SM message from a UE via NG1 is terminated to the serving MM CP function which is decided by MM attach procedure first. The MM CP function forwards the session setup request to the proper SM CP function (e,g. decided based on the requested DN Name)
- The details about MM aspects with individual CP function depends on the solutions related to MM.

Editor's note: The details on two MM CP functions when 3GPP access network and Non-3GPP access network belong to the same slice are FFS. It depends on the solutions related to Network Slicing.

- When a PDU session is transferred from one access network to another access network, SM CP function is reallocated or not reallocated (e.g. based on the desired Data Network) while MM CP function is reallocated.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 278 of 501

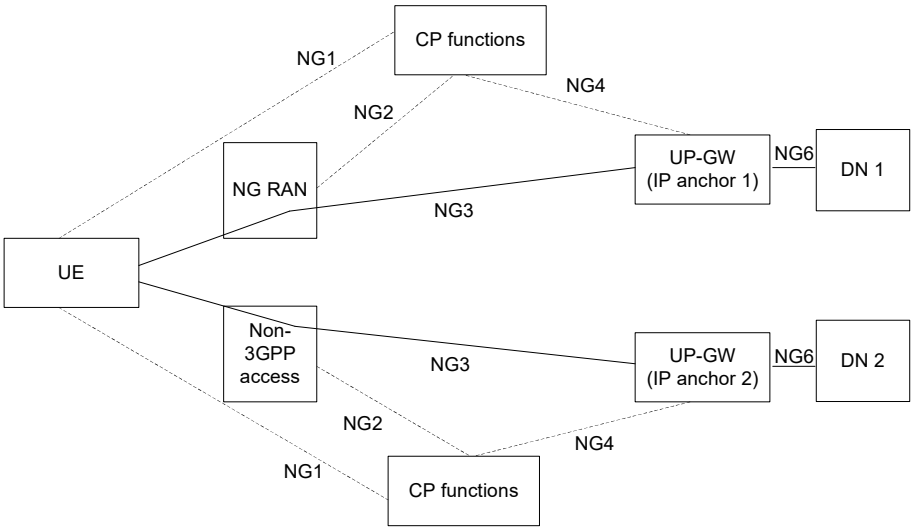


Figure 6.4.24.1-1: Multiple PDU sessions via different accesses to the different data networks

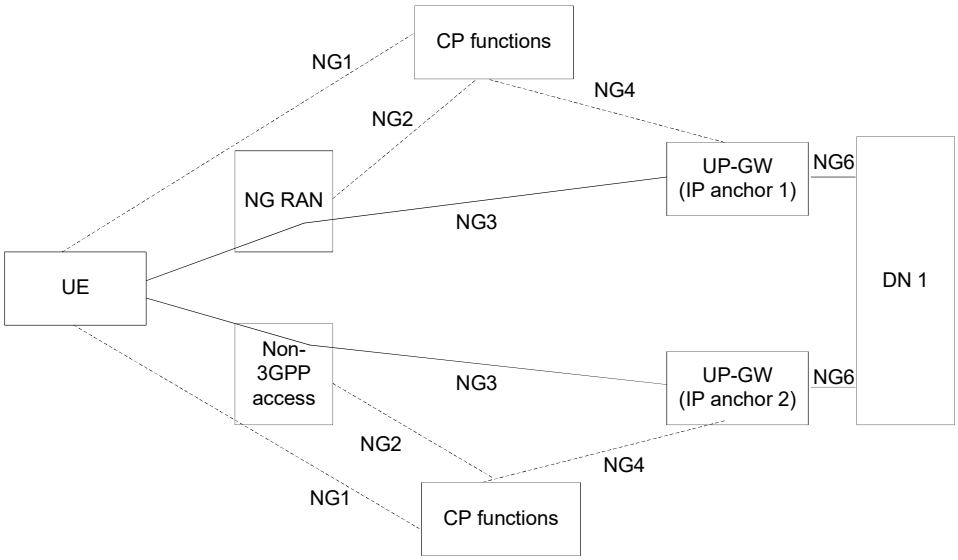


Figure 6.4.24.1-2: Multiple PDU sessions via different accesses to the same network

Editor's note: In case session bitrate limitation across all PDU sessions to the same data network is required (to be determined by the QoS key issue), then for UE with multiple PDU sessions towards the same DN there is the need of a Core Network User plane "convergence point" to support across session bitrate enforcement and charging. Across-session bitrate enforcement has to be run in a unique entity that handles all the DL traffic from the same DN. DL traffic Charging is to be performed after potential packet discard by across-session bitrate enforcement.

6.4.24.2 Function description

The multiple PDU session establishment procedure via different accesses are depicted in Figure 6.4.24.2-1 (for non-roaming case).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 279 of 501

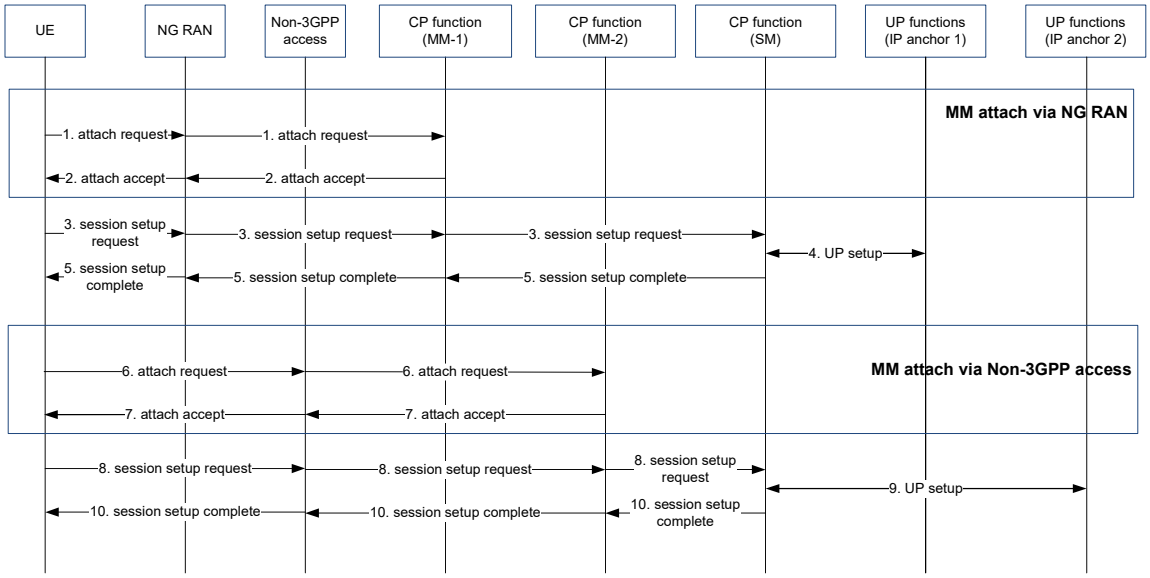


Figure 6.4.24.2-1: Multi-access PDU session setup procedure

NOTE: For the simplification, some network functions like the policy function are not showed in the procedure.

Editor's note: Further details regarding UE IP address/prefix assignment is FFS.

1. A UE initiates an attach request via NG RAN. The details depends on the solutions related to MM.
2. The CP function sends attach accept to the UE via NG RAN.
3. A UE initiates a session setup request via NG RAN. The MM CP function forwards the session setup request to the proper SM CP function (e,g, decided based on the DN Name).
4. The SM CP function selects the proper user plane function and triggers the establishment of user-plane.
5. The establishment of user-plane is completed.
6. The UE initiates a attach request via Non-3GPP access network. The details depends on the solutions related to MM.
7. The CP function sends attach accept to the UE via Non-3GPP access network.
8. A UE initiates a session setup request via Non-3GPP access network. The MM CP function forwards the session setup request to the proper SM CP function (e,g, decided based on the DN Name). It may be different to SM CP function decided in step 3.

6.4.24.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.4.25 Solution 4.25: Local Area Data Network

6.4.25.1 Architecture description

This solution is based on the architecture described in the solution 4.1.

6.4.25.2 Function description

The network may indicate to the UE the availability of the Data Network and the allowed area of the Data Network.

Editor's note: it is FFS how the allowed area is defined

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 280 of 501

Editor's note: it is FFS whether network triggers PDU session establishment when the UE enters the allowed area.

If the UE receives the information of the available Data Network, the UE may initiate the PDU session establishment procedure when it is needed.

Editor's note: It is FFS how the network provides the information to the UE of the available DNs.

Once the UE and the network established the PDU session, the PDU session is maintained while the UE moves within the area. The established PDU session is disconnected or becomes invalid when UE leaves the area.

Editor's note: it is FFS whether and how the PDU session should be terminated when the UE leaves the area

Editor's note: it is FFS how to minimize signalling when the UE moves repeatedly between an area where the local area data network and one where the local area data network is not allowed.

6.4.25.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.5 Solutions for Key Issue 5: Enabling (re)selection of efficient user plane paths

6.5.1 Solution 5.1: UP Functions selection

This solution addresses the key issue 5 on Enabling (re)selection of efficient user plane paths, special related to Criteria for user plane path selection

6.5.1.1 Architecture description

The reference architecture for the UP selection is shown in Figure 6.4.2.1-1(non-roaming) and Figure 6.4.2.1-2(home-routed).

6.5.1.2 Function description

In the EPC network two types of UP function nodes are defined, i.e. SGW/PGW. Due to the introduction of the C/U separation, the UP network functions will be defined in Next Generation Network. Session Management procedures define when UP functions are selected.

For the UP function selection, it is proposed as the following:

- The UP Function is selected by a C-plane NF during the session establishment procedure.
- The UP function can be selected/reselected on per UE and per Session granularity basis.
- The UP Function is selected/reselected based on any combination of the following factors:
  - UE mobility profile, including:
    - UE mobility level.

Editor's note: mobility profiles other than UE mobility level are FFS.

  - UE location;
  - UE session continuity requirements (e.g. session continuity required, not required);

Editor's note: Session continuity requirements will be determined based on the conclusion of key issue 6.

  - UE session QoS requirements;
  - Load conditions of the candidate selected UP function;
  - UE session information, including:
    - Data network name (DNN).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 281 of 501

- PDU session type (e.g. Non-IP/IP).

- The UP Function can be dynamically reselected based on any combination of the following factors:
  - Mobility events. , i.e. handover or location update.
  - Change of UE mobility profile, including:
    - UE mobility level.
  - Load conditions of the UP function

6.5.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.5.2 Solution 5.2: Solution to support Session continuity to enable (re)selection of efficient user plane paths

The Solution applies to Key issue 5: Enabling (re)selection of efficient user plane paths, especially the following issues:

- Reselection of user-plane path between a UE attached to the mobile network and communication peers outside of the mobile network (e.g. Internet hosts) when the previous path becomes inefficient.
- Minimising impact to the user experience (e.g. minimisation of interruption time and loss of packets) when changing the anchoring point for some or all packet data connections of a UE.

The Solution applies to Key issue 6: Support for session and service continuity

- The types of sessions to be considered in the context of session continuity;
- The level of session continuity to be supported depending on e.g., the type of service such as broadband, group communications, mission critical communications, etc.;

Editor's note: This solution assumes support for IP services. Extending this for supporting non-IP (e.g. Ethernet) services is FFS.

6.5.2.1 Architecture description

This solution assumes that the Next Generation network user plane will include two functions.

- One UP function providing the following functionality: uplink classifier functionality (UL CL) that allows steering local traffic to local services and/or central UP function towards central services, i.e. the ability to apply filtering rules (e.g. to examine the destination IP address of IP packets sent by the UE) and determine how the packet should be routed. This is combined with connectivity to a local network packet routing, packet forwarding, traffic offloading to the local network as well as charging, LI and bitrate enforcement for locally offloaded traffic.
- Another UP function providing IP anchoring functionality.

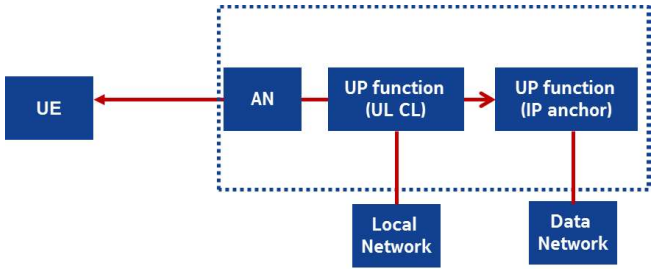


Figure 6.5.2.1-1 User plane Architecture for the solution

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 282 of 501

The operator uses configuration or policies to determine which flows are to be routed to/from the local network. Such configuration or policies are applied in the "UP function UL-CL" using uplink classification based on IP-5-tuple filtering rules. For downlink, the operator configures the network routing such that only legitimate traffic from the local server may pass via the UP function local IP point of presence.

Editor's note: Whether additional filtering rule types need to be supported is FFS.

The operator may use a dedicated IP address range for the set of UEs that need to be reachable locally. The local service network is configured such that this address range can be used for local downlink traffic.

In the case of mobility, session continuity is provided using some form of tunnelling, both for the central IP anchor point, and for the local IP point of presence.

A subscription record "Local Network Allowed", applicable in both non-roaming and roaming cases, is used to allow direct access to the local service network. In case of roaming, the visited operator is only allowed to use direct access to a local service network in case the home operator has explicitly allowed it.

Editor's note: Further detailing of the subscription data is FFS, e.g. whether more information is needed than a binary indication of "Local Network Allowed".

6.5.2.2 Function description

6.5.2.2.1 General

UE has access to centralized services (access to internet) via the IP anchoring UP function, distributed services (e.g. cached content of a CDN, content distribution network) via the UL-CL UP function that provides connectivity to the local network. The IP anchoring UP function providing access to the centralized services is assumed to be located in a more centralized location than the UL-CL UP function providing access to the distributed services. Note, that in this scenario only one host IP address that is centrally anchored has been assigned to the UE.

So, the UL-CL UP function with the local IP point of presence examines the IP packets (i.e. destination IP address) sent by the UE and decides whether to transmit the PDU within a tunnel to the central IP/PDU session anchor or it should be transmitted to the local application server (e.g. CDN) (e.g. within a tunnel).

NOTE 1: Details of the mechanism for transmitting PDUs from the UL-CL UP function to/from the local data network/local application server are beyond the scope of 3GPP.

Another option is that multiple IP addresses are assigned to the UE, one IP address for the local services and one IP address for the more central services.

In this case, i.e. when different IP addresses are assigned to the UE for local and central services rules configured into the UE determine whether the traffic is intended for the central IP anchor or the local IP anchor by choosing the appropriate source IP address.

For IPv6, RFC 4191 is used to configure rules into the UE to influence the selection of the source address. For IPv4 the same is achieved by means of RFC 3442. As an alternative for IPv4 (e.g. if DHCP is not supported), routing information is passed as a control-plane message to the UE.

Editor's note: The DHCPv4 option does not allow for subsequent updates of the routing information. Whether this limitation is an issue is FFS.

NOTE: Multiple IP addresses (e.g. one for the local anchor and one for the central anchor) could be assigned within one PDU session (a multi-homed PDU session) or via different PDU sessions. Whether only one or both approaches are supported will be concluded as part of key issue 4.

Following are the main characteristics of the single IP address variant of the solution:

- The possibility of having both a local IP point of presence (via the UL-CL UP function) and a central IP point of presence for a given session using the IP address allocated for by the central IP anchoring UP function. The local IP point of presence is applicable only for a well-defined set of traffic flows under operator control, while the central IP point of presence is used by default. The operator configures the local networks such that only the well-defined set of traffic flows can access the local IP point of presence.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 283 of 501

- An operator controlled uplink classification functionality within the UL-CL UP function determines which uplink flows to direct towards the local IP point of presence when local IP point of presence is applied by the operator.
- The network decides how the traffic is routed i.e. whether it is routed towards the local network or towards the more centrally located UP function and Data Network. Thus, the UE is not aware of the traffic redirection in this scenario.
- The core network control plane is responsible for the setup, configuration and release of the user plane functions mentioned above, based on operator policies, UE preferences and subscription information, on a per session basis.
- The CP verifies UE's permission for local network traffic offloading by obtaining "Local Network Allowed" data from user subscription repository. Then, the SM allocates UL-CL UP function and updates the UP path between AN and UP Function (IP anchor) accordingly. Also, the SM installs the filtering rules in the UL-CL UP function.

Editor's note: The main characteristics of the multiple IP address variant of the solution need to be added.

6.5.2.2.2 Mobility aspects

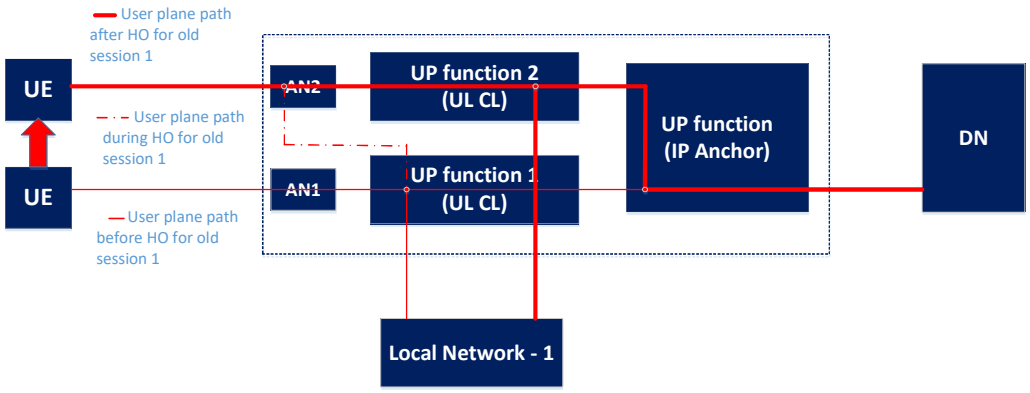


Figure 6.5.2.2-1: UL-CL UP function relocation for the same Local Network and existing PDU session.

When the UE is relocated from one UL-CL UP function 1 to UL-CL UP function 2, the existing session continues to be supported by the existing PDU session via the original local network-1 until termination. Session continuity is maintained from the UE's perspective for the PDU session as the central UP function acting as central IP anchor and the Local Network-1 remains the same when the UE is relocated from UL-CL UP function 1 to UL-CL UP function 2.

Following call flow illustrates UL CL UP function relocation:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 284 of 501

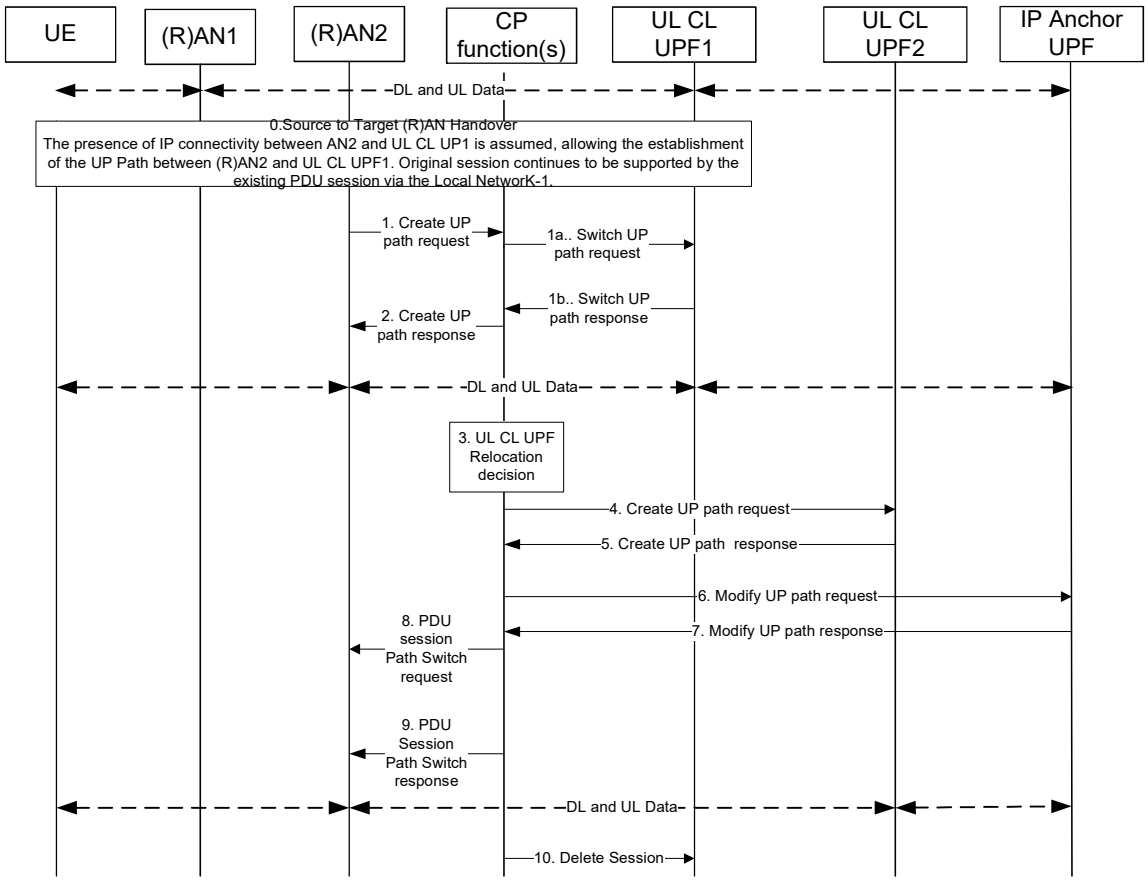


Figure 6.5.2.2-2: UL-CL UP function relocation call flow for the same Local Network and IP anchor.

0. Originally the User plane path for the UE is established from (R)AN1 to UL CL UPF1 to IP anchor UPF. The UE hands over from Source (R)AN1 to Target (R)AN2 The presence of IP connectivity between AN2 and UL CL UP1 is assumed, allowing the establishment of the UP Path between (R)AN2 and UL CL UPF1.

1. Upon completion of source to target HO at the AN, AN2 Request the establishment of a Path from the CP function(s) by sending a Create UP path request to CP function to establish a UP path for the UE towards UPF1 and includes the necessary information (e.g. tunnel ID) for DL traffic.

1.a CP function request the modification of the UP path by sending Create UP Path request. This triggers UL CL UPF1 to start DL transfer towards AN2

1.b UL CL UPF1 acknowledges the switching of the UP Path towards AN2 and provides necessary information for the establishment of the tunnel (e.g., tunnel ID) to AN2

2. The CP function acknowledges with create UP path response upon successful establishment of the Path.

3. CP Function(s) decides that the UL CL UPF should be relocated from UPF1 to UPF2.

4. CP function(s) sends create UP path request to UPF2 to establish a UP path for the UE and includes the necessary information (e.g. tunnel ID) for DL traffic

5. UPF2 acknowledges with create UP path response upon successful establishment.

6. CP Function(s) sends modify UP path request to IP anchor UPF to update the UP path for the UE.

7. IP anchor sends modify UP path response to IP anchor UPF to update the UP path for the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 285 of 501

8. CP Function(s) sends PDU Session Path Switch request to (R)AN2 to switch the path (i.e. from (R)AN2 – UPF1 to (R)AN2 – UPF2).

9. (R)AN2 sends a response to CCF once the path switch is complete.

10. CP Function(s)deletes the session in the original UPF1.

NOTE1: Since it is assumed that the details of the UP path from UL CL UPF1 to Local Network is out of scope for 3GPP, the call flow steps do not involve Local Network but it is assumed that the Local Network does not change, UP function relocation requires modification of the UP path towards Local Network to ensure DL traffic from Local Network is routed appropriately. It is also assumed that the IP address does not change.

Editor's note: Whether anything is needed from the 3GPP system e.g. transfer of transparent containers (with unspecified content) towards Local Network to support UPF relocation is FFS.

Alternatively, the UE's session towards the local network may be relocated from local network 1 to local network 2 in addition to UP function 1 relocation. Application session relocation may be necessary which is out of scope for 3GPP. This is shown in the figure below.

NOTE2: During this relocation, if the existing session moves from local network 1 to local network 2, then application context information or application instance may need to be transferred from Local network 1 to Local network 2 in such a way that there is no interruption for the application running in the UE. If this is not possible for a certain application session, then the existing session continues to be supported via Local network-1 until termination. Details of the application context relocation, including the handling of on-going TCP sessions, are out of scope of 3GPP.

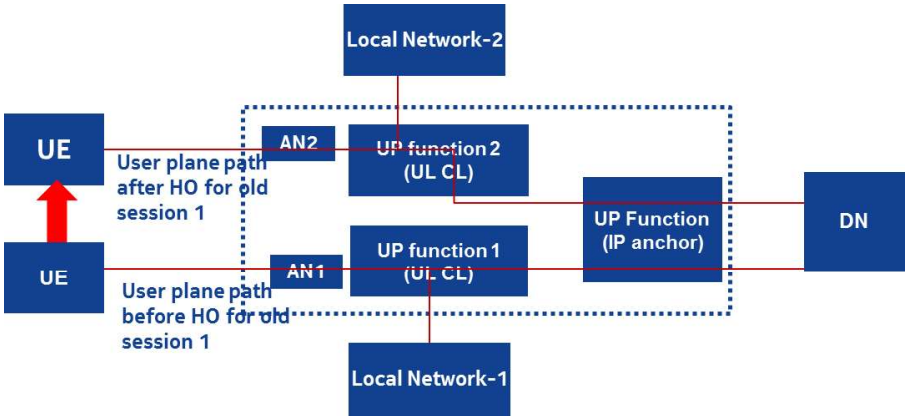


Figure 6.5.2.2-3: UL-CL UP function relocation along with relocation from Local Network 1 to Local Network 2

The IP anchoring UP function is maintained for the PDU session as the UE moves, i.e. session continuity is provided for the PDU session as the IP anchoring UP function remains the same. Thus, this solution applies also if the UP function is relocated.

6.5.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.5.3 Solution 5.3: Re-selection of user-plane path based on UE traffic pattern

6.5.3.1 Architecture Description

The solution proposed in this section is based on the architecture diagram in clause 6.2.2. Moreover, for the CN-CP function, the architectural split of mobility management and session management functions, denoted by CP-MM and CP-SM, is taken into account. The main concept of the solution is that core-network anchor (UP-GW) for the UE is

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 286 of 501

changed by CP-SM based on information provided by the user plane node in the core network. This information can be information about the destination IP addresses/servers that the UE is accessing.

Editor's note: Applicability to roaming scenario is FFS.

6.5.3.2 Function description

The high-level flow for this solution is provided in the figure below.

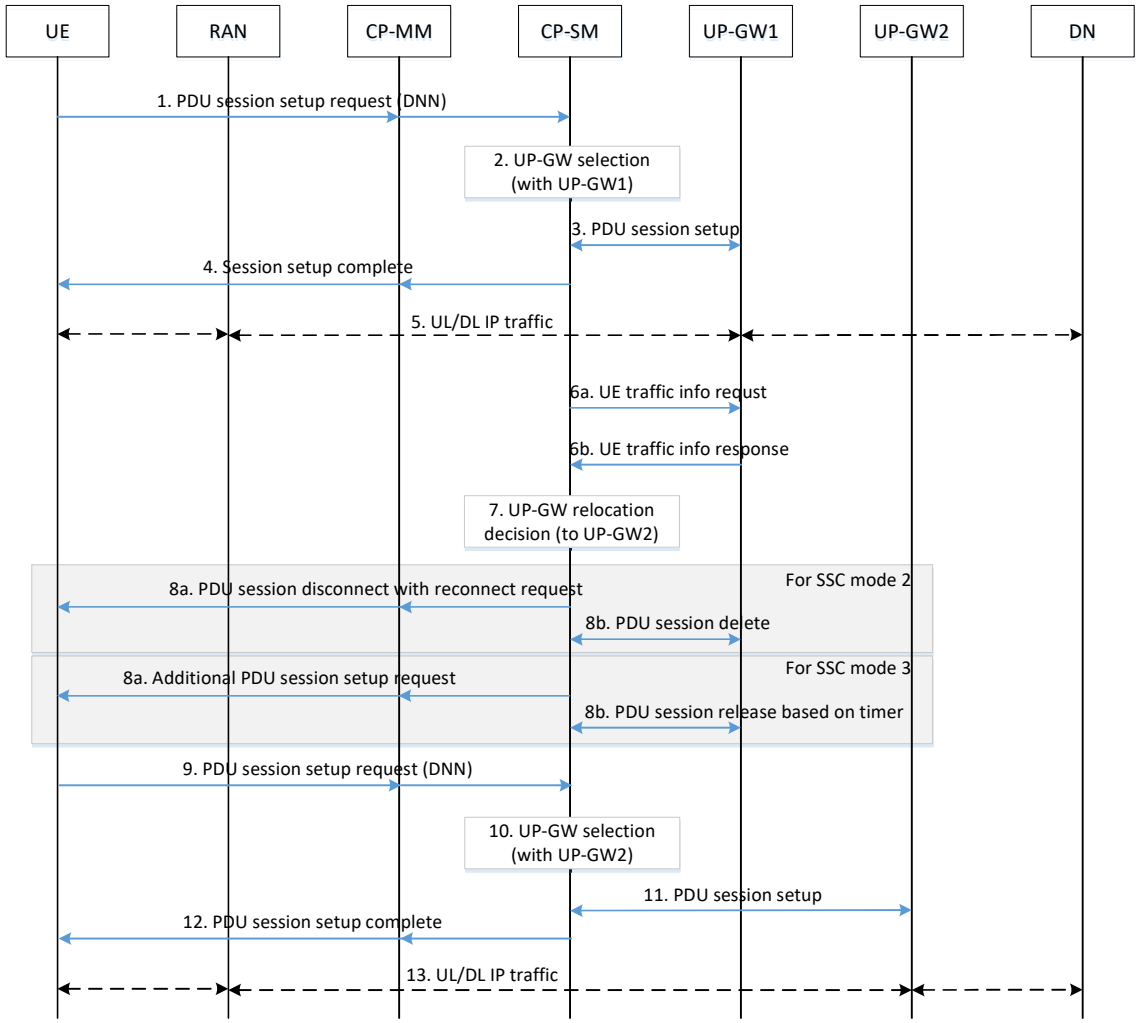


Figure 6.5.3.2-1: User-plane path reselection based on UE traffic information from UP-GW.

1. The UE sends a PDU Session Establishment Request (Data Network Name (DNN)) message to CP-SM.

Editor's note: It is FFS if DNN is different from APN

2. The CP-SM selects UP-GW1, based on information e.g. DNN, subscription information of the UE, current mobility information of the UE (if available).

3. The CP-SM provides forwarding rules to UP-GW1. The CP-SM subscribes to specific UE traffic events such as access to specific applications/servers, summaries of destination IP address, etc.

4. The CP-SM sends a PDU Session Establishment Accept message to the UE.

5. The UL and DL IP Traffic of the UE are via UP-GW1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 287 of 501

6. The CP-SM sends a UE traffic information request to the UP-GW1 either periodically or in an event-based way (6a). Then the UP-GW1 provides the requested information about the UE's traffic to the CP-SM(6b). This information can include for example, information about destinations/servers that the UE is accessing.

NOTE: The number of UE traffic information request to be sent from the CP-SM may depend on the load status of the CP-SM in order to prevent signalling congestion.

7. Based on the IP traffic information provided from the UP-GW1. e.g. UE is accessing content hosted closer to another anchor, and other information such as mobility pattern information of the UE and SSC mode of corresponding PDU session, the CP-SM decides to change the serving UP-GW for the UE such that the new UP-GW2 provides a more efficient user plane path for the UE.

8. The operation of CP-SM depends on the SSC mode of the PDU session.

   For SSC mode 2:

   The CP-SM triggers the relocation of the UP-GW by sending a PDU session disconnection request with "reconnect request" to the UE to connect again to the same DNN. The existing PDU session of the UE is torn down by CP-SM using PDU session delete procedure (8b). The CP-SM temporarily stores the information of the new UP-GW for the UE which is selected in step 7.

   For SSC mode 3:

   The CP-SM sends the additional PDU session setup trigger to the UE so that the UE can establish the additional PDU session to the same DN before the previous PDU session is terminated. The existing PDU session can be deleted using the timer established by CP-SM (8b). The CP-SM stores the information of the new UP-GW for the UE which is selected in step 7.

9. The UE sends PDU Session Establishment Request (DNN) to reconnect to the same DNN.

10. The CP-SM selects UP-GW 2, based on information stored in Step 8.

NOTE 1: If the network supports "make before break" for PDU sessions, this feature can be used to minimize disruption to existing IP connections, if needed.

NOTE 2: To minimize impact to user experience, the anchor reselection may occur when UE is idle or lull in UE traffic. But, it is noted that the procedure may incur unnecessary transitions from NG CM-idle to NG CM-connected state for the UE.

Editor's note: How this can be achieved if the SM changes during the disconnection/reconnection is FFS.

11. The CP-SM provides forwarding rules to UP-GW2. The CP-SM subscribes to specific UE traffic events such as access to specific applications/servers, summaries of destination IP address, etc.

12. The CP-SM sends a PDU Session Establishment Accept message to the UE.

13. The UL and DL IP Traffic of the UE are now via UP-GW2.

6.5.3.3 Solution Evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.5.4 Solution 5.4: Multiple Tunnel based traffic offload

6.5.4.1 Architecture Description

The solution proposed in this section is based on the architecture diagram in Annex G. The main concept is to offload traffic to an operator's local network based on the creation of secondary tunnel that is anchored at the UP close to the local network. The UE is provided with a UL TFT of the traffic to be offloaded onto the secondary tunnel. The UE then puts this traffic on the newly created secondary tunnel. The solution is depicted at a high level in the figure below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 288 of 501

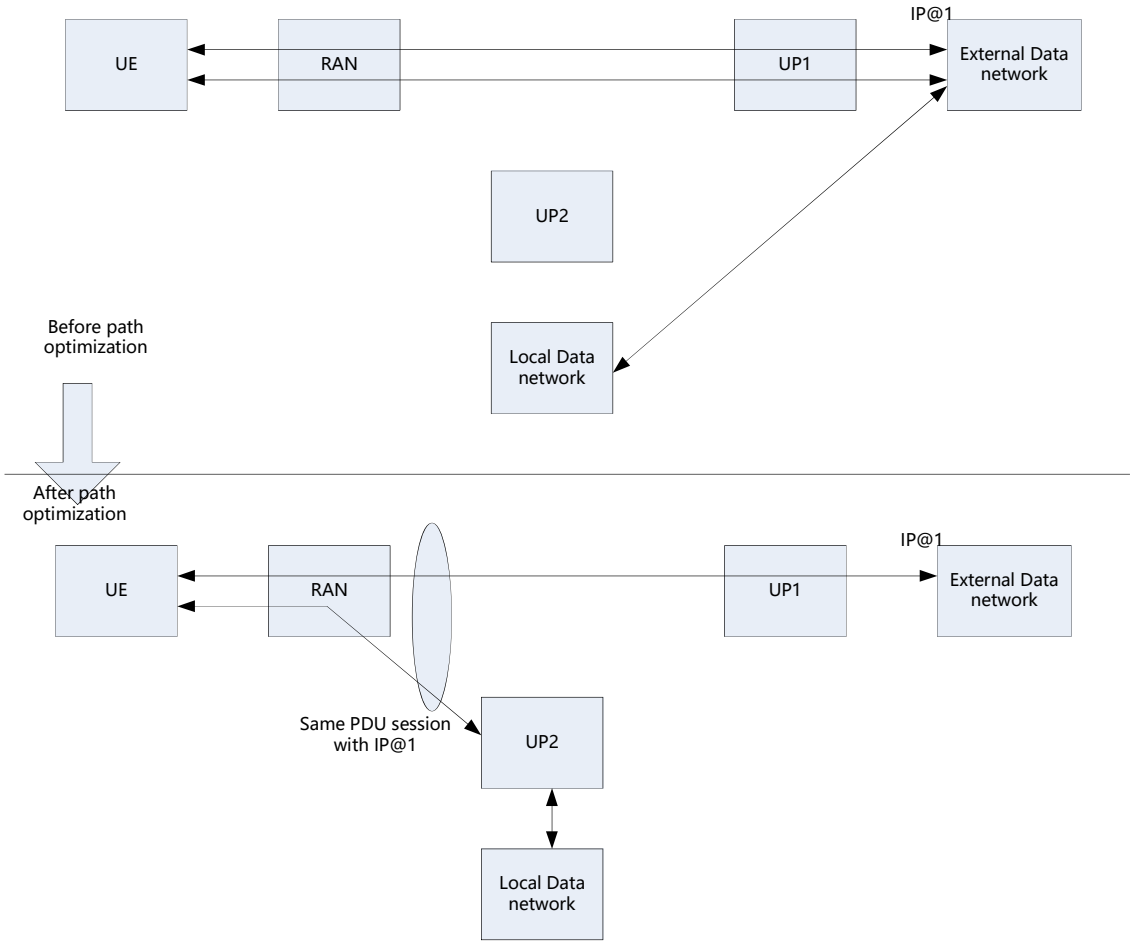


Figure 6.5.4.1-1: Tunnel based traffic offload

In this solution, before path optimization both the flows are in the primary tunnel. An IP address is allocated to the UE. Based on information from the user plane anchor about the destination IP addresses used by the UE, the CP may initiate the creation of a secondary tunnel which will be offloaded at a new user-plane node UP-2. The RAN node is also provided with rules to route the secondary tunnel to UP-2. The UE uses the UL TFT to put packets into the secondary tunnel. This carries the traffic to and from the local network. This traffic is served in the local network itself, i.e. does not leave the operator's local network. The user-plane node 2 performs charging, LI and session bitrate enforcement for locally offloaded traffic.

Editor's note: How this solution works for traffic which is not first routed to central anchor is FFS.

Editor's note: How APN AMBR is enforced is FFS.

Any user traffic not directed to the local network (eg. DNS lookups) are carried on the primary tunnel, e.g. due to matching the *.* filter.

This solution only works for "deducible" IP flows, i.e when a valid TFT can be created and provided to UE to offload the UE's traffic.

Packets may be re-ordered during the path switch of flows between the primary tunnel and secondary tunnel.

6.5.4.2 Function description

The high-level flow for this solution is provided in the figure below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 289 of 501

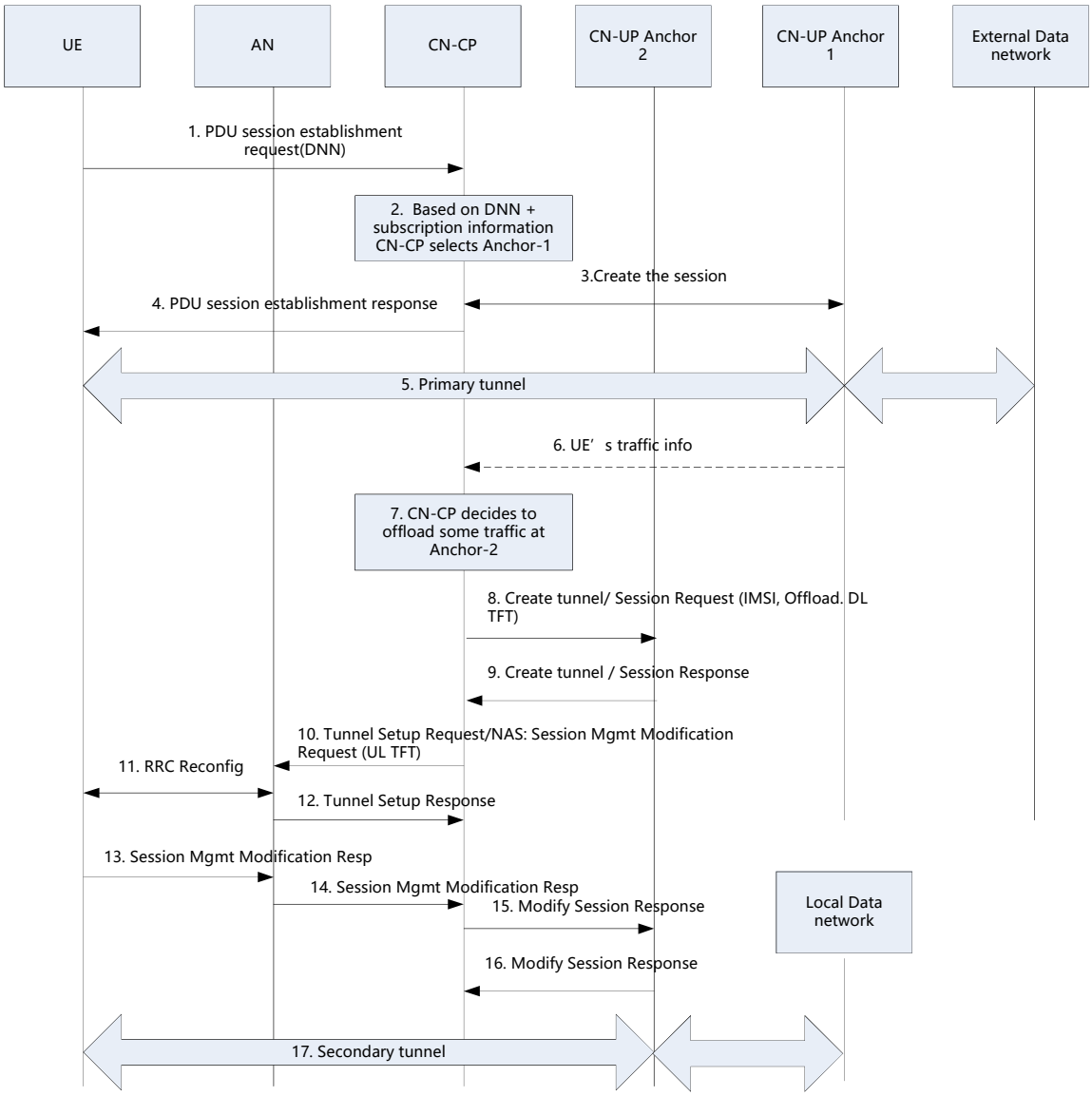


Figure 6.5.4.2-1: User-plane path reselection based on multiple tunnels

1. The UE sends a PDU Session Establishment Request (Data Network Name (DNN)) message to CN-CP.
2. The CN-CP selects CN-U Anchor-1, based on information e.g. DNN, subscription information of the UE, current mobility information of the UE (if available).
3. The CN-CP provides forwarding rules to CN-U Anchor 1. The CN-CP subscribes to specific UE traffic events such as access to specific applications/servers, summaries of destination IP address, etc.
4. The CN-CP sends a PDU Session Establishment Accept message to the UE.
5. The UL and DL IP Traffic of the UE are via primary tunnel to CN-U Anchor 1.
6. The CN-U Anchor 1 may provide periodic/event-based information about the UE's traffic to CN-CP. This information can include for example, information about destinations/servers/the application information that the UE is accessing. The application information at least includes pairs of OSId and OSAppId which can uniquely identify the application in the UE and is determined by configured rules associating the traffic to a specific application (e.g. based on destination IP address). The signalling traffic between CN-U and CN-CP can be

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 290 of 501

limited by tailoring the event-based notification to be specific to IP addresses of servers in the operator's local network (e.g. for CDNs, DNS response for content hosted in operator's local network)

7. Based on the IP traffic information provided from the CN-U, e.g., UE is accessing content hosted closer to another anchor, and other information such as mobility pattern information of the UE, the CN-CP decides that a new tunnel should be created for the UE. Also that this tunnel should be anchored at CN-U Anchor 2.

8. If the CN-U Anchor 2 is already in the path of the primary tunnel of the UE, the CN-CP sends a Create session request (Offload flag, DL TFT). The Offload flag is an indication to the CN-U that the tunnel should be offloaded locally. Additional information for charging may also be included. The DL TFT indicates what DL traffic should be included on that tunnel. If the CN-U Anchor 2 is not in the path of the primary tunnel, the message sent by the CN-CP is Create Session Request (IMSI, Offload flag, DL TFT) instead.

9. The CN-U anchor 2 confirms the setup of the tunnel, including a tunnel information.

10. The CN-CP triggers the creation of a new tunnel by sending a Session Management Request (UL TFT) to the UE and tunnel setup request (CN-UP anchor 2 tunnel information) to the RAN. The UL traffic flow template (TFT) is associated with the new secondary tunnel and is an IP filter used by the UE to put UL traffic destined to the local network on the new secondary tunnel. The UL TFT may include the application information. The application information pair corresponding to the OSId of the UE is used for the UE to do the uplink traffic tunnel binding.

11. The AN performs RRC Reconfiguration with the UE to setup a new radio tunnel.

12. The AN sends a Tunnel Setup Response (Second tunnel information) message to the CN-CP.

13. The UE confirms the setup of the secondary tunnel by sending a session management response to the network.

14. The AN forwards the session management response message to the CN-CP.

15. The CN-CP sends modify session request message to CN-UP2, including the second tunnel information of eNodeB.

Editor's note: How the application information is reflected in the DL TFT is FFS.

The local server also now provides downlink traffic to the CN-U Anchor 2via NAT collocated with CN-U Anchor 2 or a tunnel between local server and CN-U Anchor 2.

16. The CN-UP2 responses the modify session response message to CN-CP.

17. The UL and DL IP Traffic of the UE destined to the local network is sent in the secondary tunnel via CN-U Anchor 2.

6.5.4.3 Solution Evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.5.5 Solution 5.5: Application-aware UP Path (Re)selection

6.5.5.1 Architecture description

This solution assumes the following architecture: UP path (re)selection is performed by Control Plane functions and an AS controller (a non-3GPP function) is in charge of AS (re)selection/(re)location. The interfaces marked by dashed lines are out of the scope of 3GPP.

NOTE 1: The AS controller is a function under the control of the operator and within the trusted domain, and is assumed to have a certain knowledge of the topology of the CN User plane with respect to the AS network.

NOTE 2: The focus of this solution is on the interaction necessary to enable an application aware (re)selection of user plane path. The behaviour of the AS controller and the actual relocation of the application or application context are outside the scope of 3GPP and can be defined by other SDOs.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 291 of 501

NOTE 3: The actual set of Control Plane functions involved in the procedure or interfacing the AS controller are defined by other KIs, and are collectively referred here as "the Control Plane".

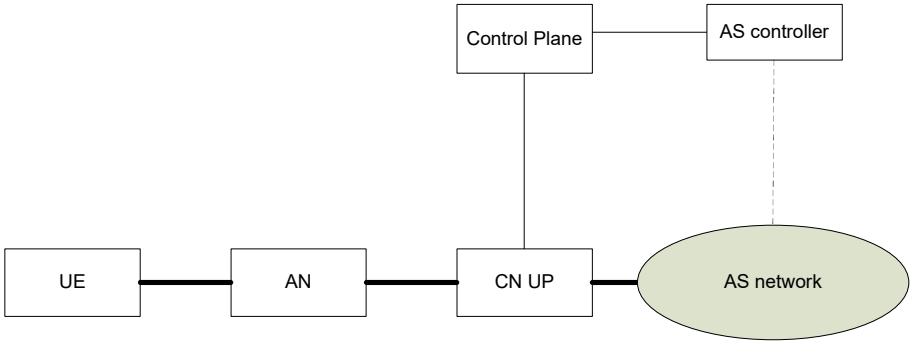


Figure 6.5.5.1-1: UP (re)selection architecture

6.5.5.2 Function description

The following flow diagram describes the procedure of enabling application-awareness to UP path (re)selection.

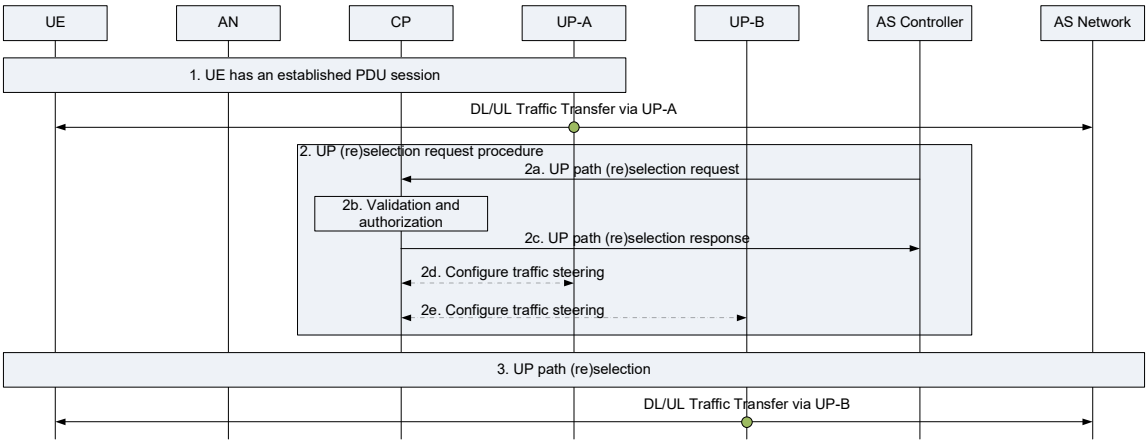


Figure 6.5.5.2-1: UP (re)selection according to AS Request

1. UE has an established PDU session with the application via UP_A and DL/UL traffic associated with the session has started to flow. This step is optional in the case of UP path selection.

2. A UE (re)selection request procedure takes place upon a request from AS controller

   2a. The Control Plane receives a UP path (re)selection Request for the PDU session associated with the application.

   - The request may include UE filter information that indicates the PDU sessions to which the requested UP path (re)selection is applied.

NOTE 4: The PDU sessions may be future sessions in the case of UP path selection or ongoing sessions in the case of UP path reselection.

NOTE 5: The procedure describes the case where a single UE is connected to the AS; however, an AS can serve a number of UEs simultaneously, which could result in the UP paths of PDU sessions of multiple UEs being reselected.

   - It may include a list of UP functions or AS locations suitable and/or unsuitable for selection, to be taken in account during UP path (re)selection. The UP functions and AS locations may be specified using network addresses such as IP address, MAC address, or other type of addresses.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 292 of 501

- In case of reselection, the request may include time periods indicating when the requested UP path reselection should be applied. The absence of such time periods indicates the requested UP path reselection should proceed immediately.

- The request may include an SSC indicator for the PDU sessions. The indicator indicates that the CP should configure traffic steering for maintaining the SSC; the absence of the indicator implies that the SSC will be handled by the AS network. If the SSC indicator is included and the AS controller did not provide an SSC mode for the PDU session, the SSC mode associated with the PDU session is determined according to clause 6.6.1.

Editor's note: Whether the AS controller communicates with Control Plane directly or via SCEF is FFS.

Editor's note: The actual information provided to communicate the list of UP functions suitable and/or unsuitable for selection is FFS.

2b. The Control plane performs validation and authorization for the UP path (re)selection request. Other security measure such as authentication can also be carried out at this step.

Editor's note: Which CP function should perform the validation/authorization is FFS.

2c. The Control Plane sends a response back to the AS controller, acknowledging the acceptance of the requested UP path (re)selection or its rejection.

2d. The CP generates traffic steering rules according to the UP (re)selection request and configures the rules into UP GW-A. This step is optional if this is an initial UP path selection request or if the UP path reselection request does not include an SSC indicator.

2e. The CP generates traffic steering rules according to the UP (re)selection request and configures the rules into UP GW-B. This step is optional if the UP path (re)selection request does not include an SSC indicator.

NOTE 6: This step allows traffic steering rules (e.g for UL traffic) to be configured at UP GW before session setup in the case of UP path selection. It is optional if traffic steering is configured dynamically in the Step 3 in Figure 6.5.5.2-2.

3. The Control Plane knows from the step 2(a) which PDU sessions are impacted and which UP functions or AS locations are suitable and/or unsuitable for use and (re)selects the UP for the PDU sessions accordingly. The control plane establishes PDU resources on the UP_B; in the case of UP reselection, it further updates the PDU session resource to change the PDU session path from the UP_A to UP_B.

The following diagram describes the procedures of UP change notification and traffic steering configuration. The two procedures are part of the UP path (re)selection procedure, which may be triggered either by the UP (re)selection request from the AS controller, as shown by the Step 3 in Figure 6.5.5.2-1, or due to internal factors such as UE mobility or load balancing.

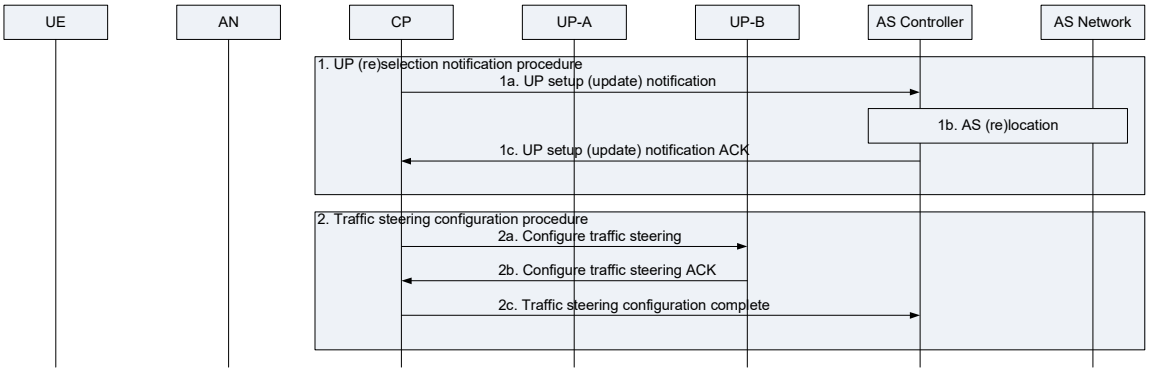


Figure 6.5.5.2-2: UP Change Notification and Traffic Steering Configuration

1. When the Control Plane determines the UP gateway during session setup or when the Control Plane determines the new UP gateway for the PDU session as a result of UP path reselection, the Control Plane initiates the UP (re)selection notification procedure for a PDU session associated to an AS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 293 of 501

1a. The CP notifies the UP setup or change of the PDU session associated to an AS to the AS controller.

1b. The AS controller performs the necessary steps for the AS (re)location or AS state (re)location procedure, which may include traffic steering configuration for SSC. The details of AS (re)location are out of 3GPP scope.

1c. The AS controller acknowledges to the Control Plane about the acceptance of the notification. The acknowledgement may further include an SSC indicator, implying that the CP should be configured by the CP for maintaining SSC. The absence of the indicator implies that the SSC has been handled by the AS network.

2. The CP initiates a traffic steering configuration procedure if an SSC indicator is detected in the step 1c.

2a. The Control Plane updates the UP to setup the routing of the traffic between the new UP and the new AS serving the UE.

2b. The CP receives traffic steering configuration acknowledgement indicating the successful update of traffic routing.

2c. The CP notifies the AS controller about the completion of traffic steering configuration so that they can start to use the new UP. The notification may trigger the AS controller to finalize AS relocation such as releasing resources and cleaning up data structures. The details of AS controller behavior are out of 3GPP scope.

NOTE 7: The step 2 is optional if traffic steering has been pre-configured before UP path (re)selection, in the UP path (re)selection request procedure.

6.5.5.2.1 Co-ordination the Session and Service Continuity with the Application-aware UP Path (Re)selection

The following diagram describes the procedure of Application-aware UP Path (Re)selection without IP anchor UP change. In this case, the PDU session is kept with the IP anchor User Plane, while the traffic towards to the AS network is offloaded via a local User plane (as specified in subclause 6.5.2.1).

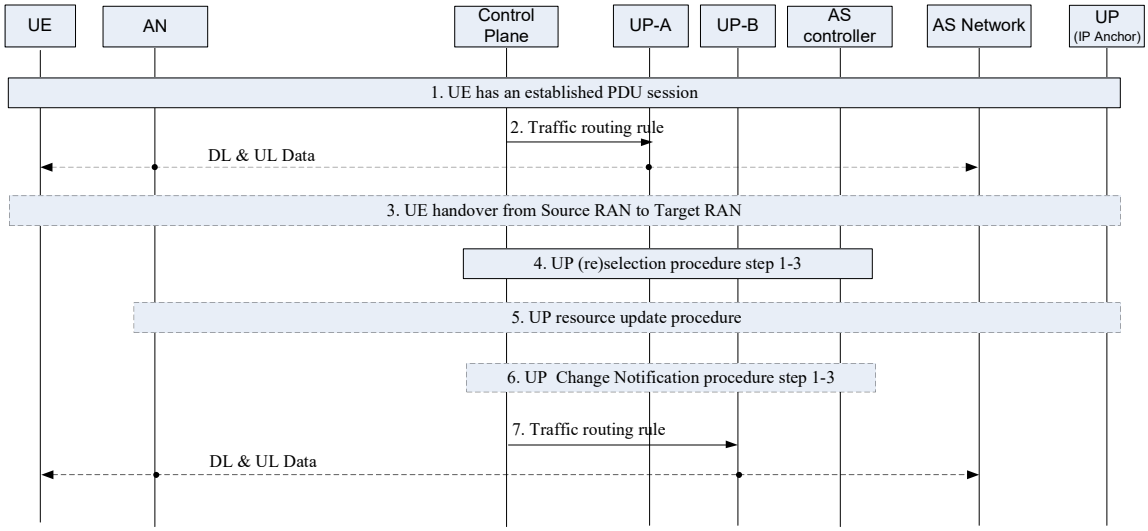


Figure 6.5.5.2.1-1: Local UP reselection for without IP anchor UP change

1. UE has an established PDU Session with the IP anchor UP. UP-A supports UL CL function on the path between the UE and the IP anchor, as specified in subclause 6.5.2.1.

2. The Control Plane sends the Traffic routing rule to the UP-A to offload the traffic to the AS network. The traffic routing rule includes the flow description.

3. UE performs handover from source RAN node to target RAN node. If the UP reselection is triggered by the AS controller internally, this step will not happen.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 294 of 501

4. The AS controller triggers the UP reselection procedure as specified in Figure 6.5.5.2-1. The AS controller may make the decision to trigger UP reselection according to the UE location change or AS load balance, of which the details is out of 3GPP scope.

5. If the UP reselection is triggered by the AS controller internally, e.g. load balancing, the CP may indicate UP to update related resource.

6. The CP may notifies the UP change event to the AS controller.

7. The Control Plane sends the Traffic routing rule to the UP-B to route the traffic to the AS network.

NOTE: Only traffic towards to the AS network is offloaded by the UP-A and UP-B. All other traffic, e.g. traffic towards to Internet, will still be routed to the IP anchor UP.

NOTE: If no available local UP, the CP will reject the UP reselection procedure.

The following diagram describes the procedure of Application-aware UP Path (Re)selection with IP anchor UP change. In this case, the traffic towards to the AS network is offloaded via IP anchor UP (SSC mode 1, 2, 3, as specified in subclause 6.6.1.1.3).

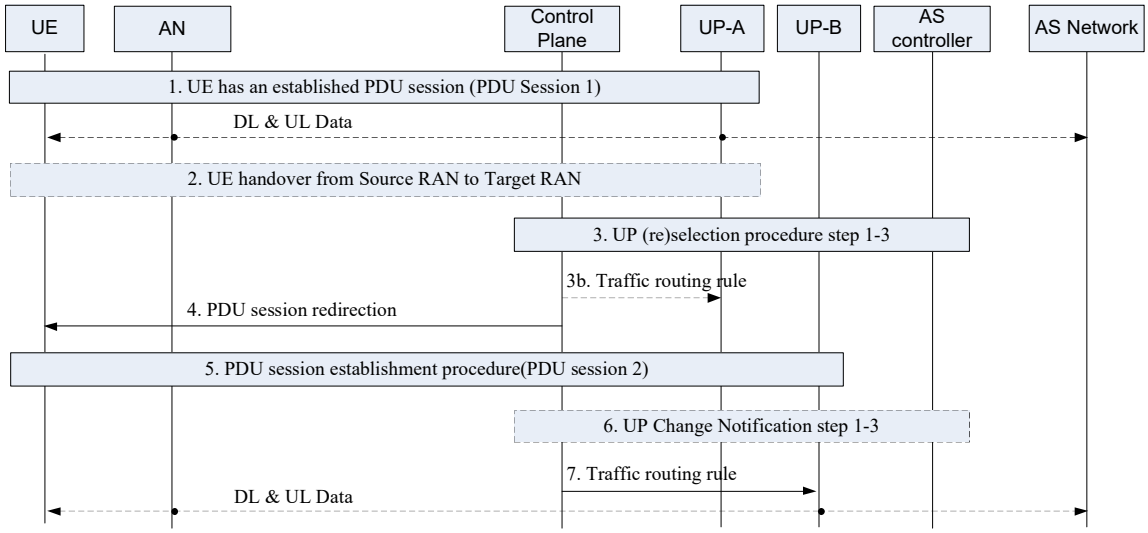


Figure 6.5.5.2.1-2: UP reselection with IP anchor UP change

1. UE has an established PDU Session 1 with UP-A.

2. UE performs handover from source RAN node to target RAN node. If the UP reselection is triggered by the AS controller internally, this step will not happen.

3. The AS controller triggers the UP reselection procedure as specified in Figure 6.5.5.2-1. The AS controller may make the decision to trigger UP reselection according to the UE location change or AS load balance, of which the details is out of 3GPP scope. For SSC mode 1, the CP rejects the relocation request, however traffic routing may be adjusted to route traffic towards the new AS location in step 3b; for SSC mode 2 and 3, the CP will accept the request.

4. The CP function sends a PDU Session Redirection message to the UE that triggers the UE to request a new PDU Session for the same data network if the SSC mode 2 & 3 is selected for the UE.

5. The UE establishes PDU session 2 with UP-B. In this step, the traffic routing rule is sent from the CP to the UP.

6. The Control Plane may trigger the UP Change Notification procedure as specified in Figure 6.5.5.2-2.

7. The Control Plane sends the Traffic routing rule to the UP-B to route the traffic to the AS network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 295 of 501

6.5.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.6 Solutions for Key Issue 6: Support for session and service continuity

6.6.1 Solution 6.1: Session and service continuity framework

This solution addresses WTs #1, #2, #3 and #5 of Key issue 6.

6.6.1.1 Architecture description

6.6.1.1.1 Overview

This solution provides a framework to support three distinct session and service continuity modes (SSC) in the NextGen system. The modes are defined in clause 6.6.1.1.1.3, the related solution principles are described in clause 6.6.1.1.1.4.

6.6.1.1.2 Assumptions

The solution assumes a PDU session to exist between a UE and a user-plane function (called terminating user-plane function (TUPF)). The TUPF terminates the 3GPP user plane and interfaces with the data network.

It is not precluded that the TUPF can also be co-located with the access network, e.g. to enable stationary UE scenarios.

Editor's note: These assumptions and definition above need to be revisited once they key issue on session management has progressed and common terminology for the user-plane functions has been agreed.

6.6.1.1.3 Session and service continuity modes

The NextGen system shall support the following session and service continuity (SSC) modes:

- **SSC mode 1:** The same TUPF is maintained regardless of the access technology (e.g. RATs and cells) a UE is using to access the network.

- **SSC mode 2:** The same TUPF is only maintained across a subset (i.e. one or more, but not all) of the access network attachment points (e.g. cells and RATs), referred to as the serving area of the TUPF. When the UE leaves the serving area of a TUPF, the UE will be served by a different TUPF suitable for the UE's new point of attachment to the network.

NOTE: The serving area of a TUPF may also be limited to a single cell only, e.g. in case of stationary UEs.

- **SSC mode 3:** In this mode the network allows the establishment of UE connectivity via a new TUPF to the same data network (DN) before connectivity between the UE and the previous TUPF is terminated. When trigger conditions apply, the network selects a target TUPF suitable for the UE's new point of attachment to the network. While both TUPFs are active, the UE either actively rebinds applications from the previous to the new address/prefix, or alternatively, the UE waits for flows bound to the previous address/prefix to end.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 296 of 501

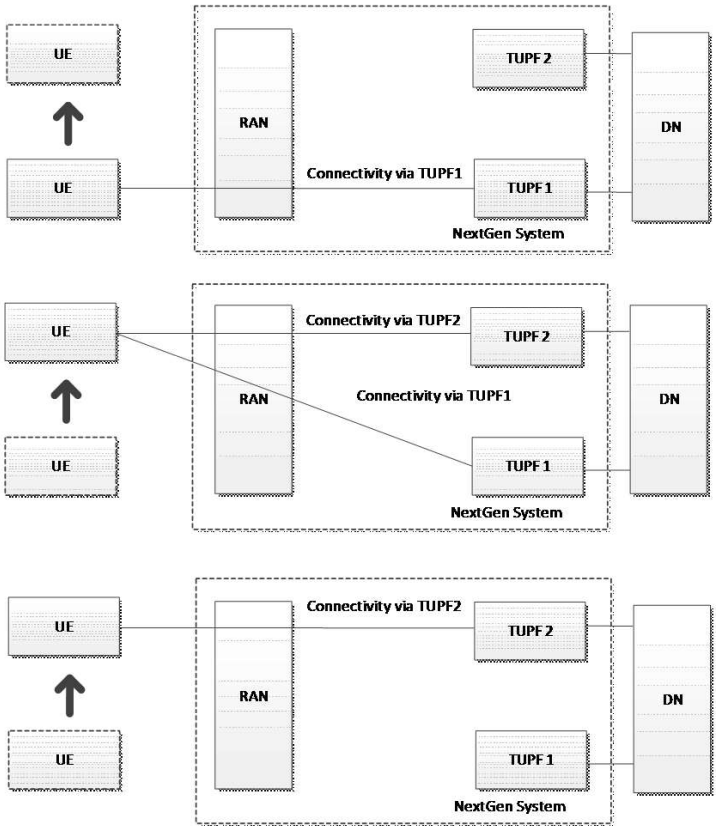


Figure 6.6.1.1.3-1: TUPF relocation in session and service continuity mode 3

6.6.1.1.4 Solution principles

6.6.1.1.4.1 Mode selection and network support

The following principles apply:

- When requesting a PDU session, the UE may indicate the requested session and service continuity (SSC) mode as part of the PDU session setup signaling to the network. How the UE can determine the requested SSC mode is specified in clause 6.6.1.1.4.

Editor's note: It is FFS whether the requested SSC mode is indicated as part of the DN name or as a separate indication.

- The serving network receives the list of supported SSC modes and the default SSC mode per data network per subscriber as part of the subscription information from the subscriber database.

- The serving network selects the SSC mode by either accepting the requested SSC mode or modifying the requested SSC mode based on subscription and/or local configuration.

NOTE 1: A serving network may be configured to modify the SSC mode requested by the UE for different reasons, e.g. the serving network may prefer to avoid SSC mode 1 for a specific data network to avoid concentrating traffic on centralized peering points with the related data network.

- If a UE does not provide an SSC mode when requesting a new PDU session, then the network selects the default SSC mode listed in the subscription (for the data network to connect to) or applies local configuration to select the SSC mode.

- After selecting the SSC mode, the network either (a) accepts the PDU session request from the UE and indicates the selected SSC mode to the UE, or (b) the network rejects the PDU session request and sends the selected SSC

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 297 of 501

mode and a cause value to the UE e.g. indicating that the selected SSC mode is already used by another PDU session in the UE.

NOTE2: The indication that the selected SSC mode is already used by another PDU session may be used by the UE as an indication to use an existing PDU session for the new traffic.

- A UE can have multiple PDU sessions to the same DNN with the same SSC mode
- SSC modes apply per PDU session. A UE may request different SSC modes for different PDU sessions, i.e. different PDU sessions which are active in parallel for the same UE may have different SSC modes.
- The SSC mode is not changed during the lifetime of a PDU session.
- TUPF selection: When selecting the TUPF for a PDU session, the network takes the UE's current point of attachment and the requested SSC mode into account.

NOTE 3: It is not precluded that other information is also taken into account for TUPF selection (e.g. as determined by other key issues).

6.6.1.1.4.2 SSC mode 1

The following principles apply:

- The assigned TUPF is maintained during the lifetime of the PDU session, i.e. the TUPF is not changed by the network.

6.6.1.1.4.3 SSC mode 2

The following principles apply:

- Triggers for redirection to a different TUPF
  - The network decides whether the TUPF assigned to a UE's PDU session needs to be reassigned based on UE mobility, local policies (e.g. information about the serving area of the assigned TUPF).
- Redirection procedure
- The network redirects the UE's traffic to a different TUPF by first releasing the user plane path associated with the current TUPF and then setting up a user plane path corresponding to a new TUPF. Two solution variants are described below, one where the PDU session is preserved when reallocating the TUPF and one where the network is disconnecting the UE's PDU session corresponding to the current TUPF and requesting the UE to reactivate the PDU session immediately which results in selection of a new TUPF.
- During this process, the UE remains attached.
- The network selects a TUPF based on the UE's current point of attachment to the network.

NOTE: It is not precluded that other information is also taken into account for TUPF selection (e.g. as determined by other key issues).

6.6.1.1.4.4 SSC mode 3

The following principles apply:

- Triggers for redirection to a different TUPF:
  - The network decides whether the TUPF assigned to a UE's PDU session needs to be reassigned based on local configuration (e.g. information about the serving area of the assigned TUPF).
- Redirection procedure:
  - The network indicates to the UE that traffic on one of the UE's active PDU sessions needs to be redirected. The network also starts a timer and indicates the timer value to the UE.
  - The user plane path is established towards a new TUPF. Two solution variants are described below, one where the PDU session is re-used also for the additional user-plane path and one where an additional PDU

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 298 of 501

session is established. The network selects a new TUPF based on the UE's current point of attachment to the network.

NOTE 1: It is not precluded that other information is also taken into account for TUPF selection (e.g. as determined by other key issues).

- If the UE has sent a request for an additional PDU session to the same DN without a prior indication from the network that the active PDU session needs to be redirected, then the network rejects the UE's request.

- Once the new user plane path associated with the new TUPF has been established, the UE may perform one of the following options:

  - Option 1: The UE actively redirects application flows bound to the previous TUPF to the new TUPF e.g. by using upper layer session continuity mechanisms. Once the UE has finished redirecting applications flows to the new TUPF, the previous TUPF is released.

  - Option 2: The UE steers new application flows to the new TUPF. Existing flows via the previous TUPF continue until the flows terminate. Once all flows using the previous TUPF have ended, the previous TUPF is released.

  When Option 2 is used, Multi-homed PDU session may be used to send application flows bound to the previous TUPF. Tunnel between the previous TUPF and new TUPF is used to forward those flows.

Editor's note: It is FFS whether Multi-homed PDU session based session continuity is selected as a solution.

NOTE 2: The details of the previous options are beyond the scope of 3GPP.

- If the previous TUPFhas not been released when the timer expires, or alternatively if the network detects inactivity on the previous TUPF, the network releases the previous TUPF.

Editor's note: Whether there is an issue related to per session bitrate enforcement when the UE temporarily has two active PDU sessions to the same data network depends on the QoS key (specifically whether the session bitrate applies per PDU session or across all PDU sessions to the same data network and where the session bitrate is enforced, i.e. in AN or UP entity)issue and is FFS.

6.6.1.1.5 How the UE determines the required SSC mode

A UE can determine the SSC mode required for an application using one of the following methods:

1. The app that starts a new flow (i.e. opens a new socket) indicates the type of session continuity required by this flow as shown in the Figure 6.6.1.1.5-1 below. This may be indicated by using the sockets API extensions specified in RFC 3493, RFC 3542 and in *draft-ietf-dmm-ondemand-mobility*. In other words, the app may use already specified software APIs to indicate what type of session continuity is required. For example, if the app requests a socket with a *nomadic* IP address, essentially, the app requests SSC mode 2. If the app requests a socket with a *fixed* IP address or a *sustained* IP address, essentially, the app requests SSC mode 1 or SSC mode 3 respectively. The definition of *nomadic*, *sustained* and *fixed* IP address can be found in *draft-ietf-dmm-ondemand-mobility*.

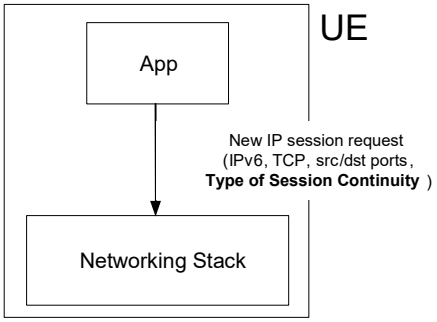


Figure 6.6.1.1.5-1

2. If the app that starts a flow does not indicate the type of required session continuity, the UE may determine the required session continuity by using provisioned policy, as shown in Figure. 6.6.1.1.5-2.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 299 of 501

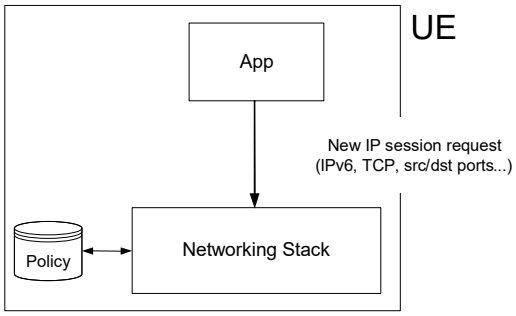


Figure 6.6.1.1.5-2

The policy contains a list of prioritized rules and each rule indicates the required SSC mode for entire applications or specific flow types. For example, the policy in the UE may contain the following rules:

Rule 1, priority 1: App = com.example.skype, Required continuity type = SSC mode 3.

Rule 2, priority 2: App = com.example.web.server, Required continuity type = SSC mode 1.

Rule 3, priority 3: Protocol = TCP; DstPort = 80, Required continuity type = SSC mode 2.

Default rule: Default continuity type = SSC mode 2.

When the UE attempts to establish a PDU session before receiving a request from an application (e.g. during the initial attach), or the application does not request an SSC mode, or the UE does not have a policy for the specific application, then the UE cannot determine an SSC mode as defined above (in bullets 1, 2). In this case:

- If the UE is provisioned with a default SSC mode (e.g. as part of the policy shown in Figure 6.6.1.1.5-2), then the UE requests the PDU session with the default SSC mode. The default SSC mode can be one of the three SSC modes discussed in the previous clause. For example, a fixed IoT sensor or even a smartphone may be provisioned with default SSC mode 2.
- If the UE is not provisioned with a default SSC mode, then the UE requests the PDU session without providing an SSC mode. In this case, the network determines the SSC mode of the PDU session (e.g. based on subscription data and/or network policy) and provides the selected mode back to the UE.

6.6.1.2 Function description

6.6.1.2.1 PDU session establishment/release triggered by handover procedure

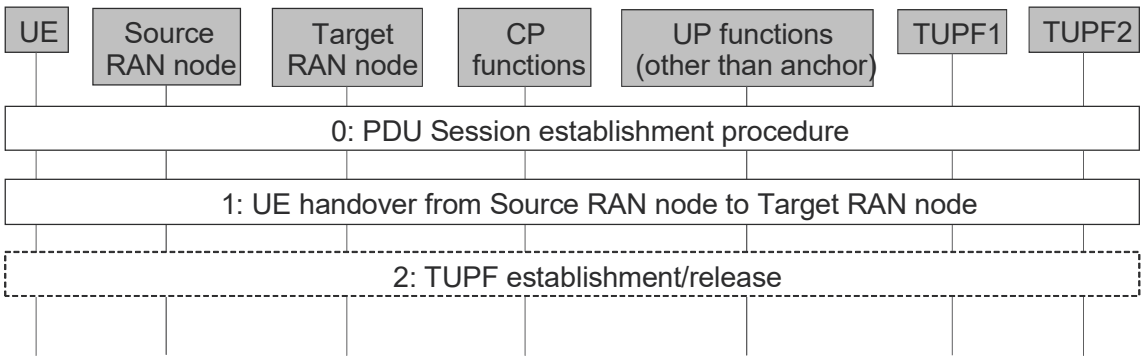


Figure 6.6.1.2.1-1: Handover triggered PDU session establishment/release for different SSC modes

0. The UE attaches to the network and establishes PDU sessions with DNs. A UE may request different SSC modes for different PDU sessions.
1. UE performs handover from source RAN node to target RAN node.

NOTE: The detailed handover procedure is to be discussed in mobility management key issue.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 300 of 501

2. For SSC mode 2 or 3, the redirection of TUPF is triggered as described in session 6.6.1.1.4.

6.6.1.2.2 Service continuity call flows

The establishment of the new TUPF for SSC mode 2 and 3 is always triggered by the CP functions in the NextGen core. There are two options:

- CN-provided trigger followed by UE-requested PDU Session establishment.
- CN-prepared PDU Session modification followed by notification to UE (applicable to multi-homed PDU Sessions only).

The different cases are elaborated in the sections below, first for SSC mode 3, and then for SSC mode 2.

Editor's note: It is FFS whether both procedures need to be supported.

6.6.1.2.3 CN-provided trigger followed by UE-requested PDU Session (SSC mode 3)

This procedure corresponds to the PDN connection model in EPS where a new PDN connection is always requested by the UE. Depicted in Figure 6.6.1.2.3-1 is an example flow illustrating how UE-requested PDU Session is established to support SSC mode 3.

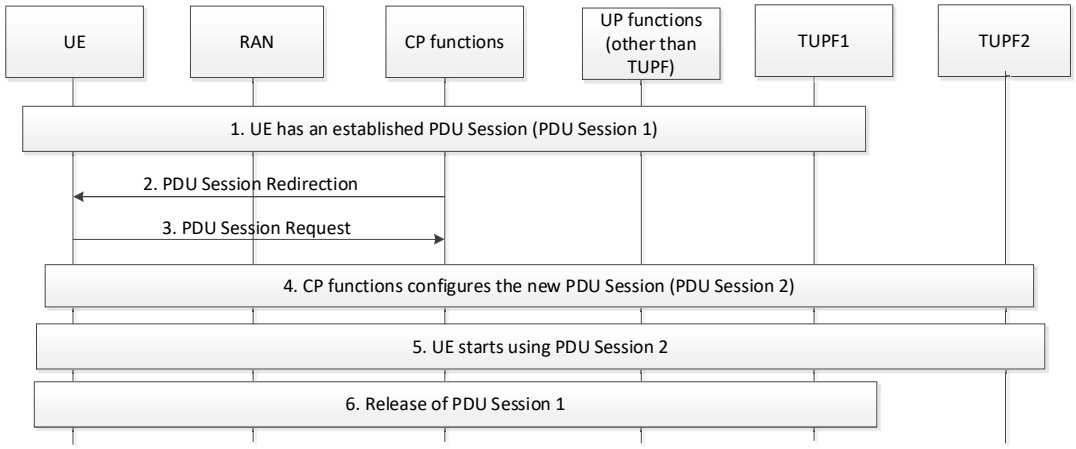


Figure 6.6.1.2.3-1: CN-provided trigger followed by UE-requested PDU Session

1. UE has an established PDU Session (PDU Session 1) with TUPF1. The PDU Session user plane path involves the RAN, TUPF1 and possibly some intermediate user plane functions (other than TUPF).
2. At some point the CP functions decide to establish a new PDU Session because TUPF1 has become suboptimal due to UE mobility. The CP functions send an [NG1] PDU Session Redirection (Reason, Timer) message to the UE with a Reason code that triggers the UE to request a new PDU Session for the same data network, without releasing PDU Session 1. The Timer value indicates how long the network is willing to maintain PDU Session 1.

Editor's note: For PDU Session of IPv6 type it is FFS whether the Timer value for the remaining lifetime of the IPv6 prefix is also sent using RA.

3. UE sends [NG1] PDU Session Request (Reason) message to request a new PDU Session. The Reason code indicates that this message is in response to a network-provided trigger.
4. The CP functions selects a new TUPF (TUPF 2) that is geographically closer to the current UE location and configures the user plane path for PDU Session 2 involving the RAN, TUPF2, and any intermediate U-plane nodes. In case of PDU Session of IP type a new IP address/prefix (IP@2) is allocated and sent to the UE (e.g. directly using Router Advertisement or via CP functions and NG1 signalling).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 301 of 501

5. UE starts using PDU Session 2 for all new traffic flows and may also proactively move existing traffic flows (where possible) from PDU Session 1 to PDU Session 2 by leveraging upper layer mobility mechanisms (e.g. SIP reINVITE, DASH, MPTCP, Host ID, SCTP).

6. PDU Session is released either by the UE (e.g. once UE has consolidated all traffic on PDU Session 2) or by the network upon expiry of the Timer indicated in step 2.

6.6.1.2.4 CN-prepared PDU Session modification followed by notification to UE (SSC mode 3)

This procedure applies to multi-homed PDU Session as described in clause 6.4.13. In this case the NextGen core can prepare a new PDU Session "leg" and in the end simply notify the UE of the existence of a new IP address/prefix, as depicted in Figure 6.6.1.2.4-1.

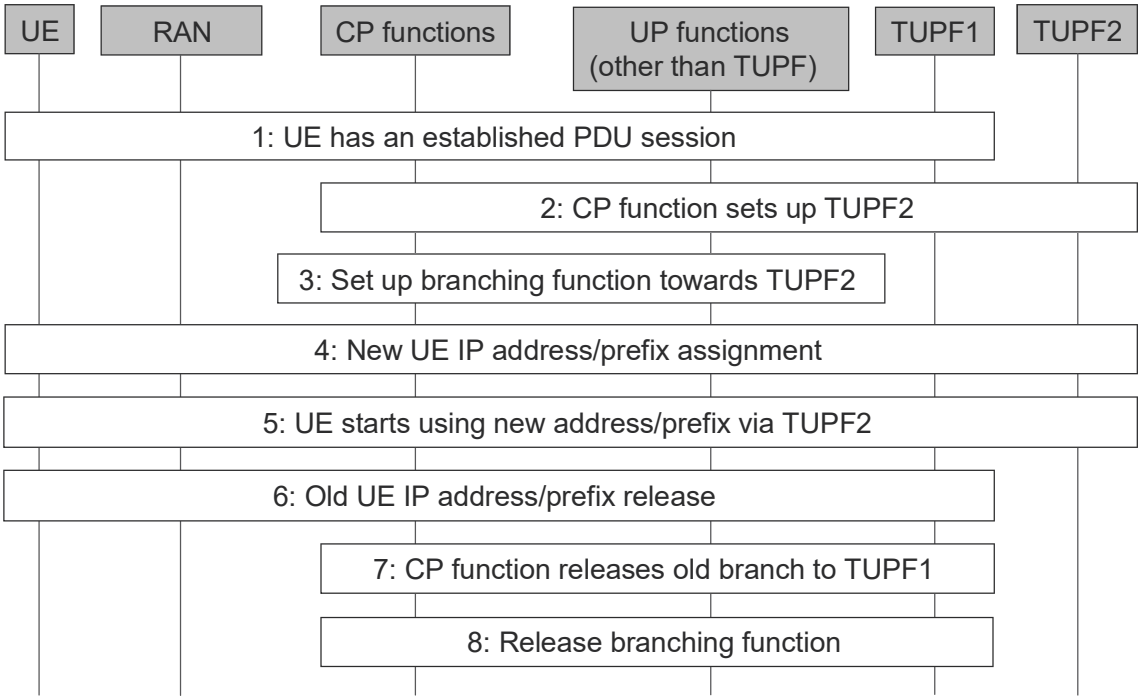


Figure 6.6.1.2.4-1: CN prepared PDU Session followed by notification to UE

1. UE has an established PDU Session with TUPF1. The PDU Session user plane involves the RAN, TUPF1 and possibly some intermediate user plane functions (other than IP anchors).

2. At some point the CP functions decides to establish a new branch of PDU Session 1 because the existing branch has become suboptimal due to UE mobility. The CP functions selects a new TUPF (TUPF2) that is geographically closer to the current UE location and configures TUPF2 as a new branch of a multi-homed PDU Session. In the process a new IP address/prefix (IP@2) is allocated.

3. The CP functions configures one of the intermediate U-plane nodes as a branching point for the multi-homed PDU Session. It is possible that the CP may insert a new U-plane node into the path to act as a branching point. The U-plane node acting as a branching point may be collocated with other entities, e.g. with RAN.

4. The network notifies the UE of the availability of the new IP address/prefix. This may be performed using an IPv6 Router Advertisement or a control message.

Editor's note: it is FFS whether additional information needs to be sent to the UE on the time on how long the network is willing to keep the old address/prefix. If additional information is needed, it is FFS whether the Router Advertisement message can be enhanced to carry the information.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 302 of 501

5. UE starts using IP@2 for all new traffic and may also proactively move existing traffic flow (where possible) from IP@1 to IP@2 by leveraging upper layer mobility mechanisms (e.g. SIP reINVITE, DASH, MPTCP, Host ID, SCTP).

6. The network releases the UE's old IP address/prefix. At this point the UE stops using the old IP address prefix.

7. The CP releases the old branch at TUPF1.

8. The CP releases the branching function. If needed, the branching entity may be removed from the user plane path.

6.6.1.2.5 CN-provided trigger followed by UE-requested PDU Session establishment (SSC mode 2)

This procedure corresponds to the PDN connection model in EPS where a new PDN connection is always requested by the UE. Depicted in Figure 6.6.1.2.5-1 is an example flow illustrating how UE-requested PDU Session is established to support SSC mode 2.

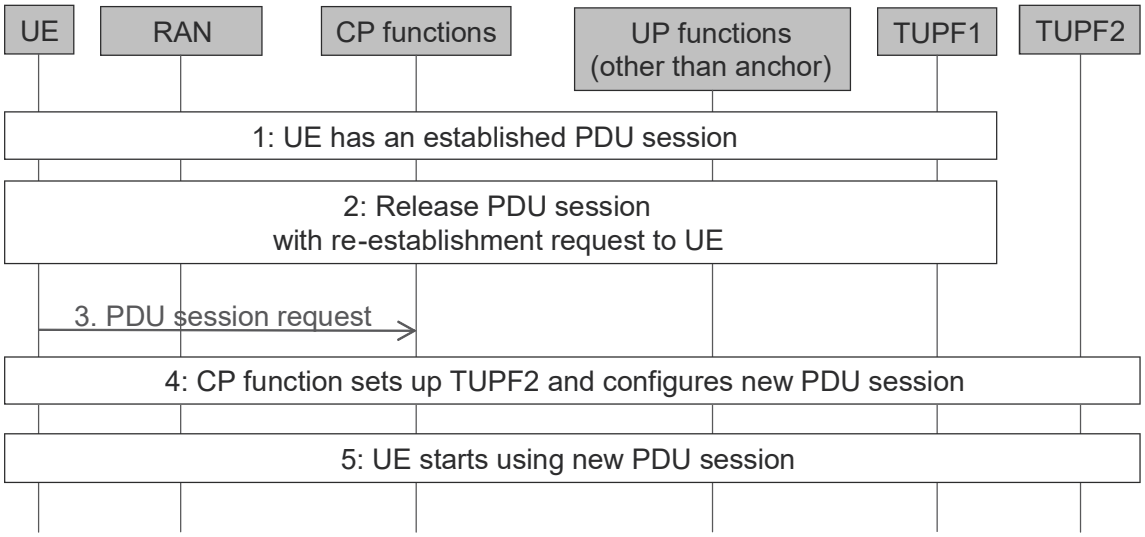


Figure 6.6.1.2.5-1: CN-provided trigger followed by UE-requested PDU Session

1. UE has an established PDU Session with TUPF1. The PDU Session user plane path involves the RAN, TUPF1 and possibly some intermediate user plane functions (other than TUPF).

2. At some point the CP functions decide that a new TUPF is because TUPF1 has become suboptimal due to UE mobility. The CP functions release the existing PDU session, with a message to the UE that a new PDU session should be re-established.

3. UE sends [NG1] PDU Session Request message to request a new PDU Session.

4. The CP functions select a new TUPF (TUPF 2) that is geographically closer to the current UE location and configure the user plane path for new PDU Session the RAN, TUPF2, and any intermediate U-plane nodes. In case of PDU Session of IP typea new IP address/prefix (IP@2) is allocated and sent to the UE (e.g. directly using Router Advertisement or via CP functions and NG1 signalling).

5. UE starts using the new PDU Session for all traffic flows. Where possible, the UE may move traffic flows (where possible) from TUPF1 to TUPF2 by leveraging upper layer mobility mechanisms (e.g. SIP reINVITE).

6.6.1.2.6 CN-prepared PDU Session modification followed by notification to UE (SSC mode 2)

This procedure applies to multi-homed PDU Session using IPv6 as described in clause 6.4.4. In this case the NextGen core can prepare a new PDU Session "leg" and in the end simply notify the UE of the existence of a new IP address/prefix, as depicted in Figure 6.6.1.2.6-1.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 303 of 501

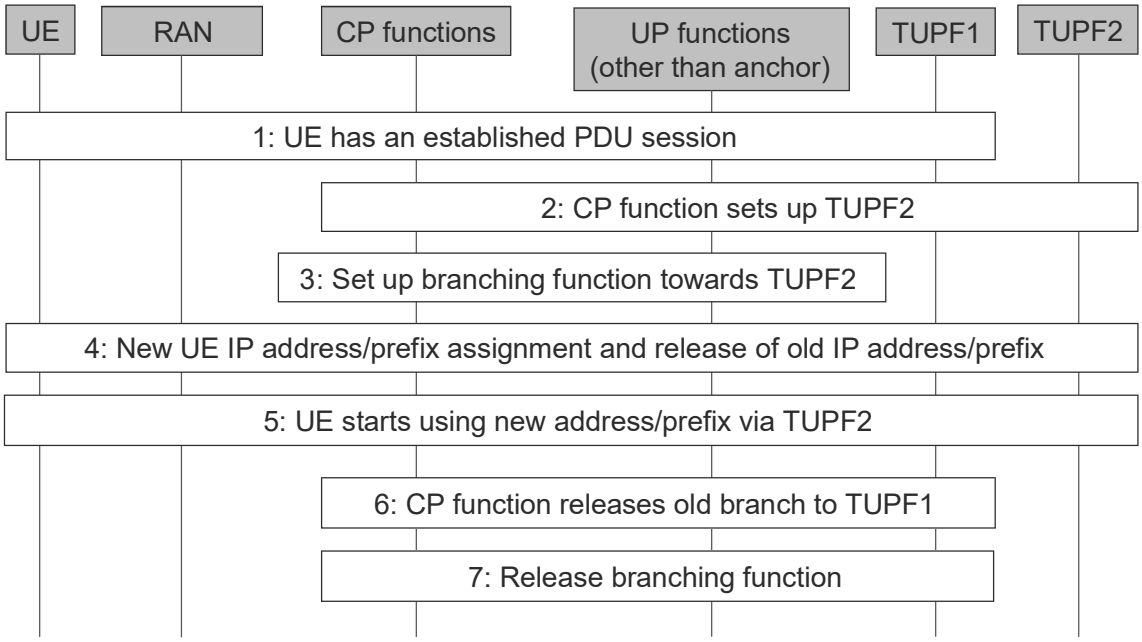


Figure 6.6.1.2.6-1: CN prepared PDU Session followed by notification to UE

1. UE has an established PDU Session with TUPF1. The PDU Session user plane involves the RAN, TUPF1 and possibly some intermediate user plane functions (other than IP anchors).
2. At some point the CP functions decides to establish a new branch of PDU Session 1 because the existing branch has become suboptimal due to UE mobility. The CP functions selects a new TUPF (TUPF2) that is geographically closer to the current UE location and configures TUPF2 as a new branch of the session. In the process a new IP address/prefix (IP@2) is allocated. At this point, the UE is not yet involved.
3. The CP function configures one of the intermediate U-plane nodes as a branching point for the PDU Session. It is possible that the CP may insert a new U-plane node into the path to act as a branching point. The U-plane node acting as a branching point may be collocated with other entities, e.g. with RAN.
4. The network notifies the UE of the availability of the new IP address/prefix. The UE releases the old IP address/prefix as soon as it configures the use of the new IP address/prefix. This may be performed using an IPv6 Router Advertisement or a control message.
5. UE starts using IP@2 for all new traffic and may also proactively move existing traffic flow (where possible) from IP@1 to IP@2 by leveraging upper layer mobility mechanisms (e.g. SIP reINVITE).
6. The CP releases the old branch at TUPF1.
7. The CP releases the branching function. If needed, the branching entity may be removed from the user plane path.

6.6.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

Void.

6.6.2 Solution 6.2: Mobility on Demand using Mobility and Session classes

The solution for the Mobility on demand part of Key Issue 6 is described in the corresponding solution chapter for Key Issue 6: Chapter 6.3.9 Mobility levels using Mobility and Session classes.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 304 of 501

6.6.3 Solution 6.3: Multi-homing over multiple PDU sessions with network-provided routing rules

6.6.3.1 Architecture description

When a UE already has an existing PDU session to a given Data Network, a second PDU session to the same Data Network may be established via a trigger from the network to the terminal. This may arise in the following cases.

- When the network determines that a service that the UE uses or intends to use (based on e.g., subscription information, local configuration or explicit signalling) can be better served via another TUPF, such as a local TUPF.

- In case of mobility, when a new PDU session to a new TUPF should be established before the old PDU session to an old TUPF is released. This case is common with Solution 6.1 SSC mode 3 and the description in Section 6.6.1.2.3 (CN-provided trigger followed by UE-requested PDU Session (SSC mode 3)) applies to this solution as well.

When a UE has multiple PDU sessions to the same Data Network with multiple addresses/prefixes, the network provides rules to the terminal to decide which address to apply in case of a given traffic flow. This is analogous to the multi-homing variant of Solution 5.2 with the difference that in this solution, the multiple addresses/prefixed are used over different PDU sessions. Hence, in this case the rules determine not only the IP address to be used, but also the PDU Session.

Specifically, for IPv6 the solution relies on RFC 4191 which includes mechanisms by which the network can configure rules into the UE to influence the selection of the address and thereby the selection of the PDU session. This is achieved via sending routing rules together with the IPv6 Router Advertisements.

For IPv4 the same can be achieved by means of RFC 3442. As an alternative for IPv4 (e.g. if DHCP is not supported), routing information is passed as a control-plane message to the UE.

Editor's note: It is FFS if IPv4 need to be supported in this solution.

Editor's note: The DHCPv4 option does not allow for subsequent updates of the routing information. Whether this limitation is an issue is FFS.

Using this mechanism, the network can e.g., trigger the setup of an additional PDU session with an additional address/prefix using a local TUPF whenever the network determines that the user intends to use a service for which a local server is available. Using the routing rules configured into the terminal, the network can direct the appropriate flows via the local TUPF using the corresponding address. At mobility events, the network may determine whether or not to trigger the use of a new local TUPF at a new location, depending on how the specific application is supported locally and based on the specific network deployment.

Editor's note: It is FFS how service continuity is handled for applications in case they are moved to a different PDU Session because of the routing rule update.

6.6.3.2 Function description

6.6.3.2.1 CN-provided trigger for new UE-requested PDU Session, no mobility case

Depicted in Figure 6.6.3.2.1-1 is an example flow illustrating how UE-requested PDU Session is established base on CN-provided trigger.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 305 of 501

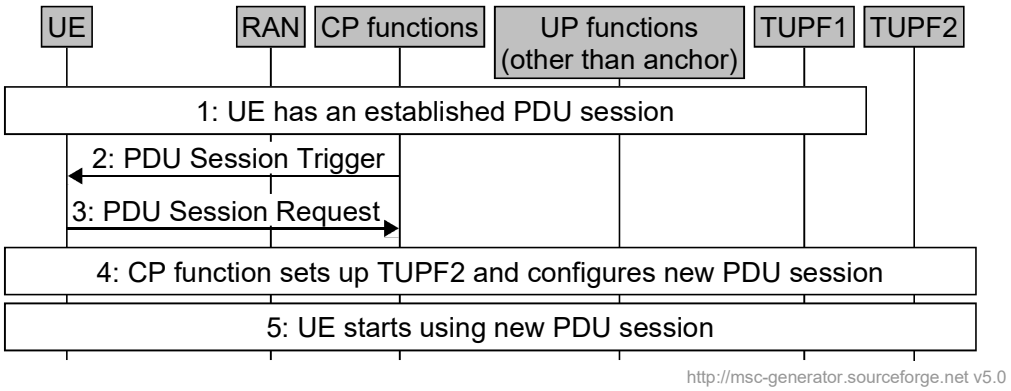


Figure 6.6.3.2.1-1: CN-provided trigger followed by UE-requested PDU Session

1. UE has an established PDU Session (PDU Session 1) with TUPF1. The PDU Session user plane path involves the RAN, TUPF1 and possibly some intermediate user plane functions (other than TUPF).

2. At some point the CP functions decide to establish a new PDU Session because TUPF1 may not be optimal considering the current services used by the UE. This trigger may be based e.g., on a combination of subscription information, local configuration and explicit indication from the UE, application or policy entities or from a user plane entity. The CP functions send an [NG1] PDU Session Trigger message to the UE which triggers the UE to request a new PDU Session for the same data network, without releasing PDU Session 1.

Editor's note: When the CP function decides to establish a new PDU session due to UE location change or subscription information, it is FFS how the routing rules are determined.

3. UE sends [NG1] PDU Session Request message to request a new PDU Session.

4. The CP functions select a new TUPF (TUPF 2) and configure the user plane path for PDU Session 2 involving the RAN, TUPF2, and any intermediate U-plane nodes. TUPF2 allocates the new IP address/prefix (IP@2) and sends it to the UE using an IPv6 Router Advertisement. Together with the Router Advertisement, TUPF2 also sends routing rules to the UE which govern when the newly allocated address should be used.

5. UE starts using PDU Session 2. In case an existing data flow is moved over from PDU session 1 to PDU session 2, upper layer mobility mechanisms may be invoked for service continuity.

6.6.3.2.2 CN-provided trigger for new UE-requested PDU Session, mobility case

In this case, the new PDU session is triggered by UE mobility, and the network decides to set up a new PDU session before releasing the old one. This procedure is executed as defined for Solution 6.1, SSC mode 3, described in Section 6.6.1.2.3.

6.6.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.7 Solutions for Key Issue 7: Network function granularity and interactions between them

6.7.1 Solution 7.1: Interconnection and Routing Function (IRF) based network function interconnection model

6.7.1.1 General (Assumptions and applicability)

This solution is applicable only to the interconnection of the network functions. The network function's definition and its functionalities are assumed to be defined by solutions to other key issues.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 306 of 501

Assuming that only one of the control plane access network function is required to interface with only one of the control plane core network function, the interconnection model between them can be point-to-point interface based, e.g. control plane core network function 1 interfaces with control plane access network function 1 over a point-to-point interface between them. However, if it is decided to allow multiple control plane access network functions to interface directly with multiple control plane core network functions then the principles of this solution can be extended to interconnect control plane access network and core network functions as well.

Similarly, it is assumed that the user plane core network functions are required to interface only with their respective control plane core network functions. And hence the interconnection model between them can be point-to-point interface based. However, if it is decided to allow any control plane function to interface with any user plane function then the principles of this solution can be extended to interconnect control plane and user plane core network functions as well.

The solution assumes that multiple control plane core network functions are required to interact with multiple other control plane core network functions in the next generation core network architecture.

NOTE: Unless explicitly specified, the term "network function" refers to "control plane core network function" in this solution. Just for the sake of understanding the "control plane core network functions" in the EPC context are MME, control plane of PGW, PCRF, HSS, control plane of TDF, TSSF, RCAF, SCEF etc.

6.7.1.2 Architectural description

6.7.1.2.1 Reference model

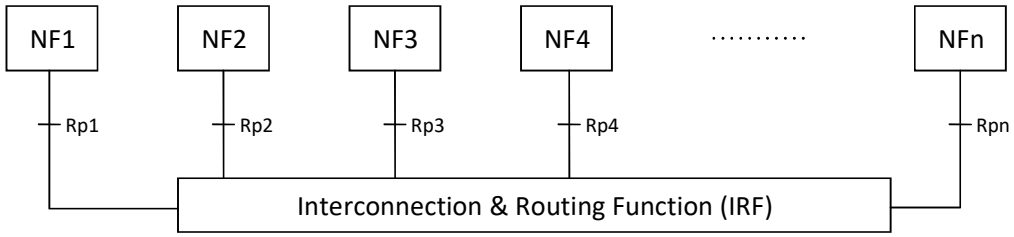


Figure 6.7.1.2.1-1: Non-roaming reference model for the interconnection of network functions

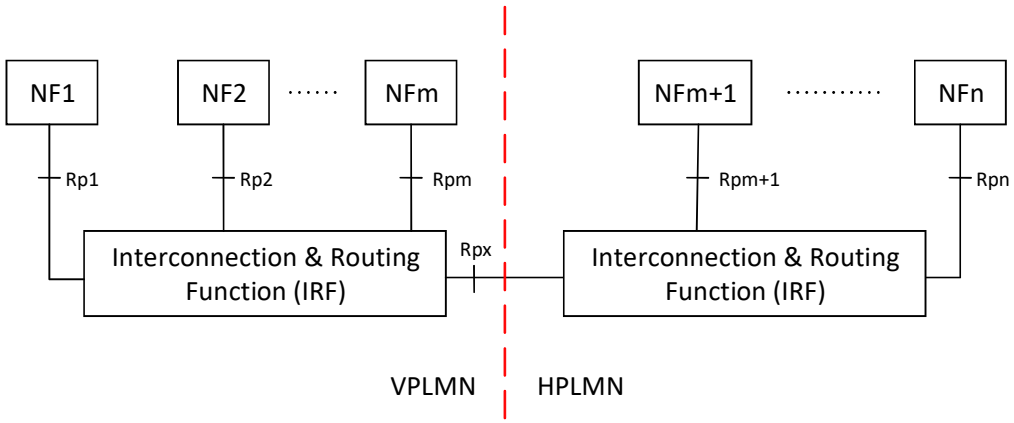


Figure 6.7.1.2.1-2: Roaming reference model for the interconnection of network functions

NOTE 1: The roaming reference model describes home routed traffic type of scenario. Other reference models, e.g. local breakout, can be derived from this and not shown here for simplicity.

NF1: Network functions (NF) no. 1.

NFn: Network functions (NF) no. "n".

Rp1: Reference point between the network function NF1 and Interconnection & Routing Function (IRF).

Rpn: Reference point between the network function NFn and Interconnection & Routing Function (IRF).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 307 of 501

Rpx: Inter-PLMN reference point between two Interconnection & Routing Functions.

NOTE 2: Above reference points are proposed to be 3GPP defined reference points. Not all the messages supported on each reference points are same, e.g. some of the messages supported over Rp1 may be different than some of the messages supported over Rp2.

Editor's note: Whether the interface between NF and the IRF is referred to as "reference point" or not is FFS.

6.7.1.2.2 High level principles

Below are the high level principles of the Interconnection & Routing Function (IRF) based interconnection model:

- Each NF interfaces with the IRF via a given reference point in its own PLMN. NFs do not interface with each other directly but can communicate (i.e. send request or response message) with each other via IRF. Thus, when required, this model allows any NF to communicate with any other NF directly without involving any other unrelated network functions in the path, e.g. NF1 can send message to NF3 via IRF without involving NF2 if the involvement of NF2 is not needed.

- In this model each NF supports only one reference point towards the IRF. All the procedures towards the other NFs are supported over this single reference point, e.g. NF1 supports Rp1 towards IRF instead of supporting Rpa towards NF2, Rpb towards NF4 etc.

- The NFs are not required to maintain interface layer association for each peer-NFs in the network, and thus resulting into connection-less interconnection of NFs. However, the application layer state for the UE associated or non UE associated session is required to be maintained. If the NF wants to change its instance (e.g. VM instance) for a given session (e.g. to support scale-in, scale-out and restoration features) it just has to update the IRF and not the peer-NFs, e.g. NF1 can move the session from its instance1 to instance2 and update the IRF with the new instance number while there is no need to update NF2, NF3, NF4 etc. of the network.

Editor's note: Non UE associated signalling may include load, congestion, or management related signalling (as described in GTP-C and S1AP of LTE), but defining the signalling procedures is out of scope of this key issue.

- The IRF is mainly responsible for routing of the message between NFs. The NF is responsible for determining the destination NF for the message and populating it in the message header. The IRF examines the message header to determine the interface layer identity (e.g. instance number) of the destination NF for the session and routes it to the appropriate NF. For the routing purpose, the IRF maintains the repository of the binding between the binding key identity (e.g., UE identity) and interface layer identity of the serving NFs. Please refer to sec. 6.7.3.2 for the set of functions performed by IRF.

- If the procedures over the reference point between the NF and IRF are defined generically, then this model allows re-use of those procedures by any other NF in the network, e.g. if NF1 supports procedures such as "UE location change reporting" or "UE congestion level change reporting" without restricting which other NFs in the network can invoke it, then it can be invoked by NF2 as well as by NF5 while no special support needed at NF1 to enable this. This can also be achieved via subscribe-notify type of mechanism for appropriate procedures, e.g. NF2 and NF5 subscribe to the "UE location change reporting" from NF1; NF1 keeps the subscription info and when the UE location change takes place, it notifies NF2 and NF5 individually. In future, NF6 can also subscribe to the same procedure and no special support needed at NF1.

6.7.1.3 Functional description

6.7.1.3.1 General

The proposed interconnection model introduces Interconnection & Routing Function (IRF). The IRF is proposed as 3GPP defined network function. This clause provides functional description of IRF and any other related aspects.

6.7.1.3.2 Functions of Interconnection & Routing Function (IRF)

The functions of IRF include:

- Stores the binding between UE's identity and the interface layer identity (e.g. instance number) of each serving NF, which has active session for the UE. For the non UE associated signalling, any identifier which allows the NF to locate the non UE associated signalling session can be used as the key value for binding network functions. For the NFs, which do not interface with the IRF directly, e.g. in roaming scenario, the IRF stores the identity of the remote-PLMN's IRF via which those NFs are reachable.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 308 of 501

- Updates the binding repository when the identity of the serving NF changes for a given UE, e.g. due to UE mobility, load re-balancing (i.e. scale-in or scale-out of VMs) or restoration reasons.

- Examines the message header to determine the identity of the session and the destination NF. For a given binding key identity, looks up the internal binding repository to determine the interface layer identity (e.g. instance number) of the destination NF or the identity of the remote IRF. If the binding does not exist, then the IRF selects appropriate instance of NF (e.g. based on load/overload information) or remote IRF (e.g. based on the PLMN information within destination NF's logical identity) and updates its local repository with the binding. Routes the message accordingly.

- Optionally performs authorization of the message based on the operator's configuration, e.g. if operator's configuration prohibits NF1 from invoking certain message (such as "change of UE's APN-AMBR") towards NF4 then the IRF rejects the corresponding message (see NOTE 2). Optionally protects NFs during the signalling storm by performing overload control, e.g. pacing of messages sent to a given NF based on its load/overload condition.

NOTE 1: The protocol between each NF and the IRF will be defined by stage 3. If different protocols are defined then the IRF may have to perform protocol conversion while routing the message between two NFs.

NOTE 2: For performing message authorization, the IRF checks the "message type", "source NF" and "destination NF" parameters from the message header and either allows it or rejects it based on the local configuration.

Editor's note: The exact set of functions performed, e.g. whether it understands application level procedures etc., by IRF are FFS.

6.7.1.3.3 Sample binding repository of IRF

Below is an example of internal binding repository of IRF assuming that the network has network functions NF1 to NF5.

Table 6.7.1.3.3-1: Sample binding repository of IRF

Network scenario	Binding repository at IRF					
	Binding key identity	**NF1's identity**	**NF2's identity**	**NF3's identity**	**NF4's identity**	**NF5's identity**
All NFs are in the same PLMN as IRF	UE-A	Instance1-logical-id-NF1	Instance3-logical-id-NF2	Instance2-logical-id-NF3	Instance1-logical-id-NF4	Instance1-logical-id-NF5
All NFs are in the same PLMN as IRF; No active session for the UE in NF3, NF4	UE-B	Instance1-logical-id-NF1	Instance3-logical-id-NF2	X	X	Instance1-logical-id-NF5
NF4, NF5 are in different PLMN	UE-C	Instance3-logical-id-NF1	Instance1-logical-id-NF2	Instance1-logical-id-NF3	Logical-id-remote-PLMN-IRF	Logical-id-remote-PLMN-IRF
NF4 in different PLMN; No active session for the UE in NF3, NF5	UE-D	Instance2-logical-id-NF1	Instance2-logical-id-NF2	X	Logical-id-remote-PLMN-IRF	X
Non UE associated signalling session. All NFs are in the same PLMN as IRF; Active non UE associated session only in NF3 and NF4.	Binding Key-a	X	X	Instance3-logical-id-NF3	Instance2-logical-id-NF4	X
NOTE 1: The "instance number" is used to signify "an interface layer association" between the IRF and NF for a given UE's session. However, other identity/format to reflect the same can also be used. NOTE 2: The binding key identity of UE associated signalling session could be anything which allows the NF to locate the UE's session uniquely while processing the received message, e.g. IMSI, IP address etc. NOTE 3: The binding key identity of non UE associated signalling session could be anything which allows the NF to locate the related non UE associated signalling session uniquely while processing the received message, e.g. global RAN ID signalling sessions dedicated to a specific RAN.						

Editor's note: The case that a binding key identity is associated with multiple NF instances of the same NF type is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 309 of 501

6.7.1.4 Sample call flows

6.7.1.4.1 General

This clause provides some sample call flows to better explain how the messages are routed between NFs via IRF, in various scenarios, and any other related aspects.

6.7.1.4.2 Basic routing of message between two NFs

Below is the sample call flow for NF1 to send a message NF4 via IRF. NF4 could be in the same PLMN as NF1 or in the different PLMN for UE associated signalling.

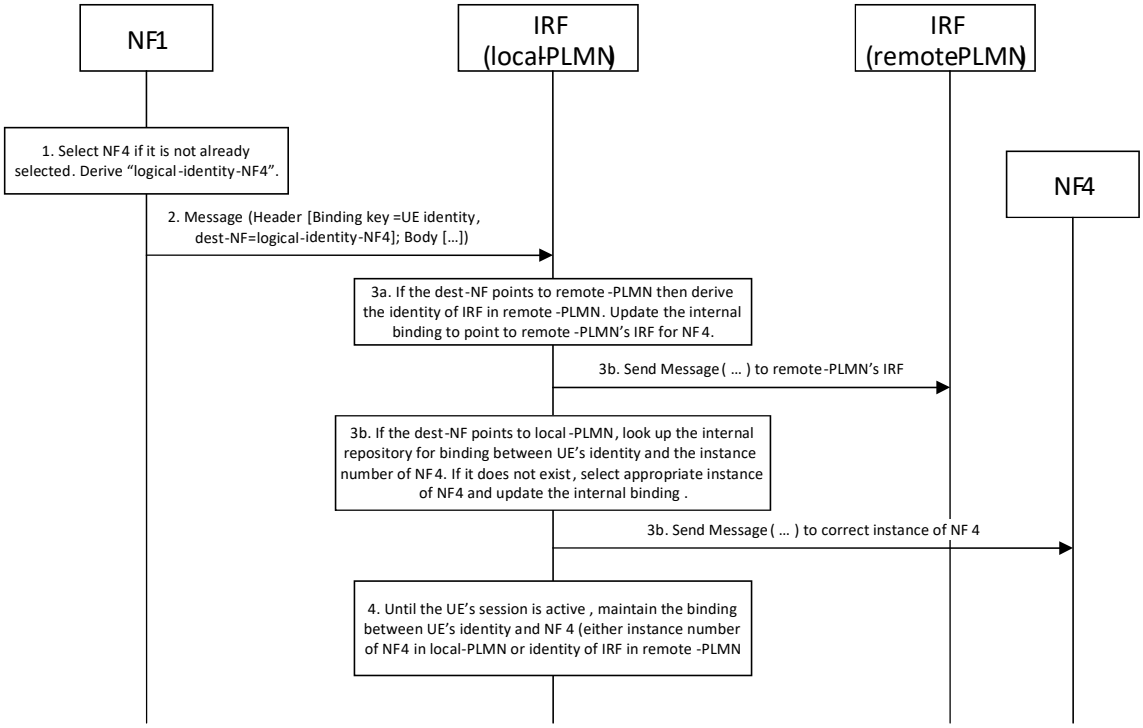


Figure 6.7.1.4.2-1: Sample call flows for routing of message between NF1 and NF4

1. If the UE's session already exists in NF4, NF1 would simply use its logical identity (e.g. FQDN) to send the message to NF4. If the UE's session does not exist in NF4 (e.g. this message creates new session in NF4 as part of attach or relocation types of procedure) then NF1 selects NF4 and derives its logical identity, taking into account appropriate parameters.

2. NF1 includes UE's identity and NF4's logical identity as "destination NF" in the message header and sends it to the IRF. The information related to IRF could be locally provisioned in the NFs.

3a. On reception of the message, the IRF examines the message header to derive UE's identity and destination NF's logical identity. If the logical identity points to NF4 in a remote-PLMN then IRF derives the identity of the IRF in the target PLMN, e.g. based on local configuration or DNS based resolution. The IRF updates the internal binding to point to remote-PLMN's IRF for NF4.

The IRF sends message to the remote-PLMN's IRF. The remote-PLMN's IRF processes the message as described from step 3b onwards.

3b. If the logical identity points to NF4 in the same PLMN, the IRF looks up its internal repository for the binding between the UE's identity and interface layer identity of the NF4 (e.g. the instance number of the NF4). If the binding exists, the IRF sends the message to appropriate instance of NF4.

NOTE 1: Refer to clause 6.7.1.4.4 for more details how the IRF is made aware about the binding between the UE's session and its serving NF instance.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 310 of 501

If the binding does not exist, e.g. this is the very first message for the UE's session to NF4, then IRF selects appropriate instance of NF4 (e.g. based on load/overload information) and sends message to it. The IRF also updates its local repository with the binding between UE's identity and NF's instance number.

NOTE 2: It is assumed that each NF periodically sends the list of its active set of instances along with the load/overload information to the IRF.

4. Until the UE's session remains active, the IRF maintains the binding between UE's identity and NF4's identifier, i.e. either instance number of NF4 in the local-PLMN or identity of IRF in remote-PLMN. This binding will allow IRF to route any message to NF4 for the UE's session.

6.7.1.4.3 Support for subscribe-notify type of mechanism

Editor's note: Call flows for describing the support for subscribe-notify type of mechanism is FFS.

6.7.1.4.4 NF binding management at IRF

Below is a sample call flow of the management of the binding between the UE's session and its corresponding serving NF, at the IRF for UE associated signalling.

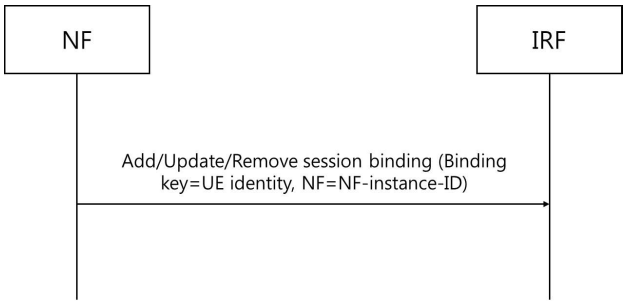


Figure 6.7.1.4.4-1: Sample call flow of NF binding management at IRF

1. When a UE's session is created at an NF, e.g. during the procedures such as attach, new PDU session establishment, relocation etc., the NF updates the IRF by sending "Add UE binding" message. The IRF creates new binding in its binding repository.

   For updating the existing binding, the NF sends "Update UE binding" message to the IRF. Correspondingly, the IRF updates the binding repository. This could take place if the NF changes its instance for an existing UE's session, e.g. due to scale-in, scale-out or restoration feature.

   When the existing UE's session is released by the NF, e.g. during relocation or PDU session release procedures, the NF sends "Remove UE binding" message to the IRF. The IRF clears its binding repository for the UE's session.

NOTE 1: The above messages can be sent independently or by piggybacking on other relevant messages, e.g. While sending "PDU session establishment" message to NF2, NF1 can piggyback "Add UE binding" message for creating binding between the UE's session and NF1's serving instance, at the IRF.

6.7.1.5 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.7.2 Solution 7.2: The interconnection of NFs and discovery of NFs via NF Repository Function

This solution is to address the interconnection of NFs, discovery of the NFs, which is related to the key issue "Network Function Granularity and Interactions between them".

6.7.2.1 Architecture description

The function architecture to enable the discovery of control plane NFs is depicted as the following figure:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 311 of 501

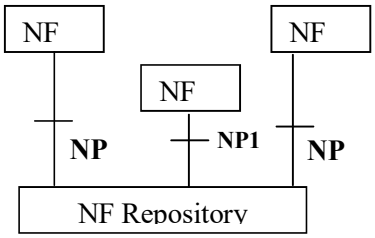


Figure 6.7.2.1-1: The reference architecture for the discovery of NFs

The architecture includes the following functions:

- NF Repository Function: It provides the Function Management function such as NF registration and discovery to enable that one NFs discover the other NFs.
- NP1: the interface between NF Repository Function and NFs for NF discovery.

6.7.2.2 Function description

6.7.2.2.1 General model of Network Function

One general model for Network Function is depicted as the following figure.

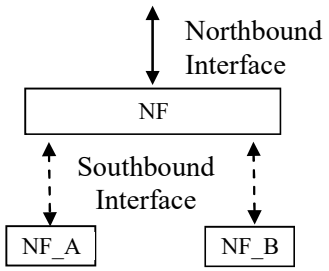


Figure 6.7.2.2.1-1: The general model of Network Function

One network function has the following characteristics:

- The northbound interface to provide the NF's functionality to other Network Functions. This interface shall not be a specific interface towards another Network Functions.
- Southbound Interface: If the Network Function (Function Consumer) requires the functionality from other Network Functions (Function Provider), it shall obtain this functionality via the interface provided by Network Function (Function Provider).

One network function have an associated Function Template Profile. The Function Template Profile includes the following information:

- The Function Type of this Network Function, which identify the function of this NFs. It is similar as the meaning of the "MME" in the EPC network.
- The Service related parameters, which identify the related service parameters. For example the EAP-AKA is the service parameter to indicate which authentication mechanism supported by the Authentication NF.
- The Function Type of other Network Functions it can be interconnected. This information identifies which Function type of other NF it can be interconnected. Also it include the interconnection type per NF, which indicates whether the interconnection between two NFs is permanent or it is on demand.

When instantiating one Network Function, the parameter on the Function template will be configured. Also this function will be registered.

6.7.2.2.3 General model for the interconnection of CP NFs

The Figure 6.2.7.2.2.3-1 represents the general model for the interconnection of CP NFs in the same PLMN:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 312 of 501

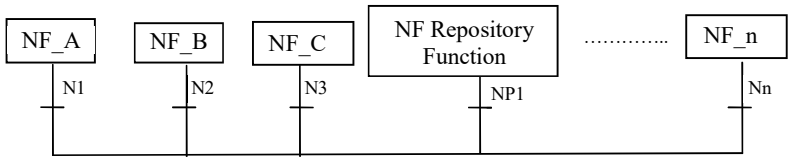


Figure 6.7.2.2.3-1: The general model of the interconnection of CP NFs in the same PLMN

The Figure 6.2.7.2.2.3-2 represents the general model for the interconnection of CP NFs across different PLMNs:

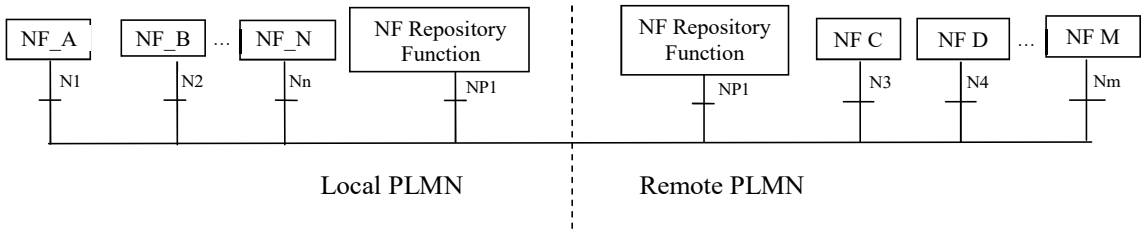


Figure 6.7.2.2.3-2: The general model of the interconnection of CP NFs across different PLMNs

The high level principles are utilized in the general model of the interconnection of CP NFs

- The NF (Function Consumer) determines the function type of the NF (Function Provider) that it needs to access;
- The NF (Function Consumer) shall be able to obtain the instance of the NF (Function Provider) after performing NF discovery;
- The NFs (Function Consumer) shall be able to obtain the function of the NF (Function Provider) via the same interface provided by the NF (Function Provider);
- A common communication protocol is used to transfer the message between the NF (Function Consumer) and the NF (Function Provider);
- The NF (Function Provider) authorizes the functionality that one NF (Function Consumer) can access per UE granularity.
- The interface over which one NF provides its functionality to other NFs does not change per peer NFs, i.e. the interfaces N1, N2, etc., are one per NF and each NF provides all its functionality via this interface.

6.7.2.2.4 NF Discovery

The NF Repository Function supports the following functionalities:

- NF registration: receives and maintains the profile information of NF when deploying new NF in control plane.
- NF discovery in one PLMN: when receiving the discovery request including e.g. class type of NF Identity from one NF, it provides the instance information (i.e. IP address and port) to the NF after authorizing the request of this NF is allowed. NF discovery is the generic method for NF instances to discover and access the required NF instance, and the session per UE granularity between the NF instances is maintained by the peer NF instances.

NOTE: Besides NF registration and discovery function above, other support functionalities can be further studied.

NOTE: Whether the "NF Repository Function" is realized based on the enhancement of the DNS can be determined by stage-3 work.

The flow below indicates one possible example of the NF registration procedure. This can also be done by other mechanism.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 313 of 501

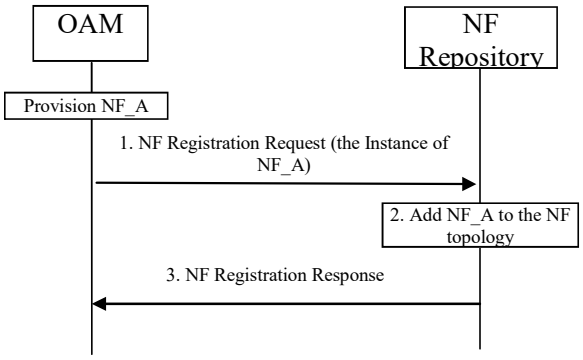


Figure 6.7.2.2.4-1: NF registration procedure

NOTE: It is assumed that OAM deploys the NFs in control plane. The procedure for NF registration is for information only, and it is out of SA2 scope.

1. The new network function NF_A is deployed in control plane of one PLMN's core network. OAM registers the instance of the NF_A into NF Repository Function;
2. NF Repository Function add the NF_A's instance information to the NF topology.
3. NF Repository Function sends NF Registration Response to OAM to confirm that the NF registration is finished.

The NF discovery procedure in one PLMN is depicted in the following figure:

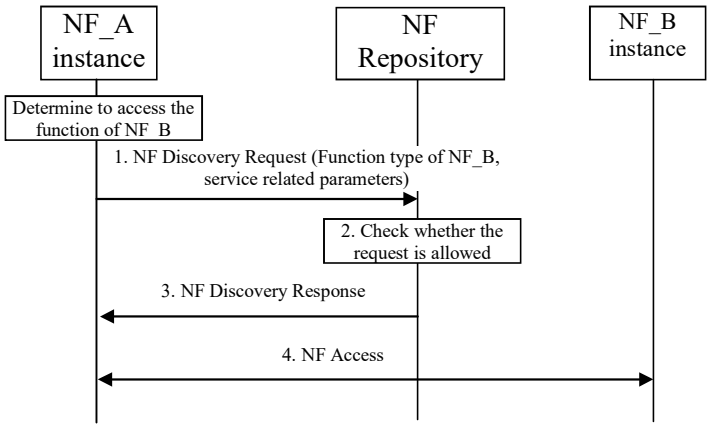


Figure 6.7.2.2.4-2: NF discovery procedure in one PLMN

1. Per user's request the NF_A needs to access the functionality provided by the NF_B. NF_A sends NF Discover Request including the Function Type of NF_B and/or the service related parameters, e.g. Authentication type in case that NF_B is Authentication NF and handles one special type of Authentication mechanism. The service related parameters help to select the special capability NF. The Function type is used to discover the related NF instance.
2. NF Repository Function check if NF_A is authorised to access NF_B based on criteria of the NF permission list.

NOTE: whether the authorization is needed if the NFs are in the same PLMN depends on the operator policy and requirements.

3. If the request is allowed, NF Repository Function provides the candidate of NF_B's instance to NF_A by NF Discovery Response message based on i.e. the load level of NB's instance. Further NF Repository Function can store the discovery request of NF_A, and it notices the alternative instance of NF_B to NF_A when detecting that the original instance of NB_B can't continue to provide its function. Alternatively, the NF Repository Function provides a list of NF instances of the requested Function Type, together with their associated IP

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 314 of 501

addresses to the NF_A. NF_A select a suitable NF_B to access from the list based on other information, e.g. weight factor.

4. NF_A access the NF_B instance based on the interface supported by NF_B, and the generic communication protocol is used to transfer the messages between NF instances.

In case that the NF (Function consumer) and the NF (Function provider) are not in the same PLMN, the NF discovery procedure is depicted in the following figure:

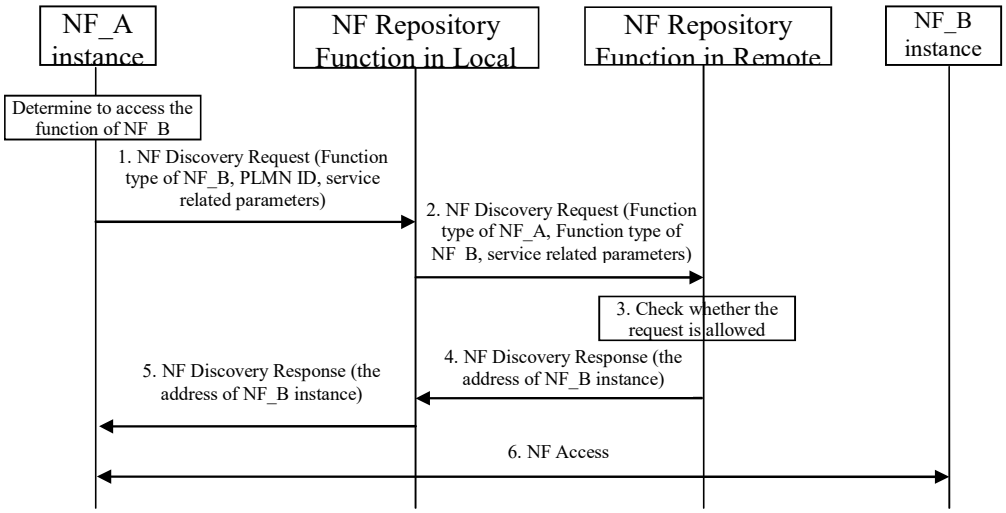


Figure 6.7.2.2.4-3: NF discovery procedure across PLMNs

1. The NF_A instance is serving one UE. Per user's request the NF_A needs to access the functionality provided by the NF_B in Remote PLMN. For example, the Session Management NF in VPLMN needs to request the Session Management NF in HPLMN to allocate the User Plane functions in HPLMN for the home routed PDU Sessions. NF_A sends NF Discovery Request including the Function Type of NF_B, PLMN ID and/or the service related parameters to NF Repository Function in VPLMN, e.g. the PDU type of the PDU session.

2. NF Repository Function in Local PLMN identifies NF Repository Function in Remote PLMN based on the PLMN ID, and it sends NF Discovery Request including Function type of NF_A, Function Type of NF_B, and/or the service related parameters to NF Repository Function in Remote PLMN.

3. NF Repository Function in Remote PLMN checks whether the request is allowed.

4. If the request is allowed, NF Repository Function selects the candidate of NF_B's instance based on e.g. the load level of NB's instance and provides to NF Repository Function in Local PLMN by NF Discovery Response message. Alternatively, the NF Repository Function in remote PLMN provides a list of NF instances of the requested Function Type, together with their associated IP addresses to the NF Repository Function in Local PLMN.

5. NF Repository Function in Local PLMN provides the candidate of NF_B's instance to NF_A by NF Discovery Response message. If in step 4 a list of NF instances are provided, the NF Repository Function in Local PLMN forward the list of NF instances of the requested Function Type, together with their associated IP addresses to NF_A. NF_A select a suitable NF_B to access from the list based on other information, e.g. weight factor.

6. NF_A access the NF_B instance based on the interface supported by NF_B, and the generic communication protocol is used to transfer the messages between NF instances.

One example for the NF discovery procedure in the EPC domain can be that the NF-A is the MME and the NF-B is the PGW.

6.7.2.2.5 NF Monitor

The NF instance periodically reports its status including e.g. load level, the abnormal status indication in case that the abnormal situation occurs to NF Repository Function. Based on that information the NF Repository Function can determine which NF instance (provider) is to be returned to the NF (consumer).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 315 of 501

After the NF Repository Function determines which target NF instance is for communication, the interactions between NFs include two scenarios:

- The request-response type interaction, which the NF does not need to maintain the session context. In this case the NF does not need monitor status of the peer NF.
- One session is established between the two NFs. In this case the NF need detects the status of peer NFs via e.g. periodically heart-beat message.

6.7.2.3 Solution evaluation

The solution addresses Key Issue 7 Work Task "Interconnection of NF". The solution proposes NF Repository Function maintains the profile of the deployed NF instance and support NF selection and discovery, and the NF directly interacts with the peer NFs after performing NF selection and discovery.

The impact on OAM system is OAM system needs to interact with NF Repository Function to support NF Registration and NF monitor.

The impacts on NF instance include: NF instance needs to interact with NF Repository Function to enable NF Selection and Discovery, and the NF itself directly interconnects with the peer NF instance.

The following benefits are supported:

- Supports the potential diverse requirements on NF selection and discovery; NF Repository Function proposed by the solution maintains the profile of the deployed NF instance in the network, and it is able to provide the correct NF instance to the requesting NF based on the received NF discovery request;
- Support direct interconnection between NFs: The NF (function consumer can directly interact with the NF (function provider) via the interface message supported by the NF (function provider). The direct interaction among NFs avoid introducing intermediate NF and impact on other NFs, and the delay on the NF interaction can be minimized as possible to address the requirement on performance and efficiency.
- Support the reusable function interface of NF. The function interface of NF (function provider) allows the NF (function provider) to provide its functionality to other NFs (function consumer), and the interface messages can be reusable to avoid the specific interaction message defined between the two NFs.
- Support the authorization on NF Discovery. The NF Repository Function maintains the profile of the deployed NF instances, and the authorization of NF discovery can be supported by NF Repository Function based on operator policy e.g. the dependence relationship between NFs.

6.7.3 Solution 7.3: Interconnection Function Solution

6.7.3.1 Architecture description

Editor's note: This clause will contain e.g., terminology, overview, architecture description of the solution.

This section addresses the WT#1 of key issue 7 on Network Function interconnection. In the following description, the Network Function refers to Network Function Instance.

The **Network Function Repository Function** stores the local Network Function information, including the IP address of the Network Function, Network Function type. ANetwork Function queries the NF Repository Function to retrieve the list of all NF instances of any NF type, together with their associated IP-addresses. When a Network Function is instantiated, it sends registration to NF Repository Function. When the Network Function is torn down, it sends deregistration to NF Repository Function. When Network Function needs to communicate with another Network Function, it asks for the IP address(es) of all instances of the target Network Function type from the NF Repository Function.

Direct communication is used between any two Network Functions. See the following figure for direct communication. The NGx/NGy/NGz interface is per Network Function pair.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 316 of 501

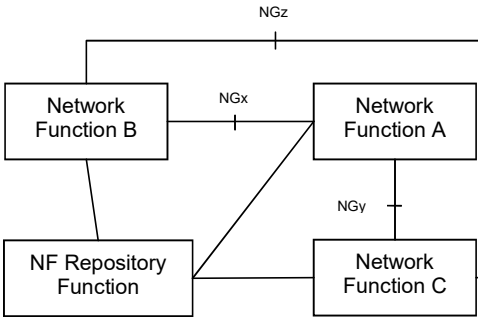


Figure 6.7.3.1-1 Direct NF communication

Editor's note: It is FFS if Network Function Repository Function is a separate repository or DNS can be re-used for that purpose.

In case direct communication between Network Functions is not possible, for example if one operator doesn't want to exposure its Network Function interfaces to other operators, indirect communication could be used. In this case the Network Functions may be registered in different Network Function Repositories. Interconnection Function may be used for indirect communication. See the following figure for indirect communication.

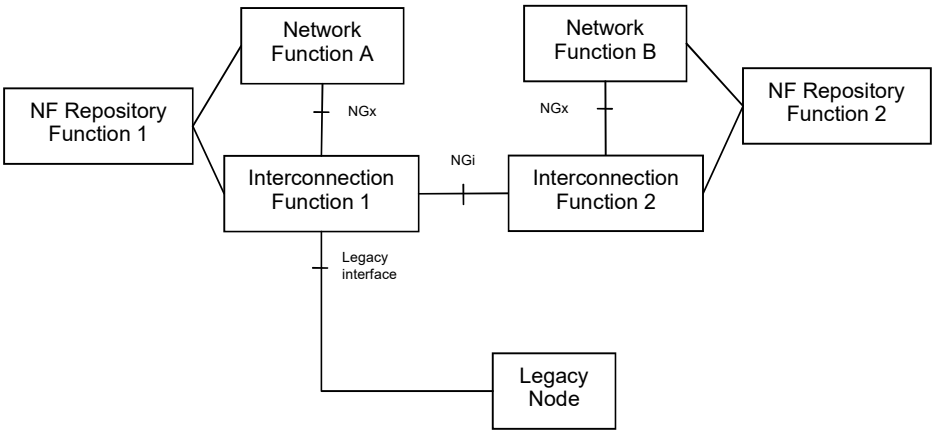


Figure 6.7.3.1-2 Indirect NF communication

The **Interconnection Function** is an intermediate function which provides routing function for indirect communication between two Network Functions, or is used for interworking with legacy Node. The NGx interface is per Network Function pair(i.e. between Network Functions which handle the session messages). The Interconnection Function doesn't handle session messages. The NGi interface is a common interface between the Interconnection Functions. The Network Function communicates to the Interconnection Function directly. For the case of interworking with Legacy Node, the Interconnection Function may perform application layer protocol conversion.

NOTE 1: There could be multiple Interconnection Functions on the message routing path.

Editor's note: It is FFS whether the Interconnection Function and NGi interface are within the scope of 3GPP.

NOTE 2: NGx, NGy, NGz and NGi interfaces are proposed to be 3GPP reference points.

6.7.3.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

This section addresses the WT#2 of key issue 7 on Network Function interconnection.

The following is a message flow example to establish direct communication and indirect communication connectivity between two Network Functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 317 of 501

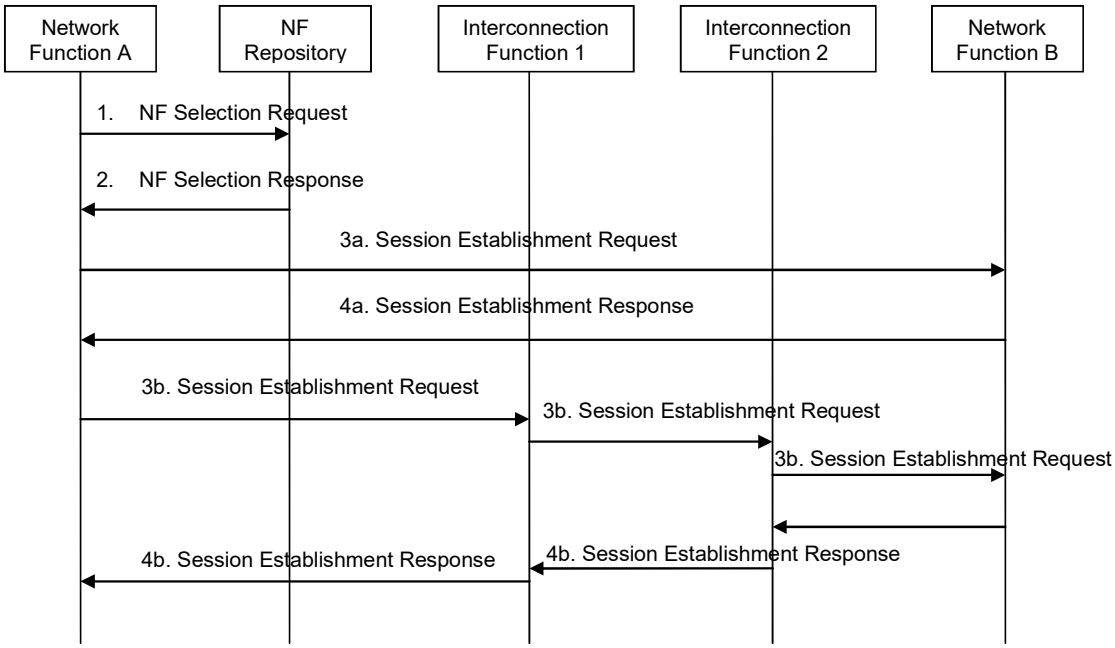


Figure 6.7.3.2-1 Message flow to establish session between two Network Functions

Step 1, The Network Function A decides to establish a new session with a Network Function of type B. It sends Function Selection Request message to Network Function Repository Function, including the Requested Network Function Type.

Step 2, The Network Function Repository Function sends Function Selection Response message including the list of all instances of the requested type (B) together with their associated IP addresses.

Step 3a, If the Network Function Repository Function responds with one or more IP addresses of the Network Function B, Network Function A selects one of the instances and sends Session Establishment Request message to that instance of Network Function B directly, including necessary information for session establishment.

Step 3b. If the Network Function Repository Function response with an list of all instances of the Interconnection Function with their associated IP addresses, the Network Function A selects one of the instances and sends Session Establishment Request message to that instance of Interconnection Function 1, including necessary information for session establishment. The Interconnection Function 1 may decide the Interconnection Function B address by using DNS mechanism or by pre-configuration. The Interconnection Function 1 forwards Session Establishment Request message to Interconnection Function 2. The Interconnection Function 2 performs Network Function discovery procedure as described in step 1 and 2. The Interconnection Function 2 forwards Session Establishment Request message to the instance of the Network Function B.

Step 4a, The Network Function B establishes the session context per request and sends Session Establishment Response to Network Function A directly.

Step 4b, The Network Function B establishes the session context per request and sends Session Establishment Response to Interconnection Function 2. The Interconnection Function 2 forwards Session Establishment Response to Interconnection Function 1. The Interconnection Function 1 forwards Session Establishment Response to Network Function A.

Editor's note: It is FFS whether the selection of the instance of B may be done with assistance of a 3rd Network Function. The 3rd Network Function may then provide the selected instance of B to A prior to the Session Establishment Request in step 3. The reason for doing it this way would be that A might not be able to access all information needed to do the selection, for instance subscription data, geographical location of a UE, etc.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 318 of 501

6.7.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.7.4 Solution 7.4: A Framework of Modular Network Functions

This solution proposes a reference model for a modular network architecture based on the ability of direct communication between those NFs. It defines a reference model, both for Control plan and User plane that enables granularity and modularization to fulfil dynamic deployment of network functions according to the requirements of the different use cases coming from the vertical businesses. It relies on sec. 6.7.1 or 6.7.2 for the interconnection of the NFs.

NOTE: The detail of the NF information exchange is FFS

6.7.4.1 Reference Model

Figure 6.7.4.1-1illustrates the reference model for modular network architecture. It depicts the model for a logical network providing communication service to a population of UEs via an Access Network (AN) served by the NextGen Core.

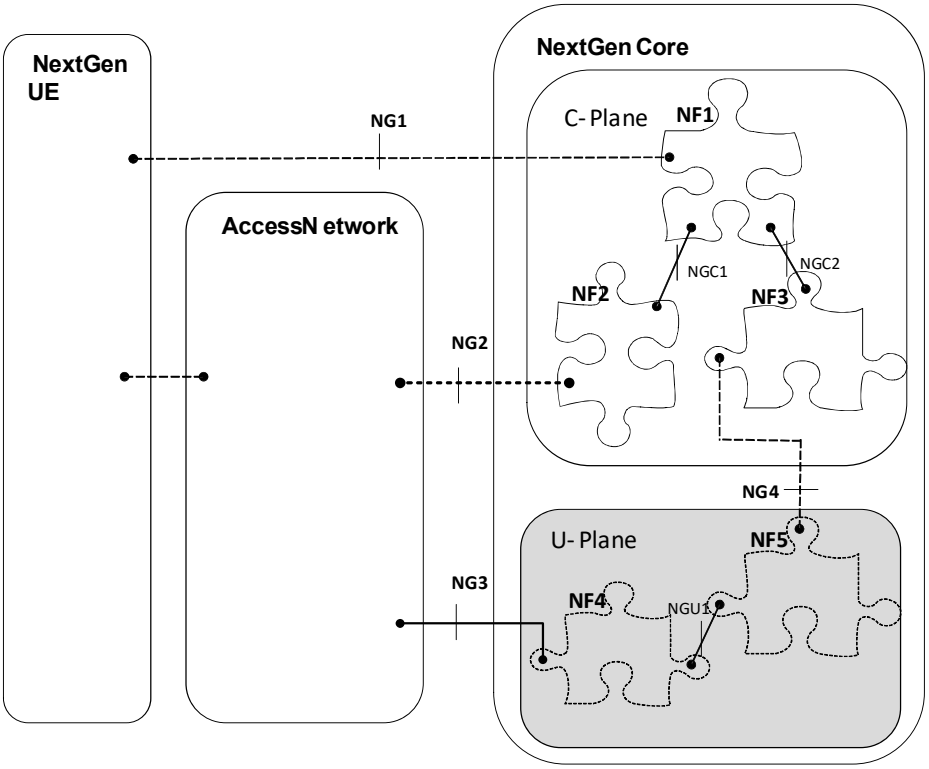


Figure 6.7.4.1-1: Architecture Modularisation Reference Model

6.7.4.2 Functional Description

NOTE: Details on the functional description of modular network functions is FFS.

6.7.4.3 Composition of Network Function

The NextGen Core architecture is composed by interconnected Network Functions (NFs, e.g. NF1, NF2, NF3, NF4 and NF5 are depicted) which exchange information directly with each other.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 319 of 501

NOTE: Exchanging information via direct reference points does not mandate any specific routing functionality. E.g., routing of messages between two given function can be done in accordance to principles described in section 6.7.1 or 6.7.2

Each NF can have different flavours of implementations.

Different NFs compose the Control Plane and the User Plane. In the Figure 6.7.xx, NFs composing the Control Plane are drawn with continuous line (NF1, NF2 and NF3), while NF composing the User Plane are drawn with dashed line (NF4, NF5).

NOTE: The reference model provides a high level principle for modularization, the specification of reference points and explicit detailed definition of NFs is FFS.

6.7.5 Solution 7.5: Control Plane Interconnection model with a Data Layer

Editor's note: The solution was updated based on S2-166284 although not all aspects of S2-166284 were fully discussed due to lack of time.

This is a solution for key issue #7 and key issue #9.

The main principle of this solution is to store (expose) UE related context data to a data layer. This can include both near real-time storage of structured data and opaque data.

It addresses Key Issue #7 as it impacts how Network functions interact with each other.

It addresses Key Issue #9 as it impacts how and what data can be exposed within MNO domain and to 3rd party.

6.7.5.1 Architecture description

6.7.5.1 Reference model

This solution assumes the following reference model for non-roaming and roaming Data Layer interconnection model.

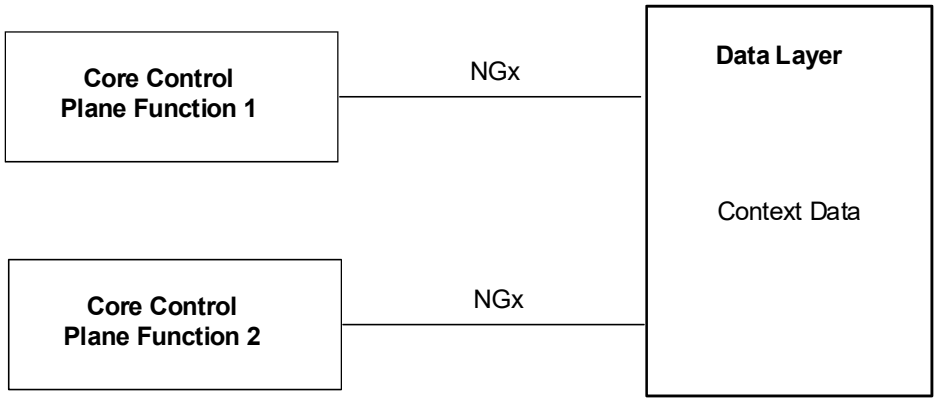


Figure 6.7.5.1-1: Non-roaming Data Layer interconnection model

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 320 of 501

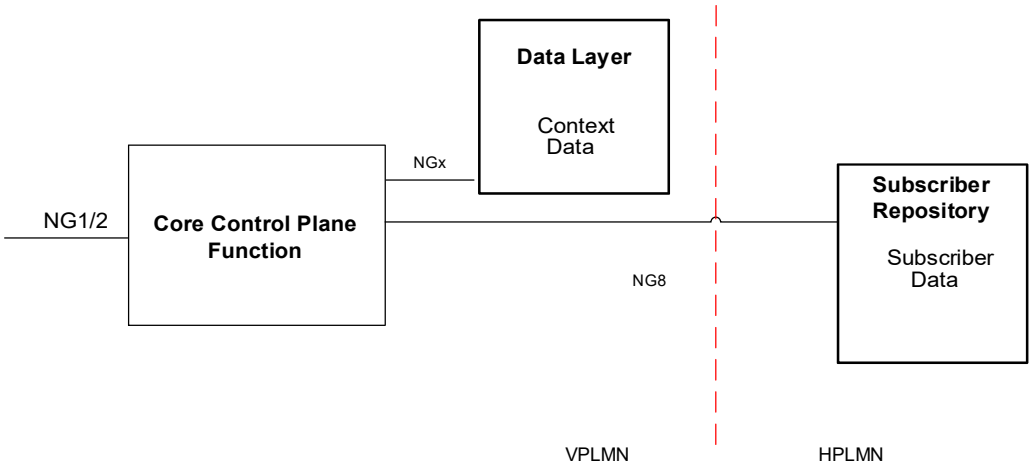


Figure 6.7.5.1-2: Roaming Data Layer interconnection model

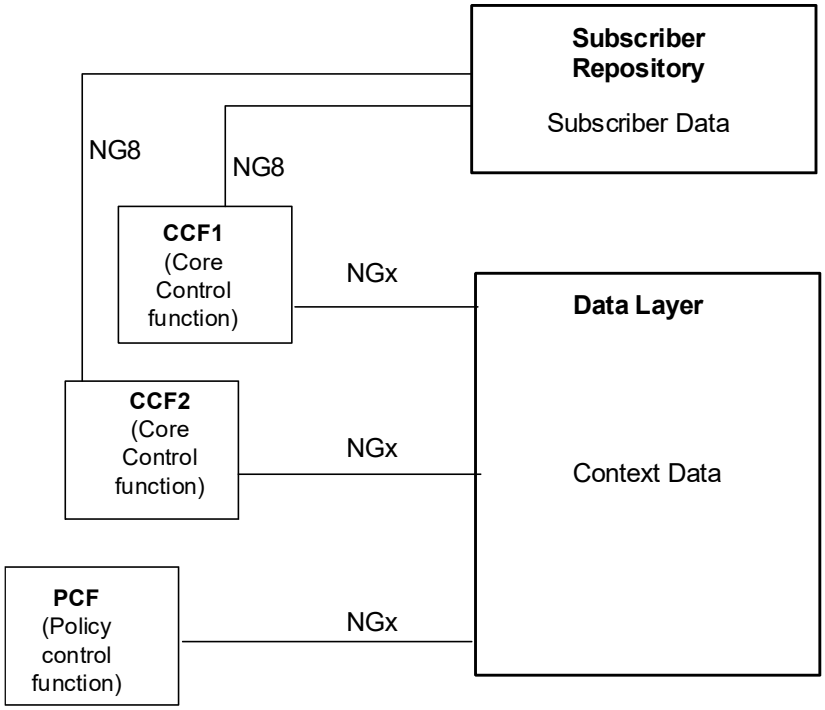


Figure 6.7.5.1-3: Data Sharing between Core Network Nodes

NOTE: The location and component(s) of the Data Layer(s) is up to deployments to decide.

It should be noted that access to Context Data and Subscriber Data have different characteristics in terms of expected location, frequency of data access etc. While the subscriber data can be placed in a centralized location (e.g. NG SDM/HSS), context data (context data for a certain network function) should be placed close to the network function to reduce latency for data access and to meet the necessary performance criteria. Data may be stored in a distributed or

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 321 of 501

centralized manner. The data can be replicated across multiple locations transparently for the application. If context data is placed close to a network function for performance criteria reasons, then context data for this network function (e.g. CCF) can only be exchanged via the data layer if the involved functions (e.g. two CCFs) are both located close to the data layer.

NG8: Reference point between the Core Network Functions (e.g. CCF, PCF) and the Subscriber Repository.

NGx: Reference point between the Core Network Functions (e.g. CCF, PCF) and the Data Layer.

6.7.5.2 Architecture principles

Editor's note: This clause will contain e.g., terminology, overview, architecture description of the solution.

Following are the architecture principles that are proposed for the control plane interconnection model:

1. The solution supports distributed and near real time storage of data as primary or secondary storage, both for structured and opaque data.

2. NFs require direct message centric interfaces with other NFs in addition to data centric interface via the Data Layer. This statement implies that messages can be exchanged (e.g. create session request, update session request) via network functions with direct interface.

3. Network functions store UE context into data repository. It is assumed that UE context such as UE MM, Security context information (e.g. context information exchanged via messaging as part of the EPC architecture) may be shared across network functions.

4. Allows any Network function to use the single interface (i.e. the same service with one interface) provided by the data layer. So even if a new Network function is being introduced, the single interface exposed by data layer can be re-used (without having to introduce a new interface for new network function).

Following are some assumptions on the type of contexts. There are two types of contexts:

1) Context used for NF resiliency: Certain network function (e.g. MMF) can store the UE contexts in the data layer in order to support network function resiliency. In this case, Network function reads the context at the beginning of MO/MT procedure, marks itself as the serving network function for the given UE and updates the context in the data layer upon completion of the procedure.

2) Context shared across NFs: Multiple network functions (e.g. MMF, SMF, PCF) may store some contexts in the data layer in order to support exposure functionality. In this case, storage of context is event driven depending on the type of context (e.g. upon UE reachability indication, ULI can be stored).

Editor's note: In case two (or more) NFs interact by direct messaging (e.g. to send a create session request) and via the data layer (e.g. to send location information): how can it be ensured that the information transferred via the data layer reaches the target function before the direct messaging reaches the target function? Alternatively (if this cannot be ensured), it is FFS which information can be safely send via the data layer in parallel to direct messaging without causing race conditions, e.g. because the target function operates on this information such as PCF, which takes ULI into account for policy decisions).

Editor's note: The solution illustrates user location information (e.g. TAI, Cell ID) , UE MM context can be stored and exchanged via Data Layer. Identification of all other information that can be exchanged via Data Layer is FFS. This also depends on the outcome of 5G architecture, relevant solutions (i.e. needed context transfer information) for Key Issues such as MM, SM, QoS. Network Slicing etc.

6.7.5.3 Function description

6.7.5.3.1 Data Layer (DL)

The Data Layer (DL) consists of session data. It provides the following services:

1) distributed and near real-time storage of structured UE context such as MM, SM related context information (i.e. allowing the control plane function to create, read, update, delete their own data and subscribe to notifications upon data change);

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 322 of 501

2) In addition, opaque data can also be stored by the network functions. The network functions can use data layer to store opaque data as a secondary storage and also optionally use it for primary storage. Whether the network function uses the data layer for primary storage for opaque data can be an implementation choice.

3) The possibility of data sharing between same type of Core Network Functions as in Figure 6.7.5.1-1 and different type of Core network functions as in Figure 6.7.5.1-3; In the latter case, it is also assumed that only the network function that stored the data owns the data (e.g. a CCF creates, updates, deletes the own data such as ULI) and other network functions can access it or subscribe to notifications upon data change (i.e. PCF subscribes for ULI and reads the ULI information).

NOTE: This data ownership rule implies that sharing of data across network functions of different type can only be used for data that is provided/modified by a single network function type only (e.g. ULI provided by MM function).

4) Provides a unified way how UE context and session context is stored across network functions. This also helps avoid signalling incurred due to transfer/synchronization of data between Core Control Plane Functions.

5) Allows "compute" (Network function) to be decoupled from the "storage" (data layer) functionality thus improving the resiliency of a Network Function. Also Network function resources do not need to be used for idle UEs, e.g. the Data Layer can store UE contexts for a massive number of IoT devices and Network functions need only to be involved for the active devices.

6) Helps ease the support for data analytics and network capability exposure.

7) Data Layer exposes one interface for any network function that needs to leverage the services of Data Layer. This helps eases the introduction of new network functions as the same interface can be reused (and a new interface need not be introduced).

Editor's note: In case NFs interact by direct messaging and via the data layer: how can it be ensured that the information transferred via the data layer reaches the target function before the direct messaging reaches the target function?

6.7.5.3.2 Core Control Plane Function (CCF)

This is a 3GPP defined network function capable for processing UE specific transactions.

Network functions can use direct message centric interfaces with other NFs in addition to data centric interface via the Data Layer. This statement implies that messages can be exchanged (e.g. create session request, update session request) via network functions with direct interface.

Following are some assumptions to ensure that there is no synchronization issue regarding contexts for NF resiliency:

1) If the Network function uses the data layer for storing, updating and retrieving certain context information, then it always uses the data layer for storing and retrieving the corresponding context information.

2) At the beginning of the procedure (triggered either by the UE (Uplink MO request) or the network (based on Downlink transaction), the network function reads the context information for the UE and stores its information as serving network function for the given UE.

1) When a procedure (e.g. complete attach procedure, Service request procedure) is being processed, the network function is assumed to store the UE context information within its cache. In other words, the network function is considered to store UE contexts when it is serving the UE (i.e. processing a certain procedure such as attach).

2) Upon completion of the whole procedure, it can update the data layer with its context information and cancel the serving node information.

Use of data layer does not preclude NFs to maintain a "Context Information" Cache for Performance Optimization reasons within the network function. If it is using both the data layer and the cache, the network function shall ensure synchronization of context. Some NFs may support Data Layer Function, but additionally maintain a local cache for Sessin State storage, with a lazy flush into Data Layer for Performance Optimization reasons.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 323 of 501

Editor's note: How the stateless CCF is selected is FFS. How to ensure that the same CCF is selected for subsequent transactions from the UE/RAN or other network functions (while a previously selected CCF still holds state for the same UE is FFS.

6.7.5.4 Information exchange across different types of Network functions for capability exposure

These calls flows illustrate how Network functions exchange structured data across different type of Network functions. The call flows in this section make no assumption on whether network functions are stateless or not.

6.7.5.4.1 Capability Exposure to PCF, CEF

Contents stored in the data layer can be leveraged to support network capability exposure (both within MNO domain, outside MNO domain) and to perform data analytics. This can include exposure of capabilities such as UE reachability, location of the UE, change in location of the UE of the UE, roaming status, success/failure of registration events, success/failure of PDU session establishments for KPI calculation etc.

Figure 6.7.5.3.6-1 shows the example call flow for a UE location being reported to PCF, CEF.

User Location (changes) are notified to the PCF, CEF (e.g. for exposure, for data analytics) via subscribe/notify procedure. Access to read/subscribe to User Location needs to be controlled by the VPLMN to enable a network entity from a particular PLMN to access the ULI of a particular UE under the control of the CCF and/or the data layer.

Context data stored in the data layer is meant for exposure (e.g. publication of ULI change) i.e. for the case where the producer of the information does not need an ack. Such data can be replicated in a central location and no synchronization issue is expected.

This call flow makes the following assumption:

1) When CCF has an indication that it needs to provide User Location information, it stores the ULI information in the data layer whenever it gets a trigger (e.g. MO transaction, notification from RAN etc) that there is a change in User location information.

2) When network functions such as PCF, CEF require this information, it subscribes for this information with the data layer.

3) When Data Layer receives an update from CCF, it notifies the registered network functions (PCF, CEF)

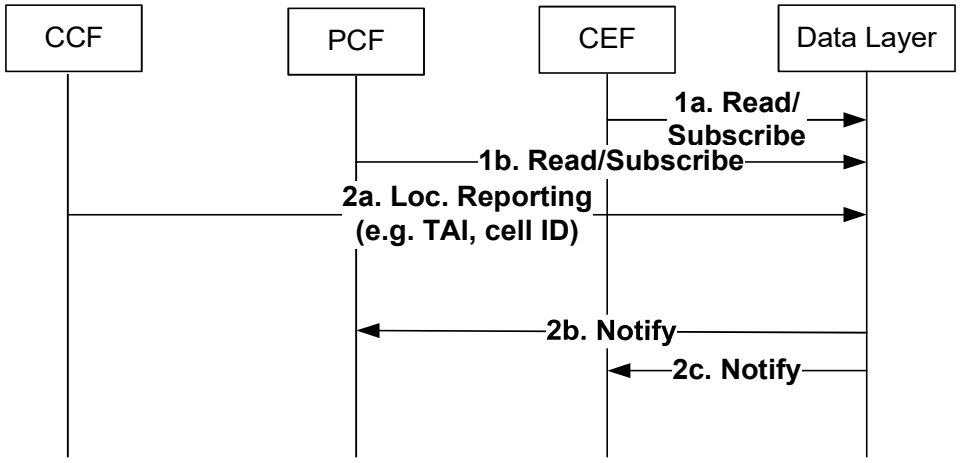


Figure 6.7.5.4.1-1: User location Information subscription and notification

6.7.5.5 Information exchange across same types of Network functions

These calls flows illustrate how Network functions exchange structured data both within the same type of Network functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 324 of 501

The network functions store UE context upon completion of a certain procedure. More specifically, it can be expected for the network function to store UE context information in the data layer based e.g. on the following triggers:

1) Completion of registration (e.g. attach/TAU) procedure.

2) When the UE transitions from active to idle mode (i.e. release of NG2/1 signaling connection).

3) Completion of HO procedure

It is expected that the network function has the knowledge to determine the appropriate time for storing UE context information thus it can decide the optimal trigger for storing context information in the data layer.

NOTE: Although some call flows in the subsequent sections assume CCF as a single network function, solution does not preclude a split CCF configuration. Even if the CCF is split into MMF, AUF and SMF, then the split network functions can share UE context via data layer.

6.7.5.5.1 Registration procedure

Figure 6.7.5.4.1-1 shows an example call flow of a UE initial registration (i.e. attach/TAU). In this example, as part of the previous registration, the old Core Control Plane Functions (CCF) stored UE context data (including subscription data downloaded from the SDM) in the Data Layer; the new and the old CCF share the context data via the Data Layer.

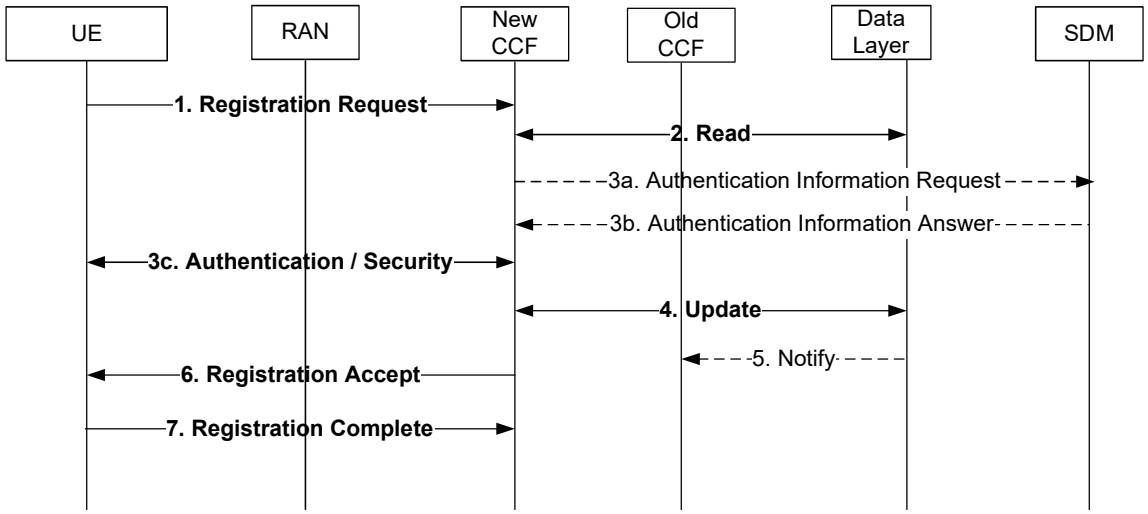


Figure 6.7.5.5.1-1: Registration Procedure

Figure 6.7.5.5.1-2 shows an example call flow of a UE initial registration (i.e. attach/TAU) when CCF is split into multiple network functions – MMF, AUF and SMF (SMF is not involved as part of this procedure thus not shown).

The call flow below makes the following assumption:

1) Only MMF stores and reads the UE context to/from the data layer.

2) MMF is not exposing UE context in the data layer for other network function.

Editor's note: how the procedure works when multiple network functions (e.g. MMF, AUF) use the data layer is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 325 of 501

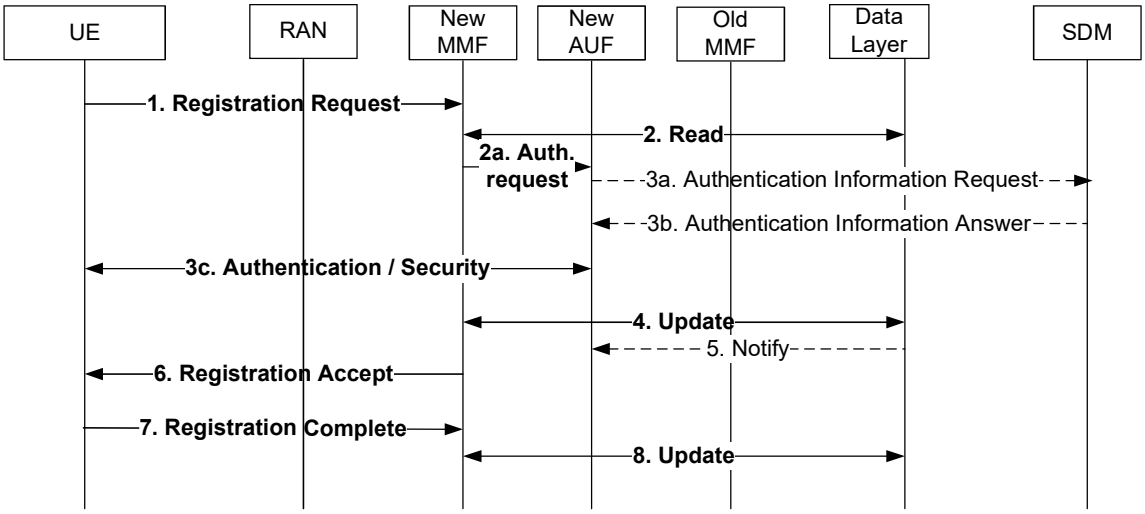


Figure 6.7.5.5.1-2: Registration Procedure with split CP functions

1. The UE initiates the Registration procedure by the transmission of an Registration Request. The Message will carry appropriate information such as IMSI, IMEI or TempID to identify the UE.

2. Upon reception of Registration Request message, the new CCF queries the Data Layer for the UE context data and marks itself as the serving node. The UE context data contains the UE MM context (such as last visited TAI, UE capabilities, DRX parameters), security related information (such as authentication vectors KASME, NAS Sequence number), subscription data downloaded from the SDM.

NOTE: There is no Identification Request (Attach) nor Context Request (TAU) sent towards the old CCF, as the data will be retrieved from the Data Layer.

3. If new authentication data is needed, then in steps 3a, 3b, 3c the new CCF sends Authentication Information Request to the SDM and receives Authentication Information Answer.

3d. Authentication and Security procedure is carried out.

NOTE: There is no need to send a Update Location Request to the SDM.

4. The new CCF updates the UE context data in the Data Layer.

5. The old CCF is notified about the change of CCF assuming old CCF was subscribed to such a notification.

6. The new CCF sends a Registration Accept message towards UE to indicate successful Registration procedure.

7. The UE acknowledges the reception of the Registration Accept message.

6.7.5.5.2 Handover Procedure

Figure 6.7.5.5.2-1 shows an example call flow of X2 (like) Handover. In this example, as part of the previous procedure (e.g. registration procedure), the source Core Control Plane Functions (CCF) stored UE context data (including subscription data downloaded from the SDM) in the Data Layer; the target and the source CCF share the context data via the Data Layer.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 326 of 501

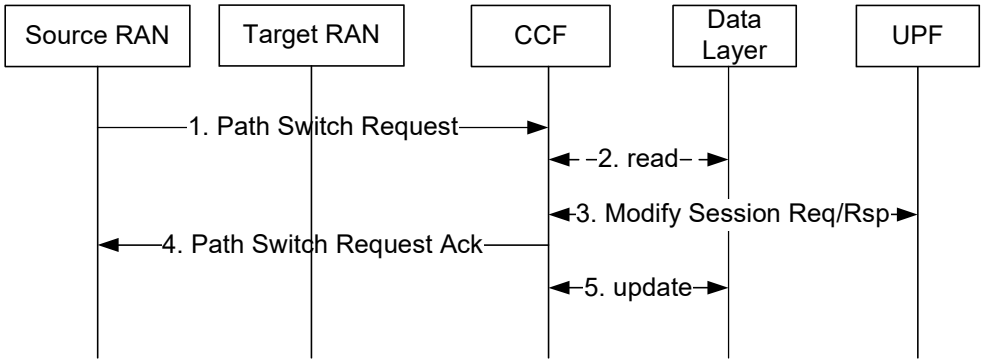


Figure 6.7.5.5.2-1: X2 (like) Handover

NOTE 1: X2 (like) Handover would become possible even with a change of CCF, provided the target and source CCF share the context data via the Data Layer.

Figure 6.7.5.5.2-2 shows an example call flow for NG2 (like) Handover. In this example, as part of the previous registration, the source Core Control Plane Functions (CCF) stored UE related data (including subscription data downloaded from the SDM) in the Data Layer; the target and the source CCF can share the context data via the Data Layer.

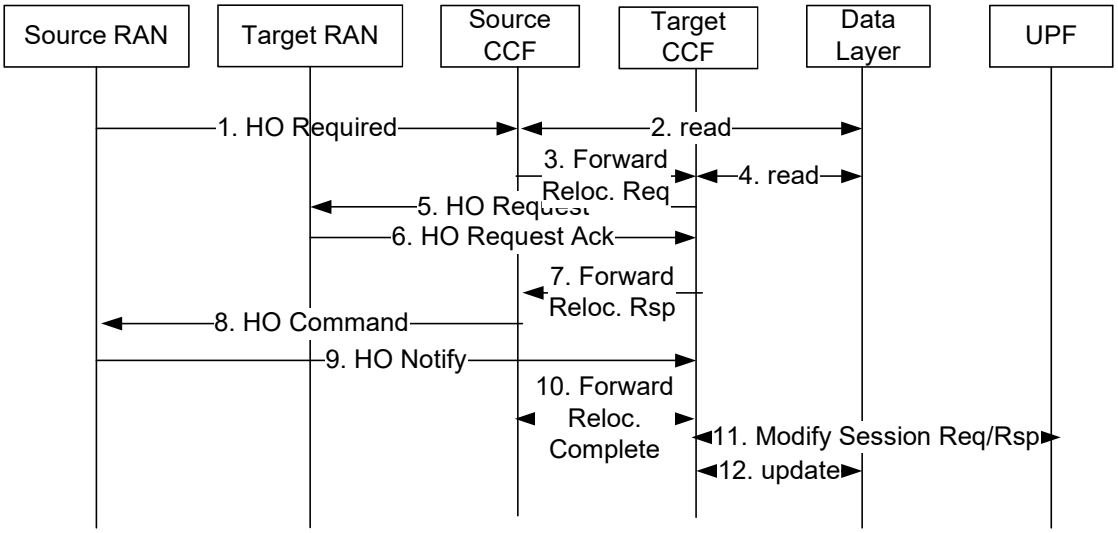


Figure 6.7.5.5.2-2: NG2 (like) Handover

2. The source CCF does not need to include the UE's context in the Forward Relocation Request (resulting in a much lighter message). Upon reception of the Forward Relocation Request message, the target CCF queries the Data Layer for UE's context for that specific UE.

NOTE 2: There is no need to send a Update Location Request to the HSS FE.

6.7.5.5.3 Service Request Procedure

Figure 6.7.5.5.3-1 shows an example call flow for a UE triggered service request.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 327 of 501

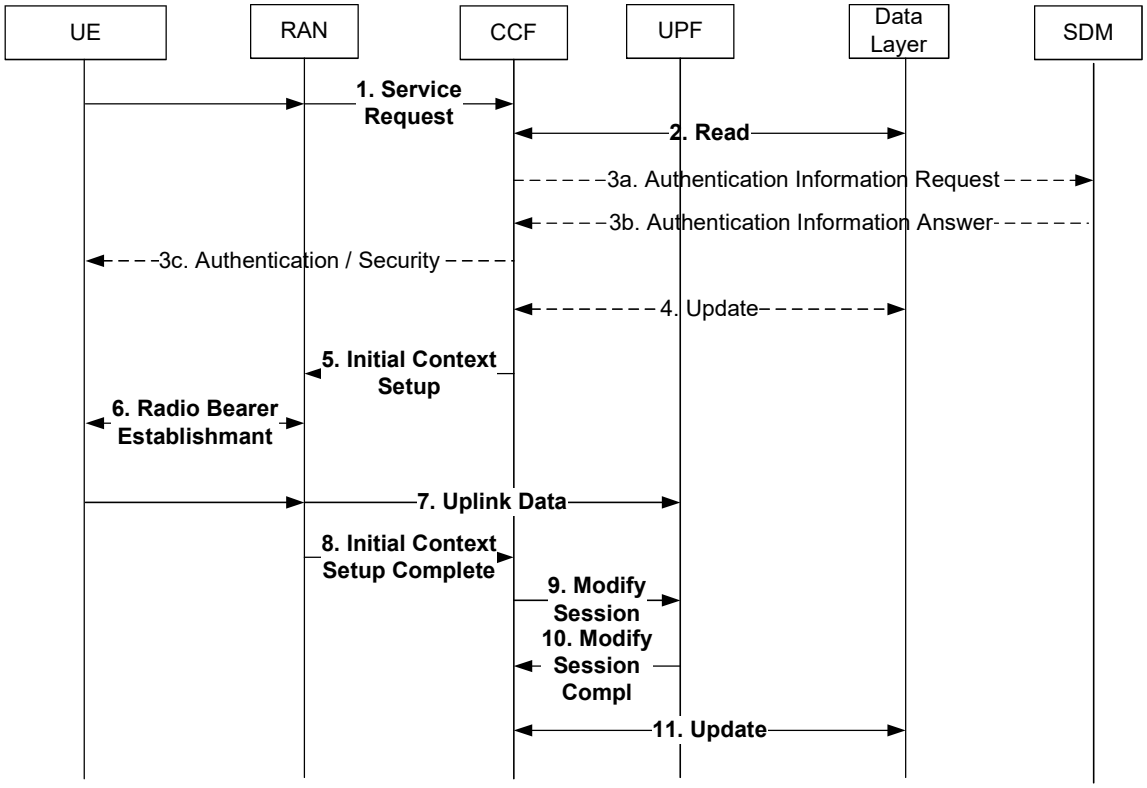


Figure 6.7.5.5.3-1: Service Request

1. The UE sends the Service Request towards the CCF encapsulated in an RRC message to the eNodeB. The RAN forwards the Service Request message towards the CCF.

2. Upon reception of the Service Request message, the new CCF queries the Data Layer for the UE context data. The UE context data contains the UE MM context, security related information, subscription data downloaded from the SDM, PDN connections contexts as well as possible other parameters.

3a – 3c. If new authentication data is needed, then in steps 3a, 3b, 3c the new CCF sends Authentication Information Request to the SDM and receives Authentication Information Answer.

4. If the optional Authentication and Security procedure has been carried out, then CCF updates the Data Layer. The new security context is sent to the Data Layer.

5. The new CCF sends Initial Context Setup Request message to RAN. The message contains UPF address and additional parmeters.

6. The RAN performs the radio establishment procedure.

7. The UE can send Uplink Data which are forwarded by the RAN to the appropriate User Plane entity.

8. The RAN sends a Initial Context SetupComplete message indicating successful completion of the procedure and containing relevant parameters.

9 -10 The CCR sends Modify Session Request and receives Modify Session Complete.

11 The CCF updates the UE context in the Data Layer with the activated sessions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 328 of 501

6.7.5.5.4 MMF Failover

Figure 6.7.5.5.4-1 shows the example call flow of a UE initiating signalling towards the Core Mobility Management Function (e.g. Mobility Management signalling) after a MMF failure.

The new MMF serving the UE (MMF 2 in the call flow) accesses the UE context data stored in the Data Layer and proceeds with the UE request successfully.

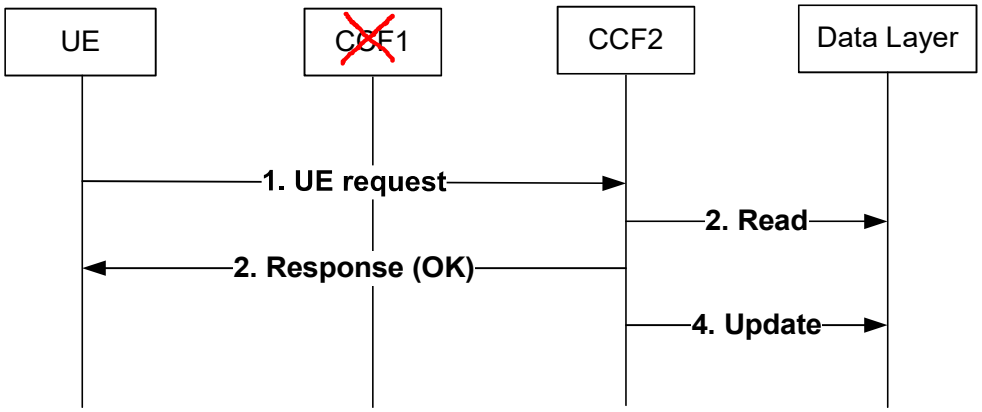


Figure 6.7.5.5.4-1: MMF Failover

The restoration procedures specified for EPC requires the capability for a restarted or alternative MME to store and retrieve UE context data (e.g. eDRX parameter negotiated with the UE, temporary identities, paging area, etc), see e.g. sub-clause 25.2.3 of 3GPP TS 23.007 [x]. As this is achieved by vendor specific means, operators may need to deploy different solutions and restoration scenarios cannot be supported between MMEs from different vendors.

The Data Layer provides a uniform way for MMFs to store UE context data and to make them available to any other MMFs entities in restoration scenarios, thus allowing the continuation of the sessions and services provided to UEs after a CCF failure.

Editor's note: How recovery and restoration can be supported while a network function holds state (i.e. before it writes its state to the data layer) for scenarios where multiple network functions are involved (e.g. as part of a procedure involving multiple network functions) is FFS.

6.7.5.5.5 Context Clean-up scenario

Figure 6.7.5.3.5-1 shows the example call flow of a UE context clean-up triggered by CCF.

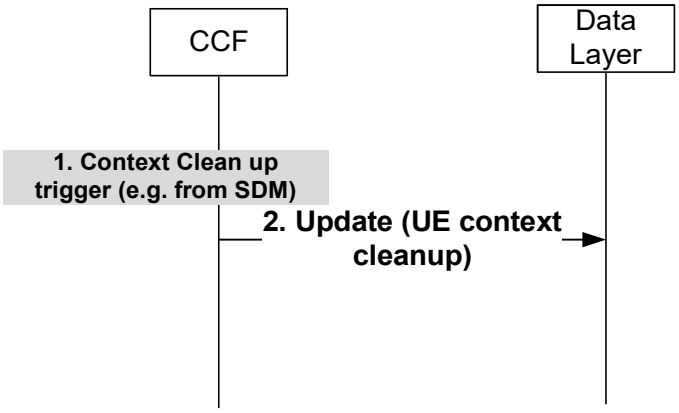


Figure 6.7.5.5.5-1: Context Cleanup

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 329 of 501

6.7.5.5.6 Data Layer and Network slicing

When a deployment supports network slicing, data layer can either be shared across network slices or support isolation requirement for isolated network slices (based on operator policies). Whether the data layer is considered to be a shared or an isolated resource depends on the type of network slice scenario supported in the network.

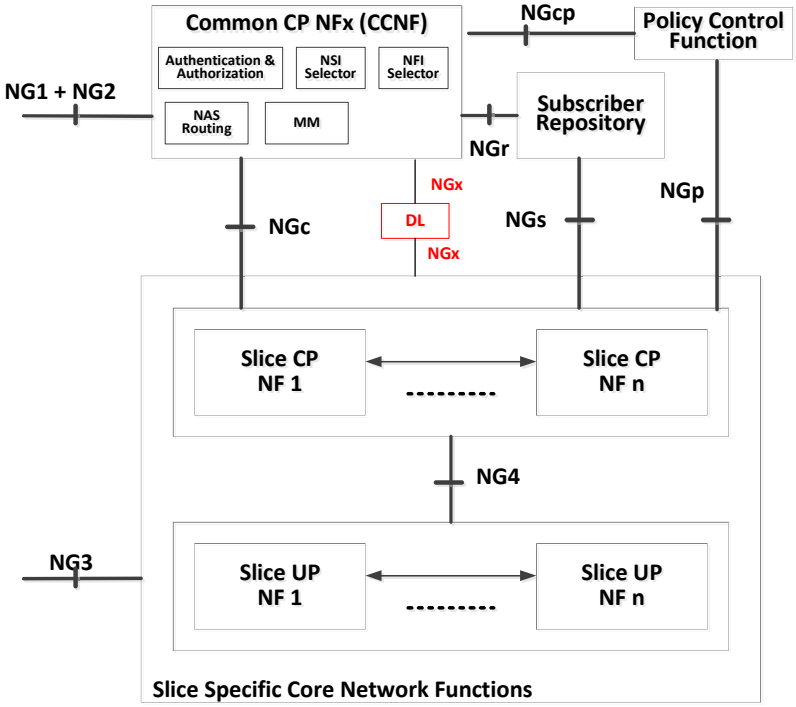


Figure 6.7.5.5.6-1: Core Part of Network Slicing concept (Non-roaming scenario)

6.7.5.6 Stateless Network Function

In addition to structured UE context information, network function can also store opaque data in the data layer and become completely stateless. In this case, the trigger for storage, update and retrieval is implementation specific.

A network implementation based on Network Functions only relying on standardised state information and using the data layer as the primary and only storage for their state information (both standardized and opaque data) could enable the following example scenario illustrated below:

At first UE attach RAN selects a CCF in the selected slice based e.g. on load balancing algorithms, For subsequent transactions RAN routes the NAS signalling from the UE to a CCF in the serving network slice based on the NSSAI provided by the UE and according the same logic, e.g. based on load balancing algorithms. If the CCF is stateless in a slice that receives the NAS message, it will retrieve the user's Context Data from the Data Layer and will execute the transaction.

Editor's note: Selection of stateless network functions needs to be further studied.

6.7.5.7 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 330 of 501

6.8 Solutions for Key Issue 8: Next Generation core and access - functional division and interface

6.8.1 Solution 8.1: Solution for Common Core support

6.8.1.1 Architecture description

Based on the high-level architecture requirements clause 4.1 and key issue#8 that were captured in this TR, the following presents the architecture framework for the NextGen system with Common Core based on the introduction of new network function, Multi-RAT Adaptation Function (MRA):

NOTE: The proposed architecture framework described here requires further analysis by RAN.

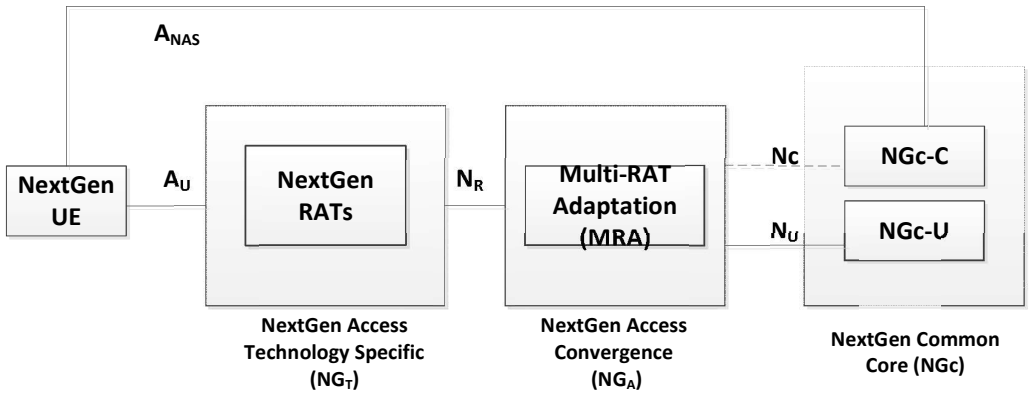


Figure 6.8.1-1: NextGen Architecture with Common Core Interface

Editor's note: The support for non-3GPP access, interworking with EPC and roaming architecture is FFS.

- The NextGen network is partitioned into three parts as shown in Figure 6.8.1-1 above:
  - NextGen Common Core part (NGC):
    - NGC consists of common NextGen core network functions to support the multiple accesses:- such as mobility control and anchoring support for session continuity, session management, core-level QoS management, subscriber management, policy management, access control, charging and accounting, gateway selection, roaming support etc.
  - NextGen Access Convergence part (NGA):
    - NGA consists of the Multi-RAT Adaptation (MRA) function which supports the 3GPP access, so that, an access technology specific function can be generalized into common access function for NGc to process and vice versa.

Editor's note: MRA support for non-3GPP is FFS.

    - The main functions of MRA are to support converged interface between NextGen access and NextGen Core, RAT specific mobility management (such as access restriction, paging, area registration, mobility state transition, etc.), etc.

Editor's note: Details on the access dependent network functions are FFS.

Editor's note: How NGA communicate with the NGc for subscription information is FFS.

  - NextGen Access Technology Specific part (NGT):

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 331 of 501

- NGT supports the access technology specific functions for the 3GPP accesses.

NOTE: The function of NGT is outside the scope of SA WG2.

- A common interface (i.e. NC) is defined between NGC and NGA
- Between NGA and NGT, the new interface, NR, is defined. NR may be different among different RATs.
- Between NGT and the NextGen UE, the new interface, AU, is defined.
- Between the NGc and the NextGen UE, the new interface, ANAS, is defined to support common access signalling (e.g. Session management, Authentication etc.) between the NextGen UE and the NextGen Core.

6.8.1.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.8.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.8.2 Solution 8.2: Architecture for decoupling and independent evolution of CN and AN

This solution addresses Key Issue #8, and in particular the following:

- identify how the functionality can be modularized for the definition of a modular Next Generation Core -ANs interface that minimizes access dependencies and applies to any access networks
- identify how to decouple the access network and the core network, and identify its effects and implications to the Next Generation Core. Such decoupling shall allow for parallel and independent design and evolution of access networks and core networks.

This solution is orthogonal to the discussion on detailed CN-RAN functional split. Whatever the CN-RAN split defined for 3GPP-only access, the same architecture proposed here applies to the case of non-3GPP access, with or without 3GPP cellular umbrella coverage.

6.8.2.1 Architecture description

Depicted in Figure 6.8.2.1-1 is a simplified system architecture that allows for decoupling and independent evolution of access network and core network. Three different deployment cases are illustrated, as follows:

Case 1: NextGen architecture with 3GPP access only.

Case 2: NextGen architecture with non-3GPP access under umbrella coverage of controlling 3GPP access.

Case 3: NextGen architecture with stand-alone non-3GPP access.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 332 of 501

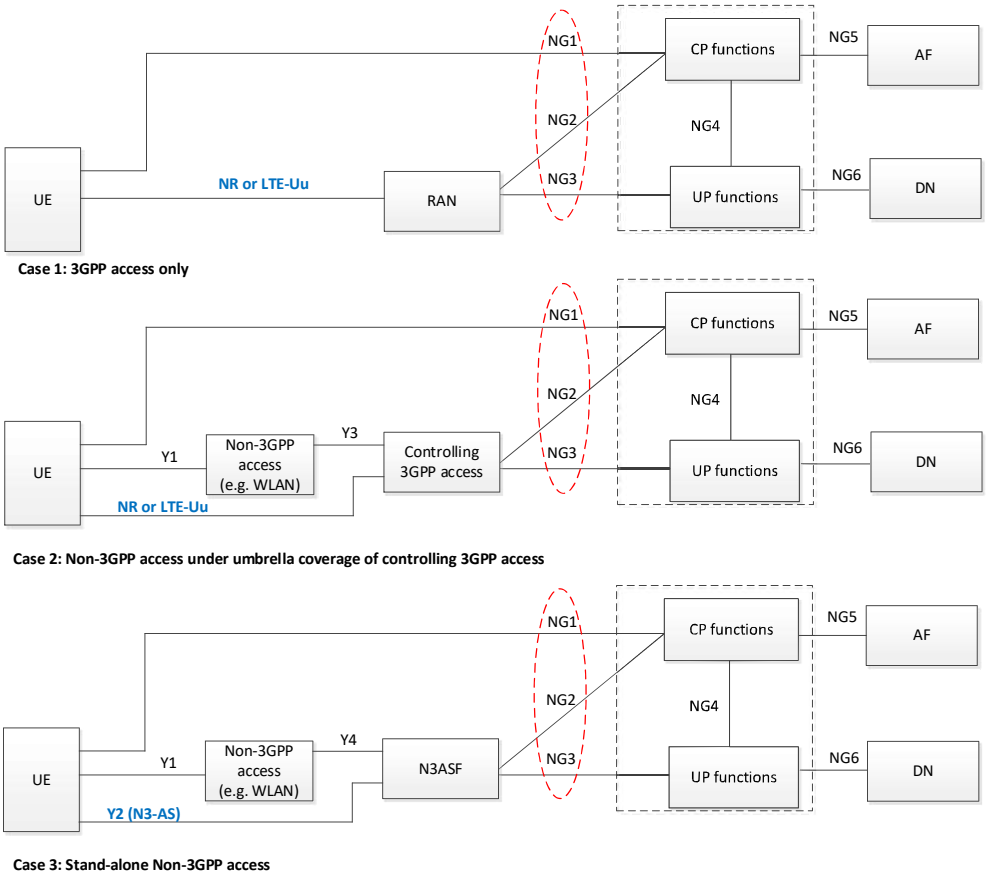


Figure 6.8.2.1-1: Architecture for decoupling and independent evolution of AN and CN

The Control plane functions of the NextGen core are assumed to be grouped into Control Plane functions (CP functions) and User Plane functions (UP functions).

In addition to the reference points described in Annex G, the following reference points are assumed for the purpose of describing the architecture for decoupling and independent evolution of AN and CN:

Y1: Reference point between the UE and the non-3GPP access (e.g. WLAN).

Y2: Reference point between the UE and the Non-3GPP Access Stratum Function (N3ASF). The protocol used over Y2 is referred to as Non-3GPP Access Stratum (N3-AS) protocol which may be transported on different protocols as depicted in 6.8.2.2.2, 6.8.2.2.3 and 6.8.2.2.4.

Y3: Reference point between the controlling 3GPP access and the non-3GPP access. Whether this interface is in scope of 3GPP is up to RAN WGs to determine.

Y4: Reference point between the N3ASF and the non-3GPP access. Whether this interface is in scope of 3GPP is up to RAN WGs to determine.

The following are the salient features of this solution:

- Case 2 architecture is similar to the LWA/LWIP architecture for LTE-WLAN aggregation/interworking defined in Rel-13.
- Case 3 architecture is similar to the GAN architecture for 3GPP-WLAN interworking defined in Rel-6.
- In all three cases a common set of interfaces (NG1, NG2, NG3) is exposed to the NextGen core network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 333 of 501

- Specific to Case 3, the architecture for support of standalone non-3GPP access is aligned with the initial high-level architecture view in clause 4.2.1 in that NG2/NG3 is used to connect the NG Core to the non-3GPP access network.

- Specific to Case 3, an intermediate Non-3GPP Access Stratum Function (N3ASF) is used to serve as NG2/NG3 termination. The N3ASF node is an operator node that is logically part of the non-3GPP access network.

- Specific to Case 3, the N3-AS protocol is used primarily for transparent transport of NAS messages between UE and N3ASF, as well as for exchanging information for the U-plane bearers between UE and N3ASF, including security information. In case untrusted WLAN is used, the IPSec tunnel transports the N3-AS protocol which carries the NAS message between UE and N3ASF. In case of trusted WLAN the N3-AS protocol is transported in a secure transport layer such as DTLS between UE and N3ASF.

- In all three cases a common NAS protocol is used between UE and the CN over NG1, though the UE may not use all the features of NG1 over all the scenarios.

- Specific to Case 3, in case the non-3GPP access is a WLAN, the following observations apply:

  - Given that there is no Idle/Connected mode distinction in WLAN, when connected over WLAN the UE appears to be in permanent Connected state.

  - Idle mode mobility procedures (e.g. Paging) are not needed, as well as procedures for switching between Idle and Connected mode (e.g. NG2/NG3 Release).

  - The N3ASF node, while logically part of the access network, can serve a geographical area of an arbitrary size. This is particularly true for the IKEv2 approach (see clause 6.8.2.2.3) which, being a layer-3 approach, has no direct linkage with the geographic location of the WLAN access point that it may traverse. In the EAP-over-EAPoL approach (a "layer-2" approach; see clause 6.8.2.2.2) the size of the N3ASF "serving area" may be limited by the number of Diameter interfaces that the N3ASF maintains with the WLAN access points with which it has pre-established security associations. Nevertheless, for any practical implementations the N3ASF "serving area" is expected to be sufficiently big so that UE mobility between areas served by different N3ASF is expected to be a very rare event. In the latter case the UE performs a full attach.

  - Connected mode mobility procedures (e.g. Path Switch) are unlikely due to the nomadic use of WLAN.

  - The user plane between UE and N3ASF can be similar to those used with trusted WLAN access and untrusted WLAN access flavours today.

  - NG2 procedures used with N3ASF are expected to be a subset of NG2 procedures used with NG RAN (e.g. some NG2 management procedures may not be needed).

- It is also possible to have a Case 1+3 scenario where the UE is simultaneously engaged in one connection with the network as described in Case 1, and in another connection with the network as described in Case 3. As illustrated in Figure 6.8.2.1-2,in this scenario the UE has two NG1 connections with the NextGen core, possibly using a subset of NG1 functionality on the Case 3 side. In the Case 1+3 the UE maintains two independent mobility management states for the two NG1 instances. For instance, UE can be in CN_Connected state on the non-3GPP access side and in CN_Idle state on the 3GPP access side.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 334 of 501

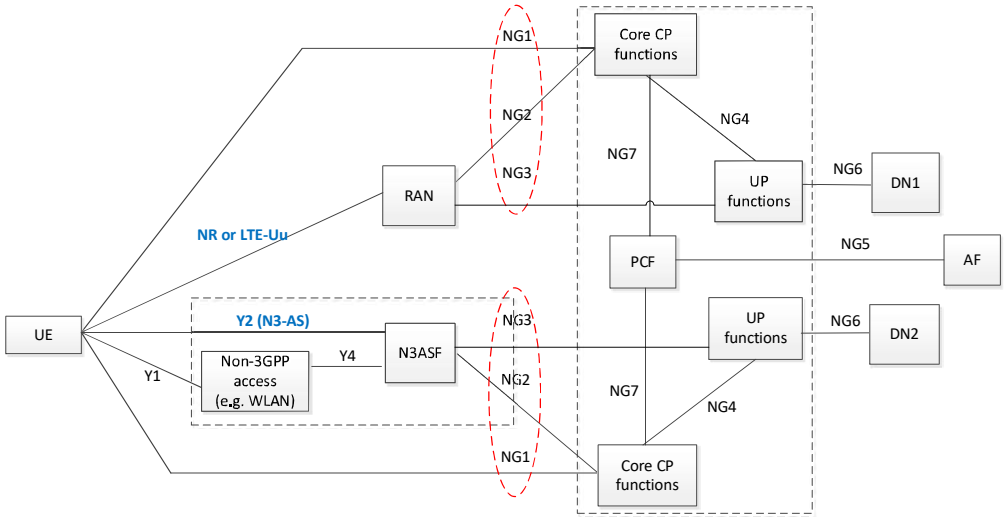


Figure 6.8.2.1-2: Architecture for Case 1+3

Editor's note: The roaming architecture is FFS.

6.8.2.2 Function description

6.8.2.2.1 General

This clause focuses on Case 3. It contains example call flows for the Attach procedure, as well as the NG1 protocol stack, for the following interworking approaches (all three for Case 3):

- EAP-over-EAPoL transport used between UE and the WLAN access point.
- IKEv2 [14] transport used between UE and the N3ASF.
- PANA [15] transport used between UE and the N3ASF.

The first approach (EAP-over-EAPoL) is specific to trusted WLAN.

The other two approaches (IKEv2 and PANA) are layer-3 approaches and can be applied to any non-3GPP access, including untrusted WLAN and fixed access without WLAN.

Editor's note: The transport protocols and call flows are provided as examples. The security aspects of the illustrated options (and any other alternatives) need to be studied by SA3. The actual protocols are to be determined by Stage 3 working groups.

In all three cases the authenticator function resides in the CP functions, as with 3GPP access.

The N3-AS protocol stack depicted in Figure 6.8.2.2.2-3 and Figure 6.8.2.2.3-3 is used when Attach procedure is complete and a N3-AS connection is bootstrapped between the UE and the N3ASF.The N3-AS protocol has two main functions:

- Transparent and secure transport of further NAS protocol messages.
- Information about U-plane bearers e.g. transport address, QoS, etc.

NOTE: While N3ASF is logically part of the Access Network, the N3-AS protocol functions do not rely on RAN WG expertise.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 335 of 501

6.8.2.2.2 EAP-over-EAPoL transport between UE and WLAN access point

The call flow in Figure 6.8.2.2.2-1 describes a possible Attach procedure via non-3GPP access without umbrella 3GPP coverage (Case 3) to a common NextGen core using a common CN-RAN interface. In this example EAP-over-EAPoL transport is used between UE and WLAN access point.

Editor's note: The call flow uses existing NAS message names (Attach Request, Attach Accept, Attach Complete) as well as existing S1-AP message names (Initial UE Message, DL/UL NAS Transport, etc.) for illustration purposes. Those names will be replaced with the actual message names defined for NextGen.

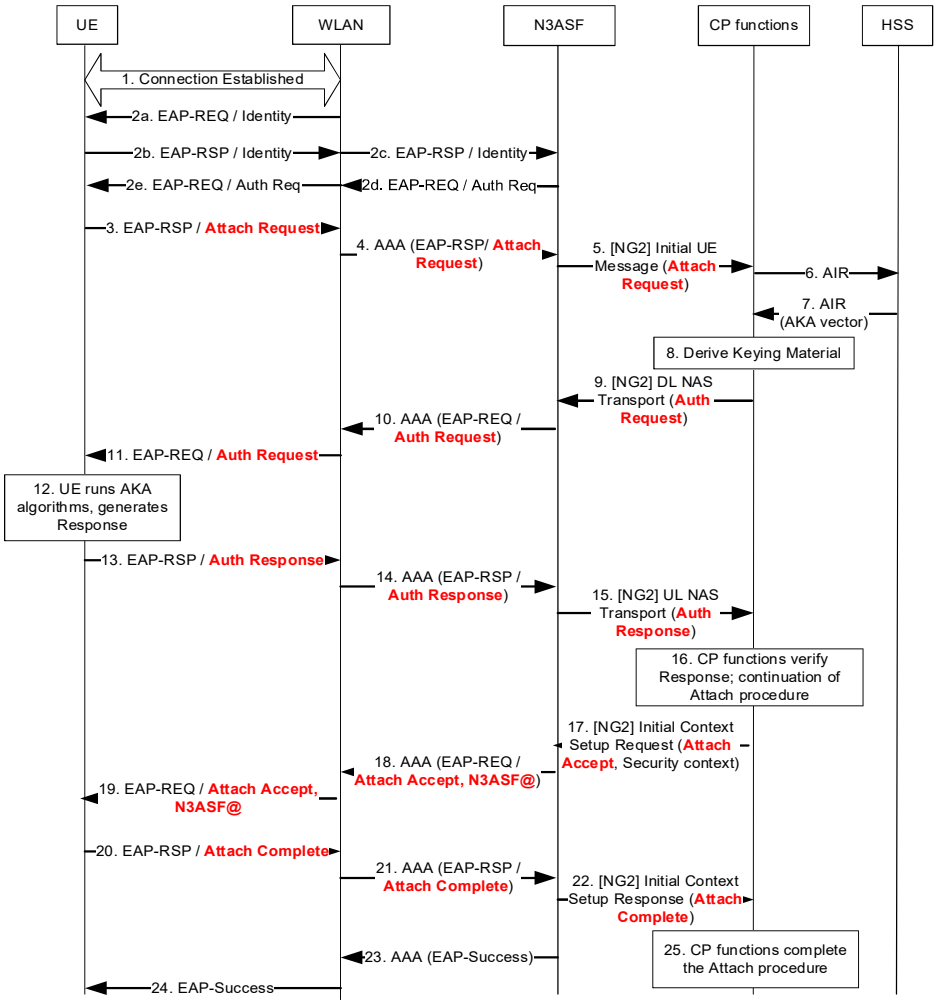


Figure 6.8.2.2.2-1: Example of Attach procedure using common NextGen core for Case 3 using EAP-over-EAPoL between UE and WLAN Access Point

In this example it is assumed that the following protocols and the following assumptions are used:

- EAP-over-EAPoL between UE and WLAN.
- EAP inside Diameter (or equivalent) protocol between WLAN and N3ASF.
- EAP extended to carry NAS messages for attach procedure.

The call flow is self-explanatory, with the exception of the following steps:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 336 of 501

1. Before attempting connection establishment the UE may need to discover (e.g. by using ANQP procedures; or new parameters in the 802.11 Beacon / Probe Request / Probe Response messages) the attributes / capabilities of the WLAN. In this way the UE knows that it should embed the cellular [NAS] Attach Request message as part of WLAN access authentication.

Editor's note: It is FFS what new requirements case 3 imposes on WLAN access points.

3-4. The EAP-RSP message carries the [NAS] Attach Request message.

NOTE: In step 4 the EAP message is further encapsulated in a Diameter message. The same applies to steps 10, 14, 18, 21 and 23.

10-11. The EAP-REQ message carries the [NAS] Authentication Request message.

17. Step 17 provides the access independent security context that is to be used by the N3ASF to derive keying material for the protection of the N3-AS connection. Note that UE derives the keying material for protection of the N3-AS connection in step 12.

13-14. The EAP-RSP message carries the [NAS] Authentication Response message.

18-19. The EAP-REQ message carries the [NAS] Attach Accept message. In addition it carries material for bootstrap of the N3-AS protocol connection. The type of bootstrap material depends on the N3-AS protocol stack. As an example, it may consist of an IP address of the N3ASF and a UDP port number.

20-21. The EAP-RSP message carries the [NAS] Attach Complete message.

Depicted in Figure 6.8.2.2.2-2 is an example protocol stack of the NG1 protocol (i.e. NAS) during the Attach procedure. The protocol stack of the NG1 protocol after bootstrapping of the N3-AS connection is depicted in Figure 6.8.2.2.2-3.

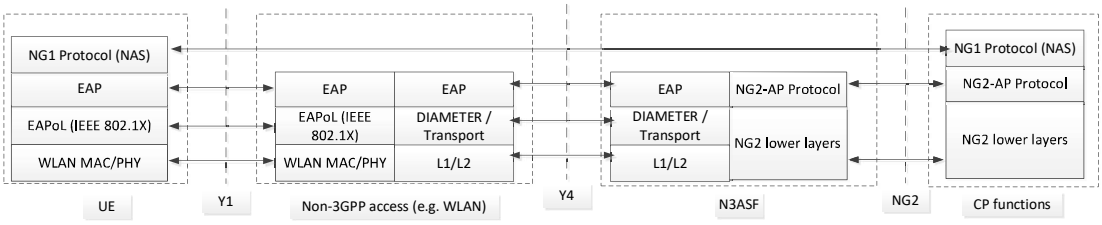


Figure 6.8.2.2.2-2: Example protocol stack of NG1 protocol (NAS) during Attach procedure

Once the Attach procedure is complete, UE and N3ASF rely exclusively on the N3-AS protocol depicted in Figure 6.8.2.2.2-3 for further message exchange (e.g. Session Management or Mobility Management procedures). In this example N3-AS is carried over the DTLS protocol.

NOTE: The NG1 call flows for subsequent SM and MM procedures are expected to be the same as for 3GPP access.

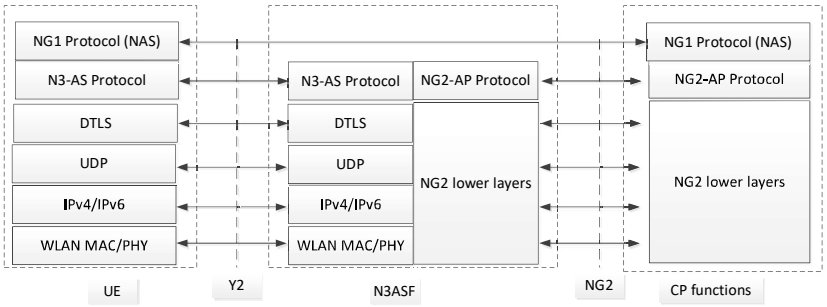


Figure 6.8.2.2.2-3: Example of NG1 protocol stack after bootstrapping of the N3-AS connection in EAP-over-EAPoL transport case

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 337 of 501

6.8.2.2.3 IKEv2 transport between UE and N3ASF

The call flow in Figure 6.8.2.2.3-1 describes a possible Attach procedure via non-3GPP access without umbrella 3GPP coverage (Case 3) to a common NextGen core using a common CN-RAN interface. In this example IKEv2 transport is used between UE and N3ASF.

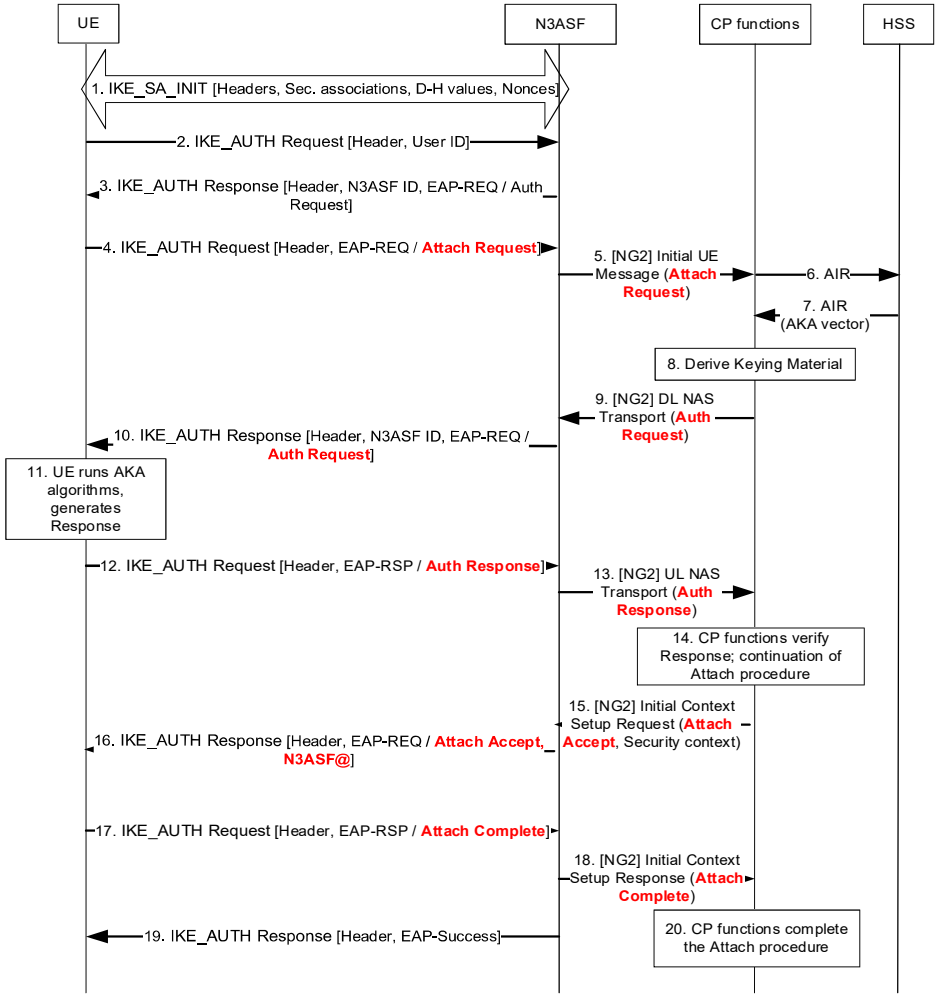


Figure 6.8.2.2.3-1: Example of Attach procedure for Case 3 using IKEv2 between UE and N3ASF

In this example it is assumed that the following protocols and the following assumptions are used:

- EAP inside IKEv2 between UE and N3ASF.
- EAP extended to carry NAS messages for attach procedure.

The call flow is self-explanatory, with the exception of the following steps:

1. Before attempting IKEv2 connection establishment, the UE first needs to discover a N3ASF. This is achieved by configuring in the UE one or more of the following:
   - an IP address (or set of IP addresses) of N3ASF node(s).
   - an FQDN (or set of FQDNs) that can be resolved into IP address of a N3ASF.
   - using DHCP configuration.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 338 of 501

3-19. In the example of Figure 6.8.2.2.3-1 it is assumed that NAS messages are carried inside EAP payload, to avoid impact on the IKEv2 protocol. Alternatively, it is possible to carry NAS messages directly as IKEv2 parameters (e.g. inside 3GPP-specific IKEv2 Configuration Payloads) or using IPsec transport.

15. Step 15 provides the access independent security context that is to be used by the N3ASF to derive keying material for the protection of the N3-AS connection. Note that UE derives the keying material for protection of the N3-AS connection in step 11.

Depicted in Figure 6.8.2.2.3-2 is an example protocol stack of the NG1 protocol (i.e. NAS) during the Attach procedure when IKEv2 is used.

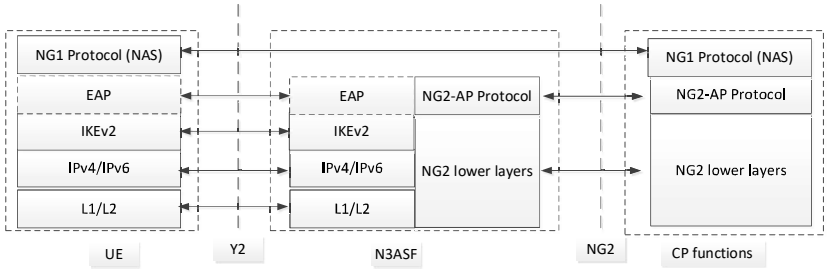


Figure 6.8.2.2.3-2: Example of IKEv2-based NG1 protocol stack during Attach procedure

MOBIKE mechanisms may be used to maintain the security association between the UE and the N3ASF when UE's local IP address changes (e.g. due to mobility).

Once the Attach procedure is complete, UE and N3ASF rely exclusively on the N3-AS protocol depicted in Figure 6.8.2.2.3-3 for further message exchange (e.g. Session Management or Mobility Management procedures). In this example N3-AS is transported on IPsec protocol.

NOTE: The NG1 call flows for subsequent SM and MM procedures are expected to be the same as for 3GPP access.

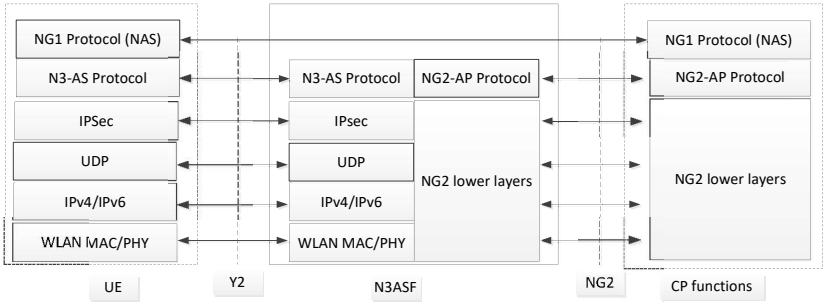


Figure 6.8.2.2.3-3: Example of NG1 protocol stack after bootstrapping of the Y2 secure connection in IPsec transport case

6.8.2.2.4 PANA transport between UE and N3ASF

The PANA call flow and protocol stack are similar to those that apply to the IKEv2 option (Figure 6.8.2.2.3-1 and Figure 6.8.2.2.3-2) and are omitted for brevity.

6.8.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 339 of 501

6.8.3 Solution 8.3: Alternative A for the interface between UE and Next Generation Core

It is stated in clause 4.2 that "The method how the NextGen UE interfaces with the NextGen Core - if any - is FFS". The nature of this interface has significant impacts on other key issues.

In this solution, a method is described where the UE interfaces with the Next Generation Core and similar AS-NAS interworking in the AN is applied as in the EPS.

6.8.3.1 Architecture description

In this alternative of the interface between the UE and the Next Generation Core

1. the UE establishes connections with the AN for AS-specific signalling and data transfer over the UE-to-AN interface
2. the AN relays the user plane data between the UE and the CN user plane entity
3. the UE establishes specific signalling connections with the AN for the purpose of exchanging NAS signalling with the CN control plane entity in a manner that is transparent to the AN
4. the AN piggybacks the NAS signalling between the UE and the CN control plane entity, as e.g. between RRC and S1-AP in the EPS

Items #1 and #2 in the list above are independent of the interface between the UE and the Core. Items #3 and #4 in the above list mark the characteristics of the interface between the UE and the Next Generation Core that are specific to this solution alternative. Figure 6.8.3-1 shows the connections that are relevant in this UE - Core signalling solution.

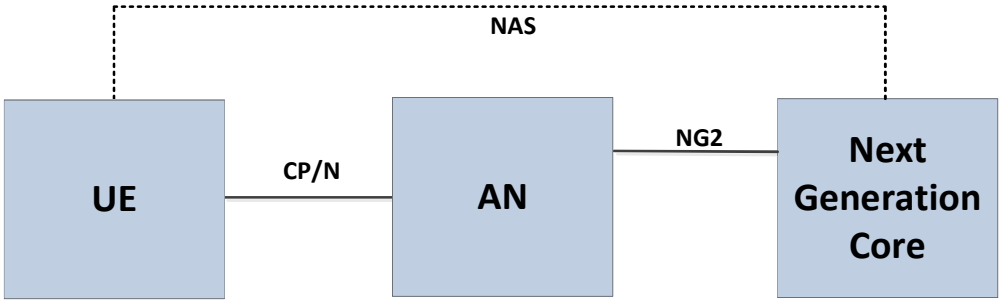


Figure 6.8.3-1: Characteristics specific to solution alternative A

"CP/N" denotes the NAS signalling aspects of the UE-to-AN signalling interface. AN transfers the content of the NAS signalling information between "CP/N" and NG2. The dotted line labelled "NAS" denotes the logical signalling connection between the UE and the Next Generation Core that is used to perform non-AS signalling.

The content of NAS signalling is transparent to the AN.

6.8.3.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

In this solution, signalling is separated between UE-AN interface (CP/N) and AN-CN interface (NG2). The NextGen UE interfaces with the NextGen Core through these two kinds of interfaces. NAS messages are transparently delivered to the AN from the UE over CP/N and forwarded to the CN over NG2, and vice versa for the response messages from the CN.

Figure 6.8.3-2 shows an example of AS and NAS protocol stack between the UE and the CN. The NAS protocols run directly between the UE and the CN, while the AN just acts as a transparent relay. The AS protocols transport the AS

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 340 of 501

and NAS messages in the UE to the AN via the CP/N interface and the messages are delivered to the CP functions in the CN via the NG2 interface.

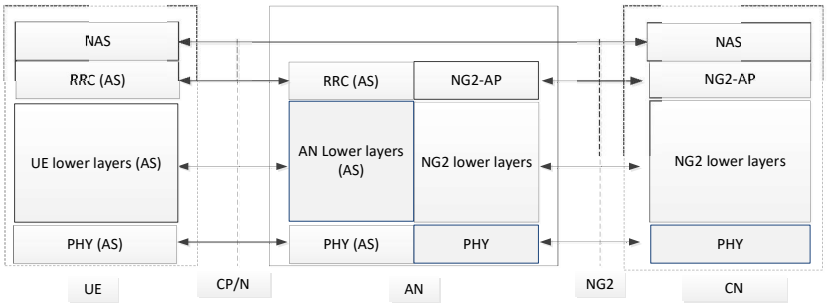


Figure 6.8.3-2: An example of AS and NAS protocol stack between UE and CN

Editor's note: The support for non-3GPP access is FFS.

6.8.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

For this solution, both AS and NAS signalling run on dedicated signalling resources and are separated from the user plane, and the NAS and AS protocols are distinguished between the UE, the AN and the CN. So, there is no impact between the control plane signalling and user plane signalling each other. In addition, this solution supports two levels of security between the UE and the CN:

- AS security: This protects the AS (RRC) signaling and the user data between the UE and the AN (e.g. integrity protection, ciphering).
- NAS security: This protects the NAS signaling between the UE and the CN (e.g. integrity protection, ciphering).

Editor's note: The AS level security is to be studied by RAN groups.

The use of two levels of security encompasses a certain complexity for handling the security functions and keying parameters. Further, with this solution AN impact when new MM or SM messages are defined in a future release of NGC can be avoided.

6.8.4 Solution 8.4: Alternative B for the interface between UE and Next Generation Core

It is stated in clause 4.2 that "The method how the NextGen UE interfaces with the NextGen Core - if any - is FFS". The nature of this interface has significant impacts on other key issues.

In this solution, a method is described where the UE does not interface with the Next Generation Core and the AN translates any non-AS signalling between the UE-to-AN signalling and AN-to-Core signalling.

6.8.4.1 Architecture description

In this alternative of the interface between the UE and the Next Generation Core

1. the UE establishes connections with the AN for AS-specific signalling and data transfer over the UE-to-AN interface
2. the AN relays the user plane data between the UE and the CN user plane entity
3. the AN terminates also any non-AS signalling towards the UE and communicates with the CN control plane entity as required, in a manner that is not visible to the UE

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 341 of 501

Items #1 and #2 in the list above are independent of the interface between the UE and the Core. Item #3 in the above list marks the characteristics of the interface between the UE and the Next Generation Core that are specific to this solution alternative. Figure 6.8.4-1 shows the connections that are relevant in this UE - Core signalling solution..

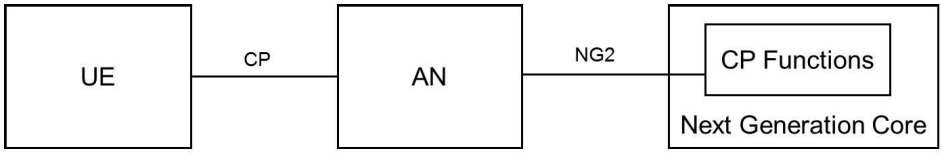


Figure 6.8.4-1: Characteristics specific to solution alternative B

In this alternative, the UE uses "CP" for any signalling, i.e. it does not differentiate between AS and non-AS signalling. AN terminates both AS and non-AS signalling from the UE, and translates / forwards the non-AS signalling between the UE and the Next Generation Core. It is up to the AN to determine when, and what, to signal with the CN control plane entity based on and triggered by messages exchanged on "CP".

Content of the NAS signalling with the Next generation Core is determined by and visible to the AN, and may be translated by the AN between AS and NAS as needed. The UE does not distinguish between AS and NAS, and does not have a signalling association with the Next Generation Core.

6.8.4.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

In this solution, signalling is separated between user network interface (CP) and network to network interface (NG2) and the NextGen UE interfaces with the NextGen Core through these two kinds of interfaces. AN translates different types of signalling messages over CP from the UE into common signalling messages over NG2 and then forwards them to CN, and vice versa for the response messages from CN.

AN has two following functions:

- Message translation: It converts different types of signalling messages over CP interface with the UE to the common signalling messages over NG2 provided by the CN.
- Message forwarding: one message may be forwarded to one or multiple messages between the UE and the CN Control Plane (CP) functions.

Figure 6.8.4-2 shows an example of AS and NAS protocol stack between the UE and the CN via the AN. UE transmits messages where AS and NAS protocols are not separated each other, and then the AN distinguishes NAS protocol from the messages and delivers them to the CN control plane as NAS protocol which is carried over NG2 interface.

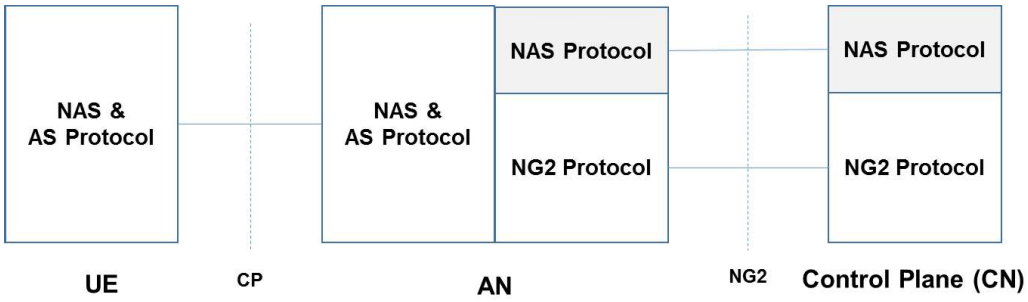


Figure 6.8.4-2: An example of AS and NAS protocol stack between UE and CN

Editor's note: How to support security associations between AN and CN is FFS and AS level security between UE and AN is to be studied by RAN groups.

6.8.4.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 342 of 501

For this solution, the need for and complexity of establishing a security association between the AN and the CN need to be considered and should be analysed by SA3.

The solution increases the complexity of the AN in that the AN must implement the NAS protocol and translate it to its signalling protocol with the UE. This issue impacts on RAN working groups.

On the other hand, the protocols between the AN and the CN can be the same in 3GPP and non-3GPP accesses as the AN shields the CN from the differences inherent to the various access systems. The AN would operate the translation function in a way that, although the UE-AN signalling is access specific, the signalling between AN and CN would be identical to all accesses.

6.8.5 Solution 8.5: Alternative C for the interface between UE and Next Generation Core

It is stated in clause 4.2 that "The method how the NextGen UE interfaces with the NextGen Core - if any - is FFS". The nature of this interface has significant impacts on other key issues.

In this solution, a method is described where the UE interfaces with the Next Generation Core and the AN user plane is used for signalling on this interface.

6.8.5.1 Architecture description

In this alternative of the interface between the UE and the Next Generation Core

1. the UE establishes connections with the AN for AS-specific signalling and data transfer over the UE-to-AN interface
2. the AN relays the user plane data between the UE and the CN user plane entity
3. the UE exchanges non-AS signalling with the Next Generation Core via the AN user plane, in a manner that is transparent to the AN

Items #1 and #2 in the list above are independent of the interface between the UE and the Core. Item #3 in the above list marks the characteristics of the interface between the UE and the Next Generation Core that are specific to this solution alternative. Figure 6.8.5-1 shows the connections that are relevant in this UE - Core signalling solution.

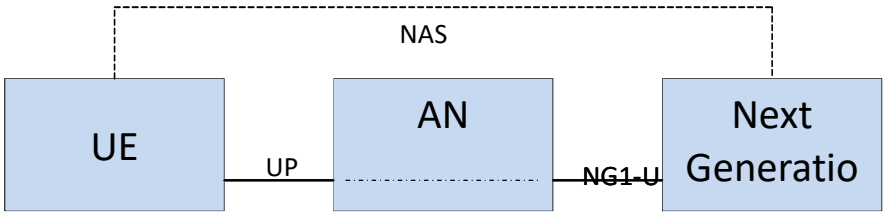


Figure 6.8.5-1: Characteristics specific to solution alternative C

"UP" denotes the user plane interface between the UE and the AN, which the UE uses to transfer non-AS signalling towards the AN. This is then forwarded by the AN to the Core in the same way as all other user plane traffic, so that NG1-U also carries the non-AS signalling messages. The line labelled "NAS" denotes the signalling connection between the UE and the Next Generation Core that is used to perform non-AS signalling directly between the UE and the Core.

Editor's note: it is ffs how "UP" is set up in this solution.

The NAS signalling is controlled solely by the UE and the CN control plane entity and is fully transparent to the AN. Content of the NAS signalling, or even the fact that NAS signalling takes place, is not visible to the AN; hence the AN plays no role in the exchange of non-AS signalling between the UE and the Next Generation Core.

6.8.5.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 343 of 501

6.8.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.8.6 Solution 8.6: Architecture for support of untrusted Non-3GPP Access

The solution focuses specifically on the support of untrusted Non-3GPP Accesses. The solution applies to UEs supporting the NGC NAS defined for the NextGen CN.

6.8.6.1 Architecture description

Depicted in Figure 6.8.6.1-1 represent a proposal for the integration of untrusted Non-3GPP Access access in NextGen CN based on the reference points in Annex G. The specific aspects of the CN architecture in terms of control plane and user plane are illustrated by grouping the functions into Control Plane functions (CP functions) and User Plane functions (UP functions).

The key points of the architecture are:

- introduction of a Non-3GPP Packet Data Gateway (ngPDG) standardized as part of the NextGen CN definition and deployable close to the access network. The ngPDG supports:
  - a control plane component for the establishment of a secure tunnel between the UE and the ngPDG (e.g. via IKEv2) , interfaced to the CN CP functions in the CN with NG2. The ngPDG uses a set of NG2 capabilities to support the EAP authentication and the NG1 NAS signalling between the UE and the CN CP functions.
  - a user plane component, implementing the termination of an IPSec secure tunnel between the UE and the ngPDG in order to provide secure access to the NextGen CN over the untrusted non-3GPP access to the UE. The ngPDG interfaces with the u-plane functions in the CN with NG3.

  NOTE: the ngPDG is a function defined by SA2. Procedures between the UE and the ngPDG and between the ngPDG and the CN are defined in SA2.
- the interface between the UE and the CN CP functions is NG1. NG1 is transported transparently between the UE and the CN CP functions, using IP transport between the UE and the ngPDG, and NG2 between the ngPDG and the CN CP functions.
- After obtaining IP connectivity over the untrusted non-3GPP access, the UE discovers the ngPDG with a mechanism similar to the ePDG discovery in the EPC.
- The UE performs an attach to the network in two steps:
  - The UE establishes an IPSec tunnel with the ngPDG with the same procedures defined for the ePDG in EPC. The IPSec tunnel established at this step is needed to protect subsequent NG1 signalling between the UE and the CN CP functions and transported between the UE and the ngPDG.
  - Once the tunnel is established, and the UE is therefore authenticated, the UE send NAS signalling containing a NAS Attach Request
- The network, upon receiving the NAS attach request from the UE, verifies that the UE is already authenticated and processes the attach procedure without re-authenticating the UE
- The attach procedure is separate from the PDU session establishment procedure.

The architecture proposes that ngPDG acts both as a control plane and a user plane function. Definition of the interface between the control plane and user plane functions in the ngPDG is out of scope. The ngPDG acts as an evolution of an ePDG in the EPC.

In this solution, the following is assumed:

- the UE is dual radio, i.e. can connect to both a 3GPP RAN and the untrusted N3GPP AN;
- Before exchanging NAS signalling between the UE and the CN CP functions (e.g. attach), the UE needs to establish an IPSec tunnel with the ngPDG.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 344 of 501

- the NAS protocol stack the UE uses over untrusted N3GPP AN is the same NAS protocol stack the UE uses over an NG RAN.
- one secure tunnel between the UE and the ngPDG is used for the support of NAS signalling between the UE and the ngPDG.
- For the support of multiple PDU sessions, one child SA may be created to protect each PDU session user plane between the UE and the ngPDG, and distinguish the traffic of each PDU sessions and enable appropriate routing between NG3.

Editor's note: whether child SAs or other mechanisms are used for this

- attach is performed via EAP authentication over IKEv2, and the UE is authenticated by the CN CP Functions.

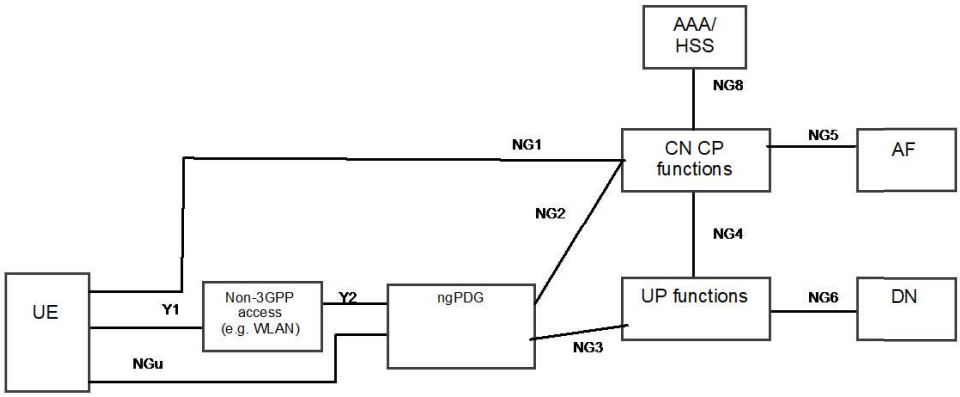


Figure 6.8.6.1-1: Architecture for NextGen CN access via untrusted WLAN.

In addition to the reference points described in Annex G, the following reference points are considered:

Y1: Reference point between the UE and the non-3GPP access (e.g. WLAN).

Y2: Reference point between the untrusted non-3GPP access and the ngPDG for the transport of UE user plane and the transport on NGu.

NGu: NGu represents interface between the UE and the ngPDG for establishing a secure tunnel between the UE and the CN, similar to the interface between the UE and the ePDG, and for securing the control plane and user plane exchanged between the UE and the CN.

NG2: NG2 represents the interface between the ngPDG and the CP functions. In the case of ngPDG, the NG2 functions used include transporting signalling between the UE and the CP Functions for UE authentication and secure tunnel establishment, transporting NG1 NAS signalling, enabling the CN CP functions to configure the ngPDG (e.g. at PDU session establishment).

NG3: represents the user plane interface between the ngPDG and the UP functions.

6.8.6.2 Function description

The proposed architecture is characterized by the following functionality:

- The UE obtains an IP address from the Non-3GPP access;

Editor's note: UE authentication with the Non-3GPP access is not covered in this proposal.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 345 of 501

- The UE discovers and selects an ngPDG, similarly to the way a UE selects an ePDG in EPC;

Editor's note: ngPDG discovery is not covered in this proposal and is expected to be based on ePDG discovery mechanisms defined for the EPC.

- The UE performs procedures (e.g. IKEv2) over NGu for the establishment of an IPSec tunnel with the ngPDG. As part of IKEv2 set-up the UE performs EAP authentication over IKEv2.

- As part of establishing the IPSec tunnel, the ngPDG interacts with the CN CP functions to authenticate the UE. EAP signalling is transported between the ngPDG and the CN CP functions via NG2

- The establishment of the IPSec tunnel and the authentication performed by the CN of the UE during the tunnel establishment (i.e. by the CP-AU in solution 6.12.1) creates a security context for the UE in the CN CP functions, indicating the UE is successfully authenticated;

  - Upon successful EAP authentication of the UE:

  - The CN CP functions provide to the ngPDG (via NG2) the security context necessary to establish the IPSec tunnel between the UE and the ngPDG;

  - The ngPDG provides to the UE the ngPDG C-plane addressing information to be used by the UE for subsequent NAS signalling (e.g. a specific IP address and/or port number) to enable the UE to transport NAS over IP

- Upon successful UE attachment over untrusted non-3GPP access, the CN CP function is informed of the type of access the UE is attached to, in order to perform mobility management procedures appropriate to the access (e.g. avoid paging procedures over untrusted non-3GPP access).

- The UE exchanges any further NG1 signalling with the CN CP functions over the secure tunnel established with the ngPDG and over NG2 between the N3CNGW and the CN CP functions. Such signalling is transported over UDP/IP in the IPSec tunnel between the UE and the ngPDG, using the ngPDG C-plane addressing information provided to the UE by the ngPDG. The NAS signalling is extracted by the ngPDG and forwarded to the CP Functions over NG2;

- The UE performs a NAS Attach procedure with the CN by sending an Attach message over NGu. Upon receiving the Attach message, the CN CP functions verify that the UE is already authenticated and the UE profile has already been retrieved, and process the attach request without authentication the UE again.

Editor's note: It is FFS whether further MM signalling is required for the UE in this solution besides attach. This depends on mobility and network slicing solutions defined for mobility between an NG RAN and untrusted WLAN.

- the UE exchanges explicit SM signalling for the establishment of PDU Sessions over the IPSec tunnel established with the ngPDG. The ngPDG extracts the NAS signalling and routes it over, NG2 between the ngPDG and the other CP functions

- The main difference between this solution and an ePDG-based solution is that

  - the ngPDG interfaces, over NG2 between the ngPDG and the core network CP Functions for UE authentication, encapsulating the EAP signalling for the authentication in NG2. Authentication and PDU session management is performed in the CN CP functions, whereas in EPC they were performed in the ePDG. This enables using the same set of CN CP functions for both a 3GPP access and an untrusted non-3GPP access for the same UE when the UE is connected simultaneously to both accesses or to handover traffic between a 3GPP access and a non-3GPP access without having to relocate the serving functions;

Editor's note: How QoS is supported for different PDU session may be based on the solutions developed for the ePDG solution in the EPC and is FFS.

- upon PDU session establishment, user plane function selection is performed. The ngPDG can be selected as the only user plane function for the UE, acting as a GW towards data networks, or separate user plane function(s) can be selected and interconnected to the ngPDG via NG3;

  - upon the creation of a PDU session, the CN CP functions select a User Plane function (UPF) for routing the traffic of the PDU session to the corresponding Data Network.

  - The CN CP functions provide to the UPF the routing tunnel end point corresponding to the ngPDG.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 346 of 501

  - The CP CN functions provide to the ngPDG the routing tunnel end point corresponding to the UPF and the IP address(es) for the corresponding to the PDU session.

  - Upon receiving the indication that a new PDU session has been established, the ngPDG establishes a child Security Association with the UE, and both the UE and the ngPDG associate the new SA to the PDU session and the corresponding UE address(es)

- the IPSec tunnel is used as follows to transport NAS signalling and user plane data:

  - the ngPDG provides to the UE, upon successful IPSec tunnel establishment, the ngPDG C-plane addressing information to be used by the UE to send NAS signalling to the network

  - for each PDU session activated for the UE, a child security association is created and the IP address(es) assigned to the UE as part of the PDU session activation are associated to the child SA corresponding to the PDU session

Editor's note: When UE is connected via both 3GPP and non-3GPP access, the impact of multiple NG1 instances on mobility management solutions is FFS in terms of the mobility management model maintained by the network for the UE.

- The ngPDG performs the following additional functionality:

  - Routing of packets from/to the NextGen CN to/from UE by interfacing via NG3 with other user plane functions or via NG6 with the Data Network;

  - De-capsulation/Encapsulation of packets for IPSec;

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

Editor's note: ngPDG functionality in terms of transport of level packet marking and QoS Enforcement are FFS and depend on the QoS solutions defined in NextGen.

- support of network slicing is provided by the UE using the same NAS NG1 procedures between the UE and the CN CP functions that the UE uses over an NG RAN.

Editor's note: The extent of required network slicing support over a non-3GPP access and what features of network slicing can be supported over a non-3GPP access are FFS. Further network slicing considerations are not covered by the present proposal.

The proposal has the following difference with respect to the use of NG2 for NG RAN:

- NG2 in case of NG RAN transports authentication signalling within NAS request messages (specifically the Attach Request). In this proposal NG2 carries the EAP signalling for UE authentication and IPSec tunnel establishment

- not all parameters delivered to a 3GPP AN (i.e. parameters specific to a 3GPP access) are delivered to the ngPDG over NG2

Editor's note: Consideration for handover of traffic between NG RAN and untrusted non-3GPP access connected to the NGC are FFS. Considerations for simultaneous connectivity over NG RAN and over untrusted non-3GPP access connected to the NGC are FFS.

6.8.6.2.1 Initial attach procedure for Untrusted N3GPP Access

The call flow in Figure 6.8.6.2-1 describes the Attach procedure via untrusted N3GPP.

In this procedure it is assumed that:

- EAP is transported in IKEv2 between UE and ngPDG for the IPSec tunnel establishment;

- The ngPDG extracts the EAP messages sent in IKEv2 in uplink and forwards them to the Serving CN CP Function over NG2 to carry out the authentication in the CP AU function. The ngPDG, upon receiving EAP messages over NG2 from the Serving CN CP function, forwards them to the UE in IKEv2;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 347 of 501

- to attach to the network, the UE first performs the IPSec tunnel establishment and, once the tunnel is established, the UE performs a NAS attach procedure with NAS messages transported over IP between the UE and the ngPDG. The ngPDG extracts the NAS messages in uplink and forwards them over NG2 to the CN CP function.

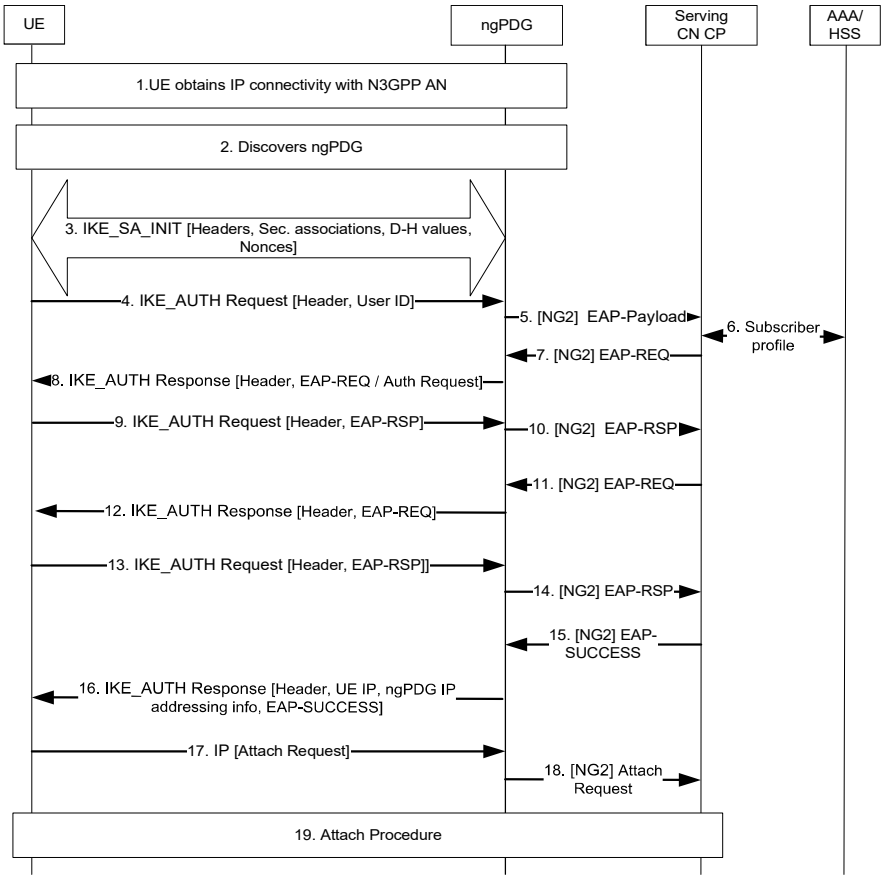


Figure 6.8.6.2.1-1: Attach procedure for untrusted N3GPP access using EAP-over-IKEv2 between UE and N3ANF

The call flow is as follows:

1. The UE gains IP connectivity with the untrusted N3GPP AN.

Editor's note: UE authentication with the Non-3GPP access is outside the scope of this proposal.

2. The UE discovers a ngPDG via a procedure similar to ePDG discovery of Rel. 13.

Editor's note: It is assumed that an NGC UE discovers an ngPDG or a PDG that has both the ePDG and ngPDG functionality. Details of the ngPDG discovery are FFS.

3. UE initiates the IKE setup procedure via an IKE_SA_INIT exchange, triggered by the need to attach and establish connectivity over untrusted N3GPP AN

4. UE sends IKE_AUTH Request and provides the UE identity. The UE does not provide any information to identify a Data Network.

NOTE 1: The behaviour of the UE is similar to the IPSec tunnel establishment with an ePDG in EPC, with the difference that the UE does not provide any APN information.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 348 of 501

5. The ngPDG selects a Serving CN CP function, and forwards the request to the Serving CN CP Functions

Editor's note: How the ngPDG selects the Serving CN CP function is FFS.

6. The Serving CN CP Function interacts with the HSS/AAA to perform EAP authentication and retrieve the subscriber profile.

7. The Serving CN CP Functions sends an EAP Request to the ngPDG.

8. ngPDG responds with an IKE_AUTH Response including the EAP request

9. The UE sends the IKE_AUTH Request.

10. The ngPDG forwards the EAP request to the Serving CN CP Functions.

11. The Serving CN CP Function (e.g.CP-AU of solution in 6.12.1) process the EAP Request and send an Authentication Request over NG2

12. The ngPDG forwards the Authentication Request over IKEv2 to the UE

13. The UE computes an authentication response and sends an Authentication Response to Serving CN the CP Functions encapsulating it in IKEv2 to the ngPDG

14. The ngPDG forwards the Authentication response to the Serving CN CP Functions over NG2

15. The Serving CN CP Functions complete the authentication procedure towards the UE and provides the security context for the setup of the IPSec Tunnel. The Serving CN CP functions forward the security context for the establishment of the IPSec Tunnel over NG2 to the ngPDG. The Serving CN CP Function may store a context for the UE indicating that the UE has been successful authenticated. The Serving CN CP function also provide the UE with the temporary secure identity.

Editor's note: The Serving CN CP function may include an SEAF (Security Anchor Function) function to store the UE security context.

16. The ngPDG sends an EAP response to the UE over IKEv2. The ngPDG sends the IP address of the UE in the final IKEv2 message with the ngPDG IP address in IKEv2 Configuration payloads, similarly to the ePDG procedure. However, the IP address of the UE shall be not be used for user plane traffic but only used to transmit and receive NAS signalling to the CN CP functions via the ngPDG, The ePDG also includes in the IDr payload of IKEv2 the ngPDG C-plane addressing information to be used by the UE for subsequent NAS signalling to the Serving CN CP Function via the ngPDG (e.g. a specific IP address and/or port number), and the the IKEv2 procedure is completed. An NG2 interface instance for the UE is established between the ngPDG and the Serving CN CP Function.

NOTE 2: With respect to the IKEv2 procedure used for the UE tunnel setup with the ePDG in EPC, the IP address for the UE returned in the IKEv2 message is not for user plane data, but for transport of NAS signalling between the UE and the Serving CN CP Function via the ngPDG.

17. The UE sends a NAS Attach Request to the Serving CN CP Function over UDP/IP addressing the ngPDG C-plane termination. The UE provides in the Attach Request the same identity it provided in step 4 or, if received in step 14, provides the temporary secure identity.

18. The ngPDG forwards the NAS Attach Request to the Serving CN CP Function.

19. The Serving CN CP Function verifies that the UE has been previously authenticated based on the identity provided by the UE (i.e. the secure temporary identity provided by the Serving CN CP function in step 15, or the UE identity provides by the UE in step 4 if the Serving CN CP function has not provided the secure temporary identity) and by verifying the context in the Serving CN CP function, and proceeds with the attach procedure without re-authenticating the UE. NAS security material is derived from the existing security context in the Serving CN CP function.

Editor's note: The details of storage, retrieval and use of the security context created in the Serving CN CP function at UE authentication are FFS and depend on the security architecture defined by SA WG3.

NAS security mode command is sent as per current NAS procedures.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 349 of 501

Editor's note: The solution may change the NAS behaviour in the CN because the UE is authenticated before the Attach is sent.

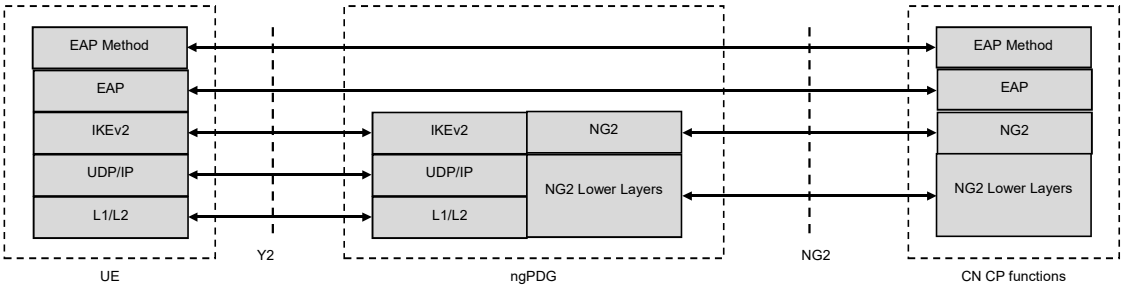


Figure 6.8.6.2.1-2: Protocol stack for IPSec Tunnel Establishment

The following Figure 6.8.6.2.1-3 describes the protocol stack during the UE attach.

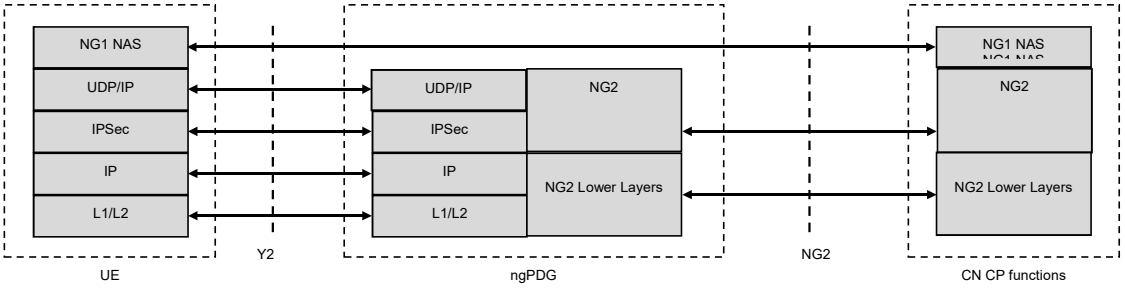


Figure 6.8.6.2.1-3: Protocol stack for Attach procedure

6.8.6.2.2 PDU session establishment via untrusted N3GPP access

Subsequent NAS signalling for PDU Session establishment is transported over UDP and IP in the IPSec tunnel. The UE addresses the NAS signalling using the addressing information provided to the UE by the ngPDG in step 15 during the IPSec tunnel establishment. The NAS signalling is extracted by the ngPDG and forwarded to the Serving CN CP Function selected during the attach procedureover NG2.

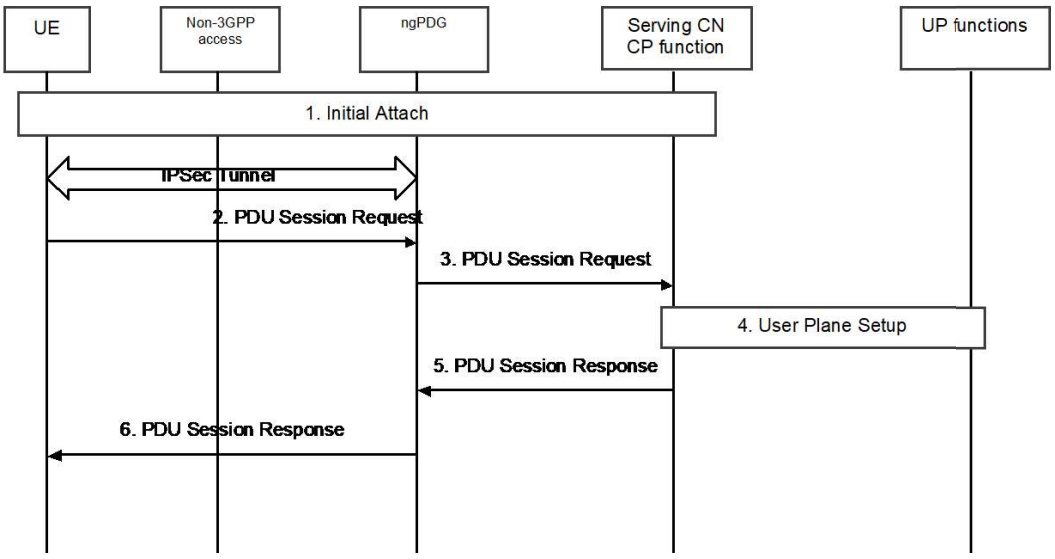


Figure 6.8.6.2.2-1: PDU session establishment via non-3GPP access procedure

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 350 of 501

Once the initial attach procedure as described in subclause 6.8.6.2.1 is completed, the UE can initiate PDU session establishment procedure as described in Figure 6.8.6.2.2-1 above.

1. The UE performs the attach procedure over non-3GPP access as shown in subclause 6.8.6.2.1.
2. The UE sends a PDU session request message to ngPDG using UDP/IP between the UE and the ngPDG and using the c-plane ngPDG addressing information obtained during step 15 of the attach procedure.
3. The ngPDG de-capsulates the received message and forwards it to the Serving CN CP function via NG2 interface. The ngPDG also includes an IP address for a tunnel termination point for the establishment of the user plane for a PDU Session.

NOTE: The ngPDG is not aware of the content of the NAS message. The ngPDG however assigns an IP address for a tunnel termination point for the establishment of the user plane for a PDU Session anyway, and forwards it to the Serving CN CP Function. If at the completion of the procedure the ngPDG does not receive from the Serving CN CP Function the user plane information for the UP functions, the ngPDG releases the allocated IP address.

4. The CP function performs the UP setup (including UP function selection) with the UP function, including assigning the UE IP address(es) for the PDU session, providing to the UP function the IP address for the tunnel termination point at the ngPDG, and retrieving the UP function tunnel termination address.
5. The Serving CN CP function sends a PDU session response message to the UEover NG2 including the IP address(es) assigned to the UE. The Serving CN CP function provides to the ngPDG over NG2 the PDU session related information (including IP address(es) assigned to the UE, QoS rules, the UP function tunnel termination address, etc.).
6. The ngPDG forwards the PDU session response message over UDP/IP and encapsulated in an IPSec packet to the UE. Based on the received PDU session related information, the ngPDG may trigger the establishment of a child SA with the UE and associates the IP address(es) allocated to the UE for the PDU session with the child SA.Editor's note: whether the UE and the ngPDG use one child SA per-PDU session with QoS differentiation based on packet marking, or one child SA per-PDU session and per-QoS level, or other solutions is FFS.

The protocol stack for the PDU session setup is described below.

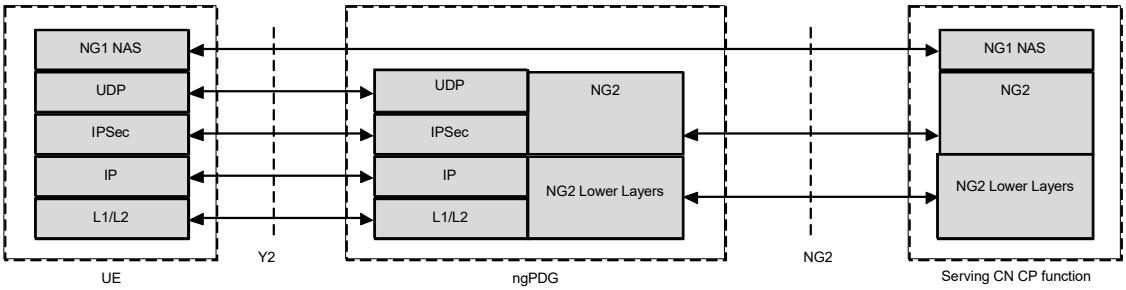


Figure 6.8.6.2.2-2: Protocols for control plane

Editor's note: the user plane stack figure is FFS.

6.8.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

The solution enables the UE to use the same NAS stack and procedures defined over an NG RAN connected to the NGC also over an untrusted non-3GPP access connected to the NGC via an ngPDG.

The solution does not require modification to the EAP authentication methods to support NectGen-specific information (e.g. a NAS Attach message or parameters regularly transported in a NAS attach message). Therefore the solution does not require interactions with external standardization fora, e.g. IETF. The UE can e.g. attach to NextGen core over trusted non-3GPP access by carrying out the normal EAP-AKA' procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 351 of 501

The proposal makes the ngPDG functionality independent from the NAS functionality, therefore future enhancements to e.g. NGC NAS MM, like an Attach Message and the parameters included, has no impacts on the ngPDG functionality and does not require modifications to IKEv2 or EAP.

The proposal enables the CN aspects of support of network slicing (e.g. UE providing NSSAI to CN CP functions for slice selection, etc.), since the UE uses the same NAS NG1 procedures between the UE and the CN CP functions that the UE uses over an NG RAN. .

Editor's note: the solution may change the NAS behaviour in the CN because the UE is authenticated before the Attach is sent.

6.8.7 Solution 8.7: Support standalone non-3GPP access via NG2/NG3

6.8.7.1 Architecture description

The proposed architecture is shown in Fig. 6.8.7.1-1 and is based on a new network function called the *Non-3GPP* Interworking Function (N3IWF). The N3IWF enables UEs to attach to the NextGen core either via trusted non-3GPP access or via untrusted non-3GPP access. In both cases, the NG2 interface is used to carry out the attach procedure. After attachment, a secure connection is established between the UE and the N3IWF via which NAS signaling can be exchanged between the UE and the CP functions.

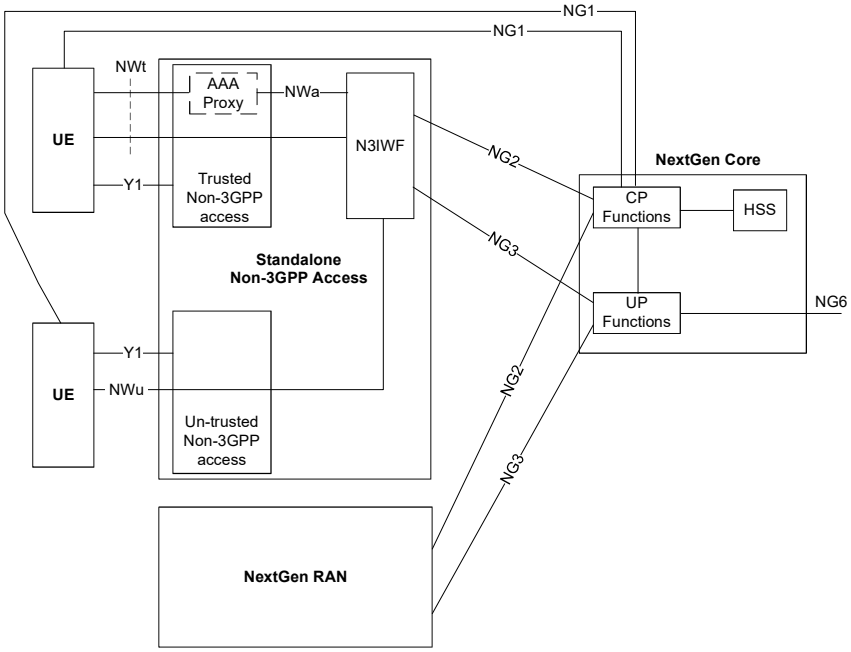


Figure 6.8.7.1-1: Architecture to enable 3GPP and non-3GPP access to NextGen Core via NG2/NG3

The N3IWF forms the key functional element of a standalone non-3GPP access network. The term 'standalone' signifies the fact that the non-3GPP access network can operate independently from the 3GPP access network (i.e. without any tight integration).

In some deployments, the trusted non-3GPP access can be configured to forward all AAA traffic directly to N3IWF. In such cases, the AAA Proxy is not required (thus shown with dotted outline).

The primary characteristics of the solution are the following:

1. The N3IWF is used to enable access to NextGen CN via standalone trusted and untrusted non-3GPP accesses by re-using the NG2 interface.

2. From the UE point of view, the N3IWF has a role similar to TWAG for trusted non-3GPP (WLAN) access and a role similar to ePDG for untrusted non-3GPP access.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 352 of 501

3. The N3IWF supports network slice selection based on "assistance information" provided by the UE within the EAP-AKA' messages (see details below).

4. Over trusted non-3GPP access the UE can attach to NextGen CN by re-using the existing EAP-AKA' authentication procedure. There is no need to define a new EAP authentication method (e.g. for carrying NAS messages within EAP packets) and there is no need to transfer EAP messages over NG2.

5. Over untrusted non-3GPP access, the UE can attach to NextGen CN by re-using the existing IKEv2 procedure with EAP-AKA' authentication. There is no need to define a new EAP authentication method (e.g. for carrying NAS messages within EAP packets) and there is no need to transfer EAP messages over NG2.

6. From the NextGen CN point of view, an Attach over non-3GPP access (trusted or untrusted) is carried out via NG2 with the same procedure as an Attach over 3GPP access. However, the NextGen CN is informed that the UE attaches over a certain type of non-3GPP access so it can adopt its behaviour accordingly (e.g. does not initiate paging over WLAN access, does not transition the UE to CN Idle state, etc.).

7. The standalone non-3GPP access may include one or more N3IWFs. When the UE moves from a non-3GPP access served by one N3IWF to a non-3GPP access served by another N3IWF (which is considered a very rare event), the UE performs a full attach to NextGen core. That is, inter-N3IWF mobility is not currently supported.

The following new reference points are used:

Y1: Reference point between the UE and the non-3GPP access (e.g. WLAN). This is outside the scope of 3GPP and is used for non-3GPP access signalling (e.g. WLAN association, local IP address assignment, etc).

NWt: Reference point between the UE and the N3IWF via trusted non-3GPP access. It is similar to the SWw reference point specified in TS 23.402 [17] clause 16 (between UE and trusted WLAN). It is used to support the EAP-AKA' authentication procedure, for establishing a DTLS connection between the UE and N3IWF and for transferring NAS signalling via the DTLS connection. It is also used to support user-plane communication.

NWu: Reference point between the UE and the N3IWF via untrusted non-3GPP access. It is similar to the SWu reference point specified in TS 23.402 [17] (between the UE and ePDG). It is used for establishing an IPsec connection between the UE and N3IWF and for transferring NAS signalling via the IPsec connection. It is also used for supporting user-plane communication.

NWa: Reference point between the AAA proxy in a trusted non-3GPP access and the N3IWF. It is used to transfer AAA signalling.

6.8.7.2 Function description

6.8.7.2.1 Overview

A high-level overview of the procedures applied to attach the UE to NextGen CN via trusted and untrusted non-3GPP access is illustrated in Fig. 6.8.7.2.1-1. The figure shows WLAN as an example of non-3GPP access but it is applicable to other non-3GPP accesses too. The key characteristic of these procedures is that the N3IWF starts an Attach procedure over NG2 on behalf of the UE when the UE carries out the normal EAP-AKA' procedure (over trusted access) or when the UE carries out the normal IKEv2/EAP-AKA' procedure (over untrusted access). The N3IWF terminates the EAP-AKA' signalling, thus, from an EAP point of view, it functions as an EAP authenticator. However, the UE is authenticated by the NextGen CN (not by the N3IWF) as explained below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 353 of 501

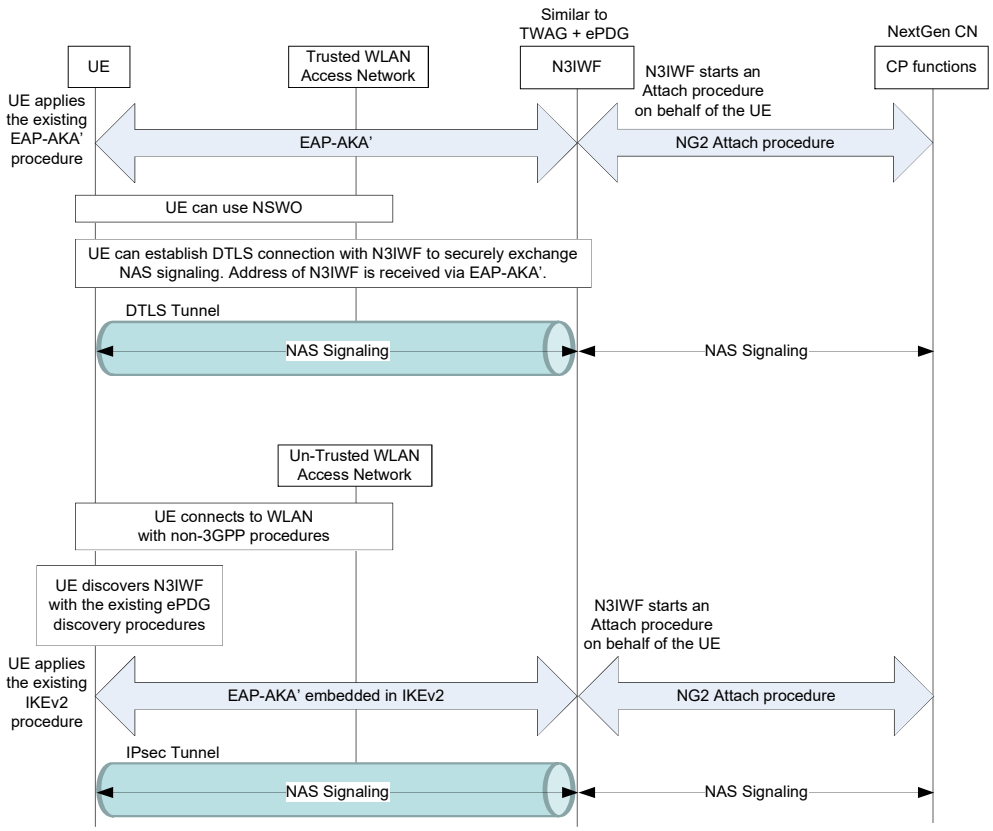


Figure 6.8.7.2.1-1: High-level overview of control-plane procedures

6.8.7.2.2 Protocol architecture for Trusted non-3GPP access

In subsequent clauses the WLAN access is used as an example of non-3GPP access in order to better explain the solution. However, any non-3GPP access that supports EAP authentication can be used.

The protocols utilized when the UE attaches to NextGen via a trusted WLAN access network are shown in figure 6.8.7.2.2-1. The UE attaches to NextGen core during the EAP-AKA' procedure. In fact, the EAP-AKA' and the NextGen Attach procedures are executed in parallel as explained in clause 6.8.7.2.4.

The Interworking function is a functional component of N3IWF that performs interworking between EAP-AKA' signaling and NG2 signaling and, specifically, initiates an attach procedure toward NextGen core on behalf of the UE. The Adaptation Layer in the UE enables the operation of the Non-Access Stratum (NAS) layer over EAP-AKA' (as opposed to RRC layer). It starts an EAP-AKA' procedure when the NAS layer requests network attachment and enables interworking between EAP-AKA' and NAS messages. For example, the Adaptation layer receives an Attach Request from the NAS layer and copies the IEs in the Attach Request into the EAP-RSP/AKA-Identity message. The operation of Adaptation layer and Interworking function during the attach procedure is further discussed in clause 6.8.7.2.4.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 354 of 501

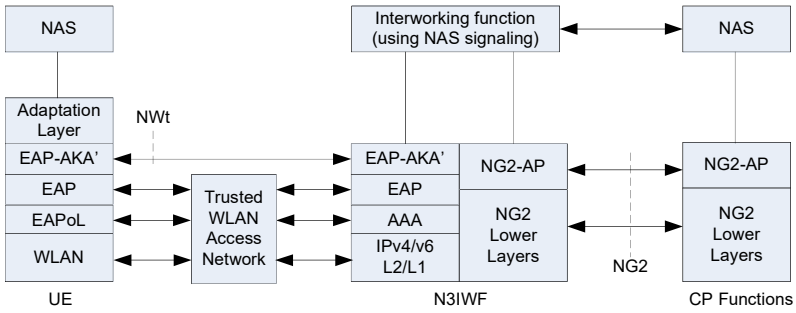


Figure 6.8.7.2.2-1: CP protocols used during attachment via trusted non-3GPP access

After the UE completes the EAP-AKA' procedure and attaches to NextGen core, the UE can exchange NAS signaling with the CP functions using the protocol architecture shown in figure 6.8.7.2.2-2. The UE may use the NG1 interface to request a PDU session, e.g. to communicate with an external data network through the NextGen core and the trusted WLAN. The Relay layer in the N3IWF relays NAS messages coming from the UE via the DTLS connection to CP functions via the NG2 interface, and vice versa.

In the figure 6.8.7.2.2-2 (i.e. after attachment) the Adaptation layer implements a control-plane protocol between the UE and N3IWF: It creates and maintains an "access stratum" connection (i.e. a DTLS connection), it encapsulates NAS messages into Adaptation layer "UL/DL NAS Transport" PDUs and transparently forwards them, and it creates and maintains UP connections between the UE and N3IWF for carrying the traffic of PDU sessions. These UP connections are referred to as Non-3GPP UP (N3UP) connections.

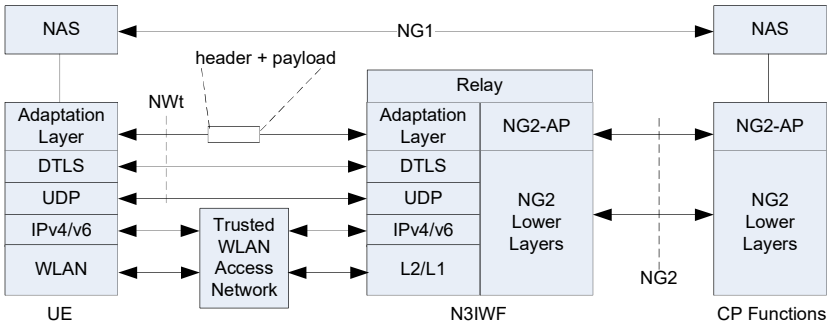


Figure 6.8.7.2.2-2: CP protocols used after attachment via trusted non-3GPP access

Figure 6.8.7.2.2-3 shows the protocols used to transport the traffic of a PDU session between the UE and the UP functions. When the UE requests a new PDU session (via NAS signaling) the Adaptation layer establishes a new N3UP connection between the UE and N3IWF and creates a new network interface in the UE bound to this N3UP connection (see details in clause 6.8.7.2.5). The N3UP connection may be associated with several QoS rules.

The N3UP layer shown in figure 6.8.7.2.2-3 implements a user-plane protocol between the UE and N3IWF. It encapsulates the UP data received from the upper layer (e.g. from Ethernet or IP layer) into N3UP PDUs. Each N3UP PDU includes a header that can contain PDU session information and QoS information (e.g. a Flow Priority Indicator (FPI), a Reflective QoS Indicator (RQI) or other parameters according to the selected QoS solution). As shown in figure 6.8.7.2.2-3 the N3UP layer performs also QoS handling (i.e. QoS marking, queuing, etc).

NOTE: If the N3UP connection between UE and N3IWF utilizes IP (L3 connection), then the N3UP layer operates on top of IP/WLAN (not over WLAN only as shown in figure 6.8.7.2.2-3).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 355 of 501

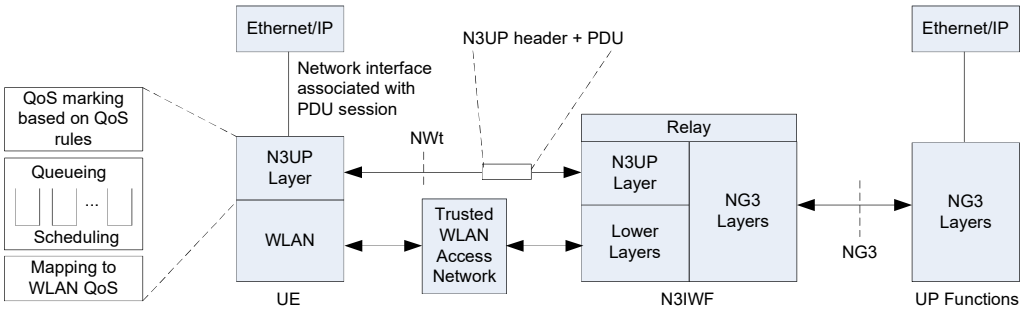


Figure 6.8.7.2.2-3: UP protocols used for a PDU session via trusted non-3GPP access

6.8.7.2.3 Protocol architecture for Untrusted non-3GPP access

The protocols utilized when the UE attaches to NextGen via a untrusted WLAN access network are shown in figure 6.8.7.2.3-1.

The Adaptation layer in the UE discovers the IP address of N3IWF (e.g. by using the existing procedures for ePDG discovery) and informs the NAS layer that the lower layers are ready. When the NAS layer sends an Attach Request to the Adaptation layer, the Adaptation layer establishes an IPsec tunnel with the N3IWF. This tunnel is established with the existing IKEv2/EAP-AKA' procedures. During the establishment of the IPsec tunnel, the Interworking function in N3IWF starts an attach procedure over NG2 of behalf of the UE and attaches the UE to NextGen core.

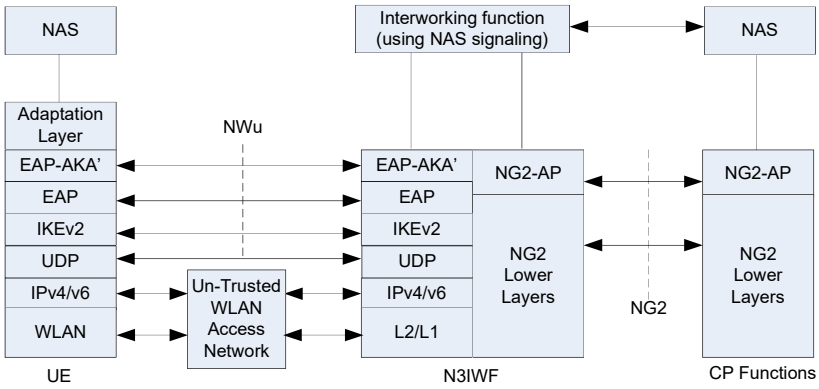


Figure 6.8.7.2.3-1: CP protocols used during attachment via untrusted non-3GPP access

After the IPsec tunnel between the UE and N3IWF is established, the protocol architecture shown in figure 6.8.7.2.3-2 is used for CP signaling. The UE can send NAS messages to N3IWF via the IPsec tunnel which are relayed to the NAS layer in the CP functions, and vice versa.

After attachment, the Adaptation layer implements a control-plane protocol between the UE and N3IWF: It creates and maintains an "access stratum" connection (i.e. an IPsec tunnel), it encapsulates NAS messages into Adaptation layer "UL/DL NAS Transport" PDUs and transparently forwards them, and it creates and maintains UP connection between the UE and N3IWF for carrying the traffic of PDU sessions. These UP connection are referred to as Non-3GPP UP (N3UP) connections.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 356 of 501

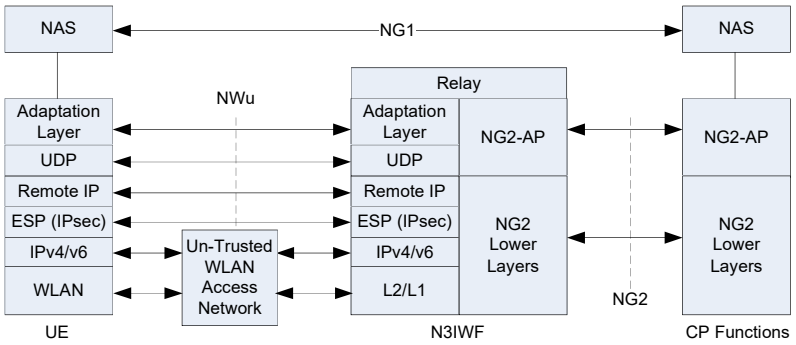


Figure 6.8.7.2.3-2: CP protocols used after attachment via untrusted non-3GPP access

Figure 6.8.7.2.3-3 shows the protocols used to transport the traffic of a PDU session between the UE and the UP functions. When the UE requests a new PDU session (via NAS signaling) the Adaptation layer establishes a new N3UP connection between the UE and N3IWF and creates a new network interface in the UE bound to this N3UP connection (see details in clause 6.8.7.2.7). The N3UP connection may be associated with several QoS rules.

The N3UP layer shown in figure 6.8.7.2.3-3 implements a user-plane protocol between the UE and N3IWF over the established IPsec tunnel. It encapsulates the UP data received from the upper layer (e.g. from Ethernet or IP layer) into N3UP PDUs. Each N3UP PDU includes a header that can contain PDU session information and QoS information (e.g. a Flow Priority Indicator (FPI), a Reflective QoS Indicator (RQI) or other parameters according to the selected QoS solution). As shown in figure 6.8.7.2.3-3 the N3UP layer performs also QoS handling (i.e. QoS marking, queuing, etc).

NOTE 1: Some of the functionality of N3UP shown in figure 6.8.7.2.3-3 (e.g. queuing and scheduling) may reside below the ESP layer.

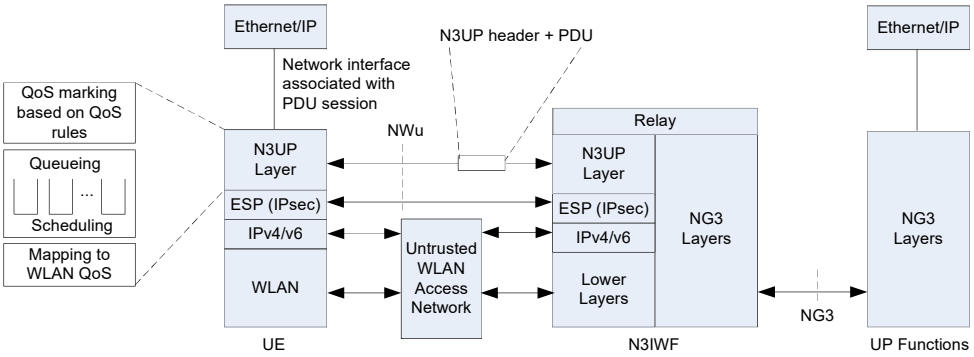


Figure 6.8.7.2.3-3: UP protocols used for a PDU session via untrusted non-3GPP access

6.8.7.2.4 Attach via Trusted Non-3GPP Access

Figure 6.8.7.2.4-1 shows the signaling when the UE attempts to connect to a WLAN (the WLAN is used as an example non-3GPP access). The UE is authenticated by the NextGen core network (via NG2) and is authorized to access the WLAN. This authentication and authorization is performed by "attaching" the UE to the NextGen core.

Editor's note: It is FFS how the signalling shown in figure 6.8.7.2.4-1 can be modified to cover also the cases when the UE uses an EAP authentication method other than EAP-AKA'.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 357 of 501

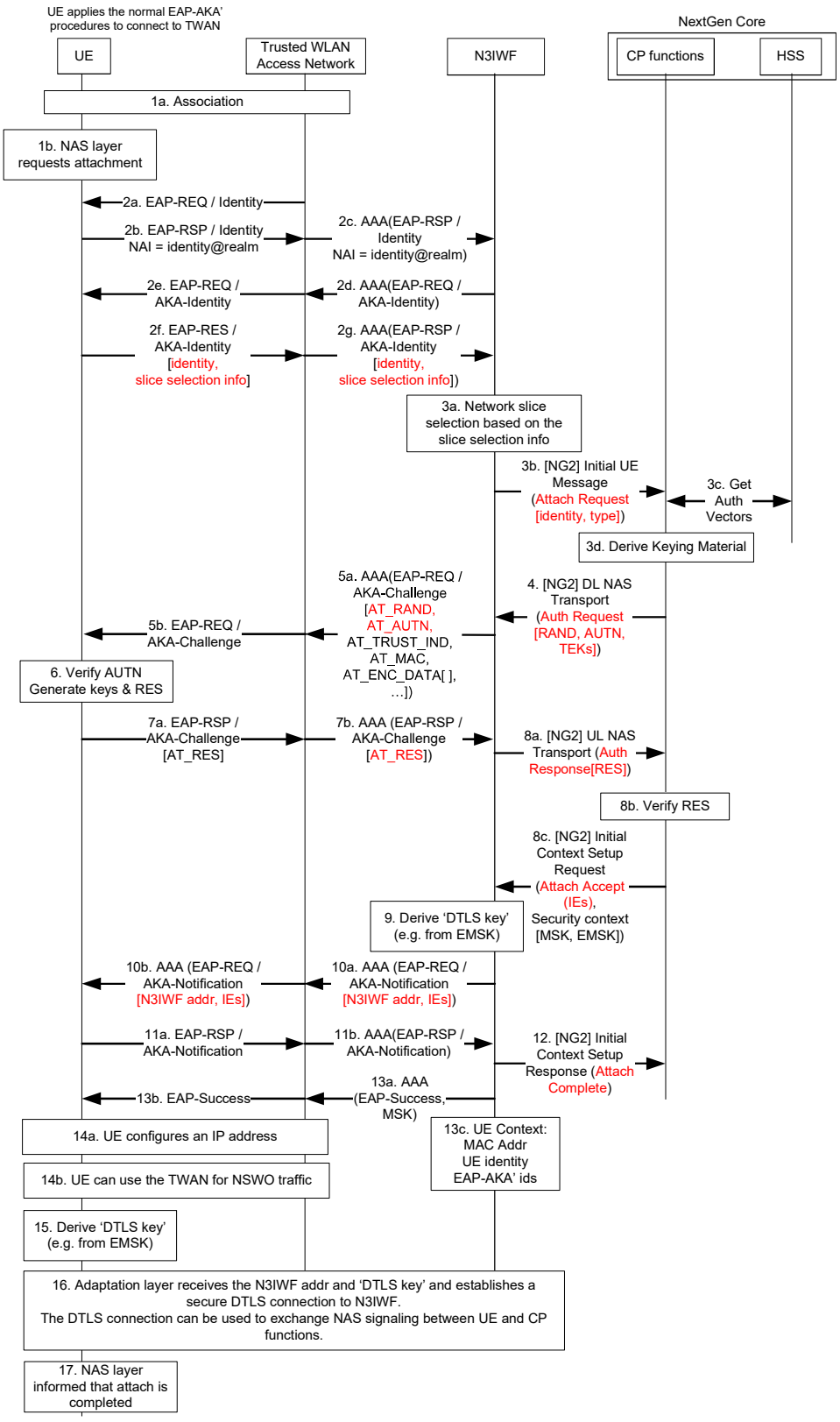


Figure 6.8.7.2.4-1: Attach procedure via Trusted WLAN using the NG2 interface

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 358 of 501

1. The UE discovers and associates with the WLAN according to the existing procedures. At this point, the NAS layer in the UE sends an Attach Request to the Adaptation layer in order to attach to the NextGen over the WLAN.

2. The WLAN starts the IEEE 802.1x access control procedure by transmitting an EAP-REQ/Identity request. Note that 802.1x messages (i.e. EAP-over-LAN) are not shown in the figure. The UE provides an identity along with a realm, which is primarily used for routing purposes (as per RFC3748). Based on the provided realm, the WLAN access network routes the EAP-RSP/Identity message to the N3IWF, which then requests a specific identity (e.g. a permanent or temporary) from the UE. From the WLAN access network point of view, the N3IWF serves as an AAA server.

   If the UE supports network slice selection over non-3GPP access, the UE may provide slice selection 'assistance information' in one of the following two ways:

   - The UE includes a new EAP-AKA' attribute (defined by 3GPP) in the AKA-Identity message. This new attribute is used to carry the slice selection 'assistance information' from the UE.

   - Alternatively, the UE may decorate the provided identity with slice selection 'assistance information'. For example, if the UE provides its IMSI identity "295023820005424", then the decorated identity could be "295023820005424%<assistance info>". A special character can be used to separate the identity from the 'assistance information'.

Editor's note: The method used for network slice selection needs to be aligned with the agreements in KI#1. This may require further study.

3. The N3IWF selects a network slice instance based on the 'assistance information'. Then it creates an Attach Request (identity, type) message on behalf of the UE and sends this message to the CP functions of the selected slice instance over NG2. The identity IE includes the identity received in step 2g and the type IE indicates that this is an attach request over trusted non-3GPP access. The UE sends to N3IWF the information required to create the Attach Request by including the appropriate attributes in message 2f (EAP-RES/AKA-Identity). These attributes will be defined by 3GPP.

   The Attach Request message in this scenario is a simple message that carries the UE identity, the type IE and the identity of the WLAN access (e.g. the ESSID). This message is essentially used to authenticate the UE and to authorize access to the trusted WLAN network. It does not need to carry IEs specific to 3GPP access, such as old LAI, DRX params, etc.

NOTE 1: If the Attach Request in step 3b needs to include more IEs from the UE, these IEs could be sent by the UE in step 2f (i.e. include more attributes in AKA-Identity).

4. The CP functions send an Authentication Request (RAND, AUTN, TEKs) back to N3IWF. The TEKs are the Transient EAP Keys (i.e. K_aut and K_encr) which are used to protect the EAP-AKA' signalling between the UE and N3IWF. The TEKs keys are generated as specified in RFC5448. These keys are included in the Authentication Request only when the type IE in the Attach Request indicates non-3GPP access. Depending on SA3 decisions, the Authentication Request message may include additional IEs than those shown in the above figure.

5. The N3IWF sends an EAP-REQ/AKA-Challenge message to UE. The RAND, AUTN received in step 4 are included in this message. Also the AT_MAC is calculated based on the K_aut key received in step 4. If there is need to send encrypted parameters to the UE (inside the AT_ENC_DATA attribute), these parameters are encrypted based on the K_encr key received in step 4.

6-8. The UE verifies the AUTN, generates the session keys (MSK, EMSK, K_aut, K_encr, etc) and derives the Result (RES) which is sent to N3IWF in an EAP-RSP/AKA-Challenge message. The N3IWF sends an Authentication Response (RES) to CP functions over NG2. As normally, the CP functions verify RES and, if correct, they respond with an Attach Accept message. This message may include parameters (referred to as IEs in the above figure) that should be transferred to UE, e.g. a new temporary UE identity.

   In step 8c the N3IFW receives also the session keys (MSK, EMSK) which are needed to protect the WLAN air interface traffic. The MSK is further transferred to the WLAN access network (in step 13a) in order to derive the Pairwise Master Key (PMK), as defined in the IEEE 802.11 specification.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 359 of 501

9. The N3IWF derives a 'DTLS key' (e.g. from EMSK) which will be needed later for the establishment of a secure DTLS connection with the UE. The same 'DTLS key' is also derived by the UE after the successful authentication in step 15.

10. The N3IWF sends an EAP-REQ/AKA-Notification message to UE which includes the address of N3IWF and other parameters (IEs) that were included in the Attach Accept message (e.g. a new temporary identity). After step 10b, the Adaptation layer in the UE creates an Attach Accept message and sends it to the NAS layer. Note: A legacy UE will ignore the address of N3IWF and the other parameters (IEs).

11-12. The UE responds with an EAP-RES/AKA-Notification which triggers the N3IWF to send an Attach Complete message to CP functions.

13. The EAP authentication procedure completes with an EAP-Success message. The N3IWF creates a UE Context which stores information such as the UE MAC address, the UE identity (included in the Attach Accept message), the EAP-AKA' identities of the UE (e.g. a pseudonym and/or fast re-authentication identities), etc.

14. At this point, the UE is connected to the WLAN access network and can establish layer-3 connectivity, e.g. by receiving IPv4 address via DHCP. The UE can then use the WLAN for NSWO traffic.

15. After successful authentication the UE derives the 'DTSL key' as discussed above.

16. The Adaptation layer in the UE receives the address of N3IWF and the 'DTLS key' and establishes a secure DTSL connection to N3IWF (DTLS with pre-shared key as defined in RFC 6347). Note that the same procedure has been specified to protect the WLCP signalling between the UE and a TWAG (see TS 33.402).

17. The Adaptation layer in the UE notifies the NAS layer that the attachment via trusted WLAN access is completed. It also provides to the NAS layer the IEs provided by the network in the Attach Accept message (and received by the UE in step 10b).

    After this step, the NAS layer in the UE may initiate NAS signalling with the CP functions in the network in order e.g. to setup a PDU session over WLAN access.

Editor's note: The attach procedure shown in figure 6.8.x.2.4-1 needs to be updated to indicate how NAS security is setup between the UE and CP functions.

6.8.7.2.5 PDU session setup via Trusted Non-3GPP Access

A PDU session is established via trusted non-3GPP access as shown in the figure below.

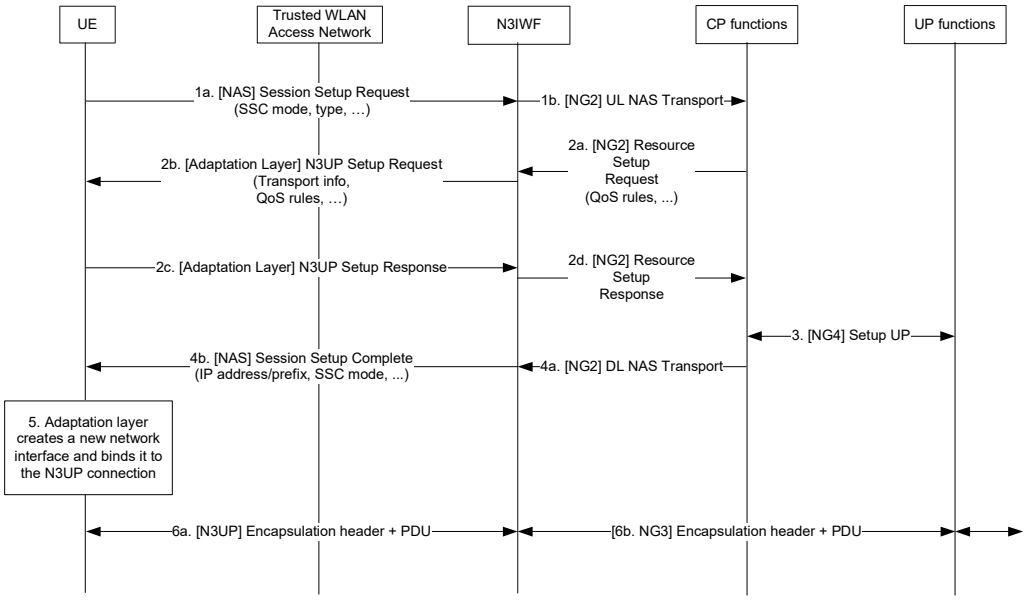


Figure 6.8.7.2.5-1: PDU session setup via Trusted WLAN

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 360 of 501

1. UE sends a Session Setup Request message via the established DTLS channel which is relayed by N3IWF to the CP functions. Essentially, message 1a is an Adaptation layer "UL NAS Transport" message which encapsulates the Session Setup Request.

2. The CP functions send a Resource Setup Request message to N3IWF via NG2. This message is the same as the one used for 3GPP access and may include QoS rules that can be applied for flow-based QoS (as per solution 2.2). In turn, the Adaptation layer in N3IWF initiates a new N3UP connection setup procedure and transmits an Adaptation layer "N3UP Setup Request" to UE. The purpose of this setup procedure is to establish an N3UP connection between the UE and N3IWF that can be used to transport all traffic of the PDU session. The Transport info includes information required to establish this connection e.g. a MAC address of N3IWF (same as in SaMOG), information for setting up a L2 or L3 tunnel, etc.

Editor's note: The type of N3UP connection established between the UE and N3IWF is FFS.

3. After the N3UP connection is setup, the CP functions setup the UP with the UP functions over NG4.

4. The CP functions respond with a Session Setup Complete message which typically includes an assigned IP address/prefix for PDU sessions of IP type, the selected SSC mode, etc.

5. The Adaptation layer in the UE creates a new network interface (e.g. a new IP interface) and binds this interface to the established N3UP connection. All traffic sent by the UE on this interface will be transferred to N3IWF via the N3UP connection and then to the corresponding NG3 tunnel.

6. Data traffic (PDUs) sent over the N3UP connection is encapsulated into a N3UP header, which can carry e.g. a Flow Priority Indicator (FPI), a Reflective QoS Indicator (RQI) or other parameters according to the selected QoS solution.

6.8.7.2.6 Attach via Untrusted Non-3GPP Access

The attach procedure via untrusted non-3GPP access is shown in figure 6.8.x.2.6-1 and is very similar to the attach procedure via trusted non-3GPP access (shown in figure 6.8.x.2.2-1). The differences are the following:

1. Step 1b: There is no 3GPP-based authentication over the WLAN. The UE instead can use any non-3GPP method to authenticate and connect with the WLAN, e.g. no authentication (in case of a free WLAN), EAP with pre-shared key, username/password, etc.

2. Step 1d: The UE needs to discover the IP address of N3IWF. This is performed with the existing procedures for ePDG discovery.

3. The establishment of a secure IPsec tunnel between the UE and N3IWF (steps 2-8) is triggered by the NAS layer in the UE which sends an Attach Request to the Adaptation Layer. The Adaptation Layer does not forward this Attach Request but instead it initiates the normal IKEv2 procedure for establishing an IPsec tunnel with the N3IWF. During this IPsec tunnel establishment the N3IWF initiates an Attach procedure over NG2 and then performs interworking between the attach signaling and the IKEv2/EAP-AKA' signaling. If this attach over NG2 is successful, the IPsec tunnel is established and it can be used to exchange NAS signaling between the UE and the CP functions.

   Once the UE is authenticated and the IPsec tunnel is established, a NAS Security Mode Command (SMC) runs between the CP functions and UE (over NG2 and IP). Subsequently any NAS signaling exchanged between the UE and CP functions is sent over NG2 and NWu (over IP) and is protected by NAS security. Note that the NAS SMC may be replaced by an equivalent procedure in NG (this is under SA3 responsibility).

Editor's note: It is FFS how the signalling shown in figure 6.8.7.2.6-1 can be modified to cover also the cases when the UE uses an EAP authentication method other than EAP-AKA'.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 361 of 501

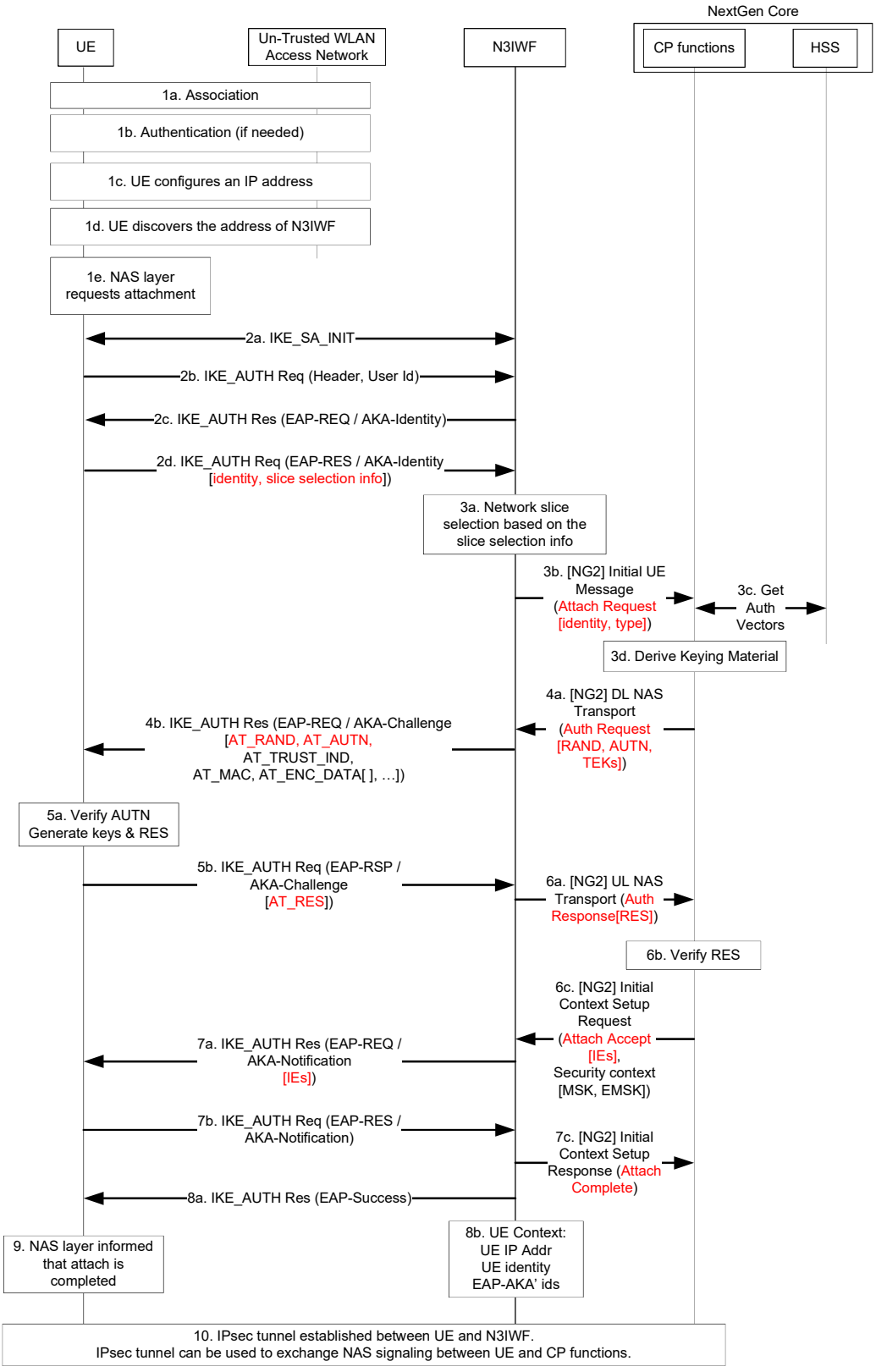


Figure 6.8.7.2.6-1: Attach procedure via Untrusted WLAN using the NG2 interface

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 362 of 501

6.8.7.2.7 PDU session setup via Untrusted Non-3GPP Access

The same procedure as the one shown in figure 6.8.7.2.5 applies (for the PDU session setup via trusted non-3GPP access). The only difference is that the N3UP connections are established over the IPsec tunnel.

Editor's note: It is FFS if the use of a single IPsec tunnel (for both CP and UP traffic) creates any limitations to QoS.

6.8.7.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.8.8 Solution 8.8: Architecture for support of untrusted Non 3GPP access

6.8.8.0 Overview

The solution applies only to UE that support NGC NAS.

The solution focuses specifically on the support of untrusted Non 3GPP access in the NextGen architecture and addresses Key Issue #8.

Editor's note: A similar solution should be defined for Trusted WLAN access to NGC where a ngTWAN would play a similar role than the ngPDG.

The key points of the architecture are:

- introduction of a Non-3GPP Core Network interworking function called ngPDG in this solution) standardized as part of the NextGen CN. The ngPDG supports:
  - a control plane component for the establishment of a secure tunnel between the UE and the network (via IKEv2) . For this purpose it interfaces to other CN CP functions in the CN via NG2. A subset of NG2 capabilities is used including at least the relay of NAS signalling between the UE and the CN CP functions.
  - a user plane component, implementing the termination of an IPSec secure tunnel between the UE and the ngPDG in order to provide secure access to the NextGen CN over the untrusted WLAN to the UE. The traffic of multiple PDU sessions for the same UE is multiplexed over this IPSec tunnel.. In case of Home Routed deployment, a ngPDG located in the VPLMN supports charging and LI requirements for the VPLMN

NOTE: the ngPDG is a function defined by SA2.

- the interface between the UE and the CN control plane functions beyond the ngPDG is NG1. NG1 is transported transparently between the UE and the CP functions in the CN, using IP transport between the UE and the ngPDG.
- IPSec tunnels are established between the UE and the ngPDG function upon UE attach to the network, and protectsuser plane data and subsequent NG1 signalling between the UE and the CP functions in the CN. The attach procedure is separate from the PDU session establishment procedure.

The architecture proposes that ngPDG acts both as a control plane and a user plane function but does not aim at defining an internal interface within the ngPDG. The ngPDG acts as an evolution of an ePDG in the EPC.

In this solution, the following is assumed:

- the UE is dual radio, i.e. can connect to both a 3GPP RAN and the untrusted N3GPP AN;
- the protocol stack the UE uses over untrusted N3GPP AN is different from the protocol stack the UE uses over an NG RAN, similarly to the way the protocol used between a UE and the ePDG in EPC is different from the protocol used by the UE with a RAN connected to the EPC. Nevertheless some layers are common e.g. SM NAS signalling is used between the UE and SMF regardless of whether the UE is using 3GPP or Untrusted access.
- one secure tunnel between the UE and the ngPDG is used for the support of multiple PDN connections, with security over the untrusted radio secured by a single security context for all the UE PDU sessions
- attach is initiated by the UE by indicating "a desire to use EAP by leaving out the AUTH payload from the first message in the IKE_AUTH exchange " sent over IKEv2 (NWu)., Once the UE has been authenticated by the CP Functions, the IPsec tunnel is established and a NAS Security Mode Command (SMC) is run between MMF and

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 363 of 501

UE (over NG2 and IP). From there any NAS signalling exchanged between the UE and the network is sent over NG2 and IP over NWu and is protected by NAS security.

Editor's note: The NAS SMC may be replaced by an equivalent procedure in NG, This is under SA3 responsibility.

6.8.8.1 Architecture description

As an UE may set up multiple PDU sessions in association with a single IKE session, thus in association with a single IP address managed by the ngPDG there is the need to multiplex the flows of these PDU sessions on top of the IP address seen by the IKE and IPSec layer of the ngPDG. This also allows setting-up PDU session for non IP services over a ngPDG. This multiplexing requires some signalling between the UE and the network to signal to the UE the association between a PDU session and the multiplexing Identifier to be used over NWu.

In case of a PDU session working in Home Routed mode, the ngPDG (in the VPLMN) needs to support VPLMN charging and LI. This requires a NG4 interface from the SMF to the ngPDG

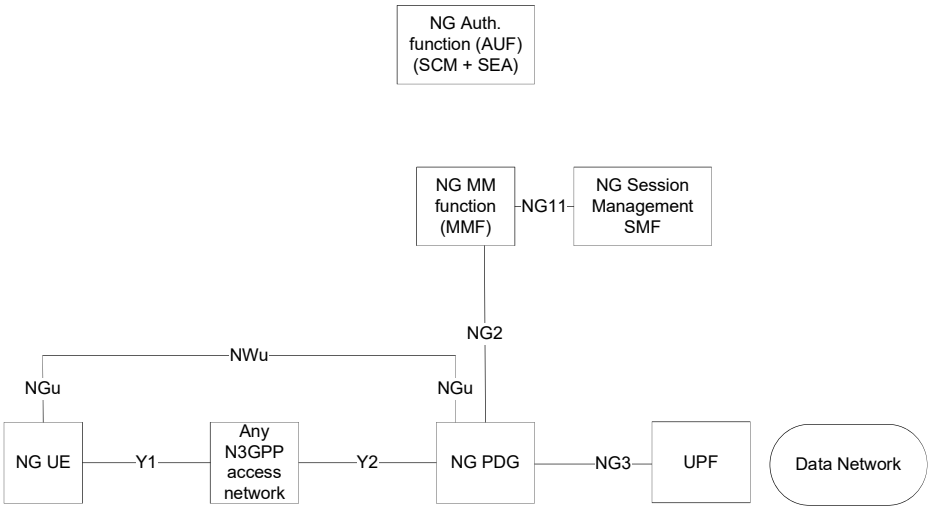


Figure 6.8.8.1-1: Architecture for NextGen CN access via untrusted Non 3GPP access (non roaming or LBO case)

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 364 of 501

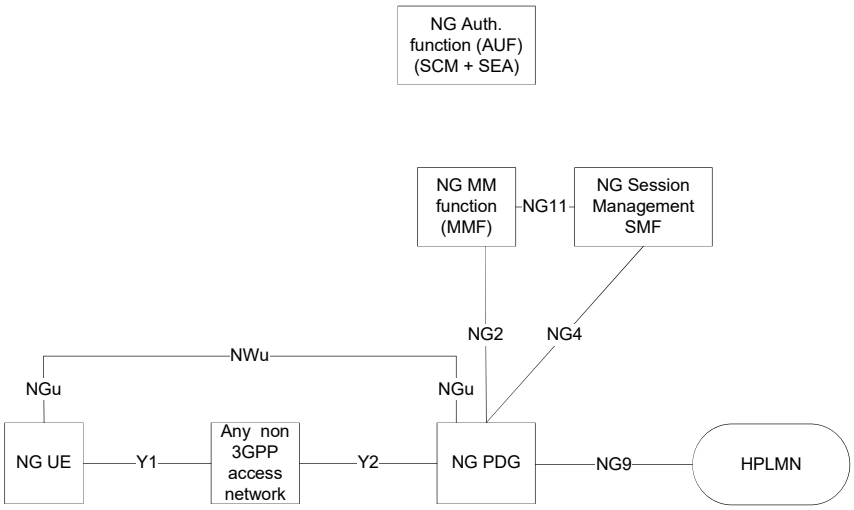


Figure 6.8.8.1-2: Architecture for NextGen CN access via untrusted Non 3GPP access (Home Routed case)

Following reference points are introduced:

Y1: Reference point between the UE and the non-3GPP access (e.g. WLAN).

Y2: Reference point between the untrusted non-3GPP access and the ngPDG for the transport of UE user plane and the transport on NWx.

NWuNWu: NWu represents interface between the UE and ngPDG for establishing a secure tunnel between the UE and the NextGen CN, similar to the interface between the UE and the ePDG, and for securing the control plane and user plane exchanged between the UE and the NextGen CN. The control plane is further secured by NAS security end to end between UE and CCF (MMF).

NG2, NG3, NG4, NG9: As defined in the overall architecture.

NOTE: EAP signalling is sent over NAS and over NG2

Editor's note: In Home Routed case the SMF controls the ngPDG via NG2 and via NG4. This configuration requires Further studies

Editor's note: potential optimizations where the ngPDG would fully act as an UPF e.g. where the ngPDG would terminate both NWu and NG6 are FFS. These optimizations would require an NG4 interface from SMF also in case of non roaming and LBO.

6.8.8.2 Function description

The proposed architecture is characterized by the following functionality:

- The UE obtains an IP address from the Non-3GPP access.

NOTE 1: Potential UE authentication with the Non-3GPP access and the way for the UE to get an IP address to reach the ngPDG are out of scope (as the access network and Y1 are undefined in case of Untrusted access).

- The UE discovers and selects an ngPDG, similarly to the way a UE selects an ePDG in EPC.
- The UE performs procedures (e.g. IKEv2) over NWu for the establishment of an IPSec tunnel with the ngPDG.
- attach is initiated by the UE by indicating "a desire to use EAP by leaving out the AUTH payload from the first message in the IKE_AUTH exchange" sent over IKEv2 (NWu).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 365 of 501

1. The UE sends an initial IKE-AUTH. This is understood by the UE and the network as an ATTACH request. The ngPDG generates an ATTACH request on behalf of the UE that contains an EAP-Resp/Identity created based on IDi provided by the UE and sends it over NG2. The ATTACH request may contain also other information extracted from IKE signalling generated by the UE.. This triggers Core CP to initiate UE authentication and to create a context associated with the UE.

2. The UE gets authenticated (further IKE-AUTH exchanges).

3. When IKE authentication succeeds a cryptographic key can be provided by the CN to the ngPDG (via NG2) in order to complete UE authentication within IKEv2 and allow the establishment of the IPsec tunnel between the UE and the ngPDG.

4. A NAS Security Mode Command (SMC) is run between MMF and UE (over NG2 and IP). From there any NAS signalling exchanged between the UE and the network is sent over NG2 and IP over NWu and is protected by NAS security.

5. The MMF sends to the UE a NAS ATTACH Accept that may contain any 3GPP defined parameters.

- As part of IKE signaling the ngPDG provides also the UE with following configuration information:
  - addressing information for the UE to send its NAS signaling (addressing information for NAS); and
  - addressing information for the UE to send its User plane flows (addressing information for User plane tunneling).

NOTE 2: This addressing information may actually correspond to internal resources in the ngPDG. This would ensure that the UE does not have direct IP access to Core CP (that could reachable only via private IP address range)

- The UE exchanges any further NG1 (NAS) signalling (e.g. PDU Session Establishment) with the CN CP functions over the secure tunnel established with the ngPDG and over NG2 between the ngPDG and the CN CP functions. Such signalling is transported over UDP/IP in the IPSec tunnel between the UE and the ngPDG. The NAS signalling is extracted by the ngPDG and forwarded to the CP Functions over NG2.

Editor's note: it is FFS whether further MM signalling is required for the UE in this solution besides attach. This depends on mobility solutions defined for mobility between an NG RAN and untrusted WLAN.

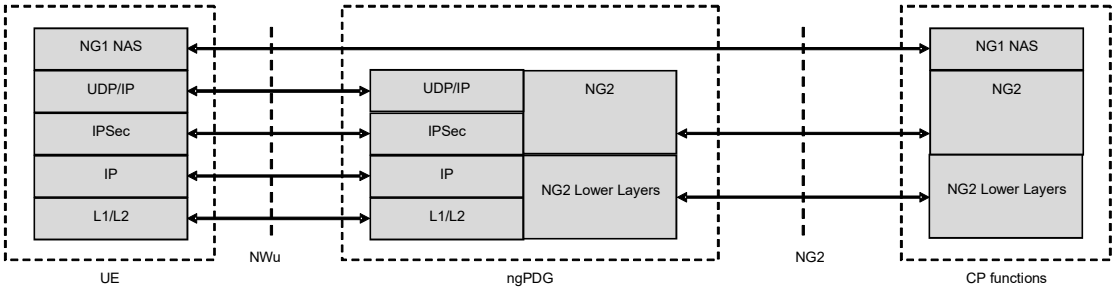


Figure 6.8.8.2-1: Protocol stack for signalling transfer once NAS SMC has been exchanged

- User plane transport over NWu: The traffic of multiple PDU sessions for the same UE is multiplexed over an IPSec tunnel set-up via IKE. Multiple multiplexing solutions may be envisaged depending on whether the IPSec tunnel set-up via IKE works in tunnel or in transport mode. The following refers to the case where IPSec in tunnel mode would be used.

  The outermost IP address of a PDU packet exchanged over NWu is the IP address allocated by the non-3GPP access network and serves to route the packet between the UE and the ngPDG. It is stripped off by the ngPDG when it receives UL traffic from the UE.

  The IP address allocated to the UE as part of IKE signaling serves as the address of a tunnel (over NWu) where the traffic of multiple PDU sessions may be multiplexed. This level of multiplexing allows to exchange traffic belonging to multiple PDU sessions within a single IPsec tunnel. It also supports the exchange of traffic of PDU sessions for non IP services.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 366 of 501

This means that the IP address allocated to the UE as part of IKE signaling is not the IP address with which the UE is reachable over the Data Network (DN) (is not the IP address provided to the applications on the UE) ; the IP flows of the applications on the phone are encapsulated within an IP based tunnel using as a transport address the IP address allocated to the UE as part of IKE signaling.

Editor's note: It is FFS Whether IPSec is set up in tunnel or in transport mode . The solution currently assumes tunnel mode.

Editor's note: It is FFS How QoS of PDU flows maps onto potential CHILD SA.

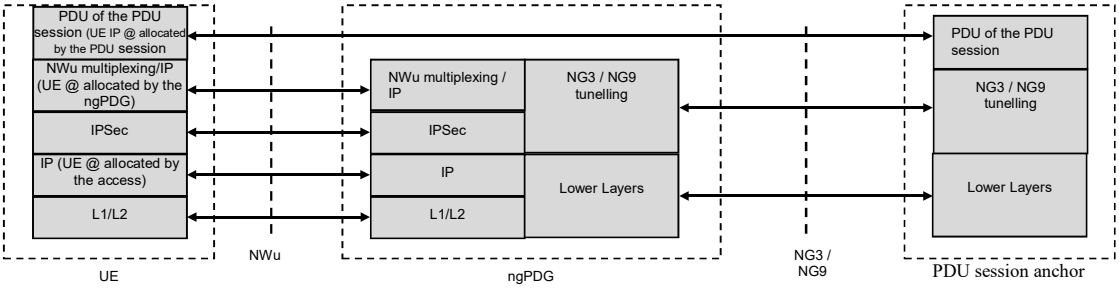


Figure 6.8.8.2-2: Protocol stack for the User plane

- The main differences between this solution and an ePDG-based solution are:
  - the ngPDG interfaces over NG2 with the core network CP Functions for UE attachment authentication, encapsulating the EAP signalling for the authentication in NG2.
  - the UE exchanges explicit SM signalling for the establishment of PDU Sessions over the IPSec tunnel established with the ngPDG between the UE and the ngPDG. The ngPDG extracts the NAS signalling and routes it over, NG2 between the ngPDG and the core network CP functions.

NOTE: This means that as opposed to ePDG, the ngPDG is not involved in PDU session set-up (e.g. is not responsible of checking whether the parameters requested by the UE in a PDU session related request are compliant with the subscription or is not responsible of selecting a PDU session anchor). Furthermore the ngPDG does not handle subscription data for the UE

Editor's note: How QoS is supported for different PDU session may be based on the solutions developed for the ePDG solution in the EPC and is FFS.

- upon PDU session establishment, user plane function selection is performed. The ngPDG can be selected as the only user plane function for the UE, acting as a GW towards data networks, or separate user plane function(s) can be selected and interconnected to the ngPDG via NG9.

Editor's note: When UE is connected via both 3GPP and non-3GPP access, the impact of multiple NG1 instances on mobility management solutions is FFS in terms of the mobility management model maintained by the network for the UE.

- The ngPDG performs the following additional functionality:
  - Routing of packets from/to the NextGen CN to/from UE by interfacing via NG3 or NG9 with other user plane functions.
  - De-capsulation/Encapsulation of packets for IPSec.
  - Local mobility anchor within untrusted non-3GPP access networks using MOBIKE (if needed).

Editor's note: ngPDG functionality in terms of transport of level packet marking and QoS Enforcement are FFS and depend on the QoS solutions defined in NextGen.

The proposal has the following difference with respect to the use of NG2 for NG RAN:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 367 of 501

- No Hand-Over signalling takes place over NG2 when it is terminated in ngPDG. This does not preclude the ngPDG from supporting intra N3GPP access mobility such as defined by MOBIKE.
- Information exchanged over NG2 in case of RAN (e.g. list of supported TAC) is not exchanged over NG2 when it is terminated in ngPDG.
- EAP signalling is sent over NAS and over NG2.

6.8.8.2.1 Initial attach procedure for Untrusted N3GPP Access

The call flow in Figure 6.8.8.2-1 describes the Attach procedure via untrusted N3GPP access.

NOTE 1: The whole procedure is to be fine tuned based on SA3 feedback and based on further definition of NG2 procedures.

Editor's note: This version of the solution decribes only option A in 6.8.6.2. A revised version is needed to also describe option B.

In this procedure it is assumed that:

- EAP is transported in IKEv2 between UE and ngPDG for the IPSec tunnel establishment.
- The EAP-based authentication during the establishment of the secure tunnel via IKEv2 triggers an attach procedure; When the ngPDG determines through the received IKE_AUTH request that the UE needs to be authenticated via EAP the ngPDG sends an EAP Identity Response message within an ATTACH message sent over NG2.
- The ngPDG extracts the EAP messages and forwards them to the CP Functions over NG2 to carry out the authentication in the CP AU function.

Solution 8.8: Support standalone non-3GPP access via NG2/NG3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 368 of 501

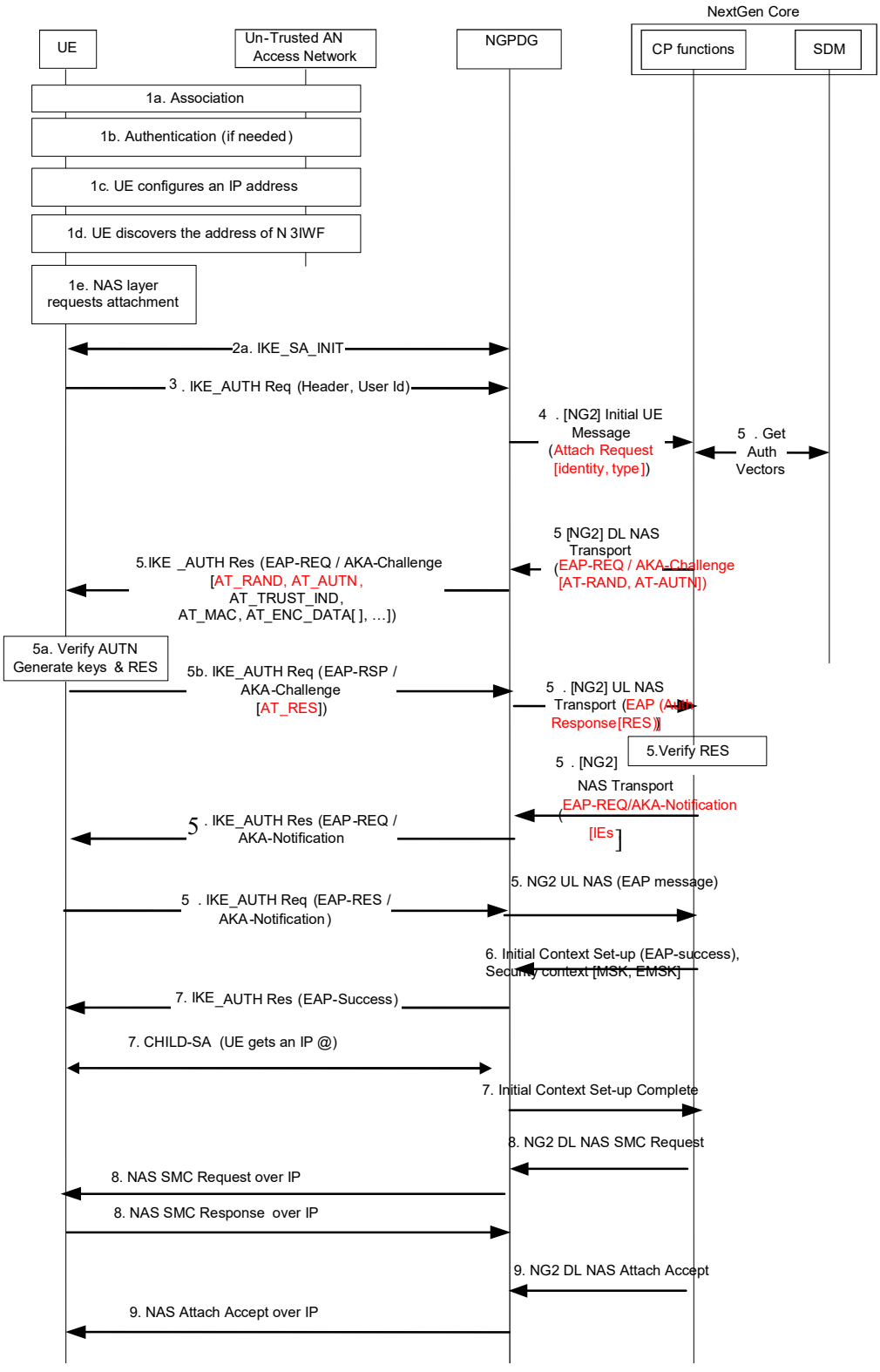


Figure 6.8.8.2.1-1: Attach procedure for untrusted N3GPP access

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 369 of 501

The call flow is as follows:

1. The UE gains IP connectivity with the untrusted N3GPP AN.

NOTE 2: Potential UE authentication with the Non-3GPP access and the way for the UE to get an IP address to reach the ngPDG are out of scope (as the access network and Y1 are undefined in case of Untrusted access).

2. The UE discovers a ngPDG via a procedure similar to ePDG discovery of Rel. 13 and initiates the IKE setup procedure via an IKE_SA_INIT exchange, triggered by the need to attach over untrusted N3GPP AN.

3. The UE sends the user identity (in the IDi payload) in the first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ngPDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format. The UE shall send the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to indicate it desires to obtain an IPv4 or IPV6 Address. This step is equivalent to step2 of Initial Attach as described in33.402 (Rel13) apart that it does **not** provide "APN information (in the IDr payload)".

4. The ngPDG creates an ATTACH request that contains an EAP-resp/Identity created based on IDi provided by the UE and sends it over NG2.

5. This triggers Core CP to initiate UE authentication and to create a context associated with the UE. The Core CP Functions exchanges EAP signalling with the UE. This EAP signalling is exchanged back and forth via EAP over NAS over NG2 and via EAP sent over IKE over SWu. The N3IWK/ngPDG relays transparently the EAP signalling.

NOTE 3: This is similar to what takes place in EPC where the ePDG relays EAP signalling back and forth between EAP over AAA (SWm) and EAP sent over IKE.

6. When EAP authentication succeeds the CN provides to the ngPDG (via NG2) with:

   - An EAP-Success message to be transferred over SWu to the UE.

   - a cryptographic key in order to complete the IKEv2 set-up procedure and allow the establishment of the IPsec tunnel between the UE and the ngPDG.

NOTE 4: Whether this step corresponds to one or 2 NG2 exchanges is to be fine tuned based on further definition of NG2 procedures.

7. The ngPDG sends an EAP Success to the UE over IKEv2 and completes the IKE set-up with the UE (checking the correctness of the AUTH sent by the UE). As part of this procedure the ngPDG provides the following information which completes the KE procedure and the UE attachment to the network:

   - addressing information for the UE to send its NAS signaling (addressing information for NAS); and

   - addressing information for the UE to send its User plane flows (addressing information for User plane tunneling).

8. A NAS Security Mode Command (SMC(NAS security algorithms, etc.. parameters to be defined by SA3) is run between MMF and UE (over NG2 and IP). From there any NAS signalling exchanged between the UE and the network is sent over IP over NWu and is protected by NAS security.

9. The MMF sends to the UE a NAS ATTACH Accept that may contain any 3GPP defined parameter. This is transparently relayed towards the UE by the ngPDG.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 370 of 501

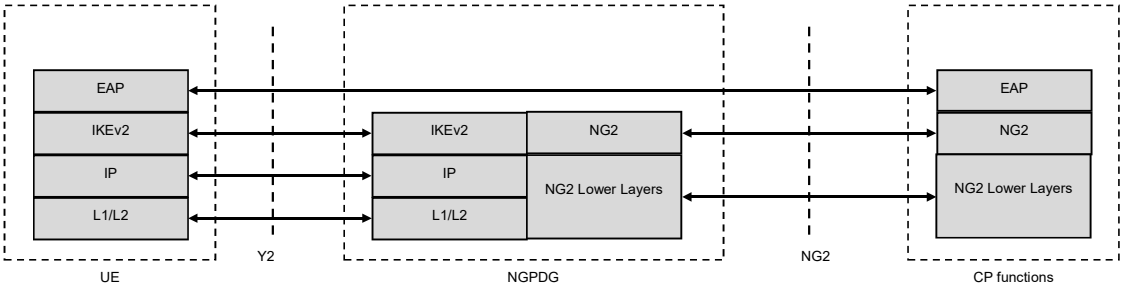


Figure 6.8.8.2.1-2: Protocol stack for Attach procedure

NOTE 5: Whether EAP can be sent directly over NG2 or needs to be further encapsulated in NG1 is to be fine tuned based on further definition of NG2 procedures.

6.8.8.2.2 PDU session establishment via untrusted N3GPP access

This sub-clause assumes that a NAS Security Mode Command (SMC) has run between MMF and UE (over NG2 and IP).

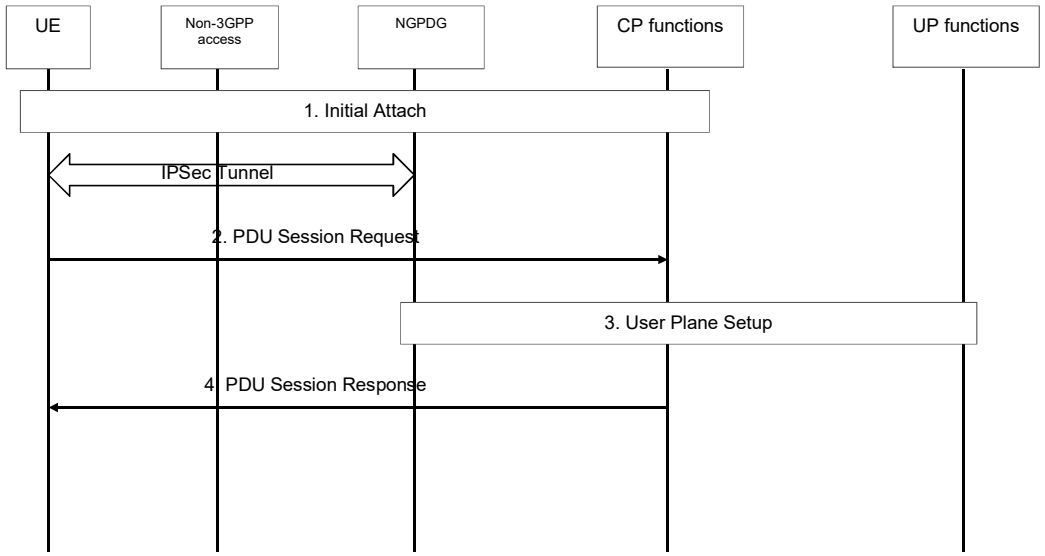


Figure 6.8.8.2.2-1: PDU session establishment via non-3GPP access procedure

Once the initial attach procedure as described in subclause 6.8.8.2.1 is completed, the UE can initiate PDU session establishment procedure as described in Figure 6.8.8.2.2-1 above.

1. The UE performs the attach procedure over non-3GPP access as shown in subclause 6.8.8.2.1.
2. The UE sends a NAS PDU session request message to the CP function over UDP. The UE sends the request to the addressing information for NAS obtained as part of IKE signalling and uses a specific UDP port number (either a standardized value or a value assigned during the IKE procedure), and encapsulates it in an IPSec packet. The ngPDG de-capsulates the received message and forwards it to the CP function via NG2 interface.
3. The CP function performs the UP setup (including UP function selection).
4. The CP function sends a PDU session response message to the UE. The PDU session response message is sent over NG2 and is encapsulated in an IPSec packet by the ngPDG.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 371 of 501

The protocol stack for the SM signalling exchange is described below.

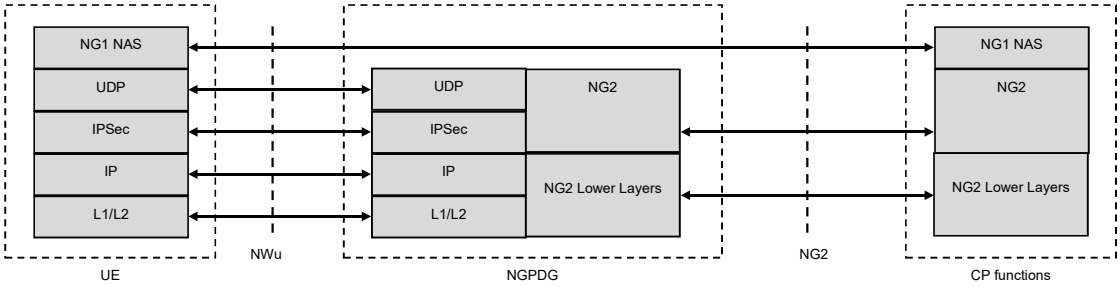


Figure 6.8.8.2.2-2: Protocols for signalling exchange once the IKE phase has successfully completed

6.8.8.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.9 Void

6.10 Solutions for Key Issue 10: Policy Framework

6.10.1 Solution 10.1: Policy Framework alternative solution 1

In this solution, it is proposed to reuse the existing EPC's policy framework with the modifications needed for supporting the Control and User Plane split as described below.

NOTE: The rationale behind this solution is that:

- In case there is separate key issue for some specific functionality potentially interacting with Policy Framework (e.g. 3rd party interactions etc.), the results of that key issue resolution may influence Policy Framework and will be considered once the corresponding key issue is stable.
- In case there are no new NextGen requirements for some particular functionality, it is assumed that the functionality and handling remains same as in case of EPC.

6.10.1.1 Overall policy architecture

Overall roaming and non-roaming policy related architecture is the same as defined by the TS 23.203 [3] with the same functionality and the same functional entities, except the following deviations:

Editor's note: The functionality of Policy Framework in case of roaming architecture depends on overall roaming architecture agreed for NextGen.

1. Following User and Control split concept adopted for R14 CUPS architecture, User and Control Plane Functions will support Policy related functionality following the similar split principles as defined by CUPS for policy-enforcing functional split.
   a. Correspondingly, the Control Plane entities resulted from the split will interface with Policy and with Charging Functions.

Editor's note: It is FFS whether there is a single or multiple Control Plane entities serving a different/ multiple User-Plane entities communicating with Policy Function for getting the policy enforcing rules. It will also depend on outcomes of

key issues#4-6 about the possible User Plane entities that may be used to enforce the policies received from the Policy Function

key issue#7 on Network function granularity and interactions between them.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 372 of 501

Editor's note: Policy Control for non-IP traffic is FFS.

NOTE: The split will depend on overall functionality, subject to eventually selected solutions for the other key issues.

2. The NextGen policy protocols shall be designed with consideration of the outcomes of the Key issue 7: Network function granularity and interactions between them, in purpose of realizing a common approach.

In addition, the following corresponding modifications may be needed once the corresponding key issue's solution is stable:

3. QoS control solution will be determined based on outcomes of Key Issue 2 : QoS. Existing QoS enforcement actions (bandwidth limitation, redirection, gating etc.), if applicable in the NextGen QoS model, shall be preserved.

4. Potential interaction with Access Network Discovery and Selection Framework is FFS and will be determined based on outcomes of Key Issue 17: 3GPP architecture impacts to support network discovery and selection.

5. Potential interaction with access traffic steering, switching and splitting is FFS and will be determined based on outcomes of Key issue 20: Traffic Steering, Switching and Splitting between 3GPP and non-3GPP Accesses.

6. Potential interaction with 3rd party provided services is FFS and will be determined based on outcomes of the Key issue 9: 3GPP architecture impacts to support network capability exposure.

7. Potential interaction with Session management is FFS and will be determined based on outcomes of the Key issue 4: Session management.

8. Potential interaction with Mobility management is FFS and will be determined based on outcomes of the Key Issue 3: Mobility management framework.

9. Potential interaction with Network Slicing is FFS and will be determined based on outcomes of the Key issue 1: Support of network slicing.

6.10.2 Solution 10.2: Analytics-based Policies

Editor's note: The details for this solution can be considered after phase 1.

This solution addressed key issue 10 on Policy Framework and specifies functional elements in this framework that can generate the analytics-based policies. The goal of the analytics-based policies is to enable operators better understand the behaviour of mobile users and accordingly provision the network with dynamic policy that improves the network performance and the user experience.

The solution is based on a functional element in the Policy Framework, referred to as the Analytics Function. The Analytics function takes measurements (also called "usage reports") from the UE and from various network functions, processes these measurements (e.g. by applying Big Data and Analytics techniques) and derives meaningful trends or patterns describing the behavior of the users and their devices. Examples of such trends / patterns are given below.

6.10.2.1 Architecture description

The following figure shows the high-level architecture of the solution.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 373 of 501

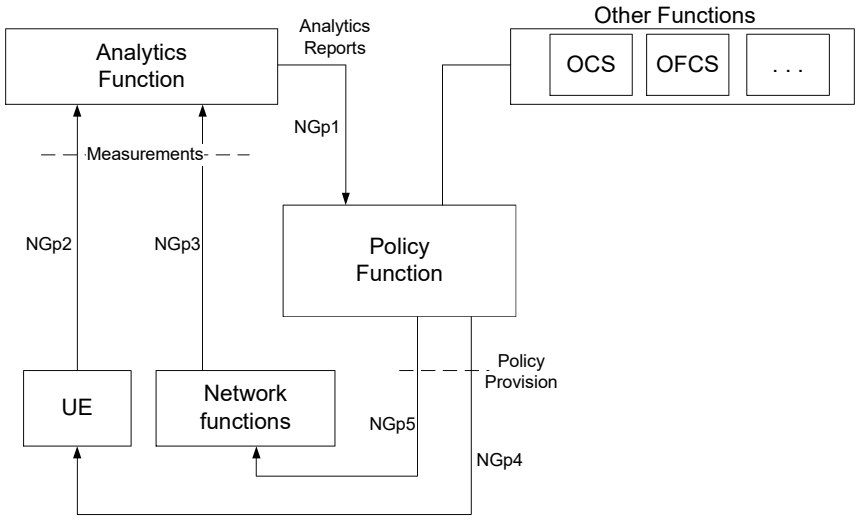


Figure 6.10.2.1-1: High-level architecture for analytics-based policies

Elements of the architecture:

UE

The UE collects usage data (aka measurements) and forwards this data to the Analytics function via NGp2.

The UE does not send usage data in real-time. Such data is internally collected in the UE and is sent to the Analytics function in batches, e.g. every X hours when battery is above 50%, or when the size of the collected data exceeds a threshold, etc. The Analytics function provides to UE the events that can trigger the transmission of a usage report which contains the collected usage data, as well as the types of usage data that should be collected by the UE.

Editor's note: It is FFS which usage data should be collected by the UE.

As an example, a usage report sent by the UE can contain the following usage data:

- Report duration: 10:35am - 11:35pm
- Battery level: 65% at 10:47am
- Battery consumption rate: 8% per hour
- Battery charging: 11:06am - 11:23am
- Visited cells: (Cell-1, entry time, exit time), (Cell-2, entry time, exit time), … These cells are visited in Idle mode and thus may not be known to the network.
- Connected WLANs: (SSID-x, connection time, disconnection time), …
- Apps used: (YouTube, start time, end time), (Skype, start time, end time), …
- Location: (X1, Y1, Z1 @ 10:36am), (X2, Y2, Z2 @ 11:14am)
- Speed: 5Km/h @ 10:38am

NOTE 1: To address potential privacy concerns, the UE is expected to obtain user's consensus before sending usage reports to the Analytics Function.

Analytics Function

The Analytics Function collects the "usage data" provided the UE (via NGp2) and generates Analytics reports, i.e. data that shows meaningful patterns or trends for the mobile user and the UE. These reports can then be provided to the Policy Function (via NGp1) and can be used by the Policy Function to dynamically generate analytics-based policy

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 374 of 501

rules. The Analytics Function is a logical function and can be implemented within the Policy Function, if needed, or in a separate application server.

Examples of UE-specific analytics reports that can be generated by the Analytics function include the following:

1. "From 5pm to 8pm battery drops to 20% or below"
2. "Device connects to WLAN SSID-x from 8pm to 6am"
3. "On weekdays the location of the device follows the same path X"
4. "Video streaming is used from 9pm to 10pm"

Each one of the above analytics reports can be associated with a *confidence value* showing how likely the outcome of the report is to happen.

As shown in Figure 6.10.2.1-1, the analytics function may also collect measurements from various network functions via NGp3. For example, a NextGen radio cell may send load data to the Analytics function or a UP element in the NextGen CN may send traffic rate data or traffic type data (e.g. data about streaming traffic, voice traffic, etc.). By using the network provided data, the Analytics function can generate network-specific analytics reports such as:

1. "From 6am to 9am the average radio resource utilization in cell-x exceeds 90%"
2. "From 8am to 10am the video streaming rate in area-x exceeds 100Mbps for 95% of time"

Editor's note: The provision of measurement data from various network functions is typically addressed by SA5. It is FFS if this solution should consider measurement data provided by network functions.

Policy Function

The Policy Function receives the analytics reports generated by the Analytics function (via NGp1) or pulls the analytics reports from a data-storage in case these reports are placed in a data store. Based on these analytics reports and their confidence values, the policy function may dynamically generate analytics-based policy rules and provide these rules to UE (via NGp4) or to some network functions (via NGp5). The NGp5 and NGp4 interfaces are considered general policy-provisioning interfaces and may not be specific to this solution. How policy is provisioned via NGp5 and NGp4 is considered a general policy issue and is not specified in this solution.

Some examples of the analytics-based policy rules that may be generated by the policy function are provided below.

1. Based on the analytics report "From 5pm to 8pm battery drops to 20% or below"
   - The policy function may create routing policy that steers video sessions established by the UE between 5pm and 8pm to a video transcoder configured to apply power-efficient video coding (note that state-of-the-art codecs like the H.264/AVC or HEVC suffer from very high complexity and thus can consume a lot of energy in the UE). Similarly, voice sessions established by the UE between 5pm and 8pm may be enforced to utilize power-efficient voice codecs. In addition, the policy function may enforce new QoS policy between 5pm and 8pm (e.g. apply higher scheduling priority) so that data transfer delay (and hence battery consumption) is minimized.
2. Based on the analytics report "Device is located in cell-x from 10am to 2pm"
   - The policy function may create paging policy so that the network pages the device only in cell-x (not in a range of cells as usually) between 10am and 2pm.
3. Based on the analytics report "Video streaming is used from 9pm to 10pm"
   - The policy function may create new policy that optimizes the streaming experience from 9pm to 10pm, e.g. create new QoS policy or invoke a video optimizer.
4. Based on the analytics report "On weekdays the location of the device follows the same path X"
   - The policy function can predict the location of the UE and can create appropriate paging policy or create policy to optimize the mobility procedures in the network.

Other Functions

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 375 of 501

The Other Functions (e.g. the Online Charging, the Offline Charging, the billing function, etc.) are shown in Figure 6.10.2.1-1 for completeness. They are outside the scope of this solution.

6.10.2.2 Functional Description

Editor's note: This clause is FFS.

6.10.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.10.3 Solution 10.3: Policy function and framework for non-roaming case

This solution addresses Key issue 10, WT#1, i.e. an overall non-roaming policy framework for NextGen is described.

6.10.3.1 Architecture description

The figure 6.10.3.1-1 shows the NextGen policy architecture for non-roaming case.

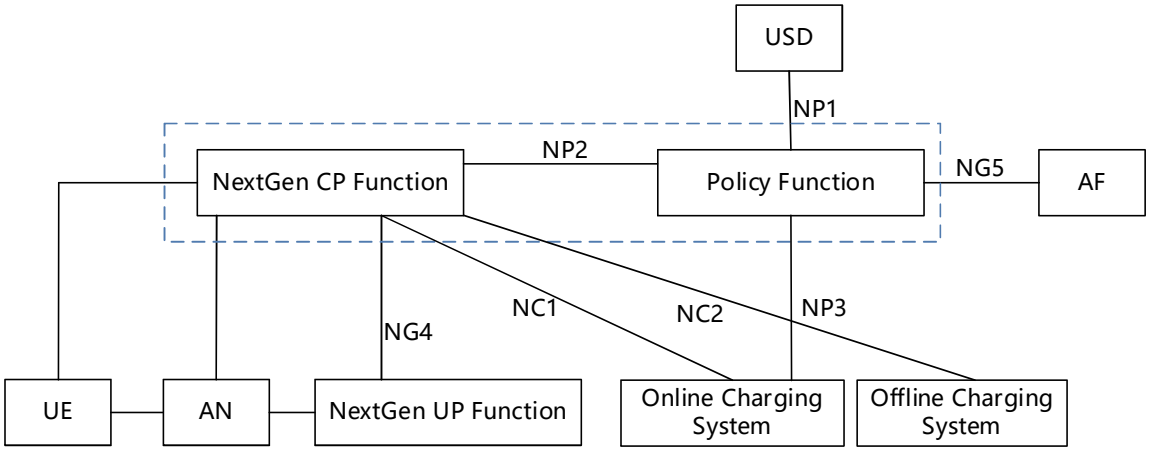


Figure 6.10.3.1-1: Non-roaming NextGen Policy Architecture

NOTE 1 : Policy Function is regarded as part of control plane. The CP function in this figure includes other control plane functions, e.g. SM function, MM function. Only policy related interfaces are shown with corresponding names in this figure. This architecture only includes those reference points relevant for policy in this solution. It does not depict other interfaces such as a direct interface between the CP function towards the USD for authentication or keeping track of the subscriber information.

The following functions are involved in the NextGen Policy framework:

Policy Function: The Policy Function is the policy decision point to provide different control rules to NextGen CP Function based on the application session information received from the AF, operator's configuration, user subscription from the USD (User Subscription Database) and spending information from the Online Charging System. The Policy Function also supports the access type selection and RAT/Frequency selection priority index selection.

Editor's note: How to support other policy functionalities, such as mobility policy, roaming policy and the third party policy are FFS.

User Subscription Database: The User Subscription Database stores the subscriber/subscription related information needed to support policy functionality.

Editor's note: Whether or not the user subscription database for policy is collocated with the user subscription database for other CP functions is FFS.

NextGen UP Function: NextGen UP Function provides the packet core related user plane functionalities, including:

- QoS enforcement

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 376 of 501

- Measurement enforcement
- Gating
- SAF (Service Awareness Function): provides application detection and enforcement function.

Editor's note: Whether or not the SAF is a standalone function as TDF in EPC is FFS.

- TSF (Traffic Steering Function): enforces the user plan traffic steering related policy received from the Policy Function via NextGen CP Function, e.g. moving individual IP flows from one access network to another, and or from one service function to another service function (e.g. for video analytics, optimized local content distribution and data caching, Firewall, Parental Control).

Editor's note: The access related traffic steering has dependency on the key issue#20, and it is FFS.

NOTE 2: The functionalities related to traffic steering for the services are the same as in EPC.

The NextGen UP Function may provide all above functionalities or part of these functionalities based on the operator's configuration/deployment.

NextGen CP Function: The NextGen CP Function provides the packet core control plane function.

- When receiving the control rules from the Policy Function, the NextGen CP Function instructs the NextGen UP Function to enforce the policy (e.g. QoS policy, charging policy, gating policy, SAF policy, TSF policy).
- When receiving access type selection related control rules from the Policy Function, the NextGen CP Function transfers them to the UE.
- When receiving RAT/Frequency selection priority related control rules from the Policy Function, which contains the RAT/Frequency Selection Priority Index (RFSP Index) to be applied, the NextGen CP Function transfers the RFSP Index to the AN.NOTE 1: The NextGen CP Function can change the value of RFSP Index received from the Home Policy Function when the RFSP Index is to be transferred to the AN, according to local policy configured in the NextGen CP Function.

NOTE 3: The Home Policy Function sends the policies in some cases e.g. RFSP Index policy, to the MMF within NextGen CP for policy enforcement.

- When enforcing charging control from the Policy Function
  - For online charging, the NextGen CP Function sends the credit request for a charging key to the Online Charging System, and reports the usage when the threshold is reached, as defined for credit management in TS 23.203 [3].
  - For offline charging, the NextGen CP Function collects usage information per charging key /and service identifier combination and reports to the Offline Charging System as defined for reporting in TS 23.203 [3].

Online Charging System: Provides support to credit management with the NextGen CP Function and support for policy decision based on spending limits as defined in TS 23.203 [3].

Offline Charging System: Provides support for receiving usage information per charging key /and service identifier combination from the NextGen CP Function.

Editor's note: How the access type selection related control policy can be transported to the UE is FFS.

The following reference points are defined for the NextGen Policy framework:

NP1: Reference point between the Policy Function and the USD. Similar to Ud/Sp interface in EPC.

NP2: Reference point between the Policy Function and NextGen CP Function.

NP3: Reference point between the Policy Function and the AF, the AF provides the application session information to the Policy Function. Similar to Rx interface in EPC.

NG5: Reference point between the Policy Function and the AF, the AF provides the application session information to the Policy Function. Similar to Rx interface in EPC.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 377 of 501

NG4: Reference point between NextGen CP Function with NextGen UP Function, which is used by this solution to provide policy rules to NextGen UP Function.

NP3: Reference point between the Policy Function and the Online Charging System, same functionality as Sy defined in the TS 23.203 [3].

NC1: Reference point between the NextGen CP Function and the Online Charging System, same functionality as Gy defined in the TS 32.251 [19].

NC2: Reference point between the NextGen CP Function and the Offline Charging System, same functionality as Gz defined in the TS 32.240 [20].

NOTE: The Online Charging System and the Offline Charging System, and the protocols of NP3, NC1 and NC2 reference points are defined by SA WG5.

6.10.3.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.10.3.2.1 Input for Policy Decision

The Policy Function is responsible for the policy decision, such as QoS, charging , gating , TS policy. The following information is provided as policy decision input:

From the User Subscription Database:

- User subscription (user's type, user's priority, etc): this information could allow the operator supply differentiated service for the UE, e.g. service for Gold User/Silver User;

From the NextGen CP Function:

- UE currentlocation (location, etc.): this information could allow the operator adjust QoS policy to balance the load of access network. Also, the location information could help operator to make various charging; which is also defined in TS 23.203 [3];
- Radio access Information (RAT, etc): radio access information is helpful for the QoS/charging policy decision, e.g. the operator may authorize more bandwidth and lower charging rate if the UE access via non-3GPP access; which is also defined in TS 23.203 [3];
- PDU session information (PDU session type, APN, etc.): the policy function need the PDU session type (IPv4/Ipv6/Ethernet, etc.) to generate correct traffic filter in the policy; the policy function may select charging rate according to the date network, i.e. APN information;
- Roaming status: for roaming user, the operator may use specific QoS/charging rate;

From the Application Function:

- Application type (video, web browsing, IM, etc.): the operator may use different QoS/charging/DPI policies according to application type;
- Application QoS requirement (bandwidth, latency, session continuity requirement, etc.): this information is the key input for QoS policy is provided by the application (e.g. URLLC M2M/IoT) for the QoS enforcement in NextGen System;
- Application protocol (HTTP, P2P, encryption status, etc): the operator may perform traffic steering policy, e.g. proxy, accelerate, cache, DPI, according the application protocol; Normally well known port number in the application flow is used to identify the application protocols.
- Application provider (My tube, etc.) : the application may be a sponsor of some traffic, therefore the application provider information will impact on the charging policy, which is also defined in TS 23.203 [3];
- Expected packet handling (video compression, cache, etc.): this information if provided by the application provider can be used to select the traffic steering policy which defines to steer the subscriber's traffic to appropriate service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the (S)Gi-LAN which is defined in TS 23.203 [3];

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 378 of 501

From the local configurations:

- Operator's policies: operator specific policies may allow operator's flexible policy decision.

Editor's note: The list above of inputs for policy decision are not exhaustive and it is FFS whether more information are available as the input for policy decision. It is FFS if the list of inputs are available at the Policy Function or may be received from the Application Function or from the CP Function.

Editor's note: The alignment of detailed description of policy parameters with descriptions in other network functions is FFS.

Editor's note: It is FFS if policy decision input can be provided by the UE.

6.10.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.10.4 Solution 10.4: Policy Reference Architecture

Editor's note: This solution will evolve as the work in the different KIs progresses.

6.10.4.1 Overview

It is expected that in the NextGen System the network behaviour can be dynamically shaped via operator policies, allowing carriers to deliver differentiated services to their users (see Key Issue #10).

Sometimes, the operator policies can be local to the NG Control Plane function that requires them, responding to internal inputs (internal events, internal data) and acting on resources internal to the function.

But other times, the operator policies to deploy in the network require:

- Inputs from several sources (e.g. subscription information, subscriber location changes, etc.)
- Coordinated actions on different resources of the different NextGen System functions (e.g. changes in the authorized QoS and authorized PDU sessions depending on time of day).

In these scenarios, a separated Policy Function that gathers the complex decision control logic provides the flexibility needed for a fast deployment of differentiated services.

The Policy Function, taking into account the input provided by the NG Control Plane in the Policy requests, together with the operator-defined rules and other information (as e.g. subscription information), responds to the NG Control Plane with Policy decisions that indicate the selected choice of network behaviour (QoS network behaviour, Session Management network behaviour, etc.).

The NG Control Plane will propagate the received Policy decision information to the Policy enforcement points of the e.g. QoS Control, the Session Management or the Mobility Management frameworks.

The Policy Function also reacts at the reception of events (for example Application session events, core network events) or data updates from various sources (for example, changes in subscription information) to deliver Policy decisions to NG Control Plane.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 379 of 501

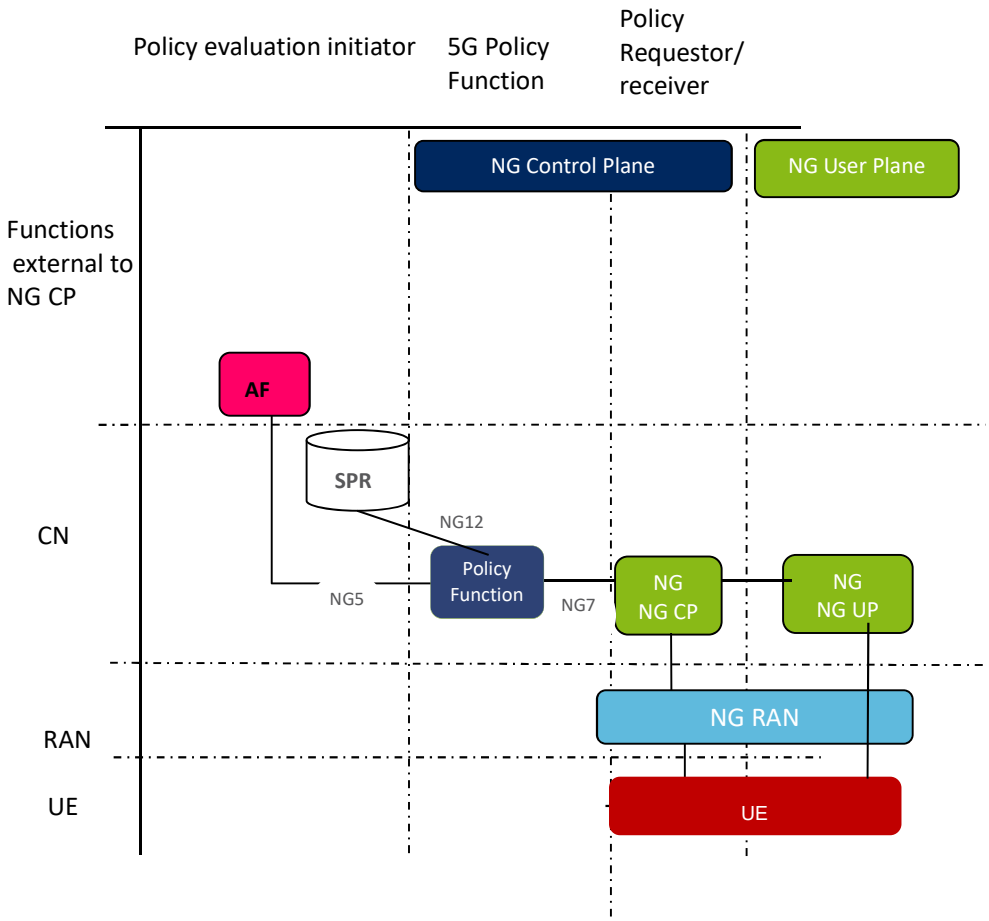


Figure 6.10.4.1-1: Baseline Policy Reference Architecture (non-roaming)

The figure above shows an architectural view of the Baseline Policy Reference Architecture (for non-roaming cases), where the Policy Function is separated from the NG Control Plane box and interfaces with the NG Control Plane. The figure also depicts the relation of the Policy Function with other functions external to NG Control Plane that can initiate Policy decision re-evaluation.

The proposed solution follows the principles of the EPS Policy and Charging control architecture, retaining a centralized control based on policies to govern the operator choices of network behaviour.

The NG5 reference point lies between the Application Function (AF) and the Policy Function, and enables the transport of application level events and service information from the AF to the Policy Function.

NOTE: Service information provided by the application is listed in clause 6.2.1.1.2.

The NG7 reference point resides between the NG Control Plane and the Policy Function. It enables the transport of network events and Policy Requests from the NG Control Plane to the Policy Function, and the delivery of Policy Decisions from the Policy Function, with the specific treatment for QoS control, Mobility Management, Session Management, etc., to the NG Control Plane.

The NG12 reference point resides between the subscription profile repository and the Policy Function and enables the Policy Function access to up-to-date subscription information.

Note that as the work in the different KIs evolves, it will be settled how the NG Control Plane functions control the network resources. The dependencies with the Policy Function for the selection of specific choices for the control of the network resources could be completed then, including:

- the identification of the events that trigger the NG Control Plane to request Policy decisions,

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 380 of 501

- the detailed information provided by the NG Control Plane to the Policy Function
- the Policy decision information conveyed between the Policy Function and the NG Control Plane,
- the required Policy interactions.

Also, the complete set of external functions that will trigger the evaluation of Policies could be completed, as well as the detailed information required in the corresponding reference points.

Editor´s note: Whether there is a need to provide policies to the UE using a new interface is FFS.

6.10.4.2 The Policy Function

The Policy Function, at request from the NG Control Plane, delivers Policy decisions that e.g. enable:

- For IP and non-IP based services:
  - Application and service data flow detection
  - Service gating
  - QoS control: QoS authorization and provisioning,

Editor's note: The specific aspects of the QoS control in the Policy Framework have dependencies with the results of the Key Issue#2 on QoS Framework.

- For Mobility management
  - Operator control of mobility levels. Assistance for mobility on demand function as described in clause 6.3.9, providing level(s) of mobility support for the UE based on conditions as e.g. geographical location, time, date, etc., according to the Interim Agreements on Mobility on Demand described in clause 8.4.

Editor's note: The specific aspects of Mobility Management in the Policy Framework depend on the results of the Key Issue#3 on Mobility Management.

- For Session Management
  - Authorization of the PDU Connectivity Service. This means the Policy Function determines the QoS property of the PDU session, as described in clause 6.4.2. It also means that if the PDU session set up is not authorized by the Policy Function the session is terminated

Editor's note: The specific aspects of Session Management in the Policy Framework depend on the results of the Key Issue#4 on Session Management.

6.10.4.3 The NG Control Plane input to the Policy Function

The NG Control Plane provides input information that the Policy Function combines with other information sources (e.g. subscription information, time of day, etc., in line with operator-defined-rules) to make policy decisions. The included information may consist of:

- Subscriber identifier (e.g. UE identifier)
- PDU Connectivity Service information (PDU session information, e.g. PDU session type, DN name)
- Network event that triggers the Policy request (e.g. change of location, including then the Location of the subscriber),

Editor's note: The complete set of input information to the Policy Function is FFS.

6.10.4.4 The Enforcement of Policy Decisions

The NG Control Plane decides what policy decisions are locally enforced, what policy decisions to propagate to the policy enforcement points.

For example, the solutions for QoS key issue define how the QoS information provided by the Policy Function is enforced in NG Control Plane and what QoS information is sent to the NG User Plane for enforcement. In addition, the QoS information is sent to NG Access Network and the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 381 of 501

Another example, for the solution for Mobility on demand, The Mobility levels are provided by the Policy Function. The NG Control Plane enforces the mobility level(s)

The Policy Enforcement in the NextGen Core Network is both in the NG Control Plane and the NG User Plane.

6.10.4.5 Functions external to NG Control Plane

Some functions external to the NG Control Plane, i.e. AF need the network behaves according to their requirements. Other functions external to the NG Control Plane (e.g. issuing subscription change events) provide valuable information for determining the choice of network behaviour.

These functions trigger a policy re-evaluation to the Policy Function, which considering the input information in the request, subscription information and operator-defined-rules, indicates the resulting change in the network behaviour with new Policy decisions.

The systems described below may interact with the Policy Function:

- Application Function (AF)
  - The NG5 reference point between the AF and the Policy Function conveys the requirements the application sets in the network for the delivery of the requested service. The AF may provide Service information listed in clause 6.2.1.1.2.
  - The QoS authorization information delivered to the NG Control Plane is derived by the Policy Function from AF interaction in combination with subscription information and in line with the operator defined rules.
- The Subscription profile repository (SPR) provides up-to-date subscription information to the Policy Function via N12 reference point. Updates in subscription data trigger a policy re-evaluation. The subscription information typically handled by the Policy Function is:
  - Subscriber's allowed services, subscriber's allowed QoS (per PDU session and per Service), usage monitoring profiles, subscriber category, etc.

6.10.5 Solution 10.5: Policy function and framework for roaming cases

This solution addresses Key issue 10, WT#1, i.e. an overall roaming policy framework for NextGen is described.

6.10.5.1 Architecture description

The figure 6.10.5.1-1 shows the NextGen Roaming Policy framework for home routed.

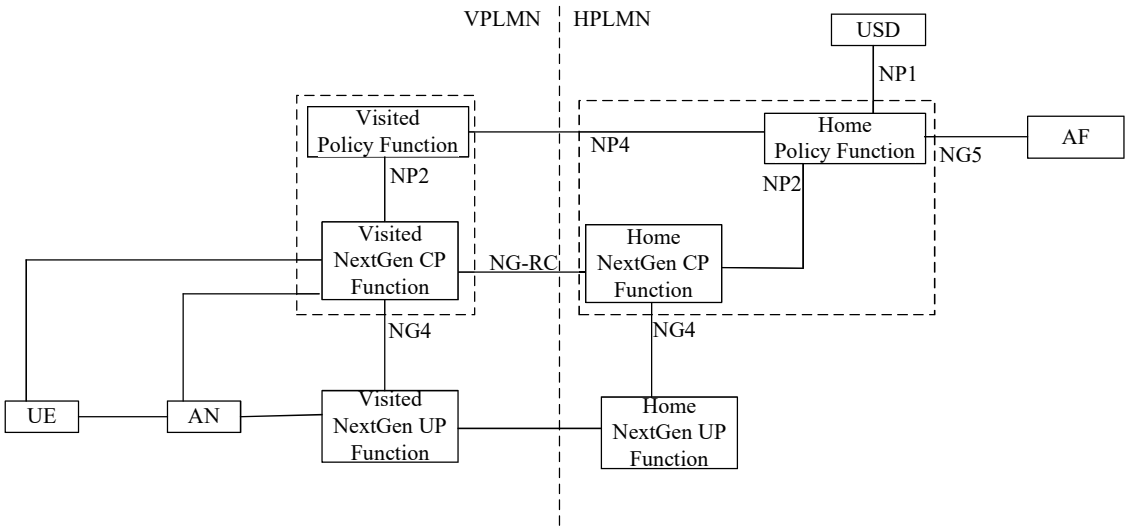


Figure 6.10.5.1-1: NextGen Roaming Policy framework for home routed

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 382 of 501

The figure 6.10.5.1-2 shows the NextGen Roaming Policy framework for local breakout.

Editor's notes: The reference points NP2, NG-RC have dependencies on other key issues, the outcome of those key issues needs to be taken into account for policy control.

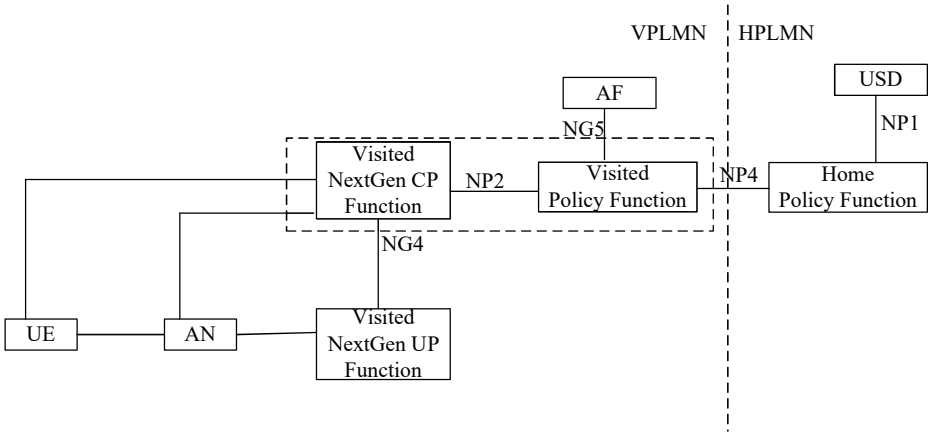


Figure 6.10.5.1-2: NextGen Roaming Policy framework for local breakout

NOTE : Policy Function is regarded as part of control plane. The CP function in this figure includes other control plane functions, e.g. SM function, MM function. Only policy related interfaces are shown with corresponding names in this figure. This architecture only includes those reference points relevant for policy in this solution. It does not depict other interfaces such as a a direct interface between the CP function towards the USD for authentication

Compared with non-roaming architecture, the following functions are introduced:

Home Policy Function: For roaming with home routed, the Home Policy Function is the policy decision function to provide policy rules for QoS, Usage monitoring and charging to Home NextGen CP Function, and provide mobility policies and RAT/Frequency selection priority index policies which contains the RAT/Frequency Selection Priority Index (RFSP Index) to be applied to Visited NextGen CP Function via a home NextGen CP Function or via a Visited Policy Function, by which the local mobility policies and RAT/Frequency selection priority index policies in visited network can be taken into account. Moreover, the Home Policy Function can provide access type selection policy similar as defined by ANDSF functionalities in EPC to the Visited Policy Function and then the Visited Policy Function delivers it to the UE.

NOTE 1: The NextGen CP Function can change the value of RFSP Index received from the Home Policy Function or Visited Policy Function when the RFSP Index is to be transferred to the AN, according to local policy configured in the NextGen CP Function.

NOTE 2: The Home Policy Function or Visited Policy Function sends the policies in some cases e.g. RFSP Index policy, to the MMF within NextGen CP for policy enforcement.

Editor's note: It is FFS how to provide access type selection policy to the UE and whether the policies from Home Policy Function are provided to the VPLMN via NP4 or via NP2 and NG-RC.

For roaming with local breakout, the Home Policy Function is the policy decision function to provide policy rules for QoS, Usage monitoring and charging , mobility policies to Visited Policy Function.

Visited Policy Function: The Visited Policy Function receives the policy rules from Home Policy Function and adjusts the policy rules based on visited operator's local policy for mobility and RAT/Frequency selection priority index, and provides policy rules to Visited NextGen CP Function.

The following reference points are defined for the NextGen Roaming Policy framework:

NG-RC: Reference point between the Visited NextGen CP Function and Home NextGen CP Function. For Home Routed, the Home Policy Function provides policy (except access type selection policy) to Visited NextGen CP Function through NP2 and NG-RC.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 383 of 501

NP4: Referenct point between the Visited Policy Function and Home Policy Function.The Home Policy Function provides policy rules for QoS, Usage monitoring and charging, mobility policies, RAT/Frequency selection priority index policies to Visited Policy Function.

NOTE: For Home Routed, the Home Policy Function provides access type selection policy and RAT/Frequency selection priority index policy to Visited Policy Function through NP4.

Editor's note: For local breakout , it is FFS whether the access type selection policy is needed to be provided to the Visited Policy Function

6.10.5.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.10.5.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.10.6 Solution 10.6: Encrypted traffic detection

6.10.6.1 General description of the solution

The method of this solution is to enable the policing functionality to detect, differentiate and validate encrypted traffic from an external 3rd party content provider.

The solution relies on the exchange of service identification information and corresponding authentication data between the NextGen CN and the content provider, which are mapped in the NextGen CN to specific policies by the policy infrastructure. Such information is then used in the traffic sent in the user plane to enable the NextGen CN to verify the validity of the data and implement policies defined by the policy infrastructure (e.g. QoS, charging, etc.)

NOTE 1: Once the NG policy architecture is stable (e.g. CP/UP split, slicing, etc.), this solution needs to be updated to comply with it.

6.10.6.2 Procedures For Traffic Authorization and Validation at Flow Setup

Precondition:

- Asynchronously to the establishment of an application session (e.g. initiating HTTPS handshake), a Service ID (which may identify both the content provider and a specific application provided by the content provider) and related authentication information are negotiated between the NextGen CN and content provider. This is in order to enable appropriate traffic identification, validation and policing by the CN. .
- The authentication information includes security material used to generate authentication data (e.g. by hash computation).
- Multiple Service IDs can be generated by the content provider, and specific authentication information associated to each Service ID. This enables to distinguish in the NextGen CN different services or contents from the same content provider (e.g. for QoS, charging, etc.)
- The Service ID(s) and the corresponding authentication information are made available at the UE, the NextGen CN and the content provider.

The procedures include the following components:

- When initiating an application session (e.g. the HTTPS handshake(TLS hello), the UE forwards the application traffic in uplink and adds service ID and authentication data in a service token extension. The service ID is related to the application which initiated the application session (e.g. the HTTPS handshake). The authentication data is generated by the UE based on the authentication information which the UE has been provided by the content provider and that is associated to the Service ID.
- Upon detecting that the UE has generated traffic with a service token extension, the NextGen CN that has received the Service ID(s) and the corresponding authentication information verifies the validity of the service token extension, using the mechanism defined for generating and comparing the authentication data in the service token extension. If the authentication data generated by the NextGen CN corresponds to the one in

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 384 of 501

service token extension, the NextGen CN can relate the received traffic (even if encrypted) with the service or application identified by the service ID, and can enforce the corresponding policy rules on this traffic (including e.g. QoS and charging).

- Similarly, for downlink traffic the content provider can generate service token extensions to enable the NextGen CN to identify, differentiate, and validate the encrypted traffic, and to identify the corresponding policy rule to be enforced.

NOTE 2: Whether the service token extension is normalized by 3GPP or by IETF is FFS.

NOTE 3: Whether the service token extension for uplink and downlink traffic are the same or created differently via different authentication information is FFS.

Editor's note: the details of the security mechanisms need to be defined by SA3.

6.10.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.10.7 Solution 10.7: Policy Architecture with CP functional split

Editor's note: This solution will evolve as the work in the different KIs progresses.

6.10.7.1 Overview

It is expected that Next Generation System.supports dynamically modified network behaviour based on operator policies as in EPC (TS 23.203 [3]). However, the main difference we expect with NextGen system is that the policy framework should be unified to also support mobility management, network selection related policies in addition to the current PCC framework as stated in Key issue for policy framework in clause 5.10.1.

This solution proposes the need for a separate NG policy function considering the fact real time computing might be involved taking into account information received from various sources and dynamically occurring events in the network. This solution analyses the potential enforcement points and reference points that will be impacted in order to support a unified policy framework fulfilling the requirements listed in the key issue. The following table summarizes the type of policies, enforcement point, reference points impacts.

Table 6.10.7.1-1

Type of Policy	Enforcement point, Potential reference points impacted
QoS Enforcement	SM function->RAN (NG3/NG4/NG11/NG2)
Charging Control	SM function->UPF(NG3/NG4)
Policing, Gating, (including redirection) -	SM function->UPF(NG3/NG4)
Traffic Routing / Local DN versus Central DN	SM function->UPF(NG3/NG4)
Congestion Management	SM function->UPF(NG3/NG4)
Service Steering & Service Chaining	SM function->UPF(NG3/NG4)
Network (e.g. PLMN) Selection	MMF->RAN, UE (NG3/NGmp -> NG2, NG1)
Access Type Selection*)	MMF->RAN, UE (NG3/NG2/NG1)
Roaming	SMF/MMF (NG3/NGmp)
Mobility	MMF->RAN, UE (NG3/NG2/1)
Policies related to group of users.	Enforcement point and reference points impacted depends on the type of group (whether it is subscription based groups, dynamically created groups and also where the group is managed)
Third party service handling.	Depends on the type of service
NOTE: NGmp ref. point name assumed for a potential PCF<->MMF interface. *) assumes conveying access type selection policies via 3GPP RAT. No assumption on the need to support traffic steering between 3GPP access and non-3GPP access.	

From the table, it is observed that in order to develop a unified policy framework in operator network, the policy function needs the ability to provide policies both to MM function and SM function thus need a direct interface from

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 385 of 501

NG PCF to SMF and NG PCF to MMF to avoid 2 step forwarding of policies when the NG Core Control plane functions are split into MMF and SMF functions.

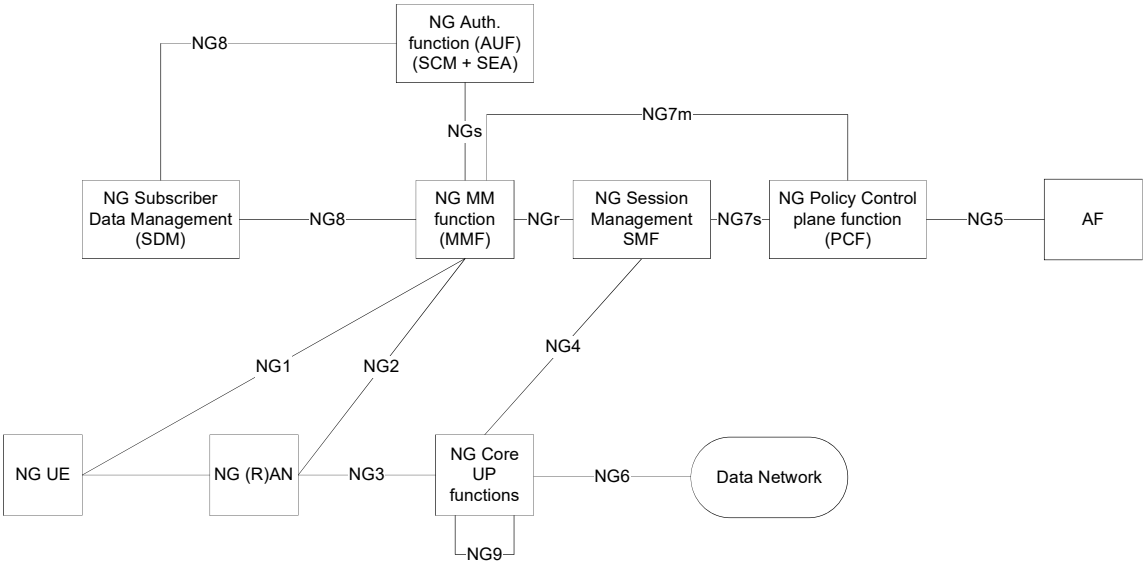


Figure 6.10.7.1-1 Policy architecture with MMF, SMF split

NOTE: Subscriber data relevant for policy decisions is either stored in dedicated database NG SPR or in a subscriber data repository NG UDC, the latter follows UDC principles as described in TS 23.335.

In all other aspects, this solution is complimentary to the other solutions present in the TR for policy framework.

6.10.8 Solution 10.8: Dual Level Policy framework

This solution presents the dual level policy framework that supports both non-roaming and roaming scenarios.

6.10.8.1 Acronyms/definitions

CCNF: The Common Control Network Functions is a group of functions that are shared across the slices concurrently supported for a UE

- NF: Network Function
- NS: Network Slice

SCNF: Slice Specific Core Network Functions is the set of functions of a Network Slice that are not shared with other Network slices. It includes Slice Specific CP Network functions and Slice Specific UP network functions.

- SCNF-CP : Control plane functions applicable to a SCNF
- SCNF-UP : User Plane functions applicable to a SCNF

PCF: Policy Control Function controls the Slice Selection policies in CCNF and other dynamic policies for its serving UE.

- S-PCF : Secondary Level PCF, i. e. supporting specific policy control for the UE within the local domain (e.g. within the slice which is part of the SCNF-CP).
- C-PCF : Common PCF, i.e. top level PCF communicating with S-PCF to support and coordinate the common policy control for the UE within the NextGen system.

NOTE: In case that S-PCF is not deployed, the C-PCF operates as main PCF.

Subscriber Repository: Repository of subscription information.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 386 of 501

6.10.8.2 Architecture descriptions

The figure 6.10.7.2-1 below shows the dual-level policy control architecture.

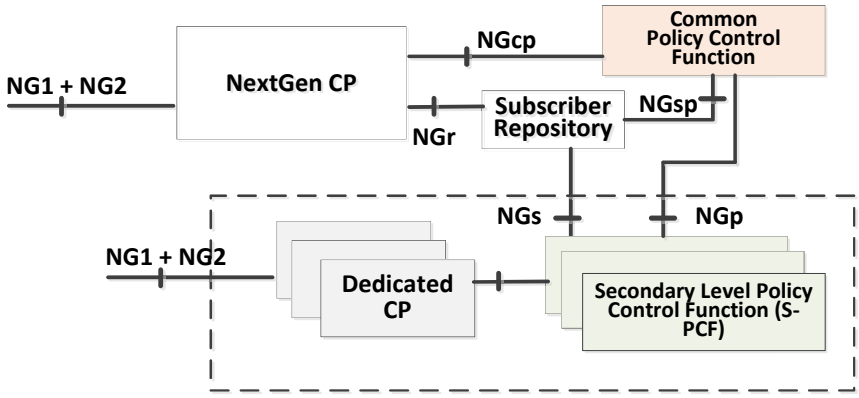


Figure 6.10.8.2-1: Overview of Dual-level Policy Control Architecture (Non-roaming scenario)

The solution below leverages the example of network slicing architecture to demonstrate the use case of dual level policy control support. Other deployment leveraging the second level policy control is not precluded.

The Figure 6.10.8.2-2 below shows the dual level policy control support for Network Slicing for non-roaming case. In case of network slicing, the C-PCF communicates with the CCNF as defined in solution 6.1.2, the S-PCF serves the slice specific core part. The C-PCF and S-PCF are interconnected over NGp and their respective responsibilities are described as follows.

Functions of C-PCF

C-PCF provides the common policy control support at the UE level, more specifically:

1. Initial NS selection - Assisting the CCNF perform NS selection during initial attach procedure (see clause 6.1.2.2.3.1.Initial Access as described in this TR). For example, the C-PCF provides the CCNF the MM mobility control policy support for the target UE.

2. NS Re-selection - During the lifetime of the user attachment, the C-PCF may notify the CCNF about change of policy. This change may be related to user subscription (e.g. user was upgraded from a bronze tier to a gold tier, and so is entitled to use apps or/and bandwidth, which may require a re-selection of a NS) or it may be related to network conditions (e.g. the eNodeB serving the user is experiencing a congestion, and there is a need to re-select a new NS, which has WLAN connectivity).

3. Acting as a top level PCF to support S-PCF's policy control decision whenever needed, e.g. notifying S-PCF for the change of UE's subscription.

4. The C- PCF provides the coordinated dynamic policy control at the UE level of which the UE may have multiple PDU sessions associated with more than one NSIs.

5. Fundamentally, C-PCF is responsible for interfacing with Subscriber Repository and RCAF which is similar to what PCRF support in EPC today

Functions of S-PCF

1. Secondary level PCF (S-PCF) provides the similar legacy PCRF functionality, however, it is to focus on the specific session level related dynamic policy for the given UE so that it can offload C-PCF involvement.

2. S-PCF supports new policy control function introduced for the NextGen UE (e.g. NextGen PDU marking), so that, it enables more optimal PCF implementation according to the specific service requirements of the corresponding area. Some S-PCFs may need to provide a full blown PCRF functions, which support similar interfaces as shown in figure 5.1-1 of TS 23.203 [3] (eg Sp, Gx, Rx, Sy, Np, St etc) assuming most of these

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 387 of 501

interfaces remained in NextGen. Some S-PCFs could just provide a reduced version of PCRF (e.g only Gx and Sp like interfaces).

Furthermore, this solution proposed to support direct interface (i.e. NGcp) between the Subscriber Repository and C-PCF allows the consistent support for the preconfigured and the dynamic policy control between these two network functions. For example, the handling the subscriber policy changes that impact both the Subscriber Repository and C-PCF.

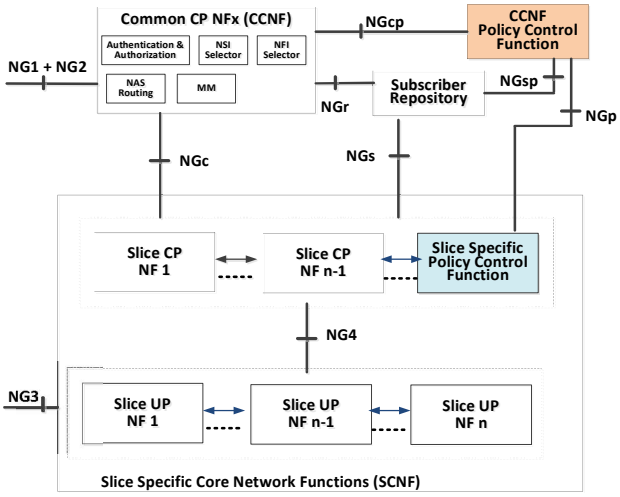


Figure 6.10.8.2-2: Core Part of Network Slicing concept (Non-roaming scenario)

The Figures 6.10.8.2-3 and 6.10.8.2-4 below describe the example of the dual level NextGen Policy framework applying for Network Slicing for roaming cases.

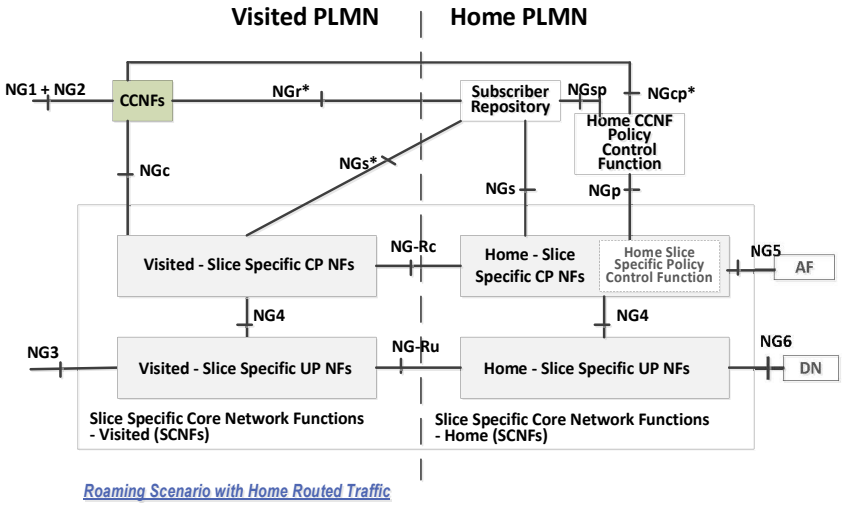


Figure 6.10.8.2-3: Example of Core Part of Network Slicing concept (Home Routed Roaming scenario) with Dual Level Policy Control support

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 388 of 501

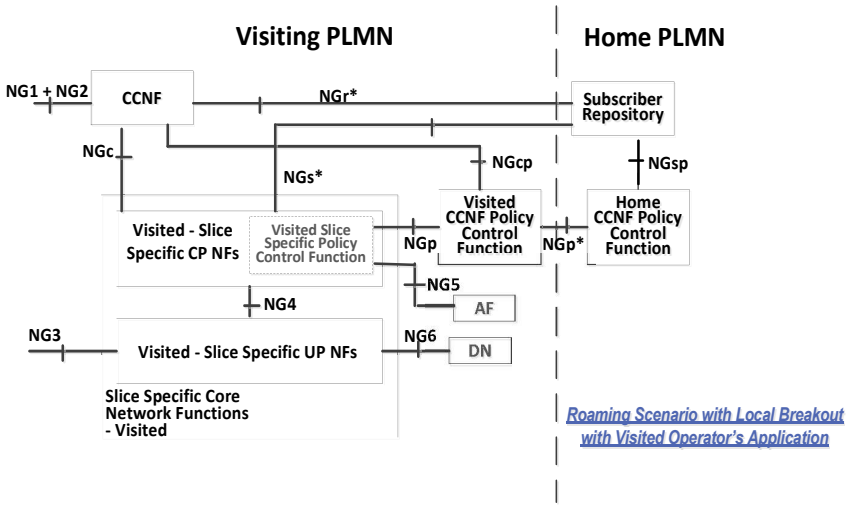


Figure 6.10.8.2-4: Example of Core Part of Network Slicing concept (Local Breakout Roaming scenario) with Dual Level Policy Control support

NOTE: Policy Function is regarded as part of control plane. The three figures above include other control plane functions, e.g. SM function, MM function, as described in solution 6.1.2.

For the roaming support, the following describes the responsibilities of the home and visited policy control functions:

Home Policy Control Function:

- For roaming with home routed, the Home Policy Control Function is the policy decision function to provide policy rules for QoS, Usage monitoring and charging to Home NextGen CP Function, and provide mobility policies to Visited NextGen CP Function via a home NextGen CP Function or via a Visited Policy Control Function, by which the local mobility policies in visited network can be taken into account.
- For roaming with local breakout, the Home Policy Control Function is the policy decision function to provide policy rules for QoS, Usage monitoring and charging , mobility policies to Visited Policy Function.
- The Home Policy Control Function may further distributed between Home C-PCF and Home S-PCF, if available, as described for C-PCF and S-PCF above.

Visited Policy Control Function:

- The Visited Policy Control Function receives the policy rules from Home Policy Control Function and adjusts the policy rules based on visited operator's local policy for mobility, and provides policy rules to Visited NextGen CP Function.
- The Visited Policy Control Function may further distributed between Visited C-PCF and Visited S-PCF as described for C-PCF and S-PCF above.

6.10.8.3 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.10.8.4 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.11 Solutions for Key Issue 11: Charging

Void.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 389 of 501

6.12 Solutions for Key issue 12: Authentication and security framework

6.12.1 Solutions 12.1: Authentication and security framework

This solution addressed the key issue 12 for authentication and security framework.

In order to address the requirements from SA WG1, the following principles are adopted:

- Support authentication of UE connecting to the 5G NextGen CN via different access network, including 3GPP technologies, non-3GPP wireless technologies, fixed broadband access, including trusted and untrusted Non-3GPP accesses.
- The UE is assumed to possess credentials which are verifiable by an entity in the NextGen core network. The procedure for providing credential to UE is out of scope of this solution.
- Support a unified authentication framework enabling UEs connecting via different access network technologies to access the 5G NextGen CN. The realization of a unified authentication framework will be dependent on how the different access network technologies, especially the non-3GPP accesses will be integrated into the 5G NextGen CN.

Furthermore, the following assumptions apply to the solution:

- IMS registration is not considered within the scope of this solution.
- Threats, potential requirements and solutions for the security and authentication architecture in next generation mobile networks are under investigation in SA WG3 under the scope of TR 33.899 [16].

Editor's note: Aspects related to support of network slicing are FFS.

Editor's note: mechanisms for the support of connectionless based service are FFS.

Editor's note: Authentication in roaming scenario is FFS.

6.12.1.1 Authentication and Security Framework description

Editor's note: Whether this framework is applicable only to session based connectivity is FFS.

6.12.1.1.1 Security Architecture

In this reference architecture for the unified security framework it is assumed that for non-3GPP accesses there may be either security protection provided by the AN between the UE and the CN, or no security protection or insufficient security protection provided by the AN between the UE and the NextGen CN.

Figure 6.12.1.1-1 describes the relationship between the network functions and the UE functions for the authentication framework.

NOTE: the functional interfaces identified between the network functions do not necessarily correspond to the NextGen CN interfaces (e.g. as described in Annex G) but represent the exchange of security context between the functions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 390 of 501

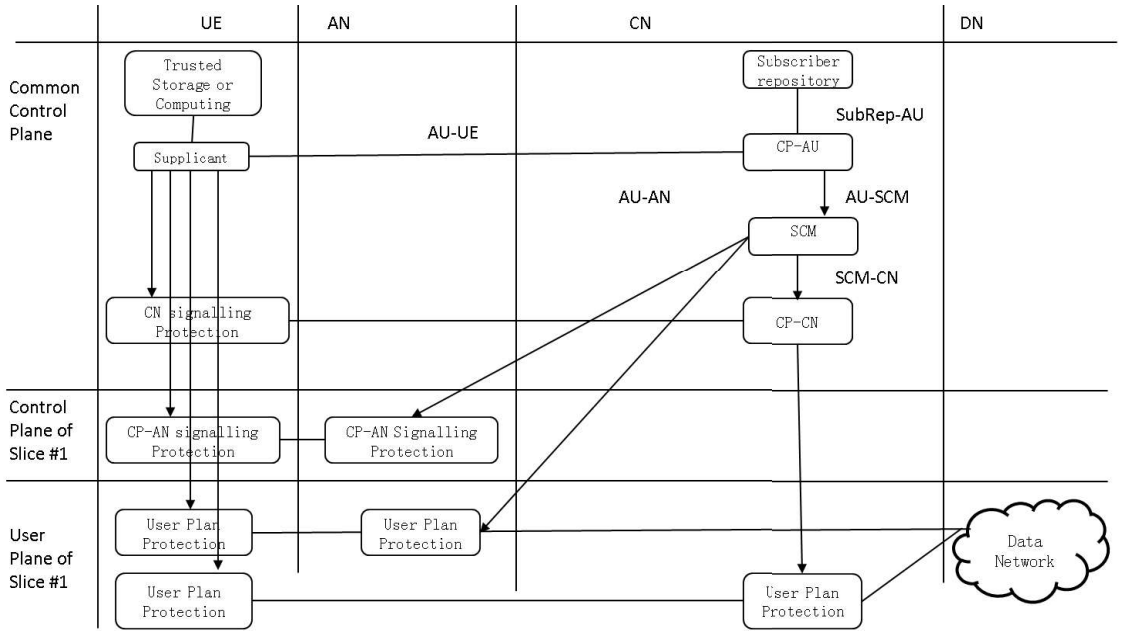


Figure 6.12.1.1.1-1: Reference architecture for Unified authentication framework for in non-roaming scenario

The unified authentication framework is defined in the following and shown in figure 6.12.1.1-1.

Supplicant function: The function inside the UE that executes the authentication process with the peer on network side.

Subscriber Repository Function: This function contains subscriber profiles for authorization, user identities and corresponding long-term credentials for authentication.

CP-AU authentication Function: A function in the core network that performs UE authentication process and interacts with Subscriber Repository Function for retrieving authentication materials.

User Plane Protection Function: This function provides the protection (e.g. encryption, integrity protection, etc.) of the user plane data exchanged between the UE and the Access network and/or between the UE and the Core Network (e.g. in case of untrusted non-3GPP accesses). The Protection function may be located the Core Network e.g. when not present in AN.

NOTE: The authentication between the UE and the CP-AU Function is performed only in the signalling plane.

Editor's note: The definition of protection mechanisms for control plane and user plane are is out of the scope of SA WG2 and it left to SA WG3 and RAN.

CP CN function: indicates a CP-CN function defined for other mechanisms (e.g. mobility management, session management)

CP-AN Signalling Protection function: applies to control plane information exchanged between the UE and the Access network.

Security Context Management function (SCM): A function in the core network that upon successful UE authentication maintains an authentication security context from which the security contexts for the specific functionality as applicable for the CN and the specific AN will be derived.

Editor's note: Whether the SCM function can be co-located with CP-AU, with a CP CN function or it can be a standalone NextGen CN function needs to be coordinated with SA WG3.

The following functional interfaces are considered:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 391 of 501

- AU-UE: Supports authentication mechanisms between the UE and the entity performing the UE authentication in the NextGen CN. AU-UE represents the end-to-end set of messages and parameters exchanged between the UE and the CP-AU Authentication Function. The authentication mechanisms supported by this functional interface may be transported over NG1via other 5G NextGen mechanisms (e.g. encapsulated in mobility management signalling or session management signalling) and forwarded to CP-AU by the CP function implementing the 5G NextGen mechanism (e.g. mobility management CP function), to enable UE authentication for such procedures. The authentication mechanisms supported by this functional interface may otherwise be exchanged between the UE and the CP-AU directly over NG1 and separately from mobility management and session management signalling. In either case, the authentication exchange is end to end between the UE and the CP-AU Authentication Function.

Editor's note: Exchange of the authentication mechanism signalling between UE and CP-AU will depend on how the authentication architecture in NextGen CN will support roaming scenarios. The decision where to place CP-AU in roaming scenarios (i.e. at VPLMN vs HPLMN) needs to be coordinated with SA WG3.

- AU-SCM: Supports interaction between the CP-AU function and the SCM function for the exchange of the authentication security context.

- SCM-AN: Supports interaction over NG2between the AN and the SCM function for provision of security context (e.g. depending on the security requirements in terms of ciphering, integrity protection, etc.) upon authentication, connectivity establishment, mobility, etc.

NOTE: Whether the SCM function provides the security context to the control plane or user plane part of the AN depends on the RAN design, the specific AN and needs to be coordinated with SA WG3.

- SCM-CN: supports interaction between the SCM function and CP-CN (CN Signalling Protection function) for distribution of security context from SCM to CP-CN.

Editor's note: Whether CP-AU is collocated with other CP-CN functions (in the HPLMN or in the VPLMN) needs to be coordinated with SA WG3.

- SCM-UP: supports interaction over NG4 between the SCM function and a User Plane Protection Function in the core network (e.g. in a UP-GW) for distribution of security context from SCM to user plane protection function.

- AU-SubRep: supports interaction between the CP-AU Authentication Function and Subscriber Repository Function for authentication of the UE.

Editor's note: Some of these interfaces may be actual reference points in the 5G NextGen architecture, others are captured just to represent the logical relation between functional entities and to describe the functional model, as described below.

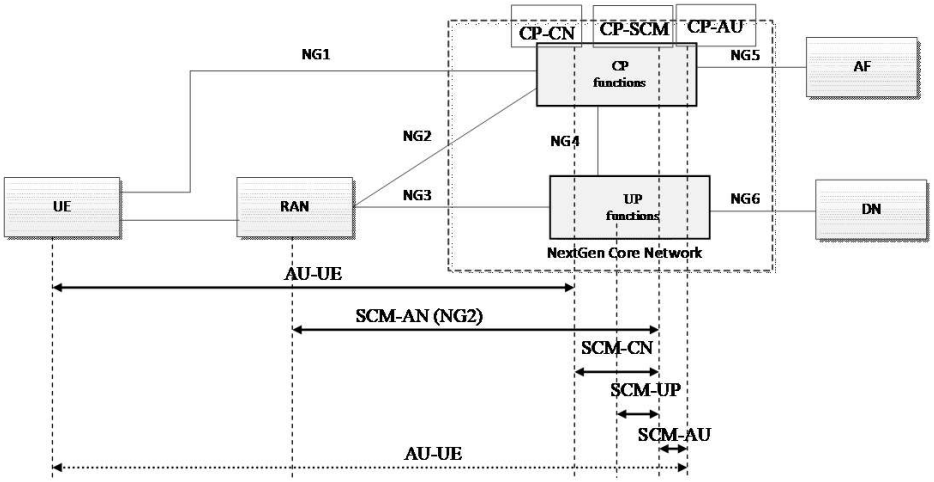


Figure 6.12.1.1-2: Mapping of functional interfaces

The definition of an authentication framework for different access systems connecting to the NextGen core network needs to consider the following aspects:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 392 of 501

- The types of UEs in terms of capabilities
  - UEs supporting capabilities specific to the NextGen CN (including e.g. protocols and procedures specific to the 5G NextGen system)
  - UEs supporting only a subset of the capabilities specific to 5G NextGen CN (e.g. not supporting NextGen MM).

Editor's note: Whether stationary UEs with reduced or no mobility requirements make still a basic use of the MM function within the NextGen CN is FFS.

In order to take these aspects into consideration, this solution proposes an authentication framework based on the following principles:

- Decoupling authentication and key management from other CN functionality (e.g. mobility management, session management, etc.) to enable the definition of a separate CP_AU function from other NextGen CN functions. The CP-AU function is a function used for authenticating UEs independently of the UE's support for 5G NextGen CN capabilities (e.g. support for mobility).
- Supporting the transport of authentication mechanisms that may be access network specific over a common authentication transport between the AN and the CN.
  - Authentication mechanism include 3GPP authentication mechanisms for the 5G RAT and for evolved LTE, 3GPP authentication mechanisms for non-3GPP access networks (e.g. 3GPP mechanisms for trusted Wi-Fi scenarios), and possibly mechanisms for other access technologies that may not be defined by 3GPP. As an example, depending on the specific authentication mechanisms to be supported, the common authentication transport may be AAA to support authentication mechanisms based on EAP.

Editor's note: Whether it is possible to assume a single transport of authentication mechanism common to all access networks and whether this can be based on EAP is left for SA WG3 to decide.

- The transport of authentication mechanism over the AU-UE logical interface may be performed via other mechanisms depending by procedure (e.g. via MM function if the UE is authenticated upon attachment and the establishment of an MM context).

6.12.1.1.2 Authentication and Key Agreement

The functional allocation for authentication and key agreement is as follows:

- the CP-AU is a function located in the NextGen CN. The CP-AU performs authentication for the UE agnostically to the access network(s) the UE is connected to.
- The authentication framework supporting a security context hierarchy to introduce flexibility in deriving the required security context, while maintaining access-dependent aspects in the access networks. Specifically, in this solution:
  - The CP-AU generates at UE authentication and subsequently maintains the authentication security context. An authentication security context is generated upon UE authentication and is applicable to all security functionality for the UE, i.e. CP-CN Signalling Protection, CP-AN Signalling Protection, and User Plane Protection. The authentication security context may be used to derive additional security contexts, e.g. for the specific access network or the CP signalling protection, depending on the UE capabilities and the other functionality (e.g. MM, SM, etc.) required to provide services to the UE.
  - The SCM function, upon successful UE authentication derives from the authentication security context, the UE security context(s) for the specific functionality as applicable, further processing the context as follows, e.g.:
    - for AN UP and CP protection: delivers, over AU-AN in NG2, per-UE access independent security context (e.g. keying material) at least to the AN functions.
    - for CP-CN signalling protection: if control plane needs to be protected between the UE and the CN, CP-AU distributes the CP security context required to protect it.

Editor's note: Which entities are provided such security context is FFS and dependent on the solutions for mobility management and session management.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 393 of 501

Editor's note: How and where the authentication security context is generated depends on the actual authentication mechanism and is left for SA WG3 to decide.

- The CP-AN receives the access independent security context for the UE and generates and maintains the access network specific UE AN Security Context (e.g. for ciphering and integrity protection) based on the AN Security Context provided by the SCM function. This includes deriving, in the AN, keying material for use with that access technology.

  - in case of inter-AN mobility, the source AN may transfer to the target AN the access independent security context received from the SCM function. Then the target AN derives the access dependent AN Security Context specific to the target AN. As an alternative, the source AN or the target AN may trigger the SCM function to deliver the access independent security context to the target AN, which in turn derives the access dependent AN Security Context for the UE.

Editor's note: Whether and how established security associations or contexts are transferred between Network Functions and (re)used, e.g. when the UE's serving Network Function(s) change due to mobility is left for SA WG3 to decide.

Editor's note: whether a change of the security context for CP-CN should trigger in certain scenarios also a change of the security context for the AN should be decided by SA3.

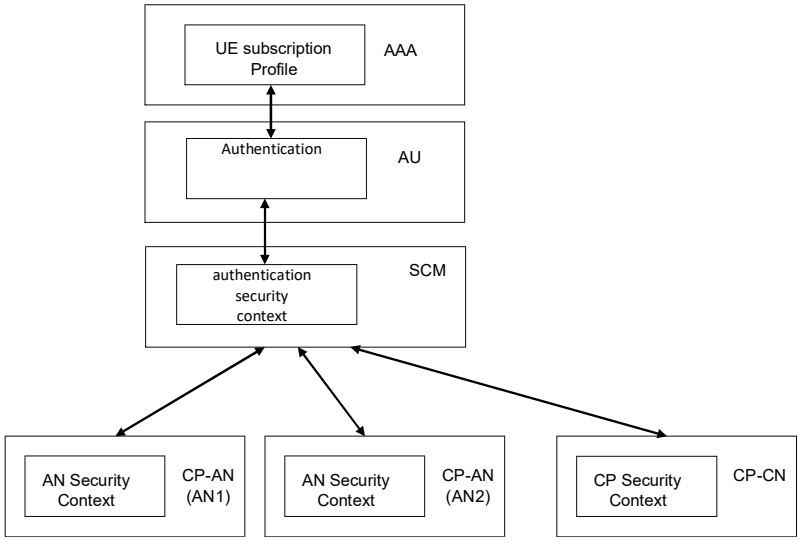


Figure 6.12.1.1-3: Security Context Hierarchy in the Unified Authentication Framework

6.12.1.1.3 User Identity and ME Identity Confidentiality

Editor's note: The mechanisms for supporting enhanced user identity confidentiality within NextGen CN are subject to proper threat analysis and security evaluation in SA WG3.

In order to support user identity and ME identity confidentiality, the following principles apply:

- the user identities and ME identity used by the UE with the NextGen CN for mobility management and session management are protected between the UE and the NextGen CN over NG1 such that they are never transferred in the clear

Editor's note: Whether a single user identity or multiple user identities are needed for the various functionalities (e.g. MM, SM, etc.) is FFS, depends on the solutions for such functionalities, and requires SA3 input.

Editor's note: It is FFS whether the transfer of these identities in the clear can be avoided in all circumstances, e.g. when the UE arrives in a new country or when the UE initiates an emergency service without authentication procedure.

- for 3GPP accesses, the user identities and ME identity used by the UE with the 3GPP AN are protected during access signalling

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 394 of 501

- for non-3GPP accesses, the 3GPP identities used by the UE to gain access to the non-3GPP access are protected during access signalling

Editor's note: Any protection of non-3GPP identities not visible to the NextGen CN is FFS and may be out of scope of SA2 and SA3.

6.12.1.1.4 System Signaling Protection

In this solution it is proposed that AN and CN control plane signalling are protected via separate mechanisms.

Editor's note: The final determination on the use of a single mechanism or separate mechanism is responsibility of SA3 and depends on solutions for other key issues (e.g. key issue 1).

Control plane signalling for AN is protected between the UE and the AN, and terminated by a function in the AN. The function receives from the CP-AU an access-independent AN Security Context for AN-specific key generation.

Control plane signalling between the UE and a CP-CN function in the NextGen CN is protected over NG1 for other mechanisms (e.g. mobility management, session management).

Editor's note: Whether control plane protection over NG1 is distributed (e.g. a specific security context is delivered to all CP-CN functions that interface with the UE over NG1) or centralized (e.g. a function acts as termination point of the control plane protection over NG1 for all control plane related to the NextGen CN functionalities) is FFS and depends on the solutions for other key issues.

6.12.1.1.5 User Plane Protection

For 3GPP access technologies, the user data protection is provided over the access link between the UE and the AN as per 3GPP specifications.

For non-3GPP access technologies, the user data protection is provided over the access link between the UE and the AN when the AN is considered trusted by the core network and when the AN provides such functions.

The user data protection may also be provided by a user plane function in the CN, e.g. for access networks that do not provide sufficient user data protection (e.g. untrusted AN) or for scenarios in which additional user data protection is required.

Editor's note: input is required from RAN and SA3 regarding the different connectivity modes supported and the impact on the user plane protection.

6.12.1.2 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.12.2 Solution 12.2: For security and authentication with Network Slice Support

This solution builds on Solution 12.1 adding additional aspects for supporting network slicing.

Threats, potential requirements and solutions for the security and authentication architecture in next generation mobile networks are under investigation in SA WG3 under the scope of TR 33.899 [16].

To support network slicing, the authentication security context may be used to derive the network slice dependent security context for the UE.

1) Different security key might be allocated to different Network Slice Instances for support network slicing with common and slice specific functions (i.e. for the slice architecture group B).

The UE may be required to conduct the network slice authentication with a 3rd party if the slice provides services to the 3rd party. The operator providing the slice shall be informed by authentication results and allow the access to the slice on behalf 3rd party.

2) Different NAS/AS security suites might be applied to different Network Slice Instances depending on required security level for network slices.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 395 of 501

Editor's note: Whether the authorization and/or authentication is needed per Network Slice Instance (NSI) is FFS and needs to be confirmed by SA WG3

6.13 Void

6.14 Void

6.15 Void

6.16 Void

6.17 Solutions for Key Issue 17: 3GPP architecture impacts to support network discovery and selection

6.17.1 Solution 17.1: Network discovery and selection in idle mode

This solution applies to Key Issue 17 - 3GPP architecture impacts to support network discovery and selection. This solution introduces the high-level solution for network discovery and selection in idle mode.

The solution is based on the following concepts in addition to concepts already included for network selection in the EPS:

- Network selection and discovery refers to discovering and selection a network in terms of network identifier (e.g. PLMN) and, when applicable, RAT combination.
- Network selection and discovery considers the support of network slices in the network. The UE takes into account which network slices, or network slice types, are supported by each network during network selection. Discovery of the supported slices in a given network may happen e.g. by provisioning, dedicated NAS signalling, overhead broadcast information or other discovery mechanisms.

Editor's note: it is FFS if support of slicing in a network refers to support of a specific type of slice or a specific slice instance

- Initiation and termination of a service may trigger network reselection. Network discovery and selection allows, conditional to the UE's radio capabilities, the selection of a RAT different from the current RAT on which the UE is camped to initiate a service, taking into account the service characteristics and the UE's context (e.g. speed, location, etc.).
- The network discovery and selection framework enables the association between a specific partner network, and one or more services, with an assigned priority for network selection for in-network roaming. Under control of the HPLMN, the network discovery and selection framework enables the HPLMN to steer the UE to a partner network (unconditionally or for a specific service) even when HPLMN coverage is available.

6.17.1.1 Architecture description

The solution is based on the architecture described in figures 6.17.1.1-1 and 6.17.1.1-2.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 396 of 501

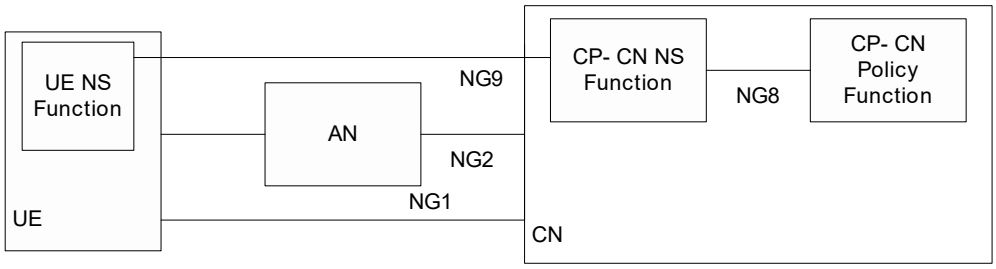


Figure 6.17.1.1-1: Non-roaming architecture for network discovery and selection

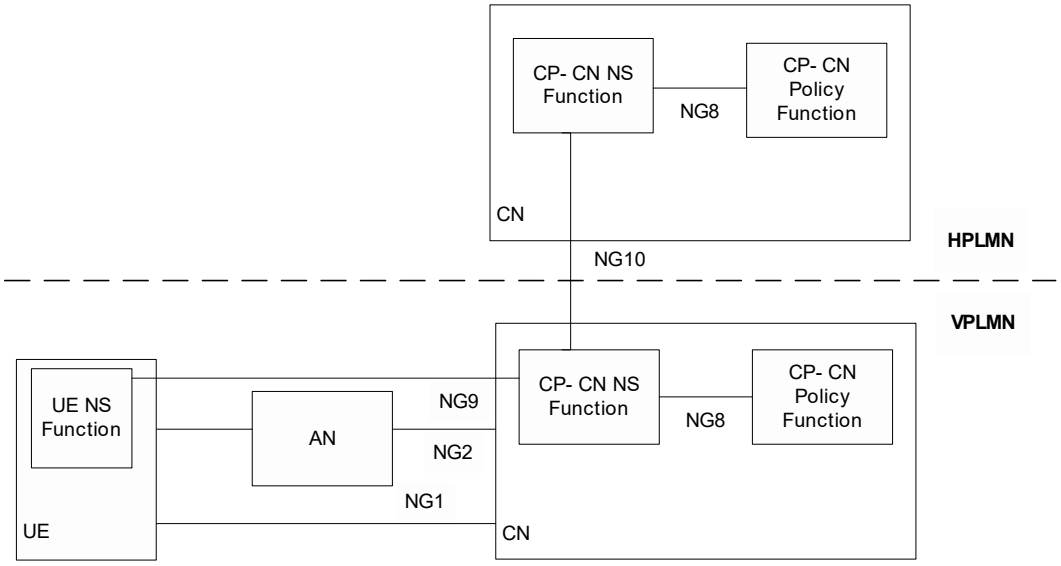


Figure 6.17.1.1-1: Roaming architecture for network discovery and selection

The following reference points are assumed for the proposed solution description:

NG1: Reference point between the UE and the CP functions

NG2: Reference point between the AN and the CP functions

NG8: Reference point between the CP-CN NS Function and the CP-CN Policy Function

NG9: Reference point between the UE NS Function and the CP-CN NS Function

NG10: Inter-PLMN CP-CN NS Function Reference point

Editor's note: It is FFS whether reference point between the CP-CN NS Function and the CP-CN Policy Function is required, i.e. whether the CP-CN NS Function is subset of the CP-CN Policy Function.

The functional entities in the architecture are defined as follows:

- CP-CN NS: the Control Plane CN Network Selection function is in charge of determining the content of, and conveying to the UE, the NDS policies about network discovery and selection.
- UE NS: the Network Selection function at the UE is in charge of:

  1) selecting a network to camp on upon power-up or recovery from lack of coverage;

  2) assessing whether a new network needs to be selected upon service initiation/termination;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 397 of 501

- CP-CN Policy: the Control Plane CN Policy function implements CN policing and control.

The policies may consist of the following information about network discovery and selection:

1) Preferred networks list, where a network is defined as a network identifier (e.g. PLMN, WLAN SSID), when applicable, RAT type, and optionally frequency information;

2) List of services/network slices supported by each network, optionally with associated information (e.g. RAT associate to the slice type);

3) Priority associated with each network for a given service, relative to other networks which also support the same service;

4) Optionally, a validity Condition specifying when/where a particular policy is valid (e.g. PLMN, time, location and RAN specific parameters). If this information is not included, the NDS policy is always considered as a valid.

Editor's note: It is FFS whether NDS policies include core network information (e.g. EPC or NextGen). It dependent on the solution to Key Issue #18: Interworking and Migration.

6.17.1.2 Function description

The solution is based on the following model:

- The CP-CN NS function determines the contents of the information to be conveyed to the UE for network discovery and selection. The CP-CN NS function may interact with the CP-CN Policy function to make this determination. The actual interaction depends on how dynamic the information conveyed to the UE is.

- The CP-CN NS function conveys the information necessary for network discovery and selection listed above to the UE.

Editor's note: How the CP-CN NS function conveys the information to the UE is FFS. It could include e.g. OOT mechanisms, pre-provisioning in the USIM, UE-implementation specific means, dedicated NAS signalling, or dedicated RRC signalling.

- Upon power-up, the UE NS function selects an initial network (PLMN + RAT combination) to camp on based on default preferred service(s) configured at the UE, and the UE's context;

- Upon service initiation/termination, the UE NS function assesses whether a new network (PLMN + RAT combination) needs to be selected. Impact to on-going services must be taken into account, for instance based on the provisioning of relative priorities assigned to different types of services at the UE.

Editor's note: impact on non-3GPP accesses is FFS

6.17.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.18 Solution for Key Issue 18: Interworking and Migration

6.18.1 Solution 18.1 : interworking between NextGen core and EPC

The solution introduces the high-level solution for interworking between NextGen core and EPC.

Interworking scenarios between NextGen core and EPC to be considered are as follows;

- intersystem changes between NextGen Core/Evolved LTE and EPC/LTE; and

- intersystem change between NextGen Core/New RAT and EPC/LTE.

6.18.1.1 functional description for interworking

Per UE mobility the mobility & session management mechanisms resolve the following aspects;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 398 of 501

- Interworking between EPC/LTE and NextGen Core/Evolved LTE:

1. It is the scenario for intersystem change using the inter-CN interface with or without change of RAT node.
2. Source system's security context can be reused for mutual authentication in the target system at least for some duration.

Editor's note: How to reuse source system's security context is responsibility of SA3.

3. Mobility anchor point changes.
4. Per application's characteristics service continuity and session continuity level should be determined.

    - When session continuity supported, in case of change from EPC to NextGen Core, PDN anchor point is kept and the data forwarding is made between NextGen UP and P-GW in EPC. In case of change from NextGen Core to EPC, PDU anchor point is kept and the data forwarding is made between NextGen UP and S-GW in EPC.

    - When session continuity not supported but service continuity supported, fast session recovery in the target system is needed.

Editor's note: Which service continuity and session continuity level is used for Voice service is FFS.

Editor's note: How to support PDN/PDU anchor point preservation during intersystem change is FFS.

- Interworking between EPC/LTE and NextGen core/New RAT:

1. It is the scenario for intersystem change using the inter-CN interface with change of RAT node.
2. Source system's security context can be reused for mutual authentication in the target system at least for some duration.

Editor's note: How to reuse source system's security context is responsibility of SA3.

3. Mobility anchor point changes
4. Per application's characteristics service continuity and session continuity level should be determined.

    - When session continuity supported, in case of change from EPC to NextGen Core, PDN anchor point is kept and the data forwarding is made between NextGen UP and P-GW in EPC. In case of change from NextGen Core to EPC, PDU anchor point is kept and the data forwarding is made between NextGen UP and S-GW in EPC.

    - When session continuity not supported but service continuity supported, fast session recovery in the target system is needed.

Editor's note: Which service continuity and session continuity level is used for Voice service is FFS.

Editor's note: How to support PDN/PDU anchor point preservation during intersystem change is FFS.

6.18.1.2 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.18.2 Solution 18.2: Solution for interworking

This solution addresses Key Issue #18 based on the following possible scenarios:

- interworking scenarios (including mobility):

    - Scenario I1: an operator deploys one of the NG RAN options in conjunction with a NextGen CN and upgrades all the installed E-UTRAN nodes to support the new CN-RAN NG2/NG3 for NG UEs. In this scenario service continuity is only provided between the Evolved E-UTRAN base and the NG RANs connected to the Next Gen core network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 399 of 501

- Scenario I2: an operator has not upgraded all the installed E-UTRAN nodes, has upgraded only parts of the installed E-UTRAN nodes to support the new CN-RAN NG2/NG3, or has deployed Option 3 for macro coverage and stand-alone NR with NextGen CN for e.g. small cells. CN interworking is provided from EPC to NextGen CN to provide full service continuity.

6.18.2.1 Architecture description

It is assumed that on the radio side the upgraded E-UTRAN and options 5 and 7 of [11] support the legacy LTE-Uu interface.

In this solution we refer to NG Core (NGC) capable UE as a UE that is capable of supporting NG NAS via NG1 interface.

It is assumed that in addition a NGC UE is capable of supporting:

- EPC NAS: this is the Rel. 15 NAS protocol defined for EPC, at least to operate in legacy networks e.g. in case of roaming.

The UE will use EPC NAS or NG NAS depending on the core network by which it is served.

The UE will always use the NG NAS when connecting to the NG RAN (option 2, 4, 5 and 7 of [11]). The UE may use the NG NAS when connecting to E-UTRAN (scenario I1).

In all the architectures for the various scenarios, it is assumed that the EPC and the NGC have access to a common subscriber database.

In this solution, all interworking scenarios assume single-CN registration at any point in time for the 3GPP RATs (i.e. similar to EPC).

Service continuity is provided for the various scenarios as described below.

6.18.2.1.1 Architecture for Scenario I1

Figure 6.18.2.1-1 describes the architecture for tight interworking for scenario I1.

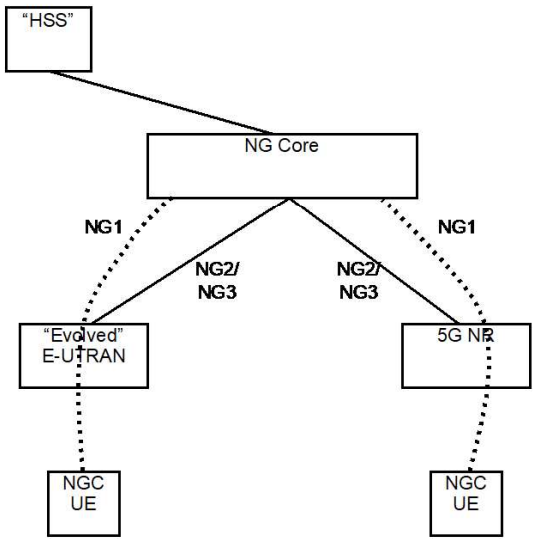


Figure 6.18.2.1-1: Architecture for interworking for scenario I1

In this scenario:

- If E-UTRAN supports access to NG Core (i.e. E-UTRAN is "evolved") then interworking e.g. idle and connected mode mobility is performed using only NG Core procedures.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 400 of 501

This solution provides no service continuity between the non-Evolved E-UTRAN and the NG RANs. If/once the whole base of E-UTRAN is upgraded to Evolved E-UTRAN, service continuity is implicitly provided between the various NG RAN options the operator decides to deploy since they commonly interface to NGC via NG2/NG3.

6.18.2.1.2 Architecture for Scenario I2

6.18.2.1.2.1 Architecture for the non-roaming and roaming with local breakout scenarios

Figure 6.18.2.1-2 describes the architecture for tight interworking for scenario I2.

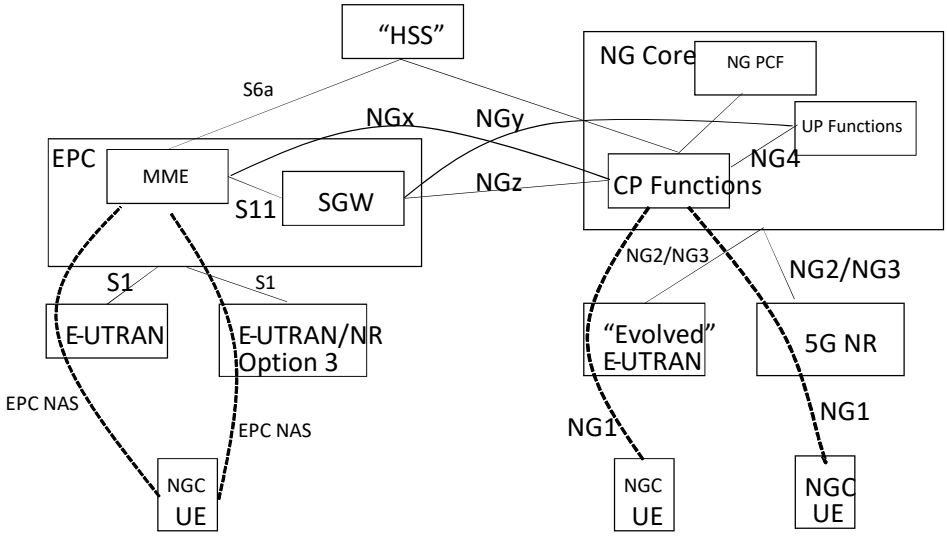


Figure 6.18.2.1-2: Architecture for interworking scenario I2(non-roaming and roaming with local breakout scenarios)

In this solution, NGx and NGy interfaces are introduced between the MME and SGW respectively and NG Core CP and UP functions in order to enable interworking between EPC and the NG core. NGx and NGy are inter-CN interfaces respectively for c-plane and u-plane, and may correspond to inter-NG CN interfaces; the interfaces are explicitly named for references in the definition of procedures. In addition, NGz interface is defined between the SGW and the NG Core CP function. The NG PCF is involved if policy and charging is controlled in a dynamic way.

NOTE: The NG PCF is capable of supporting functionalities of EPS PCRF.

When connecting to E-UTRAN (including option 3), the UE uses EPC NAS with the core network. In such scenario, when connected to a non-evolved E-UTRAN, the UE authentication, mobility management and session management are performed by the MMEtowards the UE.

In order to support idle or connected mode mobility between EPC and NG Core,the UEs serving MME connects via a control plane NGx interface to CP functions in the NGC, and the UE's serving SGW connects via a user plane NGy interface to user plane functions in the NGC and via a control plane NGz interface to CP functions in the NGC. User plane should always be anchored in NG CN for UE with NG RAN subscription. The GW selection can still be done by the MME with the current mechanisms, but based on UE subscription (that enables 5G CN) will result in a GW in the 5G CN.

Editor's note: Whether NGx/NGy/NGz is a new NG Core interface or S10/S5-U/S5-C is FFS.

Editor's note: Whether and how the GW selection mechanism is impacted is FFS.

Interworking with NextGen in this solution is performed by:

- enabling the UE to perform initial attach over E-UTRAN (including option 3) using EPC NAS, and later move to Evolved E-UTRAN or 5G NR and use NG NAS by interworking with the NG core (e.g. moving the UE context to the NG core). During initial attach the UE user plane may be anchored in user plane function(s) provided by the NGC to support mobility

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 401 of 501

Editor's note: the details of interworking upon UE mobility depend on the solutions for mobility management (e.g. handover) defined in other key issues.

- enabling the UE to perform initial attach and session management over Evolved E-UTRAN or 5G NR using NG1, and later move to E-UTRAN and use EPC NAS by interworking with the NG core (e.g. moving the UE context from the NG core).

Service continuity is provided between E-UTRAN and the NG RAN options deployed by the operator via the Interworking Function and the common anchoring of the user plane. Inter-RAN PDU forwarding may be supported.

6.18.2.1.2.2 Architecture for the home-routed roaming scenario

Figure 6.18.2.1-3 shows the reference architecture for the home-routed roaming scenario.

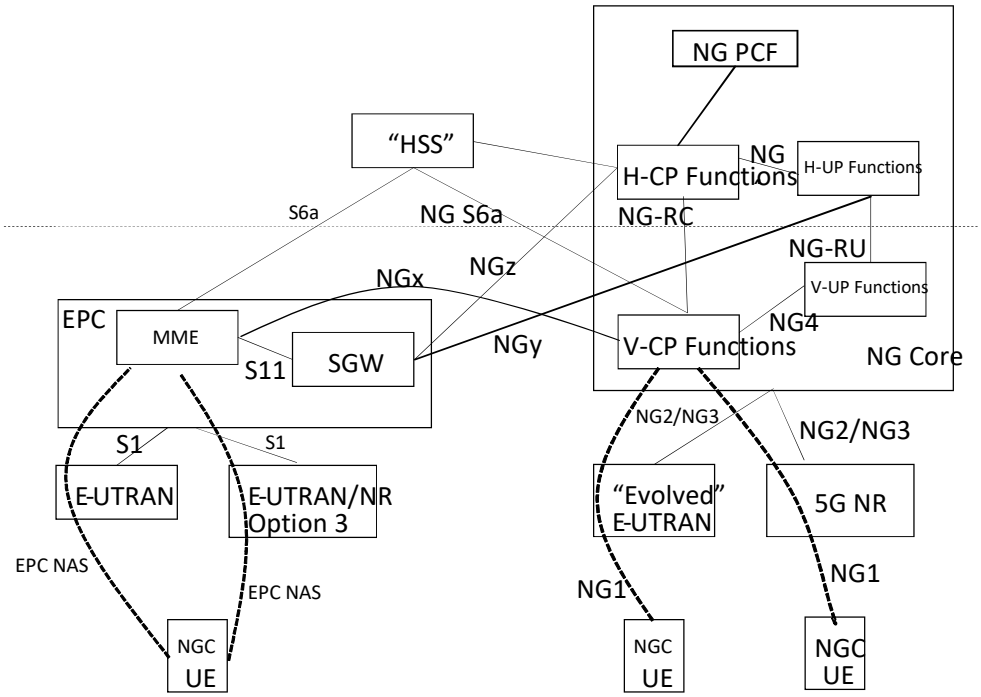


Figure 6.18.2.1-3: Architecture for interworking scenario I2 (home-routed roaming scenario)

Differences compared to the non-roaming and roaming with local breakout scenarios include:

- The MME is connected to the NGC CPF in the HPLMN via the NGx interface; and
- The SGW is connected to the NGC CPF and NGC UPF in the VPLMN respectively via the NGz and NGy interfaces.
- If policy and charging is controlled dynamically, the NG PCF is connected to the NGC CPF in the VPLMN.

Editor's note: Whether NGx/NGy/NGz are new NG Core interfaces or S10/S8-U/S8-C is FFS.

6.18.2.1.2.3 Signalling flows

Figure 6.18.2.1.2.3-1 shows a signalling flow for handover from the EPS to the NGS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 402 of 501

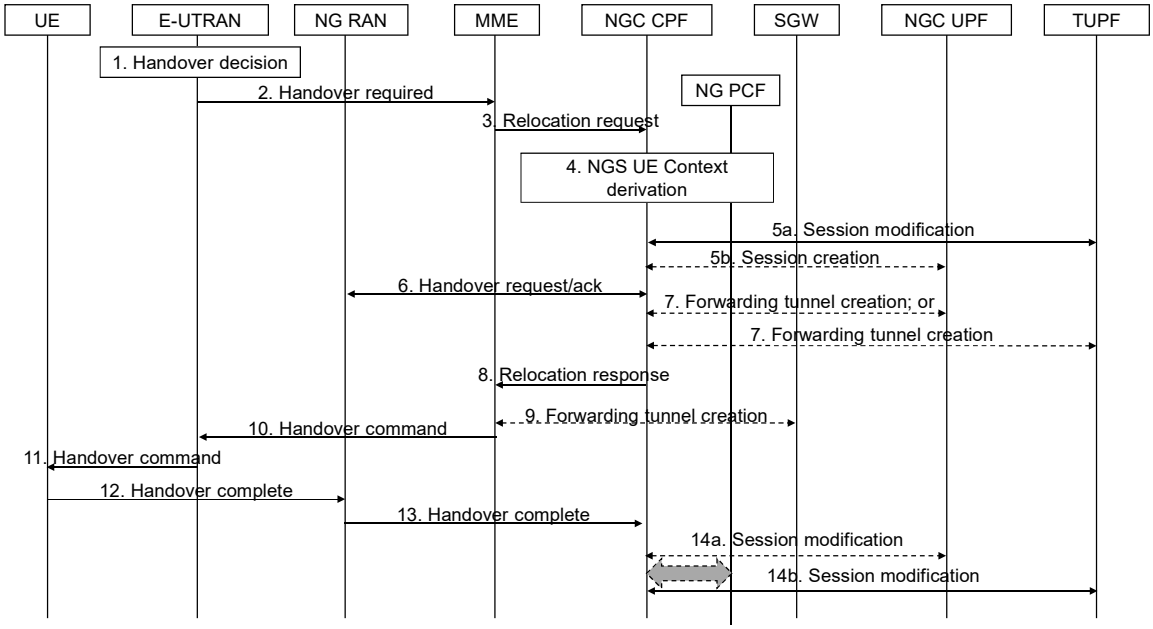


Figure 6.18.2.1.2.3-1: Signalling flow for handover from the EPS to the NGS

1. E-UTRAN decides that the UE should be handed over to the NG RAN. The UE PDU sessions are anchored in the NGC and the user plane PDU path includes the anchoring NGC UPF (TUPF), an EPC SGW supporting NGy, and E-UTRAN.

2. The E-UTRAN sends a Handover Required (Target NG RAN Node ID, Source to Target Transparent Container) message to the MME.

3. The MME selects an NGC CPF and sends a Relocation Request (Target NG RAN Node ID, Source to Target Transparent Container, MM and SM EPS UE Context) message to the selected NGC CPF.

4. The NGC CPF converts the received MM EPS UE Context into the NGS MM UE Context. The NGC CPF reconciles the SM NGS UE context(s) with the SM EPS UE Context (including EPS QoS information), since the NGC CPF function already has a UE SM context. The NGS UE Context includes the NG QoS Rules for NG RAN and NGC UPF(s).

Editor's note: It is FFS whether the NGC CPF performs mapping of EPS QoS information into NG QoS Rules or NGC CPF should interact with the NG PCF to derive NG QoS Rules. This will be clarified as NG policy framework becomes clear.

Editor's note: How the NGS Security Context is derived is FFS.

5. The NGC CPF may decides whether another NGC UPF should be selected in addition to the TUPF. If the traffic for at least one PDU session is home routed (i.e. the TUPF is in the HPLMN), then an NGC UPF is selected in the VPLMN.

Editor's note: whether the traffic of all PDU sessions is routed via this new NGC UPF in the VPLMN, or only for the home routed PDU sessions, depends on the conclusions on the overall architecture.

If the NGC CPF decides to put an additional NGC UPF between the NG RAN and the TUPF, the NGC CPF:

- requests session modification towards the TUPF providing updated NG QoS Rules (step 5a);

- receives the NG9/NG-RC UL Tunnelling Information from the TUPF (step 5a), if needed;

Editor's note: It is FFS whether the NGy UL Tunnelling Information can be reused and thus the providing NG9/NG-RC UL Tunnelling Information is not necessary.

- requests session creation towards the additional NGC UPF including NG9/NG-RU UL Tunnelling Information (step 5b); and

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 403 of 501

- receives the NG3 UL Tunnelling Information from the non-terminating NGC UPF (step 5b).

  Otherwise, the NGC CPF requests session modification towards the TUPF including NG QoS Rules in the session creation request message (step 5a). The NGC UPF responds with the NG3 UL Tunnelling Information (step 5a).

6. The NGC CPF sends a Handover Request (Source to Target Transparent Container, NG QoS Rules, NG3 UL Tunnelling Information) message to the NG RAN.

   The NG RAN sends a Handover Request Acknowledge (Target to Source Transparent Container, NG3 DL Tunnelling Information for PDU Forwarding) to the NGC CPF.

Editor's note: Details on the PDU forwarding negotiation are FFS and are in the scope of other WGs (e.g. RAN3, CT4).

7. If the NG RAN provided NG3 DL Tunnelling Information for PDU Forwarding, the NGC CPF requests forwarding tunnel creation to the NGC UPF (either TUPF or non-terminating UPF in case additional NGC UPF is selected in step 5). The NGC UPF responds to the forwarding tunnel creation request including NGC UPF-side NGy Tunnelling Information for PDU Forwarding.

8. The NGC CPF sends a response message to the Relocation Request message (sent in step 3). The response message includes the Target to Source Transparent Container and may include the NGC UPF-side NGy Tunnelling Information for PDU Forwarding.

9. If the Relocation Response message includes the NGC UPF-side NGy Tunnelling Information for PDU Forwarding, the MME sends a Create Indirect Data Forwarding Tunnel Request (NGC UPF-side NGy Tunnelling Information for PDU Forwarding) message to the SGW. The SGW sends a Create Indirect Forwarding Tunnel Response (S1 UL Tunnelling Information for PDU Forwarding)

10. The MME sends a Handover Command (Target to Source Transparent Container, S1 UL Tunnelling Information for PDU Forwarding) message to the E-UTRAN.

11. Towards the UE, the E-UTRAN commands handover to the NG RAN. The UE detaches from the E-UTRAN and synchronizes to the NG RAN.

    The E-UTRAN forwards PDUs coming from the SGW to the NGC UPF using the S1 UL Tunnelling Information for PDU Forwarding, the SGW forwards the PDUs to the NGC UPF using the NGC UPF-side NGy Tunnelling Information for PDU Forwarding, and the NGC UPF forwards the PDUs to the NG RAN using the NG3 DL Tunnelling Information for PDU Forwarding.

Editor's note: It is FFS how the PDUs can be forwarded via NGy and mapped to QoS flows.

12. The UE confirms handover to the NG RAN.

13. The NG RAN notifies to the NGC CPF that the UE is handed over to the NG RAN. The notification message includes the NG3 DL Tunnelling Information.

14. If the additional non-terminating NGC UPF was selected in step 5, the NGC CPF:

    - updates the non-terminating NGC UPF with the NG3 DL Tunnelling Information (step 14a);

    - receives the NG9/NG-RU DL Tunnelling Information (step 14b); and

    - updates the TUPF with the NG9/NG-RU DL Tunnelling Information (step 14b).

      Otherwise, the NGC CPF updates the TUPF with the NG3 DL Tunnelling Information (step 14b).

      The NGC CPF may inform NG PCF of the UE's handover to the NG RAN. The NGC CPF may notify the MME that the relocation is complete and session/context in the EPS-side can be deleted. The location registration procedure can be performed.

Figure 6.18.2.1.2.3-2 depicts a signalling flow for handover from the NGS to the EPS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 404 of 501

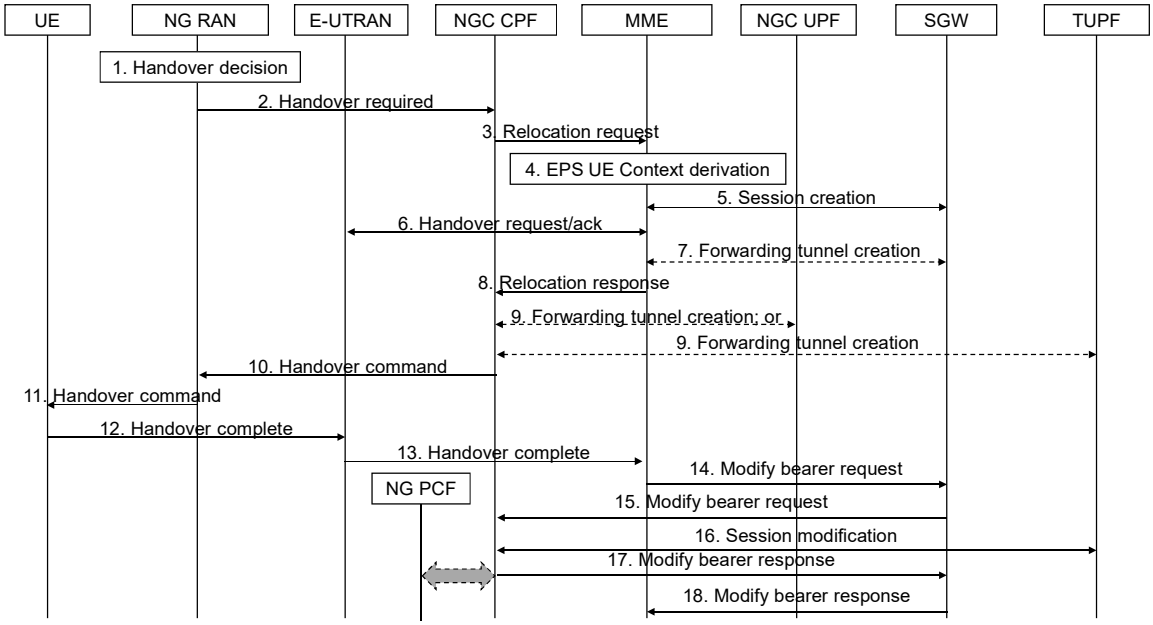


Figure 6.18.2.1.2.3-2 Signalling flow for handover from the NGS to the EPS

1. The NG RAN decides that the UE should be handed over to the E-UTRAN. The use plane PDU path includes the anchoring NGC UPF (TUPF), non-terminating NGC UPF (optional), and NG RAN.

2. The NG RAN notifies the NGC CPF that handover is required. The notification message includes Target eNB ID, Source to Target Transparent Container.

3. The NGC CPF selects an MME and sends a Relocation Request (Target eNB ID, Source to Target Transparent Container, NGS UE Context) message to the selected MME.

4. The MME converts the received NGS UE Context into EPS UE Context.

Editor's note: How the EPS Security Context is derived is FFS.

5. The MME sends a Create Session Request (PDN Connection Information (including EPS Bearer Contexts)) message to the SGW and the SGW responds to the MME with a Create Session Response (S1 UL Tunnelling Information) message.

6. The MME sends a Handover Request (Source to Target Transparent Container, E-RAB Contexts (including S1 UL Tunnelling Information)) message to the E-UTRAN.

   E-UTRAN sends a Handover Request Acknowledge (Target to Source Transparent Container, S1 DL Tunnelling Information for PDU Forwarding) message to the MME.

Editor's note: Details on the PDU forwarding negotiation are FFS and are in the scope of other WGs (e.g. RAN3, CT4).

7. If the E-UTRAN provided S1 DL Tunnelling Information for PDU Forwarding, the MME requests forwarding tunnel creation to the SGW. The SGW responds to the forwarding tunnel creation request including SGW-side NGy Tunnelling Information for PDU Forwarding.

8. The MME sends a response message to the Relocation Request message (sent in step 3). The response message includes the Target to Source Transparent Container and may include the SGW-side NGy Tunnelling Information for PDU Forwarding.

9. If the Relocation Response message includes the SGW-side NGy Tunnelling Information for PDU Forwarding, the NGC CPF requests forwarding tunnel creation towards the NGC UPF (either TUPF or non-terminating NGC UPF if available). The request message includes the SGW-side NGy Tunnelling Information for PDU Forwarding. The NGC UPF responds to the NGC CPF with the NG3 UL Tunnelling Information for PDU Forwarding.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 405 of 501

10. The NGC CPF sends a Handover Command (Target to Source Transparent Container, NG3 UL Tunnelling Information for PDU Forwarding) message to the NG RAN.

11. Towards the UE, the NG RAN commands handover to the E-UTRAN. The UE detaches from the NG RAN and synchronizes to the E-UTRAN.

    The NG RAN forwards PDUs coming from the NGC UPF to the NGC UPF using the NG3 UL Tunnelling Information for PDU Forwarding, the NGC UPF forwards the PDUs to the SGW using the SGW-side NGy Tunnelling Information for PDU Forwarding, and the SGW forwards the PDUs to the E-UTRAN using the S1 DL Tunnelling Information for PDU Forwarding.

Editor's note: It is FFS how the PDUs can be forwarded via NGy and mapped to bearers.

12. The UE confirms handover to the E-UTRAN.

13. The E-UTRAN notifies to the MME that the UE is handed over to the E-UTRAN. The notification message includes the S1 DL Tunnelling Information.

14. The MME sends a Modify Bearer Request (S1 DL Tunnelling Information) message to the SGW.

15. The SGW sends a Modify Bearer Request (EPS Bearer Contexts (including NGy DL Tunnelling Information)) message to the NGC CPF.

16. The NGC CPF requests session modification to the TUPF. The TUPF receives EPS Bearer Contexts including NGy DL Tunnelling Information from the NGC CPF. The NGC CPF obtains Per-Bearer NGy UL Tunnelling Information from the TUPF.

17. The NGC CPF sends a Modify Bearer Response (Per-Bearer NGy UL Tunnelling Information) message to the SGW. The SGW replaces the NGy UL Tunnelling Information received in step 5 with the Per-Bearer NGy UL Tunnelling Information.

    The NGC CPF may inform NG PCF of the UE's handover to the E-UTRAN.

18. The SGW sends a Modify Bearer Response message to the MME.

    The MME may notify the NGC CPF that the relocation is complete and session/context in the NGS-side can be deleted. The location registration procedure can be performed.

6.18.2.2 Function description

Architecture I2 impacts the following functional entities:

MME:

- NGx interface to perform idle and connected mode mobility procedures to/from NG Core

SGW:

- NGy interface to perform mobility procedures to/from NG Core and to anchor user plane in NG Core
- NGz interface to perform mobility procedures to/from NG Core

CP Functions in NG Core:

- NGx interface to perform idle and connected mode mobility procedures to/from EPC
- NGz interface to perform mobility procedures to/from EPC

UP Functions in NG Core:

- NGy interface to perform connected mode mobility procedures to/from EPC by always anchoring user plane in NG CN

Editor's note: Depending on whether NGx, NGy, and NGz are new NG Core interfaces or S10, S5/S8-U, and S5/S8-C impacts to some of the above entities are omitted, e.g. if NGx is S10 then there is no impact in the MME since the CP functions of NG Core will look like another MME to the UEs "source" MME.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 406 of 501

NOTE: Using appropriate core network selection mechanisms e.g. DECOR, network slicing etc the UEs that are capable of interworking using this solution can be directed to specific EPC and NGC functions that support NGx/NGy/NGz and therefore this solution does not need to impact the whole EPC or NextGen CN deployment in a particular PLMN.

6.18.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.18.3 Solution 18.3: Solutions for migration from E-UTRAN/EPC including option 3 to option 2,4,5, or 7

This solution addresses Key Issue #18 based on the following possible scenario:

- Migration scenarios
  - Scenario M1: an operator that deploys option 3 of [11] first, and then deploys one of the NG RAN options in [11] in conjunction with a NextGen CN.

6.18.3.1 Architecture description

In this solution we refer to NG Core (NGC) capable UE as a UE that is capable of supporting NG1 interface procedures in at least one or more of Options 2, 4, 5, and 7. A UE supporting only Option 3 is not an NGC UE, since it only supports EPC NAS (e.g. procedures defined in TS 23.401 [2], etc.).

It is assumed that in addition a NGC UE may also be capable of supporting EPC NAS (this is the NAS protocol defined for EPC) at least to operate in legacy networks e.g. in case of roaming

The UE will use EPC NAS or NG1 procedures depending on the core network by which it is served.

In all the architectures for the various scenarios, it is assumed that the EPC and the NGC have access to a common subscriber database.

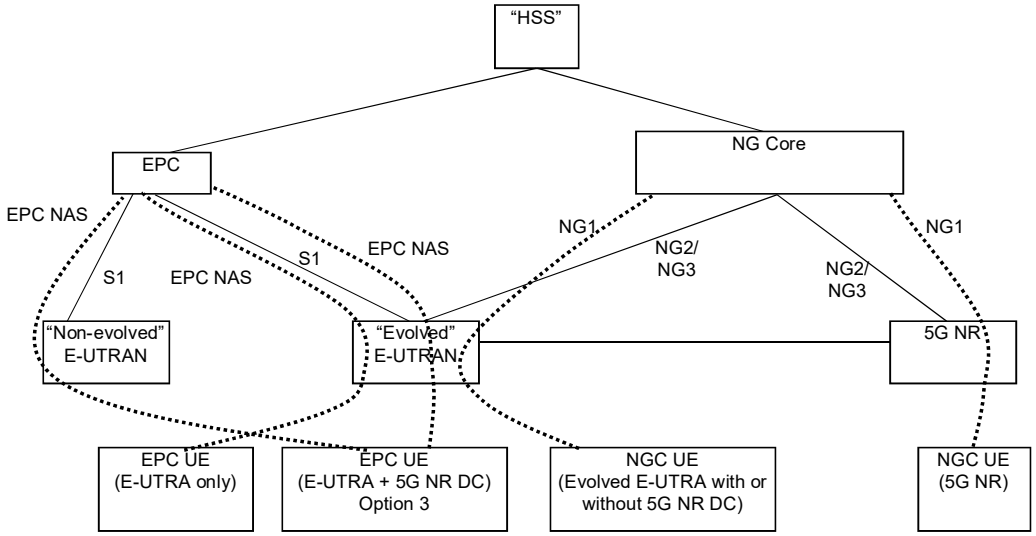


Figure 6.18.3.1-1: Architecture for migration scenario M1

A UE that supports only option 3:

- always performs initial access through E-UTRA (LTE-Uu) but never through 5G NR

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 407 of 501

- performs EPC NAS procedures over E-UTRA (i.e. mobility management, session management, authentication, etc)
- has to support "non-evolved" E-UTRA procedures for backwards compatibility with pre-rel.15 networks (e.g. for roaming, mobility between NSA NR and E-UTRA)

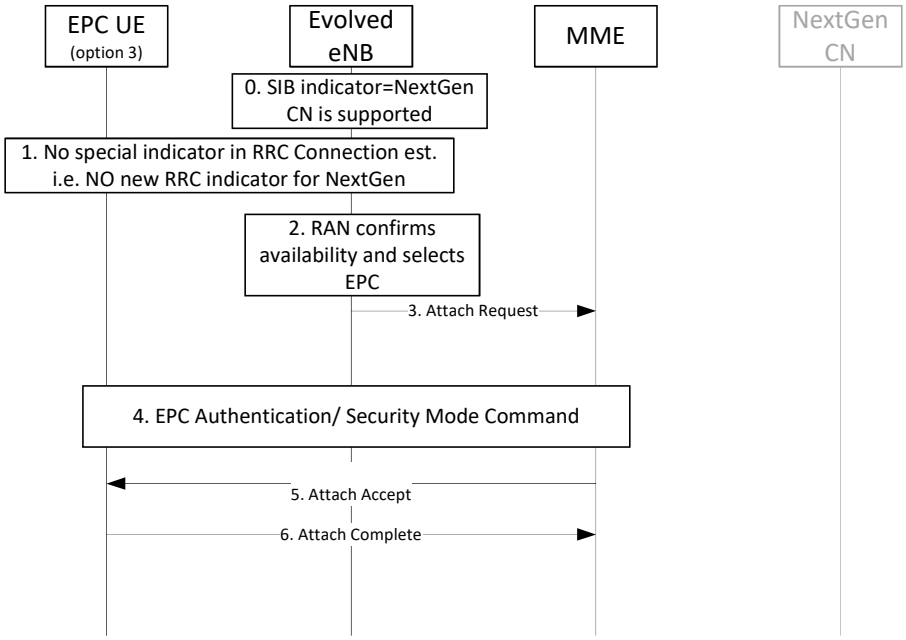


Figure 6.18.3.1-2: Initial access for EPC UE supporting only option 3 over "Evolved" E-UTRAN

A NGC UE that supports one or more of options 2, 4, 5, and 7:

- performs initial access through "evolved" E-UTRA (LTE-Uu) (in option 7, 5) or 5G NR (in option 2, 4);
- performs EPC or NG1 procedures over E-UTRA or "evolved" E-UTRA respectively (i.e. mobility management, session management, authentication, etc) depending on capability indicated by E-UTRA, if the NGC UE also supports EPC NAS;
- may support "non-evolved" E-UTRA procedures for backwards compatibility with pre-rel.15 networks (e.g. for roaming, mobility between NSA NR and E-UTRA).

NOTE 1: A UE supporting Option 3 and one or more of Options 2, 4, 5, or 7 operates like NGC UE when NG CN is supported by the serving PLMN.

NOTE 2: What the NGC UE does if the NextGen CN rejects the NGC UE because it does not have related subscription will be addressed in normative phase.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 408 of 501

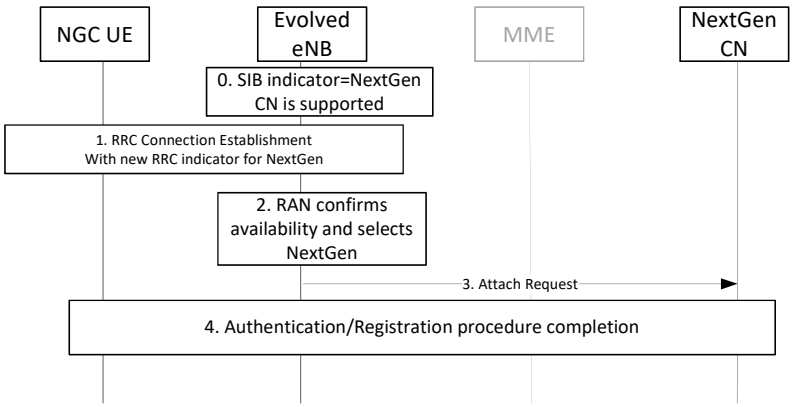


Figure 6.18.3.1-3: Initial access for NGC UE over "Evolved" E-UTRAN

In order to support option 3-only UEs and NGC UEs in the same network:

- If E-UTRAN supports access to NG Core (i.e. E-UTRAN is "evolved") then it indicates this to the UEs (e.g. in SIB)
- The NGC UE that supports NG NAS provides an indication in RRC when it performs initial access (e.g. a mechanism similar to that used for CIOT and can be used to indicate ability to support NGC)
- The option 3-only UE (that only support EPC NAS) does not provide this indication in RRC when it performs initial access and therefore E-UTRAN uses the "default" CN selection mechanism to direct this UE to an MME

The Evolved E-UTRAN shall direct the NGC UE to NG Core. The non-evolved E-UTRAN always directs the UE to the EPC.

6.18.3.2 Function description

The UE that only supports option 3:

- always performs initial access through E-UTRA (LTE-Uu) but never through 5G NR;
- performs EPC NAS procedures over E-UTRA (i.e. mobility management, session management, authentication, etc);
- has to support "non-evolved" E-UTRA procedures for backwards compatibility with pre-rel.15 networks (e.g. for roaming, mobility between NSA NR and E-UTRA).

The NGC UE has the following characteristics:

- When it is camped in a Evolved E-UTRAN uses NG1 procedures;
- If supported, when it is camped in (non-evolved) E-UTRAN uses EPC NAS;
- Provides an indication of support of NG1 procedures in RRC when it performs initial access (e.g. a mechanism similar to that used for CIOT and can be used to indicate ability to support NG Core).

E-UTRAN:

- If it supports access to NG Core (i.e. E-UTRAN is "evolved") then it indicates this to the UEs (e.g. in SIB)
- Direct the UE to the right CN based on the RRC indication provided at initial access

6.18.3.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

This solution provides migration between E-UTRAN/EPC including option 3 and other NG Core based options (i.e. option 2,4,5, and 7) and describes co-existence of option 3-only UEs and NGC UEs.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 409 of 501

Impacts in the UE and E-UTRAN are identified in clause 6.18.3.2.

6.18.4 Solution 18.4: Solution for interworking and migration

6.18.4.1 Architecture description

This solution addresses Key Issue #18 (in particular WT#1, WT#2 and WT#3) based on the following principles:

- Where possible the installed E-UTRAN access base is upgraded to support the new CN-RAN interface towards the NG Core (NG2/NG3). This approach allows for tight interworking between upgraded E-UTRAN access and NG RAN access.

- Loose interworking based on "dual attach" or "Handover Attach"operation(with either "single radio" or "dual radio" support at the lower layers) in areas where the installed E-UTRAN access base has not been upgraded. The same type of interworking is supported to/from GERAN and UTRAN access.

Depicted in Figure 6.18.4.1-1 is a simplified system architecture that allows for tight interworking between evolved NG RAN anchored on E-UTRA (options 5, 7) and NG RAN anchored on NR (options 2, 4).

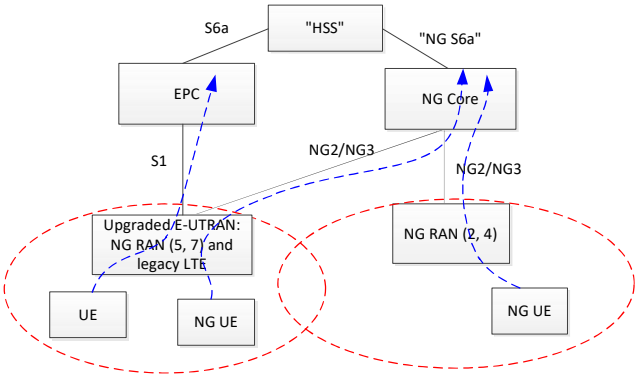


Figure 6.18.4.1-1: Architecture for tight interworking between upgraded E-UTRAN base (supporting options 5, 7 and legacy LTE) and NG RAN anchored on NR (options 2, 4)

It is assumed that the installed E-UTRAN base has been upgraded to support the new CN-RAN interface ("NG2/NG3" in Figure 6.18.4.1-1) in addition to supporting the S1 interface towards the EPC. On the radio side it is assumed that the upgraded E-UTRAN base supports the legacy LTE-Uu interface, in addition to the E-UTRA anchored NR (options 5, 7).

When under coverage of the upgraded E-UTRAN base the legacy UEs are steered towards EPC, whereas NG UEs are steered towards the NG Core.

The NAS protocol used between NG UE and NG Core ("NG NAS") is different from the legacy NAS protocol used between the legacy UE and the EPC ("EPS NAS").

The EPC and the NG Core have access to a common subscriber database ("HSS"), but have no other interworking interfaces with each other. Therefore there is no legacy baggage carried over in the NG Core.

Depicted in Figure 6.18.4.1-2 is a simplified system architecture that allows for loose interworking between GERAN, UTRAN or non-evolved E-UTRAN access on one side and NG RAN on the other.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 410 of 501

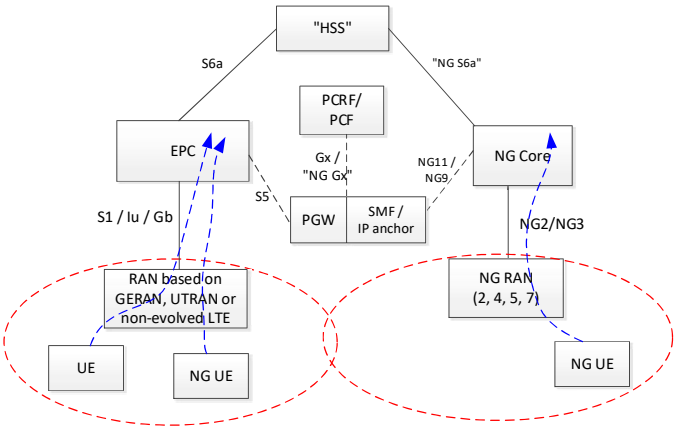


Figure 6.18.4.1-2: Architecture for loose interworking between GERAN, UTRAN or non-evolved E-UTRAN and NG RAN

In this case an NG UE under the coverage of GERAN, UTRAN or non-evolved E-UTRAN access is steered towards the EPC.

When in dual coverage (i.e. both under GERAN/UTRAN/EUTRAN access and under NG RAN access (options 2, 4, 5, 7) the UE operates in "dual attach" mode i.e. it is simultaneously attached over two independent systems, and uses two independent Mobility Management and Session Management contexts. At the lower layers UE may be operating in either "single radio" or "dual radio" mode, depending on the support that will be defined by the RAN working groups.

Again the EPC and the NG Core have access to the common subscriber base ("HSS"). However, they may optionally also share a common PGW / SMF / IP anchor in order to enable handovers with IP address preservation (similar to how 3GPP-WLAN handovers work in EPS). The common PGW/ SMF/ IP anchor supports NG11 towards the MMF in the NextGen Core and NG9 towards a UPF in the NextGen Core. If dynamic PCC support is needed, the EPC and the NG Core also share a common PCRF/PCF node.

NOTE 1: In this solution there are two user plane functions in the non-roaming case (i.e. one in the NG Core and another one in the common PGW / SMF / IP anchor).

NOTE 2: As a deployment option, the shared nodes can also be part of the NG Core.

The handover procedure from the source to the target system is based on the "Handover Attach" procedure defined for 3GPP-WLAN interworking. On the target side all QoS constructs (i.e. EPS bearers or QoS Flows) are re-established from scratch and the mapping between the two will be defined as part of Key Issue #2.

If the EPC and the NG Core do not share a common PGW / SMF /IP anchor, it is still possible to provide service continuity upon handover by leveraging "upper layer" service continuity mechanisms, as described by some solutions in clause 6.6.

For IMS voice service established via the NG Core it is possible to provide service continuity upon handover to/from GERAN or UTRAN by using Dual Radio VCC (DRVCC) as described in TS 23.237 [18].

The loose interworking solution described previously can also be applied for interworking between Option 3 RAN connected to EPC and NG RAN connected to NG Core, as illustrated in Figure 6.18.4.1-3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 411 of 501

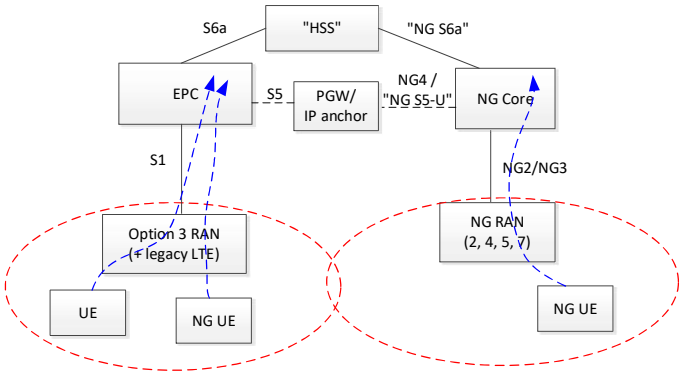


Figure 6.18.4.1-3: Architecture for loose interworking between Option 3 RAN connected to EPC and NG RAN connected to NG Core

The interworking can be made seamless if the combination of radio bands used in the areas served by Option 3 RAN and those used in areas served by NG System allow for "dual attach" (or "Handover Attach") operation. Alternatively, interworking between Option 3 RAN connected to EPC and NG RAN can also be supported using tight interworking (not illustrated) along the principles illustrated in Figure 6.18.4.1-1. This means that the E-UTRAN nodes that have been upgraded once to support Option 3 need to be upgraded a second time to support NG2/NG3 towards NG Core.

6.18.4.2 Function description

Depicted in Figure 6.18.4.2-1 is a call flow for the "Handover Attach" procedure when UE moves from the NG System to the EPS. The call flow for the opposite direction is similar and is omitted for brevity.

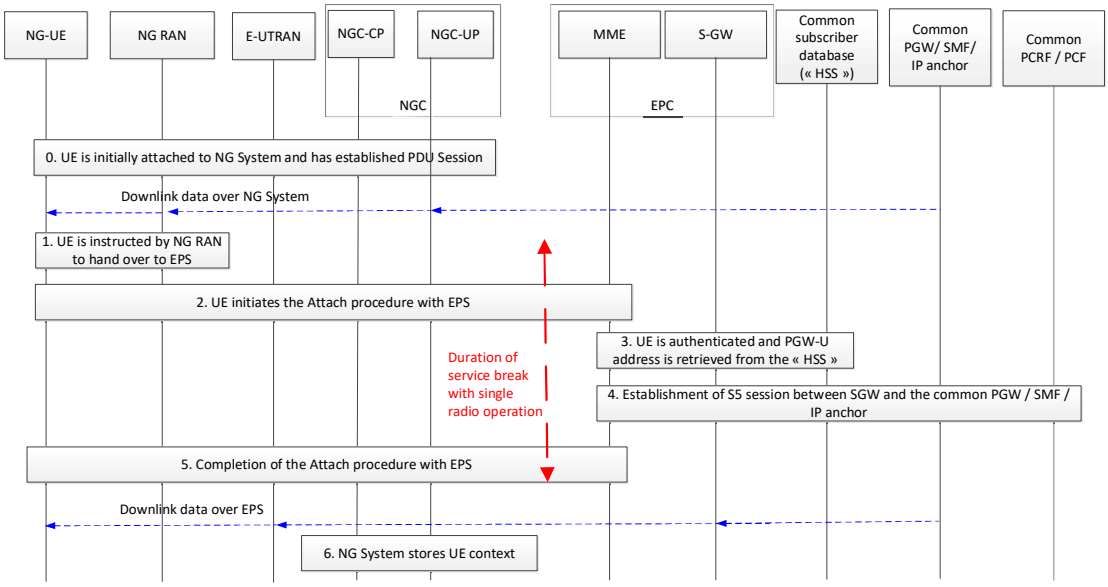


Figure 6.18.4.2-1: Call flow for "Handover Attach" from NG System to EPS

0. Initially UE is attached to the NG System and has established PDU Session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 412 of 501

1. At some point (e.g. UE being on the border area of a NG System island) the UE is instructed by NG RAN to perform "Handover Attach" to the target system (i.e. the EPS, in this case). It is expected that RAN will design measurements of E-UTRAN cells while UE is under NR coverage, and vice versa.
2. UE initiates the Attach procedure with EPS.
3. As part of the Attach procedure, the UE is authenticated and the PGW address is retrieved from the common subscriber database ("HSS").
4. The S5 session between the SGW and the PGW part of the common PGW / SMF / IP anchor is established and at this point the DL traffic diverted towards the EPS access.
5. Completion of the Attach procedure with UE communicating over EPS. If there is a need for dedicated EPS bearers, they are established as part of the Attach procedure based on the information provided from the PCRF/PCF.
6. The CP function in the NG System stores UE context for certain period of time.

If there is "dual radio" support at the lower layers, the handover can be made seamless by establishing a connection towards the target system before releasing the connection with the source system.

Editor's note: When and how the connection towards the source system is released is FFS.

If there is only "single radio" support from the lower layers, the "Handover Attach" is performed in break-before-make manner and the service break duration is comparable to the duration of the Attach procedure in the target system. The duration of the Attach procedure further depends whether the target CN function (e.g. MME in EPS) has stored security context of the UE or not.In order to minimise the service break duration for subsequent handbacks to the other system it is expected that the old system will keep UE's security context for some time (e.g. similar to how the MME today stores UE context even after UE hands over to WLAN).

6.18.4.3 Solution evaluation

The solution allows for seamless (dual radio) or non-seamless (single radio) handovers.

In order to minimise the handover duration for subsequent handbacks it is expected that the source system keeps the UE security context for certain period of time.

6.18.5. Solution 18.5: Solution for full and partial migration scenarios from EPS to NG System

6.18.5.1 Architecture for full and partial migration scenarios from EPS to NG System

Common to migration scenarios is the requirement for interworking between EPS and NextGen System. This is necessary to allow mobility in case UEs moving across deployment borders while providing service continuity. We expect such requirement to exist at least for voice services.

The architecture to support service continuity for NextGen UEs is depicted below:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 413 of 501

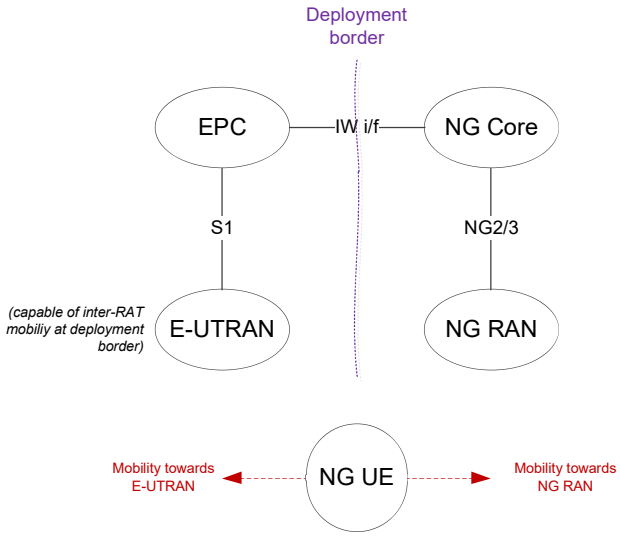


Figure 6.18.5.1-1: Architecture to support migration scenarios for NG UEs

Architectural elements necessary to support migration for NG UEs:

- C- and U-Plane interface between EPC and NextGen Core for mobility signalling and transfer of user data
- inter-RAT interworking functions in E-UTRAN and NG RAN ("source adapts to target") and in UE
- X2-like connectivity is possible between the RAN parts at the deployment border, but not assumed to be absolutely necessary

When looking at the main protocol entities that need to be present in the nodes, further peculiarities for interworking can be deduced (Note, that the figure below depicts a collection of main protocol entities to be supported in the involved nodes. This does not mean that those entities are always simultaneously in use):

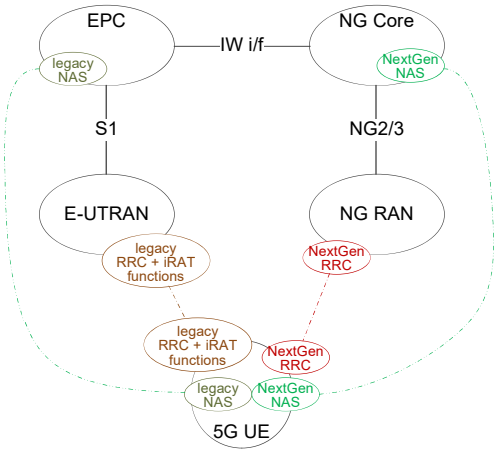


Figure 6.18.5.1-2: Main protocol entities in Core, RAN and UE for 5G UEs.

- The NG Core and UE will support the new NAS including e.g. the expected new Session Management/QoS concept. For mobility, and interworking a mapping would need to be performed between the EPS based concept and the NG concept.
  Such aNAS would be applied, regardless whether the UE consumes radio resources from evolved LTE or NR.
- It is also assumed that RRC will be impacted - as similar as it might be designed compared to LTE - at least to cater for the assumed new flow-based concept, so a UE capable of transiting between NG System and EPS

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 414 of 501

would need to "talk" LTE RRC and NG RRC. Interworking details between LTE RRC and NG RRC are regarded to be up to discussions in RAN2.

- The new access interface from NG Core to NG RAN would need to support connected mobility via the Core, i.e. preparation and execution of handover involves CN entities, similar to what is called "S1 Handover" in EPS.

6.18.6 Solution 18.6: Migration solution with Evolved E-UTRAN to operate EPC and NextGen Core simultaneously

This solution addresses Key Issue #18 with the following migration scenarios

- An operator deploys Evolved E-UTRAN partially, that is, the E-UTRAN has not been fully upgraded, so there are Non-evolved E-UTRAN and Evolved E-UTRAN together in the network. In the first phase, only option 3 of Annex J may be operated, then whole NextGen system may be operated in any time.

This solution applies to the following example scenarios

- In the first phase, the operator may configure Evolved E-UTRAN directs the smartphone type of NGC UE to EPC for emergency call or voice call, while Evolved E-UTRAN directs the tablet type of NGC UE to NGC for only data service.

- In EPS fallback case for emergency call or voice call after initially attaching to NGC via Evolved E-UTRAN, the operator may configure the Evolved E-UTRAN can direct the NGC UE to EPC.

Editor's note: The justification on above use cases are FFS.

6.18.6.1 Architecture description

Figure 6.18.6.1-1 shows a simplified system architecture for this migration scenario.

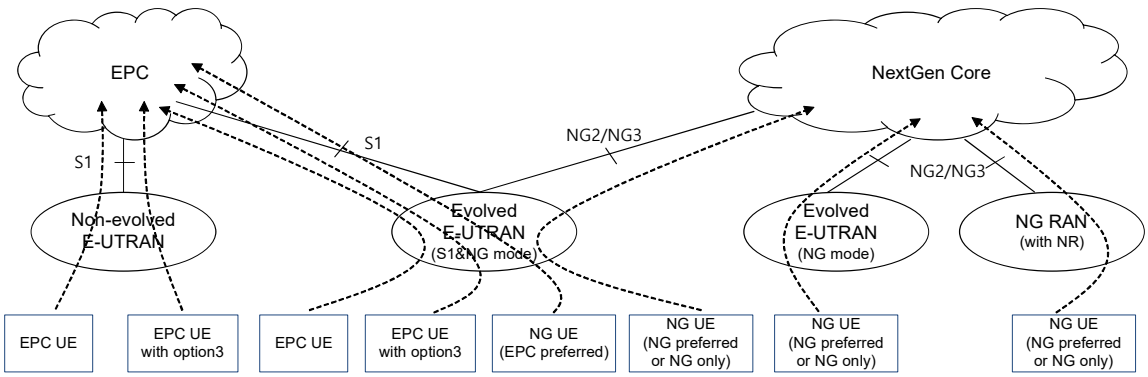


Figure 6.18.6.1-1: Architecture for migration scenario

This solution assumes the followings;

- The EPC and the NextGen Core have access to a common subscriber database (e.g. HSS), like solution 18.2, 18.3 and 18.4.

- Non-evolved E-UTRAN supports only EPC, and it directs a UE to EPC as a default.

- NG RAN with only new radio supports only NextGen Core, and it directs a UE to NextGen Core as a default.

- Evolved E-UTRAN supports either EPC or NextGen Core, or both, and it can direct a UE to either EPC or NextGen Core according to the mode configuration.

- Evolved E-UTRAN is operated with one of the following modes, and the mode configuration is informed of the UEs (e.g. via SIB)

  1) S1 mode (supporting access to only EPC, it may be similar to non-evolved E-UTRAN operation)

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 415 of 501

2) NG mode (supporting access to only NextGen Core, it performs only NG RAN operation)

3) S1&NG mode (supporting access to both EPC and NextGen Core)

"S1 mode" Evolved E-UTRAN may not need to broadcast the mode information, and the flexibility of the Evolved E-UTRAN mode depends on the operator's policy, the local configuration, etc.

Editor's note: The feasibility of this assumption should be determined in RAN WG.

- The EPC UE always connects to EPC using EPC NAS.
- The NG UE connects to EPC or NextGen Core using EPC NAS or NG NAS according to its capability, RAN mode operation and the following UE mode operation (i.e. UE preference by pre-configuration or network provisioning);

1) EPC preferred

An operator may configure it for some UEs in the environment which the NextGen system has not been fully deployed, or for the management reason at any time.

A UE configured as "EPC preferred" tries to connect to EPC using legacy NAS first, and if it is failed or under "NG mode" Evolved E-UTRAN, it can try to connect to NextGen core.

Editor's note: It is FFS whether the UE with option 3 is considered as a NG UE configured "EPC preferred".

2) NG preferred

An operator may configure it for some UEs according to their migration strategy or operator policy.

A UE configured as "NG preferred" tries to connect to NextGen Core first, and if it is failed, it can try to connect to EPC.

3) NG Only

An operator may configure it for dongle-type UE supporting Evolve E-UTRA and/or NR.

A UE configured as "NG preferred" always tries to connect to NextGen Core.

- Evolved E-UTRAN determines which core network (i.e. EPC or NextGen Core) a UE should be directed to, when receiving the signal or data from a UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 416 of 501

6.18.6.2 Function description

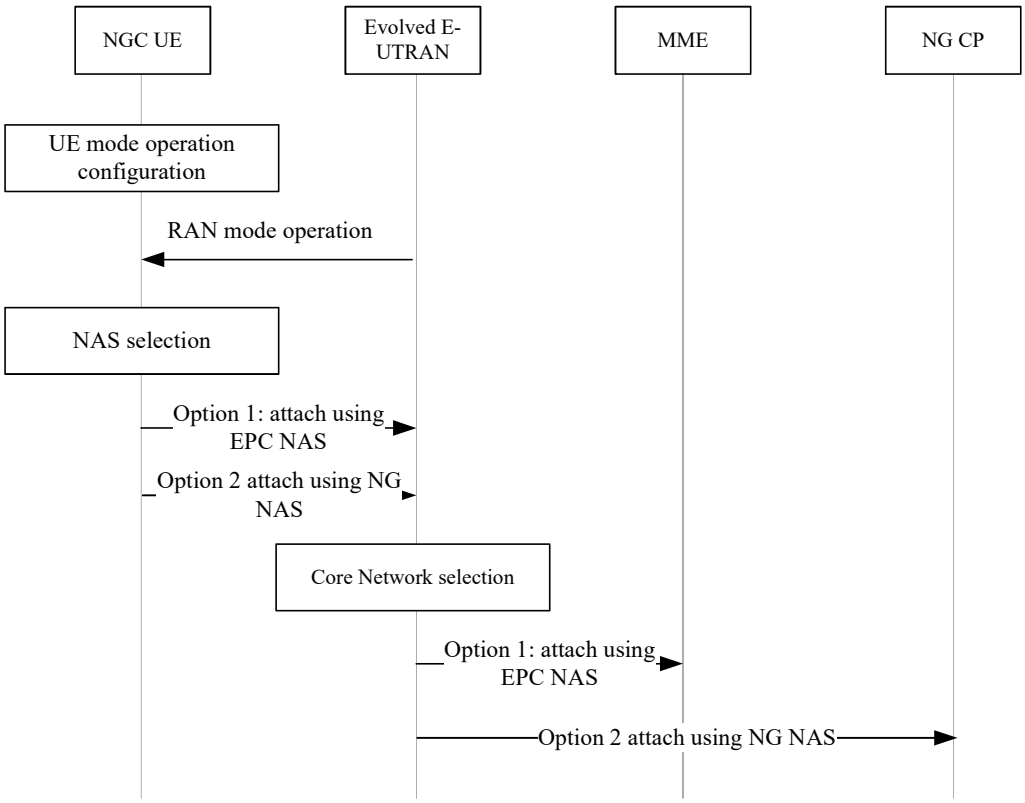


Figure 6.18.6.2-1: Initial access for NGC UE over Evolved E-UTRAN

- Evolved E-UTRAN informs the RAN mode operation (i.e. supporting access to NG Core or not) of the UEs (e.g. via SIB).
- The NGC UE determines to use EPC NAS or NG NAS, based on RAN mode operation (i.e. indicated by Evolved E-UTRAN) and UE mode operation (i.e. UE preference by pre-configuration or network provisioning).
- If the NGC UE selects to use NG NAS, the NGC UE provides an indication in RRC when it performs initial access
- Evolved E-UTRAN determines which core network (i.e. EPC or NextGen Core) a UE should be directed to.
- If the access to core network is failed, the NGC UE decides if it tries to connect to different core network or not, based on UE mode operation configured.

6.18.6.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.19 Solutions for key issue 19: Architecture impacts when using virtual environments

6.19.1 Solution 19.1: Avoiding UE interaction from NF Load Balancing, Scaling and Migration

When allocating UE related identifiers (c.f. the control plane and user plane "IP address and TEID" IEs in EPS's GTP-C protocol) for communication between NGCN Network Functions (and for communication between NGCN Network

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 417 of 501

Functions and NG RAN), an appropriately structured "NF name" should be used instead of (or in addition to) the current IP address of that Network Function.

Editor's note: It is FFS whether the above only applies to the control plane entities.

Changes in the IP address of the remote NF should then be able to be handled without releasing the UE's PDU session(s) and/or requiring reallocation of the UE's temporary ID (c.f. EPS' GUTI).

NOTE: the current "MME name" in S1-AP (TS 36.413 [21]) was not designed for this purpose.

6.20 Solutions for Key Issue 20: 3GPP architecture impacts to support access traffic steering and switching

6.20.1 Solution 20.1: Access traffic steering and switching

This solution applies to Key Issue 20 - 3GPP architecture impacts to support access traffic steering, switching and splitting. This solution addresses only the traffic steering and switching aspects.

6.20.1.1 Architecture description

The solution is based on the architecture described in Figures 6.20.1.1-1 and 6.20.1.1-2. Only new interfaces with respect to the NG interfaces already identified in other solutions are considered.

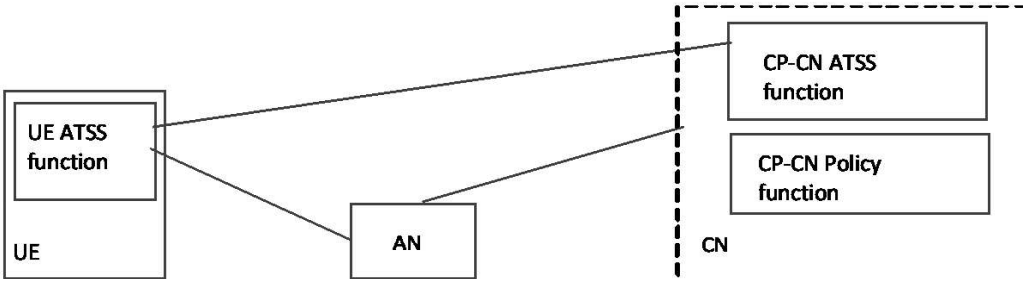


Figure 6.20.1.1-1: Non-roaming architecture for access traffic steering and switching

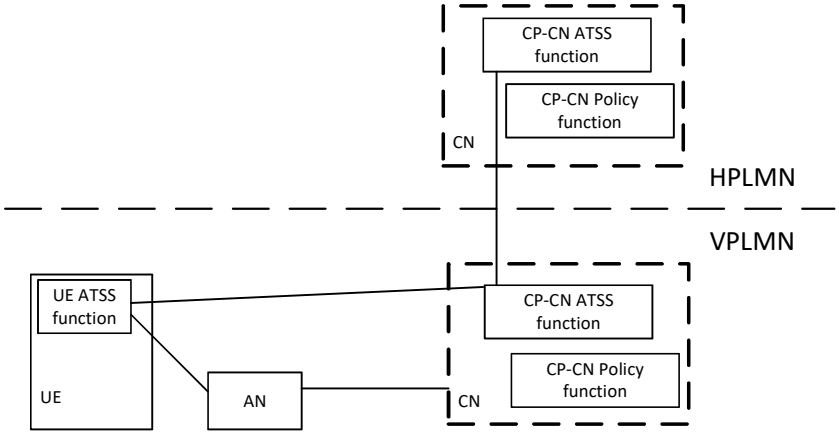


Figure 6.20.1.1-2: Roaming architecture for access traffic steering and switching

The functional entities in the architecture are defined as follows:

- CP-CN ATSS: the Control Plane CN Access Traffic Steering & Switching function is in charge of:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 418 of 501

1) conveying to the UE the policy controlling the access traffic steering and switching decisions at the UE;

2) deciding to which access to steer a new DL data flow;

Editor's note: How the CP-CN ATSS function is informed of the accesses currently available to the UE is FFS and will need to be addressed in relation with SM_WT_#5 (UE connected via multiple accesses) and MM_WT_#2 (reachability management).

3) deciding whether to switch an ongoing data flow to another access.

- UE ATSS: the Access Traffic Steering & Switching function at the UE is in charge of:

1) deciding to which access to steer a new UE-initiated data flow, based on the policy provisioned to the UE;

2) deciding whether to switch an ongoing data flow to another access, based on the policy provisioned to the UE.

- CP-CN Policy: the Control Plane CN Policy function implements CN policing and control.

Editor's note: Whether the UE is singled-attached or dual-attached (e.g. attached to both NGCN and EPS) for 3GPP accesses is FFS and will need to be addressed in relation with key issue 18 (Interworking and Migration).

The solution is based on the following model:

- the CP-CN ATSS function conveys the information necessary for access traffic steering and switching to the UE.

Editor's note: How the CP-CN ATSS function conveys the information to the UE is FFS. It could include e.g OMA-DM, pre-provisioning in the USIM or UE-implementation specific means, dedicated NAS signalling or RRC signalling.

This information may include e.g.:

1) For traffic steering:

a) A prioritized list of preferred accesses for a given service;

b) A prioritized list of services, to handle potential interruption to ongoing data flows;

c) Signal strength thresholds (optionally per service) for a given access (e.g. do not use WLAN for voice when the WLAN signal strength is below threshold X);

d) UE context-related thresholds (optionally per service) for a given access (e.g. do not use WLAN if the UE's speed is above 10 mph).

2) For traffic switching:

a) The permission to autonomously switch a data flow (optionally per service);

b) A prioritized list of preferred accesses for a given service;

c) A prioritized list of services, to handle potential interruption to ongoing data flows;

d) Signal strength thresholds (optionally per service) for a given access (e.g. do not use WLAN for voice when the WLAN signal strength is below threshold X);

e) UE context-related thresholds (optionally per service) for a given access (e.g. do not use WLAN if the UE's speed is above 10 mph).

- When initiating a new data flow, the UE ATSS function selects the access to be used based on the above-listed information;

- While the UE has active PDU sessions, the UE ATSS function periodically assesses whether an ongoing data flow needs to be switched to a different access based on the above-listed information;

- When a new DL data flow directed towards the UE is initiated, the CP-CN ATSS function select the access to be used based on the following criteria:

1) The type of service that the new data flow being initiated corresponds;

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 419 of 501

2) The UE's subscription info;

3) The potential impact to existing ongoing data flows;

4) The UE's context (e.g. speed, location);

5) The radio conditions for each access;

6) The network load for each access

- While the UE has active PDU sessions, the CP-CN ATSS function periodically assesses whether an ongoing data flow needs to be switched to a different access based on the following criteria:

  1) The type of service that the data flow considered as candidate for switching corresponds to;

  2) Potential service interruption resulting from switching;

  3) The UE's subscription info;

  4) The potential impact to existing ongoing data flows;

  5) The UE's context (e.g. speed, location);

  6) The radio conditions for each access;

  7) The network load for each access;

  8) The type of service that the new data flow being initiated corresponds to.

- The CP-CN ATSS makes steering decisions by interacting with the CP-CN Policy function.

The proposed functionality applies also for flow mobility cases (e.g. flows of a PDU session being routed over different accesses, such as in the case of NBIFOM).

Editor's note: the applicability of a mechanism similar to pre Rel. 14 RAN rules is FFS.

Editor's note: whether the solution should consider single radio UEs is FFS.

6.20.1.2 Function description

Editor's note: the following procedures apply to steering from a 3GPP access to another access.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 420 of 501

6.20.1.2.1 Steering of a new data flow by the UE

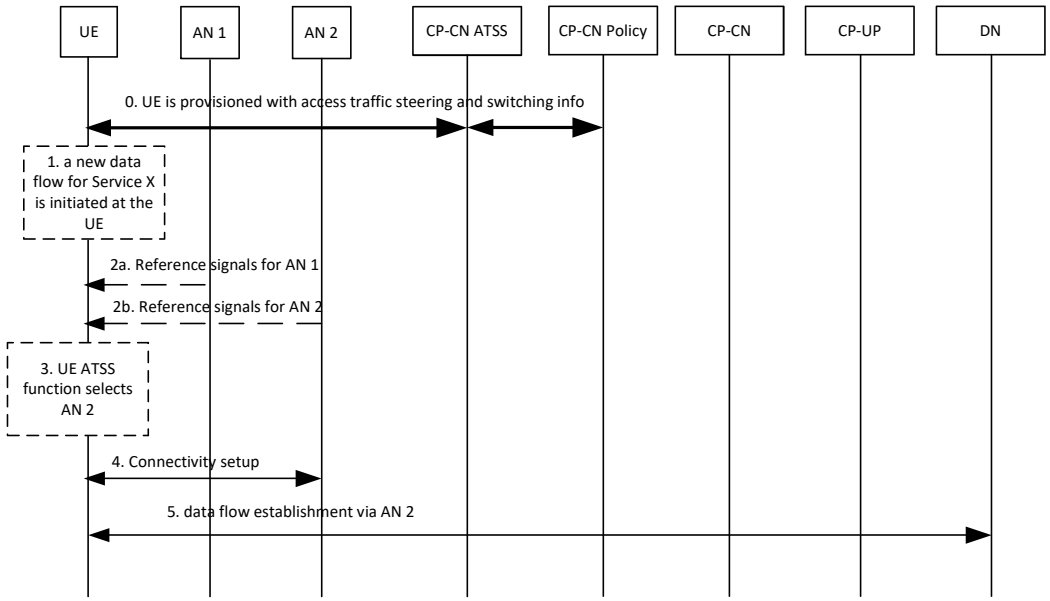


Figure 6.20.1.2.1-1: Steering of a new data flow by the UE

0. The UE is provisioned with access steering and switching info by the CP-CN ATSS function (which may obtain them from the CN-CP Policy function).

Editor's note: How the CP-CN ATSS function conveys the information to the UE is FFS. It could include e.g OMA-DM, pre-provisioning in the USIM or UE-implementation specific means, dedicated NAS signalling or RRC signalling.

1. A new data flow for Service X is initiated at the UE.

2a. Optionally, the UE receives reference signals to perform signal strength measurements for access #1 via AN 1.

2b. Optionally, the UE receives reference signals to perform signal strength measurements for access #2 via AN 2.

3. Based on the access steering and switching info provisioned to the UE, and current conditions including e.g radio conditions for each access, the UE's context, etc, the UE ATSS function selects access #2.

4. The UE establishes connectivity with AN 2.

5. The UE establishes the new data flow for Service X via AN 2.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 421 of 501

6.20.1.2.2 Steering of a DL data flow by the network for a dual radio-capable UE

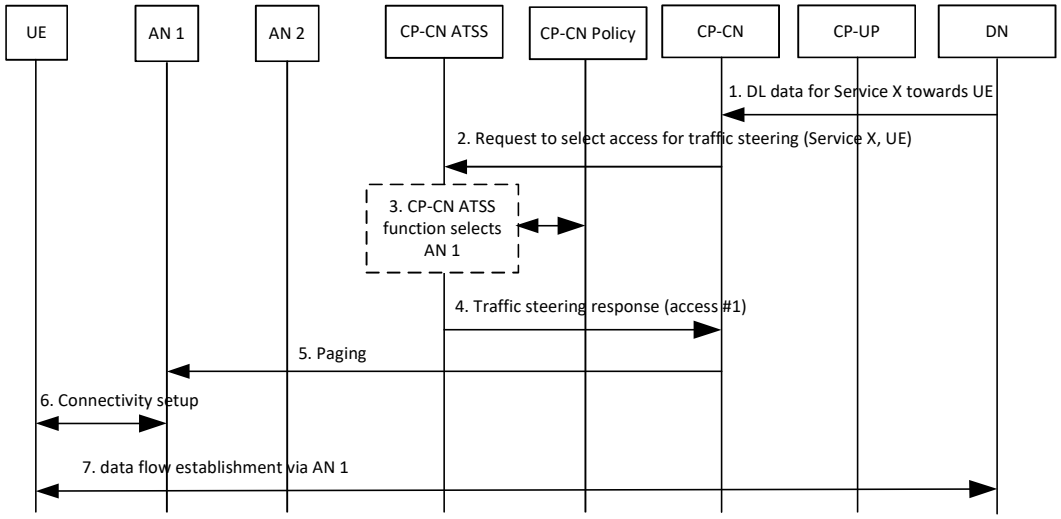


Figure 6.20.1.2.2-1: Steering of a DL data flow by the network for a dual radio-capable UE

1. The CP-CN function gets a request for a new data flow establishment for Service X towards the UE (e.g. there is incoming mission-critical video data to be delivered to the UE).
2. The CP-CN function requests the CP-CN ATSS function to select an access to steer the traffic for this DL data.

Editor's note: How the CP-CN ATSS function is informed of the accesses currently available to the UE is FFS and will need to be addressed in relation with SM_WT_#5 (UE connected via multiple accesses) and MM_WT_#2 (reachability management).

3. Based on the criteria listed in subclause 6.20.1.1 and the policies in the CN-CP Policy function, the CP-CN ATSS function selects access #1 via AN 1.
4. The CP-CN ATSS functions sends a response to the CP-CN function indicating access #1 is selected for the DL data.
5. In case of a 3GPP access, the CP-CN function sends a paging message to AN 1. For non-3GPP accesses, step 5 is skipped
6. AN1 may (re)-establish connectivity with the UE (e.g. in case of a 3GPP access, it establishes the radio link).
7. The new data flow for Service X is established via AN 1.

6.20.1.2.3 Switching of an ongoing data flow by the UE

For dual-radio UEs, it is assumed that the UE is attached to only one core network at a time (in case of flow switching between an access connected to the NG Core and an access connected to the EPC). For flow switching for the UE to a second access network, the UE may need to re-authenticate to establish connectivity with the second access network, depending on solutions for other key issues including authentication and security, mobility management, and session management.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 422 of 501

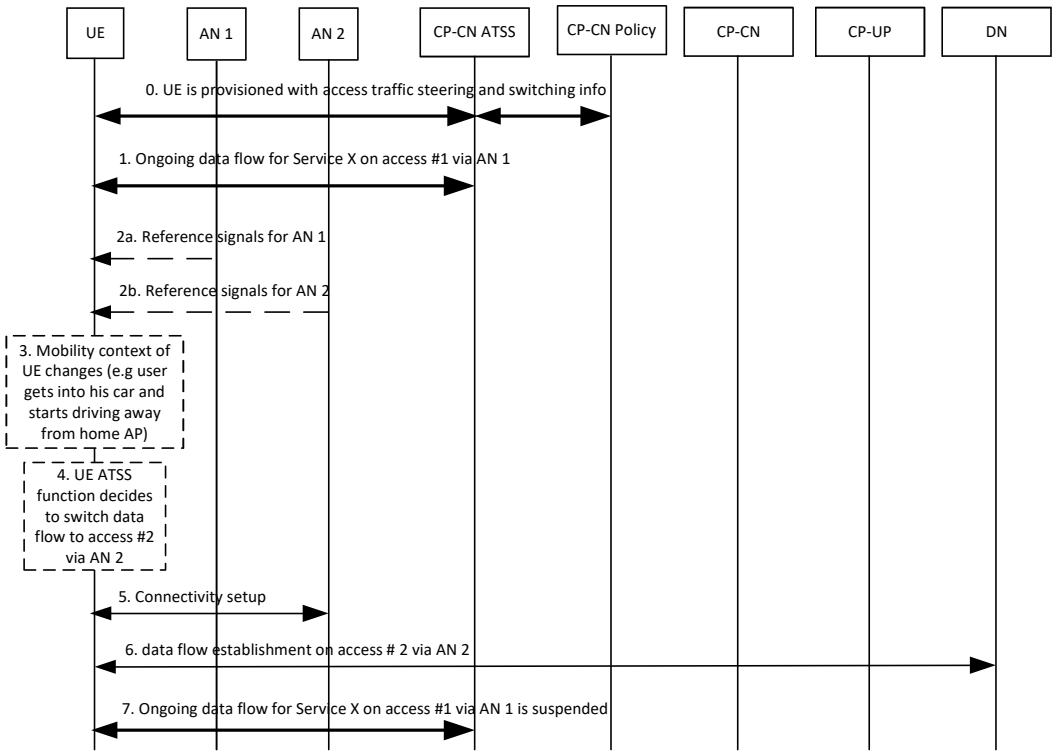


Figure 6.20.1.2.4-1: Switching of an ongoing data flow by the UE

0. The UE is provisioned with access steering and switching info by the CP-CN ATSS function (which may obtain them from the CN-CP Policy function). This can be done via e.g OMA-DM, provisioning on the USIM or via UE implementation-specific means.

Editor's note: How the CP-CN ATSS function conveys the information to the UE is FFS. It could include e.g dedicated provisioning mechanisms, OTT mechanisms, pre-provisioning in the USIM or UE-implementation specific means, dedicated NAS signalling or RRC signalling.

1. The UE has an ongoing data flow for Service X on access #1 via AN 1 (for simplicity, steps for access steering of this data flow when it is initiated, and steps for establishment of the data flow, are not shown).

2a. Optionally, the UE receives reference signals to perform signal strength measurements for access #1 via AN 1.

2b. Optionally, the UE receives reference signals to perform signal strength measurements for access #2 via AN 2.

3. The mobility context of the UE changes (e.g. the user gets into his car and starts driving away from the home AP).

4. Based on the access traffic and steering information provisioned to the UE and current conditions including e.g radio conditions for each access, the UE's context, etc, the UE ATSS function decides to switch the ongoing data flow to access #2.

5. The UE establishes connectivity with AN 2 (e.g. establish a radio link in case of 3GPP access or WLAN).

6. The UE establishes a data flow over access #2 via AN 2.

7. The UE suspends the ongoing data flow on access #2 via AN 1

NOTE: Depending on the UE's radio capabilities and the network configuration, Step 7 might happen before Steps 5&6, in parallel with Steps 5&6 or after Steps 5 & 6.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 423 of 501

6.20.1.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

6.20.2 Solution 20.2: Solution based on ATSSS Function

This solution addressed key issue 20 on Access Traffic Steering, Switching and Splitting (ATSSS).

The solution enables

a) the UE to perform access traffic *steering*, i.e. to perform access selection (3GPP access or WLAN access) when it initiates a new data flow;

b) the network to initiate access traffic *switching*, i.e. to switch a data flow from 3GPP access to WLAN access or vice versa; and

c) the network to initiate access traffic *splitting*, i.e. to split a data flow over both 3GPP access and WLAN access (for bandwidth aggregation).

To enable the above capabilities, the following rules are defined:

1) Access traffic *steering* rules: These rules are provided to UE by the network and are used by the UE for access selection when initiating a new data flow. As an example, an access traffic steering rule may indicate "select 3GPP access for app-x" or "select WLAN access for non-IMS traffic between 9am and 5pm".

2) Access traffic *switching* rules: These rules are configured in the policy function in the NextGen CN and are used to determine when one or more data flows should be moved from 3GPP to WLAN or vice versa. As an example, an access traffic switching rule may indicate "move video streaming flows to WLAN when the 3GPP access gets congested" or "move video streaming flows to WLAN when their duration exceeds 20s" or "move data flows to WLAN when the data balance of subscriber exceeds 80%".

3) Access traffic *splitting* rules: These rules are configured in the policy function in the NextGen CN and are used to determine when one or more data flows should be split across 3GPP and WLAN accesses. The split of flows can facilitate bandwidth aggregation. As an example, an access traffic splitting rule may indicate "split HD video streaming flows for 'gold' users when their duration exceeds 10s".

6.20.2.1 Architecture Description

The architecture diagram is shown in Figure 6.20.2.1-1 for the case of trusted WLAN.

Editor's note: The intention of this solution is to apply (a) for trusted WLANs and un-trusted WLANs and also (b) for both seamless and non-seamless WLAN offload (as defined in TS 23.402 [17]). However, the solution currently concentrates on trusted WLANs. How it can be applied to un-trusted WLANs with seamless or non-seamless offload is FFS and will be covered in future updates.

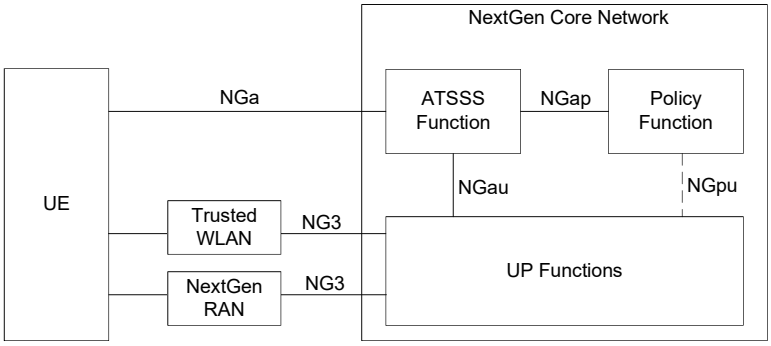


Figure 6.20.2.1-1: Architecture diagram

NOTE 1: The architecture diagram does not display some CP interfaces (e.g. NG2, NG4) because such interfaces are not used by this solution.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 424 of 501

Elements of the architecture:

- ATSSS Function:This is the main functional element of the solution. The ATSSS Function is user plane function. All traffic that can be switched or split is anchored in the ATSSS Function as specified below (it operates as a kind of transparent proxy). The ATSSS Function receives switching & splitting rules from the policy function and applies these rules to determine when traffic should be switched or split between 3GPP and WLAN access. In addition, the ATSSS Function may receive steering rules from the policy function and may send these rules to UEs. The ATSSS Function maintains a control connection with the UE (via NGa interface) over which it can send to UE switch/split commands and steering rules.

- Policy Function: The details of the policy function are expected to be specified as part of the Policy Framework. This solution only assumes that there is a policy function in the NextGen CN which can provide to ATSSS Function rules for access traffic steering, switching and splitting. In addition, the policy function may need to provide to UP functions steering rules for steering certain flows to the ATSSS Function. The policy function may interface with additional functional elements not shown in Figure 6.20.2.1-1.

- UE: The UE establishes a control connection with the ATSSS Function over the NGa interface. Via this connection, it may receive steering rules which are applied for access selection (selecting between 3GPP and WLAN) when initiating a new data flow. Also, the UE may receive switching and/or splitting commands from the ATSSS Function when the network decides to switch or split one or more of the UE's data flows.

- NGa: An interface used by the UE to establishes a "control" connection with the ATSSS Function. This control connection is realized over TCP, i.e. over the NextGen user plane. Via the NGa interface the ATSSS Function may send steering rules to UE and commands for switching or splitting certain data flows.

- NG3: The regular UP interface between the NextGen RAN and the UP functions in the NextGen CN. It is assumed that an NG3 interface exists also between a trusted WLAN and the UP functions in the NextGen CN.

- NGau: Via the NGau interface the UP functions can forward certain data flows to the ATSSS Function in order for these flows to be later switched or split between 3GPP and WLAN access. This interface carries UP traffic only.

- NGpu: Via the NGpu interface the policy function sends to UP functions steering policy which is applied to steer selected data flows (both in the uplink and downlink direction) to the ATSSS Function via NGau. These data flows can then be switched or split between 3GPP and WLAN accesses based on the switching & splitting rules. This interface is not required when the ATSSS Function is configured in the UE as a proxy (this is further discussed below).The details of this interface are FFS (and should possibly be considered as part of the Policy Framework).

Editor's note: It is FFS if the NGpu interface is a direct interface between the policy function and the UP functions or if it goes through the session management function.

- NGap: Via the NGap interface the policy function can send steering rules to the ATSSS Function, which may then be sent to UE via NGa. Also the policy function may send switching & splitting rules to the ATSSS Function which can be used to determine when certain flows should be switched or split between 3GPP and WLAN accesses.

6.20.2.2 Functional Description

6.20.2.2.1 Operation Overview

The high-level operation of the solution is illustrated in Figure 6.20.2.2.1-1. More details are provided in subsequent clauses (see e.g. the clause on signalling flows).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 425 of 501

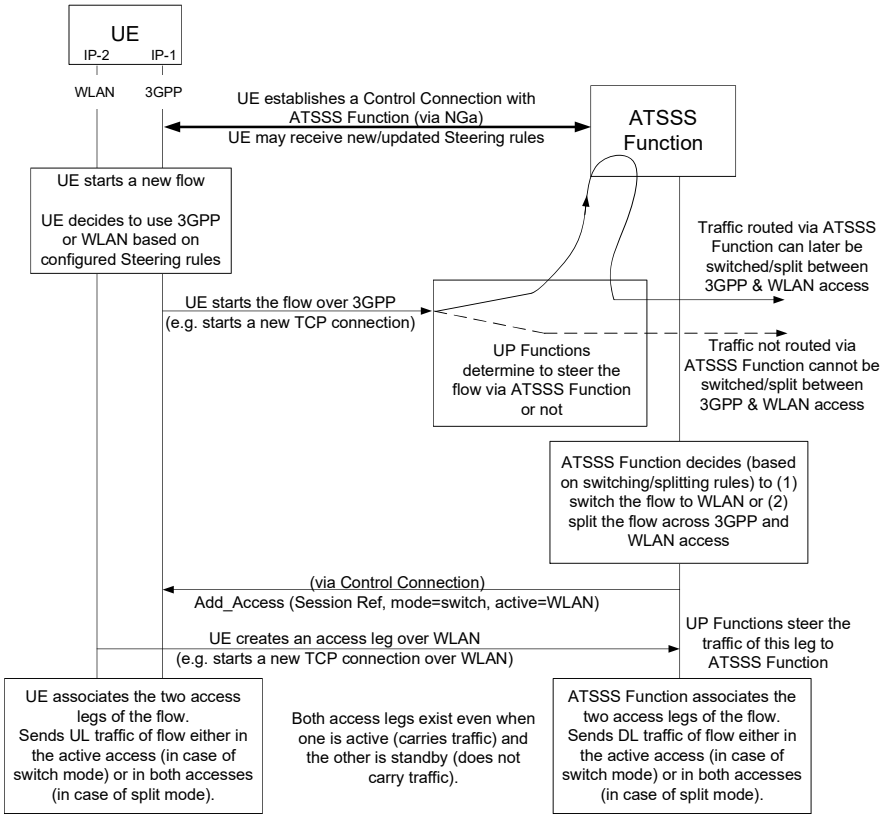


Figure 6.20.2.2.1-1: High-level concept of operation

The ATSSS Function may expose a private IP address (accessible via the NextGen CN only), a public IP address (accessible via the public Internet), or both. A public IP address would facilitate connections to ATSSS Function via un-trusted WLANs but the details of this scenario are currently FFS.

After the UE establishes the control (TCP) connection with the ATSSS Function, the UE and the ATSSS Function are mutually authenticated (e.g. similarly to how the UE and the ANDSF in EPC are mutually authenticated). Via this connection the UE may receive new/updated steering rules. Also, the UE informs the ATSSS Function of its IP address over 3GPP access and of its IP address over WLAN access. These addresses are used by the ATSSS Function (a) to determine if the UE has connectivity to both accesses and (b) to determine (by looking at the IP source address) which UE is associated with a data flow and which access is being used for this data flow.

The ATSSS Function operates as a *transparent* TCP/UDP proxy (i.e. the UE does not know if its traffic goes through the ATSSS Function). Traffic initiated by the UE can be steered to the ATSSS Function via the steering rules provided to UP functions by the policy function (via NGpu).

Editor's note: Alternatively, the ATSSS Function may be configured in the UE (via NGa) e.g. as a SOCKS proxy. In this case, the UE sends some/all data flows to the IP address of ATSSS Function and therefore the UP functions need not be configured with steering rules by the policy function (so the NGpu interface is not required). It is FFS if this alternative is preferable over the transparent proxy case.

Note in Figure 6.20.2.2-1 that all data flows which may be switched or split between 3GPP and WLAN are anchored at the ATSSS Function. When the ATSSS Function decides to switch or split a data flow it sends a command to UE (via NGa) to establish a new access leg for this flow (see the *Add_Access* message) and to either switch all flow traffic to this access leg (mode=switch) or to split the flow traffic across the two access legs (mode=split).

In case of a TCP flow, a new access leg is established by creating a new TCP connection over the new access. The new and the old TCP connections over 3GPP and WLAN accesses respectively are associated with each. The operation of the two associated TCP connections is based on the Multipath TCP (MPTCP) protocol specified in RFC6824 as further explained below.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 426 of 501

In case of a UDP flow, a new access leg is established by creating a new UDP association (being defined by a new 5-tuple) between the UE and the ATSSS Function over the new access.

Editor's note: How UDP flows can be switched and split are currently FFS.

Editor's note: The solution can support traffic steering for IP and non-IP data flows (by provisioning the appropriate steering rules in the UE). However, traffic switching and splitting is currently considered only for TCP and UDP flows. It is FFS if traffic switching and/or splitting is required for non-TCP and non-UDP data flows.

6.20.2.2.2 Protocol Architecture

Figure 6.20.2.2.2-1 below shows the protocols running in the UE and in the ATSSS Function as well as how these protocols can realize multiple access legs (over 3GPP and WLAN accesses) for a single data flow.

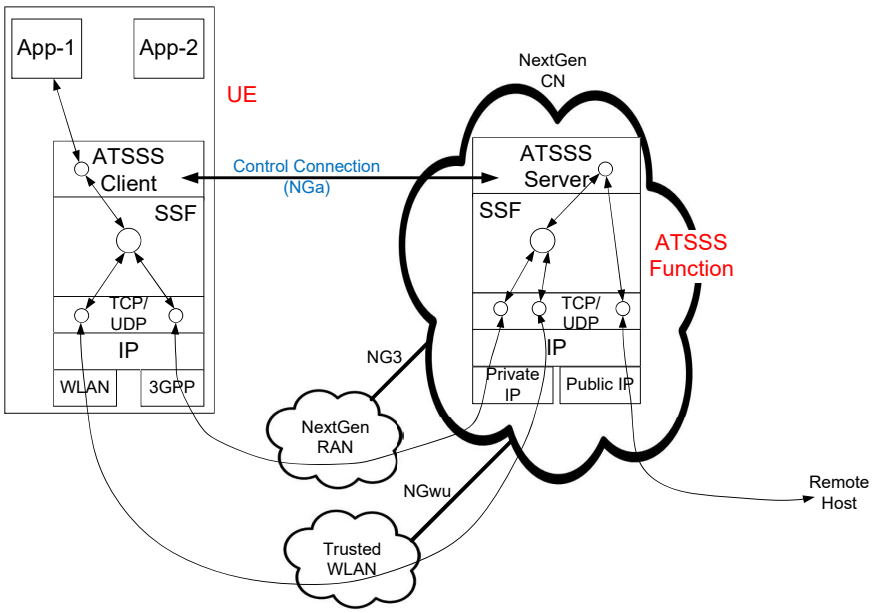


Figure 6.20.2.2.2-1: Protocol Architecture

- ATSSS client/server: The ATSSS client in the UE and the ATSSS server in the ATSSS Function are the two endpoints for the control connection over NGa. The ATSSS client in the UE receives switching and splitting commands from the ATSSS server and configures the SSF in the UE to operate according to these commands (e.g. to initiate an new access leg for a data flow, to split the traffic of a data flow across two access legs, etc.).

- Switching/Splitting Function (SSF): The SSF protocol operates on top of TCP/UDP and is responsible for creating one or more access legs for a data flow and then scheduling the traffic of the flow across these access legs. The scheduling behaviour of SSF is configured by the layer above SSF (i.e. by the ATSSS client in the UE and the ATSSS server in the ATSSS Function). The SSF may send all traffic of the flow onto one access leg (when configured in switch mode) or may send all traffic of the flow onto two access legs (when configured in split mode).

For TCP flows the SSF operation is based on the Multipath TCP (MPTCP) protocol as specified in RFC6824. The ATSSS client in the UE and the ATSSS Server in the network maintain an API with their SSF via which they can control the MPCTP behaviour of SSF. Details of this API are provided in RFC6897. It is noted however that since the UE and the ATSSS Function maintain a control connection (via NGa) some aspects of MPTCP may be optimized. For example:

1. When the UE sends its IP addresses to ATSSS Function via the control connection, the UE can indicate which IP address is used for WLAN access and which IP address is used for 3GPP access. This way, when the ATSSS Function receives a new data flow, it knows (by looking at the IP source address) if it is carried over WLAN or 3GPP access. Such capability is not supported by the address advertisement mechanism of MPTCP.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 427 of 501

2. When the ATSSS Function receives a new data flow it can identify the UE that originated this data flow (again by looking at the IP source address). This way the ATSSS Function can enforce UE-specific switching and splitting policies, e.g. policies based on subscription information, policies based on the UE type, etc.

3. The UE does not need to advertise its addresses (via the MPTCP ADD_ADDR option; see RFC6824) every time it starts a new TCP connection. In fact, address addition or removal is implemented "out-of-band" (via NGa) and applies to all ongoing TCP connections of the UE.

Editor's note: Further details are needed here to clarify how the "out-of-band" signalling (via NGa) between the UE and ATSSS Function can optimize the MPTCP operation. Such optimizations need to be compliant with the MPTCP protocol so that no MPCTP changes are needed.

The SSF can operate in two modes as shown in Figure 6.20.2.2.2-2. In split mode, all data flow traffic is transmitted on both access legs. In switch mode, all data flow traffic is transmitted on the 'active' access leg, the other leg being in standby. The ATSSS Function can change the 'active' access leg whenever the data flow traffic needs to be moved to a different access.

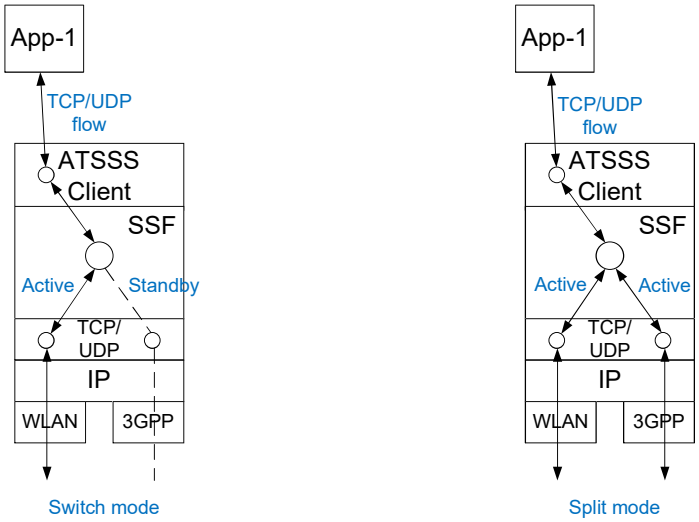


Figure 6.20.2.2.2-2: Modes of SSF operation (UE side)

Editor's note: For UDP flows the operation of SSF is FFS. Switching a UDP flow between 3GPP and WLAN accesses should be straightforward. However, splitting a UDP flow on both 3GPP and WLAN accesses may be more challenging since UDP does not provide link-quality metrics to be used for scheduling.

6.20.2.2.3 Signalling Flows

Figure 6.20.2.2.3-1 illustrates how a TCP flow can be *switched* between 3GPP and WLAN access.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 428 of 501

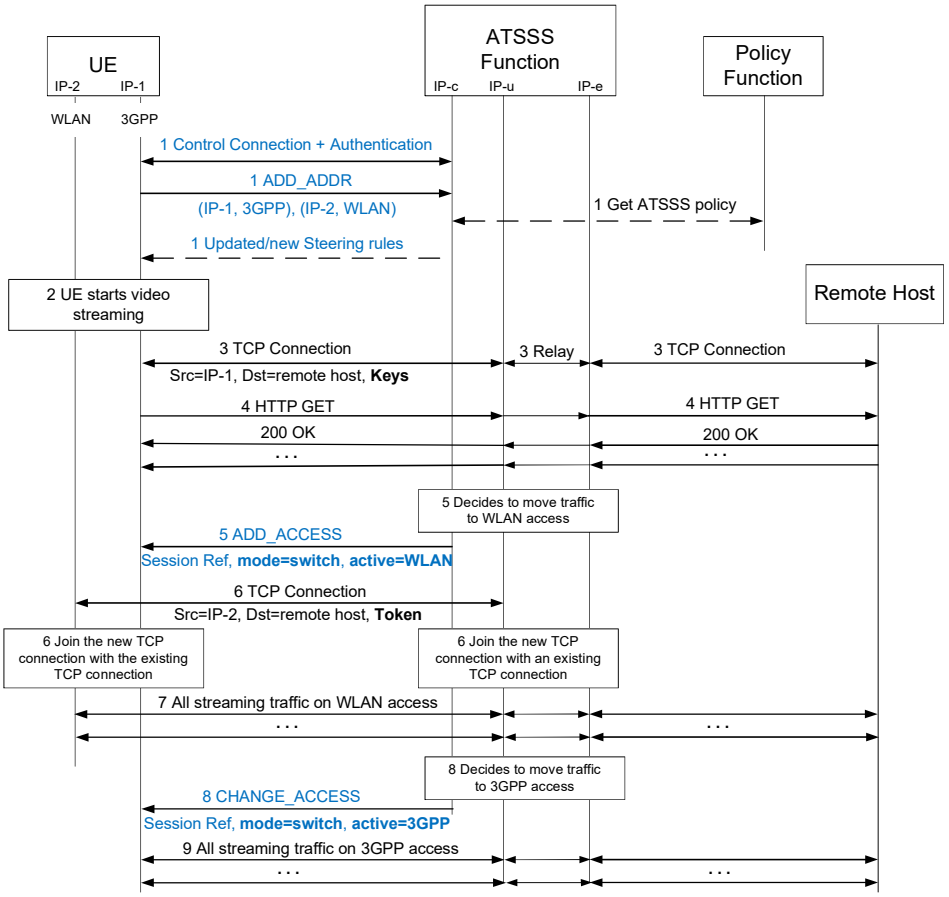


Figure 6.20.2.2.3-1: Switching the traffic of a TCP flow between 3GPP & WLAN access

1. The UE establishes a control connection with the ATSSS Function. The IP address of ATSSS Function (IP-c) can either be pre-configured or discovered by the UE (e.g. via DNS lookups). After a mutual authentication the UE sends to ATSSS Function its IP address over WLAN and its IP address over 3GPP access. This way the ATSSS Function is informed that the UE is connected to both accesses and it can later identify when the UE initiates a new data flow over WLAN or over 3GPP access (by looking at the IP source address). The ATSSS Function may send new Steering rules to UE which are used for access selection every time the UE initiates a new data flow.

2. The UE starts a TCP-based video streaming flow toward a remote host in the Internet. Based on the configured Steering rules the UE starts the flow over 3GPP access.

3. The UE initiates a TCP connection to the remote host. This TCP connection is steered by the UP functions in NextGen CN to the ATSSS Function, which terminates the TCP connection and initiates a second TCP connection to the remote host (via its IP-e address which is accessible from the Internet). By looking at the IP source address, the ATSSS Function identifies the UE that originated this flow and the access being used. The TCP connection between the UE and ATSSS Function is an MPTCP connection i.e. carries the MP_CAPABLE option and exchanges 64-bit keys between the UE and ATSSS Function. These keys are used for authenticating and associating future TCP connections with the existing TCP connection (see details in RFC6824).

4. TCP/HTTP traffic is exchanged between the UE and the remote server via the ATSSS Function which relays traffic between the internal and external TCP connections.

5. At some point, the ATSSS Function decides (e.g. based on the switching rules received from the policy function) to move the streaming flow to WLAN access. The ATSSS Function knows the UE is connected to WLAN because the UE (in step 1) has advertised an IP address for WLAN access (IP-2). Via the control connection, the ATSSS Function sends an ADD_ACCESS request to UE in order to establish an access leg over WLAN access. This message includes a session reference which references the existing TCP connection established in step 3. It

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 429 of 501

also indicates that the new access leg should be established over WLAN and that the two access legs should operate in switch mode with the WLAN leg being the active one.

NOTE 1: Apparently, the UE may reject the ADD_ACCESS request e.g. when the UE considers that the WLAN signal is currently too small.

NOTE 2: The ADD_ACCESS request may request the UE to establish an additional access leg for several existing data flows (not only for one). This way the ATSSS Function may request the UE to move several data flows to WLAN access at once.

6. The ATSSS client in the UE instructs the SSF in the UE to establish a new leg for the existing MPTCP connection. So, the UE initiates a new TCP connection which carries the MPTCP MP_JOIN option according to RFC6824. The Token in the MP_JOIN option is used for authenticating this new TCP connection and joining it with the existing TCP connection (see details in RFC6824).

7. The UE and the ATSSS Function forward all data flow traffic over the WLAN access.

8. Further later, the ATSSS Function decides to move the data flow traffic back to 3GPP access. Since the UE has already a 3GPP access leg (in standby mode), the ATSSS Function sends a CHANGE_ACCESS request to UE which changes the 3GPP access leg to active mode.

9. The UE and the ATSSS Function forward all data flow traffic over the 3GPP access.

Figure 6.20.2.2.3-2 illustrates how a TCP flow can be *split* on both 3GPP and WLAN accesses.

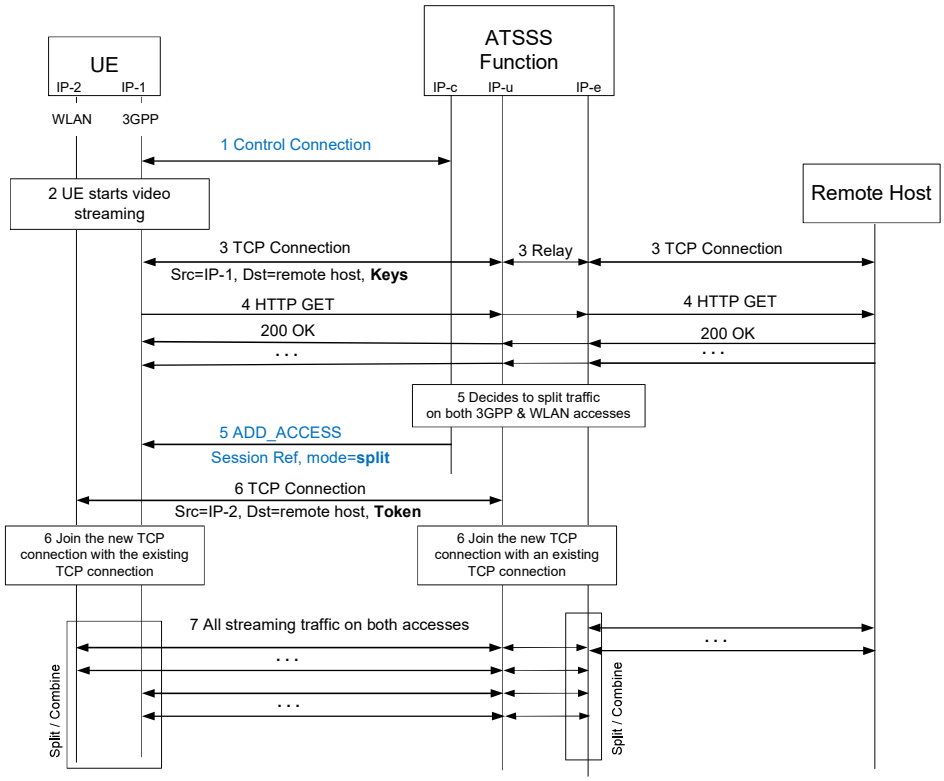


Figure 6.20.2.2.3-2: Splitting the traffic of a TCP flow on both 3GPP & WLAN accesses

All the steps are essentially the same as the steps in Figure 6.20.2.2.3-1 discussed before. The difference is in step 5 where the mode in now indicated as 'split'. As mentioned above, the ADD_ACCESS message may reference not only one existing TCP connection but multiple so it can request the UE to split multiple data flows on both accesses. The UE establishes a new TCP connection over WLAN access which carries the MPTCP MP_JOIN option and is thus joined with the existing TCP connection. This join occurs in the SSF in the UE and in the ATSSS Function (see the protocol architecture). As a result, the DL streaming traffic sent by the remote host is split by the ATSSS Function across 3GPP and WLAN accesses and the UE recombines the traffic by following the applicable MPTCP procedures.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 430 of 501

Editor's note: Several aspects of the solutions are still FFS. For example, the operation of UDP flows, the operation with un-trusted WLANs, the operation when the UE losses the WLAN signal, etc. need to be considered and specified.

6.20.2.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g., UE, access network and non-access network.

6.x Solution x - Title

Editor's note: It should be indicate here to which issue(s) the solution applies.

6.x.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

6.x.2 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

6.x.3 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

7 Architecture(s) for the Next Generation System

Editor's note: This clause will be consolidated and refined later during the study.

7.1 Consolidated architecture option 1

7.1.1 General

Only architectural aspects, either based on the progress of the key issues of this study or other critical aspects such as support for roaming, etc., are considered for the consolidated overall architecture of NG CN. The functional aspects, e.g. the exact set of functionality supported by each NF, and the interaction between NFs, e.g. the messages and the parameters between two NFs, are left to the conclusion of the individual key issues.

7.1.2 High level architectural principles

Following high level architectural principles are considered for the NG CN reference architecture:

- **Separation of control and user plane functions:** For allowing independent scaling of control and user plane functions their separation is critical. Principles of Rel-14 CUPS feature are followed, i.e. control plane dynamically configures user-plane functions (i.e. activates various operations of the user-plane functions as needed) to provide the traffic handling functionality needed for a session.
- **Standalone Subscriber DB:** Since Subscriber DB is mainly responsible for subscription profile management, it belongs to the database domain, while the other NFs in the CN mostly belong to the networking domain. For the independent evolution of Subscriber DB, which is linked to the evolution of the database domain, it should be separated from the other NFs in CN.
- **Separated MM and SM control functions:** For the following reasons MM and SM control functions are required to be separated into standalone NFs:
  - **Support for home-routed roaming architecture:** In the home-routed roaming architecture, the MM control function will be part of visiting PLMN while the SM control function will be within the home PLMN. .

NOTE 1: For home-routed roaming scenario, some subset of the SM functionality, e.g. selection and programming of the user plane function in the visiting PLMN for inter-operator charging, etc., will have to be supported in the visiting PLMN as well.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 431 of 501

- **Support for Gateway CN like network sharing configuration:** Under the Gateway CN network sharing configuration of EPC, the functionality supported by MM control function is hosted by the MNO while the functionality supported by the SM control function is hosted by the MVNO (e.g. enterprise customer). To support this basic network sharing configuration in NG, it is important to define standalone MM control function and SM control function.

NOTE 2: Roaming and network sharing are identified as priority architectural enablers for Rel-14 study in Annex C.

- **Support for UE simultaneously accessing multiple network slice:** In this case, the MM functionality should be part of common control function while the SM functionality should be part of slice specific control function.

NOTE 3: The interim agreement for network slicing key issue, clause 8.2, hints at MM as part of common control function when UE accesses multiple network slices simultaneously.

- **Separating the access related and PDU session functionality:** The PDU session management functions (the core functionality of SM control function) which include charging, UL/DL service level rate enforcement etc. are common for all types of accesses. These are very different compared to the access related functions (the core functionality of MM control function) which include registration management, reachability management, mobility restriction etc. Hence, their separation for, e.g. independent evolution, independent scaling purpose, and for distributed v/s centralized deployment, is vital.

- **Access common CN design:** By defining unified authentication framework, NAS protocol which is common to all the accesses and (R)AN-CN interface which is common to all the accesses, we define access common CN. This CN supports functionality specific to an access (e.g. CN idle mode reachability management) as well as common to all the accesses (e.g. PDU session establishment). Thus, NG1, NG2 and NG3 interfaces which are common to the 3GPP as well as non-3GPP accesses are used.

- **Single termination point for NG1 in CN, for a given access:** This also allows a single security association between the UE and the CN for a given access.

NOTE 4: The above also satisfies architecture principles, mentioned in clause 4.3, to minimize number of reference points between the UE and the NextGen CN for the control plane over a single (R)AN.

- **Standalone Authentication function:** For supporting unified authentication framework and for supporting UEs which may support only subset of 5G functionality (e.g. not supporting MM functionality), the Authentication function should be separate from the MM function. This is also needed to allow centralized deployment of Authentication function while distributed deployment of MM function. Authentication function is also kept separate from the Subscriber DB since both of them belong to different technology domain, i.e. networking v/s database.

NOTE 5: The above is based on the solution in clause 6.12.1 which defines "CP-AU Authentication Function" for the Authentication function. If it also includes "Session Context Management" function is FFS.

- **Standalone Application Function**: The Application Function could belong to 3rd party and hence part of different administrative domain compared to NG CN. Hence it should be defined as standalone NF.

- **Scalable, efficient and simplified interconnection model for CN control plane NFs**: Following aspects are considered for the interconnection of the CN control plane NFs:

  - **Extendable, scalable while maintaining efficient communication path between NFs**: The interconnection model needs to be able to allow easy insertion of new NFs in future while maintaining the efficient communication path between new and existing NFs, without increasing the overall complexity of the system. Hence, an interconnection model allowing communication between any CN control plane NFs is preferred over the traditional point-to-point interface based model.

  - **Reduced complexity of NFs and overall system while ensuring multi-vendor deployment**: The interfaces need to be open and standardized for allowing multi-vendor NG CN while there is no real need for defining multiple (e.g. one per each peer NF) interfaces and corresponding number of protocols. Thus, by defining one standardized interface over which the NF provides all its functionality, we reduce the overall complexity of the NFs, we reduce total number of interfaces in the system while ensuring the architecture that allows multi-vendor CN deployment.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 432 of 501

- **Cost-effective and agile for development and for deployment**: Reducing complexity of NF will allow cost-effective and faster development of new features. In turn, it would result in the overall system which is relatively agile for rolling out of new features and services.

- **Generic user-plane architecture:** Various user-plane scenarios (e.g. access to local and centralized data networks (in both the visited and the home network in roaming situations), data forwarding for session continuity and other purposes, etc.) need to be supported by the NG system. While the scenarios differ, the actual functionality required to support them can be reduced to a rather small set of basic user-plane operations. Therefore, a generic user-plane architecture supporting various operations (forwarding operations to other user-plane functions/ data networks/the control-plane, bitrate enforcement operations, service detection operations, etc.) is defined. One or multiple user-plane functions per session can be activated and configured by the control-plane as needed for a given user-plane scenario.

7.1.3 Reference architecture

7.1.3.1 Non-roaming

Editor's note: the Interfaces to IRF is expected include all the procedures, messages and IEs each function needs to interact with all possible peer functions directly, so it is FFS whether the IRF may at some point in time be bypassed or whether it is always involved in any interaction

Editor's note: it is FFS whether the access to IRF by application functions is allowed for third party applications

Editor's note: it is FFS whether the NG4 interface can also be via IRF.

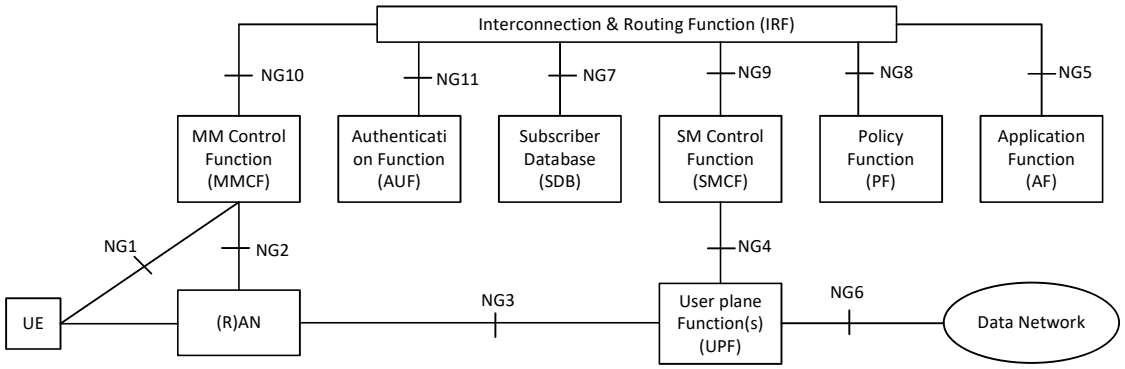


Figure 7.1.3.1-1: Non-roaming reference architecture

7.1.3.2 Roaming

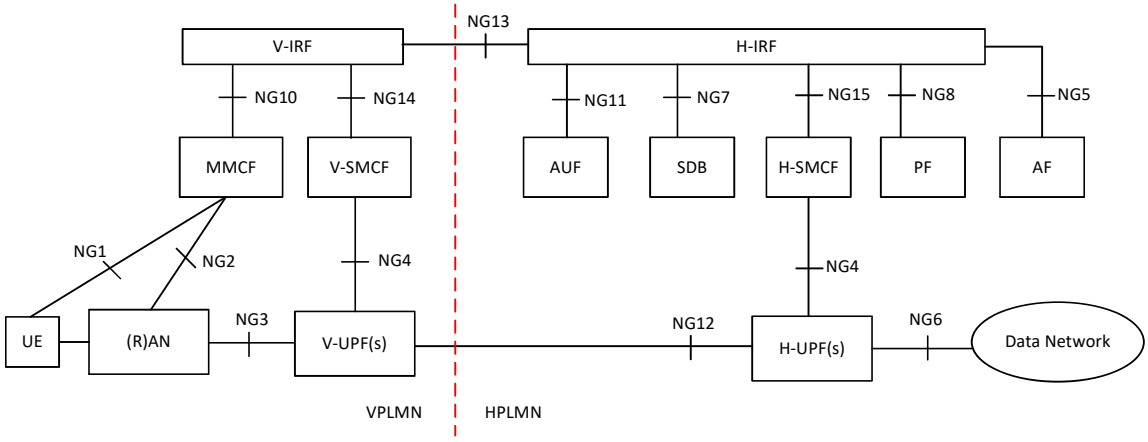


Figure 7.1.3.2-1: Roaming reference architecture for home routed traffic

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 433 of 501

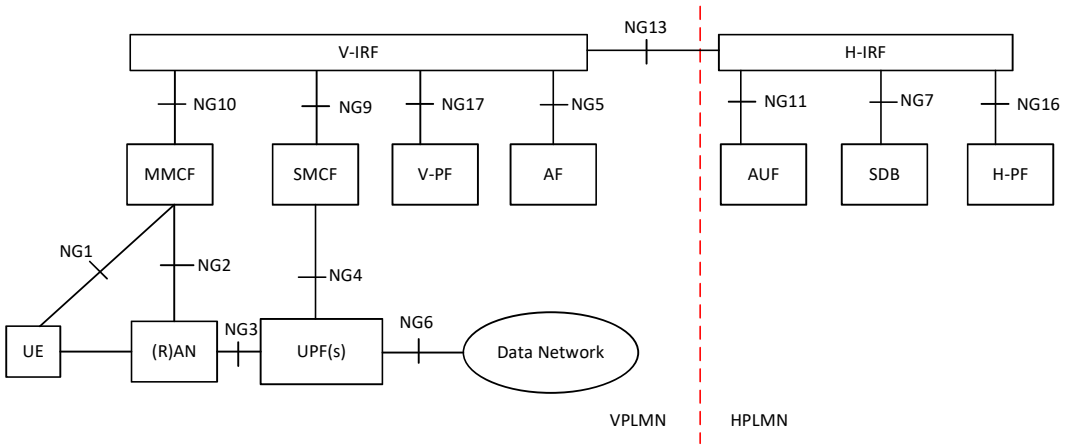


Figure 7.1.3.2-2: Roaming reference architecture for local breakout

7.1.3.3 Reference points

NG1: Reference point between the UE and the MMCF in NG CN.

NG2: Reference point between the (R)AN and the MMCF in NG CN.

NG3: Reference point between the (R)AN and the UPF in NG CN.

NG4: Reference point between the SMCF and UPF(s).

NG5: Reference point between the AF and the IRF.

NG6: Reference point between the UPF(s) and Data Network.

NG7: Reference point between the SDB and the IRF.

NG8: Reference point between the PF and the IRF.

NG9: Reference point between the SMCF and the IRF.

NG10: Reference point between the MMCF and the IRF.

NG11: Reference point between the AUF and the IRF.

NG12: Reference point between the UPF(s) in VPLMN and UPF(s) in HPLMN.

NG13: Reference point between the IRF in VPLMN and the IRF in HPLMN.

NG14: Reference point between the V-IRF and the V-SMCF.

NG15: Reference point between the H-IRF and the H-SMCF.

NG16: Reference point between the PF and the IRF in the HPLMN for the roaming architecture for local breakout.

NG17: Reference point between the PF and the IRF in the VPLMN for the roaming architecture for local breakout.

NOTE 1: Reference points between user plane functions (if the control plane configures multiple user-plane functions for a session) are not shown above for brevity's sake.

NOTE 2: Although the reference architecture is common, not all NFs may be needed within a network slice in a given deployment, e.g. Policy Function may not be deployed for CIoT network slice.

NOTE 3: The NG13 reference point enables interaction between NFs in the HPLMN and NFs in the VPLMN, e.g. between the MMCF in the VPLMN and the SDB in the HPLMN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 434 of 501

Editor's note: In home routed roaming architecture, the placement of AUF may be revisited based on inputs from SA WG3.

Editor's note: The need for IRF and its functionality (clause 6.7.1), or the need for "NF Repository function" and its functionality (clause 6.7.2) are based on the conclusion of KI#7 (interconnection of NF).

Editor's note: Although the figure shows only a single roaming NG13 reference point, it needs to support roaming variants of multiple interfaces e.g. to enable interaction between MMF in the VPLMN and SDB in the HPLMN, V-SMF and H-SMF, V-SMF and PF in the HPLMN etc. Impact due to this for the roaming interface is FFS.

NOTE 4: The use of multiple IRFs is needed to ensure optimized communication amongst a set of locally deployed NFs and a set of centrally deployed NFs, respectively.

Editor's note: The use of multiple IRFs in the non-roaming case has not been reflected yet in figure 7.1.3.1-1.

Editor's note: More standalone NFs may be defined based on the other KIs, e.g. separation of the access specific and access common functionality of MMCF into independent NFs, network slice selector NF for supporting network slicing, traffic steering support NF for traffic steering feature, etc.

7.1.4 High level functional description

The exact set of functionality of each of the NF and the interaction between NFs will be defined as part of the conclusion of individual key issues. The reference architecture defined in 7.1.3 is capable of supporting any type of interactions between any two NFs, without the need to add new interfaces.

NOTE 1: The interaction between two NFs will be based on the example call flow described in either clause 6.7.1.4.2 or clause 6.7.2.2.4.

Following is the nature of the functionality supported by the NFs in the reference architecture.

- **Subscriber DB (SDB)**: Management of subscription profile.
- **SM Control Function (SMCF)**: Allocation of UE IP address, User plane function selection, enforcement of policy and charging rules, etc. The exact set of functionality will be based on the conclusion of key issues 2, 3, 4, 6.

  The SM' is a subset of SM functionality that needs to be supported in the VPLMN for roaming architecture for home routed traffic, e.g. for collecting inter-operator charging data.
- **MM Control Function (MMCF)**: Terminates control plane interface, NG2, from the Access Network carrying both access specific and access common information. Also terminates the NG1 interface. Performs access specific, e.g. UE reachability management, mobility restriction, etc., and access common, e.g. UE registration management, etc., functionality. Forwards the SM related NG1 and possibly NG2 messages to SMCF. The exact set of functionality will be based on the conclusion of key issues 1, 2, 3, 4, 18.

NOTE 2: Generic name needs to be used to reflect the fact that MMCF is common to all accesses.

- **Policy Function (PF)**: Provides dynamic policies for QoS enforcement, charging control, traffic routing, etc. The exact set of functionality will be based on the conclusion of key issue 10.
- **Application Function (AF):** Requests dynamic policies and/or charging control.
- **Authentication Function (AUF)**: Performs authentication process with the UE. The exact set of functionality will be based on the conclusion of key issue 12.
- **User-plane Function(s) (UPF)**: Supports user-plane operations (forwarding to other user-plane functions/a data networks/the control-plane, bitrate enforcement, service detection, etc.). Multiple user-plane functions per session can be activated and configured by the control-plane as needed for a given user-plane scenario. The exact set of functionality will be based on the conclusion of key issue 4.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 435 of 501

7.2 Consolidated architecture option 2

7.2.1 General

Key architecture principles:

- Separate the UP and CP functions, allowing independent scalability and evolution.
- Allow for a flexible deployment of UP and CP functions, i.e. central location or distributed (remote) location.
- Modularize the function design to enable flexible and efficient network slicing.
  - Separated Authentication and Mobility management for supporting unified authentication framework and for supporting UEs which may support only subset of 5G functionality (e.g. not supporting MM functionality)
  - Separated mobility management and session management, they are significantly different on access handling and PDU session handling. Separated MM and SM enables independent evolution and scaling.
- Support a flexible information model with subscription, policy separated from network functions and nodes.
- Minimize access and core network dependencies by specifying a converged access-agnostic core with a common AN - CN interface which integrates different 3GPP and non-3GPP access types.
- Procedures (i.e. set of interactions between two NFs) are defined as a service, wherever applicable, so that its re-use is possible.
- The architecture shall support capability exposure.

7.2.2 Non-roaming reference architecture and reference points

The NextGen architecture consists of the following functions illustrated as the Figure 7.2.2-1:

NG Core Control Plane (NG-CP) consists of the following functions:

- MIF, Message Interconnection Function. Termination of the Provide message connection for protocol between NG-CP functionNFs with other NFsand function outside of CP, e.g., UE, AN, NG-UP. MIF performs as NAS security termination and routsing subsequent message to corresponding function for proper NG-CP NF for message processing.
- NF Repository Function (NRF): It provides NFs registration and discovery functionality so that NG-CP NFs can discover each other and communicate directly without making message pass through MIF.

Editor's note: Whether NRF is a enhancement of DNS is FFS.

- AUF: The authentication related functionalities: ARPF, AUSF, SCMF and SEAF as defined by SA3.
- UMF: UE Management Function. Handles the UE level management function including UE Location management, UE network access management and UE reachability function. UM function supports the UE access the network via multiple access types including 3GPP access and non-3GPP access.

Editor's note: Final naming of UE management is TBD

- SM: Session Management. Allocation of UE IP address, User plane function selection and control, enforcement of policy and charging rules, etc. It may also consist of the control part of enforcement of Charging and Lawful Intercept functions.
- PCF: Policy Control Function. It interacts with other NG-CP functions such as SM, UM to provides dynamic policies for QoS enforcement, charging, access control, traffic routing, etc.
- NCE: Network Capability Exposure function.

Editor's note: The list of the functions of the NFs above may be updated based on the progress of related Key Issues.

The MIF is introduced to minimize the dependencies between the NG-CP functions with the protocols used to transfer the message. Through it, a single interface is exposed towards the radio while abstracting the modular (elementary) functions supported in the core network. The MIF decrypt the NAS message and forwarding the NAS-application

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 436 of 501

related message (e.g., NAS-MM, NAS-SM) to the corresponding CP function (i.e., MM and SM correspondingly) where the NAS application related message content is processed. Therefore, update the NAS-application related message does not need to update the MIF. If there are multiple instances of one CP function, e.g., MM instances, the MIF routes the control plan message to the proper one. The MIF may maintain the session and protocol related state (e.g., security information for message decryption).

The NG-CP NFs (e.g., MM, SM) may be different for scenarios supported by variant Network Slices.

NG Core User Plane (NG-UP) function, a generic user-plane architecture supporting various operations and functionalities such as:

- External PDU session point of interconnect (e.g. IP)
- Packet routing & forwarding
- Traffic handling (e.g. QoS enforcement)
- Anchor point for Intra-/Inter-RAT mobility (when applicable)
- Optional functionalities such as Packet inspection, Lawful intercept (UP collection)

There may exist multiple NG-UP functions in one PDU session to offload traffic to the local DN.

UDM, NG Unified Data Management. It stores three types of user data, i.e., subscription, policy (e.g. on QoS and charging), session related context (e.g., UE location) in a unified data layer.

Editor's note: Whether UDM could be part of NG-CP is FFS.

SA3 defined the security framework with Authentication Credential Repository and Processing Function (ARPF), Authentication Server Function (AUSF), Security Context Management Function (SCMF), Security Anchor Function (SEAF) in 3GPP TR 33.899 [16]. In the architecture defined here, the AU should support SCMF and SEAF.

Editor's note: The architecture impact on ARPF, AUSF, SCMF and SEAF will be updated based on SA WG3 work.

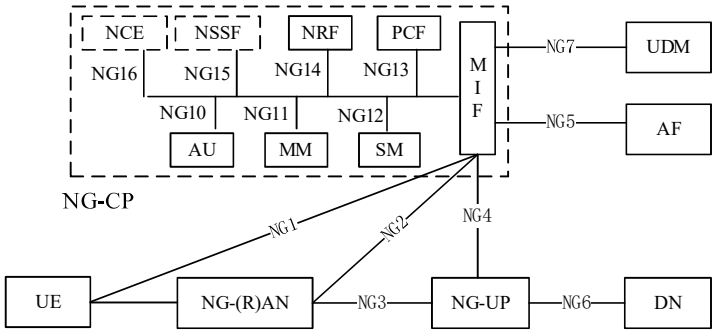


Figure 7.2.2-1: Non-Roaming NextGen Architecture

The following reference points and interfaces are illustrated in the Figure 7.2.2-1:

NG1: Reference point for the control plane between NG UE and NG Core.

NG2: Reference point for the control plane between NG (R)AN and NG Core.

NG3: Reference point for the user plane between NG (R)AN and NG-UP.

NG4: Reference point between NG-CP function and NG-UP Functions

Editor's note: Whether MIF is integrated with MM is FFS. If MIF is integrated with MM, the NG4 reference point will be from NG-UP to SM of NG-CP.

NG5: Reference point between NG-CP function and Application Function

NG6: Reference point between the NG-UP and the data network. Data network may be an operator external public or private data network or an intra-operator data network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 437 of 501

NG7: Reference point between NG-CP function and NG User Data Management.

NG10, NG11, NG12, NG13, NG14, NG15, NG16: Service-based interfaces of the NG-CP NFs such as AU, MM, SM, PCF, NRF, NSSF, NCE, through which other NG-CP functions can invoke them for service. Those interfaces are independent on the communication protocol.

Editor's note: Whether the NG7 can be a service-based interface is FFS.

It is important to enable multi-vendor interworking between radio and network functions within the core network and between the network functions within the core network. At the same time, it is sufficient if a single interface is exposed towards the radio while abstracting the modular (elementary) functions supported in the core network.

7.2.3 Roaming reference architectures

The Figures 7.2.3-1 and 7.2.3-2 introduces roaming functional reference architectures for local-breakout and Home-routed scenarios.

For the local breakout case, the visited CP function fetches UE home subscription/policy data through NG8 from hUDM. The home PCF plays a role that controls how the user subscription and policy related data will be provided to to the visited PLMN CP functions, e.g., the visited PCF, MM.

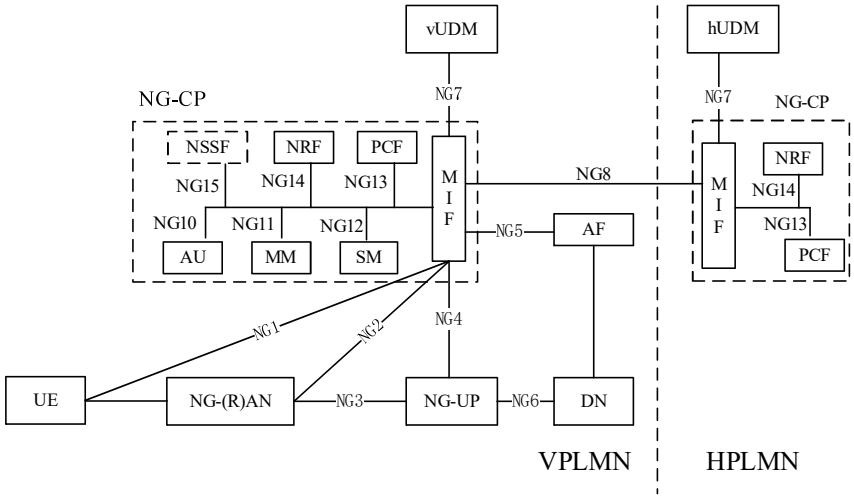


Figure 7.2.3-1 Roaming reference architecture - local breakout scenario

NG8: Reference point between VPLMN NG-CP MIF and HPLMN NG-CP MIF.

Editor's note: Whether there is reference point between vUDM and hUDM is FFS.

For the home-routed case, the UE session related state will be stored both in the vUDM and hUDM. To setup and maintain the home-routed session, the VPLMN NG-CP NFs need to communicate with HPLMN NG-CP NFs such as PCF and SM though the MIF with NG8. In the HPLMN, the PCF provide SM with policy which further be executed in the NG-UP.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 438 of 501

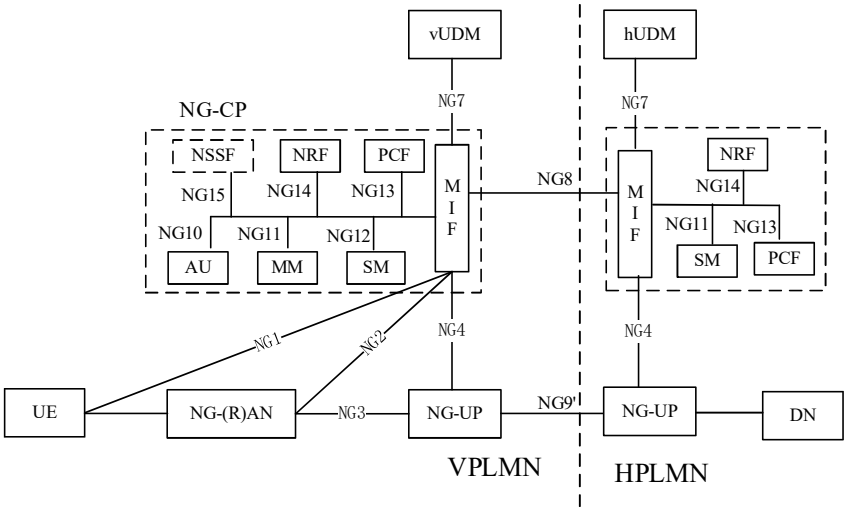


Figure 7.2.3-1 Roaming reference architecture – home routed scenario

NG9: Reference point between VPLMN UP function and the HPLMN UP function.

7.3 Consolidated architecture option 3

7.3.1 General

The NextGen network reference architecture should consider the following aspects:

1) Support 5G use cases and service requirements
2) Enable Operational agility (enable extreme automation (faster deployments, upgrades, reduce TCO)
3) Allow independent evolution of different parts of the network (e.g. access and core).

Key Architecture principles:

- Abstract the transport domain from 3GPP network functions to allow for independent evolution and to enable operators to use different transport technologies (e.g. Ethernet, MPLS, SDN-based transport, etc.). 3GPP network functions should neither mandate nor rule out support for any of these technologies in the transport domain.

Allow scalability of UP and CP functions independently

- Allow for a flexible deployment of UP separate from the CP, i.e. central location or distributed (remote) location (i.e. with no restriction in the location).
- Support transmission of different PDU types, e.g. IP, Ethernet
- Separation of functions including subscription database from functions providing the end user service
- Separation of Policy function to govern the network behaviour and end user experience
- Allows for different network configurations in different network slices.

Control Plane:

- It is important for the UE to trust that certain functionalities are supported in the network thus important to enable multi-vendor interworking between UE and network functions. However, from the UE perspective, it is irrelevant how and where it exists within the network (e.g. which function module or software supports a certain function).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 439 of 501

- It is important to enable multi-vendor interworking between radio and network functions within the core network and between the network functions within the core network. At the same time, it is sufficient if a single interface is exposed towards the radio while abstracting the modular (elementary) functions supported in the core network.

User plane:

- A generic user-plane function (UP function) is defined, which supports various user-plane operations (incl. forwarding operations to other UP functions/data networks/the control-plane, bitrate enforcement operations, service detection operations, etc.)

NOTE 1: The detailed list of user-plane operations will be based upon the conclusion of key issue 4.

- The control plane configures the UP functions to provide the traffic handling functionality needed for a session. One or multiple UP functions per session can be activated and configured by the control-plane as needed for a given user-plane scenario.

- To support low latency services and access to local data networks, user plane functions can be deployed close to the radio. For central data networks, UPFs can be deployed centrally.

Concurrent access to local and centralized services is supported as follows

- Multiple PDU sessions to both a local UP function (providing access to local data networks) and a central UP function (providing access to central data networks); or

- A single PDU session, for which the control plane has configured two UP functions: one UP function performing traffic classification and traffic steering towards either the local data network or the central data network, the other UP function providing access to the central data network (as depicted in figure 7.3.2-3).

NOTE 2: The control plane can also configure multiple UP functions in the single PDU session case for local data network access.

7.3.2 Reference architecture

Figure 7.3.2-1 depicts the non-roaming architecture functional view.

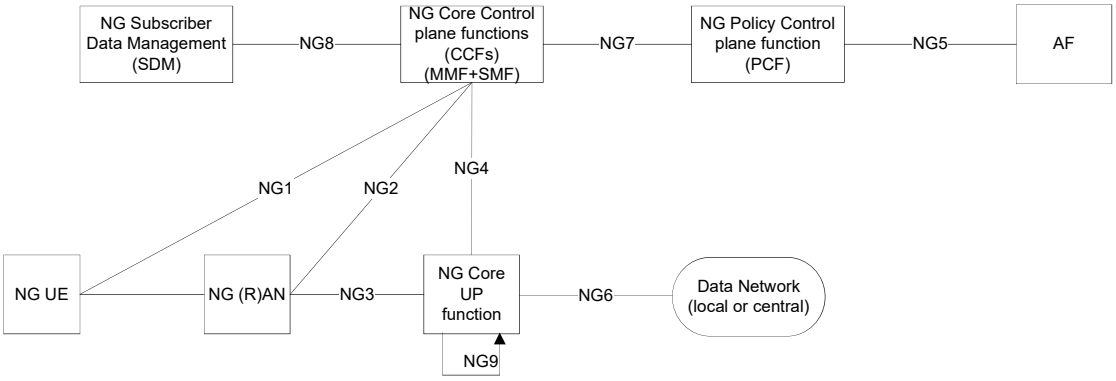


Figure 7.3.2-1: Non-roaming reference architecture

Figure 7.3.2-2 depicts the non-roaming architecture for UEs concurrently accessing a local and a central data network using multiple PDU Sessions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 440 of 501

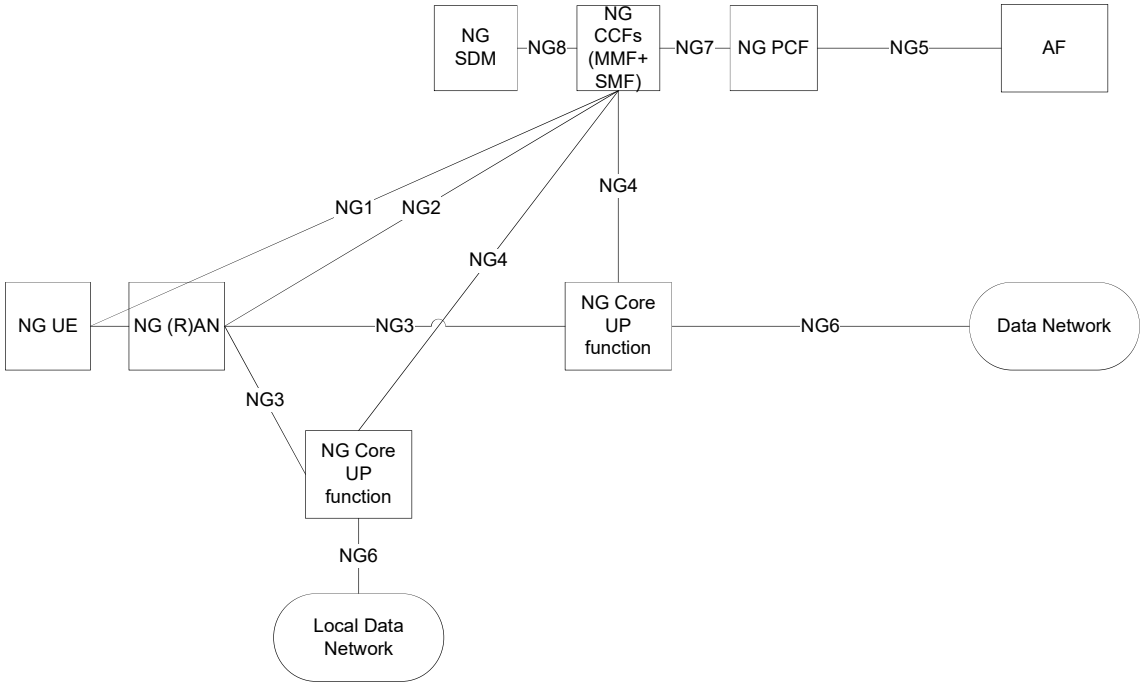


Figure 7.3.2-2: Applying Non-roaming reference architecture for concurrent access to local and central data networks (multiple PDU session option)

Figure 7.3.2-3 depicts the non-roaming architecture in case concurrent access to local and central data networks is provided within a single PDU session:

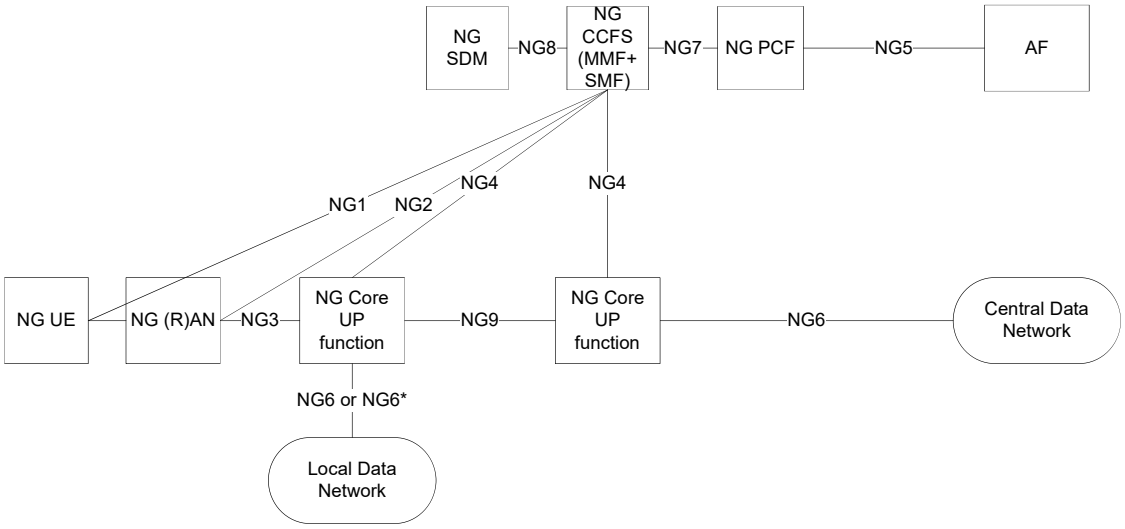


Figure 7.3.2-3: Applying Non-roaming reference architecture for concurrent access to local and central data networks (single PDU session option)

Following figure 7.3.2-4 depicts the roaming architecture in case of home routed scenario:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 441 of 501

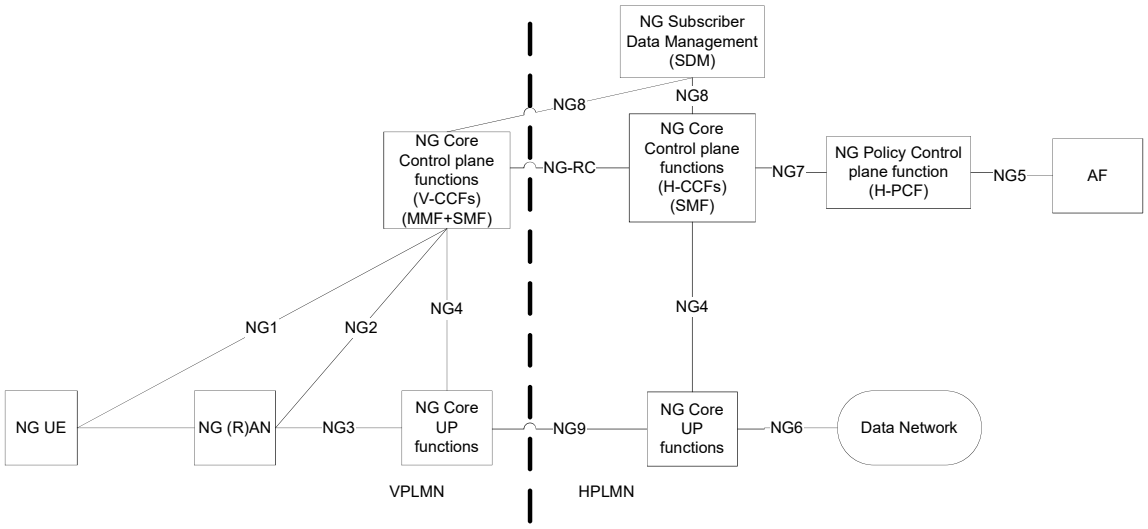


Figure 7.3.2-4: Roaming reference architecture - Home routed scenario

Following figure 7.3.2-5 depicts the roaming architecture in case of local break out scenario:

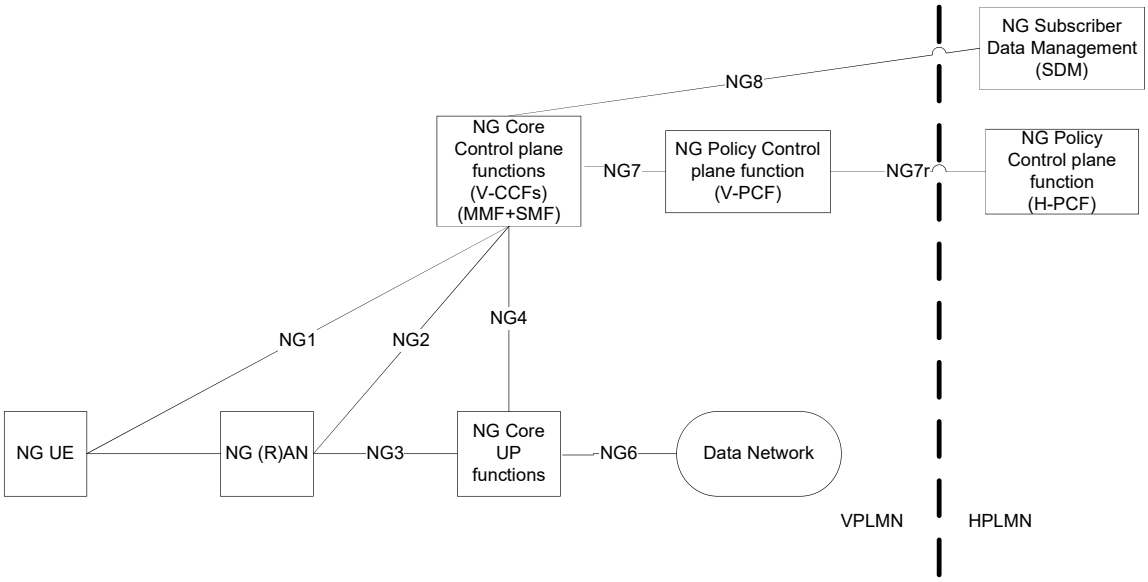


Figure 7.3.2-5: Roaming reference architecture - local breakout scenario

Editor's note: The choice between NG6* and NG6 depends on whether the PDU Session has a single IP address/prefix or multiple IP address/prefixes. It is FFS whether both types need to be supported. Whether the distinction between NG6 and NG6* is needed is also FFS.

Editor's note: The list of individual NG Core Control network functions (e.g. SMF versus MMF, or access specific versus access independent, etc.) is FFS. The interconnection model for all control plane network functions is FFS.

Editor's note: Need for NG8 from H-CCFs to NG-SDM (i.e. in the home routed scenario) is FFS.

NOTE 3: Regardless of the number of CCFs, there is only one NAS interface instance between the UE and the CN, terminated at one of the CCFs that implements at least access authentication and mobility management.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 442 of 501

NOTE 4: Criteria to select multi-vendor open (standardized) interfaces should be determined.7.3.3Network functions and reference points.

The 5G Reference Architecture consist of the following functions:

- NG Subscriber Data Management (NG SDM)
- NG Policy Control function (NG PCF)
- NG Core Control functions (NG CCFs)
- NG Core User plane function (NG UPF)
- NG RAN
- NG UE
- Data network, e.g. operator services, Internet access or 3rd party services.

The following is a high level split of functionality between the control plane and the user plane.

The NG Core Control functions include the following functionality:

- Termination of RAN CP interface
- Termination of NAS
- Access Authentication
- NAS Ciphering and Integrity protection
- Mobility management
- Session Management
- UE IP address allocation & management (incl optional Authorization)
- Selection of UP function
- Termination of interfaces towards Policy control and Charging functions
- Policy & Charging rules handling, incl control part of enforcement and QoS
- Lawful intercept (CP and interface to LI System)

NOTE 5: Not all of the CCF functions are required to be supported in an instance of CCFs of a network slice.

The NG Core User plane function includes the following functionality:

- Anchor point for Intra-/Inter-RAT mobility (when applicable)
- External PDU session point of interconnect (e.g. IP).
- Packet routing & forwarding
- QoS handling for User plane
- Packet inspection and Policy rule enforcement
- Lawful intercept (UP collection)
- Traffic accounting and reporting

NOTE 6: Not all of the UPF functions are required to be supported in an instance of user plane function of a network slice.

The NG Policy function includes the following functionality:

- Supports unified policy framework to govern network behaviour.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 443 of 501

- Provides policy rules to control plane function(s) to enforce them.

Editor's note: The need for an interface between NG Policy Function and SDM is FFS.

The 5G Reference Architecture contain the following reference points:

NG1: Reference point between the UE and the NG Core Control plane function.

NG2: Reference point between the RAN and the NG Core Control plane function.

NG3: Reference point between the RAN and the NG Core User plane function.

NG4: Reference point between the NG Core CP functions and the NG Core User plane function.

NG5: Reference point between the NG Core CP functions and an Application Function.

NG6: Reference point between the NG Core UP functions and a Data Network (DN).

NG6*: Reference point between a NG Core UP function and a local Data Network (when concurrent access to both a local and central data network is provided for one PDU session with a single IP address/prefix).

NOTE 7: Details of NG6* mechanism are beyond the scope of 3GPP.

NG7: Reference point between the NG Core Control plane function and the NG Policy Control function.

NG8: Reference point between the NG Core Control plane function and the Subscriber Data Management.

NG9: Reference point between two NG Core User plane functions.

NG7r: Reference point between the V-PCF and the H-PCF.

NG-RC: Reference point between the V-CCFs and the H-CCFs.

Editor's note: Whether additional reference points between UPFs need to be defined for other user-plane scenarios is FFS.

7.3.2 Applicable solutions

Editor's note: List the solutions from chapter 6 that are applicable to the architecture.

7.3.3 Evaluation

Editor's note: Evaluation for consolidated architecture option 3.

7.4 Consolidated architecture option 4

7.4.1 Non-roaming reference architecture and reference points

Based on the above principles and requirements, a minimal system should be specified as the baseline that can serve the most basic use cases. Additional functionality can then be added on demand as needed to serve more demanding use cases. This architecture is depicted in figure 7.4.1-1. It also highlights the potential common functionality and interfaces in the NextGen system.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 444 of 501

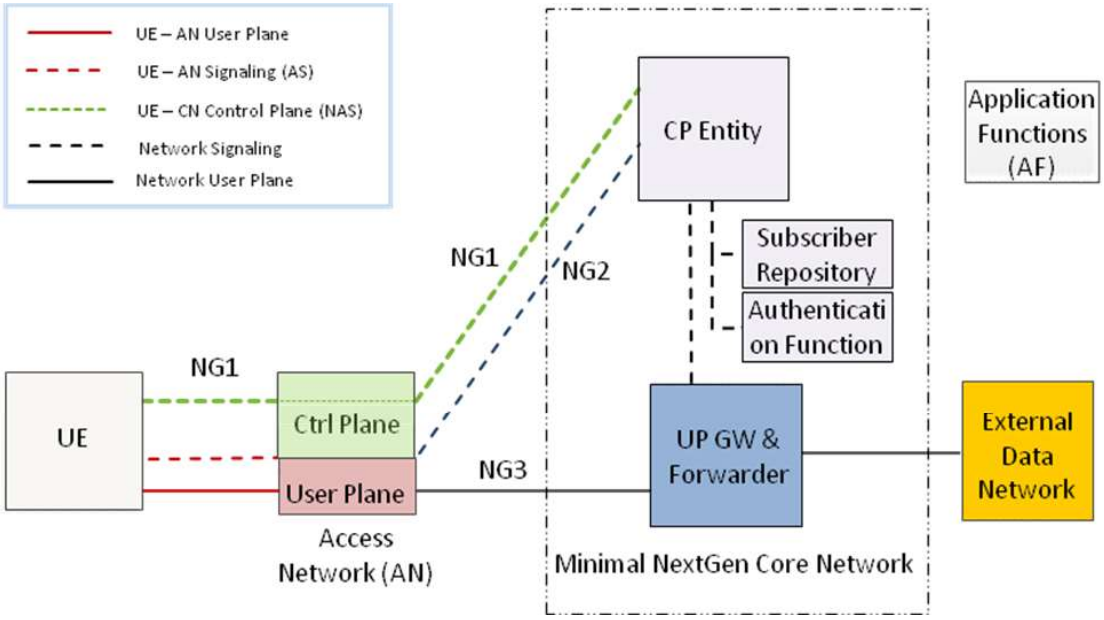


Figure 7.4.1-1: Baseline NextGen system

The communication (CP and UP) between UE and AN as well as any AN internal communication is access specific. All other communication can be designed in a access independent fashion:

- The CP entity authenticates the subscriber and obtains the subscription information interacting with an access independent subscriber repository and authentication function.
- Following successful authentication, the CP entity informs the UP GW & Forwarder aout the permitted UP flows for this UE, based on the information obtained from the subscriber profile.
- The User Plane GW & Forwarder function routes service data flows between AN and external Data Network (e.g. Internet).

Additional CN functions (QoS, charging, …) beyond this baseline system are needed in more demanding usage scenarios. Such additional CN control plane functions are enabled on demand, as required by the specific customer use case. Figure 7.4.1-2. depicts this principle.

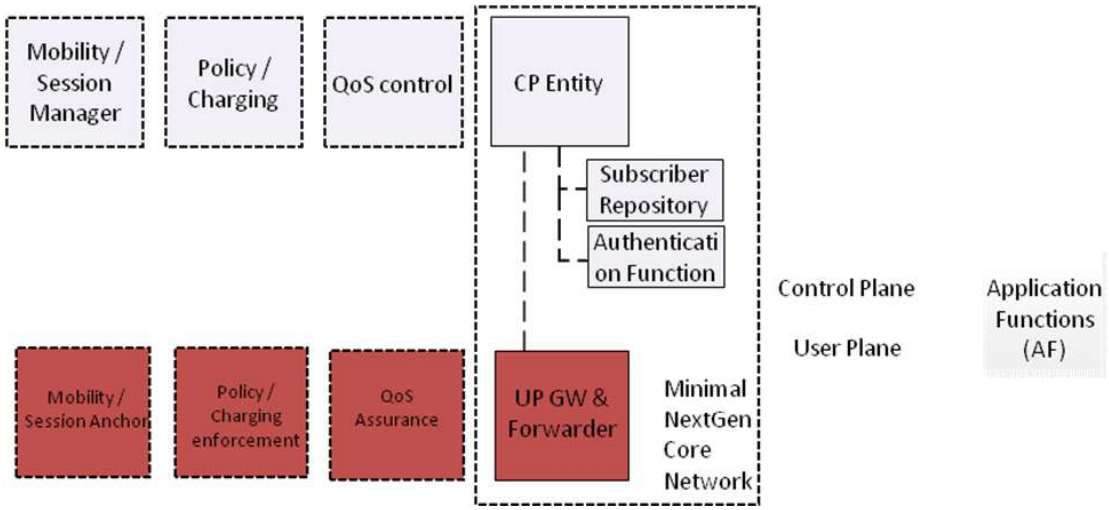


Figure 7.4.1-2: Extended NextGen CN showing on-demand network functions

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 445 of 501

It is thereby possible to configure e.g. the following CP functions per UE / flow:

- Quality of Service.
- Charging.
- Policy Control.
- Mobility Management.
- Session/Service Continuity.
- with or without intra-AN mobility.
- with or without AN change.

CN user plane functions associated with the active CP functions can be chained into the user plane path as shown above.

NOTE 1: The above functions are examples only and are neither intended to define the overall functionality of the network nor the granularity of the network functions.

NOTE 2: AF may be shared with external network, or exist exclusively within or outside of the operator domain.

7.4.1.1 Communication between Network functions

The communication between the baseline NextGen System is performed by making use of a Message Routing and Forwarding Function (MRFF). Basis for all information exchange between NFs and between NFs and the UDM is the MRFF where all Control plane functions and User plane functions are able to retrieve, share, or modify information located on the UDM representing a shared data layer.

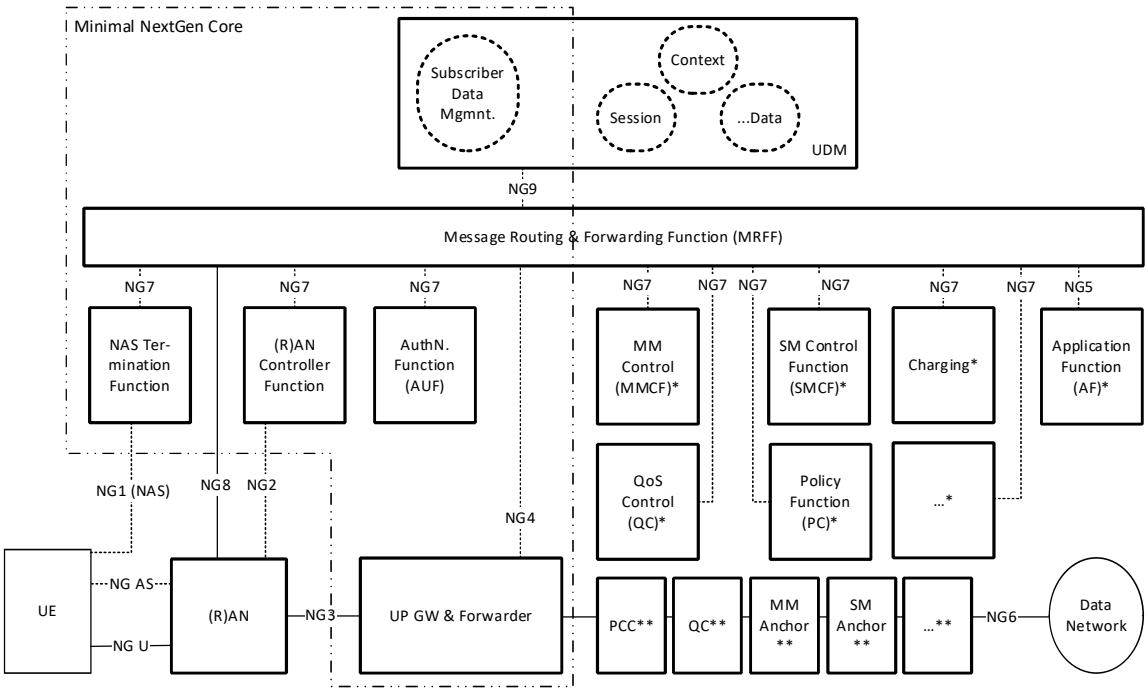


Figure 7.4.1.1-3: Information Exchange in the NextGen System

This 5G Reference Architecture contains the following reference points:

NG1: Reference point between the UE and NAS Termination Function.

NG AS: Reference point between UE and the (R)AN function for AS signalling.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 446 of 501

NG U: Reference point between UE and the (R)AN function for user data.

NG2: Reference point between the (R)AN and the (R)AN Controller Function.

NG3: Reference point between the (R)AN and the UP functions.

NG4: Reference point used for MRFF communication by the UP functions.

NG5: Reference point used for MRFF communication by an Application Function.

NG6: Reference point between the UP functions and a Data Network (DN).

NG7: Reference point used for MRFF communication by the CP functions.

NG8: Reference point used for MRFF communication by the (R)AN functions

NG9: Reference point used for MRFF communication by the UDM

The minimal NextGen Core network as described in clause 7.4.1 consists of the NAS Termination Function, the (R)AN Controller Function, the Authentication Function, the Subscriber Data Management and UP Forwarding and Gateway Functions. Beyond this baseline system, additional and superior CP-NFs are enabled on-demand (CP-NF*) and will exchange information via the MRFF, too. Similarly, UP-NFs** associated with the respective CP-NFs can be chained into the user plane path as shown above.

CP functions can communicate via the MRFF using NG7. UP functions can communicate via the MRFF using NG4 (note that for the UP-NFs**, the NG4 reference point is not shown in the diagram). (R)AN can communicate via the MRFF using NG8. The UDM can communicate via the MRFF using NG9.

Editor's note: Whether all NG4, NG7 and NG8 instances are identical or different is FFS.

The NG7 offers communication where every CP-NF is able to retrieve, share, or modify information, located in the UDM, via the MRFF. Each CP-NF has its own NG7 communication towards the MRRF. Each UP-NF has its own NG4 communication towards the MRRF. Each (R)AN may have its own NG8 communication towards the MRFF. The number and complexity of on-demand functions is based on the driven use case.

(R)AN control function terminates the access specific communication with the (R)AN. All further communication can be access-agnostic.

The User Data Management (UDM) stores user subscription data, policy data (e.g. on QoS and charging), session/user related context and state in a unified data layer.

7.4.1.2 Functional Description

The discussed option and its functional description is based on the MRFF and the data storage on the UDM which serves as the Shared Data Layer (SDL).

When a new NF-instance is deployed, instantiated and configured by the network management and is ready to perform its specified functionality, it registers itself on the MRFF. The registration may contain the service description and/or subscription(s) to certain notifications. Appropriate security functions (e.g., Authorization of Subscription) may be performed before the NF-instance is allowed to communicate. When removing the NF-instance (e.g., scale-in), the NF-instance de-registers itself from the MRFF.

NOTE: By registering and de-registering of NF-instances, the MRFF maintains a directory of all available and active NF-instances together with their service capabilities and subscriptions.

When a NF-instance wants to send a message to another NF, it first publishes the message towards the MRFF. The message includes certain meta-information, and the message content itself. The MRFF uses the meta-information and the directory to select an appropriate target NF-instance, i.e. a NF-instance which has registered the corresponding service and/or subscriptions. The selection of a target NF-instance may also consider enforcement of message constraints and/or load-balancing. The message is then made available to the selected destination by the MRFF.

NFs should operate stateless. When the NFs require certain information, they may retrieve appropriate state and context information from the SDL. However, messages within a transactional context require an identifier on meta-information level to provide the messages and the results onto the appropriate NF or, more specific, the appropriate NF-instance. Transactions may be finalized by the original NF-instances, which keeps an internal transaction state. This could by solved by using a Reply-To-mechanism inside the meta-information.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 447 of 501

The NFs only need to store the transaction state until their task is performed for that specific transaction. The results of the transactions are stored on the SDL. Upcoming NF requests may fetch the data directly from the SDL.

Details on the SDL are handled in 6.7.5 (Solution 7.5).

7.4.2 Roaming architectures

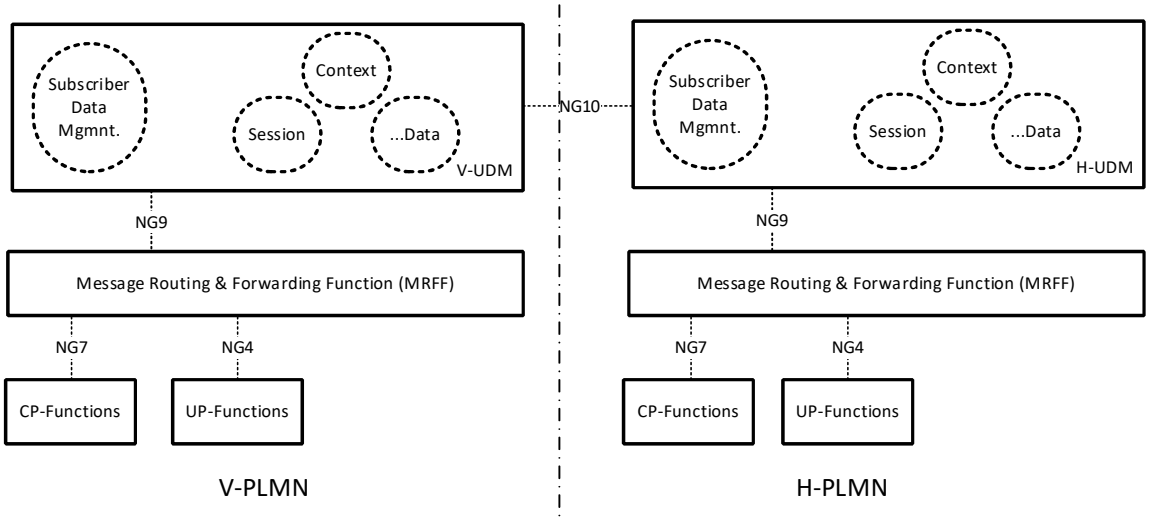


Figure 7.4.2-1: Information Exchange in the NextGen System in the roaming scenario

In the roaming scenario, the exchange of subscriber data and credentials will be managed between H-PLMN and V-PLMN via the Reference Point NG10.

This 5G roaming Reference Architecture contains in both the VPLMN and the HPLMN the reference points specified in the non-roaming architecture in clause 7.4.1.1, plus the following roaming reference point.

NG10: Reference point between the V-UDM and the H-UDM.

NOTE: Further required reference points between the VPLMN and the HPLMN in addition to NG10 are specified in solutions to other key issues.

7.5 Roaming interface functional distribution

7.5.1 Architecture description

Editor's note: This clause will contain e.g. terminology, overview, architecture description of the solution.

This solution describes the roaming scenario for home-routed traffic, including functional allocation between HPLMN and VPLMN.

Potential roaming interfaces for aspects such as Subscriber Data Management, authentication/security, policy control and charging are not fully addressed in this solution.

Editor's note: Functional distribution of the local breakout roaming case is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 448 of 501

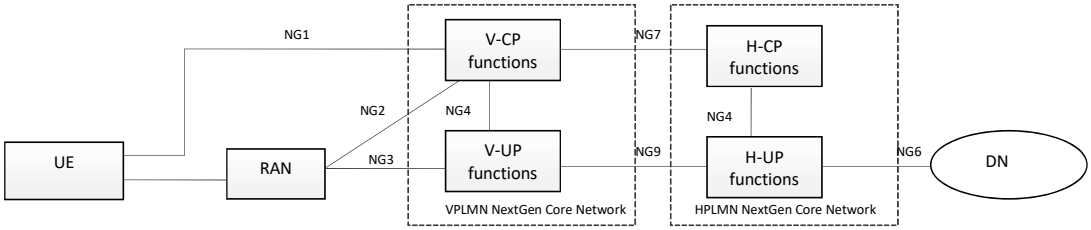


Figure 7.5.1.1-1: Home routed roaming reference architecture (not all functions shown)

NG7: Reference point between the V-CP and H-CP functions (home routed roaming scenario).

NG9: Reference point between the V-UP and H-UP functions (home routed roaming scenario).

The final names for the reference points are assumed to be defined in the work for the consolidated architecture.

V-CP functionality:

- MM functionality
- NAS handling for SM, e.g. to make Home CP selection based on PDU type, Data Network name etc. It is assumed that the SM-specific NAS is terminated in VPLMN, while SM parameters are forwarded to HPLMN.
- Selection of HPLMN CP function using DN name, parameters from UE, from SDM as well as provisioned parameters (it is assumed that slice specific selection is handled by MM)

Editor's note: The details of H-CP selection and what information that can be taken into account by V-CP needs further study.

Editor's note: Discovery and selection of Network Functions and the interconnection between VPLMN and HPLMN is is also dependent on the outcome of Key Issue 7.

- Determining appropriate QoS taking information from HPLMN, roaming agreements and local policies into account (assuming that HPLMN is not allowed to dictate on its own what QoS to use in VPLMN)
- Handling of QoS related information towards AN and UE
- Handling of roaming interface
- Handling SM related information exchange between UE/RAN and HPLMN
- Selection of V-UP function(s)
- Managing mobility related changes of user plane paths, e.g. in case of V-UP relocation
- Managing idle-active related information
- Charging support:
  - Collecing appropriate information from CP and UP
  - Providing CDRs or equivalent to external entities
- Lawful intercept CP and interface to LI System

H-CP functionality:

- Handling interface towards UP function(s)
- Selection of H-UP function(s)
- Selection of DN using parameters from V-SM as well as provisioned parameters
- Determining appropriate QoS taking information from SDM, PCC etc. into account

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 449 of 501

- PDU-specific SM functionality:
  - Authorization of PDU type
  - For PDU-type IP: UE IP address allocation & management, RADIUS/DHCP client (IP Address & Authorization)
  - For other PDU types: required address assignment etc
- Provisioning of external server identities like DNS, P-CSCF etc for the UE if found needed
- Managing mobility related changes of user plane paths, e.g. in case of V-UP relocation
- Charging support:
  - Collecing appropriate information from CP and UP
  - Providing CDRs or equivalent to external entities
- Gx, Gy termination or equivalent if found needed
- Policy enforcement control part, including Policy & Charging (PCC) rules handling
- Lawful intercept CP and interface to LI System

V-UP functionality:

- Anchor point for Intra-access and Inter-access mobility
- Packet forwarding
- QoS transport level marking
- Packet inspection and PCC rule enforcement
- User data duplication (for lawful intercept)

Editor's note: Local breakout in the VPLMN, e.g. to access a local Data Network, is FFS.

H-UP functionality:

- Packet routing & forwarding
- External IP point of interconnect
- Policy enforcement
- QoS marking
- Packet inspection and PCC rule enforcement
- User data duplication (for lawful intercept)

Editor's note: Whether H-UP is anchor point for inter-access mobility is FFS and depends e.g. on conclusions for non-3GPP access integration solutions.

Editor's note: If it brings advantages to use the NG7 and NG9 interfaces also in a non-roaming scenario as has been done in EPC for S5 vs S8 is FFS.

7.5.1 Function description

Editor's note: This clause will contain function descriptions and the interactions among the network functions.

7.5.1 Solution evaluation

Editor's note: This clause will contain evaluation on the system impacts, e.g. UE, access network and non-access network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 450 of 501

7.6 Consolidated architecture option 6

7.6.1 General

The NextGen network reference architecture should consider the following aspects:

1) Support 5G use cases and service requirements
2) Enable Operational agility (enable extreme automation (faster deployments, upgrades, reduce TCO)
3) Allow independent evolution of different parts of the network (e.g. access and core).

Key Architecture principles:

- Abstract the transport domain from 3GPP network functions to allow for independent evolution and to enable operators to use different transport technologies (e.g. Ethernet, MPLS, SDN-based transport, etc.). 3GPP network functions should neither mandate nor rule out support for any of these technologies in the transport domain.

Allow scalability of UP and CP functions independently

- Allow for a flexible deployment of UP separate from the CP, i.e. central location or distributed (remote) location (i.e. with no restriction in the location).
- Support transmission of different PDU types, e.g. IP, Ethernet
- Separation of functions including subscription database from functions providing the end user service
- Separation of Policy function to govern the network behaviour and end user experience
- Allows for different network configurations in different network slices.
- Separation of Mobility Management and Session Management functionality which also supports:
  - UE simultaneously connected to multiple network slices
  - Independent "access agnostic" and "access specific" functionality.

Control Plane:

- It is important for the UE to trust that certain functionalities are supported in the network thus important to enable multi-vendor interworking between UE and network functions. However, from the UE perspective, it is irrelevant how and where it exists within the network (e.g. which function module or software supports a certain function).
- It is important to enable multi-vendor interworking between radio and network functions within the core network and between the network functions within the core network. At the same time, it is sufficient if a single interface is exposed towards the radio while abstracting the modular (elementary) functions supported in the core network.
- Procedures (i.e. set of interactions between two NFs) are defined as a service, wherever applicable, so that its re-use is possible. This will be evaluated on a case by case basis when specifying the procedure.
- It is important that the separation between Mobility Management and Session Management enables support of individual UEs simultaneously connected to multiple network slices
- It is important that a separation between functions in the control plane support roaming with both Home routed traffic as well as Local breakout traffic in the visited PLMN in an efficient way.

User plane:

- A generic user-plane function (UP function) is defined, which supports various user-plane operations (incl. forwarding operations to other UP functions/data networks/the control-plane, bitrate enforcement operations, service detection operations, etc.)

NOTE1: The detailed list of user-plane operations will be based upon the conclusion of key issue 4.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 451 of 501

- The control plane configures the UP functions to provide the traffic handling functionality needed for a session. One or multiple UP functions per session can be activated and configured by the control-plane as needed for a given user-plane scenario.
- To support low latency services and access to local data networks, user plane functions can be deployed close to the radio. For central data networks, UPFs can be deployed centrally.
- To support home routed roaming a UP function is located in the HPLMN, and there also needs to be another UP function located in the VPLMN which includes roaming functionality such as Charging, LI, etc.

Concurrent access to local and centralized services is supported as follows

- Multiple PDU sessions to both a local UP function (providing access to local data networks) and a central UP function (providing access to central data networks); or
- A single PDU session, for which the control plane has configured two UP functions: one UP function performing traffic classification and traffic steering towards either the local data network or the central data network, the other UP function providing access to the central data network (as depicted in figure 7.6.2-3).

NOTE 2: The control plane can also configure multiple UP functions in the single PDU session case for local data network access.

7.6.2 Reference architecture

Figure 7.6.2-1 depicts the non-roaming architecture functional view.

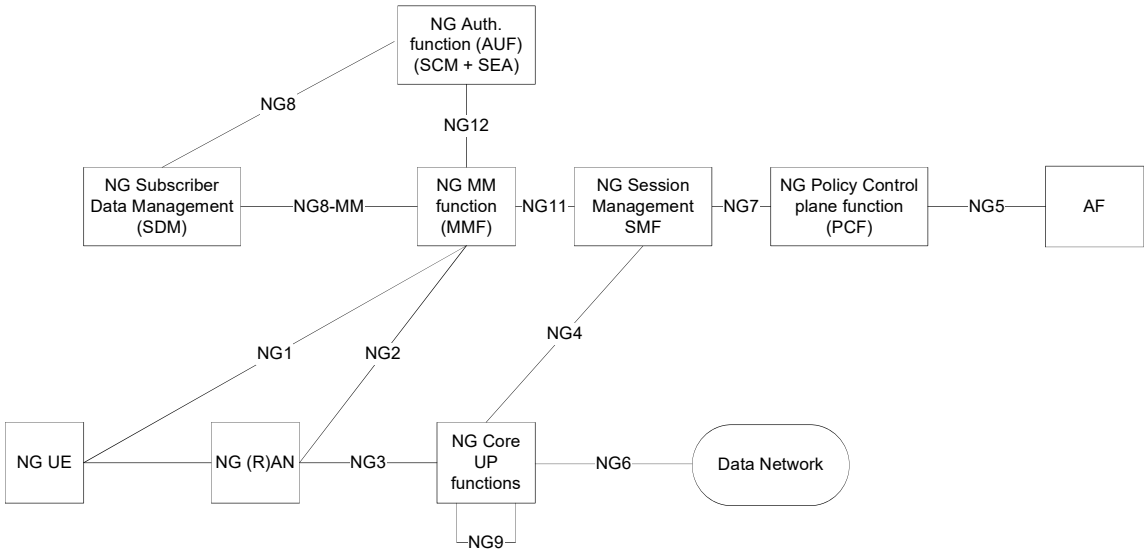


Figure 7.6.2-1: Non-roaming reference architecture

Figure 7.6.2-2 depicts the non-roaming architecture for UEs concurrently accessing a local and a central data network using multiple PDU Sessions.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 452 of 501

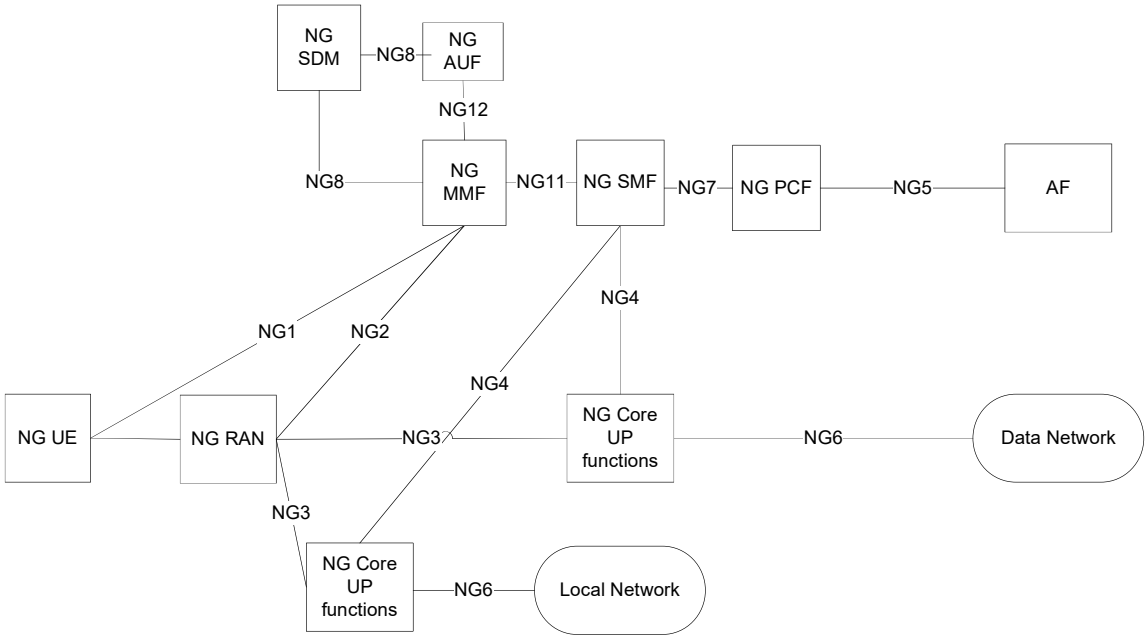


Figure 7.6.2-2: Applying Non-roaming reference architecture for concurrent access to local and central data networks (multiple PDU session option)

Figure 7.6.2-3 depicts the non-roaming architecture in case concurrent access to local and central data networks is provided within a single PDU session:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 453 of 501

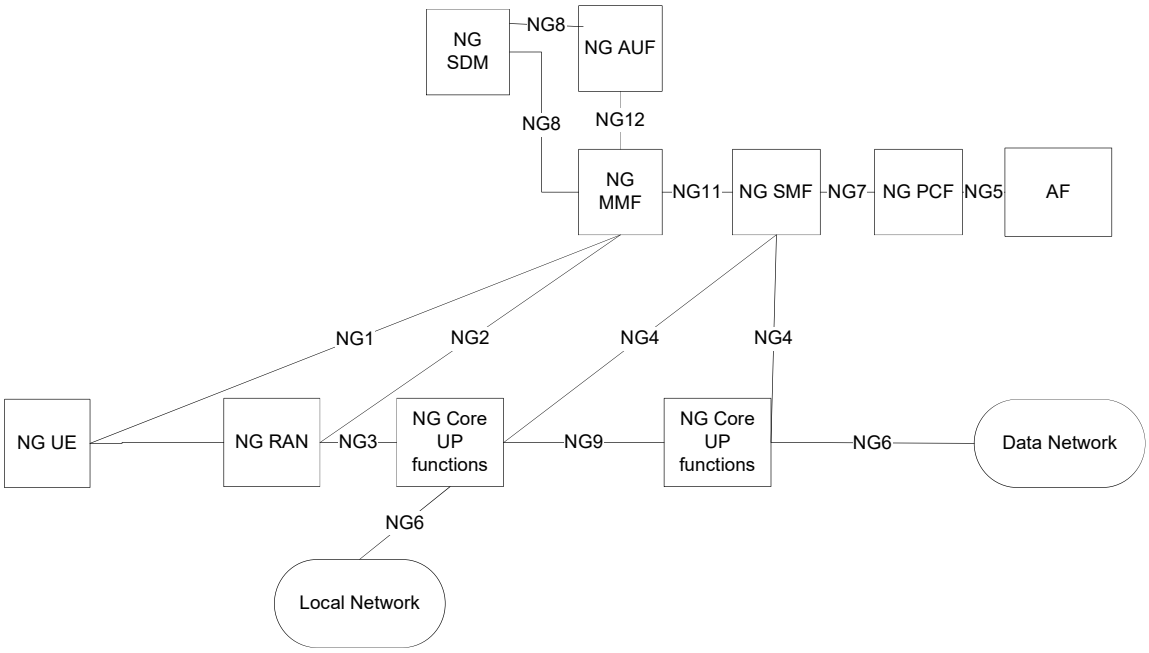


Figure 7.6.2-3: Applying Non-roaming reference architecture for concurrent access to local and central data networks (single PDU session option)

Following figure 7.6.2-4 depicts the roaming architecture in case of home routed scenario:

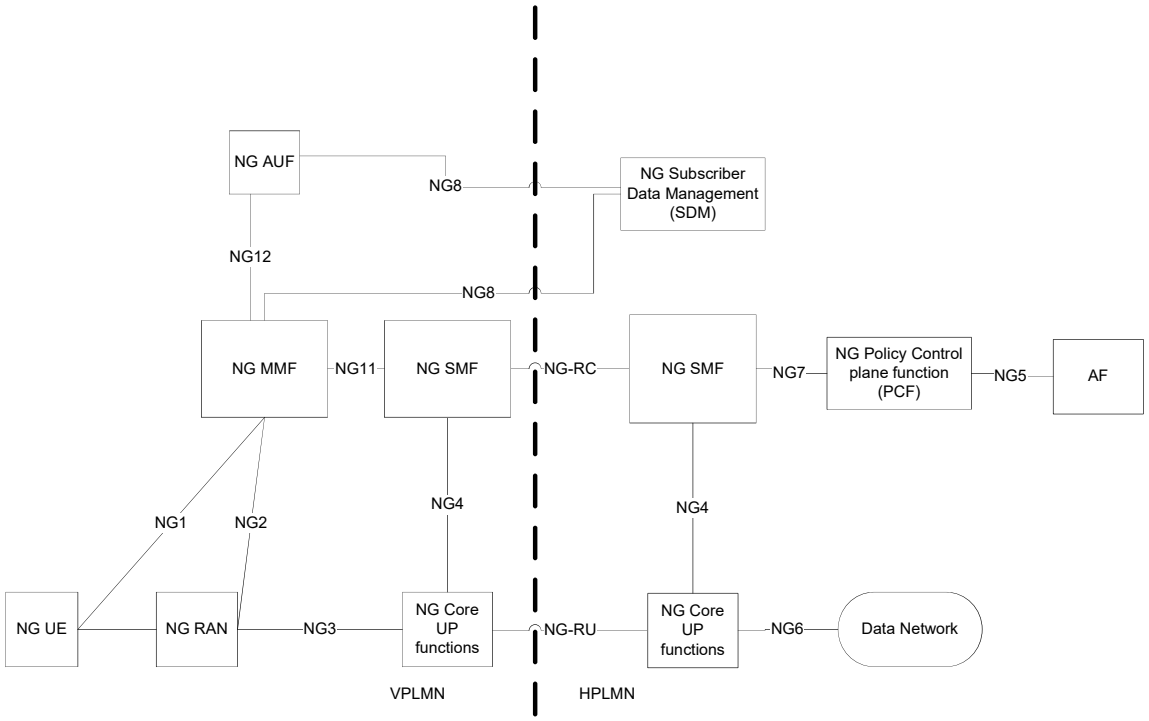


Figure 7.6.2-4: Roaming reference architecture - Home routed scenario

Following figure 7.6.2-5 depicts the roaming architecture in case of local break out scenario:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 454 of 501

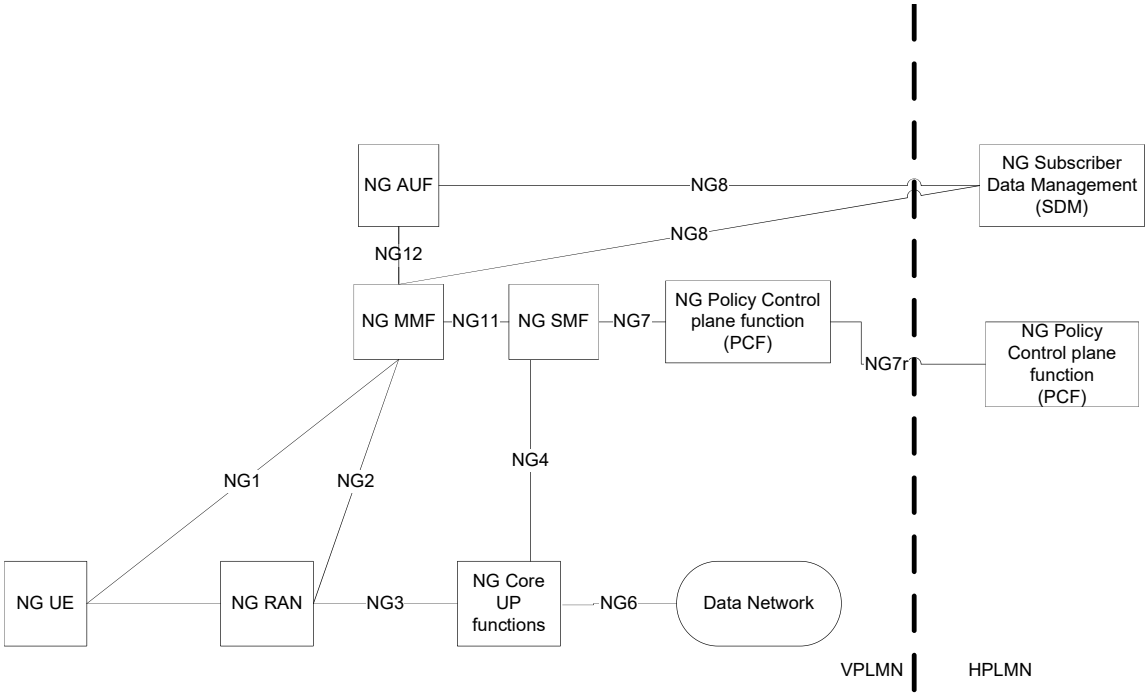


Figure 7.6.2-5: Roaming reference architecture - local breakout scenario

Editor's note: How SMF obtains subscription information is FFS as multiple options are being investigated as part of KI#4.

NOTE 1: Regardless of the number of Network functions, there is only one NAS interface instance between the UE and the CN, terminated at one of the Network functionsthat implements at least NAS security and mobility management.

NOTE 2: As an alternative, AUF (supporting SEA and SCM) and MMF can be collocated.

Editor's note: It is FFS whether NG12 needs to be a standardized reference point or whether the AUF (supporting SEA and SCM) is collocated with the MMF.

Network functions within the NG Control plane may exhibit service based interfaces for procedures that can be re-used by multiple network functions. The following figure shows how service based architecture can be supported. Each function exhibits a service interface for reusable procedures.

Editor's note: The list of procedures that can be exhibited as service is FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 455 of 501

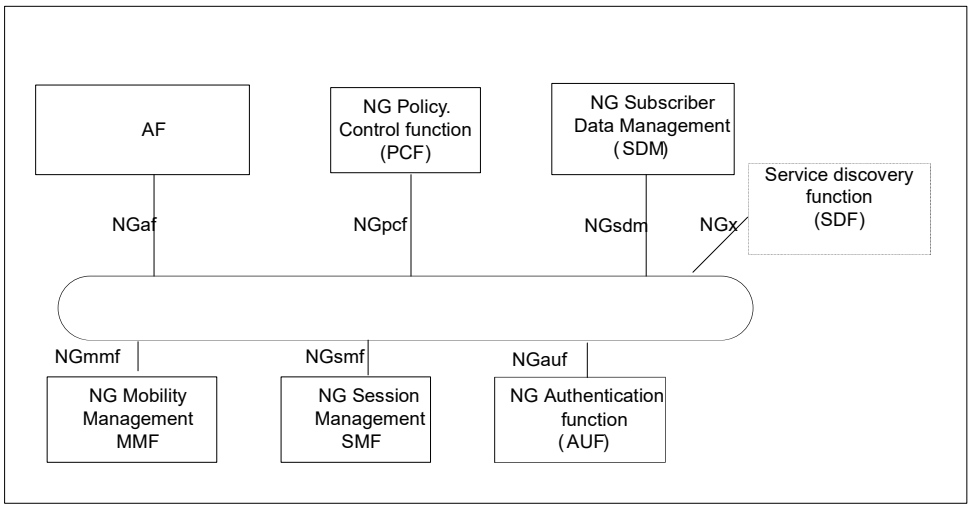


Figure 7.6.2-6: NG CP Service based architecture

Editor's note: Whether Service discovery function is an enhancement of DNS server is FFS, also need for NGx from SDF is FFS.

7.6.3 Network functions and reference points

The 5G Reference Architecture consist of the following functions:

- NG Subscriber Data Management (NG SDM)
- NG Policy Control function (NG PCF)
- NG Core Mobility Management Function (NG MMF)
- NG Core Session Management Function (NG SMF)
- NG Authentication Function (NG AUF)
- NG Core User plane function (NG UPF)
- NG RAN
- NG UE
- Data network, e.g. operator services, Internet access or 3rd party services.

The following is a high level split of functionality between the control plane and the user plane.

The NG Mobility Management function (MMF) includes the following functionality:

- Termination of RAN CP interface (NG2)
- Termination of NAS (NG1), NAS ciphering and integrity protection
- Mobility Management
- Lawful intercept (for MM events and interface to LI System)
- Transparent proxy for routing access authentication and SM messages.

The NG Authentication function (AUF) includes the following functionality:

- Access Authentication
- Derivation of keys required by other functions of NGC for serving the UE.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 456 of 501

- Security Anchor Function (SEA). It interacts with the SDM and the UE, receives the intermediate key that was established as a result of the NG-UE authentication process.
- In case of USIM based authentication, the AUF retrieves the security material from the SDM. In case of non USIM based authentication for a roamer, the AUF acts as a proxy towards the AUS which acts as an AAA authentication server.
- Security Context Management (SCM). The SCM receives a key from the SEA that it uses to derive access-network specific keys.

The NG Session Management function (SMF) includes the following functionality:

- Session Management
- UE IP address allocation & management (incl optional Authorization)
- Selection and control of UP function
- Termination of interfaces towards Policy control and Charging functions
- Policy & Charging rules handling, including control part of enforcement and QoS
- Lawful intercept (for SM events and interface to LI System)
- Termination of SM parts of NAS messages
- Data DL Notification
- Initiator of AN specific SM information, sent via MMF to NG2
- Roaming functionality
  - Handle local enforcement to apply QoS SLAs (VPLMN)
  - Charging data collection and charging interface (VPLMN)
  - Lawful intercept (in VPLMN for SM events and interface to LI System)

NOTE 1: Not all of the functions are required to be supported in a CN instance of a network slice

The NG Core User plane function includes the following functionality:

- Anchor point for Intra-/Inter-RAT mobility (when applicable)
- External PDU session point of interconnect (e.g. IP).
- Packet routing & forwarding
- QoS handling for User plane
- Packet inspection and Policy rule enforcement
- Lawful intercept (UP collection)
- Traffic accounting and reporting

NOTE 2: Not all of the UPF functions are required to be supported in an instance of user plane function of a network slice.

The NG Policy function includes the following functionality:

- Supports unified policy framework to govern network behaviour.
- Provides policy rules to control plane function(s) to enforce them.

NOTE 3: The NG PC function is assumed to retrieve subscription information from a subscription repository (UDR or SDM).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 457 of 501

The NG SDM supports the following functionality:

- Supports Authentication Credential Repository and Processing Function - This function stores the long-term security credentials used in authentication.
- Supports Authentication Server Function (AUS) - This function interacts with the AUF.
- Subscription repository.

Editor's note: Mapping of AUSF to the appropriate network function needs to be revisited.

The 5G Reference Architecture contain the following reference points:

NG1: Reference point between the UE and the NG Mobility Management function.

NG2: Reference point between the RAN and the NG Mobility Management function.

NG3: Reference point between the RAN and the NG Core User plane function.

NG4: Reference point between the NG Core Session Management function and the NG Core User plane function.

NG5: Reference point between the NG Core Session Management function and an Application Function.

NG11: Reference point between Mobility Management function and Session Management function.

NG12: Reference point between Mobility Management function and Authentication function.

NG8: Reference point between Authentication function and ASR function.

NG6: Reference point between the NG Core UP functions and a Data Network (DN).

NOTE 4: Details of NG6is beyond the scope of 3GPP.

NG7: Reference point between the NG Session Management function and the NG Policy Control function.

NG8: Reference point between the NG Mobility Management function and Subscriber Data Management or between Authentication function and the Subscriber Data Management.

NG9: Reference point between two NG Core User plane functions.

NG7r: Reference point between the V-PCF and the H-PCF.

NG-RC: Reference point between the V-SMF and the H-SMF.

NGmmf: Service based interface exhibited by MMF.

NGsmf: Service based interface exhibited by SMF.

NGauf: Service based interface exhibited by AUF.

NGpcf: Service based interface exhibited by PCF.

NGsdm: Service based interface exhibited by SDM.

NGaf: Service based interface exhibited by AF.

7.6.4 Applicable solutions

Editor's note: List the solutions from chapter 6 that are applicable to the architecture.

7.6.5 Evaluation

Editor's note: Evaluation for consolidated architecture option 6.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 458 of 501

7.7 Consolidated architecture option 7

7.7.1 General

The solutions and interim agreements of each Key Issue and architecture assumptions are considered for the consolidated overall architecture of NG system, which includes the NF granularity in the architecture, roaming support and the interaction between network functions. For the exact set of functionality supported by each NF, and the interaction between NFs, e.g. the services exposed and consumed by NFs, are left to the conclusion of the individual key issues.

7.7.2 High level principles

The following high level principles are considered in the consolidated architecture.

Support network slicing to enable diverse scenarios

- The required network functions can be configured and deployed per network slice requirement (see clause 8.2).
- Select the correct network slice for the UE based on the slice selection assistance information, and direct the UE to be served by the correct network slice.
- Support the scenario where one UE is able to access multiple network slices simultaneously.
- Allows for different network configurations in different network slices.

Allow scalability of UP and CP functions independently

- Allow for a flexible deployment of UP separate from the CP, with no restriction in the location of the UP functions (e.g. central UP locations or distributed UP locations, or any other deployment scenario).
- Support transmission of different PDU types, such as IP, Ethernet.

The finer NF granularity and direct interaction of NF to enable function flexibility:

- The function overlapping between CN NFs shall be avoided to efficiently support new services, while minimizing at the same time the impact on other NFs, flexibly adding/removing NFs based on service requirements in a network slice. The granularity of NF shall consider the guideline as indicated in Annex I.
- For the interaction between core network NFs, the NF (requester/consumer) shall be able to directly access the NF (provider) to avoid the functional and signalling impact on unrelated NFs, and the service-based interface of NF (provider) is utilized to provide its functionality to other NFs (requesters) (see clause 8.8).
- The service-based interface of an NF is independent on the communication protocol between the NFs. One general communication protocol can be utilized for the interaction between CP NFs.

NOTE 1: The legacy Reference points between two CN NFs are avoided in order to support the on-demand direct interconnection between NFs, avoid multiple reference points between NFs to be specified, and minimize the standards work load on the interaction between NFs. Instead, the service based interface is adopted, which represents the set of services provided/exposed by a given NF.

NOTE 2: The actual communication exchange protocol is specified as part of stage 3 work.

- The NF discovery function is supported to enable the direct interaction between NFs (see clause 8.8).

User plane to support diverse UP scenarios:

- A generic user plane function (UP function) is defined, which supports various user plane operations (incl. forwarding operations to other UP functions/data networks/the control plane, bitrate enforcement operations, service detection operations, etc.)

NOTE 3: The detailed list of user plane operations will be based upon the conclusions of key issues 4 and 6 (see clauses 8.5 and 8.6).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 459 of 501

- The control plane configures the UP functions to provide the traffic handling functionality needed for a session. One or multiple UP functions per session can be activated and configured by the control plane as needed for a given user plane scenario.

Unified data management

- A unified data layer is defined to manage and store subscriber data, policy data, network data and other service information in a unified data layer.

Network service exposure

- To allow network functions, operator-controlled applications and 3rd party applications to access information/services provided by the network and to customize the network capability for different diverse use cases within limits set by the operator, the NextGen system provides a suitable access/exchange of network/connectivity information (e.g. via APIs) to applications and Network Functions.

7.7.3 Reference architecture

Figure 7.7.3-1 depicts the non-roaming architecture functional view for UEs concurrently accessing a local and a central data network using multiple PDU Sessions.

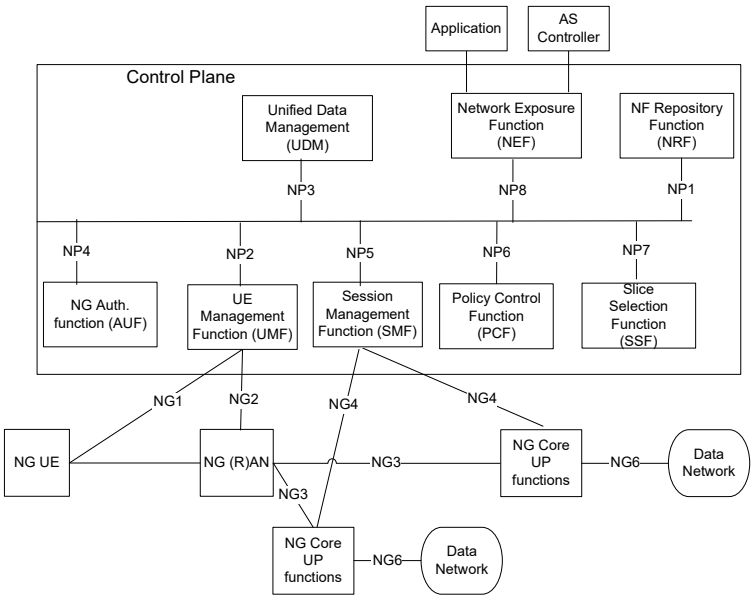


Figure 7.7.3-1: Non-roaming reference architecture

Editor's note: Whether an additional UPA-UMF NF that controls NG Core UP anchor functions is need or not is FFS.

Following figure 7.7.3-2 depicts the roaming architecture for UEs concurrently accessing a local and a home-routed data network using multiple PDU Sessions:

NOTE: In the roaming case the NF in the serving VLMN discover the NF in the HPLMN via the assistance from the NRF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 460 of 501

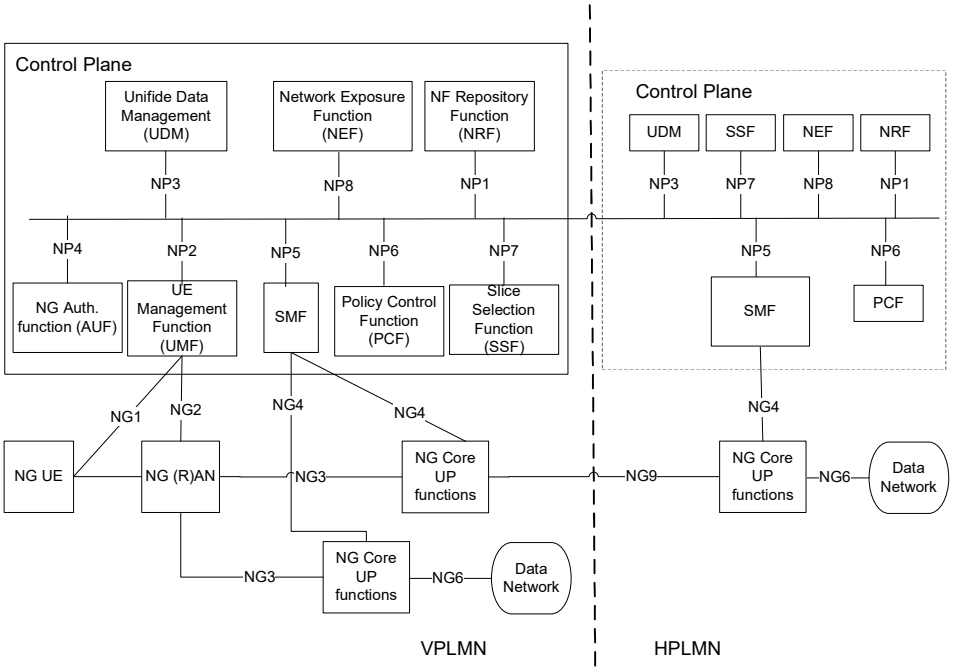


Figure 7.7.3-2: Roaming reference architecture

7.7.4 Network functions and reference points

7.7.4.1 Network functions

The NextGen system Reference Architecture consists of the following functions:

- NG Unified Data Management (NG UDM)
- NG Policy Control Function (NG PCF)
- NG UE Management Function (NG UMF)
- NG Session Management Function(NG SMF)
- NG Authentication Function (NG AUF)
- NG Slice Selection Function (NG SSF)
- NF Repository Function (NRF)
- Network Exposure Function (NEF)
- NG User Plane Function (NG UPF)
- NG RAN
- NG UE
- Data networks, e.g. operator services, Internet access or 3rd party services.

The NG UE Management function (UMF) includes the following functionality:

- Termination of RAN CP interface (NG2)
- Termination of NAS (NG1), NAS ciphering and integrity protection
- Mobility Management

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 461 of 501

- Lawful intercept

The NG Session Management function(SMF) includes the following functionality:

- Session Management
- UE IP address allocation & management
- Selection and control of UP anchor function
- Reselection of UP function and user plane path
- Policy & Charging rules handling, including control part of enforcement and QoS
- Lawful intercept

The NG Authentication function (AUF) includes the following functionality:

- User Authentication
- Maintaining the security contexts that are applicable to all security functionality for the UE, i.e. CP-CN Signalling Protection, CP-AN Signalling Protection, and User Plane Protection.

The NG Core User plane function includes the following functionality:

- Anchor point for Inter-RAT mobility (when applicable)
- External PDU session point of interconnect (e.g. IP).
- Packet routing & forwarding
- Handling traffic rules towards AS network
- QoS handling
- Packet inspection and Policy rule enforcement
- Lawful intercept (UP collection)
- Traffic accounting and reporting

NOTE 1: Not all of the UPF functionality are required to be supported in an instance of User Plane Function of a network slice.

The NG Policy Control Function (PCF) includes the following functionality:

- Supports unified policy framework to govern network behaviour.
- Provides policy rules to control plane function(s) to enforce them.

The NG Unified Data Management (UDM) supports the following functionality:

- Store the data in a unified data layer including:
  - user subscription data,
  - policy data (i.e. per UE related policy data and per application related policy data),
  - network data (e.g. UE traffic reports from UP NFs, the NF topology information in user plane for UP NF discovery and selection), and
  - service information (e.g. the user location information and UP anchor information used for handover between different access networks).
- The data stored in the unified data layer can also be used for network data exposure and data analytics.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 462 of 501

NOTE 2: The NF topology information includes network nodes hosting UP NFs and logical links connecting network nodes. Attributes of network nodes include resources reserved for UP NFs, such as input and output ports and their processing capabilities (e.g. throughput and number of supported UEs and/or PDU sessions). Attributes of logical link include, e.g. link capacity limit.

The NG Slice Selection Function (SSF) supports the following functionality:

- Determines the corresponding network slice instances that one UE is allowed to access based on the slice selection assistance information from UE, subscriber profile, etc.

The NF Repository Function (NRF) supports the following functionality:

- Maintain the deployed NF Instance information when deploying/updating/removing NF instances;
- Receive NF Discovery Request from NF instance, and Provides the information of the discovered NF instances (be discovered) to the NF instance.

The Network Exposure Function (NEF) supports the following functionality:

- Maintains the list of services provided/exposed by the network;
- As the entry function towards applications, it receive the service request from the applications including operator's application and the 3rd party application, and further interact with the corresponding NFs to provide the requested services;
- Authorization on the applications, the charging and load control on the exposed network services.

NOTE 3: The interactions between NEF and CP NFs depend on the exposed network services and are identified case by case.

NOTE 4: To allow the VPLMN and HPLMN Network Functions interact securely the message between them may go through gateway.

7.7.4.2 Control Plane service interfaces

For the interaction between core network functions, the NF provides a service-based interface to communicate with other NFs. The service interface allows the services provided by the NF to be used by other NFs. The NextGen system supports the following NF service interfaces:

- NP1: Service interface of NF Repository Function;
- NP2: Service interface of UE Management Function;
- NP3: Service interface of Unified Data Management Function;
- NP4: Service interface of Authentication Function;
- NP5: Service interface of SMF;
- NP6: Service interface of Policy Control Function;
- NP7: Service interface of Slice Selection Function;
- NP8: Service interface of Network Exposure Function;

7.7.4.3 Other Reference points

The NextGen system Reference Architecture contain the following reference points:

- NG1: Reference point between the UE and the NG UE Management Function.
- NG2: Reference point between the RAN and the NG UE Management Function.
- NG3: Reference point between the RAN and the NG User Plane Function.
- NG4: Reference point between the NG SMF and the NG User Plane Function.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 463 of 501

- NG6: Reference point between the NG User Plane Function and a Data Network (DN).
- NG9: Reference point between two NG User Plane Functions.

7.7.5 Applicable solutions

Editor's note: List the solutions from chapter 6 that are applicable to the architecture.

7.7.6 Evaluation

Editor's note: Evaluation for consolidated architecture option

8 Conclusions

Editor's note: This clause is intended to list conclusions, interim or/and final conclusions, which have been agreed during the course of the work item activities.

8.1 Interim Agreements on Key Issue #1: Network slicing

The following bullets are the current status of agreements on the network slicing:

1. The network slice is a complete logical network (providing Telecommunication Services and Network Capabilities) including AN and CN. Whether RAN is sliced is up to RAN WGs to determine.

   a) AN can be common to multiple network slices.

   b) Network slices may differ for features supported and Network Functions optimisations use cases

   c) Networks may deploy multiple Network slice instances delivering exactly the same optimisations and features as per but dedicated to different groups of UEs, e.g. as they deliver a different committed service and/or because they may be dedicated to a customer.

2. A UE may provide network slice selection assistance information (NSSAI) consisting of a set of parameters to the network to select the set of RAN and CN part of the network slice instances (NSIs) for the UE.

   a) The NSSAI can have standard values or PLMN specific values for the slice/service type.

   b) The UE may store a configured NSSAI per PLMN.

   c) If the UE stores NSSAI for the ID of the PLMN that the UE accesses, the UE provides NSSAI in RRC and NAS. The NSSAI indicates slice/service type(s), which refers to the expected network behaviour in terms of features and services. The RAN uses NSSAI for routing the initial access to a CCNF (see bullet 4 for CCNF definition).

      The UE may provide NSSAI in RRC and NAS that is complementing the slice/service type(s) further by differentiation for selecting from the potentially multiple network slice instances that all comply with the indicated slice/service type(s).

Editor's note: whether RAN uses NSSAI for purposes other than routing, e.g. select RAN behaviour, is FFS

Editor's note: whether NSSAI in RAN and NAS are exactly the same, is FFS what parameters are needed for selecting the RAN slice is for RAN

   d) If the UE doesn't store any Accepted NSSAI for the ID of the PLMN that the UE accesses, the UE provides the configured NSSAI in RRC and NAS, if the UE stores a configured NSSAI. The UE provides the NSSAI configured for the PLMN, if it has one. Otherwise, it provides a configured default NSSAI, if it has one. RAN uses NSSAI for routing the initial access to a CCNF. If the If the UE doesn't store any NSSAI for the ID (Accepted or configured) of the PLMN that the UE accesses and also no configured default NSSAI, the UE provides no NSSAI in RRC and NAS, and the RAN sends NAS signalling to a default NF.

Editor's note: whether RAN uses NSSAI for purposes other than routing, e.g. select RAN behaviour, is FFS

   e) After (initial) slice selection, attachment provides the UE with a Temp ID that is provided by the UE in RRC during subsequent accesses to enable the RAN to route the NAS message to the appropriate CCNF, as long

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 464 of 501

as the Temp ID is valid. In addition the serving PLMN may return an Accepted NSSAI that the UE stores for the PLMN ID of the serving PLMN. If the UE stores an Accepted NSSAI for the PLMN ID of the serving/selected PLMN, it indicates this one always, when NSSAI needs to be indicated.

Editor's note: what the Accepted NSSAI is specifically referring to, is FFS

f) For a "Service Request" the UE is registered/updated and has a valid temp ID, which is sufficient in the RAN to route the request to the serving Common CP NF. It is assumed that the slice configuration doesn't change within the UE's registration areas.

Editor's note: whether and how there is additional info for routing the Service Request to a serving SM-NF is FFS.

Editor's note: whether NSSAI is needed in addition may depend e.g on using it for RAN behaviour, which is FFS

g) For enabling routing of a TA update request the UE includes always Accepted NSSAI and a complete Temp ID in RRC,

Editor's note: whether Accepted NSSAI and complete Temp ID are always used by the network is FFS.

h) "SM NSSAI" that the UE shall include in the PDU session establishment Request, shall enable the selection of an SM-NF.

Editor's note: Whether this "SM NSSAI" consists of slice/service type and complementing info or something else is FFS.

Editor's note: Whether this "SM NSSAI" is used to select functions other than SM-NF is FFS.

3. If a network deploys network slicing, then it may use UE provided network slice selection assistance information to select a network slice. In addition, the UE capabilities and UE subscription data may be used.

4. A UE may access multiple slices simultaneously via a single RAN. In such case, those slices share some control plane functions, e.g. MMF, AUF. These common functions are collectively identified as CCNF (Common Control Network functions).

5. The CN part of network slice instance(s) serving a UE is selected by CN not RAN.

6. With reference to Annex D: move forward with Group B type of solution in rel-15 (Group C is subsumed under Group B). Group A is not pursued in R15.

7. It shall be possible to handover a UE from a slice in NGC to a DCN in EPC. There is not necessarily a one-to-one mapping between slice and DCN.

Editor's note: Interworking slicing with EPS is FFS

8. The UE need to be able to associate an application with one out of multiple parallel established PDU sessions. Different PDU sessions may belong to different slices.

Editor's note: it is FFS whether those are identified by DNN or SM-NSSAI+DNN. PDU session identification in a PLMN supporting network slicing may also require alignment with Key issue #4.

8.2 Interim Agreements on Key Issue #2: QoS framework

Interim agreements for Key issue #2 QoS framework are as follows:

1a. Support Reflective QoS over RAN under control of the network. The network decides on the QoS to apply on the DL traffic and the UE reflects the DL QoS to the associated UL traffic. When the UE receives a DL packet for which reflective QoS should be applied, the UE creates a new derived QoS rule. The packet filter in the derived QoS rule is derived from the (i.e. the header of the) DL packet. For traffic that is subject to Reflective QoS the UL packet gets the same QoS treatment as the reflected DL packet. It shall be possible to apply Reflective QoS and non-reflective QoS on the same PDU session.

Editor's note: It is FFS whether Reflective QoS indication is signalled via C-plane or inband.

Editor's note: It is FFS whether derived QoS rules (derived via Reflective QoS) have higher or lower precedence order compared to signalled QoS rules.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 465 of 501

Editor's note: It is FFS whether Reflective QoS can be applied for every access network connecting to the NG Core.

1b Reflective QoS can be used for non-GBR service data flows.

Editor's note: It is FFS whether Reflective QoS can also be used for GBR service data flows.

2. U-plane marking for QoS is carried in encapsulation header on NG3 i.e. without any changes to the e2e packet header.

3a. A default QoS rule shall be provided at PDU Session establishment to UE.Pre-authorised QoS rules may be provided at PDU Session establishment to UE.

NOTE 1: A pre-authorised QoS rule is any QoS rule (different from the Default QoS rule) provided at PDU Session establishment.

Editor's note: QoS related signalling to the UE for non-3GPP access is FFS.

3b. The NAS-level QoS profiles of the QoS rules provided at PDU Session establishment to the UE shall also be provided at PDU Session establishment to the RAN using NG2 signalling. QoS rules can be provided at PDU Session establishment to a NG AN based on non-3GPP access (e.g. depending on access capabilities) using NG2 signalling.

Editor's note: It is FFS whether RAN needs to be aware which QoS rule is the Default QoS rule.

3c. QoS rule consists of NAS-level QoS profile (A- or B-type), packet filters and precedence order.

3d. To a UE connected via NG RAN based on 3GPP access, the signalled QoS rules are provided using NG1 signalling. To a UE connected via NG AN based on non-3GPP access, the signalled QoS rules may be provided using NG1 signalling.

NOTE 2: In this release it is assumed that UEs that access the NextGen CN over non-3GPP access utilise the 3GPP NAS signalling.

Editor's note: The bullet 3d above is the working assumption made by SA2 and can be reviewed in case RAN groups identify a scenario where AS awareness of packet filters is required.

4. GBR SDF shall be supported in the NextGen System and QoS Flow-specific QoS signalling via the C-plane is needed for GBR SDF.

5. NG2 signalling related to QoS, outside of PDU Session establishment, corresponding to a pre-authorised QoS rule should be minimised for initiation, modification or termination of SDFs with no GBR requirements.

Editor's note: This is target for SA2, but the feasibility needs to be confirmed by RAN WG.

Editor's note: NG2 QoS related signalling for non-3GPP access is FFS.

6. NG1 signalling related to QoS, outside of PDU Session establishment, corresponding to a pre-authorised QoS rule should be minimised for initiation, modification or termination of SDFs with no GBR requirements.

Editor's note: NG1 QoS related signalling for non-3GPP access is FFS.

7a. For the purpose of subscription and service differentiation, enforcement of Max bit rate limits in UL and DL per Service Data Flow (SDF) shall be done in a CN_UP, being a trusted point of enforcement in the network. Rate limit enforcement per PDU session applies for flows that do not require guaranteed flow bit rate.

7b. Max bit rate limit (MBR) in UL and DL per PDU session is enforced in CN_UP for flows that do not require guaranteed flow bit rate. For multi-homed PDU session, the PDU session MBR is enforced in each UPFs terminating the NG6 interface . The enforcement is done separately by each of these UPFs.

Editor's note: It is FFS which type of flows the CN_UP applies "per SDF", "per PDU session" rate limitation on. It is FFS whether additional rate limit enforcement functionality is needed in the UP function.

NOTE 3: AMBR per DN name is not supported.

8. The AN shall enforce Max bit rate limit in UL and DL per UE for flows that do not require guaranteed flow bit rate.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 466 of 501

Editor's note: It is FFS which type of flows the AN applies rate limitation on.

Editor's note: How to handle UL rate limitation per UE when the UE has access over non-3GPP AN and when the UE has access over multiple ANs including 3GPP and non-3GPP ANs is FFS

Editor's note: UL Rate limitation requirements for the UE is FFS.

9. QoS Flow is the finest granularity for QoS treatment in the NG System. User plane traffic with the same NG3 marking value within a PDU session correspond to a QoS flow.

10.1.1. In the downlink the (R)AN binds QoS Flows onto access-specific resources based on the NG3 marking and the corresponding QoS characteristics provided via NG2 signalling, also taking into account the NG3 tunnel associated with the downlink packet. Packet filters are not used for binding of QoS Flows onto access-specific resources in (R)AN.

10.1.2. When passing an UL packet from (R)AN to CN, the RAN determines the NG3 QoS marking and selects the NG3 tunnel based on information received from the Access Stratum.

NOTE 4: How RAN maps QoS flows onto access-specific resources based on the NG3 marking is up to RAN WGs to decide.

10.2.1. At the upper layers the UE matches the uplink packet to a QoS rule and binds the uplink packet to the NAS-level QoS profile (A- or B-type) of this QoS rule (explicitly signalled or implicitly derived via reflective QoS).

10.2.2. When passing an UL packet from the upper layers to AS in the UE, the upper layers indicate to AS the NAS-level QoS profile (via the corresponding QoS marking), including information allowing the AS to identify the PDU Session.

10.2.3. Conversely, when passing a DL packet from AS to the proper upper layer instance in the UE, it is the AS's responsibility to select the proper upper layer instance corresponding to the PDU Session. The AS also indicates the NAS-level QoS profile (via the corresponding QoS marking) to the upper layer instance.

NOTE 5: The two bullets above do not make any assumption on the need for U-plane marking from RAN to the UE. That is up to RAN2 decision.

10.2.4. For QoS-aware applications that use DSCP marking to indicate the requested QoS in the IP packet, a packet filter including the DSCP marking in the QoS rules provided by the CN_CP may be used for the purpose of binding to a specific QoS marking.

Editor's note: It is FFS how to prevent potential abuse of DSCP marking by the applications in the UE (e.g. applications in the UE always using the highest DSCP marking).

10.3. In case RAN decides that there is flexible (e.g. other than 1:1) mapping between NAS-level QoS profile and AS-level QoS, this mapping is transparent to the upper layers and has no impact on the NG3 marking. It is assumed that the access stratum will comply with the QoS characteristics associated with the NAS-level QoS profile.

NOTE 6: It is up to RAN to define the AS-level QoS of DRBs and how uplink and downlink packets (with the associated QoS profile (A- or B-type) and the associated PDU Session information) are mapped to DRBs. It is noted that SA2 does not specify APIs between the upper layers and the AS. The use of terms such as "passing between upper layers and AS" is there only to clarify the responsibilities between SA2 and RAN2.

11. Some User plane QoS markings are scalar values that have standardized QoS characteristics (referred to as A-type QoS profile).

12. Some User plane QoS markings are scalar values that point to dynamic QoS parameters signalled over NG2 (referred to as B-type QoS profile).

NOTE 7: The value of the QoS marking indicates the type of associated QoS profile (A- or B-type).

13. QoS parameters may include the following:

    a. Maximum Flow Bit Rate.

    b. Guaranteed Flow Bit Rate.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 467 of 501

c. Priority level.

d. Packet Delay Budget.

e. Packet Error rate.

f. Admission control.

NOTE 8: Parameters c, d), e) apply for both bullets #11 and #12. Parameters a), b), f) apply only to bullets #12.

NOTE 9: Need for other parameters such as packet jitter is FFS.

Editor's note: Whether Priority Level is used for more than scheduling purpose is FFS.

Editor's note: It is FFS which of the parameters listed above need to be signalled to the UE.

14. QoS framework does not assume the need for NG3 tunnel per QoS flow.

15. For non-guaranteed bit rate QoS flows corresponding to pre-authorized QoS rules, the UE sends UL traffic without any further NG1 signalling.

Editor's note: How the UE indicates the QoS level is FFS.

16. UE triggered QoS establishment for guaranteed bit rate QoS flows is based on explicit UE-requested QoS over NG1.

8.3 Interim Agreements on Key Issue #3: Mobility management

Interim agreements for CN/NAS state model on Key issue #3 Mobility Management are as follows:

1. A single MM state model shall be specified consisting of

   - An MM De-registered state, in which the UE is not attached to the network; and
   - An MM Registered state, in which the UE is attached to the network. While MM Registered, the UE may be either:
     - in a CN Idle state, in which the UE may only be tracked at CN location area level and may achieve at least a comparable power efficiency to that of LTE's ECM IDLE state; or
     - in a CN Connected state, in which the UE location is known on the level of the serving RAN node.

2. NextGen Core shall be able to optimize the MM procedures of a UE within the single MM state model.

3. RAN2 is expected to define means for a UE in MM Registered CN Connected state not transmitting or receiving data to achieve a comparable power efficiency to that of a UE in CN Idle state.

4. The network shall be able to control whether a UE in MM Registered/CN Connected state uses handover or cell reselection.

5. UE and core network shall at least support tracking area list as registration area.

Interim agreements for mobility on demand are as follows:

Interim agreements for mobility on demand aspects related to mobility restrictions are as follows:

1. The subscription data may include information which can be used to determine the UE mobility restrictions.

2. UE mobility restrictionsare determined by core network based on information such as UE subscription, UE capabilities, UE location, and/or network policies.

Editor's note: What UE capabilities, if any, that are used to determine UE mobility restrictions is FFS.

3. UE mobility restrictionscan be changed due to, e.g., subscription, location, and/or policy change. In addition, UE mobility restrictions can be updated during a mobility management procedure.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 468 of 501

4. Mobility pattern a.k.a mobility level need not be defined as a parameter that is signaled via standardized interface.
5. The mobility pattern is a concept used by the core network to characterize the expected UE mobility.
6. The core network can determine mobility pattern based on following information, e.g.:
   A. UE subscription, e.g. the size of mobility restriction area;
   B. Network policies, e.g. the criteria to quantify mobility pattern;
   C. Statistic UE mobility information, e.g. historical/predictable UE moving trajectory; and/or
   D. UE assisted mobility information, including UE location, UE capabilities, etc.
7. UE mobility pattern can be used by the core network as an input to optimize mobility support provided to the UE, e.g.:
   A. Optimizing the allocating CN registration area list;
   B. Optimizing UE mobility restriction area provided to the UE (if mobility restrictions to be applied for the UE);
   C. Selecting UP functions;
   D. Determining whether to keep the UE in CN_CONNECTED mode;
   E. Determining the CN assisted information to help RAN level paging.

Editor's note: The details of the CN assistance for RAN paging will be developed in coordination with the RAN WGs

Editor's note: If per-Node level NG3 tunnel is supported, it is FFS whether UE mobility pattern needs to be considered to determine the tunnel type, i.e. per-Node or per-Session tunnel.

Interim agreements for mobility restrictions are as follows:

1. For the mobility restriction "area" aspects, the following applies:
   A. The core network may configure an "allowed area", "non-allowed area" and "forbidden area" to a UE. At least a granularity of these areas per the TA level is to be supported.

Editor's note: Whether finer granularity than per TA level is to be supported is FFS.

   B. In an "allowed area", the UE is permitted to initiate communication (using CP and UP) with the network as allowed by the subscription.

Editor's note: How allowed area relates to the core network registration area is FFS.

   C. In a "forbidden area", the UE is not permitted to initiate any (neither CP nor UP) communication with the network.

Editor's note: Whether the UE will respond to core network paging is FFS.

   D. In a "non-allowed area" the UE is not allowed to initiate Service Request or SM signalling to obtain user services, but even in "non-allowed" area, the UE will perform periodic registration update signalling (due to periodic registration update timer expiration) and regular registration update (due to mobility outside of the TAI list).

Editor's note: Whether the UE will respond to core network paging is FFS.

NOTE 1: How to minimize registration updates due to mobility within a "non-allowed area" is to be determined during normative phase.

   E. If the UE has been provided with overlapping areas then the following applies for the UE logic:
      1. The evaluation of forbidden area has precedence over the evaluation of allowed area and the non-allowed area.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 469 of 501

2. The evaluation of non-allowed area has precedence over the evaluation of allowed area.

F. A UE accessing the network for regulatory prioritized services like Emergency services and MPS overrides any "non-allowed area" and "forbidden area" restrictions.

2. It has been agreed to specify a geographic subscription parameter to restrict the (service) area within which a UE (e.g. for fixed access) may obtain services from the network.

Interim agreements for reachability and MO only are as follows:

1. Based on UE indicated preferences, UE subscription data and network policies, or any combination of them, the NG CN determines whether MO only mode is applied for the UE and indicates it to the UE during registration signaling. The UE and core network re-initiates (or exits) the MO only mode at subsequent registration signalling.

2. A UE in MO only mode is characterized by the UE performing periodic registration (with potentially a very long periodic registration timer), but not listening to CN paging.

NOTE 2: Even for periodic registration the UE needs to ensure that the UE is properly registered.

3. The core network does not attempt to page a UE in MO only mode and hence the UE is only reachable from the core network when the UE initiates communication during the time the UE stays in CN connected mode.

Editor's note: For a UE in CN idle, it is FFS whether MT data is stored/buffered in the core network, and whether additional functionality e.g. equivalent to an active time is required.

4. For a UE in MO only mode the core network determines the frequency of periodic registration.

NOTE 3 : The network may need to track the device e.g. due to the need to track a stolen UE. The UE behavior and configuration from the network when tracking is needed is FFS.

Interim agreements for Mobility Management Parameters and their usage:

1. Table 8.3-1 shows a guidance on what Mobility Management parameters are to be specified, how they are determined, used and by which entity.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 470 of 501

Table 8.3-1

Parameter Name	Content	Example Possible values (*)	How/Where is used, who provides value and which procedures are affected by parameter (*)
Mobility Pattern (a.k.a. UE Mobility Level in some solutions)	Expected UE mobility.	- TBD	- Provided by: - Subscription assisted (e.g. via Mobility Restriction), Policy Function assisted, optionally UE assisted, Statistics captured in CN. - Used in: - Any decision where mobility pattern might be useful. - Affects triggering of procedure: - FFS.
UE Mobility Restriction	Defines different types of allowed communication per area.	- Allowed: Signaling/Data - Non-allowed: MM Signaling only without Service Request. EMC and MPS is allowed. - Forbidden: only EMC and MPS is allowed.	- Provided by: - CN to UE and RAN in connected mode. - Input possible from SDM and possibly adjusted by NG PCF - Used in: - UE to apply allowed type of communication - CN and RAN to enforce. - Affects triggering of procedure: - Service request and SM signaling, - MM signaling.
UE Reachability (Paging and idle mode parameters, MO only)	When, Where and How the UE needs to become reachable for MT data or NW originated CP procedures.	- When: Paging windows, No UE reachability (MO only).	- Provided by: - UE may indicate preference, CN provides to UE and RAN final values - Used in: - UE, CN and RAN. - Affects triggering of procedure: - Regular TAU. - Paging
UE Registration Keep-Alive Timer – Periodic TAU.	Timer for UE to update registration if no signaling has occurred.	- 0 (no need for keep-alive) to months?	- Provided by: - CN to UE (UE may request preference) - Used by: - UE to trigger registration keep-alive. - CN to implicitly detach after safeguard time - Affects triggering of procedure: - Periodic TAU.
(*): These columns are meant as guidance and to reach a common understanding. The detailed interim agreements of each parameter are captured separately in this section.			

Interim agreements on paging area management:

1. Depending on MM state, CN paging or RAN paging may be used.
2. At least for CN paging, existing Tracking Area concept should be baseline of NG system.

Editor's note: The applicability of cell list for CN paging area handling is FFS.

3. For RAN pagingCN may provideassistance information to AN.

Editor's note: The necessity and the detailed procedure of RAN paging is RAN WG decision.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 471 of 501

Interim agreements for UE reachability management are as follows:

1. The RAN-level paging maybe triggered by RAN while UE is in CN-CONNECTED mode.
2. Upon successful registration, the network may keep the UE in CN-CONNECTED mode.
3. The NW decides on which mobility procedure (e.g. paging) should be used or not based on received preferences from the UE on requested features, and also based on subscription and local policy.

8.4 Interim Agreements on Session management and Service Continuity (Key Issue #4, 5 and 6)

Interim agreements on Session Management and Service Continuity (Key Issue #4, 5 and 6) **are as follows:**

1. The NextGen system shall support an UE establishing multiple separate PDU sessions, to the same data network or to different data networks, via 3GPP and Non-3GPP access networks at the same time In this case each PDU session is routed over only a single access network. The choice of the access to use for a PDU session is based at least on network policy, service requirements and user subscription

NOTE 1: Support of WLAN integrated at RAN level is under RAN responsibility, and CN related aspects will be considered as needed based on RAN decision

NOTE 2: The definition of policy for selecting the access to route the PDU Sessions (e.g. service requirements, user subscription, etc) and how it is usedare FFS

2. The NextGen system should support PDU sessions to the same data network where the traffic of a PDU session can be simultaneously carried over multiple access, and where one access is a 3GPP access and the other is a non-3GPP . The support will be handled in phase 2.

NOTE 3: The definition of policy for selecting the access where to route the traffic of the PDU Session (e.g. service requirements, user subscription, etc) and how it is usedare FFS

3. The NextGen system should support the ability to have multiple PDU sessions to the same Data Network and served by different UP functions terminating NG6.
4. The User Plane format in NextGen on NG3 and between UP functions shall at least support per PDU Session tunnelling, as described in clause 6.4.10. This applies to both non-roaming and roaming UP interfaces.

Editor's note: The granularity of the tunnelling for non-3GPP accesses is FFS.

Editor's note: Whether an additional tunnelling granularity variant will be supported for stationary UEs is FFS.

4. The following PDU session types are supported: IPv4, IPv6, Ethernet, Unstructured.
5. As the same set of features and use cases may not be applicable to both IPv4 and IPv6 (e.g. multi-homing, access to local network etc) it is beneficial to treat IPv4 and IPv6 separately in NextGen CN. Therefore, for the first normative release, PDU sessions for PDU type IP shall contain only one IP version. This implies:
   - The NGC supports dual Stack UEs by using separate PDU sessions for IPv4 and IPv6.
   - The NGC does not support dual stack PDU Session (PDU Session type IPv4v6).

NOTE 4: To support interworking with EPC the same solution as was used for interworking between Gn/Gp and S5 can be used, i.e. by using single-stack PDN Connection in EPC for the UEs that may move to NextGen core.

6. A UE may ATTACH to the network without requiring the establishment of any PDU Session.
7. For the 3GPP access the user plane path in the NextGen core consists of user plane Functions (UPF). The number of UPFs for a PDU Session is not imposed by the specification but phase 1 specifications shall support at least deployments with one single UPF used to serve a given PDU session.

NOTE 5: Deployments with one single UPF used to serve a PDU session do not apply to the Home Routed case.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 472 of 501

8. For UE with multiple PDU sessions there is no need for mandatory "convergence point" similar to the SGW. In other words, going out of the AN, the user plane paths of different PDU Sessions (to the same or to different DNN) belonging to the same UE may be completely disjoint. This also implies that for idle mode UEs (if NextGen IDLE state is supported) there can be a distinct buffering node per PDU Session.

Editor's note: this may be revisited based on conclusions on Key Issue 2 on QoS about AMBR enforcement.

9. In case of deployments with SM PDU session control in the HPLMN, for one PDU session

   a. a SMF entity in the serving PLMN and a SMF entity in the HPLMN are involved.

   b. at least an UPF in the serving PLMN and at least an UPF in the HPLMN are involved.

Editor's note: it is FFS whether NAS SM signalling is terminated in the VPLMN or in the HPLMN. The VPLMN may have to reject PDU sessions from the UE e.g. due to overload control.

Editor's note: Whether this may apply to LBO is FFS.

10. In order to facilitate the introduction by a HPLMN of new features for PDU sessions, NGC specifications shall support deployments with SM PDU session control in the HPLMN where only the HPLMN is responsible of enforcing (service delivery) and controlling (e.g. subscription check) some parameters (e.g. related with the service on NG6) of the PDU session:

   - This means that the SMF in VPLMN is not meant to understand some of the information exchanged between the UE and the network in NAS signalling but relays it transparently to the SMF in HPLMN. The SMF in HPLMN is responsible to check whether via this NAS information transparently relayed by the SMF in VPLMN is compliant with the user subscription.

   - the SMF in the VPLMN is nevertheless assumed to understand some of the NAS information related with a PDU session for deployments with SM PDU session control in the HPLMN.

Editor's note: It is FFSS if the decision of whether the session is to be handled in LBO or HR mode is taken by the V-SMF or the H-SMF (e.g. based on the DNN).

   - the SMF in the VPLMN needs to handle and to check wrt roaming agreements QoS requests from the SMF in HPLMN.

11. For home routed traffic, a UPF in the VPLMN is allocated to support the PDU session. As an example, this is to enable routing of the traffic of a PDU session between the HPLMN and the VPLMN, to minimize the impact on the HPLMN of the UE mobility within the VPLMN (for scenarios where SSC1 is applied), and to avoid requiring for idle mode UEs (if NextGen IDLE state is supported) that the UPF in the HPLMN acts as buffering node for the PDU Session.

12. The establishment of a PDU Session may be authorized/authenticated by an external DN via the SMF.

Editor's note: the extent of specification work in 3GPP to enable such authorization/authentication is FFS and depends on SA3 work.

Editor's note: The interaction between the NGC and external Data Networks needs to be specified by 3GPP to provide transport of signalling for PDU session authorization/authentication by the external Data Network.

13. The principle of the SSC modes described in section 6.6.1 is endorsed with following additions:

   A Principles described in Sub-clause 6.6.1.2.4: "CN-prepared PDU Session modification followed by notification to UE (SSC mode 3)" is only endorsed for IPv6 traffic.

   B Sub-clause 6.6.1.2.6 is not endorsed.

Editor's note: It is FFS how to support interactions between SSC mode 1and multi homing

NOTE 6: For SSC mode 3, when an UE has been notified that a new user plane path has been established, the UE behavior wrt existing application flows is not specified in Rel-15.

Editor's note: What these principles are will be further clarified

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 473 of 501

14. The principle of the Uplink Classifier described in section 6.5.2 is supported for PDU sessions of type IP or Ethernet.

Editor's note: What these principles are will be further clarified

15. The principle of the multi homed PDU sessions described in section 6.4.13 is endorsed for IPv6 traffic

Editor's note: What this principle is will be further clarified

NOTE 7: For PDU session set-up in SSC mode 1, in case Uplink Classifier applies, the network has to take care to not change the local IP address.

Interim agreements for MM and SM interaction are as follows:

1. A single NG1 NAS connection is used for both MM and SM-related messages and procedures for a UE. The single NG1 termination point is located in MM.

Editor note: This is applied for UE only registered via 3GPP access. The case of UE registered via non-3GPP is FFS.

2. The MMF and SMF are separate NFs (Network Function), with a standard NG11 interface specified in-between. MMF handles the Mobility management part of NAS signalling exchanged with the UE. SMF handles the Session management part of NAS signalling exchanged with the UE

Editor's note: "MMF" and "Mobility Management" naming may be changed to a more access independent name such as "AMF" and "Access and Mobility control Function".

3. A UE with multiple established PDU sessions may be served by different instances of SMF. The MMF selects the SMF functions for the PDU sessions. MMF may select different SMF functions for different PDU sessions.

Editor's note: It is FFS whether, in case of roaming, the MMF selects both the SMF in the VPLMN and the SMF in the HPLMN, or whether the SMF in the VPLMN selects the SMF in the HPLMN.

4. MMF forwards SM related NAS information to the SM function.

5. Upon successful PDU session establishment, MMF stores the identification of serving SM function(s) of UE and SMF stores the identification of serving MM function of UE. The MMF is not expected to maintain any additional session context information. The MMF is not required to be aware of the content of SM NAS message.

6. NextGen system supports the independent activation/deactivation of UE-CN user plane connection per PDU session.

NOTE 8: The criteria to deactivate UE-CN user plane connection is up to RAN WGs decision.

Editor's note: The exact impact of such mechanism on the MM and SM procedures are FFS.

7. The SMF(s) supports the end-to-end control functions on PDU sessions (including any NG4 interface to control the UPF(s)),

8 (when multi-slicing per group B applies) In case of an UE served by multiple slice instances there are multiple instances of SMF that serve the UE.

Editor's note: it is FFS whether a single SMF is present in each slice, or whether multiple SMFs can serve one UE in a slice instance.

9 NG2 signalling related with UE is terminated in the MMF i.e. there is an unique NG2 termination for a given UE regardless of the number of PDU sessions (possibly zero) of a UE.

10 NAS MM messages and NAS SM messages and the corresponding procedures are decoupled, so that the NAS routing capabilities inside MMF can easily know if one NAS message should be routed to a SMF, or locally processed in the MMF. It is possible to transmit an SM NAS message together with an MM NAS message.

NOTE 9: Whether this implies encapsulating the SM NAS message in an MM NAS message or not is FFS and should be defined at stage 3.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 474 of 501

10 MMF can decide whether to accept the MM part of a NAS request without being aware of the possibly concatenated SM part of the same NAS signalling contents.

11 Some NG2 signalling (such as Hand-Over related signalling) may require the action of both MMF and SMF. In such case, the MMF is responsible to ensure the coordination between MMF and SMF

This may corresponds to following interactions:

NG2 impacts of SM events:

a. At the set-up / modification / release of a PDU session: the SMF interacts with RAN via the MMF for setup, modification and release of radio and NG3 resources for the PDU session.

b. At the set-up/modification of QoS for GBR flows or modification of QoS rules for non-GBR flows, the SMF interacts with the RAN via the MMF to provide the QoS information.

Impacts of MM events:

a. At the transition from IDLE to CONNECTED: the SMF interacts with RAN via the MMF for setting up of radio and NG3 resources for the PDU session.

b. During a Hand-Over : the SMF interacts with MMF at least to receive from the RAN the NG3 DL information.

NOTE 10: The interaction information between MMF and SMF in Handover procedure depends on the detail handover solution discussed in mobility management key issue.

c. When the UE becomes IDLE, MMF notifies SMF(s) in order for SMF(s) to modify the settings for DL data forwarding in the NGUP(s) for NG3.

d. When it is made aware by the NGUP that some DL data has arrived for an UE in IDLE mode (and the UE is not known to be in a power saving state), the SMF interacts with the MMF in order to trigger UE paging from the AN (depending on the type of AN).

Editor's note: Precise details of the interaction for paging depend on the definition of paging mechanisms for the NextGen system.

e. The SMF may need to interact with MMF in order to be able to control the NGUP(s) based on the power saving state of the UE.

f. When UE sends (non periodic) TAU request to MMF, the MMF may need to notify SMF(s) so that the SMF(s) can determine whether User Plane Function relocation is required or not (based on SSC mode and on the new user location).

12 The SMF needs to receive the permanent user identity of the UE.

13 When SMF needs to send NAS SM signalling to an UE, it provides information allowing the MMF to retrieve the corresponding UE NAS signalling context.

8.5 Void

8.6 Interim Agreements on Key Issue #6: Support for session and service continuity and efficient user plane path

The following bullets are the current status of agreements on key issue 6:

1. It shall be possible for the operator to provision the UE with SSC Mode Selection Policy (SSCMSP). This policy can be used by the UE to determine the type of SSC mode associated with an application or group of applications. When an application requests data transmission (e.g. opens a network socket) and the application itself does not specify the required SSC mode, the UE determines the SSC mode associated with this application by using the SSCMSP and:

   a) If the UE has already an active PDU session that matches the SSC mode associated with the application, then the UE routes the data of the application within this PDU session unless other conditions in the UE do not

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 475 of 501

permit the use of this PDU session. Otherwise, the UE requests the establishment of a new PDU session with an SSC mode that matches the SSC mode associated with the application.

Interim agreement for Key Issue #6 Support for session and service continuity and efficient user plane path are as follows:

1. The UP function selection and reselection is performed by the session management function:
2. The UP Function is selected/reselected based on any combination of the following factors (non-exhaustive):
   - UE location;
   - UE subscription profile in SDN;
   - SSC mode selected for the PDU session ;
   - Data Network Name;
   - UP function load.

8.7 Interim Agreements on Key Issue #7: Network function granularity and interactions between them

Interim agreements for Key issue #7 "Function Granularity and Interconnection of them" are as follows:

1. Any two NFs interacts with each other directly while avoiding the functional and signalling impact on unrelated NF.

NOTE 1: This does not preclude to pass information via a third NF if two NFs do not interact directly, e.g. if MM received subscription information from SDB then it can pass it to SM if there is an interaction between MM and SM (e.g. during PDU connection establishment procedure).

2. In order to facilitate utilization of the capability (s) of one NF the capability (s) of NFs are exposed as a service to other NF, wherever applicable, (e.g. by following the guidelines defined in Annex E). As such the NF provides a service based interface to other NFs.

NOTE 2: It is expected that SA2 will specify the services and functionalities that one NF supports, and CT WGs define the data model of service interface, i.e. information elements included in service interface.

NOTE 3: To support different variants of a service and to enable the invoking NF to discover the expected service, the service need be uniquely identified.

3. The feasibility to expose NF capabilities as service will be evaluated on a case by case basis when specifying each procedure. The service based interfaces should be considered for the interconnection between CN CP NFs. The NG1, NG2, NG4 interface are not considered to support the service based interface.
4. The NF selection and discovery shall be supported to enable NF selection and discovery, including:
   - The NF selection and discovery function maintains the function profile of the deployed NF instances, e.g. the type of the NF.
   - When deploying/removing one NF instance, the information of the NF instance is updated.
   - One NF shall be able to utilize NF type and other service parameters to discover the expected NF instance (s), and the NF selection and discovery function provides the IP address or the FQDN of NF instance(s) to the NF.

NOTE 4: whether it utilizes the NF Repository function or an enhancement of the DNS server to reach this functionality is left for CT WG to determine.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 476 of 501

8.8 Interim Agreements on Key Issue #8: Next Generation core and access - functional division and interface

8.8.1 Interim Agreements on functional split between AN and CN

The following table documents the current status of agreements on the CN-RAN functional allocation:

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 477 of 501

Table 8.8.1-1: Logical function allocation

Location: / Function:	NextGen RAN	NextGen CN	Comments
Key Issue #1 - Network Slicing			
CN instance selection when UE attach to a CN network slice	FFS	FFS	
Key Issue #3 - Mobility Management			
Mobility management control, (Subscription and Policies)		X	
Determination of mobility restriction		X	
Roaming restrictions execution		X	
Mobility restrictions execution, [CN Connected]	X		
Mobility restrictions execution, [CN Idle]		X	It is expected that the RAN design will enable minimization of CN-initiated paging and UE associated CN/RAN signaling
UE registration		X	
Area tracking	FFS	X	The need for RAN level area tracking is for RAN WGs to determine.
UE unreachability detection		X	Assumed to be supported in CN for UEs in CN Idle state.
RAN UE unreachability detection	X		Assumed to be supported in RAN for UEs in RAN Inactive state. If RAN inactive state exists.
NAS state transitions		X	
RRC state transitions	X		
Paging initiation and control in RAN Inactive state	X		RAN Inactive state is RAN state that corresponds to CN connected state. If RAN inactive state exists.
Paging initiation in CN Idle state		X	
Access Stratum UE Context storage in RAN Inactive state	X		If RAN inactive state exists.
Control of connected state mobility	X	X	
UP buffer for UE in CN Idle state		X	
UP buffer for UE in RAN Inactive state	X		If RAN inactive state exists.
Key Issue #4 - Session Management			
PDU Session address allocation		X	FFS for non-IP PDU Sessions
PDU Session Termination Point		X	Note that this refers to the ownership of the specification for the function supporting the termination point. In a NW deployment this function may be deployed on or close to a RAN site.
Session Management		X	
Termination of UP security	FFS	FFS	FFS
Subscription Data Handling (incl. default QoS profile)		X	
Key issue #12			
Authentication and Key Agreement		X	
Key Issue #2 QoS			
Radio Resource Admission Control	X		
Radio Resource management (QoS attributes)	X		Packet scheduling with regards to resource utilization and availability (RRM)
Max rate control	X	X	Maximum bitrate policing in the CN and RAN in UL and DL.
QoS Policy Control		X	
Transport marking	X	X	Used for prioritization in the transport network.
Charging Data Collection		X	
Packet classification of DL packets for QoS differentiation on the Radio	FFS	FFS	Some companies think the QoS classification for QoS differentiation of DL packets is performed in RAN.
QoS differentiation and verification for UL packets	FFS	FFS	Some companies think the QoS verification for UL packets is performed in RAN and/or CN.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 478 of 501

8.8.2 Interim Agreements on common AN-CN interface

The following list contains the current agreements on the common AN-CN interface:

1. Non-3GPP accesses are either embedded into the NextGen RAN (referred to as "non-standalone" non-3GPP accesses) or are deployed outside the NextGen RAN (referred to as "standalone" non-3GPP accesses).

2. The "non-standalone" non-3GPP accesses are outside the scope of this TR. The stage-2 aspects of "standalone" non-3GPP accesses are in the scope of this TR shall be defined by SA2.

3. A standalone non-3GPP access may support both trusted and untrusted non-3GPP accesses. However, currently only untrusted non-3GPP accesses are considered. Trusted non-3GPP accesses will be considered at a later phase of this work.

4. The NG2/NG3 interfaces are used to connect the standalone non-3GPP accesses to CP functions and UP functions respectively.

5. In this release it is assumed that UEs that access the NextGen CN over non-3GPP access utilize the 3GPP NextGen NAS signalling.

6. The following high-level architecture is used for standalone untrusted non-3GPP accesses. The details of this architecture will be specified in this TR. The name of N3IWF may need to change.

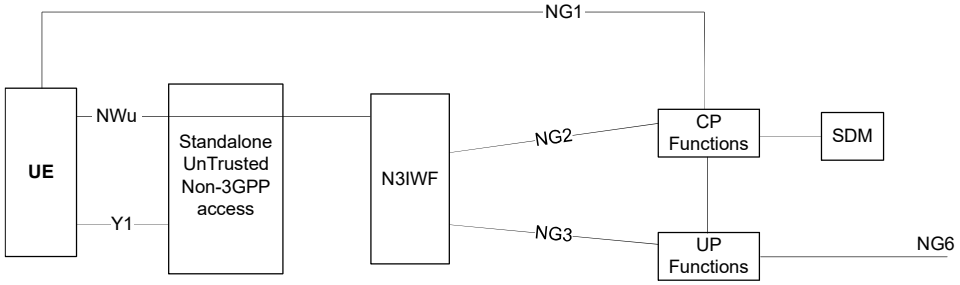


Figure 8.8.2-1: High-level architecture for standalone untrusted non-3GPP accesses

7. Over untrusted non-3GPP access:

   a) The UE discovers and selects the N3IWF with the similar procedure as the ePDG selection in TS 23.402 [17].

   b) The UE uses IKEv2 to establish an IPsec tunnel with the selected N3IWF. During this IPsec tunnel establishment the UE is authenticated to the NextGen CN via NG2.

   c) After authentication, NAS messages are exchanged between the UE and CP functions via the established IPsec tunnel and via NG2. The N3IWF transparently forwards the NAS messages via NG2.

   d) IKEv2 and IPsec are used on the interface between the UE and the N3IWF but additional protocols may be specified if needed.

   e) Regardless how many PDU sessions the UE has, there is only one IKE security association between the UE and N3IWF.

8. Open issues for untrusted non-3GPP access:

   a) Details of the Attach procedure: (a) NAS messages in EAP packets, (b) NAS messages in IKEv2 packets, (c) interworking between IKEv2 and Attach, (d) NAS Attach sent over IP after initial UE authentication at IPSec tunnel establishment.

   b) The user-plane model.

   c) For the control-plane, identify if there is need for a 3GPP-defined protocol between UE and N3IWF.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 479 of 501

8.9 Interim Agreements on Congestion and Overload Control

Interim agreements for congestion and overload control are as follows:

1. This work will be handled during the normative phase. The CP function should support congestion and overload control to prevent mobility management and session management signalling requests from UEs.

Editor's note: Which other criteria (e.g. per network slice instance, per DNN, per group, per the service type, etc.) need to be considered for congestion and overload control is FFS.

Editor's note: The interaction with access control functionality to prioritize the services is FFS.

8.10 Interim Agreements on Key Issue #10: Policy Framework

In the interim agreements below the PCC Framework refers to the Policy and Charging Control defined in EPC. The interim agreements below are subject to updates to cover all the topics listed in the WT list.

Interim agreements on the Policy Framework key issue:

1. The PCC framework defined in TS 23.203 is generic and the relevant parts is applicable to NextGen, including:

   a. The PCC Framework in NextGen includes the following Functional elements: The NG Policy Function that interfaces to the Session Management, the Application Function, and the Online Charging System.

   b. The NG Policy Function evaluates operator policies that are triggered by events received from the Application Function, the Session Management, and the Online Charging System.

   c. The NG Policy Function provides Rules for application and service data flow detection, gating, QoS and flow based charging to the Session Management.

NOTE 1: NextGen provides a PDU connectivity service of different PDU types, the existing PCC framework is applicable to PDU sessions of IP Type only.

NOTE 2: Credit management and reporting are to be defined in SA5 specification.

Editor's note: additional interim agreements, e.g. for extensions to the existing PCC framework, are FFS.

8.11 Interim Agreements on Key Issue #18

8.11.1 Interim Agreements on EPC-NextGen Core interworking

Interim agreements for Key issue #18 EPC-NextGen Core interworking are as follows:

- The standard defined for mobility procedures from NG Core to EPC shall be able to support "single radio/single attach" UEs and achieve minimal service disruption.

Editor's note: Whether similar mobility procedures for "single radio/single attach" UE will be defined for mobility from EPC to NG Core to support the SA1 requirement for minimal disruption is FFS.

- Support for these procedures in the network is optional and is based on network capabilities.

Editor's note: Whether support for the procedures in the UE is mandatory or optional is FFS. For example, only UEs requiring support for service continuity (e.g. voice centric UEs) and/or IP address preservation may need to support them, while others may not,

- Common UP anchor is required for IP address preservation.

- A common subscriber database (similar to HSS) is used between EPC and NG Core.

- The standard shall support a source to target CN interface to transfer certain context between MME and CP Function of NG Core.

Editor's note: The MME to CP Function interface in NG Core is named as NGx and its procedures are FFS.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 480 of 501

8.11.2 Interim Agreements on option 3 to NG Core migration

It is agreed to select solution 18.3 for migration from E-UTRAN/EPC including option 3 to NG Core options. RAN related aspects of migration e.g. related to RRC or user plane will be addressed by RAN WGs.

8.12 Interim Agreements on the Overall Architecture

8.12.1 Architecture principles

Key architecture principles:

- Separate the UP and CP functions, allowing independent scalability and evolution.
- Allow for a flexible deployment of UP and CP functions, i.e. central location or distributed (remote) location.
- Modularize the function design, e.g. to enable flexible and efficient network slicing.
  - Supporting unified authentication framework for UEs which may support only subset of NGS functionality (e.g. not supporting mobility).
  - Separated mobility management and session management. Separated MM and SM enables independent evolution and scaling.
- Support a flexible information model with subscription and policy separated from network functions and nodes.
- Minimize access and core network dependencies by specifying a converged access-agnostic core with a common AN - CN interface which integrates different 3GPP and non-3GPP access types.
- Principles for procedures defined as a service shall follow the agreement on Key issue#7 stated in Section 8.7.
- The architecture shall support capability exposure.

Editor's note: How the above principles will be exhibited in architecture figure is FFS.

Interim agreements on overall architecture are as follows:

1. In Rel-15, MMF and SMF functions should be standardized as separate functions with standardized interactions.
2. NAS MM and SM protocol messages terminate in MMF and SMF respectively. This is independent of whether SM protocol terminates in the H-SMF or V-SMF.
3. NAS SM messages are routed by MMF.

8.12.2 Non-roaming reference architecture and reference points

The NG-CP functionality:

- NF Repository Function (NRF): It provides NFs registration and discovery functionality so that peer NG-CP NFs can be discovered and communicate with each other.

Editor's note: whether NRF is an enhancement of DNS and whether it needs to be specified by SA2 is FFS.

Editor's note: the architecture impact related with security functionalities (ARPF, AUSF, SCMF and SEAF) will be updated based on SA3 work. How the authentication function maps to the control plane is FFS.

- Access and Mobility Management Function (AMF): Handles the UE level access and mobility management including UE network access control, UE Location management and UE reachability management. It supports the UE access the network via multiple access types including 3GPP access and non-3GPP access. The AMF terminates the NG1 reference point and also the NG2 reference point.
- Session Management Function (SMF): Supports Allocation of UE IP address, User plane function selection and control, , etc. It may also consist of the control part of enforcement of QoS related rules and session related Charging and Lawful Intercept. SMF controls the NG User Plane Function via NG4

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 481 of 501

- Policy Control Function (PCF). It interacts with other NG-CP functions such as SMF, AMF to provide dynamic policies e.g. for QoS enforcement, charging, access control, traffic routing, etc.
- Network Capability Exposure function (NEF).

Editor's note: Description of Network Exposure Function is FFS

Editor's note: the list of the functionalities above may be updated based on the progress of related Key Issues.

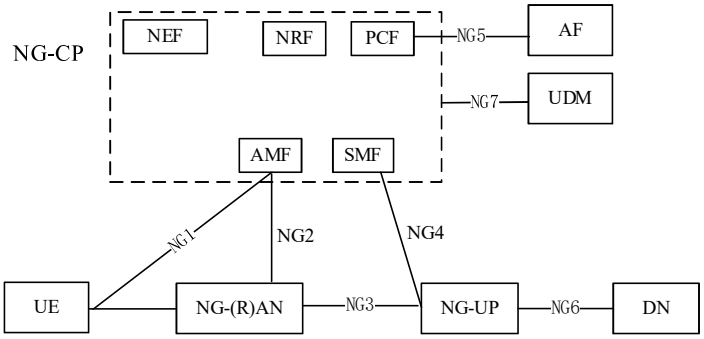


Figure 8.12.2-1: Non-Roaming NextGen Architecture

The following reference points and interfaces are defined:

NG1: Reference point for the control plane between NG UE and AMF.

NG2: Reference point for the control plane between NG (R)AN and AMF.

NG3: Reference point for the user plane between NG (R)AN and NG-UP.

NG4: Reference point between SMF and NG-UP Functions

NG5: Reference point between PCF function and Application Function

NG6: Reference point between the NG-UP and the data network. Data network may be an operator external public or private data network or an intra-operator data network.

NG7: Reference point between NG-CP function and NG Unified Data Management.

Service-based interfaces should be considered to be exposed from NG-CP functions such as AMF, SMF, PCF, NRF, NEF through which other NG-CP functions can invoke them for service.

Editor's note: Whether the NG7 can be a service-based interface is FFS.

Editor's note: Other reference points are FFS.

UDM. It stores UE related data, e.g., subscription, policy (e.g. on QoS and charging).

NG Core User Plane (NG-UP) function, a generic user-plane function supporting various operations and functionalities such as:

- External PDU session point of interconnect (e.g. IP).
- Packet routing & forwarding.
- Traffic handling (e.g. QoS enforcement).
- Anchor point for Intra-/Inter-RAT mobility (when applicable).
- Optional functionalities such as Packet inspection.
- Lawful intercept (UP collection).

Multiple NG-UP functions may be used to serve one PDU session.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 482 of 501

Annex A:
Key technical areas identified for investigation during the study

This Annex shows some possible key technical areas that have been identified for investigation during the study (i.e. technical report):

Key Areas

- Network slicing.
- Mobility framework.
- QoS framework.
- Session management.
- Unified policy framework.
- Multi-connectivity.
- Vertical services accommodation.
- Authentication, authorization.
- Charging, accounting.
- Network discovery and selection.
- Identities.
- Migration & coexistence.
- Information storage and management.
- Network capability exposure.
- RAN-CN functional split (and access agnostic core).
- Overall architecture.

Editor's note: The list of key technical areas listed in this Annex are not exhaustive and are only intended to identify at the onset of the study possible areas for investigation supporting preparation of the present document. This annex will not be maintained during the course of the study and will be deleted prior to the preparation of the final version of the present document.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 483 of 501

Annex B:
Network slicing concept by NGMN

NOTE: The concept description in this annex is copied from the NGMN paper "Description of Network Slicing Concept" [8].

B.1 Network slicing concept

As depicted in Figure B.1-1, the network slicing concept consists of 3 layers: 1) Service Instance Layer, 2) Network Slice Instance Layer, and 3) Resource layer.

The Service Instance Layer represents the services (end-user service or business services) which are to be supported. Each service is represented by a Service Instance. Typically services can be provided by the network operator or by 3rd parties. In line with this, a Service Instance can either represent an operator service or a 3rd party provided service.

A network operator uses a Network Slice Blueprint to create a Network Slice Instance. A Network Slice Instance provides the network characteristics which are required by a Service Instance. A Network Slice Instance may also be shared across multiple Service Instances provided by the network operator.

NOTE: Whether there is a need to support sharing of Network Slice Instances across Service Instances provided by different 3rd parties is up for discussion in SDOs.

The Network Slice Instance may be composed by none, one or more Sub-network Instances, which may be shared by another Network Slice Instance. Similarly, the Sub-network Blueprint is used to create a Sub-network Instance to form a set of Network Functions, which run on the physical/logical resources.

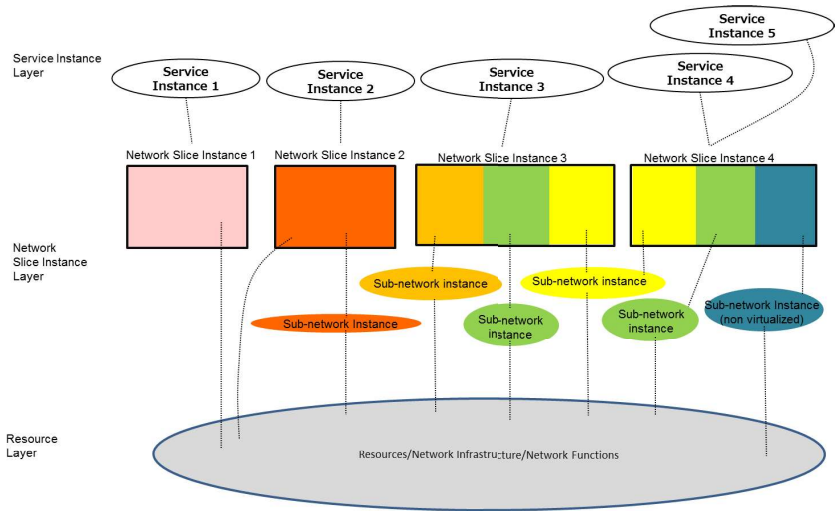


Figure B.1-1: Network slicing conceptual outline

B.2 Definitions

Service Instance: An instance of an end-user service or a business service that is realized within or by a Network Slice.

Network Slice Instance: a set of network functions, and resources to run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the Service Instance(s):

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 484 of 501

- A network slice instance may be fully or partly, logically and/or physically, isolated from another network slice instance.
- The resources comprises of physical and logical resources.
- A Network Slice Instance may be composed of Sub-network Instances, which as a special case may be shared by multiple network slice instances. The Network Slice Instance is defined by a Network Slice Blueprint.
- Instance-specific policies and configurations are required when creating a Network Slice Instance.
- Network characteristics examples are ultra-low-latency, ultra-reliability, etc.

Network Slice Blueprint: A complete description of the structure, configuration and the plans/work flows for how to instantiate and control the Network Slice Instance during its life cycle. A Network Slice Blueprint enables the instantiation of a Network Slice, which provides certain network characteristics (e.g. ultra-low latency, ultra-reliability, value-added services for enterprises, etc.). A Network Slice Blueprint refers to required physical and logical resources and/or to Sub-network Blueprint(s).

Sub-network Instance: A Sub-network Instance comprises of a set of Network Functions and the resources for these Network Functions:

- The Sub-network Instance is defined by a Sub-network Blueprint.
- A Sub-network Instance is not required to form a complete logical network.
- A Sub-network Instance may be shared by two or more Network Slices.
- The resources comprises of physical and logical resources.

Sub-network Blueprint: A description of the structure (and contained components) and configuration of the Sub-network Instances and the plans/work flows for how to instantiate it. A Sub-network Blueprint refers to Physical and logical resources and may refer to other Sub-network Blueprints.

Physical resource: A physical asset for computation, storage or transport including radio access:

- Network Functions are not regarded as Resources.

Logical Resource: Partition of a physical resource, or grouping of multiple physical resources dedicated to a Network Function or shared between a set of Network Functions.

Network Function (NF): Network Function refers to processing functions in a network:

- This includes but is not limited to telecom nodes functionality, as well as switching functions e.g. Ethernet switching function, IP routing functions.
- VNF is a virtualized version of a NF (refer to ETSI NFV for further details on VNF).

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 485 of 501

Annex C:
Work planning for NextGen Study Item on how to focus Rel-14 study

Development of a new system architecture including a new core network is a significant standardization effort. Completion of this task will take multiple 3GPP releases. A timely completion of this work that meets various deadlines for anticipated technology trials and deployments can be achieved with the help of proper planning. The goals of the planning include;

- An early availability of basic system for trials and limited deployments that fulfils the goals and expectations set about for Next Generation of System including the Core Network.
- Building of a complete and feature rich system using the basic system defined in step 1 as a foundation thereby ensuring backwards compatibility within Next Gen Ecosystem.

Based on these goals and SA considerations (see SP_69_Approved_Rep_v100 from SA#69) the following list of topics is created to help identify areas of preferred contributions for R-14 study in upcoming meetings. These lists are a work in progress and can get updated as work progresses e.g. based on new key issues introduced into the TR and feedback from RAN WGs.

Functionalities that are needed:

- QoS.
- Charging.
- Policy.
- Authentication.
- Mobility management.
- Session and service continuity.
- Session management.

Architectural enablers that need to be addressed:

- Minimizing access dependencies (incl. non-3GPP access integration aspects).
- Shared network and roaming scenarios.
- CP/UP separation.
- RAN-CN functional split.
- Architectural impacts of scaling.
- Network slicing.
- Co-existence, migration and interworking.
- Network functions granularity and interaction between them.

NOTE: System level services beyond basic data connectivity may need to be identified to understand if the listed functionalities fulfil service requirements.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 486 of 501

Annex D:
Potential solution scenarios for support of multiple slices per UE

This Annex outlines potential solution scenarios that applies to the Key issue 1: Support of network slicing. The following three groups of solutions have been found for the support of multiple network slices per UE:

- Group A includes the interpretation that the UE obtains services from different network slices and different CN instances, aiming at logical separation/isolation between the CN instances. This group is characterised by independent subscription management/mobility management for each network slice handling the UE, with the potential side effects of additional signalling in the network and over the air. On the other hand, it can be argued that the isolation in the CN part of the network is easiest to achieve.

- Group B assumes that some Network Functions are common between the network slices, while other functions reside in its individual network slices.

- Group C assumes that the control plane handling is common between the slices, while the user plane(s) are handled as different network slices.

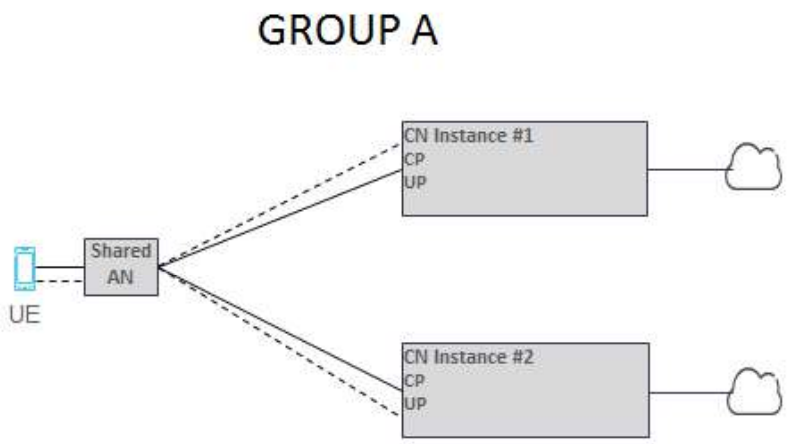


Figure D-1: Group A

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 487 of 501

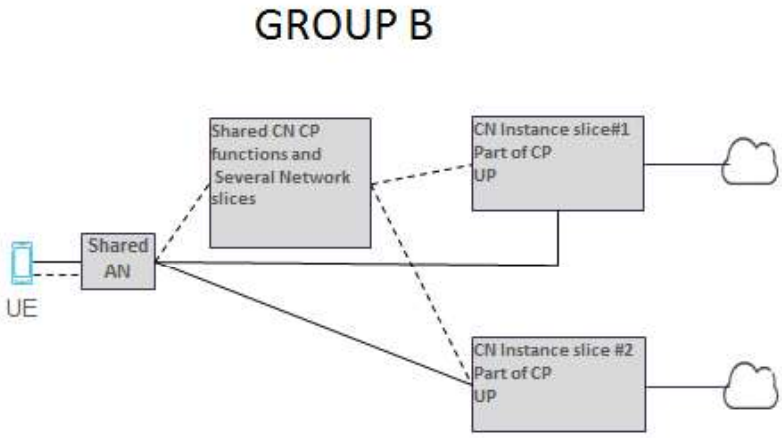


Figure D-2: Group B

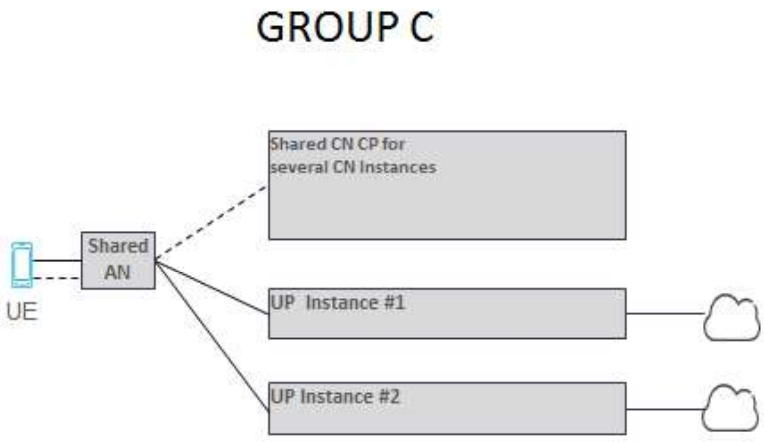


Figure D-3: Group C

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 488 of 501

Annex E:
Guidelines for specifying procedures, to allow its re-use

While defining the core network procedures, e.g. attach procedure and the messages and attributes exchanged between various network functions, the approaches for procedure specification should be analysed on a case by case basis. This Annex provides guidelines on one such approach, i.e. on specifying the core network procedures such that the procedures (and hence the corresponding functionality) can be re-used between any specific set of network functions in the current or future releases of 3GPP. The principles mentioned here can be analysed on a case-by-case basis and whenever found useful, applied while specifying the support of functionality within the Next Generation core network.

E.1 Specifying a procedure

E.1.1 As a service

Any functionality or service involves two types of network functions: service-requester and service-provider. If a functionality or service is defined without fixing the service-requester then it could be re-used by any service-requester within the network. And when, corresponding to this functionality, a procedure (which includes set of messages and the parameters exchanged in those messages) is specified while ensuring this principle, the procedure becomes generic. This procedure then can be re-used by a different service-requester while there is no or minimal impact to the service-provider.

Thus, instead of defining a procedure between a set of network functions, a procedure is defined in terms of service exposed by a service-provider network function, without fixing the service-requester network function. As part of the procedure only the service-provider network function and a set of parameters exchanged in the involved messages (e.g. servicer-request and service-response messages) are specified.

E.1.2 Authorization

Even though a procedure is defined generically, in some cases, the operator may want to restrict the set of service-requester network functions, or in other cases, the procedure itself may restrict the set of network functions which can act as a service-requester. To support both of these cases, the network needs to support the ability to authorize (i.e. allow or deny) the service-requester network function for the requested procedure.

E.2 Procedure of a network function: independent, non-overlapping of each other

If a functionality of a network function can be requested independently and also as part of another procedure then it is better to define two independent and non-overlapping procedures.

Thus, the overall functionality of a network function is first broken down into multiple smaller functionality which may be requested independently. Then for each of the smaller functionality independent procedure, such that it does not overlap (in terms of the functionality provided) with other procedures of the network function, is specified. This will result in definition of atomic procedures (and which are also relatively simpler) and higher re-use of each of the procedure.

E.3 Procedure of the system: As a sequence of network function level procedures

A system level procedure, e.g. Attach, may require support from multiple network functions. In this case, instead of specifying the system level procedure directly, multiple independent procedures at each involved network function level can be specified first. Then the system level procedure is specified in terms of call flow defining the sequence in which those independent network function level procedures are invoked.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 489 of 501

Annex F: Minimizing access dependencies in the NextGen Core and AN - CN Interface

This annex provides high level principles to interpret the requirements of minimizing access dependencies for key core network functionalities. It captures RAN-CN interface aspects as well from the perspective of making it non access specific.

F.1 QoS

QoS related parameters and QoS related signalling between the core network and access network is non access specific. For example QoS needs on a per IP flow basis are signalled to the access network via non access specific signalling using non access specific QoS parameters. Within the access network the conversion to access specific QoS parameters and signalling can occur as needed.

F.2 Authentication

Authentication framework used between the core network and access network is non access specific. The security methods (e.g. EAP AKA) used for authentication can however be access specific if needed.

F.3 Charging Framework

Charging Framework that includes functions responsible for charging data collection and communication will be non-access specific. The actual charging data collected maybe access specific however. This functionality is contained within the CN and has no implications for RAN-CN functional split.

F.4 Policy Framework

The policy framework that includes for example a concept of a policy controller, policy enforcement points, etc. will be non-access specific. There will however be access specific policies that may require for example access specific additional policy decision, communication and enforcement. This functionality is contained within the CN and has no implications for RAN-CN functional split.

F.5 Session Continuity

Sessions continuity functions in the core network will be non-access specific. The access network may have access specific session continuity mechanisms that are not visible to the core network.

F.6 Session Management

Session management functions such as techniques for allocation of IP address will be non-access specific. For any access specific session management functionality that is identified, the transport (e.g. IP) for carrying access specific session management signalling over RAN-CN interface will be non-access specific.

F.7 Mobility Management

Mobility management functions will be access specific. However the transport (e.g. IP) for carrying access specific mobility management signalling over RAN-CN interface will be non-access specific.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 490 of 501

F.8 Minimization of Access dependencies and CP/UP functional split

It is likely that there will be some access specific functional entity(ies) left in the CN for example to handle mobility management. This will result in possible communication between both access specific and non-access specific functional entities in the control plane and user plane.

- CP/UP communication functionality between non access specific functional entities in CP and UP will also be non-access specific.
- CP/UP communication functionality where at least one of the functional entities is access specific will also be access specific but it can possibly use an existing CP/UP interface with access specific extensions.

F.9 Carrying of Access Specific information over AN-CN interface

Access specific functionalities in the network should be isolated from non-access specific functions. When access specific entity(ies) exist in the core network and they have to communicate over RAN-CN interface it is possible to consider taking the following actions;

- Use a non-access specific transport (e.g. IP) to carry traffic to a core network functional node specific to that access technology.
- Possibly use a transport header extension to identify an access technology and based on that route the packet to right control plane entity.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 491 of 501

Annex G:
Reference point naming

Depicted in Figure G-1 is a reference model of a potential architecture including potential functional entities and potential reference points with the intention that the naming in particular of the reference points may be used in individual solution proposals for a better understanding and comparison. This reference model does not make any assumption on the actual target architecture i.e. the target architecture may not have all of the depicted reference points or functional entities or may have additional/other reference points or functional entities.

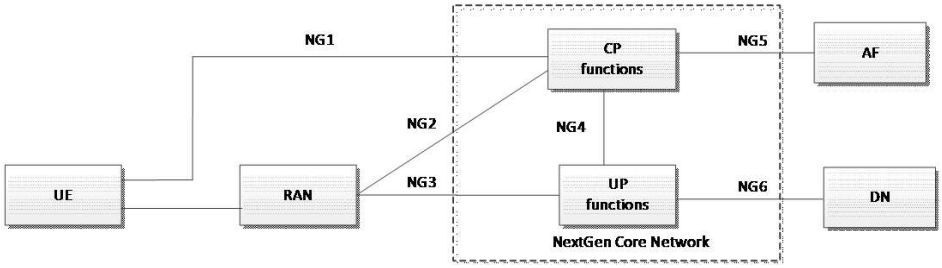


Figure G-1: Reference point naming

NOTE 1: The Control plane functions and the User plane functions of the NextGen core are depicted as single boxes (CP functions and UP functions, respectively). Individual solution proposals may further split or replicate CP or UP functions. In that case the naming of additional reference point could add an index to the depicted reference point (e.g. NG4.1, NG4.2).

RAN here refers to a radio access network based on the <5G> RAT or Evolved E-UTRA that connects to the NextGen core network.

The following reference points are illustrated in Figure G-1:

NG1: Reference point between the UE and the CP functions.

NG2: Reference point between the RAN and the CP functions.

NG3: Reference point between the RAN and the UP functions.

NG4: Reference point between the CP functions and the UP functions.

NG5: Reference point between the CP functions and an Application Function.

NG6: Reference point between the UP functions and a Data Network (DN).

NOTE 2: Some reference points in Figure X-1 may consist of several reference points depending on how the CP functions and UP functions may be further split.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 492 of 501

Annex H:
Support of edge computing

For the efficient delivery of certain operator/3rd party content related services, as well as for the provision of services over long distances in a cost-effective way, there is a need to deploy services in the operator trust domain close to the UE's access point of attachment to reduce latency and reduce the load on the transport network. The design of NextGen System should enable access to services deployed close to the UE's point of attachment from the very beginning, so that this functionality could be deployed in a flexible manner, leveraging also Network Function Virtualization (NFV).

The necessary functionality to support this is addressed as part of a number of key issues, including:

- Key issue 2: QoS framework.
- Key issue 4: Session management.
- Key issue 5: Enabling (re)selection of efficient user plane paths.
- Key Issue 9: 3GPP architecture impacts to support network capability exposure.
- Key issue 11: Charging.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 493 of 501

Annex I:
Guidelines for defining network function granularity

This annex provides in reference to Key issue 7 a methodology to obtain an adequate network granularity.

I.1 General

It is expected that each Network Function of the final architecture will be made of one or more functions (function (1...n)), to be defined in the different key issues of the TR such as session management, mobility management, session continuity, etc.

In order to obtain the optimised network architecture, it is proposed to use a well-defined methodology to determine how to combine functions into Network Functions.

The methodology is composed of 3 steps. The first step lists the different functions necessary for the 5G CN based on the solutions provided by the other key issues. The second step identifies the functions that shall be kept separated from the others and thus assimilated to Network functions, based on separation criteria. The third step gives the functions that shall be combined together into Network Function based on combination criteria.

Step 1: Identifying the functions

This step identifies the different functions necessary for the 5G CN based on the solutions provided by the other key issues of the TR.

Step 2: Identifying the functions to be kept separated

The following criteria should be considered to determine which functions should be kept separated:

- Centralized or distributed (far from / close to a UE): a distributed function is a function that needs to be located in the edge (for at least one use case) or can be across PLMN. It should not be gathered with another function that has no such constraints and that will be most probably centralised. As an example, in case of cloud access network, the access management function responsible for the physical connection with the device shall be in the edge because of access delay constraints.

- Re-usability: a function that can be potentially used by multiple service layers or have different internal variants shall be kept standalone. As an example, the HSS is today used by different types of networks: EPC, IMS and the IMS AS.

- Optionality: for resource optimisation purpose, a function that will be solicited for only some use cases should be kept separated from those that will be solicited for all use cases. For example: the policy control function may not be necessary for devices connecting through a fixed access; core network handover management function will not be used for fixed-like usages. Evolution cycle of the function: a function that will evolve rapidly (internal algorithm or new feature in normalisation every 6 to 12 month) shall be kept separated from those that have a slower evolution cycle. As an example, the authentication function may evolve rapidly and independently from the others because of the introduction of new authentication methods.

The following table shall be filled in.

Table I.1-1

functions	Distributed	Re-usability	Optionality	Evolution cycle
Example 1	Yes	Yes	Yes	Rapid
Example 2	No	No	No	Rapid
Function 1				
Function 2				
…				
Function i				

At the end of this step,

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 494 of 501

- Functions with high separation constraints (example 1 in the table) can be deduced. Each of them represents one Network function. They are not considered in step 3.
- Functions (example 2 in the table) with low or without separation constraints can be deduced (function (a…j)). They are considered in step 3 to decide whether/how to combine them within Network Functions.
- Any other function-to-function non-affinity shall be underlined at the end of this step.

Step 3: Identify the network functions to be combined

This third step handles only with functions (function (a...j)) with **low** or **without** separation constraints and considers the function-to-function non affinity deduced from the previous step to determine how they can be combined. Functions are combined in the objective of:

- Reducing the Interaction and complexity of interfaces that could exist between them,
- Obtaining a simple architecture with the less of interfaces.

Combination work shall at least look at the function from the same functional domain. Thus, the table below shall be filled in to determine the functional domain of each function. When functions are combined, implementation shall grant for each of them an independent scalability within the NF.

Table I.1-2

	network	Security	Charging	database	
example 1 : HSS				x	
Example 2 : Authentication	x				
example 3: connection management	x				
Function a					
Function b					
Function j					

NOTE: the above example assume that HSS, Authentication and connection management functions are not identified as separate network functions in step 2

Example analysis based on example 1, 2 and 3:

"Authentication" and "HSS" function can have complex interface with a high level of interaction, but as they are in different functional domain then they cannot be combined.

"Connection management" and "authentication" can have complex interface with high level of interaction however since they are in the same functional domain, we can combine them in order to have less interfaces in the network.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 495 of 501

Annex J:
Deployment Scenarios

J.1 General

This section provides high level deployment scenarios corresponding to the options listed in SP-160464/RP-16266 [11]. See TR 38.801 [13] for further details of the NextGen RAN architecture.

Architecture Option 1 is EPC with EUTRAN, and is not captured in this annex as its support is already specified.

NOTE 1: Options 6 and 8 SP-160464/RP-16266 [11]are not reflected in this Annex as they were deemed irrelevant at TSG#72 plenaries.

For Option 3, SA WG2 will only study forward compatibility, interworking and migration scenarios with the Next Generation system (see SP-160460/RP-161269[12]). For details of forward compatibility, migration and interworking, please see Key Issue 18 in this TR.

Some of the reference points names and definitions between the UE and NGC and between NG RAN and NGC are given in Annex G. Reference point for EPC and their definitions are provided in TS 23.401 [2].

NOTE 2: In the figures below the RAN is represented by a box with the RAN type (E-UTRAN or NG RAN) followed by radio access technology in brackets (NR, E-UTRA or Evolved E-UTRA).

NOTE 3: The interface names between RAN nodes and between the UE and the RAN node are in the remit of RAN groups and are left unnamed in the figures in this Annex.

J.2 Deployment Option 2 - Standalone NR in NextGen System

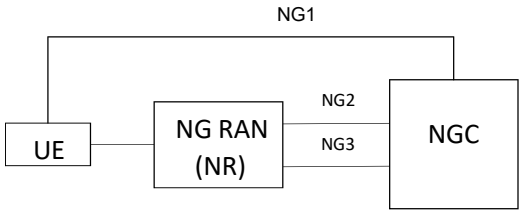


Figure J.2-1: Deployment Option 2

This deployment option is for NG RAN with the radio access based on NR in a stand-alone configuration in NextGen System.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 496 of 501

J.3 Deployment Option 3 - Non-standalone NR in EPS

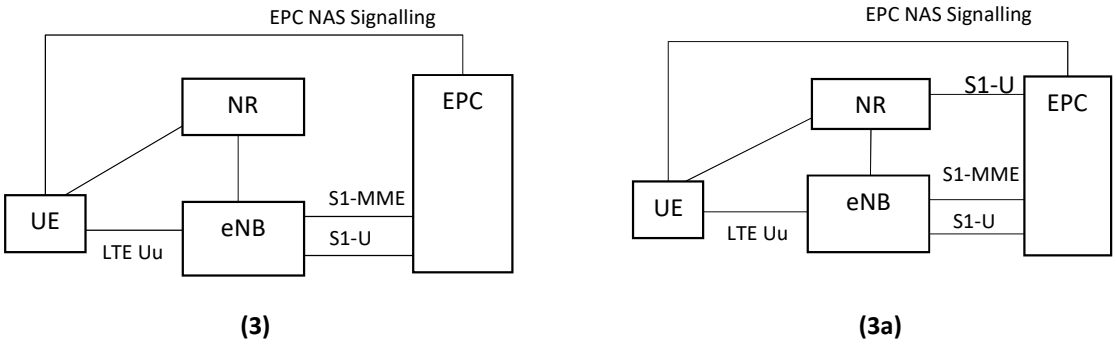


Figure J.3-1: Deployment Option 3

This deployment option is a dual connectivity deployments with E-UTRA as the anchor RAT and NR as the secondary RAT in a non-standalone configuration in EPS.

J.4 Deployment Option 4 - Non-standalone Evolved E-UTRA in NextGen System

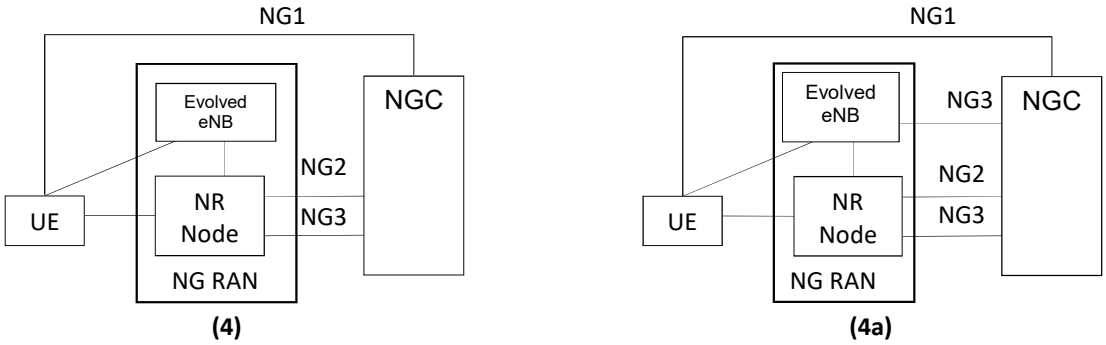


Figure J.4-1: Deployment Option 4

This deployment option is a dual connectivity deployment with NR as the anchor RAT and Evolved E-UTRA as the secondary RAT in a non stand-alone configuration in NextGen System.

J.5 Deployment Option 5 - Standalone Evolved E-UTRA in NextGen System

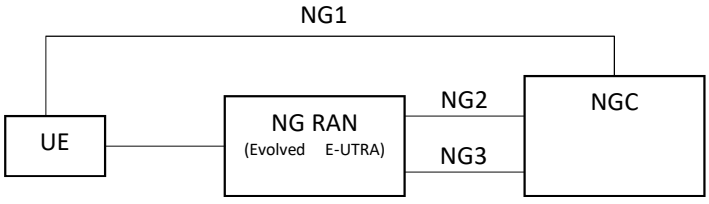


Figure J.5-1: Deployment Option 5

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 497 of 501

This deployment is for NG RAN with the radio access based on Evolved E-UTRA in a stand-alone configuration in NextGen System.

J.6 Deployment Option 7 - Non-standalone NR in NextGen System

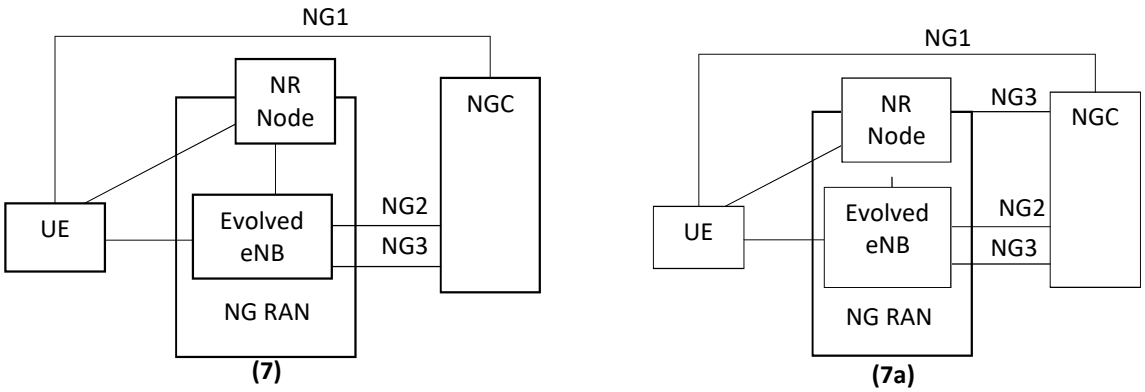


Figure J.6-1: Deployment Option 7

This deployment option is for dual connectivity deployments with Evolved E-UTRA as the anchor RAT and NR as the secondary RAT in a non stand-alone configuration in NextGen system.

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 498 of 501

Annex K:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2015-11	SA2#112	-	-	-	TR updated with S2-153848, S2-154306, S2-154308, S2-154443, S2-154462	-	0.1.0
2015-12	SP-70	-	-	-	MCC Update to add TR number after SID approval	0.1.0	0.1.1
2016-02	SA2#113	-	-	-	TR updated with S2-160704, S2-160752, S2-160754, S2-160818, S2-160872, S2-160873, S2-160875, S2-160876, S2-160877, S2-160879, S2-160880, S2-160881, S2-160930, S2-160931	0.1.1	0.2.0
2016-03	SA2#113 AH	-	-	-	TR updated with S2-161105, S2-161129, S2-161135, S2-161137, S2-161138, S2-161198, S2-161234, S2-161238, S2-161239, S2-161243, S2-161247, S2-161248, S2-161249, S2-161273, S2-161275, S2-161278, S2-161280, S2-161281, S2-161287, S2-161290, S2-161291, S2-161293, S2-161294, S2-161295, S2-161296, S2-161297, S2-161298, S2-161299, S2-161323, S2-161324, S2-161326, S2-161327, S2-161328, S2-161339, S2-161340, S2-161341, S2-161342, S2-161349, S2-161350, S2-161351, and with Editorial changes	0.2.0	0.3.0
2016-04	SA2#114	-	-	-	TR updated with S2-161420,S2-162093,S2-162143,S2-162146,S2-162150,S2-162155,S2-162156,S2-162158,S2-162251,S2-162252,S2-162253,S2-162254,S2-162255,S2-162256,S2-162257,S2-162258,S2-162259,S2-162260,S2-162261,S2-162262,S2-162263,S2-162264,S2-162265, and with Editorial changes	0.3.0	0.4.0

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 499 of 501

2016-05	SA2#115	-	-	-	TR updated with S2-162788, S2-162951, S2-163112, S2-162791,S2-162954, S2-162790, S2-162956, S2-162569, S2-162957, S2-162958, S2-163126, S2-163161, S2-163111, S2-163162, S2-162893, S2-162900, S2-162901, S2-162894, S2-163182, S2-163124, S2-162896, S2-163163, S2-162902, S2-162912, S2-162826, S2-162988, S2-162792, S2-163128, S2-163122, S2-163121, S2-162794, S2-163164, S2-162931, S2-162933, S2-163115, S2-163183, S2-162936, S2-163123, S2-163120, S2-163117, S2-163125, S2-163113, S2-163036, S2-162932, S2-162998, S2-162474, S2-163118, S2-163185, S2-163002, S2-163003, S2-162699, S2-163005, S2-162595, S2-162598, S2-163151, S2-163186,S2-163192, S2-163206, S2-163207, S2-163208, S2-163209, S2-163210, S2-163211, and with Editorial changes	0.4.0	0.5.0
2016-07	SA2#116	-	-	-	TR updated with S2-164200, S2-164201, S2-163885, S2-163886, S2-164112, S2-163888, S2-164257, S2-163890, S2-163362, S2-164238, S2-163974, S2-164115, S2-164116, S2-164258, S2-164139, S2-163981, S2-164156, S2-163254, S2-164089, S2-164090, S2-164091, S2-163799, S2-163800, S2-163801, S2-164092, S2-164276, S2-164275, S2-163991, S2-164203, S2-163993, S2-163994, S2-164239, S2-163996, S2-163997, S2-163998, S2-163512, S2-163999, S2-164071, S2-164001, S2-164102, S2-164103, S2-164004, S2-164204, S2-164250, S2-163935, S2-164068, S2-164251, S2-164252, S2-163944, S2-164253, S2-164107, S2-164254, S2-164249, S2-164110, S2-163546, S2-164255, S2-163389, S2-164065, S2-164066, S2-164256, S2-163345, S2-163983, S2-163984, S2-163986, S2-164158, S2-164259, S2-164240, S2-164260, S2-164261, S2-164117, S2-164161, S2-164242, S2-164023, S2-164243, S2-164244, S2-164026, S2-164033, S2-164184, S2-164185, S2-164262, S2-164186, S2-164187, S2-164271, S2-164031, S2-164119, S2-163392, S2-164246, S2-164247, S2-164190, S2-164021, S2-164192, S2-164265, S2-164193, S2-164194, S2-164195, S2-164196, S2-164197, S2-164278, and with Editorial changes	0.5.0	0.6.0
2016-08	SA2#116	-	-	-	TR updated with the missing parts of S2-164250, S2-164262, and with Editorial changes on Figure numbering	0.6.0	0.7.0
2016-09	SA2#116 bis	-	-	-	TR updated with S2-165376, S2-165263, S2-164920, S2-164921, S2-165391, S2-165377, S2-164968, S2-165379, S2-165255, S2-165125, S2-164500, S2-165256, S2-165257, S2-165258, S2-165259, S2-165132, S2-165131, S2-165381, S2-165382, S2-165833, S2-165260, S2-165385, S2-165386, S2-164831, S2-164832, S2-164833, S2-164834, S2-164901, S2-165004, S2-165006, S2-165388, S2-165009, S2-165010, S2-165245, S2-165105, S2-165106, S2-165246, S2-165108, S2-165109, S2-165247, S2-165389, S2-165250, S2-164954, S2-165409, S2-165410, S2-165266, S2-165267, S2-164959, S2-165114, S2-165284, S2-165119, S2-164515, S2-165285, S2-165243, S2-165244, S2-165327, S2-165328, S2-165077, S2-165078, S2-165413, S2-165330, S2-165081, S2-165414, S2-165148, S2-165332, S2-165150, S2-165152, S2-165415, S2-165334, S2-165335, S2-165336, S2-165177, S2-165424, S2-165178, S2-165425, S2-165289, S2-165181, S2-165169, S2-165419, S2-165375, S2-164923, S2-164425, S2-165373, S2-165374, S2-165458, S2-165450, S2-165449, S2-165447, S2-165448, S2-165452, S2-165396, S2-165440, S2-165397, S2-165453, S2-165455, S2-165454, S2-165441, S2-165442, S2-165451, S2-165411, S2-165412,and with Editorial changes	0.7.0	0.8.0
2016-09	SP-73	SP-160667	-	-	MCC Editorial update for presentation to TSG SA#73 for Information	0.8.0	1.0.0
2016-09		-	-	-	TR updated with editorial correction of implementation of some P-CRs approved in SA2#116, re-organize and update the numbering of Section 8	1.0.0	1.0.1
2016-09					Correct the implementation of S2-165267 as a separate clause	1.0.1	1.0.2
2016-10	SA2#117	-	-	-	TR updated with S2-165640, S2-166237, S2-166210, S2-166185, S2-166186, S2-166188, S2-166220, S2-166222, S2-166084, S2-166223, S2-166226, S2-166227, S2-166122, S2-166124, S2-166125, S2-166278, S2-166279, S2-166053, S2-166242, S2-166281, S2-166243, S2-166244, S2-166245, S2-166054, S2-166246, S2-166247, S2-166248, S2-166249, S2-166250, S2-166252, S2-166283, S2-166255, S2-166256, S2-165647, S2-166136, S2-166138, S2-166139, S2-166100, S2-166101, S2-165583, S2-166262, S2-166106, S2-166265, S2-165692, S2-166149, S2-166170, S2-166130, S2-166282, S2-166133, S2-166259, S2-166291, S2-166292, S2-166263, S2-166264, S2-166269, S2-166293, S2-166294, S2-166295, S2-166296, S2-	1.0.2	1.1.0

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 500 of 501

					166297, S2-166298, + MCC Editorials		

Petitioners' Exhibit 1020
Nokia of America Corp., et al. v. KT Corporation, et al.
Case No. IPR2025-00036; U.S. Patent No. 11,627,631
Page 501 of 501