टीईसी टीएस-३३.५०१ संस्करण १.८.०

टीएसडीएसआई मानक टीएसडीएसआई एसटीडी टी१.३जीपीपी ३३.५०१ -१७.१४.० संस्करण१.८.० से अभिग्रहण

TEC TS-33.501 V1.8.0

Adopted from TSDSI STD T1.3GPP 33.501-17.14.0 V1.8.0

5G सिस्टम के लिए सुरक्षा संरचना और प्रक्रियाएं

Security architecture and procedures for 5G System

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीद लाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, IND

www.tec.gov.in

About TEC

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For testing, four Regional Telecom Engineering Centres (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

© टीईसी, २०२६

©TEC, 2026

इस सर्वाधिकार सुरक्षित प्रकाशन का कोई भी हिस्सा, दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली की लिखित स्वीकृति के बिना, किसी भी रूप में या किसी भी प्रकार से जैसे -इलेक्ट्रॉनिक, मैकेनिकल, फोटोकॉपी, रिकॉर्डिंग, स्कैनिंग आदि रूप में प्रेषित, संग्रहीत या पुनरुत्पादित न किया जाए ।

All rights reserved and no part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form and by any means - electronic, mechanical, photocopying, recording, scanning or otherwise, without written permission from the Telecommunication Engineering Centre, New Delhi.

Release: January, 2026

Contents

Foreword 16

1 Scope 17

2 References 17

3 Definitions and abbreviations 21
3.1 Definitions 21
3.2 Abbreviations 24

4 Overview of security architecture 27
4.1 Security domains 27
4.2 Security at the perimeter of the 5G Core network 28
4.2.0 General 28
4.2.1 Security Edge Protection Proxy (SEPP) 28
4.2.2 Inter-PLMN UP Security (IPUPS) 28
4.3 Security entities in the 5G Core network 28

5 Security requirements and features 28
5.1 General security requirements 28
5.1.1 Mitigation of bidding down attacks 28
5.1.2 Authentication and Authorization 28
5.1.3 Requirements on 5GC and NG-RAN related to keys 29
5.2 Requirements on the UE 29
5.2.1 General 29
5.2.2 User data and signalling data confidentiality 29
5.2.3 User data and signalling data integrity 30
5.2.4 Secure storage and processing of subscription credentials 30
5.2.5 Subscriber privacy 31
5.3 Requirements on the gNB 31
5.3.1 General 31
5.3.2 User data and signalling data confidentiality 31
5.3.3 User data and signalling data integrity 32
5.3.4 Requirements for the gNB setup and configuration 32
5.3.5 Requirements for key management inside the gNB 33
5.3.6 Requirements for handling user plane data for the gNB 33
5.3.7 Requirements for handling control plane data for the gNB 33
5.3.8 Requirements for secure environment of the gNB 33
5.3.9 Requirements for the gNB F1 interfaces 33
5.3.10 Requirements for the gNB E1 interfaces 34
5.4 Requirements on the ng-eNB 34
5.5 Requirements on the AMF 34
5.5.1 Signalling data confidentiality 34
5.5.2 Signalling data integrity 34
5.5.3 Subscriber privacy 34
5.6 Requirements on the SEAF 35
5.7 Void 35
5.8 Requirements on the UDM 35
5.8.1 Generic requirements 35
5.8.2 Subscriber privacy related requirements to UDM and SIDF 35
5.8a Requirements on AUSF 35
5.9 Core network security 35
5.9.1 Trust boundaries 35
5.9.2 Requirements on service-based architecture 36
5.9.2.1 Security Requirements for service registration, discovery and authorization 36
5.9.2.2 NRF security requirements 36
5.9.2.3 NEF security requirements 36
5.9.2.4 Requirements on the Service Communication Proxy (SCP) 36
5.9.3 Requirements for e2e core network interconnection security 37

5.9.3.1 General 37
5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP) 37
5.9.3.3 Protection of attributes....39
5.9.3.4 Requirements for IPUPS functionality 39
5.9.3.5 Requirements for Network Functions (NF) 39
5.10 Visibility and configurability....39
5.10.1 Security visibility....39
5.10.2 Security configurability....40
5.11 Requirements for algorithms, and algorithm selection 40
5.11.1 Algorithm identifier values 40
5.11.1.1 Ciphering algorithm identifier values 40
5.11.1.2 Integrity algorithm identifier values 40
5.11.2 Requirements for algorithm selection 41
5.12 Requirements on 5G-RG 41
5.13 Requirements on NSSAAF....41

6 Security procedures between UE and 5G network functions 41
6.0 General 41
6.1 Primary authentication and key agreement....42
6.1.1 Authentication framework....42
6.1.1.1 General 42
6.1.1.2 EAP framework....43
6.1.1.3 Granularity of anchor key binding to serving network 43
6.1.1.4 Construction of the serving network name 43
6.1.1.4.1 Serving network name....43
6.1.1.4.2 Construction of the serving network name by the UE....44
6.1.1.4.3 Construction of the serving network name by the SEAF....44
6.1.2 Initiation of authentication and selection of authentication method....44
6.1.3 Authentication procedures....45
6.1.3.1 Authentication procedure for EAP-AKA' 45
6.1.3.2 Authentication procedure for 5G AKA....48
6.1.3.2.0 5G AKA 48
6.1.3.2.1 Void 50
6.1.3.2.2 RES* verification failure in SEAF or AUSF or both 50
6.1.3.3 Synchronization failure or MAC failure 50
6.1.3.3.1 Synchronization failure or MAC failure in USIM 50
6.1.3.3.2 Synchronization failure recovery in Home Network....50
6.1.4 Linking increased home control to subsequent procedures 51
6.1.4.1 Introduction....51
6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 52
6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 52
6.2 Key hierarchy, key derivation, and distribution scheme....53
6.2.1 Key hierarchy 53
6.2.2 Key derivation and distribution scheme 55
6.2.2.1 Keys in network entities 55
6.2.2.2 Keys in the UE 57
6.2.3 Handling of user-related keys....59
6.2.3.1 Key setting....59
6.2.3.2 Key identification 59
6.2.3.3 Key lifetimes....60
6.3 Security contexts....61
6.3.1 Distribution of security contexts....61
6.3.1.1 General 61
6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain....61
6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains....61
6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains 61
6.3.2 Multiple registrations in same or different serving networks 62
6.3.2.0 General 62
6.3.2.1 Multiple registrations in different PLMNs....62
6.3.2.2 Multiple registrations in the same PLMN....62

6.4 NAS security mechanisms 63
6.4.1 General 63
6.4.2 Security for multiple NAS connections 63
6.4.2.1 Multiple active NAS connections with different PLMNs 63
6.4.2.2 Multiple active NAS connections in the same PLMN's serving network 63
6.4.3 NAS integrity mechanisms 64
6.4.3.0 General 64
6.4.3.1 NAS input parameters to integrity algorithm 64
6.4.3.2 NAS integrity activation 65
6.4.3.3 NAS integrity failure handling 65
6.4.4 NAS confidentiality mechanisms 65
6.4.4.0 General 65
6.4.4.1 NAS input parameters to confidentiality algorithm 65
6.4.4.2 NAS confidentiality activation 65
6.4.5 Handling of NAS COUNTs 65
6.4.6 Protection of initial NAS message 66
6.4.7 Security aspects of SMS over NAS 67
6.5 RRC security mechanisms 67
6.5.1 RRC integrity mechanisms 67
6.5.2 RRC confidentiality mechanisms 68
6.5.3 RRC UE capability transfer procedure 68
6.6 UP security mechanisms 68
6.6.1 UP security policy 68
6.6.2 UP security activation mechanism 69
6.6.3 UP confidentiality mechanisms 71
6.6.4 UP integrity mechanisms 71
6.6.4.1 General 71
6.6.4.2 UP integrity mechanisms between the UE and the gNB 71
6.6.4.3 UP integrity mechanisms between the UE and the ng-eNB 71
6.7 Security algorithm selection, key establishment and security mode command procedure 72
6.7.1 Procedures for NAS algorithm selection 72
6.7.1.1 Initial NAS security context establishment 72
6.7.1.2 AMF change 72
6.7.2 NAS security mode command procedure 72
6.7.3 Procedures for AS algorithm selection 74
6.7.3.0 Initial AS security context establishment 74
6.7.3.1 Xn-handover 74
6.7.3.2 N2-handover 74
6.7.3.3 Intra-gNB-CU handover/intra-ng-eNB handover 75
6.7.3.4 Transitions from RRC_INACTIVE to RRC_CONNECTED states 75
6.7.3.5 RNA Update procedure 75
6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM 75
6.7.4 AS security mode command procedure 76
6.8 Security handling in state transitions 77
6.8.1 Key handling at connection and registration state transitions 77
6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states 77
6.8.1.1.0 General 77
6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED 77
6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED 78
6.8.1.1.2.1 General 78
6.8.1.1.2.2 Full native 5G NAS security context available 79
6.8.1.1.2.3 Full native 5G NAS security context not available 79
6.8.1.1.2.4 UE registration over a second access type to the same AMF 80
6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states 80
6.8.1.2.0 General 80
6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED 80
6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access 81
6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access 81
6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE 82
6.8.1.3 Key handling for the Registration procedure when registered in NG-RAN 82
6.8.2 Security handling at RRC state transitions 83
6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states 83

6.8.2.1.1 General 83
6.8.2.1.2 State transition from RRC_CONNECTED to RRC_INACTIVE 83
6.8.2.1.3 State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB 83
6.8.2.1.4 State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB 85
6.8.2.2 Key handling during mobility in RRC_INACTIVE state 85
6.8.2.2.1 General 85
6.8.2.2.2 RAN-based notification area update to a new gNB/ng-eNB 85
6.8.2.2.3 RAN-based notification area update to the same gNB/ng-eNB 85
6.9 Security handling in mobility 86
6.9.1 Void 86
6.9.2 Key handling in handover 86
6.9.2.1 General 86
6.9.2.1.1 Access stratum 86
6.9.2.1.2 Non access stratum 87
6.9.2.2 Key derivations for context modification procedure 87
6.9.2.3 Key derivations during handover 88
6.9.2.3.1 Intra-gNB-CU handover and intra-ng-eNB handover 88
6.9.2.3.2 Xn-handover 88
6.9.2.3.3 N2-Handover 89
6.9.2.3.4 UE handling 90
6.9.3 Key handling in mobility registration update 91
6.9.4 Key-change-on-the-fly 93
6.9.4.1 General 93
6.9.4.2 NAS key re-keying 93
6.9.4.3 NAS key refresh 93
6.9.4.4 AS key re-keying 94
6.9.4.5 AS key refresh 94
6.9.5 Rules on concurrent running of security procedures 95
6.9.5.1 Rules related to AS and NAS security context synchronization 95
6.9.5.2 Rules related to parallel NAS connections 95
6.9.6 Security handling in registration with AMF reallocation via direct NAS reroute 95
6.10 Dual connectivity 96
6.10.1 Introduction 96
6.10.1.1 General 96
6.10.1.2 Dual Connectivity protocol architecture for MR-DC with 5GC 96
6.10.2 Security mechanisms and procedures for DC 97
6.10.2.1 SN Addition or modification 97
6.10.2.2 Secondary Node key update 99
6.10.2.2.1 General 99
6.10.2.2.2 MN initiated 99
6.10.2.2.3 SN initiated 99
6.10.2.3 SN release and change 99
6.10.3 Establishing the security context between the UE and SN 99
6.10.3.1 SN Counter maintenance 99
6.10.3.2 Derivation of keys 100
6.10.3.3 Negotiation of security algorithms 100
6.10.4 Protection of traffic between UE and SN 100
6.10.5 Handover Procedure 102
6.10.6 Signalling procedure for PDCP COUNT check 102
6.10.7 Radio link failure recovery 102
6.11 Security handling for RRC connection re-establishment procedure 102
6.12 Subscription identifier privacy 104
6.12.1 Subscription permanent identifier 104
6.12.2 Subscription concealed identifier 104
6.12.3 Subscription temporary identifier 105
6.12.4 Subscription identification procedure 106
6.12.5 Subscription identifier de-concealing function (SIDF) 106
6.13 Signalling procedure for PDCP COUNT check 106
6.14 Steering of roaming security mechanism 107
6.14.1 General 107
6.14.2 Security mechanisms 108
6.14.2.1 Procedure for steering of UE in VPLMN during registration 108

6.14.2.2 Procedure for steering of UE in VPLMN or HPLMN after registration 109
6.14.2.3 SoR Counter 111
6.15 UE parameters update via UDM control plane procedure security mechanism 112
6.15.1 General 112
6.15.2 Security mechanisms 112
6.15.2.1 Procedure for UE Parameters Update 112
6.15.2.2 UE Parameters Update Counter 113
6.16 Security handling in Cellular IoT 114
6.16.1 Security handling in Control Plane CIoT 5GS Optimization 114
6.16.1.1 Security procedures for Small Data Transfer in Control Plane CIoT 5GS Optimisation 114
6.16.1.2 Security procedures for RRCConnectionRe-establishment Procedure in Control Plane CIoT 5GS Optimization 114
6.16.2.1 General 115
6.16.2.2 Connection Suspend 115
6.16.2.3 Connection Resume in CM-IDLE with Suspend to a new ng-eNB 116
6.16.2.4 Connection Resume in CM-IDLE with Suspend to the same ng-eNB 117
6.16.3 Protection of Non-IP Data Delivery (NIDD) interfaces 117
6.16.4 Security handling in NAS based redirection from 5GS to EPS 118

7 Security for non-3GPP access to the 5G core network 118
7.1 General 118
7.1a Determining trust relationship in the UE 118
7.2 Security procedures 119
7.2.1 Authentication for Untrusted non-3GPP Access 119

7A Security for trusted non-3GPP access to the 5G core network 121
7A.1 General 121
7A.2 Security procedures 122
7A.2.1 Authentication for trusted non-3GPP access 122
7A.2.2 Void 125
7A.2.3 Key hierarchy for trusted non-3GPP access 125
7A.2.4 Authentication for devices that do not support 5GC NAS over WLAN access 125

7B Security for wireline access to the 5G core network 128
7B.1 General 128
7B.2 Authentication for 5G-RG 128
7B.3 Authentication for FN-RG 130
7B.4 Authentication for UE behind 5G-RG and FN-RG 132
7B.5 Subscriber privacy for wireline access 132
7B.6 Subscriber privacy for N5CW over trusted WLAN access 132

8 Security of interworking 132
8.1 General 132
8.2 Registration procedure for mobility from EPS to 5GS over N26 133
8.3 Handover procedure from 5GS to EPS over N26 134
8.3.1 General 134
8.3.2 Procedure 134
8.4 Handover from EPS to 5GS over N26 137
8.4.1 General 137
8.4.2 Procedure 138
8.5 Idle mode mobility from 5GS to EPS over N26 140
8.5.1 General 140
8.5.2 TAU Procedure 141
8.6 Mapping of security contexts 142
8.6.1 Mapping of a 5G security context to an EPS security context 142
8.6.2 Mapping of an EPS security context to a 5G security context 142
8.7 Interworking without N26 interface in single-registration mode 143

9 Security procedures for non-service based interfaces 143
9.1 General 143
9.1.1 Use of NDS/IP 143
9.1.2 Implementation requirements 143
9.1.3 QoS considerations 143
9.2 Security mechanisms for the N2 interface 144

9.3 Security requirements and procedures on N3 144
9.4 Security mechanisms for the Xn interface 144
9.5 Interfaces based on DIAMETER or GTP 145
9.5.1 Void 145
9.6 Void 145
9.7 Void 145
9.8 Security mechanisms for protection of the gNB internal interfaces 145
9.8.1 General 145
9.8.2 Security mechanisms for the F1 interface 145
9.8.3 Security mechanisms for the E1 interface 146
9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs 146
9.10 Security mechanisms for the interface between W-5GAN and 5GC 147

10 Security aspects of IMS emergency session handling 147
10.1 General 147
10.2 Security procedures and their applicability 147
10.2.1 Authenticated IMS Emergency Sessions 147
10.2.1.1 General 147
10.2.1.2 UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services 147
10.2.1.3 UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services 148
10.2.2 Unauthenticated IMS Emergency Sessions 149
10.2.2.1 General 149
10.2.2.2 UE sets up an IMS Emergency session with emergency registration 149
10.2.2.3 Key generation for Unauthenticated IMS Emergency Sessions 150
10.2.2.3.1 General 150
10.2.2.3.2 Handover 151

11 Security procedures between UE and external data networks via the 5G Network 151
11.1 EAP based secondary authentication by an external DN-AAA server 151
11.1.1 General 151
11.1.2 Authentication 152
11.1.3 Re-Authentication 155
11.1.4 Secondary authentication and authorization revocation 156

12 Security aspects of Network Exposure Function (NEF) 156
12.1 General 156
12.2 Mutual authentication 156
12.3 Protection of the NEF – AF interface 156
12.4 Authorization of Application Function's requests 157
12.5 Support for CAPIF 157

13 Service Based Interfaces (SBI) 157
13.1 Protection at the network or transport layer 157
13.1.0 General 157
13.1.1 TLS protection between NF and SEPP 157
13.1.1.0 General 157
13.1.1.1 TLS protection based on telescopic FQDN and wildcard certificate 158
13.1.1.2 TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header 158
13.1.2 Protection between SEPPs 158
13.2 Application layer security on the N32 interface 159
13.2.1 General 159
13.2.2 N32-c connection between SEPPs 160
13.2.2.1 General 160
13.2.2.2 Procedure for Key agreement and Parameter exchange 161
13.2.2.3 Procedure for error detection and handling in SEPP 162
13.2.2.4 N32-f Context 162
13.2.2.4.0 N32-f parts 162
13.2.2.4.1 N32-f context ID 163
13.2.2.4.2 N32-f peer information 163
13.2.2.4.3 N32-f security context 163
13.2.2.4.4 N32-f context information 163
13.2.3 Protection policies for N32 application layer solution 164
13.2.3.1 Overview of protection policies 164

13.2.3.2 Data-type encryption policy ... 164
13.2.3.3 NF API data-type placement mapping ... 164
13.2.3.4 Modification policy ... 165
13.2.3.5 Provisioning of the policies in the SEPP ... 165
13.2.3.6 Precedence of policies in the SEPP ... 165
13.2.4 N32-f connection between SEPPs ... 166
13.2.4.1 General ... 166
13.2.4.2 Overall Message payload structure for message reformatting at SEPP ... 167
13.2.4.3 Message reformatting in sending SEPP ... 167
13.2.4.3.1 dataToIntegrityProtect ... 167
13.2.4.3.1.1 clearTextEncapsulatedMessage ... 167
13.2.4.3.1.2 metadata ... 167
13.2.4.3.2 dataToIntegrityProtectAndCipher ... 168
13.2.4.4 Protection using JSON Web Encryption (JWE) ... 168
13.2.4.4.0 General ... 168
13.2.4.4.1 N32-f key hierarchy ... 168
13.2.4.5 Message modifications in IPX ... 170
13.2.4.5.1 modifiedDataToIntegrityProtect ... 170
13.2.4.5.2 Modifications by IPX ... 170
13.2.4.6 Protecting IPX modifications using JSON Web Signature (JWS) ... 171
13.2.4.7 Message verification by the receiving SEPP ... 171
13.2.4.8 Procedure ... 171
13.2.4.9 JOSE profile ... 174
13.3 Authentication and static authorization ... 174
13.3.0 Static authorization ... 174
13.3.1 Authentication and authorization between network functions and NRF ... 174
13.3.1.1 Direct communication ... 174
13.3.1.2 Indirect communication ... 174
13.3.1.3 Authorization of discovery request and error handling ... 175
13.3.2 Authentication and authorization between network functions ... 175
13.3.2.1 Direct communication ... 175
13.3.2.2 Indirect communication ... 175
13.3.2.3 Inter-PLMN NF to NF communication ... 176
13.3.2.4 Error handling ... 176
13.3.3 Authentication and authorization between SEPP and network functions ... 176
13.3.4 Authentication and authorization between SEPPs ... 176
13.3.6 Authentication and authorization between SCP and network functions ... 176
13.3.7 Authentication and authorization between SCPs ... 177
13.3.8 Client credentials assertion based authentication ... 177
13.3.8.1 General ... 177
13.3.8.2 Client credentials assertion ... 177
13.3.8.3 Verification of Client credentials assertion ... 178
13.4 Authorization of NF service access ... 178
13.4.1 OAuth 2.0 based authorization of Network Function service access ... 178
13.4.1.0 General ... 178
13.4.1.1 Service access authorization within the PLMN ... 179
13.4.1.1.1 OAuth 2.0 roles ... 179
13.4.1.1.2 Service Request Process ... 179
13.4.1.1A Service access authorization in interconnect scenarios ... 182
13.4.1.2 Service access authorization in roaming scenarios ... 182
13.4.1.2.1 OAuth 2.0 roles ... 182
13.4.1.2.2 Service Request Process ... 183
13.4.1.3 Service access authorization in indirect communication scenarios ... 186
13.4.1.3.1 Authorization for indirect communication without delegated discovery procedure ... 186
13.4.1.3.1.1 With mutual authentication between NF Service Consumer and NRF at the transport layer ... 186
13.4.1.3.1.2 Without mutual authentication between NF and NRF at the transport layer ... 188
13.4.1.3.2 Authorization for indirect communication with delegated discovery procedure ... 189
13.5 Security capability negotiation between SEPPs ... 190

14 Security related services ... 191
14.1 Services provided by AUSF ... 191
14.1.1 General ... 191

14.1.2 Nausf_UEAuthentication service ... 192
14.1.2.1 Nausf_UEAuthentication_Authenticate service operation ... 192
14.1.2.2 Nausf_UEAuthentication_deregister service operation ... 192
14.1.2.3 Nausf_UEAuthentication_ProseAuthenticate service operation ... 193
14.1.3 Nausf_SoRProtection service ... 193
14.1.4 Nausf_UPUProtection service ... 193
14.1.5 Void ... 194
14.2 Services provided by UDM ... 194
14.2.1 General ... 194
14.2.2 Nudm_UEAuthentication_Get service operation ... 194
14.2.3 Nudm_UEAuthentication_ResultConfirmation service operation ... 194
14.2.4 Nudm_UEAuthentication_GetProseAv service operation ... 194
14.2.5 Nudm_UEAuthentication_GetGbaAv service operation ... 194
14.3 Services provided by NRF ... 195
14.3.1 General ... 195
14.3.2 Nnrf_AccessToken_Get Service Operation ... 195
14.4 Services provided by NSSAAF ... 195
14.4.1 Nnssaaf_NSSAA services ... 195
14.4.1.1 General ... 195
14.4.1.2 Nnssaaf_NSSAA_Authenticate service operation ... 196
14.4.1.3 Nnssaaf_NSSAA_Re-AuthenticationNotification service operation ... 196
14.4.1.4 Nnssaaf_NSSAA_RevocationNotification service operation ... 196
14.4.2 Nnssaaf_AIW services ... 196
14.4.2.1 General ... 196
14.4.2.2 Nnssaaf_AIW_Authenticate service operation ... 197

15 Management security for network slices ... 197
15.1 General ... 197
15.2 Mutual authentication ... 197
15.3 Protection of management interactions between the management service consumer and the management service producer ... 198
15.4 Authorization of management service consumer's request ... 198

16 Security procedures for network slices ... 198
16.1 General ... 198
16.2 Authorization for network slice access ... 198
16.3 Network slice specific authentication and authorization ... 199
16.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure ... 201
16.5 AAA Server triggered Slice-Specific Authorization Revocation ... 202
16.6 AF Authorization for network slice quota-usage information notification/retrieval ... 203
16.6.1 Introduction ... 203
16.6.2 General ... 203
16.6.3 Subscription/unsubscription procedure of NSACF notification service ... 203

Annex A (normative): Key derivation functions ... 205

A.1 KDF interface and input parameter construction ... 205
A.1.1 General ... 205
A.1.2 FC value allocations ... 205

A.2 K_{AUSF} derivation function ... 205

A.3 CK' and IK' derivation function ... 205

A.4 RES* and XRES* derivation function ... 206

A.5 HRES* and HXRES* derivation function ... 206

A.6 K_{SEAF} derivation function ... 206

A.7 K_{AMF} derivation function ... 207
A.7.0 Parameters for the input S to the KDF ... 207
A.7.1 ABBA parameter values ... 207

A.8 Algorithm key derivation functions ... 207

A.9 K_{gNB}, K_{WAGF}, K_{TNGF}, K_{TWIF} and K_{N3IWF} derivation function 208
A.10 NH derivation function 209
A.11 K_{NG-RAN}* derivation function for target gNB 209
A.12 K_{NG-RAN}* derivation function for target ng-eNB 209
A.13 K_{AMF} to K_{AMF}' derivation in mobility 210
A.14 K_{AMF} to K_{ASME}' derivation for interworking 210
A.14.1 Idle mode mobility 210
A.14.2 Handover 210
A.15 K_{ASME} to K_{AMF}' derivation for interworking 210
A.15.1 Idle mode mobility 210
A.15.2 Handover 211
A.16 Derivation of K_{SN} for dual connectivity 211
A.17 SoR-MAC-I_{AUSF} generation function 211
A.18 SoR-MAC-I_{UE}/SoR-XMAC-I_{UE} generation function 212
A.19 UPU-MAC-I_{AUSF} generation function 212
A.20 UPU-MAC-I_{UE}/UPU-XMAC-I_{UE} generation function 212
A.21 K_{AMF} to K_{ASME_SRVCC} derivation for interworking 213
A.22 K_{TIPSec} and K_{TNAP} derivation function 213
A.23 K_{IAB} generation function 213
Annex B (informative): Using additional EAP methods for primary authentication 215
B.1 Introduction 215
B.2 Primary authentication and key agreement 215
B.2.1 EAP TLS 215
B.2.1.1 Security procedures 215
B.2.1.2 Privacy considerations 218
B.2.1.2.1 EAP TLS without subscription identifier privacy 218
B.2.1.2.2 EAP TLS with subscription identifier privacy 218
B.2.2 Revocation of subscriber certificates 219
B.3 Key derivation 219
Annex C (normative): Protection schemes for concealing the subscription permanent identifier 221
C.1 Introduction 221
C.2 Null-scheme 221
C.3 Elliptic Curve Integrated Encryption Scheme (ECIES) 222
C.3.1 General 222
C.3.2 Processing on UE side 222
C.3.3 Processing on home network side 223
C.3.4 ECIES profiles 223
C.3.4.0 General 223
C.3.4.1 Profile A 224
C.3.4.2 Profile B 224
C.4 Implementers' test data 225
C.4.1 General 225
C.4.2 Null-scheme 225
C.4.2.1 IMSI-based SUPI 225
C.4.2.2 Network specific identifier-based SUPI 225
C.4.3 ECIES Profile A 225
C.4.3.1 IMSI-based SUPI 225

C.4.3.2 Network specific identifier-based SUPI 226
C.4.4 ECIES Profile B 227
C.4.4.1 IMSI-based SUPI 227
C.4.4.2 Network specific identifier-based SUPI 228

Annex D (normative): Algorithms for ciphering and integrity protection 229

D.1 Null ciphering and integrity protection algorithms 229

D.2 Ciphering algorithms 229
D.2.1 128-bit Ciphering algorithms 229
D.2.1.1 Inputs and outputs 229
D.2.1.2 128-NEA1 230
D.2.1.3 128-NEA2 230
D.2.1.4 128-NEA3 230

D.3 Integrity algorithms 230
D.3.1 128-Bit integrity algorithms 230
D.3.1.1 Inputs and outputs 230
D.3.1.2 128-NIA1 231
D.3.1.3 128-NIA2 231
D.3.1.4 128-NIA3 231

D.4 Test Data for the security algorithms 231
D.4.1 General 231
D.4.2 128-NEA1 231
D.4.3 128-NIA1 231
D.4.4 128-NEA2 231
D.4.5 128-NIA2 232
D.4.6 128-NEA3 232
D.4.7 128-NIA3 232

Annex E (informative): UE-assisted network-based detection of false base station 233

E.1 Introduction 233

E.2 Examples of using measurement reports 233

Annex F (normative): 3GPP 5G profile for EAP-AKA' 234

F.1 Introduction 234

F.2 Subscriber privacy 234

F.3 Subscriber identity and key derivation 235

F.4 Void 235

Annex G (informative): Application layer security on the N32 interface 235

G.1 Introduction 235

G.2 Structure of HTTP Message 236

Annex H (informative): Void 238

Annex I (normative): Non-public networks 239

I.1 General 239

I.2 Authentication in standalone non-public networks 239
I.2.1 General 239
I.2.2 EAP framework, selection of authentication method, and EAP method credentials 239
I.2.2.1 General 239
I.2.2.2 Credentials holder using AAA server for primary authentication 240
I.2.2.2.1 General 240
I.2.2.2.2 Procedure 240
I.2.3 Key hierarchy, key derivation and key distribution 242

I.2.3.1 General 242
I.2.3.2 Credentials holder using AAA server for primary authentication 243
I.2.4 Credentials Holder using AUSF and UDM for primary authentication 243

I.3 Serving network name for standalone non-public networks 243
I.3.1 General 243
I.3.2 Definition of SN Id for standalone non-public networks 244

I.4 Modification of CAG ID list in the UE 244

I.5 SUPI privacy for standalone non-public networks 244

I.6 Authentication in Public Network Integrated Non-Public Networks (PNI-NPN) 244

I.7 Authorization aspects in SNPNs 244
I.7.1 Credentials holder using AUSF and UDM for primary authentication 244

I.8 SEPP and interconnect related security procedures 245
I.8.1 Credentials holder using AUSF and UDM for primary authentication 245

I.9 Security of UE onboarding in SNPNs 245
I.9.1 General 245
I.9.2 Authentication 245
I.9.2.1 Requirements 245
I.9.2.2 Primary authentication without using DCS 245
I.9.2.3 Primary authentication using DCS 246
I.9.2.4 Secondary authentication 246
I.9.2.4.1 Secondary authentication using DCS 246
I.9.2.4.2 Secondary authentication using DN-AAA 246

Annex J (normative): SRVCC from 5G to UTRAN 247

J.1 SRVCC from NR to UTRAN 247
J.1.1 General 247
J.1.2 Procedure 247

J.2 Emergency call in SRVCC from NR to UTRAN 248
J.2.1 General 248
J.2.2 Procedure 248

Annex K (normative): Security for 5GLAN services 249

K.1 General 249

K.2 Authentication and authorization 249

K.3 Handling of UP security policy 249

Annex L (normative): Security for TSC service 250

L.1 General 250

L.2 Access security for a 5GS TSC-enabled UE 250

L.3 Protection of user plane data in TSC including (g)PTP control messages in bridge mode 250

L.4 Exposure of time synchronisation 250

Annex M (normative): Security for Integrated Access and Backhaul (IAB) 251

M.1 General 251

M.2 Security requirements and features 251
M.2.1 Requirements on the IAB-node (IAB-UE) 251
M.2.2 Requirements on the IAB donor 251
M.2.3 Requirements on the 5GC supporting IAB architecture 251
M.2.4 Requirements for secure environment 251
M.2.5 Requirements on the F1 interface 251

M.3 IAB-node Integration Procedure 252
M.3.1 General 252
M.3.2 Authentication and Authorization of IAB-node (Phase-1) 252
M.3.3 Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (Phase-3) 252
M.3.3.1 General 252
M.3.3.2 Security mechanisms for the F1 interface 252
M.4 Protection of management traffic between IAB-node and OAM 253
M.5 IAB inter-CU topology adaptation and backhaul RLF recovery procedure 253
Annex N (normative): Security for URLLC services 254
N.1 General 254
N.2 Security support on redundant transmission 254
N.2.1 Redundant user plane paths based on dual connectivity 254
N.2.1.1 Introduction 254
N.2.2.2 Security policy aspects 254
N.2.2 Redundant transmission on N3/N9 interfaces 255
Annex O (Informative): Authentication for non-5G capable devices behind residential gateways 256
O.1 General 256
O.2 Baseline for using non-5G capable devices with 5GC 256
O.3 Authentication procedure 256
Annex P (informative): Security aspects of DNS and ICMP 261
P.1 General 261
P.2 Security aspects of DNS 261
P.3 Security aspects of ICMP 261
Annex Q (informative): Security and privacy in 5G system location services 261
Annex R (informative): Authorization aspects in communication models for NF/NF services interaction 262
Annex S (normative): Support for Non-seamless WLAN offload (NSWO) in 5GS 264
S.1 Introduction 264
S.2 General 264
S.3 Authentication procedure 264
S.3.1 5G NSWO co-existence with EPS NSWO 264
S.3.2 5G NSWO procedures 265
S.4 Roaming 266
Annex T (normative): Security for edge computing 267
T.1 General 267
T.2 Security of network exposure to edge application server 267
T.3 Security of EAS discovery procedure via EASDF in non-roaming Scenario 267
Annex U (informative): Primary authentication using EAP-TTLS in SNPNs 268
U.1 Introduction 268
U.2 Procedure 268
Annex V (normative): User consent requirements and mechanisms 271

V.1 General 271
V.1.1 Scope 271
V.1.2 Relationship between end-users and subscriber 271
V.2 Requirements 271
V.3 User consent check 271
V.4 User consent revocation 272
Annex W (normative): Security for multicast/broadcast service for 3GPP service 273
W.1 General 273
W.2 Security requirements 273
W.2.1 Requirements of MBSF 273
W.2.2 Requirements of MBSTF 273
W.3 Security mechanisms for xMB-C/MB2-C and xMB-U/MB2-U interface 273
W.4 Security mechanisms for MBS traffic transmission 273
W.4.1 Key derivation, management and distribution 273
W.4.1.1 General 273
W.4.1.2 Control-plane procedure 273
W.4.1.3 User-plane procedure 274
W.4.2 Protection of the traffic transmission 275
W.4.3 Authentication and authorization aspects for the multicast session 275
W.5 Security protection for interworking between 5MBS and eMBMS 275
Annex X (normative): Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2 276
X.1 General 276
X.7 User consent requirements 281
Annex Y (normative): Security aspects of the Message Service for MIoT over the 5G System (MSGin5G) 282
Y.1 General 282
Y.2 Authentication and authorization between MSGin5G client and MSGin5G Server 282
Y.3 Transport security protection for MSGin5G interfaces 282
Y.4 Authentication and Authorization between Application Server and MSGin5G Server 283
Y.5 Authentication and Authorization between message Gateway and MSGin5G Server 283
Annex Z (informative): Change history 284

Foreword

This Technical Standard has been transposed from the technical specification produced by the 3rd Generation Partnership Project (3GPP), of which, TSDSI is an Organizational Partner.

The contents of the 3GPP Specification document are subject to continuing work within the 3GPP 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.

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the 5G System and the 5G Core, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio.

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 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

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

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[25] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

[26] Void

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

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available http://www.secg.org/sec1-v2.pdf

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at http://www.secg.org/sec2-v2.pdf

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] Void

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] IETF RFC 9048: "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

[77] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[94] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition".

[95] 3GPP TS 29.502: "5G System; Session Management Services".

[96] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services".

[97] 3GPP TS 23.402: "Authentication enhancements for non-3GPP accesses".

[98] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[99] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN.

[102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[108] 3GPP TS 26.502: "5G multicast–broadcast services; User Service architecture".

[109] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[110] IETF RFC 4555 (2006-06): "RFC IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[111] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

3 Definitions and abbreviations

3.1 Definitions

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

5G security context: The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

5G AS security context for 3GPP access: The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network side, UP security activation status and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

NOTE 4: UP security activation status is sent from gNB/ng-eNB in step 1b in clause 6.6.2 corresponding to the active PDU session(s).

5G AS security context for non-3GPP access: The key K_{N3IWF}, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

5G AS Secondary Cell security context: The cryptographic keys at AS level for secondary cell with their identifiers, the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

5G Home Environment Authentication Vector: authentication data consisting of RAND, AUTN, XRES*, and K_{AUSF} for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm_UEAuthentication_Get Response.

5G Authentication Vector: authentication data consisting of RAND, AUTN, HXRES*, and K_{SEAF}.

NOTE 3b: This vector is received by the SEAF from the AUSF in the Nausf_Authentication_Authenticate Response.

5G NAS security context: The key K_{AMF} with the associated key set identifier, the UE security capabilities, the uplink and downlink NAS COUNT values.

NOTE 4: The distinction between native 5G security context and mapped 5G security context also applies to 5G NAS security contexts. The 5G NAS security context is called "full" if it additionally contains the integrity and encryption keys and the associated identifiers of the selected NAS integrity and encryption algorithms.

5G Serving Environment Authentication Vector: a vector consisting of RAND, AUTN and HXRES*.

ABBA parameter: Parameter that provides antibidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network.

activation of security context: The process of taking a security context into use.

anchor key: The security key K_{SEAF} provided during authentication and used for derivation of subsequent security keys.

application Layer Security: mechanism by which HTTP messages, exchanged between a Network Function in one PLMN and a Network Function in another PLMN, are protected on the N32-f interface between the two SEPPs in the two PLMNs.

authentication data: An authentication vector or transformed authentication vector.

authentication vector: A vector consisting of CK, IK, RAND, AUTN, and XRES.

backward security: The property that for an entity with knowledge of K_n, it is computationally infeasible to compute any previous K_{n-m} (m>0) from which K_n is derived.

NOTE 5: In the context of K_{gNB} key derivation, backward security refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to compute any previous K_{gNB} that has been used between the same UE and a previous gNB.

CM-CONNECTED state: This is as defined in TS 23.501 [2].

NOTE5a: The term CM-CONNECTED state corresponds to the term 5GMM-CONNECTED mode used in TS 24.501 [35].

CM-IDLE state: As defined in TS 23.501 [2].

NOTE5b: The term CM-IDLE state corresponds to the term 5GMM-IDLE mode used in TS 24.501 [35].

consumer's IPX (cIPX): IPX provider entity with a business relationship with the cSEPP operator.

consumer's NRF (cNRF): The NRF that authenticates the service consumer NF and resides in the PLMN where the service consumer NF is located.

consumer's PLMN (cPLMN): The PLMN where the service consumer NF is located**.**

consumer's SEPP (cSEPP): The SEPP residing in the PLMN where the service consumer NF is located.

Credentials Holder: As defined in TS 23.501 [2].

current 5G security context: The security context which has been activated most recently.

NOTE5c: A current 5G security context originating from either a mapped or native 5G security context can exist simultaneously with a native non-current 5G security context.

Default Credentials Server: As defined in TS 23.501[2].

Default UE credentials: As defined in TS 23.501[2].

forward security: The fulfilment of the property that for an entity with knowledge of K_m that is used between that entity and a second entity, it is computationally infeasible to predict any future K_{m+n} (n>0) used between a third entity and the second entity.

NOTE 6: In the context of K_{gNB} key derivation, forward security refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to predict any future K_{gNB} that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n=1 or more).

full native 5G security context: A native 5G security context for which the 5G NAS security context is full according to the above definition.

NOTE6a: A full native 5G security context is either in state "current" or state "non-current".

Home Network Identifier: An identifier identifying the home network of the subscriber.

NOTE6b: Described in detail in TS 23.003 [19].

Home Network Public Key Identifier: An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI.

NOTE6c: Described in this document and detailed in TS 23.003 [19].

IAB-donor-CU: As defined in TS 38.401 [78] .

IAB-donor-DU: As defined in TS 38.401 [78].

IAB-node: As defined in TS 38.300 [52].

IAB-donor gNB: As defined in TS 38.300 [52].

IAB-UE: The function within an IAB node, which behaves as a UE.

mapped 5G security context: An 5G security context, whose K_{AMF} was derived from EPS keys during interworking and which is identified by mapped ngKSI.

Master node: As defined in TS 37.340 [51].

N32-c connection: A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.

NOTE 6d: This is a short-lived connection that is used between the SEPPs for negotiation of the N32-f protection mechanism, cipher suite and protection policy exchange, and error notifications. Every N32-f connection requires an N32-c connection that was established before establishing N32-f.

N32-f connection: Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.

NOTE 6e: When IPX providers are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

native 5G security context: An 5G security context, whose K_{AMF} was created by a run of primary authentication and which is identified by native ngKSI.

ng-eNB: As defined in TS 38.300 [52].

NG-RAN node: gNB or ng-eNB (as defined in TS 38.300 [52]).

non-current 5G security context: A native 5G security context that is not the current one.

NOTE 7: A non-current 5G security context may be stored along with a current 5G security context in the UE and the AMF. A non-current 5G security context does not contain 5G AS security context. A non-current 5G security context is either of type "full native" or of type "partial native".

Operator Group Roaming Hub: Roaming hub used by a group of network operators that reside in the same security domain to consolidate and secure operator group roaming.

partial native 5G security context: A partial native 5G security context consists of K_{AMF} with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values, which are initially set to zero before the first NAS SMC procedure for this security context.

NOTE 8: A partial native 5G security context is created by primary authentication, for which no corresponding successful NAS SMC has been run. A partial native context is always in state "non-current".

producer's IPX (pIPX): IPX provider entity with a business relationship with the pSEPP operator.

producer's NRF (pNRF): The NRF where the service producer NF is registered in the PLMN where the service producer NF is located.

producer's PLMN (pPLMN): The PLMN where the service producer NF is located.

producer's SEPP (pSEPP): The SEPP residing in the PLMN where the service producer NF is located.

Protection Scheme Identifier: An identifier identifying a protection scheme that is used for concealing the SUPI.

RM-DEREGISTERED state: This is as defined in TS 23.501 [2].

NOTE8a: The term RM-DEREGISTERED state corresponds to the term 5GMM-DEREGISTERED mode used in TS 24.501 [35].

RM-REGISTERED state: As defined in TS 23.501 [2].

NOTE8b: The term RM-REGISTERED state corresponds to the term 5GMM-REGISTERED mode used in TS 24.501 [35].

Routing Indicator: An indicator defined in TS 23.003 [19] that can be used for AUSF or UDM selection.

Scheme Output: the output of a public key protection scheme used for SUPI protection.

security anchor function: The function SEAF that serves in the serving network as the anchor for security in 5G.

Secondary node: As defined in TS 37.340 [51].

subscription credential(s): The set of values in the USIM and in the home operator's network, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

subscription identifier: The SUbscription Permanent Identifier (SUPI).

NOTE8c: As defined in TS 23.501 [2] and detailed in 23.003 [19].

subscription concealed identifier: A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.

NOTE8d: Defined in the present document; detailed in TS 23.003 [19].

subscription identifier de-concealing function: The Subscription Identifier De-concealing Function (SIDF) service offered by the network function UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI.

transformed authentication vector: an authentication vector where CK and IK have been replaced with CK' and IK'.

UE 5G security capability: The UE security capabilities for 5G AS and 5G NAS.

UE security capabilities: The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

NOTE 9: This includes capabilities for NG-RAN and 5G NAS, and includes capabilities for EPS, UTRAN and GERAN if these access types are supported by the UE.

3.2 Abbreviations

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

5GC	5G Core Network
5G-AN	5G Access Network
5G-RG	5G Residential Gateway
NG-RAN	5G Radio Access Network

5G AV	5G Authentication Vector
5G HE AV	5G Home Environment Authentication Vector
5G NSWO	5G Non-Seamless WLAN Offload
5G SE AV	5G Serving Environment Authentication Vector
ABBA	Anti-Bidding down Between Architectures
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AMF	Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
AUTN	AUthentication TokeN
AV	Authentication Vector
AV'	transformed Authentication Vector
BAP	Backhaul Adaptation Protocol
BH	Backhaul
CCA	Client Credentials Assertion
Cell-ID	Cell Identity as used in TS 38.331 [22]
CH	Credentials Holder
CHO	Conditional Handover
CIoT	Cellular Internet of Things
cIPX	consumer's IPX
CK_{SRVCC}	Cipher Key for Single Radio Voice Continuity
cNRF	consumer's NRF
CP	Control Plane
CPA	Conditional PSCell Addition
CPC	Conditional PSCell Change
cPLMN	consumer's PLMN
cSEPP	consumer's SEPP
CTR	Counter (mode)
CU	Central Unit
DCS	Default Credentials Server
DN	Data Network
DNN	Data Network Name
DU	Distributed Unit
EAP	Extensible Authentication Protocol
EDT	Early Data Transmission
EMSK	Extended Master Session Key
EN-DC	E-UTRA-NR Dual Connectivity
ENSI	External Network Slice Information
EPS	Evolved Packet System
FN-RG	Fixed Network RG
gNB	NR Node B
GUTI	Globally Unique Temporary UE Identity
HRES	Hash RESponse
HXRES	Hash eXpected RESponse
IAB	Integrated Access and Backhaul
IKE	Internet Key Exchange
IK_{SRVCC}	Integrity Key for Single Radio Voice Continuity
IPUPS	Inter-PLMN UP Security
IPX	IP exchange service
KSI	Key Set Identifier
KSI_{SRVCC}	Key Set Identifier for Single Radio Voice Continuity
LI	Lawful Intercept
MBSF	Multicast/Broadcast Service Function
MBSSF	Multicast/Broadcast Service Security Function
MBSTF	Multicast/Broadcast Service Transport Function
MeNB	Master eNB

MN	Master Node
MO-EDT	Mobile Originated Early Data Transmission
MT-EDT	Mobile Terminated Early Data Transmission
MR-DC	Multi-Radio Dual Connectivity
MSK	Master Session Key
N3IWF	Non-3GPP access InterWorking Function
NAI	Network Access Identifier
NAS	Non Access Stratum
NDS	Network Domain Security
NEA	Encryption Algorithm for 5G
NF	Network Function
NG	Next Generation
ng-eNB	Next Generation Evolved Node-B
ngKSI	Key Set Identifier in 5G
N5CW	Non-5G-Capable over WLAN
N5GC	Non-5G-Capable
NIA	Integrity Algorithm for 5G
NR	New Radio
NR-DC	NR-NR Dual Connectivity
NSSAI	Network Slice Selection Assistance Information
NSSAA	Network Slice Specific Authentication and Authorization
NSWO	Non-Seamless WLAN Offload
NSWOF	Non-Seamless WLAN Offload Function
PDN	Packet Data Network
PEI	Permanent Equipment Identifier
pIPX	producer's IPX
pNRF	producer's NRF
pPLMN	producer's PLMN
PRINS	PRotocol for N32 INterconnect Security
pSEPP	producer's SEPP
PUR	Preconfigured Uplink Resource
QoS	Quality of Service
RES	RESponse
SCG	Secondary Cell Group
SEAF	SEcurity Anchor Function
SCP	Service Communication Proxy
NOTE: Void.	Security Gateway
SEPP	Security Edge Protection Proxy
SgNB	Secondary gNB
SIDF	Subscription Identifier De-concealing Function
SMC	Security Mode Command
SMF	Session Management Function
SN	Secondary Node
SN Id	Serving Network Identifier
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TWAP	Trusted WLAN Access Point
TWIF	Trusted WLAN Interworking Function
TSC	Time Sensitive Communication
UE	User Equipment
UEA	UMTS Encryption Algorithm
UDM	Unified Data Management
UDR	Unified Data Repository
UIA	UMTS Integrity Algorithm
ULR	Update Location Request
UP	User Plane
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module
XRES eXpected RESponse

4 Overview of security architecture

4.1 Security domains

Figure 4-1 gives an overview of security architecture.

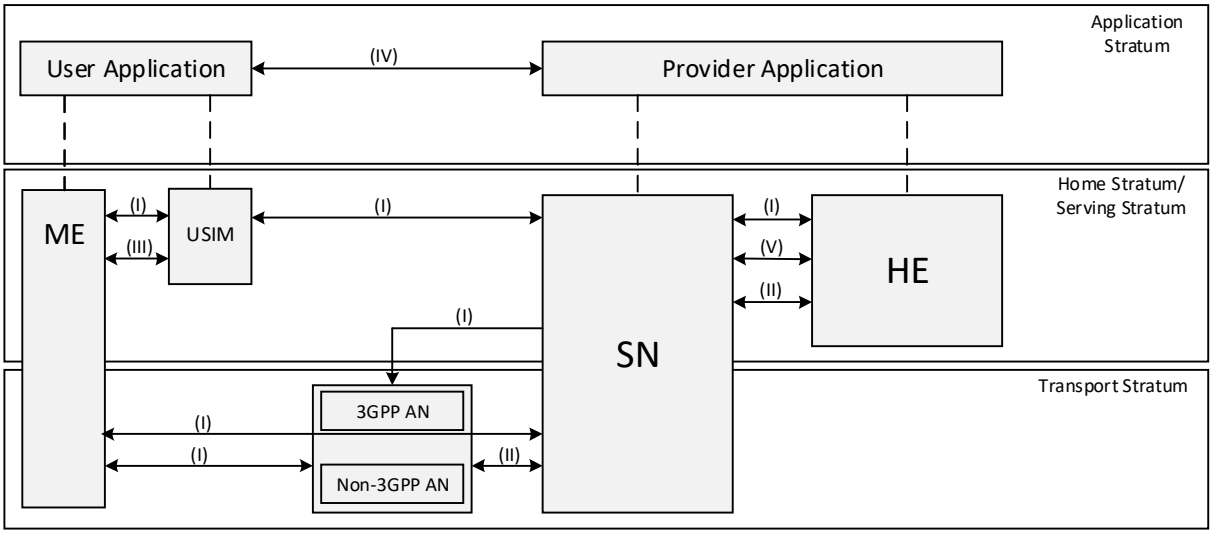


Figure 4-1: Overview of the security architecture

The figure illustrates the following security domains:

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.

- Network domain security (II): the set of security features that enable network nodes to securely exchange signalling data and user plane data.

- User domain security (III): the set of security features that secure the user access to mobile equipment.

- Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Application domain security is out of scope of the present document.

- SBA domain security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains . Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [10].

- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

NOTE: The visibility and configurability of security is not shown in the figure.

4.2 Security at the perimeter of the 5G Core network

4.2.0 General

The security specified in this document applies to both roaming and PLMN interconnect.

Editor's Note: check full specification on removing references to roaming unless specific to roaming.

4.2.1 Security Edge Protection Proxy (SEPP)

The 5G System architecture introduces a Security Edge Protection Proxy (SEPP) as an entity sitting at the perimeter of the PLMN for protecting control plane messages.

The SEPP enforces inter-PLMN security on the N32 interface.

4.2.2 Inter-PLMN UP Security (IPUPS)

The 5G System architecture introduces Inter-PLMN UP Security (IPUPS) at the perimeter of the PLMN for protecting user plane messages.

The IPUPS is a functionality of the UPF that enforces GTP-U security on the N9 interface between UPFs of the visited and home PLMNs.

NOTE: IPUPS can be activated with other functionality in a UPF or activated in a UPF that is dedicated to be used for IPUPS functionality (see also TS 23.501 [2], clause 5.8.2.14).

4.3 Security entities in the 5G Core network

The 5G System architecture introduces the following security entities in the 5G Core network:

AUSF: AUthentication Server Function;

ARPF: Authentication credential Repository and Processing Function;

SIDF: Subscription Identifier De-concealing Function;

SEAF: SEcurity Anchor Function.

5 Security requirements and features

5.1 General security requirements

5.1.1 Mitigation of bidding down attacks

An attacker could attempt a bidding down attack by making the UE and the network entities respectively believe that the other side does not support a security feature, even when both sides in fact support that security feature. It shall be ensured that a bidding down attack, in the above sense, can be prevented.

5.1.2 Authentication and Authorization

The 5G system shall satisfy the following requirements.

Subscription authentication: The serving network shall authenticate the Subscription Permanent Identifier (SUPI) in the process of authentication and key agreement between UE and network.

Serving network authentication: The UE shall authenticate the serving network identifier through implicit key authentication.

NOTE 1: The meaning of 'implicit key authentication' here is that authentication is provided through the successful use of keys resulting from authentication and key agreement in subsequent procedures.

NOTE 2: The preceding requirement does not imply that the UE authenticates a particular entity, e.g. an AMF, within a serving network.

UE authorization: The serving network shall authorize the UE through the subscription profile obtained from the home network. UE authorization is based on the authenticated SUPI.

Serving network authorization by the home network: Assurance shall be provided to the UE that it is connected to a serving network that is authorized by the home network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful authentication and key agreement run.

Access network authorization: Assurance shall be provided to the UE that it is connected to an access network that is authorized by the serving network to provide services to the UE. This authorization is 'implicit' in the sense that it is implied by a successful establishment of access network security. This access network authorization applies to all types of access networks.

Unauthenticated Emergency Services: In order to meet regulatory requirements in some regions, the 5G system shall support unauthenticated access for emergency services. This requirement applies to all MEs and only to those serving networks where regulatory requirements for unauthenticated emergency services exist. Serving networks located in regions where unauthenticated emergency services are forbidden shall not support this feature.

5.1.3 Requirements on 5GC and NG-RAN related to keys

The 5GC and NG-RAN shall allow for use of encryption and integrity protection algorithms for AS and NAS protection having keys of length 128 bits. The network interfaces shall support the transport of 256 bit keys.

The keys used for UP, NAS and AS protection shall be dependent on the algorithm with which they are used.

5.2 Requirements on the UE

5.2.1 General

The support and usage of ciphering and integrity protection between the UE and the ng-eNB is identical to the support and usage of ciphering and integrity protection between the UE and the eNB as specified in TS 33.401 [10] with the following additional requirement(s):

- The UE shall support the use of integrity protection with the ng-eNB over the Uu interface if it supports E-UTRA connected to 5GC.
- The UE shall indicate its support of integrity protection with the ng-eNB if it supports E-UTRA connected to 5GC.

The PEI shall be securely stored in the UE to ensure the integrity of the PEI.

5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

5.2.4 Secure storage and processing of subscription credentials

The following requirements apply for the storage and processing of the subscription credentials used to access the 5G network:

The subscription credential(s) shall be integrity protected within the UE using a tamper resistant secure hardware component.

The long-term key(s) of the subscription credential(s) (i.e. K) shall be confidentiality protected within the UE using a tamper resistant secure hardware component.

The long-term key(s) of the subscription credential(s) shall never be available in the clear outside of the tamper resistant secure hardware component.

The authentication algorithm(s) that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.

It shall be possible to perform a security evaluation / assessment according to the respective security requirements of the tamper resistant secure hardware component.

NOTE: The security assessment scheme used for the security evaluation of the tamper resistant secure hardware component is outside the scope of 3GPP specifications.

5.2.5 Subscriber privacy

The UE shall support 5G-GUTI.

The SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC).

The Home Network Public Key shall be stored in the USIM.

The protection scheme identifier shall be stored in the USIM.

The Home Network Public Key Identifier shall be stored in the USIM.

The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in USIM.

The ME shall support the null-scheme.If the home network has not provisioned the Home Network Public Key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME.

Based on home operator's decision, indicated by the USIM, the calculation of the SUCI shall be performed either by the USIM or by the ME.

NOTE 1: If the SUCI calculation indication is not present, the calculation is in the ME.

In case of an unauthenticated emergency call, privacy protection for SUPI is not required.

Provisioning, and updating the Home Network Public Key, Home Network Public Key Identifier, protection scheme identifier, Routing Indicator, and SUCI calculation indication in the USIM shall be in the control of the home network operator.

NOTE 2: The provisioning and updating of the Home Network Public Key, Home Network Public Key Identifier, protection scheme identifier, and SUCI calculation indication is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism. Routing Indicator can be updated, e.g., by OTA or as defined in clause 6.15.

Subscriber privacy enablement shall be under the control of the home network of the subscriber.

The UE shall only send the PEI in the NAS protocol after NAS security context is established, unless during emergency registration when no NAS security context can be established.

The Routing Indicator shall be stored in the USIM. If the Routing Indicator is not present in the USIM, the ME shall set it to a default value as defined in TS 23.003 [19].

5.3 Requirements on the gNB

5.3.1 General

The security requirements given in this clause apply to all types of gNBs. More stringent requirements for specific types of gNBs may be defined in other 3GPP specifications.

5.3.2 User data and signalling data confidentiality

The gNB shall support ciphering of user data between the UE and the gNB.

The gNB shall activate ciphering of user data based on the security policy sent by the SMF.

The gNB shall support ciphering of RRC-signalling.

The gNB shall implement the following ciphering algorithms:

- NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The gNB may implement the following ciphering algorithm:

- 128-NEA3 as defined in Annex D of the present document.

Confidentiality protection of user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.3.3 User data and signalling data integrity

The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

The gNB shall activate integrity protection of user data based on the security policy sent by the SMF.

The gNB shall support integrity protection and replay protection of RRC-signalling.

The gNB shall support the following integrity protection algorithms:

- NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The gNB may support the following integrity protection algorithm:

- 128-NIA3 as defined in Annex D of the present document.

Integrity protection of the user data between the UE and the gNB is optional to use, and shall not use NIA0.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB. NIA0 will add an unnecessary overhead of 32-bits MAC with no security benefits.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

NIA0 shall be disabled in gNB in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

5.3.4 Requirements for the gNB setup and configuration

Setting up and configuring gNBs by O&M systems shall be authenticated and authorized by gNB so that attackers shall not be able to modify the gNB settings and software configurations via local or remote access.

- The certificate enrolment mechanism specified in TS 33.310 [5] for base station should be supported for gNBs. The decision on whether to use the enrolment mechanism is left to operators.

- Communication between the O&M systems and the gNB shall be confidentiality, integrity and replay protected from unauthorized parties. The security associations between the gNB and an entity in the 5G Core or in an O&M domain trusted by the operator shall be supported. These security association establishments shall be mutually authenticated. The security associations shall be realized according to TS 33.210 [3] and TS 33.310 [5].

- The gNB shall be able to ensure that software/data change attempts are authorized.

- The gNB shall use authorized data/software.

- Sensitive parts of the boot-up process shall be executed with the help of the secure environment.

- Confidentiality of software transfer towards the gNB shall be ensured.

- Integrity protection of software transfer towards the gNB shall be ensured.

- The gNB software update shall be verified before its installation (cf. sub-clause 4.2.3.3.5 of TS 33.117 [24]).

5.3.5 Requirements for key management inside the gNB

The 5GC provides subscription specific session keying material for the gNBs, which also hold long term keys used for authentication and security association setup purposes. Protecting all these keys is important. The following requirements apply:

- Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment except when done in accordance with this or other 3GPP specifications.

5.3.6 Requirements for handling user plane data for the gNB

The following requirements apply:

- Any part of a gNB deployment that stores or processes user plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then user plane data in cleartext shall be stored and processed in a secure environment.

5.3.7 Requirements for handling control plane data for the gNB

The following requirements apply:

- Any part of a gNB deployment that stores or processes control plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then control plane data in cleartext shall be stored and processed in a secure environment.

5.3.8 Requirements for secure environment of the gNB

The secure environment is logically defined within the gNB. It ensures protection and secrecy of all sensitive information and operations from any unauthorized access or exposure. The following list defines the requirements of the secure environment:

- The secure environment shall support secure storage of sensitive data, e.g. long-term cryptographic secrets and vital configuration data.
- The secure environment shall support the execution of sensitive functions, e.g. en-/decryption of user data and the basic steps within protocols which use long term secrets (e.g. in authentication protocols).
- The secure environment shall support the execution of sensitive parts of the boot process.
- The secure environment's integrity shall be assured.
- Only authorised access shall be granted to the secure environment, i.e. to data stored and used within it, and to functions executed within it.

5.3.9 Requirements for the gNB F1 interfaces

Requirements given below apply to gNBs with split DU-CU implementations using F1 interface defined in TS 38.470 [31]. Signalling traffic (i.e. both F1-C interface management traffic defined in TS 38.470 [31] and F1-C signalling bearer defined in TS 38.472 [32]) and user plane data can be sent on the F1 interface between a given DU and its CU.

- F1-C interface shall support confidentiality, integrity and replay protection.
- All management traffic carried over the CU-DU link shall be integrity, confidentiality and replay protected.
- The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane.
- F1-C and management traffic carried over the CU-DU link shall be protected independently from F1-U traffic.

NOTE: The above requirements allow to have F1-U protected differently (including turning integrity and/or encryption off or on for F1-U) from all other traffic on the CU-DU (e.g. the traffic over F1-C).

5.3.10 Requirements for the gNB E1 interfaces

Requirements given below apply to gNBs with split DU-CU implementations, particularly with an open interface between CU-CP and CU-UP using the E1 interface defined in TS 38.460 [41].

- The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected.

5.4 Requirements on the ng-eNB

The security requirements for ng-eNB are as specified for eNB in TS 33.401 [10] with the following additional requirement:

- ng-eNB shall support the use of integrity protection with the UE over the Uu interface.

5.5 Requirements on the AMF

5.5.1 Signalling data confidentiality

The AMF shall support ciphering of NAS-signalling.

The AMF shall support the following ciphering algorithms:

- NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The AMF may support the following ciphering algorithm:

- 128-NEA3 as defined in Annex D of the present document.

Confidentiality protection NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

5.5.2 Signalling data integrity

The AMF shall support integrity protection and replay protection of NAS-signalling.

The AMF shall support the following integrity protection algorithms:

- NIA-0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The AMF may support the following integrity protection algorithm:

- 128-NIA3 as defined in Annex D of the present document.

NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected with an algorithm different to NIA-0 except for emergency calls.

5.5.3 Subscriber privacy

The AMF shall support to trigger primary authentication using the SUCI.

The AMF shall support assigning 5G-GUTI to the UE.

The AMF shall support reallocating 5G-GUTI to UE.

The AMF shall be able to confirm SUPI from UE and from home network. The AMF shall deny service to the UE if this confirmation fails.

5.6 Requirements on the SEAF

The security anchor function (SEAF) provides the authentication functionality via the AMF in the serving network. The SEAF shall fulfil the following requirements:

The SEAF shall support primary authentication using SUCI.

5.7 Void

5.8 Requirements on the UDM

5.8.1 Generic requirements

The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected.

NOTE 1: Security mechanisms for protection of subscription credentials in ARPF are left to implementation.

NOTE 2: Security mechanisms for storage of subscription credentials in the UDR and for the transfer of authentication subscription data (as specified in 3GPP TS 29.505 [70]) between UDR and ARPF are left to implementation.

5.8.2 Subscriber privacy related requirements to UDM and SIDF

The SIDF is responsible for de-concealment of the SUCI and shall fulfil the following requirements:

- The SIDF shall be a service offered by UDM.
- The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.

The Home Network Private Key used for subscriber privacy shall be protected from physical attacks in the UDM.

The UDM shall hold the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy.

The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.

5.8a Requirements on AUSF

The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access.

The AUSF shall provide SUPI to the VPLMN only after authentication confirmation if authentication request with SUCI was sent by VPLMN.

The AUSF shall inform the UDM that a successful or unsuccessful authentication of a subscriber has occurred.

5.9 Core network security

5.9.1 Trust boundaries

It is assumed for the set of requirements in this sub-clause that mobile network operators subdivide their networks into trust zones. Subnetworks of different operators are assumed to lie in different trust zones. Messages that traverse trust

boundaries shall follow the requirements in sub-clause 5.9.2 of the present document, if not protected end to end by NDS/IP as specified in TS 33.210 [3].

5.9.2 Requirements on service-based architecture

5.9.2.1 Security Requirements for service registration, discovery and authorization

NF Service based discovery and registration shall support confidentiality, integrity, and replay protection.

NRF shall be able to ensure that NF Discovery and registration requests are authorized.

NF Service based discovery and registration shall be able to hide the topology of the available / supported NF's in one administrative/trust domain from entities in different trust/administrative domains (e.g. between NFs in the visited and the home networks.)

NF Service Request and Response procedure shall support mutual authentication between NF Service Consumer and NF Service Producer.

Each NF shall validate all incoming messages. Messages that are not valid according to the protocol specification and network state shall be either rejected or discarded by the NF.

5.9.2.2 NRF security requirements

The Network Repository Function (NRF) receives NF Discovery Request from an NF instance, provides the information of the discovered NF instances to the NF instance, and maintains NF profiles.

The following NRF service-based architecture security requirements shall apply:

NRF and NFs that are requesting service shall be mutually authenticated.

NRF may provide authentication and authorization to NFs for establishing secure communication between each other

5.9.2.3 NEF security requirements

The Network Exposure Function (NEF) supports external exposure of capabilities of Network Functions to Application Functions, which interact with the relevant Network Functions via the NEF.

The interface between the NEF and the Application Function shall fulfil the following requirements:

- Integrity protection, replay protection and confidentiality protection for communication between the NEF and Application Function shall be supported.
- Mutual authentication between the NEF and Application Function shall be supported.
- Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain.
- SUPI shall not be sent outside the 3GPP operator domain by NEF.

The NEF shall be able to determine whether the Application Function is authorized to interact with the relevant Network Functions..

5.9.2.4 Requirements on the Service Communication Proxy (SCP)

The SCP has interfaces with Network Functions (NF) and peer SCPs within the PLMN (or SNPN). The interface between the SCP and the NFs and between the two SCPs shall fulfil the following requirements:

- Mutual authentication shall be performed between the SCP and NFs, and between the two SCPs within the PLMN (or SNPN).
- All communication between the SCP and NFs and between SCPs shall be confidentiality, integrity and replay protected.

If SCP endpoints are co-located with the NFs, the above two requirements may be satisfied by colocation.

The SCP shall provide confidentiality, integrity and replay protection for its internal communication over SCP internal network interfaces.

If the signalling message (service/subscription request or notification message) from the sending NF does not include the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header and the sending SCP can determine the PLMN ID or SNPN ID value to be included in the 3gpp-Sbi-Originating-Network-Id header, the sending SCP should include it.

5.9.3 Requirements for e2e core network interconnection security

5.9.3.1 General

The present sub-clause contains requirements common to sub-clauses 5.9.2 and 5.9.3.

A solution for e2e core network interconnection security shall satisfy the following requirements.

The solution shall support application layer mechanisms for addition, deletion and modification of message elements by intermediate nodes except for specific message elements described in the present document.

NOTE: Typical example for such a case is IPX providers modifying messages for routing purposes.

The solution shall provide confidentiality and/or integrity end-to-end between source and destination network for specific message elements identified in the present document. For this requirement to be fulfilled, the SEPP – cf [2], clause 6.2.17 shall be present at the edge of the source and destination networks dedicated to handling e2e Core Network Interconnection Security. The confidentiality and/or integrity for the message elements is provided between two SEPPs of the source and destination PLMN–.

The destination network shall be able to determine the authenticity of the source network that sent the specific message elements protected according to the preceding bullet. For this requirement to be fulfilled, it shall suffice that a SEPP in the destination network that is dedicated to handling e2e Core Network Interconnection Security can determine the authenticity of the source network.

The solution should have minimal impact and additions to 3GPP-defined network elements.

The solution should be using standard security protocols.

The solution shall cover interfaces used for roaming purposes.

The solution should take into account considerations on performance and overhead.

The solution shall cover prevention of replay attacks.

The solution shall cover algorithm negotiation and prevention of bidding down attacks.

The solution should take into account operational aspects of key management.

5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID or SNPN ID in the received N32 message.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications. The SEPP shall support multiple trust anchors.

NOTE 1: Such a differentiation and support of multiple trust anchors could be done e.g. by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The sending SEPP shall reject messages received from the NF (directly or via SCP) with JSON including "encBlockIndex" (regardless of the encoding used for that JSON request).

The receiving SEPP shall reject any message in which an IPX has inserted or relocated references to encBlockIndex.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP's own PLMN (or SNPN), the message is discarded.

The SEPP shall be able to use one or more PLMN IDs (or SNPN IDs). In the situation that a PLMN (or SNPN) is using more than one PLMN ID (or SNPN ID), this PLMN's SEPP (or SNPN's SEPP) may use the same N32-connection for all of the networks PLMN IDs (or SNPN IDs), with each of the PLMN's (or SNPN's) remote partners. If different PLMNs (or SNPNs) are represented by the PLMN IDs (or SNPN IDs) supported by a SEPP, the SEPP shall use separate N32-connections for each pair of home and visited PLMN (or SNPN).

Sending SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header specified in TS 29.500 [74]:

- If the sending NF or the SCP has inserted the 3gpp-Sbi-Originating-Network-Id header in the signaling message (service/subscription request or notification message), the sending SEPP shall compare the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header in the received signaling message with the PLMN ID(s) or SNPN ID(s) that the sending SEPP represents by its certificate.
  - If the PLMN ID or SNPN ID does not match with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall discard the received signaling message.
  - If the PLMN ID or SNPN ID matches with any of the PLMN IDs that the sending SEPP represents, the sending SEPP shall forward the signaling message to the receiving SEPP.
- If the sending NF and the SCP have not included the 3gpp-Sbi-Originating-Network-Id header in the signalling message, the sending SEPP shall include the 3gpp-Sbi-Originating-Network-Id header and send the updated signaling message to the receiving SEPP.
  - If the sending SEPP only represents one PLMN ID or SNPN ID, the sending SEPP shall insert the 3gpp-Sbi-Originating-Network-Id header with this ID.
  - If the sending SEPP represents multiple PLMN IDs or SNPN IDs, it is up to configuration and deployment to determine which PLMN ID or SNPN ID value should be included in the header.

Receiving SEPP behavior for the 3gpp-Sbi-Originating-Network-Id header:

- The receiving SEPP shall check whether the 3gpp-Sbi-Originating-Network-Id header included in the signalling message belongs to the sending SEPP's own PLMN or SNPN. It does this by verifying that the asserted PLMN ID in the 3gpp-Sbi-Originating-Network-Id header matches one of the sending SEPP's own PLMN ID(s) or SNPN ID(s) either in the N32-f context, the sending SEPP's certificate, or a locally configured list of PLMN IDs or SNPN IDs that the sending SEPP represents.
  - If the 3gpp-Sbi-Originating-Network-Id header does not match with any of the PLMN IDs or SNPN IDs belonging to the peer sending SEPP, the receving SEPP shall discard the received signaling message.

- If the 3gpp-Sbi-Originating-Network-Id header matches with any of the PLMN IDs or SNPN IDs belonging to the peer sending SEPP, the header is successfully verified, and the receiving SEPP shall forward the received signaling message to the target NF.

5.9.3.3 Protection of attributes

Integrity protection shall be applied to all attributes transferred over the N32-f interface.

Confidentiality protection shall be applied to all attributes specified in SEPP's Data-type Encryption Policy (clause 13.2.3.2). The following attributes shall be confidentiality protected when being sent over the N32-f interface, irrespective of the Data-type Encryption Policy:

- Authentication Vectors.
- Cryptographic material.
- Location data, e.g. Cell ID and Physical Cell ID.
- Content of SMS in case of SMS over SBI over N32.

The following attributes should additionally be confidentiality protected when being sent over the N32-f interface:

- SUPI.

5.9.3.4 Requirements for IPUPS functionality

The IPUPS shall only forward GTP-U packets that contain an F-TEID that belongs to an active PDU session and discard all others.

The IPUPS shall discard malformed GTP-U messages.

5.9.3.5 Requirements for Network Functions (NF)

The NF that sends a signalling message (service/subscription request or notification message) shall include its PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header.

If an NF supports multiple PLMN IDs or SNPN IDs, the sending NF shall include the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header on behalf of which the message is sent.

The handling of the PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header at the receiving NF is up to configuration and deployment.

NOTE: A misconfigured PLMN ID or SNPN ID in the 3gpp-Sbi-Originating-Network-Id header can lead to service interruption.

5.10 Visibility and configurability

5.10.1 Security visibility

Although in general the security features should be transparent to the user or application, for certain events and according to the user's or application's concern, greater visibility of the operation of following security feature shall be provided:

- AS confidentiality: (AS confidentiality, Confidentiality algorithm, bearer information)
- AS integrity: (AS integrity, Integrity algorithm, bearer information)
- NAS confidentiality: (NAS confidentiality, Confidentiality algorithm)
- NAS integrity: (NAS integrity, Integrity algorithm)

The UE shall provide above security information to the applications in the UE (e.g. via APIs), on a per PDU session granularity.

The serving network identifier shall be available for applications in the UE.

5.10.2 Security configurability

Security configurability lets a user to configure certain security feature settings on a UE that allows the user to manage additional capability or use certain advanced security features.

The following configurability feature should be provided:

- Granting or denying access to USIM without authentication as described in TS 33.401 [10].

5.11 Requirements for algorithms, and algorithm selection

5.11.1 Algorithm identifier values

5.11.1.1 Ciphering algorithm identifier values

All identifiers and names specified in this sub-clause are for 5G NAS and New Radio. In relation to AS capabilities, the identifiers and names for E-UTRAN connected to 5GC are specified in TS 33.401 [10].

Each encryption algorithm will be assigned a 4-bit identifier. The following values for ciphering algorithms are defined:

"0000_2"	NEA0	Null ciphering algorithm;
"0001_2"	128-NEA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NEA2	128-bit AES based algorithm; and
"0011_2"	128-NEA3	128-bit ZUC based algorithm.

128-NEA1 is based on SNOW 3G (see TS 35.215 [14]).

128-NEA2 is based on 128-bit AES [15] in CTR mode [16].

128-NEA3 is based on 128-bit ZUC (see TS 35.221 [18]).

Full details of the algorithms are specified in Annex D.

5.11.1.2 Integrity algorithm identifier values

All identifiers and names specified in the present sub-clause are for 5G NAS and New Radio. In relation to AS capabilities, the identifiers and names for E-UTRAN connected to 5GC are specified in TS 33.401 [10].

Each integrity algorithm used for 5G will be assigned a 4-bit identifier. The following values for integrity algorithms are defined:

"0000_2"	NIA0	Null Integrity Protection algorithm;
"0001_2"	128-NIA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NIA2	128-bit AES based algorithm; and
"0011_2"	128-NIA3	128-bit ZUC based algorithm.

128-NIA1 is based on SNOW 3G (see TS 35.215 [14]).

128-NIA2 is based on 128-bit AES [15] in CMAC mode [17].

128-NIA3 is based on 128-bit ZUC (see TS 35.221 [18]).

Full details of the algorithms are specified in Annex D.

5.11.2 Requirements for algorithm selection

a) UE in RRC_Connected and a serving network shall have agreed upon algorithms for

- Ciphering and integrity protection of RRC signalling and user plane (to be used between UE and gNB)
- Ciphering and integrity protection of RRC signalling and user plane (to be used between UE and ng-eNB)
- NAS ciphering and NAS integrity protection (to be used between UE and AMF)

b) The serving network shall select the algorithms to use dependent on

- the UE security capabilities of the UE,
- the configured allowed list of security capabilities of the currently serving network entity

c) The UE security capabilities shall include NR NAS algorithms for NAS level, NR AS algorithms for AS layer and LTE algorithms for AS level if the UE supports E-UTRAN connected to 5GC.

NOTE: If the UE supports both E-UTRAN and NR connected to 5GC, the UE 5G security capabilities include both the LTE and NR algorithms.

d) Each selected algorithm shall be indicated to a UE in a protected manner such that a UE is ensured that the integrity of algorithm selection is protected against manipulation.

e) The UE security capabilities shall be protected against "bidding down attacks".

f) It shall be possible that the selected AS and NAS algorithms are different at a given point of time.

5.12 Requirements on 5G-RG

The 5G-RG shall be equipped with UICC where the subscription credentials resides. If provisioned by the home operator, the 5G-RG shall store the Home Network Public Key required for concealing the SUPI in the UICC.

The 5G-RG shall support all the security requirements and features of the UE defined in clause 5.2.

5.13 Requirements on NSSAAF

The Network slice specific and SNPN authentication and authorization function (NSSAAF) shall handle the Network Slice Specific Authentication requests from the serving AMF as specified in clause 16.The NSSAAF shall also support functionality for access to SNPN using credentials from Credentials Holder using AAA Server as specified in clause I.2.2.2.

The NSSAAF is responsible to send the NSSAA requests to the appropriate AAA-S.

The NSSAAF shall support AAA-S triggered Network Slice-Specific Re-authentication and Re-authorization and Slice-Specific Authorization Revocation and translate any AAA protocol into a Service Based format.

NSSAAF shall translate the Service based messages from the serving AMF or AUSF to AAA protocols towards AAA-P/AAA-S.

6 Security procedures between UE and 5G network functions

6.0 General

When the UE is capable of connecting to 5GC and EPC and connected to an ng-eNB which is connected to both EPC and 5GC, the UE has the ability to select which core network to connect to as described in clause 4.8.4 in

TS24.501[35]. If the UE selects the EPC, the UE shall use security procedure as in TS33.401[10]. Otherwise, if the UE selects 5GC, the UE shall use the security procedures as per this document.

For an ng-eNB which can connect to EPC and 5GC, the ng-eNB shall choose the corresponding security procedures based on the UE selected type of core netowrk, i.e., when EPC is selected, the ng-eNB shall use security procedures as described in TS33.401[10]. On the other hand, when 5GC is selected, the ng-eNB shall use security procedures as described in this document.

6.1 Primary authentication and key agreement

6.1.1 Authentication framework

6.1.1.1 General

The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the K_{SEAF} provided by the AUSF of the home network to the SEAF of the serving network.

Keys for more than one security context can be derived from the K_{SEAF} without the need of a new authentication run. A concrete example of this is that an authentication run over a 3GPP access network can also provide keys to establish security between the UE and a N3IWF used in untrusted non-3GPP access.

The anchor key K_{SEAF} is derived from an intermediate key called the K_{AUSF}. The K_{AUSF} is established between the UE and HN resulting from the primary authentication procedure. The K_{AUSF} may be securely stored in the AUSF based on the home operator's policy on using such key e.g. if the control plane solution for Steering of Roaming (see clause 6.14) or UE Parameter Update procedures (see clause 6.15) or AKMA are supported by the HPLMN.

NOTE A: For standalone non-public networks when an authentication method other than 5G AKA or EAP-AKA' is used, Annex I.2 applies.

NOTE 1: This feature is an optimization that might be useful, for example, when a UE registers to different serving networks for 3GPP-defined access and untrusted non-3GPP access (this is possible according to TS 23.501 [2]). The details of this feature are operator-specific and not in scope of this document.

NOTE 2: A subsequent authentication based on the K_{AUSF} stored in the AUSF gives somewhat weaker guarantees than an authentication directly involving the ARPF and the USIM. It is rather comparable to fast re-authentication in EAP-AKA'.

NOTE 2a: Void.

UE and serving network shall support EAP-AKA' and 5G AKA authentication methods.

NOTE 2b: It is the home operator's decision which authentication method is selected.

The USIM shall reside on a UICC. The UICC may be removable or non-removable.

NOTE 3: For non-3GPP access networks USIM applies in case of terminal with 3GPP access capabilities.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA' and 5G AKA for non-3GPP access networks shall reside on the UICC.

NOTE 4: EAP-AKA' and 5G AKA are the only authentication methods that are supported in UE and serving network, hence only they are described in sub-clause 6.1.3 of the present document. For a private network using the 5G system as specified in [7] an example of how additional authentication methods can be used with the EAP framework is given in the informative Annex B.

NOTE 5: For non-public network (NPN) security the Annex I of the present document provides details.

Upon successful completion of the 5G AKA primary authentication, the AMF shall initiate NAS security mode command procedure (see clause 6.7.2) with the UE.

NOTE 6: The reason to mandatory run the NAS SMC procedure after primary authentication is because the UE does not store the new derived K_{AUSF} until receiving the NAS SMC message. The new partial native NAS security context is taken into use. It is specified in clause 6.9.4.4 whether AS key re-keying is performed.

6.1.1.2 EAP framework

The EAP framework is specified in RFC 3748 [27]. It defines the following roles: peer, pass-through authenticator and back-end authentication server. The back-end authentication server acts as the EAP server, which terminates the EAP authentication method with the peer. In the 5G system, the EAP framework is supported in the following way:

- The UE takes the role of the peer.
- The SEAF takes the role of pass-through authenticator.
- The AUSF takes the role of the backend authentication server.

6.1.1.3 Granularity of anchor key binding to serving network

The primary authentication and key agreement procedures shall bind the K_{SEAF} to the serving network. The binding to the serving network prevents one serving network from claiming to be a different serving network, and thus provides implicit serving network authentication to the UE.

This implicit serving network authentication shall be provided to the UE irrespective of the access network technology, so it applies to both 3GPP and non-3GPP access networks.

Furthermore, the anchor key provided to the serving network shall also be specific to the authentication having taken place between the UE and a 5G core network, i.e. the K_{SEAF} shall be cryptographically separate from the key K_{ASME} delivered from the home network to the serving network in earlier mobile network generations.

The anchor key binding shall be achieved by including a parameter called "serving network name" into the chain of key derivations that leads from the long-term subscriber key to the anchor key.

The value of serving network name is defined in sub-clause 6.1.1.4 of the present document.

The chain of key derivations that leads from the long-term subscriber key to the anchor key is specified in sub-clause 6.1.3 of the present document for each (class) of authentication methods. The key derivation rules are specified in Annex A.

NOTE: No parameter like 'access network type' is used for anchor key binding as 5G core procedures are supposed to be access network agnostic.

6.1.1.4 Construction of the serving network name

6.1.1.4.1 Serving network name

The serving network name is used in the derivation of the anchor key. It serves a dual purpose, namely:

- It binds the anchor key to the serving network by including the serving network identifier (SN Id).
- It makes sure that the anchor key is specific for authentication between a 5G core network and a UE by including a service code set to "5G".

In 5G AKA, the serving network name has a similar purpose of binding the RES* and XRES* to the serving network.

The serving network name is the concatenation of a service code and the SN Id with a separation character ":" such that the service code prepends the SN Id.

NOTE: No parameter like 'access network type' is used for serving network name as it relates to a 5G core procedure that is access network agnostic.

The SN Id identifies the serving PLMN and, except for standalone non-public networks, is defined as SNN-network-identifier in TS 24.501[35].

NOTE 1: For standalone non-public networks, the definition of SN Id is given in Annex I.3.

6.1.1.4.2 Construction of the serving network name by the UE

The UE shall construct the serving network name as follows:

- It shall set the service code to "5G".
- It shall set the network identifier to the SN Id of the network that it is authenticating to.
- Concatenate the service code and the SN Id with the separation character ":".

6.1.1.4.3 Construction of the serving network name by the SEAF

The SEAF shall construct the serving network name as follows:

- It shall set the service code to "5G".
- It shall set the network identifier to the SN Id of the serving network to which the authentication data is sent by the AUSF.
- It shall concatenate the service code and the SN Id with the separation character ":".

NOTE: AUSF gets the serving network name from the SEAF. Before using the serving network name, AUSF checks that the SEAF is authorized to use it, as specified in clause 6.1.2.

6.1.2 Initiation of authentication and selection of authentication method

The initiation of the primary authentication is shown in Figure 6.1.2-1.

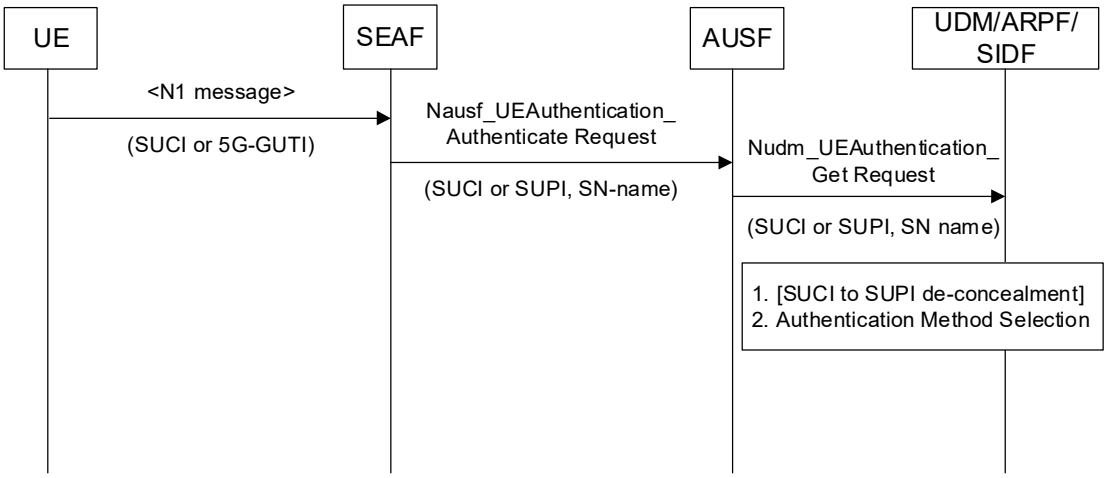


Figure 6.1.2-1: Initiation of authentication procedure and selection of authentication method

The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf_UEAuthentication service by sending a Nausf_UEAuthentication_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

The Nausf_UEAuthentication_Authenticate Request message shall contain either:

- SUCI, as defined in the current specification, or
- SUPI, as defined in TS 23.501 [2].

The SEAF shall include the SUPI in the Nausf_UEAuthentication_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf_UEAuthentication_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf_UEAuthentication_Authenticate Request shall furthermore contain:

- the serving network name, as defined in sub-clause 6.1.1.4 of the present document.

NOTE 1: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs.

The Nausf_UEAuthentication_Authenticate Request may furthermore contain:

- Disaster Roaming service indication, as specified in TS 23.502[8] clause 4.2.2.2.

Upon receiving the Nausf_UEAuthentication_Authenticate Request message, the AUSF shall check that the requesting SEAF in the serving network identified by the 3gpp-Sbi-Originating-Network-Id header specified in TS 29.500 [74] is entitled to use the serving network name in the Nausf_UEAuthentication_Authenticate Request. For the case that the 3gpp-Sbi-Originating-Network-Id header is not included, the AUSF may authorize the serving network based on its name available in the Nausf_UEAuthentication_Authenticate Request message.

NOTE 1a: As described in clause 5.9.3.2, the SEPP in the AUSF's network verifies the correctness of the 3gpp-Sbi-Originating-Network-Id header and the SEPP in the SEAF's network ensures that the 3gpp-Sbi-Originating-Network-Id is included.

The AUSF shall store the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF shall respond with "serving network not authorized" in the Nausf_UEAuthentication_Authenticate Response.

NOTE 2: The AUSF and the UDM may be configured with Disaster Condition via OAM based on operator policy and the request by the government agencies.

For the Disaster Roaming, the AUSF shall check the local configuration and, if allowed, the AUSF sends Nudm_UEAuthentication_Get Request to the UDM.

The Nudm_UEAuthentication_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;
- the serving network name;
- if received from SEAF, Disaster Roaming service indication;

Upon reception of the Nudm_UEAuthentication_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

Based on SUPI, the UDM/ARPF shall choose the authentication method.

NOTE 3: The Nudm_UEAuthentication_Get Response in reply to the Nudm_UEAuthentication_Get Request and the Nausf_UEAuthentication_Authenticate Response message in reply to the Nausf_UEAuthentication_Authenticate Request message are described as part of the authentication procedures in clause 6.1.3.

For the Disaster Roaming, the UDM shall check the local configuration and, if allowed, the UDM proceeds with the chosen authentication method.

6.1.3 Authentication procedures

6.1.3.1 Authentication procedure for EAP-AKA'

EAP-AKA' is specified in RFC 5448 [12]. The 3GPP 5G profile for EAP-AKA' is specified in the normative Annex F.

The selection of using EAP-AKA' is described in sub-clause 6.1.2 of the present document.

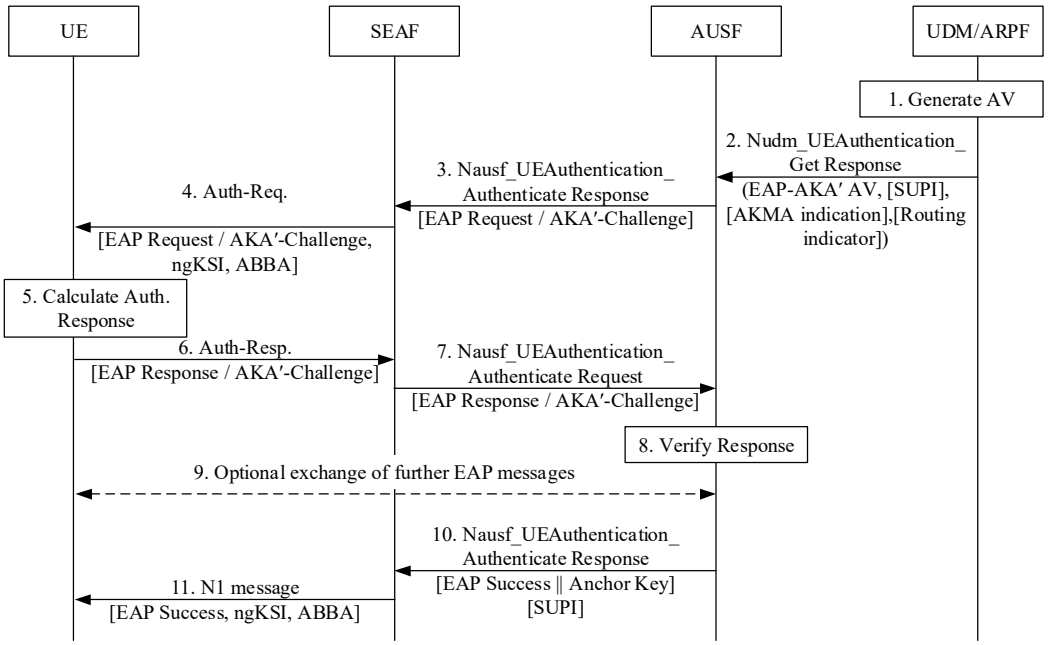


Figure 6.1.3.1-1: Authentication procedure for EAP-AKA'

The authentication procedure for EAP-AKA' works as follows, cf. also Figure 6.1.3.1-1:

1. The UDM/ARPF shall first generate an authentication vector with Authentication Management Field (AMF) separation bit = 1 as defined in TS 33.102 [9]. The UDM/ARPF shall then compute CK' and IK' as per the normative Annex A and replace CK and IK by CK' and IK'.

2. The UDM shall subsequently send this transformed authentication vector AV' (RAND, AUTN, XRES, CK', IK') to the AUSF from which it received the Nudm_UEAuthentication_Get Request together with an indication that the AV' is to be used for EAP-AKA' using a Nudm_UEAuthentication_Get Response message.

NOTE: The exchange of a Nudm_UEAuthentication_Get Request message and an Nudm_UEAuthentication_Get Response message between the AUSF and the UDM/ARPF described in the preceding paragraph is the same as for trusted access using EAP-AKA' described in TS 33.402 [11], sub-clause 6.2, step 10, except for the input parameter to the key derivation, which is the value of <network name>. The "network name" is a concept from RFC 5448 [12]; it is carried in the AT_KDF_INPUT attribute in EAP-AKA'. The value of <network name> parameter is not defined in RFC 5448 [12], but rather in 3GPP specifications. For EPS, it is defined as "access network identity" in TS 24.302 [71], and for 5G, it is defined as "serving network name" in sub-clause 6.1.1.4 of the present document.

In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM will include the SUPI in the Nudm_UEAuthentication_Get Response.

If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication and Routing indicator in the Nudm_UEAuthentication_Get Response.

3. The AUSF shall send the EAP-Request/AKA'-Challenge message to the SEAF in a Nausf_UEAuthentication_Authenticate Response message.

4. The SEAF shall transparently forward the EAP-Request/AKA'-Challenge message to the UE in a NAS message Authentication Request message. The ME shall forward the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM. This message shall include the ngKSI and ABBA parameter. In fact, SEAF shall include the ngKSI and ABBA parameter in all EAP-Authentication request message. The ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. During an EAP authentication, the value of the ngKSI and the ABBA parameter sent by the SEAF to the UE shall not be changed.

NOTE 1: The SEAF needs to understand that the authentication method used is an EAP method by evaluating the type of authentication method based on the Nausf_UEAuthentication_Authenticate Response message.

5. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME shall derive CK' and IK' according to Annex A.3.

   If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3. 3.

6. The UE shall send the EAP-Response/AKA'-Challenge message to the SEAF in a NAS message Auth-Resp message.

7. The SEAF shall transparently forward the EAP-Response/AKA'-Challenge message to the AUSF in Nausf_UEAuthentication_Authenticate Request message.

8. The AUSF shall verify the message by comparing the XRES and RES, and if the AUSF has successfully verified this message it shall continue as follows, otherwise it shall return an error to the SEAF. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for details on linking authentication confirmation).

9. The AUSF and the UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the SEAF. The SEAF shall transparently forward these messages.

NOTE 2: EAP Notifications as described in RFC 3748 [27] and EAP-AKA Notifications as described in RFC 4187 [21] can be used at any time in the EAP-AKA exchange. These notifications can be used e.g. for protected result indications or when the EAP server detects an error in the received EAP-AKA response.

10. The AUSF derives EMSK from CK' and IK' as described in RFC 5448[12] and Annex F. The AUSF uses the most significant 256 bits of EMSK as the K_{AUSF} and then calculates K_{SEAF} from K_{AUSF} as described in clause A.6. The AUSF shall send an EAP Success message to the SEAF inside Nausf_UEAuthentication_Authenticate Response, which shall forward it transparently to the UE. Nausf_UEAuthentication_Authenticate Response message contains the K_{SEAF}. If the AUSF received a SUCI from the SEAF when the authentication was initiated (see sub-clause 6.1.2 of the present document), then the AUSF shall also include the SUPI in the Nausf_UEAuthentication_Authenticate Response message. The AUSF stores the K_{AUSF} based on the home network operator's policy according to clause 6.1.1.1.

NOTE 3: For lawful interception, the AUSF sending SUPI to SEAF is necessary but not sufficient. By including the SUPI as input parameter to the key derivation of K_{AMF} from K_{SEAF}, additional assurance on the correctness of SUPI is achieved by the serving network from both, home network and UE side.

11. The SEAF shall send the EAP Success message to the UE in the N1 message. This message shall also include the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

NOTE 4: Step 11 could be NAS Security Mode Command or Authentication Result.

NOTE 5: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

The key received in the Nausf_UEAuthentication_Authenticate Response message shall become the anchor key, K_{SEAF} in the sense of the key hierarchy in sub-clause 6.2 of the present document. The SEAF shall then derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7 and send it to the AMF. On receiving the EAP-Success message, the UE derives EMSK from CK' and IK' as described in RFC 5448 and Annex F. The ME uses the most significant 256 bits of the EMSK as the K_{AUSF} and then calculates K_{SEAF} in the same way as the AUSF. The UE shall derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 6: As an implementation option, the UE creates the temporary security context as described in step 11 after receiving the EAP message that allows EMSK to be calculated. The UE turns this temporary security context into a partial security context when it receives the EAP Success. The UE removes the temporary security context if the EAP authentication fails.

The further steps taken by the AUSF upon receiving a successfully verified EAP-Response/AKA'-Challenge message are described in sub-clause 6.1.4 of the present document.

If the EAP-Response/AKA'-Challenge message is not successfully verified, the subsequent AUSF behaviour is determined according to the home network's policy.

If AUSF and SEAF determine that the authentication was successful, then the SEAF provides the ngKSI and the K_{AMF} to the AMF.

6.1.3.2 Authentication procedure for 5G AKA

6.1.3.2.0 5G AKA

5G AKA enhances EPS AKA [10] by providing the home network with proof of successful authentication of the UE from the visited network. The proof is sent by the visited network in an Authentication Confirmation message.

The selection of using 5G AKA is described in sub-clause 6.1.2 of the present document.

NOTE 1: 5G AKA does not support requesting multiple 5G AVs, neither the SEAF pre-fetching 5G AVs from the home network for future use.

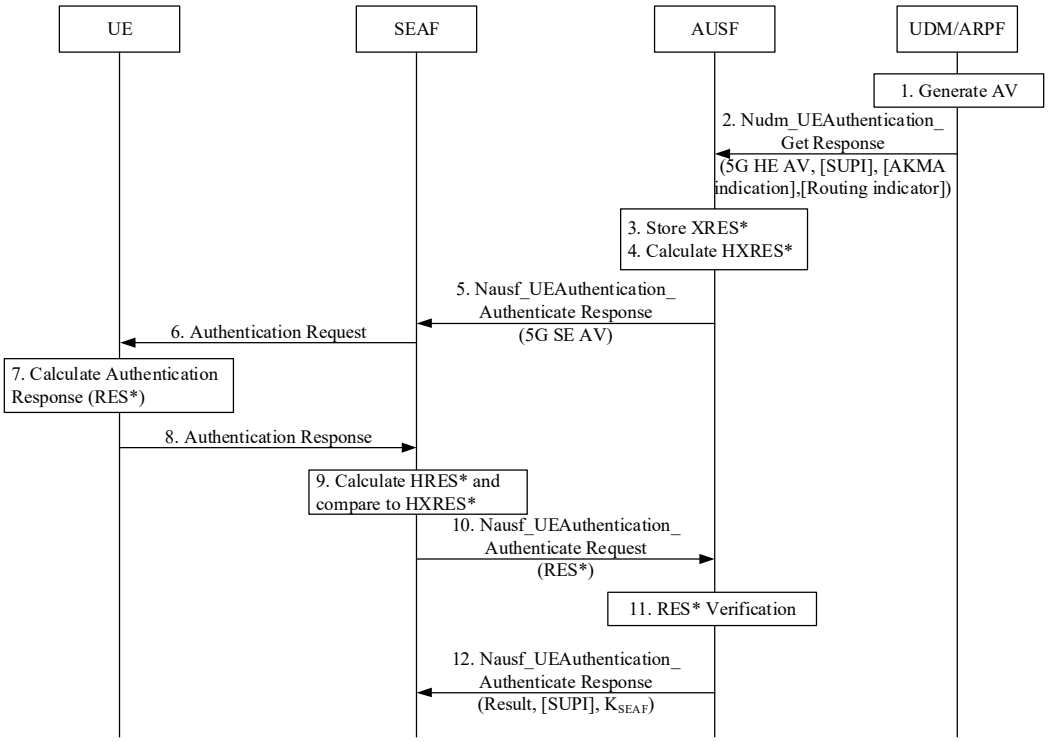


Figure 6.1.3.2-1: Authentication procedure for 5G AKA

The authentication procedure for 5G AKA works as follows, cf. also Figure 6.1.3.2-1:

1. For each Nudm_UEAuthentication_Get Request, the UDM/ARPF shall create a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [9]. The UDM/ARPF shall then derive K_{AUSF} (as per Annex A.2) and calculate XRES* (as per Annex A.4). Finally, the UDM/ARPF shall create a 5G HE AV from RAND, AUTN, XRES*, and K_{AUSF}.

2. The UDM shall then return the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G AKA in a Nudm_UEAuthentication_Get Response. In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM will include the SUPI in the Nudm_UEAuthentication_Get Response after deconcealment of SUCI by SIDF.

   If a subscriber has an AKMA subscription, the UDM shall include the AKMA indication and Routing indicator in the Nudm_UEAuthentication_Get Response.

3. The AUSF shall store the XRES* temporarily together with the received SUCI or SUPI.

4. The AUSF shall then generate the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES* from XRES* (according to Annex A.5) and K_{SEAF} from K_{AUSF} (according to Annex A.6), and replacing the XRES* with the HXRES* and K_{AUSF} with K_{SEAF} in the 5G HE AV.

5. The AUSF shall then remove the K_{SEAF} and return the 5G SE AV (RAND, AUTN, HXRES*) to the SEAF in a Nausf_UEAuthentication_Authenticate Response.

6. The SEAF shall send RAND, AUTN to the UE in a NAS message Authentication Request. This message shall also include the ngKSI that will be used by the UE and AMF to identify the K_{AMF} and the partial native security context that is created if the authentication is successful. This message shall also include the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. The ME shall forward the RAND and AUTN received in NAS message Authentication Request to the USIM.

NOTE 2: The ABBA parameter is included to enable the bidding down protection of security features.

7. At receipt of the RAND and AUTN, the USIM shall verify the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102[9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [9], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME then shall compute RES* from RES according to Annex A.4. The ME shall calculate K_{AUSF} from CK||IK according to clause A.2. The ME shall calculate K_{SEAF} from K_{AUSF} according to clause A.6. An ME accessing 5G shall check during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.

NOTE 3: This separation bit in the AMF field of AUTN cannot be used anymore for operator specific purposes as described by TS 33.102 [9], Annex F.

8. The UE shall return RES* to the SEAF in a NAS message Authentication Response.

9. The SEAF shall then compute HRES* from RES* according to Annex A.5, and the SEAF shall compare HRES* and HXRES*. If they coincide, the SEAF shall consider the authentication successful from the serving network point of view. If not, the SEAF proceed as described in sub-clause 6.1.3.2.2. If the UE is not reached, and the RES* is never received by the SEAF, the SEAF shall consider authentication as failed, and indicate a failure to the AUSF.

10. The SEAF shall send RES*, as received from the UE, in a Nausf_UEAuthentication_Authenticate Request message to the AUSF.

11. When the AUSF receives as authentication confirmation the Nausf_UEAuthentication_Authenticate Request message including a RES* it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF stores the K_{AUSF} based on the home network operator's policy according to clause 6.1.1.1. AUSF shall compare the received RES* with the stored XRES*. If the RES* and XRES* are equal, the AUSF shall consider the authentication as successful from the home network point of view. AUSF shall inform UDM about the authentication result (see sub-clause 6.1.4 of the present document for linking with the authentication confirmation).

NOTE 4: It is left to implementation to temporarily store the K_{AUSF} received in step 2 in AUSF until the RES* verification is done successfully (i.e., at step 11).

12. The AUSF shall indicate to the SEAF in the Nausf_UEAuthentication_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the K_{SEAF} shall be sent to the SEAF in the Nausf_UEAuthentication_Authenticate Response. In case the AUSF received a SUCI from the SEAF in the authentication request (see sub-clause 6.1.2 of the present document), and if the authentication was successful, then the AUSF shall also include the SUPI in the Nausf_UEAuthentication_Authenticate Response message.

If the authentication was successful, the key K_{SEAF} received in the Nausf_UEAuthentication_Authenticate Response message shall become the anchor key in the sense of the key hierarchy as specified in sub-clause 6.2 of the present document. Then the SEAF shall derive the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7. The SEAF shall provide the ngKSI and the K_{AMF} to the AMF. If the AUSF indicates that the authentication

was successful from the home network point of view, then the AMF shall initiate NAS security mode command procedure (see clause 6.7.2) with the UE, to take the newly generated partial native 5G NAS security context into use. Upon receiving the valid NAS Security Mode Command message from the AMF, the UE shall consider the performed primary authentication as successful.

If a SUCI was used for this authentication, then the SEAF shall only provide ngKSI and K_{AMF} to the AMF after it has received the Nausf_UEAuthentication_Authenticate Response message containing K_{SEAF} and SUPI; no communication services will be provided to the UE until the SUPI is known to the serving network.

The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.

6.1.3.2.1 Void

6.1.3.2.2 RES* verification failure in SEAF or AUSF or both

This clause describes how RES* verification failure in the SEAF or in the AUSF shall be handled.

In step 9 in Figure 6.1.3.2-1, the SEAF shall compute HRES* from RES* according to Annex A.5, and the SEAF shall compare HRES* and HXRES*. If they don't coincide, then the SEAF shall consider the authentication as unsuccessful.

The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf_UEAuthentication_Authenticate Response message from the AUSF in step 12in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf_UEAuthentication_Authenticate Response message to the SEAF that the verification of the RES* was not successful in the AUSF, or
- if the verification of the RES* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf_UEAuthentication_Authenticate Response message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE.

6.1.3.3 Synchronization failure or MAC failure

6.1.3.3.1 Synchronization failure or MAC failure in USIM

This clause describes synchronisation failure or MAC failure in USIM.

In step 7 in Figure 6.1.3.2-1 when 5G AKA is used; or in step 5 in Figure 6.1.3.1-1 when EAP-AKA' is used, at the receipt of the RAND and AUTN, if the verification of the AUTN fails, then the USIM indicates to the ME the reason for failure and in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [9]) to the ME.

If 5G AKA is used: The ME shall respond with NAS message Authentication Failure with a CAUSE value indicating the reason for failure. In case of a synchronisation failure of AUTN (as described in TS 33.102 [9]), the UE also includes AUTS that was provided by the USIM. Upon receipt of an authentication failure message, the AMF/SEAF may initiate new authentication towards the UE. (see TS 24.501 [35]).

If EAP-AKA' is used: The ME shall proceed as described in RFC 4187 [21] and RFC 5448 [12] for EAP-AKA'.

6.1.3.3.2 Synchronization failure recovery in Home Network

Upon receiving an authentication failure message *with synchronisation failure* (AUTS) from the UE, the SEAF sends an Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" to the AUSF and

the AUSF sends an Nudm_UEAuthentication_Get Request message to the UDM/ARPF, together with the following parameters:

- *RAND* sent to the UE in the preceding Authentication Request, and
- *AUTS* received by the SEAF in the response from the UE to that request, as described in subclause 6.1.3.2.0 and 6.1.3.3.1.

An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE.

The SEAF does not send new authentication requests to the UE before having received the response to its Nausf_UEAuthentication_Authenticate Request message with a "*synchronisation failure indication*" from the AUSF (or before it is timed out).

When the UDM/ARPF receives an Nudm_UEAuthentication_Get Request message with a "*synchronisation failure indication*" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC. The UDM/ARPF sends an Nudm_UEAuthentication_Get Response message with a new authentication vector for either EAP-AKA' or 5G-AKA depending on the authentication method applicable for the user to the AUSF. The AUSF runs a new authentication procedure with the UE according to clauses 6.1.3.1 or 6.1.3.2 depending on the authentication method applicable for the user.

6.1.4 Linking increased home control to subsequent procedures

6.1.4.1 Introduction

The 5G authentication and key agreement protocols provide increased home control. Compared to EPS AKA in EPS, this provides better security useful in preventing certain types of fraud as explained in more detail below.

This increased home control comes in the following forms in 5GS:

- In the case of EAP-AKA', the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the EAP-Response/AKA'-Challenge received by the AUSF has been successfully verified, cf. sub-clause 6.1.3.1 of the present document.
- In the case of 5G AKA, the AUSF in the home network obtains confirmation that the UE has been successfully authenticated when the authentication confirmation received by the AUSF in Nausf_UEAuthentication_Authenticate Request message has been successfully verified, cf. sub-clause 6.1.3.2 of the present document.

When 3GPP credentials are used in above cases, the result is reported to the UDM. Details are described in clause 6.1.4.1a.

The feature of increased home control is useful in preventing certain types of fraud, e.g. fraudulent Nudm_UECM_Registration Request for registering the subscriber's serving AMF in UDM that are not actually present in the visited network. But an authentication protocol by itself cannot provide protection against such fraud. The authentication result needs to be linked to subsequent procedures, e.g. the Nudm_UECM_Registration procedure from the AMF in some way to achieve the desired protection.

The actions taken by the home network to link authentication confirmation (or the lack thereof) to subsequent procedures are subject to operator policy and are not standardized.

But informative guidance is given in sub-clause 6.1.4.2 as to what measures an operator could usefully take. Such guidance may help avoiding a proliferation of different solutions.

The feature of increased home control is also used to allow the UDM to keep track of the AUSF that stores the K_{AUSF} to be used during e.g. the control plane solution for Steering of Roaming or UE Parameter Update procedures; i.e. the AUSF that stores the latest K_{AUSF} generated after successful completion of the latest primary authentication reported to the UDM.

After the UDM is informed that the UE has been successfully (re-)authenticated, the UDM shall store the AUSF instance which reported the successful authentication. If the UDM has been previously informed that the UE was authenticated by a different AUSF instance, the UDM may request the old AUSF to clear the stale security parameters (K_{AUSF}, SOR counter and UE parameter update counter). If the UDM determines to delete the security parameters in the old AUSF, then the UDM shall use the Nausf_UEAuthentication_deregister service operation (see clause 14.1.5).

6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF

The information sent from the AUSF to the UDM that a successful or unsuccessful authentication of a subscriber has occurred, shall be used to link authentication confirmation to subsequent procedures. The AUSF shall send the Nudm_UEAuthentication_ResultConfirmation service operation for this purpose as shown in figure6.1.4.1a-1.

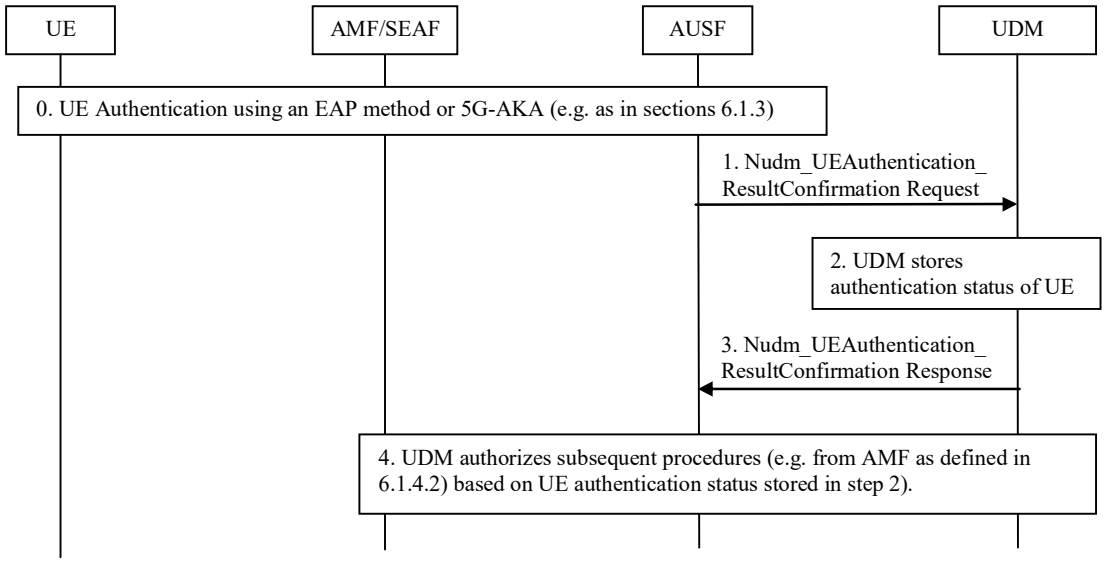


Figure 6.1.4.1a-1: Linking increased Home control to subsequent procedures

1. The AUSF shall inform UDM about the result and time of an authentication procedure with a UE using a Nudm_UEAuthentication_ResultConfirmation Request. This shall include the SUPI, a timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

NOTE: It may be sufficient for the purposes of fraud prevention to send only information about successful authentications, but this is up to operator policy.

2. The UDM shall store the authentication status of the UE (SUPI, authentication result, timestamp, and the serving network name).

3. UDM shall reply to AUSF with a Nudm_UEAuthentication_ResultConfirmation Response.

4. Upon reception of subsequent UE related procedures (e.g. Nudm_UECM_Registration_Request from AMF) UDM may apply actions according to home operator's policy to detect and achieve protection against certain types of fraud (e.g. as proposed in clause 6.1.4.2).

6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF

This sub-clause gives informative guidance on how a home operator could link authentication confirmation (or the lack thereof) to subsequent Nudm_UECM_Registration procedures from AMF to achieve protection against certain types of fraud, as mentioned in the preceding sub-clause.

Approach 1:

The home network records the time of the most recent successfully verified authentication confirmation of the subscriber together with the identity of the 5G visited network that was involved in the authentication. When a new Nudm_UECM_Registration Request arrives from a visited network, the home network checks whether there is a sufficiently recent authentication of the subscriber by this visited network. If not, the Nudm_UECM_Registration Request is rejected. The rejection message may include, according to the home networks policy, an indication that the visited network should send a new Nausf_UEAuthentication_Authenticate Request (cf. sub-clause 6.1.2 of the present document) for fetching a new authentication vector before repeating the Nudm_UECM_Registration Request.

NOTE 1: With this approach, the authentication procedure and the Nudm_UECM_Registration procedure are performed independently. They are coupled only through linking information in the home network.

NOTE 2: It is up to the home network to set the time threshold to define what 'sufficiently recent' is.

Approach 2:

As a variant of the above Approach 1, Approach 2 is based on a more fine-grained policy applied by the home network; the home network could classify roaming partners into different categories, depending on the trust - e.g. derived from previous experience placed in them, for example as follows:

- For a visited network in the first category, the home network would require a successful authentication 'immediately preceding' the Nudm_UECM_Registration Request from an AMF.
- For a visited network in the second category, the home network would only check that an authentication in a network visited by the subscriber was sufficiently recent (taking into account that there may have been a security context transfer between the visited networks).
- For a visited network in the third category, the home network would perform no checks regarding Nudm_UECM_Registration Requests and authentication at all.

Further approaches are possible, depending on the home operator's policy.

6.2 Key hierarchy, key derivation, and distribution scheme

6.2.1 Key hierarchy

Requirements on 5GC and NG-RAN related to keys are described in clause 5.1.3. The following describes the keys of the key hierarchy generation in a 5GS in detail.:

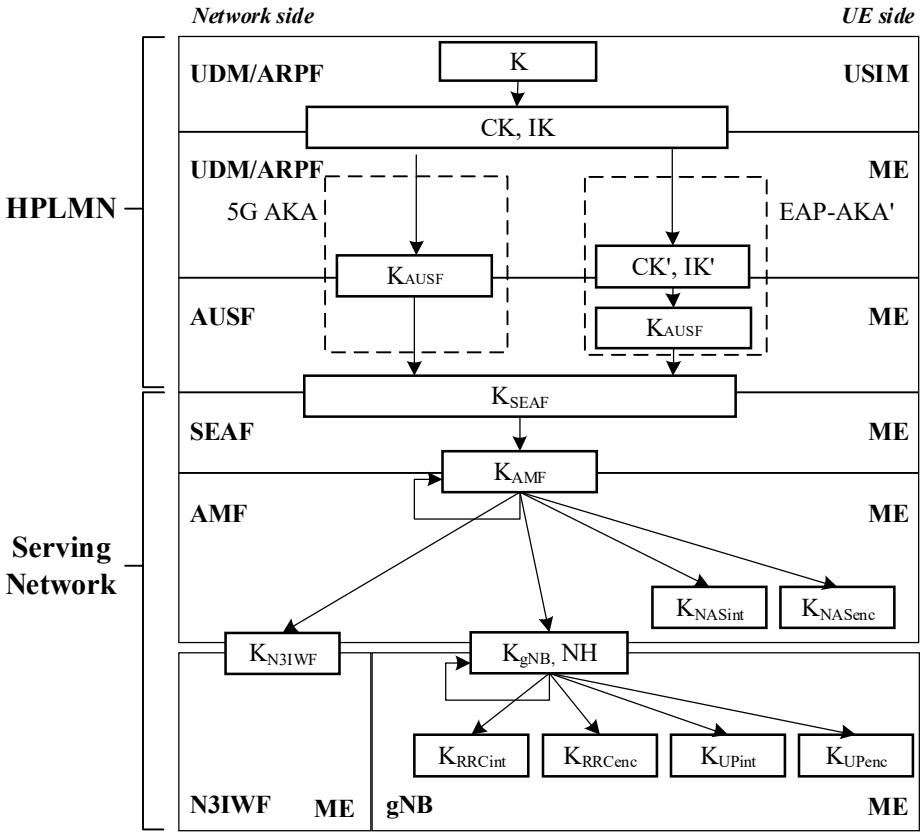


Figure 6.2.1-1: Key hierarchy generation in 5GS

The keys related to authentication (see Figure 6.2.1-1) include the following keys: K, CK/IK. In case of EAP-AKA', the keys CK', IK' are derived from CK, IK as specified in clause 6.1.3.1.

The key hierarchy (see Figure 6.2.1-1) includes the following keys: K_{AUSF}, K_{SEAF}, K_{AMF}, K_{NASint}, K_{NASenc}, K_{N3IWF}, K_{gNB}, K_{RRCint}, K_{RRCenc}, K_{UPint} and K_{UPenc}.

Keys for AUSF in home network:

- K_{AUSF} is a key derived
  - by ME and AUSF from CK', IK' in case of EAP-AKA', CK' and IK' is received by AUSF as a part of transformed AV from ARPF; or,
  - by ME and ARPF from CK, IK in case of 5G AKA, K_{AUSF} is received by AUSF as a part of the 5G HE AV from ARPF.
- K_{SEAF} is an anchor key derived by ME and AUSF from K_{AUSF}. K_{SEAF} is provided by AUSF to the SEAF in the serving network.

Key for AMF in serving network:

- K_{AMF} is a key derived by ME and SEAF from K_{SEAF}. K_{AMF} is further derived by ME and source AMF when performing horizontal key derivation.

Keys for NAS signalling:

- K_{NASint} is a key derived by ME and AMF from K_{AMF}, which shall only be used for the protection of NAS signalling with a particular integrity algorithm.

- K_{NASenc} is a key derived by ME and AMF from K_{AMF}, which shall only be used for the protection of NAS signalling with a particular encryption algorithm.

Key for NG-RAN:

- K_{gNB} is a key derived by ME and AMF from K_{AMF}. K_{gNB} is further derived by ME and source gNB when performing horizontal or vertical key derivation. The K_{gNB} is used as K_{eNB} between ME and ng-eNB.

Keys for UP traffic:

- K_{UPenc} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of UP traffic with a particular encryption algorithm.

- K_{UPint} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of UP traffic between ME and gNB with a particular integrity algorithm.

Keys for RRC signalling:

- K_{RRCint} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of RRC signalling with a particular integrity algorithm.

- K_{RRCenc} is a key derived by ME and gNB from K_{gNB}, which shall only be used for the protection of RRC signalling with a particular encryption algorithm.

Intermediate keys:

- NH is a key derived by ME and AMF to provide forward security as described in Clause A.10.

- $K_{NG\text{-}RAN}$ * is a key derived by ME and NG-RAN (i.e., gNB or ng-eNB) when performing a horizontal or vertical key derivation as specified in Clause 6.9. 2.1.1 using a KDF as specified in Clause A.11/A.12.

- K_{AMF}' is a key that can be derived by ME and AMF when the UE moves from one AMF to another during inter-AMF mobility as specified in Clause 6.9.3 using a KDF as specified in Annex A.13.

Key for the non-3GPP access:

- K_{N3IWF} is a key derived by ME and AMF from K_{AMF} for the non-3GPP access. K_{N3IWF} is not forwarded between N3IWFs.

NOTE 1: The key hierarchy for standalone non-public networks when an authentication method other than 5G AKA or EAP-AKA' is used is given in Annex I.2.3.

6.2.2 Key derivation and distribution scheme

6.2.2.1 Keys in network entities

Keys in the ARPF

The ARPF shall process the long-term key K and any other sensitive data only in its secure environment. The key K shall be 128 bits or 256 bits long.

During an authentication and key agreement procedure, the ARPF shall derive CK' and IK' from K in case EAP-AKA' is used and derive K_{AUSF} from K in case 5G AKA is used. The ARPF shall forward the derived keys to the AUSF.

The ARPF holds the Home Network Private Key that is used by the SIDF to deconceal the SUCI and reconstruct the SUPI. The generation and storage of this key material is out of scope of the present document.

Keys in the AUSF

In case EAP-AKA' is used as authentication method, the AUSF shall derive a key K_{AUSF} from CK' and IK' for EAP-AKA' as specified in clause 6.1.3.1. In case that 5G AKA is used as authentication method, the UDM/ARPF shall generate the KAUSF as specified in clause 6.1.3.2.

The K_{AUSF} may be stored in the AUSF between two subsequent authentication and key agreement procedures.

When the AUSF stores the K_{AUSF}, the AUSF shall store the latest K_{AUSF} generated after successful completion of the latest primary authentication. The authentication is considered as successful and the AUSF shall store the latest K_{AUSF} or replace the old K_{AUSF} with the new K_{AUSF} (if the AMF(s) end up selecting the same AUSF instance for (re)authentication of the UE):

- in case 5G AKA is used as authentication method, when the RES* and the XRES* are equal (see clause 6.1.3.2.0, Step 11).

- in case EAP-AKA' is used as authentication method, when the AUSF sends an EAP-Success message to the SEAF (see clause 6.1.3.1, Step 10).

The AUSF shall generate the anchor key, also called K_{SEAF}, from the authentication key material received from the ARPF during an authentication and key agreement procedure.

Keys in the SEAF

The SEAF receives the anchor key, K_{SEAF}, from the AUSF upon a successful primary authentication procedure in each serving network.

The SEAF shall never transfer K_{SEAF} to an entity outside the SEAF. Once K_{AMF} is derived K_{SEAF} shall be deleted.

The SEAF shall generate K_{AMF} from K_{SEAF} immediately following the authentication and key agreement procedure and hands it to the AMF.

NOTE 1: This implies that a new K_{AMF}, along with a new K_{SEAF}, is generated for each run of the authentication and key agreement procedure.

NOTE 2: The SEAF is co-located with the AMF.

Keys in the AMF

The AMF receives K_{AMF} from the SEAF or from another AMF.

The AMF shall, based on policy, derive a key K_{AMF}' from K_{AMF} for transfer to another AMF in inter-AMF mobility. The receiving AMF shall use K'_{AMF} as its key K_{AMF}.

NOTE 3: The precise rules for key handling in inter-AMF mobility can be found in clause 6.9.3.

The AMF shall generate keys K_{NASint} and K_{NASenc} dedicated to protecting the NAS layer.

The AMF shall generate access network specific keys from K_{AMF}. In particular,

- the AMF shall generate K_{gNB} and transfer it to the gNB.

- the AMF shall generate NH and transfer it to the gNB, together with the corresponding NCC value.
  The AMF may also transfer an NH key, together with the corresponding NCC value, to another AMF, cf. clause 6.9.

- the AMF shall generate K_{N3IWF} and transfer it to the N3IWF when K_{AMF} is received from SEAF, or when K_{AMF}' is received from another AMF.

Keys in the NG-RAN

The NG-RAN (i.e., gNB or ng-eNB) receives K_{gNB} and NH from the AMF. The ng-eNB uses K_{gNB} as K_{eNB}.

The NG-RAN (i.e., gNB or ng-eNB) shall generate all further access stratum (AS) keys from K_{gNB} and /or NH.

Keys in the N3IWF

The N3IWF receives K_{N3IWF} from the AMF.

The N3IWF shall use K_{N3IWF} as the key MSK for IKEv2 between UE and N3IWF in the procedures for untrusted non-3GPP access, cf. clause 11.

Figure 6.2.2-1 shows the dependencies between the different keys, and how they are derived from the network nodes point of view.

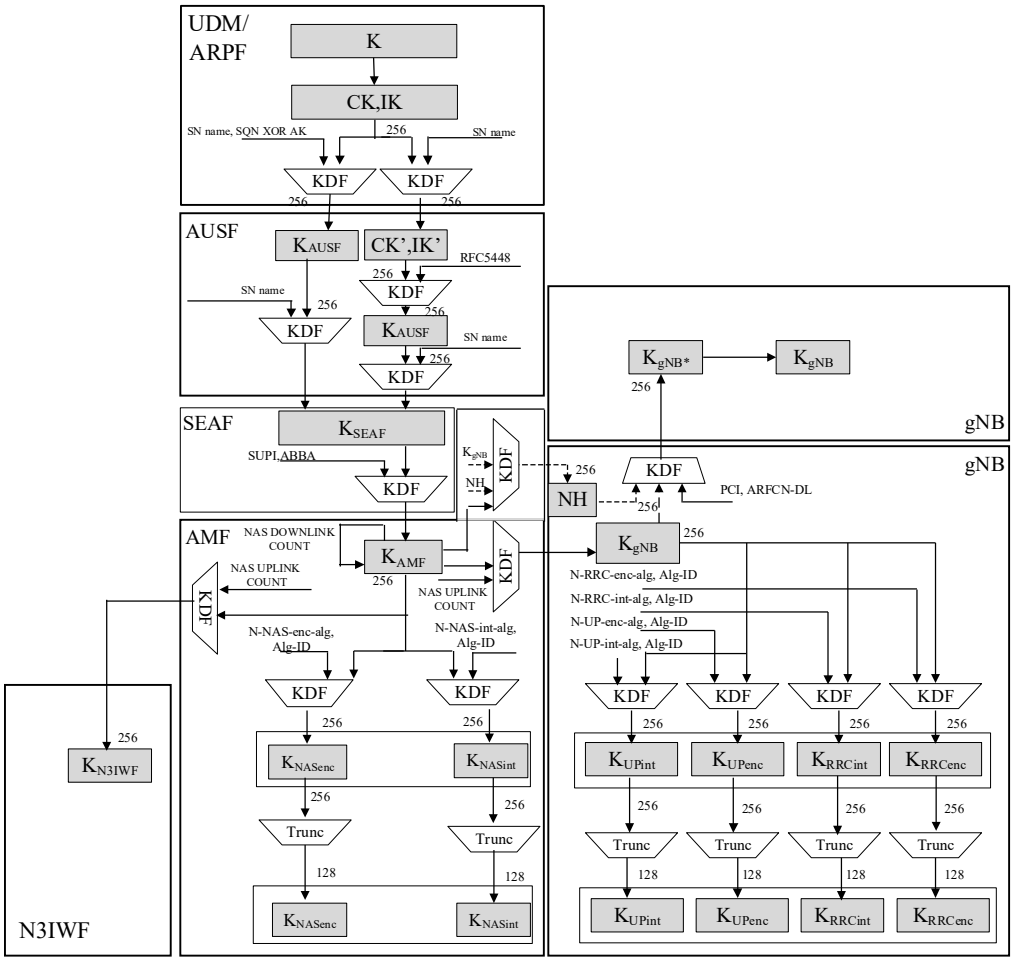


Figure 6.2.2-1: Key distribution and key derivation scheme for 5G for network nodes

NOTE 4: The key derivation and distribution scheme for standalone non-public networks, when an authentication method other than 5G AKA or EAP-AKA' is used, is given in Annex I.2.3.

6.2.2.2 Keys in the UE

For every key in a network entity, there is a corresponding key in the UE.

Figure 6.2.2-2 shows the corresponding relations and derivations as performed in the UE.

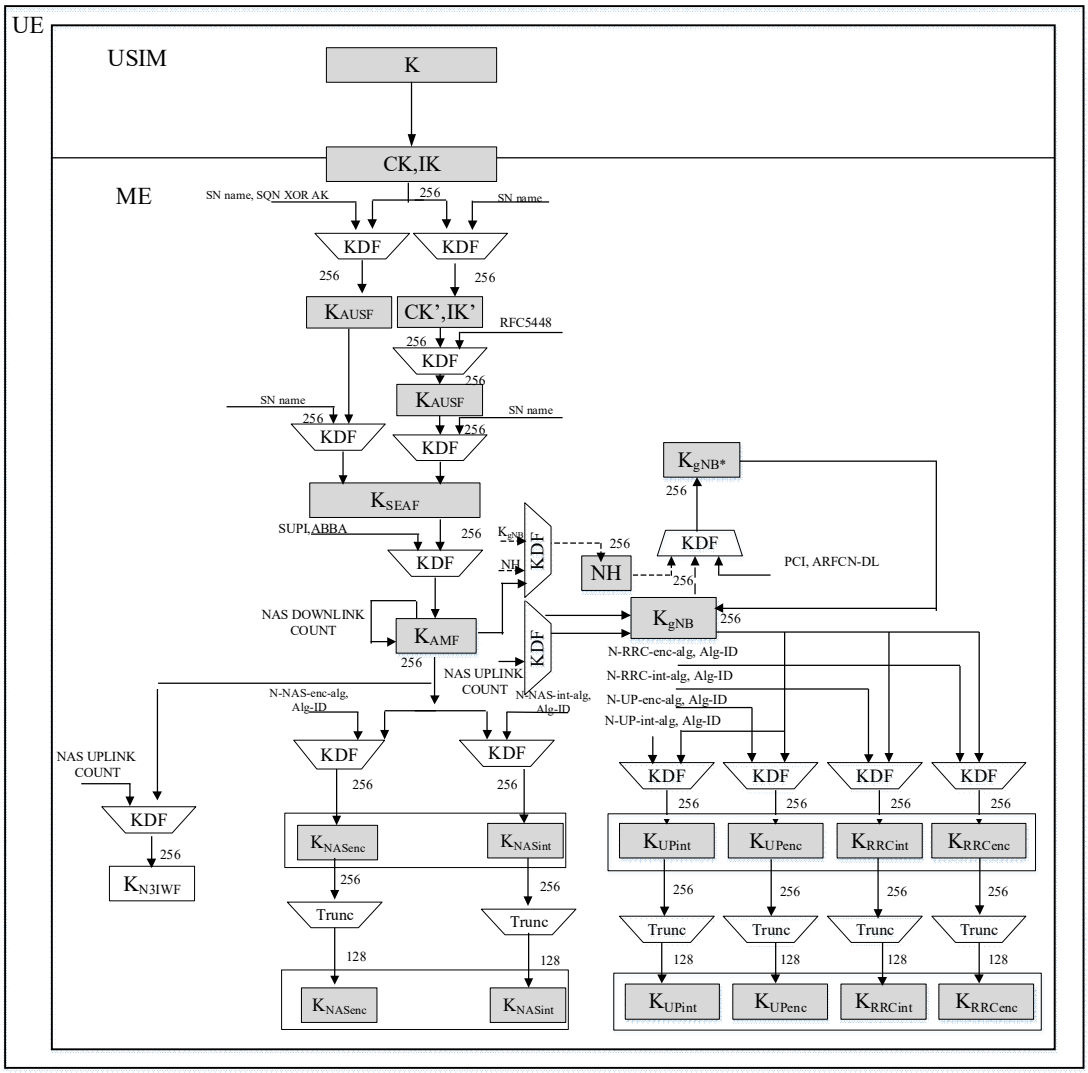


Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE

Keys in the USIM

The USIM shall store the same long-term key K that is stored in the ARPF.

During an authentication and key agreement procedure, the USIM shall generate key material from K that it forwards to the ME.

If provisioned by the home operator, the USIM shall store the Home Network Public Key used for concealing the SUPI.

Keys in the ME

The ME shall generate the K_{AUSF} from the CK, IK received from the USIM. The generation of this key material is specific to the authentication method and is specified in clause 6.1.3.

When 5G AKA is used, the generation of RES* from RES shall be performed by the ME.

The UE shall store the latest K_{AUSF} or replace the old K_{AUSF} with the latest K_{AUSF}, after successful completion of the latest primary authentication . If the USIM supports 5G parameters storage, K_{AUSF} shall be stored in the USIM. Otherwise, K_{AUSF} shall be stored in the non-volatile memory of the ME.

In case 5G AKA is used as an authentication method, upon receiving the valid NAS Security Mode Command message from the AMF (to take the corresponding partial context derived from the newly generated K_{AUSF} into use), the UE shall

consider the performed primary authentication as successful and the UE shall store the newly generated K_{AUSF} as the latest K_{AUSF} or replace the old K_{AUSF} with the latest K_{AUSF}.

In case of any key generating EAP method in the present document (EAP-AKA', EAP-TLS in Annex B, EAP methods in Annex I) is used as the authentication method for the primary (re)authentication, upon receiving the EAP-Success message, the primary authentication shall be considered as successful and the UE shall store the newly generated K_{AUSF} as the latest K_{AUSF} or replace the old K_{AUSF} with the latest K_{AUSF}.

The ME shall perform the generation of K_{SEAF} from the K_{AUSF}. If the USIM supports 5G parameters storage, K_{SEAF} shall be stored in the USIM. Otherwise, K_{SEAF} shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of K_{AMF}. If the USIM supports 5G parameters storage, K_{AMF} shall be stored in the USIM. Otherwise, K_{AMF} shall be stored in the non-volatile memory of the ME.

The ME shall perform the generation of all other subsequent keys that are derived from the K_{AMF}.

Any 5G security context, K_{AUSF} and K_{SEAF} that are stored at the ME shall be deleted from the ME if:

a) the USIM is removed from the ME when the ME is in power on state;

b) the ME is powered up and the ME discovers that the USIM is different from the one which was used to create the 5G security context;

c) the ME is powered up and the ME discovers that there is no USIM is present at the ME.

NOTE 1: The key derivation and distribution scheme for standalone non-public networks, when an authentication method other than 5G AKA or EAP-AKA' is used, is given in Annex I.2.3.

6.2.3 Handling of user-related keys

6.2.3.1 Key setting

Key setting happens at the end of successful authentication procedure. Authentication and key setting may be initiated by the network as often as the network operator wishes when an active NAS connection exists. Key setting can occur as soon as the identity of the mobile subscriber (i.e. 5G-GUTI or SUPI) is known by the AMF. A successful run of 5G AKA or EAP AKA' results in a new K_{AMF} that is stored in the UE and the AMF with a new partial, non-current security context.

NAS keys (i.e. K_{NASint} and K_{NASenc}) and AS keys (i.e. K_{gNB}, K_{RRCenc}, K_{RRCint}, K_{UPenc}, K_{UPint}) are derived from K_{AMF} using the KDFs specified in Annex A. The NAS keys derived from the new K_{AMF} are taken in use in the AMF and the UE by means of the NAS security mode command procedure (see sub-clause 6.7.2). The AS keys are taken into use with the AS security mode command procedure (see sub-clause 6.7.4) or with the key change on the fly procedure (see sub-clause 6.9.6).

For the non-3GPP access, the key K_{N3IWF} is derived from the K_{AMF}. K_{N3IWF} is stored in the UE and the N3IWF as specified in subclause 7.2.1. This key K_{N3IWF} and the IPsec SA cryptographic keys are taken into use with the establishment of IPsec Security Association (SA) between the UE and the N3IWF.

NOTE: For mapped security contexts, the K_{AMF} is derived from EPS keys during interworking with EPS (see clause 8).

6.2.3.2 Key identification

The key K_{AMF} shall be identified by the key set identifier ngKSI. ngKSI may be either of type native or of type mapped. An ngKSI shall be stored in the UE and the AMF together with K_{AMF} and the temporary identifier 5G-GUTI, if available.

NOTE 1: The 5G-GUTI points to the AMF where the K_{AMF} is stored.

A native ngKSI is associated with the K_{SEAF} and K_{AMF} derived during primary authentication. It is allocated by the SEAF and sent with the authentication request message to the UE where it is stored together with the K_{AMF}. The purpose of the ngKSI is to make it possible for the UE and the AMF to identify a native security context without

invoking the authentication procedure. This is used to allow re-use of the native security context during subsequent connection set-ups.

A mapped ngKSI is associated with the K_{AMF} derived from EPS keys during interworking, cf. clause 8 of the present document. It is generated in both the UE and the AMF respectively when deriving the mapped K_{AMF} when moving from EPS to 5GS. The mapped ngKSI is stored together with the mapped K_{AMF}.

The purpose of the mapped ngKSI is to make it possible for the UE and the AMF to indicate the use of the mapped K_{AMF} in interworking procedures (for details cf. clause 8).

The format of ngKSI shall allow a recipient of such a parameter to distinguish whether the parameter is of type native or of type mapped. The format shall contain a type field and a value field. The type field indicates the type of the key set. The value field consists of three bits where seven values, excluding the value '111', are used to identify the key set. The value '111' is reserved to be used by the UE to indicate that a valid K_{AMF} is not available for use. The format of ngKSI is described in [35]

K_{NASenc} and K_{NASint} in the key hierarchy specified in clause 6.2.1, which are derived from K_{AMF}, can be uniquely identified by ngKSI together with those parameters from the set {algorithm distinguisher, algorithm identifier}, which are used to derive these keys from K_{AMF}.

The K_{N3IWF} can be uniquely determined by ngKSI together with the uplink NAS COUNT are used to derive it according to clause A.9.

The initial K_{gNB} can be uniquely determined by ngKSI, together with the uplink NAS COUNT are used to derive it according to clause A.9.

The intermediate key NH as defined in clause 6.9.2.1.1 can be uniquely determined by ngKSI, together with the initial K_{gNB} derived from the current 5G NAS security context for use during the ongoing CM-CONNECTED state and a counter counting how many NH-derivations have already been performed from this initial K_{gNB} according to clause A.10. The next hop chaining counter, NCC, represents the 3 least significant bits of this counter.

Intermediate key $K_{NG\text{-}RAN}$*, as well as non-initial K_{gNB}, defined in clause 6.9.2.1.1 can be uniquely identified by ngKSI together with those parameters from the set {K_{gNB} or NH, sequence of PCIs and ARFCN-DLs}, which are used to derive these keys from K_{gNB} or NH.

K_{RRCint}, K_{RRCenc}, K_{UPint}, and K_{UPenc} in the key hierarchy specified in clause 6.2.1 can be uniquely identified by ngKSI together with those parameters from the set {algorithm distinguisher, algorithm identifier}, which are used to derive these keys from K_{gNB}.

NOTE 2: In addition to 5G security contexts, the UE may also cache EPS security contexts. These EPS security contexts are identified by the eKSI, as defined in TS 33.401 [10].

6.2.3.3 Key lifetimes

K_{AUSF}, and K_{SEAF} shall be created when running a successful primary authentication as described in clause 6.1.3.

K_{AMF} shall be created in the following cases:

1. Primary authentication
2. NAS key re-keying as described in clause 6.9.4.2
3. NAS key refresh as described in clause 6.9.4.3
4. Interworking procedures with EPS (cf. clauses 8 and 10)

In case the UE does not have a valid K_{AMF}, an ngKSI with value "111" shall be sent by the UE to the network, which can initiate (re)authentication procedure to get a new K_{AMF} based on a successful primary authentication.

K_{NASint} and K_{NASenc} are derived based on a K_{AMF} when running a successful NAS SMC procedure as described in clause 6.7.2.

K_{N3IWF} is derived from K_{AMF} and remains valid as long as the UE is connected to the 5GC over non- 3gpp access or until the UE is reauthenticated.

K_{gNB} and NH are derived based on K_{AMF} or K_{gNB} or NH in the following cases:

1. Inter-gNB-CU-handover as described in clause 6.9.2.3.1
2. State transitions as described in clause 6.8
3. AS key re-keying as described in clause 6.9.4.4
4. AS key refresh as described in clause 6.9.4.5

The K_{RRCint}, K_{RRCenc}, K_{UPint} and K_{UPenc} are derived based on K_{gNB} after a new K_{gNB} is derived.

6.3 Security contexts

6.3.1 Distribution of security contexts

6.3.1.1 General

The present clause focuses on the security contexts themselves; the handling of security contexts in mobility procedures is described in clause 6.9.

6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of the same serving network domain:

- SUPI in the clear
- 5G security contexts, as described in clause 6.9

A 5G authentication vector shall not be transmitted between SEAFs.

Once the subscriber identities and security data have been transmitted from an old to a new network entity the old network entity shall delete the data.

6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains

The transmission of the following subscriber identities and security data is permitted between 5G core network entities of different serving network domains:

- SUPI in the clear
- 5G security contexts, as described in clause 6.9, if the security policy of the transmitting 5G serving network domain allows this.

A 5G authentication vector or non-current 5G security contexts shall not be transmitted to a different 5G serving network domain.

6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains

NOTE 1: No direct interworking between 5G networks and network of generations prior to EPS are foreseen. Therefore, only the interaction between 5G and EPS serving network domains is addressed here.

The transmission of the SUPI in the clear is permitted between 5G and EPS core network entities if it has the form of an IMSI.

The transmission of any unmodified 5G security contexts to a EPS core network entity is not permitted. Details of security context transfer between EPS and 5G core network entities can be found in clause 8.

The transmission of a 5G authentication vector to an EPS core network entity is not permitted. The transmission of any unused EPS authentication vectors to a 5G core network entity is not permitted. If SEAF receives any unused authentication vectors (e.g. in mobility scenarios from legacy MME) they shall be dropped without any processing.

NOTE 2: The rules above differ from the corresponding rules in 3GPP TS 33.401, clause 6.1.6: The latter allows forwarding of UMTS authentication vectors from an SGSN to an MME and back to the same SGSN under certain conditions. But this feature goes against a strict security separation of EPS and 5G domains. As its performance advantage is questionable it was not copied into 5G.

NOTE 3: Security context mapping between EPS and 5G serving networks is allowed, according to clause 8.

6.3.2 Multiple registrations in same or different serving networks

6.3.2.0 General

There are two cases where the UE can be multiple registered in different PLMN's serving networks or in the same PLMN's serving networks. The first case is when the UE is registered in one PLMN serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN serving network over the other type of access (e.g. non-3GPP). The second case is where the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses. The UE will establish two NAS connections with the network in both cases.

NOTE: The UE uses the same subscription credential(s) for multiple registrations in the same or different serving networks.

6.3.2.1 Multiple registrations in different PLMNs

The UE shall independently maintain and use two different 5G security contexts, one per PLMN's serving network. Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

The ME shall store the two different 5G security contexts on the USIM if the USIM supports the 5G parameters storage. If the USIM does not support the 5G parameters storage, then the ME shall store the two different 5G security contexts in the ME non-volatile memory. Both of the two different 5G security contexts are current 5G security context.

The latest K_{AUSF} result of the successful completion of the latest primary authentication shall be used by the UE and the HN regardless over which access network type (3GPP or non-3GPP) it was generated.

The HN shall keep the latest K_{AUSF} generated during successful authentication over a given access even if the UE is deregistered from that access, but the UE is registered via another access.

6.3.2.2 Multiple registrations in the same PLMN

When the UE is registered in the same AMF in the same PLMN serving network over both 3GPP and non-3GPP accesses, the UE shall establish two NAS connections with the network. Upon receiving the registration request message, the AMF should check whether the UE is authenticated by the network. The AMF may decide to skip a new authentication run in case there is an available 5G security context for this UE by means of 5G-GUTI, e.g. when the UE successfully registered to 3GPP access.

If the UE registers to the same AMF via non-3GPP access, the AMF can decide not to run a new authentication if it has an available security context to use. In this case, the UE shall directly take into use the available common 5G NAS security context and use it to protect the registration over the non-3GPP access. If there are stored NAS counts for the non-3GPP access for the PLMN in the UE, then the stored NAS counts for the non-3GPP access for the PLMN shall be used to protect the registration over the non-3GPP access. Otherwise, the common 5G NAS security context is taken into use for the first time (partial) over non-3GPP access. In this case, the UL NAS COUNT value and DL NAS COUNT value for the non-3GPP access needs to be set to zero by the UE before the UE is taking the 5G NAS security context into use over non 3GPP access.

The AMF and the UE shall establish a common NAS security context consisting of a single set of NAS keys and algorithm at the time of first registration over any access. The AMF and the UE shall also store parameters specific to each NAS connection in the common NAS security context including two pairs of NAS COUNTs for each access (i.e. 3GPP access and non-3GPP access). The connection specific parameters are specified in clause 6.4.2.2 of the present document.

6.4 NAS security mechanisms

6.4.1 General

This sub-clause describes the security mechanisms for the protection of NAS signalling and data between the UE and the AMF over the N1 reference point. This protection involves both integrity and confidentiality protection. The security parameters for NAS protection are part of the 5G security context described in sub-clause 6.3 of the present document.

6.4.2 Security for multiple NAS connections

6.4.2.1 Multiple active NAS connections with different PLMNs

TS 23.501 [2] has a scenario when the UE is registered to a VPLMN's serving network via 3GPP access and to another VPLMN's or HPLMN's serving network via non-3GPP access at the same time. When the UE is registered in one PLMN's serving network over a certain type of access (e.g. 3GPP) and is registered to another PLMN's serving network over another type of access (e.g. non-3GPP), then the UE has two active NAS connections with different AMF's in different PLMNs. As described in clause 6.3.2.1, the UE shall independently maintain and use two different 5G security contexts, one per PLMN serving network. The 5G security context maintained by the UE shall contain the full set of 5G parameters, including NAS context parameters for 3GPP and non-3GPP access types per PLMN. In case of connection to two different PLMNs, it is necessary to maintain a complete 5G NAS security context for each PLMN independently, each with all associated parameters (such as two pairs of NAS COUNTs, i.e. one pair for 3GPP access and one pair for non-3GPP access).

Each security context shall be established separately via a successful primary authentication procedure with the Home PLMN.

All the NAS and AS security mechanisms defined for single registration mode are applicable independently on each access using the corresponding 5G security context.

NOTE: The UE belongs to a single HPLMN.

6.4.2.2 Multiple active NAS connections in the same PLMN's serving network

When the UE is registered in a serving network over two types of access (e.g. 3GPP and non-3GPP), then the UE has two active NAS connections with the same AMF. A common 5G NAS security context is created during the registration procedure over the first access type.

In order to realize cryptographic separation and replay protection, the common NAS security-context shall have parameters specific to each NAS connection. The connection specific parameters include a pair of NAS COUNTs for uplink and downlink and unique NAS connection identifier. The value of the unique NAS connection identifier shall be set to "0x01" for 3GPP access and set to "0x02" for non-3GPP access. All other parameters as e.g. algorithm identifiers in the common NAS security context are common to multiple NAS connections.

In non-mobility cases, when the UE is simultaneously registered over both types of accesses, and if NAS key re-keying as described in clause 6.9.4.2 or if NAS key refresh as described in clause 6.9.4.3 takes place over one of the accesses (say access A):

1) If the other access (access B) is in CM-CONNECTED state, then the new NAS security context shall only be activated over that access (access A). The UE and the AMF shall not change the NAS security context in use on the other access (say access B). In order to activate the new NAS security context over the other access (access B), the AMF shall trigger a NAS SMC run over that access either in the current running procedure or a subsequent NAS procedure. During the second NAS SMC run (on access B), the AMF shall include the same ngKSI associated with the new NAS security context and the same algorithm choices as for the first access. After a successful second NAS SMC procedure over the other access (access B), both the UE and the AMF shall delete the old NAS security context.

2) Whenever the AMF sends a NAS SMC over access (access A) and AMF considers the UE to not be in CM-CONNECTED state on the other access (access B), the AMF shall additionally activate (if not already in use on the other access) the security context that is active on the other accesses. Similarly, whenever the UE receives a

NAS SMC over the access (access A) and UE is not in CM-CONNECTED state on the other access (access B), the UE additionally activates (if not already in use on the other access) the security context on the other access.

In case of 3GPP access mobility or interworking with EPS, the following procedures apply:

1) If the UE is in CM-CONNECTED state on the non-3GPP access, then:

   a) if the AMF does not have the security context the UE is using on the non-3GPP access (e.g. K_{AMF} change on 3GPP access when the AMF changes), then in order to activate the same NAS security context that is in use over the 3GPP access the AMF shall run a NAS SMC procedure on the non-3GPP access; or

   b) in the case of handover from EPS, then a mapped context will be in use on the 3GPP access and a different security context will be active on the non-3GPP access. To align the security contexts in use over both accesses, the AMF shall run a NAS SMC procedure over one access to take into use on that access the security context that is in use on the other access. In the case that a native security context is in use on the non-3GPP access, then the NAS SMC procedure shall be on the 3GPP access to take the native security context into use.

2) Whenever the AMF sends a Registration Accept over the 3GPP access and AMF considers the UE to not be in CM-CONNECTED state on the non-3GPP access, the AMF shall activate (if not already in use on the non-3GPP access) the security context that is in use on the 3GPP access on the non-3GPP access. The AMF shall keep a native security context that was in use on non-3GPP access if the security context in use on the 3GPP access is a mapped security context. In order to take this native security context into use, the AMF shall run a NAS SMC procedure.

   Similarly, whenever the UE receives a Registration Accept over the 3GPP access and UE is not in CM-CONNECTED state on the non-3GPP access, the UE activates (if not already in use on the non-3GPP access) the security context that is in use on the 3GPP access on the non-3GPP access. The UE shall keep a native security context that was in use on non-3GPP access if the security context in use on the 3GPP access is a mapped security context.

To recover from a failure to align the NAS security contexts due to a state mis-match between AMF and UE, the AMF can align the security contexts in use on the 3GPP and non-3GPP access using the a NAS SMC procedure during a subsequent registration procedure (that was either initiated by the UE or sent in response to a Service Reject if the UE sends a Service Request).

6.4.3 NAS integrity mechanisms

6.4.3.0 General

Integrity protection for NAS signalling messages shall be provided as part of the NAS protocol.

6.4.3.1 NAS input parameters to integrity algorithm

The input parameters to the NAS 128-bit integrity algorithms as described in Annex D shall be set as follows.

The KEY input shall be equal to the K_{NASint} key.

The BEARER input shall be equal to the NAS connection identifier.

The DIRECTION bit shall be set to 0 for uplink and 1 for downlink.

The COUNT input shall be constructed as follows:

COUNT := 0x00 || NAS COUNT

Where NAS COUNT is the 24-bit NAS UL COUNT or the 24-bit NAS DL COUNT value, depending on the direction, that is associated to the current NAS connection identified by the value used to form the BEARER input.

A NAS COUNT shall be constructed as follows:

NAS COUNT := NAS OVERFLOW || NAS SQN

Where

- NAS OVERFLOW is a 16-bit value which is incremented each time the NAS SQN is incremented from the maximum value.
- NAS SQN is the 8-bit sequence number carried within each NAS message.

The use and mode of operation of the 128-bit integrity algorithms are specified in Annex D.

6.4.3.2 NAS integrity activation

NAS integrity shall be activated using the NAS SMC procedure or after an inter-system handover from EPC.

Replay protection shall be activated when integrity protection is activated, except when the NULL integrity protection algorithm is selected. Replay protection shall ensure that the receiver only accepts each incoming NAS COUNT value once using the same NAS security context.

Once NAS integrity has been activated, NAS messages without integrity protection shall not be accepted by the UE or the AMF. Before NAS integrity has been activated, NAS messages without integrity protection shall only be accepted by the UE or the AMF in certain cases where it is not possible to apply integrity protection.

NAS integrity shall stay activated until the 5G security context is deleted in either the UE or the AMF. It shall not be possible to change from non-NULL integrity protection algorithm to NULL integrity protection.

6.4.3.3 NAS integrity failure handling

The supervision of failed NAS integrity checks shall be performed both in the ME and the AMF. In case of failed integrity check (i.e. faulty or missing NAS-MAC) is detected after the start of NAS integrity protection, the concerned message shall be discarded except for some NAS messages specified in TS 24.501 [35]. For those exceptions the AMF shall take the actions specified in TS 24.501 [35] when receiving a NAS message with faulty or missing NAS-MAC. Discarding NAS messages can happen on the AMF side or on the ME side.

6.4.4 NAS confidentiality mechanisms

6.4.4.0 General

Confidentiality protection for NAS signalling messages shall be provided as part of the NAS protocol.

6.4.4.1 NAS input parameters to confidentiality algorithm

The input parameters for the NAS 128-bit ciphering algorithms shall be the same as the ones used for NAS integrity protection as described in clause 6.4.3, with the exception that a different key, K_{NASenc}, is used as KEY, and there is an additional input parameter, namely the length of the key stream to be generated by the encryption algorithms.

The use and mode of operation of the 128-bit ciphering algorithms are specified in Annex D.

NOTE: In the context of the present subclause 6.4.4, a message is considered ciphered also when the NULL encryption algorithm NEA0 is applied.

6.4.4.2 NAS confidentiality activation

NAS confidentiality shall be activated using the NAS SMC procedure or after an inter-system handover from EPC.

Once NAS confidentiality has been activated, NAS messages without confidentiality protection shall not be accepted by the UE or the AMF. Before NAS confidentiality has been activated, NAS messages without confidentiality protection shall only be accepted by the UE or the AMF in certain cases where it is not possible to apply confidentiality protection.

NAS confidentiality shall stay activated until the 5G security context is deleted in either the UE or the AMF.

6.4.5 Handling of NAS COUNTs

The NAS security context created at the registration time of the first access type contains the NAS integrity and encryption keys, selected algorithm common for all NAS connections. In addition, each NAS connection shall have a

unique NAS connection identifier, a distinct pair of NAS COUNTs, one NAS COUNT for uplink and one NAS COUNT for downlink, associated with it. In the NAS security context, the NAS connection identifier shall be the differentiator for the connection-specific parameters.

It is essential that the NAS COUNTs for a particular K_{AMF} are not reset to the start values (that is the NAS COUNTs only have their start value when a new K_{AMF} is generated). This prevents the security issue of using the same NAS COUNTs with the same NAS keys, e.g. key stream re-use, in the case a UE moves back and forth between two AMFs and the same NAS keys are re-derived.

In the AMF, all the distinct pairs of NAS COUNTs part of the same 5G NAS security context, shall only be set to the start value in the following cases:

- for a partial native 5GC NAS security context created by a successful primary authentication run on one of the NAS connections established between the same AMF and the UE, or,
- for a mapped 5G security context generated when a UE moves from an MME to the AMF during both idle and connected mode mobility, or,
- for a new K_{AMF} taken into use in a target AMF during mobility registration update or handover.

The start value of NAS COUNT shall be zero (0).

6.4.6 Protection of initial NAS message

The initial NAS message is the first NAS message that is sent after the UE transitions from the idle state. The UE shall send a limited set of IEs (called the cleartext IEs) including those needed to establish security in the initial message when it has no NAS security context. When the UE has a NAS security context, the UE shall send a message that has the complete initial NAS message ciphered in a NAS Container along with the cleartext IEs with whole message integrity protected. The complete initial message is included in the NAS Security Mode Complete message in a NAS Container when needed (e.g. AMF cannot find the used security context) in the latter case and always in the former case as described below.

In case, the UE selects a PLMN other than Registered PLMN/EPLMN in the 5GMM-IDLE state and the UE has a NAS security context containing the NEA0, then the UE shall discard the NAS security context and shall follow the procedure specified in this clause for protection of initial NAS message.

The protection of the initial NAS message proceeds as shown in Figure 6.4.6-1.

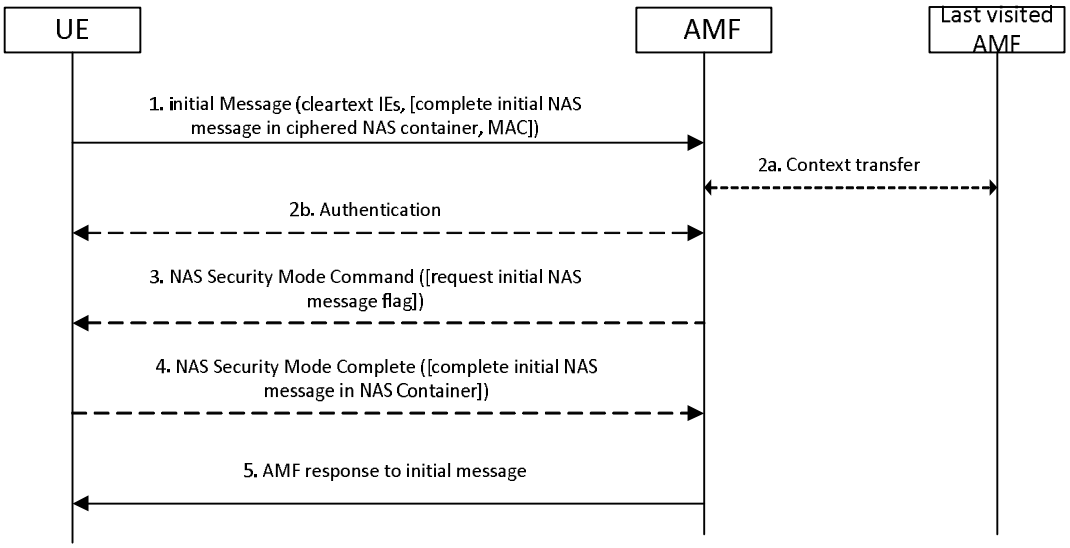


Figure 6.4.6-1: Protecting the initial NAS message

Step 1: The UE shall send the initial NAS message to the AMF. If the UE has no NAS security context, the initial NAS message shall only contain the cleartext IEs, i.e. subscription identifiers (e.g. SUCI or GUTIs), UE security capabilities,

ngKSI, indication that the UE is moving from EPC, Additional GUTI, and IE containing the TAU Request in the case idle mobility from LTE.

If the UE has a NAS security context, the message sent shall contain the information given above in cleartext and the complete initial NAS message ciphered in a NAS container which is ciphered. With a NAS security context, the sent message shall also be integrity protected. In the case that the initial NAS message was protected and the AMF has the same security context, then steps 2 to 4 may be omitted In this case the AMF shall use the complete initial NAS message that is in the NAS container as the message to respond to..

Step 2: If the AMF is not able to find the security context locally or from last visited AMF, or if the integrity check fails, then the AMF shall initiate an authentication procedure with the UE. If the AMF fetches old security context from the last visited AMF, the AMF may decipher the NAS container with the same security context, and get the initial NAS message, then the step 2b to 4 may be omitted. If the AMF fetches new K_{AMF} from the last visited AMF (receiving keyAmfChangeInd), the step 2b may be omitted.

Step 3: If the authentication of the UE is successful, the AMF shall send the NAS Security Mode Command message. If the initial NAS message was protected but did not pass the integrity check (due either to a MAC failure or the AMF not being able to find the used security context) or the AMF could not decrypt the complete initial NAS message in the NAS container (due to receiving "keyAmfChangeInd" from the last visited AMF), then the AMF shall include in the Security Mode Command message a flag requesting the UE to send the complete initial NAS message in the NAS Security Mode Complete message.

Step 4: The UE shall send the NAS Security Mode Complete message to the network in response to a NAS Security Mode Command message. The NAS Security Mode Complete message shall be ciphered and integrity protected. Furthermore the NAS Security Mode Complete message shall include the complete initial NAS message in a NAS Container if either requested by the AMF or the UE sent the initial NAS message unprotected. The AMF shall use the complete initial NAS message that is in the NAS container as the message to respond to.

Step 5: The AMF shall send its response to the Initial NAS message. This message shall be ciphered and integrity protected.

6.4.7 Security aspects of SMS over NAS

Specific services of SMS over NAS are defined in TS 23.501 [2], and procedures for SMS over NAS are specified in TS 23.502 [8].

For registration and de-registration procedures for SMS over NAS, the details are specified in subclause 4.13.3.1 and 4.13.3.2 in TS 23.502 [8]. The NAS message can be protected by NAS security mechanisms.

For MO/MT SMS over NAS via 3GPP/non-3GPP when the UE has already activated NAS security with the AMF before sending/receiving SMS, the NAS Transport message shall be ciphered and integrity protected using the NAS security context by the UE/AMF as described in sub-clause 6.4 in the present document.

6.5 RRC security mechanisms

6.5.1 RRC integrity mechanisms

RRC integrity protection shall be provided by the PDCP layer between UE and gNB and no layers below PDCP shall be integrity protected. Replay protection shall be activated when integrity protection is activated (except for when the selected integrity protection algorithm is NIA0, see Annex D). Replay protection shall ensure that the receiver accepts each particular incoming PDCP COUNT value only once using the same AS security context.

The use and mode of operation of the 128-NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA algorithms as described in Annex D are the RRC message as MESSAGE, an 128-bit integrity key K_{RRCint} as KEY, a 5-bit bearer identity BEARER which value is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION and a bearer specific direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side. UE may trigger a recovery procedure as specified in TS 38.331 [22].

NOTE: Failed integrity check does not always imply that the concerned message is silently discarded.

6.5.2 RRC confidentiality mechanisms

RRC confidentiality protection is provided by the PDCP layer between UE and gNB.

The use and mode of operation of the 128-NEA algorithms are specified in Annex D.

The input parameters to the 128-bit NEA algorithms as described in Annex D are a 128-bit cipher Key K_{RRCenc} as KEY, a 5-bit bearer identity BEARER which corresponds to the radio bearer identity, the 1-bit direction of transmission DIRECTION, the length of the keystream required LENGTH and a bearer specific direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

6.5.3 RRC UE capability transfer procedure

The network should activate AS security (i.e., perform a successful AS SMC procedure) before running the RRC UE capability transfer procedure.

With the exception of unauthenticated emergency calls and the UEs using Control plane CIoT optimization,, if the network had acquired UE capabilities using RRC UE capability transfer procedure before AS security activation, then the network shall not store them locally for later use and shall not send them to other network entities. In that case, the network shall re-run the RRC UE capability transfer procedure after a successful AS SMC procedure.

NOTE 1: For UEs without AS security (e.g., UEs using Control Plane CIoT optimization), RRC UE radio capability transfer procedure cannot be protected.

6.6 UP security mechanisms

6.6.1 UP security policy

The SMF shall provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure as specified in TS 23.502 [8].

The UP security policy shall indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy shall be used to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

The ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per each DRB, according to the received UP security policy, using RRC signalling as defined in clause 6.6.2. If the user plane security policy indicates "Required" or "Not needed", the ng-eNB/gNB shall not overrule the UP security policy provided by the SMF. If the ng-eNB/gNB cannot activate UP confidentiality and/or UP integrity protection when the received UP security policy is "Required", the ng-eNB/gNB shall reject establishment of UP resources for the PDU Session and indicate reject-cause to the SMF. If the received UP security policy is "Not needed ", then the establishment of the PDU Session shall proceed as described in TS 23.502 [8]. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the ng-eNB can activate UP integrity protection.

NOTE 1: Local SMF can override the confidentiality option in the UP security policy received from the home SMF based on its local policy, roaming agreement and/or regulatory requirements.

At an Xn-handover from the source ng-eNB/gNB to the target ng-eNB/gNB, the source ng-eNB/gNB shall include in the HANDOVER REQUEST message, the UE's UP security policy. If the UP security policy is ‘Required’, the target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF. For the accepted PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy and shall indicate that to the UE in the HANDOVER COMMAND by the source ng-eNB/gNB. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection and/or UP encryption for a PDU session is enabled at the target ng-eNB/gNB, the UE shall generate or update the UP encryption key and/or UP integrity protection key and shall activate UP encryption and/or UP integrity protection for the respective PDU session.

NOTE 2: If the security policy is 'Preferred', it is possible to have a change in activation or deactivation of UP integrity after the handover.

Further, in the Path-Switch message, the target ng-eNB/gNB shall send the UE's UP security policy and corresponding PDU session ID received from the source ng-eNB/gNB to the SMF. The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target ng-eNB/gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm.

If the target ng-eNB/gNB receives UE's UP security policy from the SMF in the Path-Switch Acknowledge message, the target ng-eNB/gNB shall update the UE's UP security policy with the received UE's UP security policy. If UE's current UP confidentiality and/or UP integrity protection activation is different from the received UE's UP security policy, then the target ng-eNB/gNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure to reconfigure the DRBs to activate or de-activate the UP integrity/confidentiality as per the received policy from SMF.

In case of the target ng-eNB/gNB receives both UE security capability and UP security policy, then ng-eNB/gNB initiates the intra-cell handover procedure which contains selected algorithm and an NCC to the UE. New UP keys shall be derived and used at both the UE and the target ng-eNB/gNB.

At an N2-handover the SMF shall send the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF via the target AMF. For all other PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

At interworking-handover from EPS to 5GS, the SMF+PGW-C provides the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB shall determine from the UP security policy received from the AMF together with the UE indication that it supports user plane integrity protection with ng-eNB in UE EPS security capabilities (i.e. bit EIA7), whether to activate user plane integrity protection with the UE or not. The target ng-eNB/gNB shall reject all DRBs for which it cannot comply with the corresponding UP integrity protection policy in the UP security policy and indicate the reject-cause to the source MME via the target AMF. For all other DRBs, the target ng-eNB/gNB shall activate UP integrity protection per DRB according to the used UP security policy. Only if the UE indicates that it supports use of user plane integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection. If the target AMF detects in a Registration procedure following interworking-handover from EPS to 5GS, and becomes aware of that there is a mismatch between the UE EPS security capabilities received from the source MME and the one received from the UE, and that the target ng-eNB may not have the UE capability indicating UP IP support in UE EPS security capabilities, then the AMF shall send an N2 CONTEXT MODIFICATION REQUEST message to inform the target ng-eNB about the correct UE EPS security capabilities and target ng-eNB shall take the new UE EPS security capabilities into account.

6.6.2 UP security activation mechanism

AS UP integrity protection and ciphering activation shall be done as part of the DRB addition procedure using RRC Connection Reconfiguration procedure as described in this clause, see Figure 6.6.2-1.

The SMF shall send the UP security policy to the gNB/ng-eNB as defined in Clause 6.6.1.

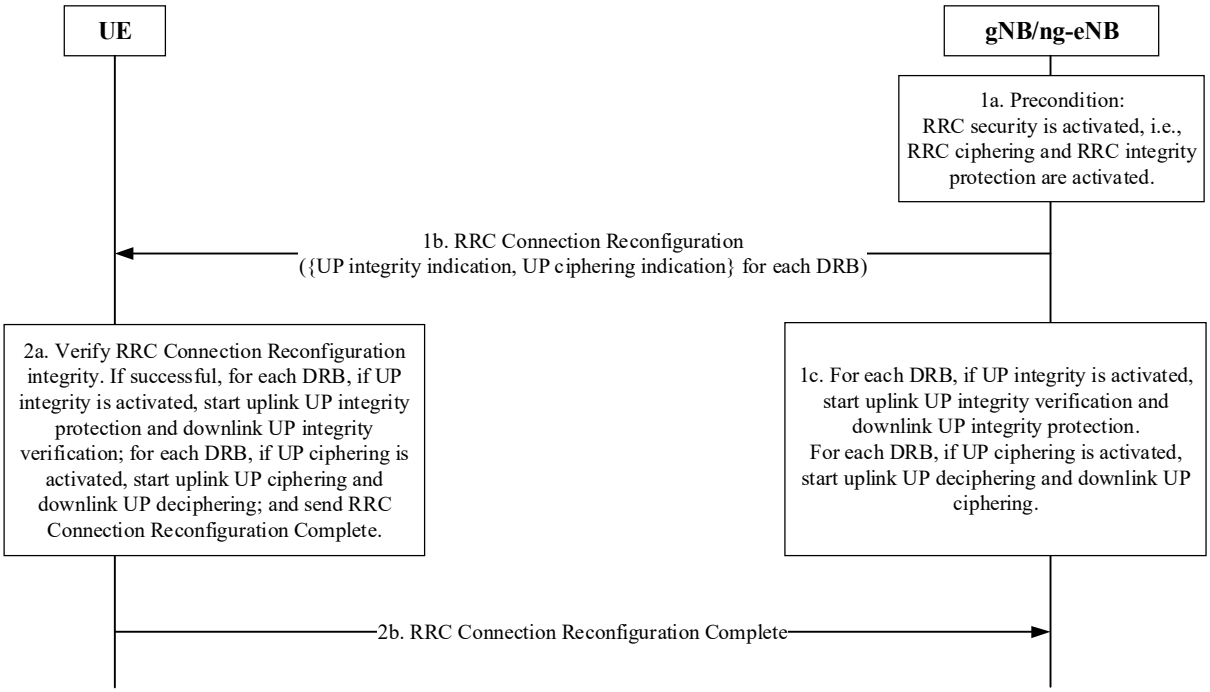


Figure 6.6.2-1: User plane (UP) security activation mechanism

1a. This RRC Connection Reconfiguration procedure which is used to add DRBs shall be performed only after RRC security has been activated as part of the AS security mode command procedure defined in Clause 6.7.4.

1b. The gNB/ng-eNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation containing indications for the activation of UP integrity protection and ciphering for each DRB according to the security policy.

1c. If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB/ng-eNB does not have K_{UPint}, the gNB/ng-eNB shall generate K_{UPint} and UP integrity protection for such DRBs shall start at the gNB/ng-eNB. Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB/ng-eNB does not have K_{UPenc}, the gNB/ng-eNB shall generate K_{UPenc} and UP ciphering for such DRBs shall start at the gNB/ng-eNB.

2a. UE shall verify the RRC Connection Reconfiguration message. If successful:

2a.1 If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have K_{UPint}, the UE shall generate K_{UPint} and UP integrity protection for such DRBs shall start at the UE.

2a.2 Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have K_{UPenc}, the UE shall generate K_{UPenc} and UP ciphering for such DRBs shall start at the UE

2b. If the UE successfully verifies integrity of the RRC Connection Reconfiguration message, the UE shall send the RRC Connection Reconfiguration Complete message to the gNB/ng-eNB.

If UP integrity protection is not activated for DRBs, the gNB/ng-eNB and the UE shall not integrity protect the traffic of such DRB and shall not put MAC-I into PDCP packet.

If UP ciphering is not activated for DRBs, the gNB/ng-eNB and the UE shall not cipher the traffic of such DRBs.

6.6.3 UP confidentiality mechanisms

The PDCP protocol, as specified in TS 38.323 [23] between the UE and the NG-RAN, shall be responsible for user plane data confidentiality protection.

The use and mode of operation of the 128-bit NEA algorithms are specified in Annex D.

The input parameters to the 128-bit NEA algorithms as described in Annex D are the message packet, an 128-bit cipher key K_{UPenc} as KEY, a 5-bit bearer identity BEARER which value is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, the length of the keystream required LENGTH and a bearer specific, and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

6.6.4 UP integrity mechanisms

6.6.4.1 General

The PDCP protocol, as specified in TS 38.323 [23] between the UE and the NG-RAN, shall be responsible for user plane data integrity protection.

6.6.4.2 UP integrity mechanisms between the UE and the gNB

The use and mode of operation of the 128-bit NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA algorithms as described in Annex D are, the message packet, a 128-bit integrity key K_{UPint} as KEY, a 5-bit bearer identity BEARER value of which is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, and a bearer specific, and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

6.6.4.3 UP integrity mechanisms between the UE and the ng-eNB

If the UE supports E-UTRA connected to 5GC, the UE shall indicate support of integrity protection by setting the EIA7 algorithm bit in 5G UE Security Capability IE (see clause 9.11.3.54 of TS 24.501 [35]) to indicate that the UE supports user plane integrity protection with an ng-eNB.

If the 128-NIA algorithm is signalled by the ng-eNB to the UE, clause 6.6.4.2 applies.

If the 128-EIA algorithm is signalled by the ng-eNB to the UE, the following applies:

- The use and mode of operation of the 128-EIA algorithms are specified in Annex B of TS 33.401 [10].
- The input parameters to the 128-bit EIA algorithms as described in Annex B of TS 33.401 [10] are, the message packet, a 128-bit integrity key K_{UPint} as KEY, a 5-bit bearer identity BEARER value of which is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, and a bearer specific, time and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

NOTE: The ng-eNB decides whether to signal 128-NIA or 128-EIA algorithm (cf. clause 5.3.1.2 of TS 36.331 [69]).

If the ng-eNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

UE and the ng-eNB (or the ng-eNB acting as the MN) shall derive UP integrity key as specified in Annex A.7 of TS 33.401 [10], with the K_{eNB} set to K_{gNB}.

6.7 Security algorithm selection, key establishment and security mode command procedure

6.7.1 Procedures for NAS algorithm selection

6.7.1.1 Initial NAS security context establishment

Each AMF shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for NAS integrity algorithms, and one for NAS ciphering algorithms. These lists shall be ordered according to a priority decided by the operator.

To establish the NAS security context, the AMF shall choose one NAS ciphering algorithm and one NAS integrity protection algorithm. The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists.

6.7.1.2 AMF change

If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document).

6.7.2 NAS security mode command procedure

The NAS SMC shown in Figure 6.7.2-1 shall be used to establish NAS Security context between the UE and the AMF. This procedure consists of a roundtrip of messages between the AMF and the UE. The AMF sends the NAS Security Mode Command message to the UE and the UE replies with the NAS Security Mode Complete message.

NOTE 1: The NAS SMC procedure is designed such that it protects the Registration Request against a man-in-the-middle attack where the attacker modifies the IEs containing the UE security capabilities provided by the UE in the Registration Request. It works as follows: if the method completes successfully, the UE is attached to the network knowing that no bidding down attack has happened. In case a bidding down attack was attempted, the verification of the NAS SMC will fail and the UE replies with a reject message meaning that the UE will not attach to the network.

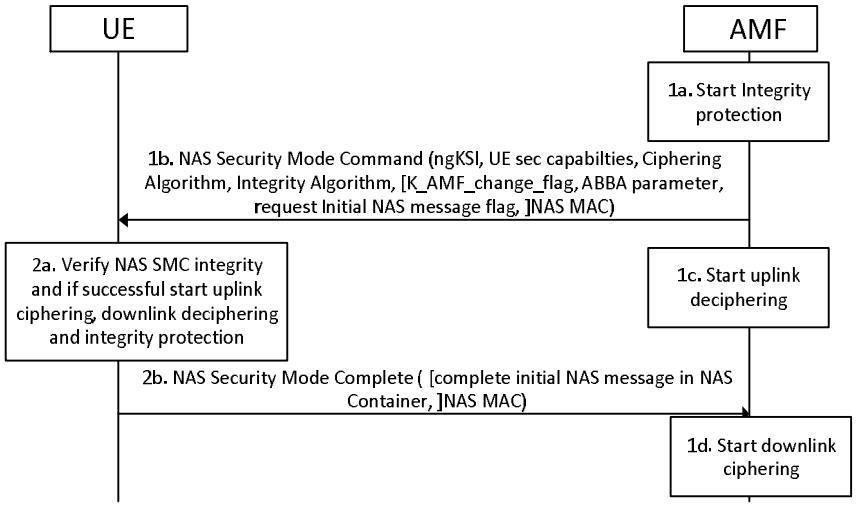


Figure 6.7.2-1: NAS Security Mode Command procedure

1a. The AMF activates the NAS integrity protection before sending the NAS Security Mode Command message.

1b. The AMF sends the NAS Security Mode Command message to the UE. The NAS Security Mode Command message shall contain: the replayed UE security capabilities, the selected NAS algorithms, and the ngKSI for identifying the K_{AMF}. The NAS Security Mode Command message may contain: K_AMF_change_flag (carried in the additional 5G security parameters IE specified in TS 24.501 [35]) to indicate a new K_{AMF} is calculated, a flag requesting the complete initial NAS message (see subclause 6.4.6), Anti-Bidding down Between Architectures (ABBA) parameter. In the case of horizontal derivation of K_{AMF} during mobility registration update or during multiple registration in same PLMN, K_AMF_change_flag shall be included in the NAS Security Mode Command message as described in clause 6.9.3.

This message shall be integrity protected (but not ciphered) with NAS integrity key based on the K_{AMF} indicated by the ngKSI in the NAS Security Mode Command message (see Figure 6.7.2-1).

NOTE 2: Void.

In case the network supports interworking using the N26 interface between MME and AMF, the AMF shall also include the selected EPS NAS algorithms (defined in Annex B of TS 33.401 [10]) to be used after mobility to EPS in the NAS Security Mode Command message (see clause 8.5.2). The UE shall store the algorithms for use after mobility to EPS using the N26 interface between MME and AMF. The AMF shall store the selected EPS NAS algorithms in the UE security context.

NOTE 2a: When AMF change happens either due to N2-handover or idle mode mobility, the selected EPS NAS algorithms is always included in the 5G UE security context and provided to the target AMF as part of the 5G UE security context.

1c. The AMF activates NAS uplink deciphering after sending the NAS Security Mode Command message.

2a. The UE shall verify the NAS Security Mode Command message. This includes checking that the UE security capabilities sent by the AMF match the ones stored in the UE to ensure that these were not modified by an attacker and verifying the integrity protection using the indicated NAS integrity algorithm and the NAS integrity key based on the K_{AMF} indicated by the ngKSI.

In case the NAS Security Mode Command message includes a K_AMF_change_flag, the UE shall derive a new K_{AMF} as described in Annex A.13 and set the NAS COUNTs to zero.

If the verification of the integrity of the NAS Security Mode Command message is successful, the UE shall start NAS integrity protection and ciphering/deciphering with the security context indicated by the ngKSI.

2b. The UE sends the NAS Security Mode Complete message to the AMF ciphered and integrity protected. The NAS Security Mode Complete message shall include PEI in case AMF requested it in the NAS Security Mode Command message. The AMF shall set the NAS COUNTs to zero if horizontal derivation of K_{AMF} is performed. The UE may include the complete initial NAS message (see subclause 6.4.6 for details).

If the verification of the NAS Security Mode Command message is not successful in the UE, it shall reply with a NAS Security Mode Reject message (see TS 24.501 [35]). The NAS Security Mode Reject message and all subsequent NAS messages shall be protected with the previous, if any, 5G NAS security context, i.e., the 5G NAS security context used prior to the failed NAS Security Mode Command message. If no 5G NAS security context existed prior to the NAS Security Mode Command message, the NAS Security Mode Reject message shall remain unprotected.

NOTE 2b: Void.

The AMF shall de-cipher and check the integrity protection on the NAS Security Mode Complete message using the key and algorithm indicated in the NAS Security Mode Command message. NAS downlink ciphering at the AMF with this security context shall start after receiving the NAS Security Mode Complete message.

1d. The AMF activates NAS downlink ciphering.

NOTE 3: If the uplink NAS COUNT will wrap around by sending the NAS Security Mode Reject message, the UE releases the NAS connection instead of sending the NAS Security Mode Reject message.

NOTE 4: If the AMF successfully validated the NAS SMC Complete message, the AMF has successfully confirmed the SUPI received from the home network and the SUPI used by the UE match (as required in clause 5.5.3). However, integrity check failure of the NAS SMC Complete message at the AMF could have other causes than a mismatch of the SUPIs.

6.7.3 Procedures for AS algorithm selection

6.7.3.0 Initial AS security context establishment

This clause provides the details for AS security algorithms negotiation and consideration during the UE initial AS security context establishment.

Each gNB/ng-eNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator. When AS security context is to be established in the gNB/ng-eNB, the AMF shall send the UE 5G security capabilities to the gNB/ng-eNB. The gNB/ng-eNB shall choose the ciphering algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities.

The gNB/ng-eNB shall choose the integrity algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities. The chosen algorithms shall be indicated to the UE in the AS SMC. The chosen ciphering algorithm is used for ciphering (when activated) of the user plane and RRC traffic. The chosen integrity algorithm is used for integrity protection (when activated) of the user plane and RRC traffic. Activation of ciphering and integrity protection for the RRC traffic shall be done as defined by clause 6.7.4. Activation of ciphering and integrity protection for the user plane traffic shall be done based on the UP security policy received from the SMF as defined by clause 6.6.2.

6.7.3.1 Xn-handover

At handover from a source gNB/ng-eNB over Xn to a target gNB/ng-eNB, the source gNB/ng-eNB shall include the UE's 5G security capabilities and ciphering and integrity algorithms used in the source cell in the handover request message. The target gNB/ng-eNB shall select the algorithm with highest priority from the received 5G security capabilities of the UE according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB/ng-eNB selects different algorithms compared to the source gNB/ng-eNB. If the UE does not receive any selection of integrity and ciphering algorithms, it continues to use the same algorithms as before the handover (see TS 38.331 [22] for gNB or TS 36.331 [69] for ng-eNB). When a Xn-handover takes place from ng-eNB to gNB or vice versa, then the selected algorithms in the target node shall always be signalled in the Handover Command to the UE. In the Path-Switch message, the target gNB/ng-eNB shall send the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB/ng-eNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm.

If the target gNB/ng-eNB receives UE's 5G security capabilities from the AMF in the Path-Switch Acknowledge message, the target gNB/ng-eNB shall update the AS security context of the UE with these 5G security capabilities of the UE. The target gNB/ng-eNB shall select the algorithm with highest priority from these 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). If the algorithms selected by the target gNB/ng-eNB are different from the algorithms used at the source gNB/ng-eNB, then the target gNB/ng-eNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure indicating the selected algorithms and an NCC to the UE.

NOTE: Transferring the ciphering and integrity algorithms used in the source cell to the target gNB/ng-eNB in the handover request message allows for the target gNB/ng-eNB to decipher and verify the integrity of the RRC Reestablishment Complete message on SRB1 in the potential RRC Connection Re-establishment procedure. The information is also used by the target gNB/ng-eNB to decide if it is necessary to include a new selection of security algorithms in the Handover Command message.

6.7.3.2 N2-handover

At handover from a source gNB/ng-eNB to a target gNB/ng-eNB over N2 (possibly including an AMF change and hence a transfer of the UE's 5G security capabilities from the source AMF to the target AMF), the target AMF shall send the UE's 5G security capabilities to the target gNB/ng-eNB in the NGAP HANDOVER REQUEST message (see TS 33.413 [34]). The target gNB/ng-eNB shall select the algorithm with highest priority from the UE's 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the

target gNB/ng-eNB selects different algorithms compared to the source gNB/ng-eNB. If the UE does not receive any selection of integrity and ciphering algorithms, it continues to use the same algorithms as before the handover (see TS 38.331 [22]).

For N2-handover, the source gNB/ng-eNB shall include AS algorithms used in the source cell (ciphering and integrity algorithms) in the source to target transparent container that shall be sent to the target gNB/ng-eNB. The AS algorithms used by the source cell are provided to the target gNB/ng-eNB so that it can use them during the potential RRC Connection Re-establishment procedure use them as specified in clause 6.11 for gNB and TS 33.401 [10] for ng-eNB.

6.7.3.3 Intra-gNB-CU handover/intra-ng-eNB handover

It is not required to change the AS security algorithms during intra-gNB-CU/intra-ng-eNB handover. If the UE does not receive an indication of new AS security algorithms during an intra-gNB-CU/intra-ng-eNB handover, the UE shall continue to use the same algorithms as before the handover (see TS 38.331 [22] for gNB and TS 36.331 [69] for ng-eNB).

6.7.3.4 Transitions from RRC_INACTIVE to RRC_CONNECTED states

At state transition from RRC_INACTIVE to RRC_CONNECTED, the source gNB/ng-eNB shall include the UE 5G security capabilities and the ciphering and integrity algorithms the UE was using with the source cell in the Xn-AP Retrieve UE Context Response message.

The target gNB/ng-eNB shall check if it supports the received algorithms, if the target gNB/ng-eNB supports the received ciphering and integrity algorithms, the target gNB/ng-eNB shall check the received algorithms to its locally configured list of algorithms (this applies for both integrity and ciphering algorithms). If the target gNB/ng-eNB selects the same security algorithms, the target gNB/ng-eNB shall use the selected algorithms to derive RRC integrity and RRC encryption keys to protect the RRCResume message and send to the UE on SRB1.

If the target gNB/ng-eNB does not support the received algorithms or if the target gNB/ng-eNB prefers to use different algorithms, the target gNB/ng-eNB shall send an RRCSetup message on SRB0 in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (fallback procedure) to the UE. Then the UE performs NAS based RRC recovery and negotiates a suitable algorithm with target gNB/ng-eNB via AS SMC procedure.

6.7.3.5 RNA Update procedure

If the source gNB/ng-eNB decides to relocate UE context to the target gNB/ng-eNB during an RNA Update procedure, the source gNB/ng-eNB shall include the UE 5G security capabilities and the ciphering and integrity algorithms the UE was using with the source cell in the <Xn-AP Retrieve UE Context Response> message. AS security algorithm selection is as described in clause 6.7.3.4.

6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM

UEs that are in limited service mode (LSM) and that cannot be authenticated by the AMF/SEAF (for whatever reason) may still be allowed to establish emergency session by sending the emergency registration request message. It shall be possible to configure whether the AMF allows unauthenticated UEs in LSM to establish bearers for emergency session or not. If an AMF allows unauthenticated UEs in LSM to establish bearers for an emergency session, then for the NAS protocol, the AMF shall use NIA0 and NEA0 as the integrity and ciphering algorithm respectively.

If the AMF allows an unauthenticated UE in LSM to establish bearers for emergency session after it has received the emergency registration request message from the UE, the AMF shall:

- Select NIA0 and NEA0, regardless of the supported algorithms announced previously by the UE as the NAS algorithms and signal this to the UE via the NAS security mode command procedure when activating the 5G NAS security context.
- Set the UE 5G security capabilities to only contain EIA0, EEA0, NIA0 and NEA0 when sending these to the gNB/ng-eNB in the following messages:
  - NGAP UE INITIAL CONTEXT SETUP
  - NGAP UE CONTEXT MODIFICATION REQUEST

- NGAP HANDOVER REQUEST

NOTE: As a result of that the AMF only sending a UE 5G security capability containing EIA0, EEA0, NIA0 and NEA0 to the gNB/ng-eNB , the gNB/ng-eNB is only able of selecting a null integrity protection for AS integrity protection and a null ciphering algorithm for AS confidentiality protection. That is, if NIA0 is used for NAS integrity protection, then NIA0 or EIA0 will always be used for AS integrity protection.

If NIA0 is disabled at the gNB for regulatory requirements and the gNB receives the UE 5G security capabilities to only contain NIA0 for integrity protection algorithms from the AMF in one of the above messages, the gNB shall reject the session.

The rules for when the AMF shall select NIA0 for NAS integrity protection, and when the UE shall accept a NAS security mode command selecting NIA0 for NAS integrity protection depends on whether the UE and AMF can be certain that no 5G NAS security context can be established. The rules for determining this is defined in clause 10 of this specification. If the AMF has selected NIA0 as the NAS integrity protection algorithm, the UE shall accept selection of NIA0 or EIA0 as the AS integrity protection algorithm. Selection of AS integrity protection algorithm happens via the AS security mode command procedure or via a handover command. The UE shall under no other circumstances accept selection of null integrity algorithm as the AS integrity protection algorithm.

6.7.4 AS security mode command procedure

The AS SMC procedure is for RRC and UP security algorithms negotiation and RRC security activation. for the gNB/ng-eNB. AS SMC procedure can be triggered to establish a secure RRC signalling-only connection during UE registration or PDU session establishment as specified in TS 38.413 [34] and TS 23.502 [8]. The activation of UP security is as described in clause 6.6.2. AS SMC procedure consists of a roundtrip of messages between gNB/ng-eNB and UE. The gNB/ng-eNB sends the AS security mode command to the UE and the UE replies with the AS security mode complete message. See Figure 6.7.4-1.

The AS security mode command message sent from gNB/ng-eNB to UE shall contain the selected RRC and UP encryption and integrity algorithms. This AS security mode command message shall be integrity protected with RRC integrity key based on the current K_{gNB}.

The AS security mode complete message from UE to gNB/ng-eNB shall be integrity protected with the selected RRC algorithm indicated in the AS security mode command message and RRC integrity key based on the current K_{gNB}.

RRC downlink ciphering (encryption) at the gNB/ng-eNB shall start after sending the AS security mode command message. RRC uplink deciphering (decryption) at the gNB/ng-eNB shall start after receiving and successful verification of the AS security mode complete message.

RRC uplink ciphering (encryption) at the UE shall start after sending the AS security mode complete message. RRC downlink deciphering (decryption) at the UE shall start after receiving and successful verification of the AS security mode command message.

If any control of the AS security mode command is not successful in the UE, the UE shall reply with an unprotected security mode failure message (see TS 38.331[22]).

Ciphering and integrity protection of UP downlink and uplink, at the UE and the gNB/ng-eNB, shall start as defined by clause 6.6.2.

AS SMC shall be used only during an initial context setup between the UE and the gNB/ng-eNB (i.e., to activate an initial K_{gNB} at RRC_IDLE to RRC_CONNECTED state transition).

NOTE: Derivation of a K_{gNB} at RRC_IDLE to RRC_CONNECTED state ensures that AS SMC establishes a fresh K_{gNB}. Consequently, the PDCP COUNTs can be reset.

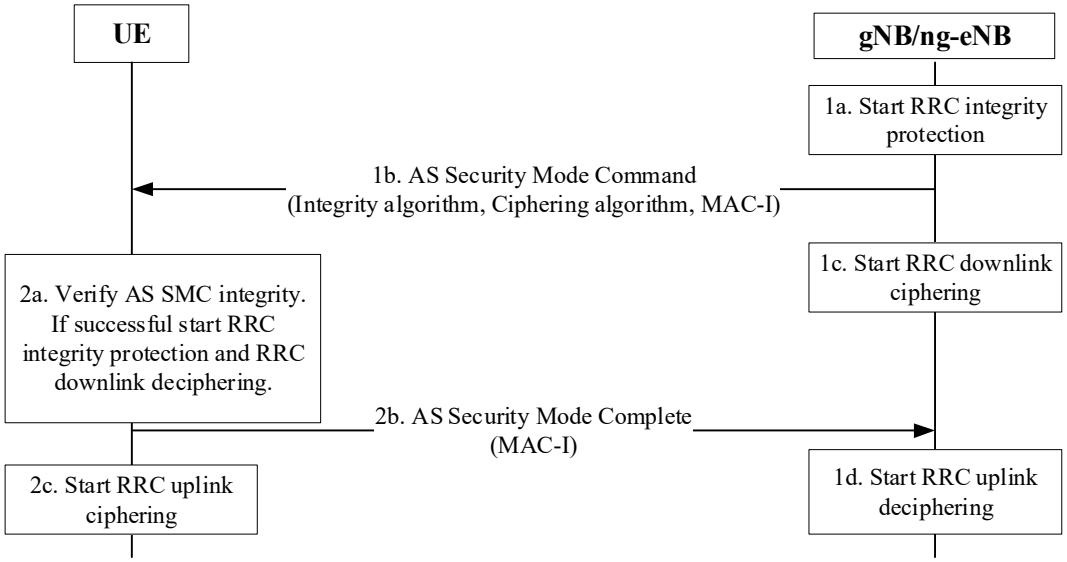


Figure 6.7.4-1: AS Security Mode Command Procedure

6.8 Security handling in state transitions

6.8.1 Key handling at connection and registration state transitions

6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states

6.8.1.1.0 General

One state machine in the UE and AMF is handling the registration states over 3GPP access and a second state machine is handling the registration states over non-3GPP access. This clause and its sub-clauses applies to both 3GPP access and non-3GPP access. UDM manages separate/independent UE Registration procedure for each access. The AMF shall associate Registration state per access type with the UE.

6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED

There are different reasons for transition to the RM-DEREGISTERED state. If a NAS messages leads to state transition to RM-DEREGISTERED, it shall be security protected by the current 5G NAS security context (mapped or native), if such exists in the UE or the AMF.

NOTE: The present document only considers the states RM-DEREGISTERED and RM REGISTERED and transitions between these two states. Other documents define additional RM states (see, e.g. 5GMM states in TS 24.501 [35]).

On transitioning to RM-DEREGISTERED, the UE and AMF shall do the following:

1. If they have a full non-current native 5G NAS security context and a current mapped 5G NAS security context, then they shall make the non-current native 5G NAS security context the current one.

2. They shall delete any mapped or partial 5G NAS security contexts they hold.

Handling of the remaining security parameters for each of these cases are given below:

1. Registration reject: All remaining security parameters shall be removed from the UE and AMF
2. Deregistration:
   a. UE-initiated
      i. If the reason is switch off then all the remaining security parameters shall be removed from the UE and AMF with the exception of the current native 5G NAS security context (as in clause 6.1.1), which should remain stored in the AMF and UE.
      ii. If the reason is not switch off then AMF and UE shall keep all the remaining security parameters.
   b. AMF-initiated
      i. Explicit: all the remaining security parameters shall be kept in the UE and AMF if the de-registration type is "re-registration required".
      ii. Implicit: all the remaining security parameters shall be kept in the UE and AMF.
   c. UDM/ARPF-initiated: If the message is "subscription withdrawn" then all the remaining security parameters shall be removed from the UE and AMF.
3. Registration reject: There are various reasons for Registration reject. The action to be taken shall be as given in TS 24.501 [35].

Storage of the full native 5G NAS security context including the pair(s) of distinct NAS COUNT values associated with each access together with respective NAS connection identifier, excluding the UE security capabilities and the keys K_{NASint} and K_{NASenc}, in the UE when the UE transitions to RM-DEREGISTERED state is done as follows:

a) If the ME does not have a full native 5G NAS security context in volatile memory, any existing native 5G NAS security context stored on the USIM or in non-volatile memory of the ME shall be marked as invalid.

b) If the USIM supports RM parameters storage, then the ME shall store the full native 5G NAS security context parameters on the USIM (except for K_{NASint} and K_{NASenc}), mark the native 5G NAS security context on the USIM as valid, and not keep any native 5G NAS security context in non-volatile ME memory.

c) If the USIM does not support RM parameters storage, then the ME shall store the full native 5G NAS security context (except for K_{NASint} and K_{NASenc}) in a non-volatile part of its memory and mark the native 5G NAS security context in its non-volatile memory as valid.

d) For the case that the AMF or the UE enter RM-DEREGISTERED state without using any of the above procedures, the handling of the remaining security parameters shall be as specified in TS 24.501 [35].

6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED

6.8.1.1.2.1 General

When starting the transition away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state, if no current 5G NAS security context is available in the ME, the ME shall retrieve native 5G NAS security context stored on the USIM if the USIM supports RM parameters storage and if the stored native 5G NAS security context on the USIM is marked as valid. If the USIM does not support RM parameters storage the ME shall retrieve stored native 5G NAS security context from its non-volatile memory if the native 5G NAS security context is marked as valid. The ME shall derive the K_{NASint} and K_{NASenc} from the K_{AMF} after retrieving the stored 5G NAS security context; see Annex A on NAS key derivation. The retrieved native 5G NAS security context with the derived K_{NASint} and K_{NASenc} shall then become the current 5G NAS security context.

When the ME is transitioning away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state, if the USIM supports RM parameters storage, the ME shall mark the stored 5G NAS security context on the USIM as invalid. If the USIM does not support RM parameters storage, the ME shall mark the stored 5G NAS security context in its non-volatile memory as invalid.

If the ME uses a 5G NAS security context to protect NAS messages, the distinct NAS COUNT values together with the NAS connection identifier associated with this access, are updated in the volatile memory of the ME. If the attempt to transition away from RM DEREGISTERED state with the intent to eventually transitioning to RM-REGISTERED state fails, the ME shall store the (possibly updated) 5G NAS security context including the distinct NAS COUNT values

together with the NAS connection identifier associated with this access, on the USIM or non-volatile ME memory and mark it as valid.

NOTE: The present document only considers the states RM-DEREGISTERED and RM REGISTERED and transitions between these two states. Other documents define additional RM states (see, e.g. 5GMM states in TS 24.501 [35]).

When the UE transits from RM-DEREGISTERED to RM-REGISTERED/CM-CONNECTED, there are two cases to consider, either a full native 5G NAS security context exists, or it does not.

6.8.1.1.2.2 Full native 5G NAS security context available

The UE shall transmit a NAS Registration Request message. This message is integrity protected using the distinct NAS COUNT values and the NAS connection identifier associated with this access. For the case that the 5G NAS security context used by the UE is non-current in the AMF, the AMF shall delete any existing current 5G security context and make the used 5G security context the current 5G security contex. Furthermore, provided that the NAS Registration Request was with "PDU session(s) to be re-activated" and there is no NAS SMC procedure before the AS SMC the NAS COUNT of the Registration Request message shall be used to derive the K_{gNB}/K_{eNB} with the KDF as specified in Annex A.

As a result of the NAS Registration Request with "PDU session(s) to be re-activated", the gNB/ng-eNB shall send an AS SMC to the UE to activate AS security. The K_{gNB}/K_{eNB} used, is derived in the current 5G NAS security context.

When the UE receives the AS SMC without having received a NAS Security Mode Command after the Registration Request with "PDU session(s) to be re-activated", it shall use the uplink NAS COUNT of the Registration Request message that triggered the AS SMC to be sent as freshness parameter in the derivation of the initial K_{gNB}/K_{eNB}. From this initial K_{gNB}/K_{eNB} the RRC protection keys and the UP protection keys shall be derived as described in sub-clause 6.2.3.1.

The same procedure for generating initial K_{gNB}/K_{eNB} can be used regardless of the fact if the UE is connecting to the same AMF to which it was connected previously or to a different AMF. In case UE connects to a different AMF and this AMF selects different NAS algorithms, the NAS keys have to be re-derived in the AMF with the new algorithm IDs as input using the KDF as specified in Annex A.

In addition, there is a need for the AMF to send a NAS SMC to the UE to indicate the change of NAS algorithms and to take the re-derived NAS keys into use. The UE shall assure that the NAS keys used to verify the integrity of the NAS SMC are derived using the algorithm ID specified in the NAS SMC. The NAS SMC Command and NAS SMC Complete messages are protected with the new NAS keys.

If there is a NAS Security Mode Command after the Registration Request with "PDU session(s) to be re-activated" but before the AS SMC, the UE and AMF use the uplink NAS COUNT of the most recent NAS Security Mode Complete and the related KAMF as the parameter in the derivation of the K_{gNB}/K_{eNB}. From this K_{gNB}/K_{eNB} the RRC protection keys and the UP protection keys are derived as described in sub-clause 6.2.3.1.

6.8.1.1.2.3 Full native 5G NAS security context not available

If in the process described in clause 6.8.1.1.2.2, there is no full native 5G NAS security context available in the AMF (i.e. either the UE has sent an unprotected Registration Request message or the UE has protected the Registration Request message with a current native 5G security context which no longer is stored in the AMF) a primary authentication run is required. If there is a full native 5G NAS security context available in the AMF, then the AMF may (according to AMF policy) decide to run a new primary authentication and a NAS SMC procedure (which activates the new 5G NAS security context based on the K_{AMF} derived during the primary authentication run) after the Registration Request.

If the Registration Request was with "PDU session(s) to be re-activated", the NAS SMC procedure is executed before the corresponding AS SMC. The NAS (uplink and downlink) COUNTs are set to start values, and the start value of the uplink NAS COUNT shall be used as freshness parameter in the K_{gNB}/K_{eNB} derivation from the fresh K_{AMF} (after primary authentication) when UE receives AS SMC the K_{gNB}/K_{eNB} is derived from the current 5G NAS security context, i.e., the fresh K_{AMF} is used to derive the K_{gNB}/K_{eNB}. The KDF as specified in clause Annex A shall be used to derive the K_{gNB}/K_{eNB}.

NOTE: Using the start value for the uplink NAS COUNT in this case cannot lead to the same combination of K_{AMF} and NAS COUNT being used twice. This is guaranteed by the fact that the first integrity protected NAS message the UE sends to the AMF after primary authentication is the NAS SMC complete message.

The NAS SMC complete message shall include the start value of the uplink NAS COUNT that is used as freshness parameter in the K_{gNB}/K_{eNB} derivation and the K_{AMF} is fresh. After a primary authentication, a NAS SMC needs to be sent from the AMF to the UE in order to take the new NAS keys into use. Both NAS SMC and NAS SMC Complete messages are protected with the new NAS keys.

6.8.1.1.2.4 UE registration over a second access type to the same AMF

It is assumed in this clause that the UE is already registered over a first access type (say access A). Clauses 6.8.1.1.2.1 and 6.8.1.1.2.2 applies as well when the UE attempts to register over a new access type (access B) to the same AMF with the following addition/exception:

Whenever the UE registers over a second access type (access B) to the same AMF, with the intention to transitioning from RM-DEREGISTERED to RM-REGISTERED state, then a full native 5G NAS security context is already available in the UE and the AMF. In this case, the UE shall directly take into use the available full 5G NAS security context and use it to protect the Registration Request over the second access using the distinct pair of NAS COUNTs for this second access type (access B).

The AMF may decide to run a new primary authentication as part of the Registration procedure on this second access (access B). If a new primary authentication is run, then the new derived partial 5G NAS security context needs to be taken into use on this second access (access B) with a NAS SMC using the distinct pair of NAS COUNTs for this second access. As the UE is already registered on the first access (access A), then the AMF needs to run a NAS SMC procedure on the first access in order to take the partial 5G NAS security context into use as described in clause 6.4.2.2.

If there is a need for the AMF to take a new partial 5G NAS security context into use, derived from primary authentication executed on the first access (access A), then the AMF needs to send a NAS SMC to the UE on the second access (access B) in order to take the new partial 5G NAS security context into use as described in clause 6.4.2.2.

6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states

6.8.1.2.0 General

One state machine in the UE and AMF is handling the connection states over 3GPP access and a second state machine is handling the connection states over non-3GPP access. This clause and its sub-clauses applies to both 3GPP access and non-3GPP access when not explicitly stated.

6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED

The UE sends an initial NAS message to initiate transition from CM-IDLE to CM-CONNECTED state (see TS 24.501 [35].

If a full native 5G NAS security context is already available in the UE and the AMF, then the UE shall directly take into use the available full 5G NAS security context and use it to protect the initial NAS message using the distinct pair of NAS COUNTs together with the NAS connection identifier for this access.

If the UE is simultaneously registered over both 3GPP access and non-3GPP access in the same AMF, then if there is a need for the AMF to take a new partial 5G NAS security context into use on this access (access A), derived from primary authentication executed on a different access, then the AMF needs to send a NAS SMC to the UE on this access (access A) in order to take the new partial 5G NAS security context also into use on this access as described in clause 6.4.2.2.

On transitions to CM-CONNECTED, the AMF should be able to check whether a new authentication is required, e.g. because of prior inter-provider handover.

If the UE is simultaneously registered over both 3GPP access and non-3GPP access in the same AMF, then if a new primary authentication is run, then the new derived partial 5G NAS security context needs to be taken into use on this access (access A) with a NAS SMC using the distinct pair of NAS COUNTs for this access. But the new derived partial 5G NAS security context also needs to be taken into use on the other accesses (access B) with a NAS SMC using the distinct pair of NAS COUNTs for the respective access as part of the NAS procedure as described in clause 6.4.2.2.

When cryptographic protection for radio bearers is established RRC protection keys and UP protection keys shall be generated as described in sub-clause 6.2.3.1 while K_{AMF} is assumed to be already available in the AMF.

The initial NAS message shall be integrity protected by the current 5G NAS security context if such exists using the distinct pair of NAS COUNTs together with the NAS connection identifier for this access. If no current 5G NAS security context exists the ME shall signal "no key available" in the initial NAS message.

K_{AMF} may have been established in the AMF as a result of a primary authentication run on this access or on a different access, or as a result of a 5G security context transfer from another AMF during N2 handover or idle mode mobility.

When the gNB/ng-eNB releases the RRC connection, the UE and the gNB/ng-eNB shall delete the keys they store such that state in the network for CM-IDLE state UEs will only be maintained in the AMF.

6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access

This sub-clause applies to establishment of keys for cryptographically protected radio bearers in 3GPP access only.

The procedure the UE uses to establish cryptographic protection for radio bearers is initiated by an NAS Service Request message or Registration Request message with "PDU session(s) to be re-activated" included from the UE to the AMF. The AMF may initiate the procedure to establish cryptographic protection for radio bearers when "PDU session(s) to be re-activated" is not included in the Registration request and but there is pending downlink UP data or pending downlink signalling.

Upon receipt of the NAS message, if the AMF does not require a NAS SMC procedure before initiating the NGAP procedure INITIAL CONTEXT SETUP, the AMF shall derive key K_{gNB}/K_{eNB} as specified in Annex A using the uplink NAS COUNT (see TS 24.501 [35]) corresponding to the NAS message that initiated transition from CM-IDLE to CM-CONNECTED state and the K_{AMF} of the current 5G NAS security context.

The AMF shall communicate the K_{gNB}/K_{eNB} to the serving gNB/ng-eNB in the NGAP procedure INITIAL CONTEXT SETUP. The UE shall derive the K_{gNB}/K_{eNB} from the K_{AMF} of the current 5G NAS security context using the NAS uplink COUNT corresponding to the NAS message that initiated transition from CM-IDLE to CM-CONNECTED state.

As a result of the NAS Service Request or Registration procedure, with "PDU session(s) to be re-activated" radio bearers are established, and the gNB/ng-eNB sends an AS SMC to the UE. When the UE receives the AS SMC without having received a NAS Security Mode Command, it shall use the NAS uplink COUNT corresponding to the NAS message that initiated transition from CM-IDLE to CM-CONNECTED state as freshness parameter in the derivation of the K_{gNB}/K_{eNB}. The KDF as specified in Annex A shall be used for the K_{gNB}/K_{eNB} derivation using the K_{AMF} of the current 5G NAS security context. From the K_{gNB}/K_{eNB} the RRC protection keys and the UP protection keys are derived by the UE and the gNB/ng-eNB as described in sub-clause 6.2.

If the NAS procedure establishing radio bearers contains a primary authentication run (which is optional), the NAS uplink and downlink COUNT for the new K_{AMF} shall be set to the start values (i.e. zero). If the NAS procedure establishing radio bearers contains a NAS SMC (which is optional), the value of the uplink NAS COUNT corresponding to the most recent NAS Security Mode Complete shall be used as freshness parameter in the K_{gNB}/K_{eNB} derivation from fresh K_{AMF} of the current 5G NAS security context when executing an AS SMC. The KDF as specified in Annex A shall be used for the K_{gNB}/K_{eNB} derivation also in this case.

The case that the UE is using Control Plane CIoT 5GS optimisation to send data over NAS and N3 bearers are established (due to either a request from the UE or decided by the AMF - see 5.31.4 of TS 23.501 [2]) works as follows. The UE and AMF shall always use the value of the uplink NAS COUNT from the Control Plane Service Request that was sent to transition the UE from idle to active as freshness parameter in the derivation of the K_{eNB} unless there has been a subsequent NAS Security Mode Complete. If there was a subsequent NAS Security Mode Complete, then the UE and AMF use the value of the uplink NAS COUNT from the latest NAS Security Mode Complete message as freshness parameter in the derivation of the K_{eNB}.

6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access

In the case of non-3GPP access, there are no individual radio bearers set up between the UE and N3IWF. For non-3GPP access, an IPsec tunnel is established between the UE and the interworking function N3IWF. The main SA is used solely for the transport of NAS messages between the UE and the AMF/SMF.

Corresponding to the PDU session of the UE, based on the policies and configuration, N3IWF determines the number of IPsec child SAs to be established and the QoS profiles associated with each IPsec child SA. For example, the N3IWF may decide to establish one IPsec child SA and associate all QoS profiles with this IPsec child SA. In this case, all QoS Flows of the PDU Session would be transferred over one IPsec child SA. N3IWF may also decide to establish different child SAs corresponding to the different QoS flows.

Corresponding to radio bearers in 3GPP access which are mapped to QoS values, for non-3GPPaccess there are only child SAs mapped to QoS values. Cryptographically each child SA is different with distinct key materials exchanged as per RFC 7296 [25].

6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE

On CM-CONNECTED to CM-IDLE transitions the gNB/ng-eNB does no longer need to store state information about the corresponding UE.

In particular, on CM-CONNECTED to CM-IDLE transitions:

- The gNB/ng-eNB and the UE shall release all radio bearers and delete the AS security context.
- AMF and the UE shall keep the 5G NAS security context stored.

6.8.1.3 Key handling for the Registration procedure when registered in NG-RAN

NOTE: This clause applies to both 3GPP access and non-3GPP access.

Before the UE can initiate the Registration procedure, the UE needs to transition to CM-CONNECTED state. The UE shall use the current 5G security context to protect the Registration Request and include the corresponding 5G-GUTI and ngKSI value. The Registration Request shall be integrity-protected, but not confidentiality-protected. UE shall use the current 5G security context algorithms to protect the Registration Request message. For the case that this security context is non-current in the AMF, the AMF shall delete any existing current 5G security context and make the used 5G NAS security context the current 5G security context.

If "PDU session(s) to be re-activated" is included in the Registration request message or if the AMF chooses to establish radio bearers when there is pending downlink UP data or pending downlink signalling, radio bearers will be established as part of the Registration procedure and a K_{gNB}/K_{eNB} will be derived. If there was no subsequent NAS SMC, the value of the uplink NAS COUNT, associated with the 3GPP access over which the Registration request message was sent from the UE to the AMF, is used as freshness parameter in the K_{gNB}/K_{eNB} derivation using the KDF as specified in clause Annex A.9.

In the case a primary authentication is run successfully, the uplink and downlink NAS COUNT shall be set to the start values (i.e. zero).

In the case source and target AMF use different NAS algorithms, the target AMF re-derives the NAS keys from K_{AMF} with the new algorithm identities as input and provides the new algorithm identifiers within a NAS SMC. The UE shall assure that the NAS keys used to verify the integrity of the NAS SMC are derived using the algorithm identity specified in the NAS SMC.

If there is a NAS Security Mode Command after the Registration Request over 3GPP access, the UE and AMF shall use the value of the uplink NAS COUNT associated with the 3GPP access of the most recent NAS Security Mode Complete and the related K_{AMF} as the parameter in the derivation of the K_{gNB}/K_{eNB}. From this K_{gNB}/K_{eNB} the RRC protection keys and the UP protection keys are derived as described in sub-clause 6.2.3.1.

In the case of Registration over non-3GPP access, the UE and AMF shall use the uplink NAS COUNT associated with the non-3GPP access of the most recent NAS Security Mode Complete and the related K_{AMF} as the parameter in the derivation of the K_{N3IWF}. IPsec SA is established between the UE and N3IWF using the K_{N3IWF} as described in sub-clause 7.2.1 of this document.

6.8.2 Security handling at RRC state transitions

6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states

6.8.2.1.1 General

In 5G, the RRC_INACTIVE state allows gNB/ng-eNB to suspend the UE's RRC connection while the gNB/ng-eNB and the UE continue to maintain the UE 5G AS security context. The UE RRC connection can be resumed at a later time by allowing the UE to transition into RRC__CONNECTED state. The UE may transition from RRC_INACTIVE state to RRC_CONNECTED state to the same last serving gNB/ng-eNB which sent the UE into RRC_INACTIVE state or to a different gNB/ng-eNB. While the UE is in RRC_INACTIVE state, the UE and last serving gNB/ng-eNB store the UE 5G AS security context which can be reactivated when the UE transitions from RRC_INACTIVE to RRC_CONNECTED. The gNB/ng-eNB and the UE shall behave as defined in following sub-clauses. The ng-eNB connected to 5GC shall also support the same security handling at RRC state transitions.

6.8.2.1.2 State transition from RRC_CONNECTED to RRC_INACTIVE

The gNB/ng-eNB shall send to the UE an RRCRelease with *suspendConfig* message that is ciphered and integrity protected in PDCP layer using a current AS security context. The gNB/ng-eNB shall include a fresh I-RNTI, and an NCC in that RRCRelease with *suspendConfig* message. The I-RNTI is used for context identification, and the UE ID part of the I-RNTI assigned by the gNB/ng-eNB shall be different in consecutive suspends of the same UE. This is to avoid tracking of UEs based on the I-RNTI. If the gNB/ng-eNB has a fresh and unused pair of {NCC, NH}, the gNB/ng-eNB shall include the NCC in the RRCRelease with *suspendConfig* message. Otherwise, the gNB/ng-eNB shall include the same NCC associated with the current K_{gNB} in the RRCRelease with *suspendConfig* message. The NCC is used for AS security.

The gNB/ng-eNB shall delete the current AS keys K_{RRCenc}, K_{UPenc} (if available), and K_{UPint} (if available) after sending the RRCRelease with *suspendConfig* message to the UE, but shall keep the current AS key K_{RRCint}. If the sent NCC value is fresh and belongs to an unused pair of {NCC, NH}, the gNB/ng-eNB shall save the pair of {NCC, NH} in the current UE AS security context and shall delete the current AS key K_{gNB}. If the sent NCC value is equal to the NCC value associated with the current K_{gNB}, the gNB/ng-eNB shall keep the current AS key K_{gNB} and NCC. The gNB/ng-eNB shall store the sent I-RNTI together with the current UE context including the remainder of the AS security context.

Upon receiving the RRC Release with *suspendConfig* message from the gNB/ng-eNB, the UE shall verify that the integrity of the received RRCRelease with *suspendConfig* message is correct by checking the PDCP MAC-I. If this verification is successful, then the UE shall take the received NCC value and save it as stored NCC with the current UE context. The UE shall delete the current AS keys K_{RRCenc}, K_{UPenc} (if available), and K_{UPint} (if available), but keep the current AS key K_{RRCint} key. If the stored NCC value is different from the NCC value associated with the current K_{gNB}, the UE shall delete the current AS key K_{gNB}. If the stored NCC is equal to the NCC value associated with the current K_{gNB}, the UE shall keep the current AS key K_{gNB}. The UE shall store the received I-RNTI together with the current UE context including the remainder of the AS security context, for the next state transition.

6.8.2.1.3 State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB

When the UE decides to resume the RRC connection to transit from RRC_INACTIVE to RRC_CONNECTED, the UE sends RRCResumeRequest message on SRB0 and hence it is not integrity protected. However, the RRCResumeRequest message shall include the I-RNTI and a ResumeMAC-I/shortResumeMAC-I. The I-RNTI (short or full I-RNTI) is used for context identification and its value shall be the same as the I-RNTI that the UE had received from the source gNB/ng-eNB in the RRCRelease with *suspendConfig* message. The ResumeMAC-I/shortResumeMAC-I is a 16-bit message authentication token, the UE shall calculate it using the integrity algorithm (NIA or EIA) in the stored AS security context, which was negotiated between the UE and the source gNB/ng-eNB and the current K_{RRCint} with the following inputs:

- KEY : it shall be set to current K_{RRCint};
- BEARER : all its bits shall be set to 1.
- DIRECTION : its bit shall be set to 1;

- COUNT : all its bits shall be set to 1;
- MESSAGE : it shall be set to VarResumeMAC-Input/VarShortInactiveMAC-Input as defined in TS 38.331 [22] for gNB and in TS 36.331 [69] for ng-eNB with following inputs:

  source PCI, target Cell-ID, source C-RNTI.

For protection of all RRC messages except RRCReject message following the sent RRCResumeRequest message, the UE shall derive a $K_{NG\text{-}RAN}$* using the target PCI, target ARFCN-DL/EARFCN-DL and the K_{gNB}/NH based on either a horizontal key derivation or a vertical key derivation as defined in clause 6.9.2.1.1 and Annex A.11/Annex A.12. The UE shall further derive K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived $K_{NG\text{-}RAN}$*.

When the target gNB/ng-eNB receives the RRCResumeRequest message from the UE, the target gNB/ng-eNB extracts the I-RNTI from the RRCResumeRequest message. The target gNB/ng-eNB contacts the source gNB/ng-eNB based on the information in the I-RNTI by sending an Xn-AP Retrieve UE Context Request message with the following included: I-RNTI, the ResumeMAC-I/shortResumeMAC-I and target Cell-ID, in order to allow the source gNB/ng-eNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.

The source gNB/ng-eNB retrieves the stored UE context including the UE 5G AS security context from its database using the I-RNTI. The source gNB/ng-eNB verifies the ResumeMAC-I/shortResumeMAC-I using the current K_{RRCint} key stored in the retrieved UE 5G AS security context (calculating the ResumeMAC-I/shortResumeMAC-I in the same way as described above). If the verification of the ResumeMAC-I/shortResumeMAC-I is successful, then the source gNB/ng-eNB calculates $K_{NG\text{-}RAN}$* using the target cell PCI, target ARFCN-DL/EARFCN-DL and the K_{gNB}/NH in the current UE 5G AS security context based on either a horizontal key derivation or a vertical key derivation according to whether the source gNB/ng-eNB has an unused pair of {NCC, NH} as described in Annex A.11/Annex A.12. The source gNB/ng-eNB can obtain the target PCI and target ARFCN-DL/EARFCN-DL from a cell configuration database by means of the target Cell-ID which was received from the target gNB/ng-eNB. Then the source gNB/ng-eNB shall respond with an Xn-AP Retrieve UE Context Response message to the target gNB/ng-eNB including the UE context that contains the UE 5G AS security context. The UE 5G AS security context sent to the target gNB/ng-eNB shall include the newly derived $K_{NG\text{-}RAN}$*, the NCC associated to the $K_{NG\text{-}RAN}$*, the UE 5G security capabilities, UP security policy, the UP security activation status with the corresponding PDU session ID(s), and the ciphering and integrity algorithms used by the UE with the source cell.

The target gNB/ng-eNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target gNB/ng-eNB does not support the ciphering and integrity algorithms used in the last source cell or if the target gNB/ng-eNB prefers to use different algorithms than the source gNB/ng-eNB, then the target gNB/ng-eNB shall send an RRC Setup/RRCSetup message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (i.e., a fallback procedure).

If the target gNB/ng-eNB supports the ciphering and integrity algorithms used with the last source cell and these algorithms are the chosen algorithms by the target gNB/ng-eNB, the target gNB/ng-eNB shall derive new AS keys (RRC integrity key, RRC encryption key and UP keys) using the algorithms the UE used with the source cell and the received $K_{NG\text{-}RAN}$*. The target gNB/ng-eNB shall reset all PDCP COUNTs to 0 and activate the new keys in PDCP layer. The target gNB/ng-eNB shall respond to the UE with an RRC Resume message on SRB1 which is integrity protected and ciphered in PDCP layer using the new RRC keys.

If the UP security activation status can be supported in the target gNB/ng-eNB, the target gNB/ng-eNB shall use the UP security activations that the UE used at the last source cell. Otherwise, the target gNB/ng-eNB shall respond with an RRC Setup message to establish a new RRC connection with the UE.

When the UE receives the RRCResume message, the UE shall decrypt the message using the K_{RRCenc} that was derived based on the newly derived $K_{NG\text{-}RAN}$*. The UE shall also verify the <RRC Connection Resume> message by verifying the PDCP MAC-I using the K_{RRCint} that was derived from the newly derived $K_{NG\text{-}RAN}$* If verification of the RRCResume message is successful, the UE shall delete the current K_{RRCint} key and the UE shall save the K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived $K_{NG\text{-}RAN}$* as part of the UE current AS security context. In this case, the UE shall send the RRCResumeComplete message both integrity protected and ciphered to the target gNB/ng-eNB on SRB1 using the current K_{RRCint} and K_{RRCenc}. The UE shall use the UP security activations that were used before tansition to the RRC Inactive.

If the UE receives RRCReject message from the target gNB/ng-eNB in response to the UE <RRC Resume Request> message, the UE shall delete newly derived AS keys used for connection resumption attempt, including newly derived

$K_{NG\text{-}RAN}$*, newly derivedRRC integrity key, RRC encryption key and UP keys, and keep the current K_{RRCint} and the K_{gNB}/NH in its current AS context.

Security is fully resumed on UE side after reception and processing of RRCResume message. The UE can receive data on DRB(s) after having received and processed RRC connection resume message. UL data on DRB(s) can be sent after RRCResumeComplete message has been successfully sent.

After a successful transition from RRC_INACTIVE to RRC_CONNECTED the target gNB/ng-eNB shall perform Path Switch procedure with the AMF. The AMF shall verify the UE security capability as described in the clause 6.7.3.1, and the SMF shall veirfy the UE security policy as described in the clause 6.6.1.

6.8.2.1.4 State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB

The target gNB/ng-eNB may be the same as the source gNB/ng-eNB in the description in the previous subclause. If so, the single gNB/ng-eNB performs the roles of both the source and target gNB/ng-eNB.

6.8.2.2 Key handling during mobility in RRC_INACTIVE state

6.8.2.2.1 General

The purpose of this procedure is to allow the UE to notify the network if it moves out of the configured RNA (RAN-based Notification Area) or if UE initiates a periodic RAN-based notification area update procedure. The UE and gNB store the AS security context in RRC_INACTIVE state and reactivate the AS security context when the UE initiates the RAN-based Notification Area Update (RNAU) procedure. The ng-eNB connected to 5GC shall also support the same key handling during mobility in RRC_INACTIVE.

6.8.2.2.2 RAN-based notification area update to a new gNB/ng-eNB

When the UE decides to initiate the RANU procedure the UE may initiate the procedure with a new gNB/ng-eNB. In this case, the UE, the target gNB/ng-eNB and the source gNB/ng-eNB follow the detailed procedure as described in clause 6.8.2.1.3 with the following deviations:

The target gNB/ng-eNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target gNB/ng-eNB does not support the ciphering and integrity algorithms used in the last source cell or if the target gNB/ng-eNB prefers to use different algorithms than the source gNB/ng-eNB, then the target gNB/ng-eNB shall send an RRCSetup message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (i.e., fallback procedure).

If the target gNB/ng-eNB selects the ciphering and integrity protection algorithms which the UE used with the last source cell and the target gNB/ng-eNB decides to send the UE directly back to RRC_INACTIVE state without bringing the UE to RRC_CONNECTED state, the target gNB/ng-eNB shall perform a Path Switch procedure with the AMF to get a fresh {NCC, NH} pair before sending the RRCRelease message to the UE. After the target gNB/ng-eNB receives a fresh {NCC, NH} pair in the Path Switch Acknowledgement message from the AMF, the target gNB/ng-eNB shall set the value of NCC in the RRCRelease message to the NCC value of the received fresh {NCC, NH} pair.

After the source gNB/ng-eNB (old gNB/ng-eNB) validates the ResumeMAC-I/shortResumeMAC-I received from the target gNB/ng-eNB (new gNB/ng-eNB) in the RETRIEVE UE CONTEXT REQUEST message, the old gNB/ng-eNB may decide not to relocate the UE context to the new gNB/ng-eNB. In this case, the old gNB/ng-eNB builds the RRCRelease message (MSG4) with a fresh I-RNTI, integrity protect it and encrypt it using the RRC keys that were derived from the new K_{gNB}* similar to RRCResume message (MSG4) protection as specified in clause 6.8.2.1.3. Then, the old gNB/ng-eNB sends the integrity protected and encrypted RRCRelease message to the new gNB/ng-eNB in the RETRIEVE UE CONTEXT FAILURE message.

6.8.2.2.3 RAN-based notification area update to the same gNB/ng-eNB

When the UE decides to initiate a periodic RNAU procedure, the target gNB/ng-eNB may be the same as the source gNB/ng-eNB. If so the single gNB/ng-eNB (same gNB/ng-eNB) performs the roles of both the source gNB/ng-eNB and the target gNB/ng-eNB.

6.9 Security handling in mobility

6.9.1 Void

6.9.2 Key handling in handover

6.9.2.1 General

6.9.2.1.1 Access stratum

The general principle of key handling for $K_{NG\text{-}RAN}$*/NH at handovers is depicted in Figure 6.9.2.1.1-1.

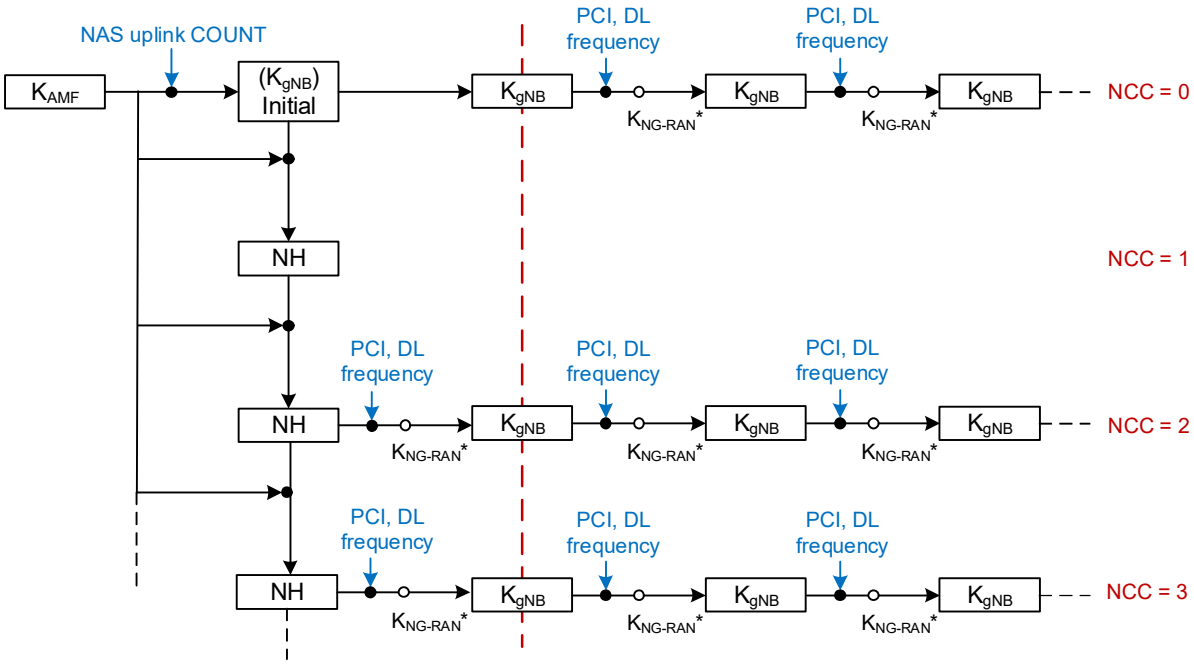


Figure 6.9.2.1.1-1: Model for the handover key chaining

The following is an outline of the key handling model to clarify the intended structure of the key derivations. The detailed specification is provided in sub-clauses 6.9.2.2 and 6.9.2.3.

Whenever an initial AS security context needs to be established between UE and gNB/ng-eNB, AMF and the UE shall derive a K_{gNB} and a Next Hop parameter (NH). The K_{gNB} and the NH are derived from the K_{AMF}. A NH Chaining Counter (NCC) is associated with each K_{gNB} and NH parameter. Every K_{gNB} is associated with the NCC corresponding to the NH value from which it was derived. At initial setup, the K_{gNB} is derived directly from K_{AMF}, and is then considered to be associated with a virtual NH parameter with NCC value equal to zero. At initial setup, the derived NH value is associated with the NCC value one.

NOTE 1: At the UE, the NH derivation associated with NCC=1 could be delayed until the first handover performing vertical key derivation.

NOTE 1a: In N2 handover, when the K_{gNB} is updated either due to K_{AMF} change or synchronising the AS security context with the NAS security context, the K_{gNB} is derived as specified in clauses 6.9.2.3.3 and 6.9.2.3.4 of the present document. In inter-RAT handover, the K_{gNB} is derived as specified in clause 8.4 of the present document. In UE context modification, the K_{gNB} is derived as specified in clause 6.9.2.2.

Whether the AMF sends the K_{gNB} key or the {NH, NCC} pair to the serving gNB/ng-eNB is described in detail in sub-clauses 6.9.2.2 and 6.9.2.3. The AMF shall not send the NH value to gNB/ng-eNB at the initial connection setup. The gNB/ng-eNB shall initialize the NCC value to zero after receiving NGAP Initial Context Setup Request message.

NOTE 2: Since the AMF does not send the NH value to gNB/ng-eNB at the initial connection setup, the NH value associated with the NCC value one cannot be used in the next Xn handover or the next intra-gNB/intra-ng-eNB-CU handover, for the next Xn handover or the next intra-gNB-CU/intra-ng-eNB handover the horizontal key derivation (see Figure 6.9.2.1.1-1) will apply.

NOTE 3: One of the rules specified for the AMF in sub-clause 6.9.2.3.3 of the present document states that the AMF always computes a fresh {NH, NCC} pair that is given to the target gNB/ng-eNB. An implication of this is that the first {NH, NCC} pair will never be used to derive a K_{gNB}. It only serves as an initial value for the NH chain.

The UE and the gNB/ng-eNB use the K_{gNB} to secure the communication between each other. On handovers and at transitions from RRC_INACTIVE to RRC_CONNECTED states (defined in clause 6.8.2.1), the basis for the K_{gNB} that will be used between the UE and the target gNB/ng-eNB, called $K_{NG\text{-}RAN}$*, is derived from either the currently active K_{gNB} or from the NH parameter. If $K_{NG\text{-}RAN}$* is derived from the currently active K_{gNB} this is referred to as a horizontal key derivation (see Figure 6.9.2.1.1-1) and if the $K_{NG\text{-}RAN}$* is derived from the NH parameter the derivation is referred to as a vertical key derivation (see Figure 6.9.2.1.1-1).

As NH parameters are only computable by the UE and the AMF, it is arranged so that NH parameters are provided to gNB/ng-eNBs from the AMF in such a way that forward security can be achieved.

On handovers with vertical key derivation the NH is further bound to the target PCI and its frequency ARFCN-DL before it is taken into use as the K_{gNB} in the target gNB/ng-eNB. On handovers with horizontal key derivation the currently active K_{gNB} is further bound to the target PCI and its frequency ARFCN-DL before it is taken into use as the K_{gNB} in the target gNB/ng-eNB.

6.9.2.1.2 Non access stratum

During mobility, NAS aspects that need to be considered are the possible K_{AMF} change, the possible NAS algorithm change at AMF change, and the possible presence of a parallel NAS connection. There is the possibility that the source AMF and the target AMF do not support the same set of NAS algorithms or have different priorities regarding the use of NAS algorithms. In this case, the target AMF re-derives the NAS keys from the existing K_{AMF} (if unchanged) or derives the NAS keys from the new K_{AMF} (if changed) using the NAS algorithm identities and NAS algorithm types as input to the NAS key derivation functions (see Annex A.8). When the K_{AMF} has not changed, all inputs, in particular the K_{AMF}, will be the same in the re-derivation except for the NAS algorithm identity. When the K_{AMF} has changed, new NAS keys are derived irrespective of change in NAS algorithms.

In case the K_{AMF} has changed or the target AMF decides to use NAS algorithms different from the ones used by the source AMF, the target AMF shall provide needed parameters to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC).

NOTE 1: It is per operator's policy how to configure selection of handover types. Depending on an operator's security requirements, the operator can decide whether to have Xn or N2 handovers for a particular gNB/ng-eNB according to the security characteristics of a particular gNB/ng-eNB.

NOTE 2: Following key change indicators are involved with N2 handovers. 1) Source AMF indicates AS key re-keying required meaning that the K_{AMF} sent by source AMF to the target AMF is not in sync with current gNB/ng-eNB with keyAmfChangeInd (K_{AMF} Change Indicator). 2) Source AMF indicates that the K_{AMF} sent by source AMF to target AMF has been calculated using horizontal K_{AMF} derivation with keyAmfHDerivationInd (K_{AMF} Horizontal Derivation Indicator). 3) The target AMF indicates a horizontal K_{AMF} derivation to the UE with K_AMF_change_flag in the NAS Container to tell the NAS layer of the UE to change K_{AMF}. 4). The target AMF indicates anAS key re-keying to the gNB/ng-eNB with NSCI (New Security Context Indicator). 5) The gNB/ng-eNB indicates a AS re-keying to the UE with *keySetChangeIndicator* so that the AS layer of the UE knows that new K_{gNB} needs to be derived from new K_{AMF} instead of NH, and NCC needs to be reset to zero.

6.9.2.2 Key derivations for context modification procedure

As outlined in clause 6.9.2.1, whenever a fresh K_{gNB} is calculated from the K_{AMF}, the AMF shall transfer the K_{gNB} to the serving ng-eNB/gNB in a message modifying the security context in the ng-eNB/gNB. The AMF and the UE shall compute the fresh K_{gNB} as defined in Annex A.9 according to the rules in clause 6.9.6.4. An NCC value 0 is associated with the fresh K_{gNB}. From the fresh K_{gNB}, the ng-eNB/gNB and the UE shall compute the $K_{NG\text{-}RAN}$* as described in Annex A.11 and A.12 and then use the computed $K_{NG\text{-}RAN}$* as the K_{gNB}/K_{eNB} as described in clause 6.9.4.4.

NOTE 1: Unlike EPS, in 5GS the NAS and the AS security contexts are synchronized as a part of handover procedure, if a handover is occurring. See sub-clauses under the clause 6.9.2.3 (key derivations during handover) of the present document.

6.9.2.3 Key derivations during handover

6.9.2.3.1 Intra-gNB-CU handover and intra-ng-eNB handover

The gNB shall have a policy deciding at which intra-gNB -CU handovers the K_{gNB} can be retained and at which a new K_{gNB} needs to be derived. At an intra-gNB-CU handover, the gNB shall indicate to the UE whether to change or retain the current K_{gNB} in the HO Command message. Retaining the current K_{gNB} shall only be done during intra-gNB-CU handover.

NOTE: The option of retaining the K_{eNB} at intra-ng-eNB handover is not supported in ng-eNB.

If the current K_{gNB} is to be changed, the gNB/ng-eNB and the UE shall derive a $K_{NG\text{-}RAN}$* as in Annex A.11/A.12 using target PCI, its frequency ARFCN-DL/EARFCN-DL, and either NH or the current K_{gNB} depending on the following criteria: the gNB shall use the NH for deriving $K_{NG\text{-}RAN}$* if an unused {NH, NCC} pair is available in the gNB (this is referred to as a vertical key derivation), otherwise if no unused {NH, NCC} pair is available in the gNB, the gNB shall derive $K_{NG\text{-}RAN}$* from the current K_{gNB} (this is referred to as a horizontal key derivation). The gNB shall send the NCC used for the $K_{NG\text{-}RAN}$*derivation to UE in HO Command message. The gNB/ng-eNB and the UE shall use the $K_{NG\text{-}RAN}$* as the K_{gNB}, after handover.

If the current K_{gNB} is to be retained, the gNB and the UE shall continue using the current K_{gNB}, after handover.

NOTE 1: This clause is also applicable when gNB is implemented as a single unit, i.e., when the gNB is not split into CU and DU.

NOTE 2: The key derivation mechanism described in this clause is also applicable to CHO defined in TS 38.300[52].

6.9.2.3.2 Xn-handover

In Xn handovers the source gNB/ng-eNB shall perform a vertical key derivation in case it has an unused {NH, NCC} pair. The source gNB/ng-eNB shall first compute $K_{NG\text{-}RAN}$* from target PCI, its frequency ARFCN-DL/EARFCN-DL, and either from currently active K_{gNB} in case of horizontal key derivation or from the NH in case of vertical key derivation as described in Annex A.11/A.12.

Next, the source gNB/ng-eNB shall forward the { $K_{NG\text{-}RAN}$*, NCC} pair to the target gNB/ng-eNB. The target gNB/ng-eNB shall use the received $K_{NG\text{-}RAN}$* directly as K_{gNB} to be used with the UE. The target gNB/ng-eNB shall associate the NCC value received from source gNB/ng-eNB with the K_{gNB}. The target gNB/ng-eNB shall include the received NCC into the prepared HO Command message, which is sent back to the source gNB/ng-eNB in a transparent container and forwarded to the UE by source gNB/ng-eNB.

When the target gNB/ng-eNB has completed the handover signalling with the UE, it shall send a NGAP PATH SWITCH REQUEST message to the AMF. Upon reception of the NGAP PATH SWITCH REQUEST, the AMF shall increase its locally kept NCC value by one and compute a new fresh NH from its stored data using the function defined in Annex A.10. The AMF shall use the K_{AMF} from the currently active 5G NAS security context for the computation of the new fresh NH. The AMF shall then send the newly computed {NH, NCC} pair to the target gNB/ng-eNB in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The target gNB/ng-eNB shall store the received {NH, NCC} pair for further handovers and remove other existing unused stored {NH, NCC} pairs if any.

If the AMF had activated a new 5G NAS security context with a new K_{AMF}, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet successfully performed a UE Context Modification procedure, the sent NGAP PATH SWITCH REQUEST ACKNOWLEDGE message shall in addition contain a NSCI (New Security Context Indicator). The AMF shall in this case derive a new initial K_{gNB} from the new K_{AMF} and the uplink NAS COUNT in the most recent NAS Security Mode Complete message as specified in Annex A.9. The AMF shall associate the derived new initial K_{gNB} with a new NCC value equal to zero. Then, the AMF shall use {the derived new initial K_{gNB}, the new NCC value initialized to zero} pair as the newly computed {NH, NCC} pair to be sent in the NGAP PATH SWITCH REQUEST ACKNOWLEDGE message. The gNB/ng-eNB shall in this case set the value of *keySetChangeIndicator* field to true in further handovers. The gNB/ng-eNB should in this case perform an intra-gNB-CU/intra-ng-eNB handover immediately .

NOTE 1: Because the NGAP PATH SWITCH REQUEST message is transmitted after the radio link handover, it can only be used to provide keying material for the next handover procedure. Thus, for Xn-handovers key separation happens only after two hops because the source gNB/ng-eNB knows the target gNB/ng-eNB keys. The target gNB/ng-eNB can immediately initiate an intra-gNB-CU/intra-ng-eNB handover to take the new NH into use once the new NH has arrived in the PATH SWITCH REQUEST ACKNOWLEDGE message.

NOTE 2: The key derivation mechanism described in this clause is also applicable to CHO defined in TS 38.300[52].

6.9.2.3.3 N2-Handover

Upon reception of the NGAP HANDOVER REQUIRED message, if the source AMF does not change the active K_{AMF} (meaning no horizontal K_{AMF} derivation) and if AS key re-keying is not required, the source AMF shall increment its locally kept NCC value by one and compute a fresh NH from its stored data using the function defined in Annex A.10. The source AMF shall use the K_{AMF} from the currently active 5GS NAS security context for the computation of the fresh NH. The source AMF shall send the fresh {NH, NCC} pair to the target AMF in the Namf_Communication_CreateUEContext Request message. The Namf_Communication_CreateUEContext Request message shall in addition contain the K_{AMF} that was used to compute the fresh {NH, NCC} pair and its corresponding ngKSI and corresponding uplink and downlink NAS COUNTs.

If the source AMF had activated a new 5G NAS security context with a new K_{AMF}, different from the 5G NAS security context on which the currently active 5G AS security context is based, but has not yet performed a UE Context Modification procedure, the Namf_Communication_CreateUEContext Request message shall in addition contain an indication that the K_{AMF} sent by source AMF to target AMF is not in sync with the current K_{gNB} used between the UE and the source gNB (i.e., keyAmfChangeInd) which means that AS key re-keying is required at the UE. Further, the source AMF shall derive a new K_{gNB} associated with NCC=0 using the new K_{AMF} and the uplink NAS COUNT from the last successful NAS SMC procedure with the UE and provide the {NH= newly derived K_{gNB}, NCC=0} pair to the target AMF in the Namf_Communication_CreateUEContext Request message.

The source AMF uses its local policy to determine whether to perform horizontal K_{AMF} derivation on currently active K_{AMF}. If horizontal K_{AMF} derivation is performed, the Namf_Communication_CreateUEContext Request shall contain an indication (i.e., keyAmfHDerivationInd) that the new K_{AMF} has been calculated, an indication (i.e., keyAmfChangeInd) that AS key re-keying is required at the UE, and the downlink NAS COUNT used in the horizontal derivation of the sent K_{AMF}. The ngKSI for the newly derived K_{AMF} key has the same value and the same type as the ngKSI of the current K_{AMF}. Further, the source AMF shall derive a new K_{gNB} associated with NCC=0 using the newly derived K_{AMF} and the uplink NAS COUNT value of 2^{32}-1 as defined in Annex A.9. The source AMF shall include the{NH=newly derived K_{gNB}, NCC=0} pair and the ngKSI for the newly derived K_{AMF} key in the Namf_Communication_CreateUEContext Request as well.

NOTE a: The uplink NAS COUNT value for the initial K_{gNB} derivation is set to 2^{32}-1. The reason for choosing such a value is to avoid any possibility that the value may be used to derive the same K_{gNB} again.

The source AMF shall always increment the downlink NAS COUNT by one after sending the Namf_Communication_CreateUEContext Request message to the target AMF.

Unlike the S10 FORWARD RELOCATION REQUEST message in EPS, the Namf_Communication_CreateUEContext Request message in 5G shall not contain data and meta-data related to old 5G security context.

NOTE 1: Void.

If the target AMF receives the indication of horizontal K_{AMF} derivation (i.e., keyAmfHDerivationInd), it shall derive the NAS keys from the received K_{AMF} as specified in clause A.8 and set the NAS COUNTs to zero. The target AMF shall create a NASC (NAS Container) containing the K_AMF_change_flag, the received downlink NAS COUNT, ngKSI, selected NAS security algorithms, and NAS MAC. The K_AMF_change_flag is set to one when the target AMF receives keyAmfHDerivationInd_. Otherwise, the K_AMF_change_flag is set to zero. If the target AMF does not receive keyAmfHDerivationInd but wants to change the NAS algorithms, it shall create a NASC using the selected NAS security algorithms in the same manner as the case for the horizontal K_{AMF} derivation. However, the target AMF shall not set the NAS COUNTs to zero.

The target AMF shall calculate a 32-bit NAS MAC over the parameters included in the NASC using the K_{NASint} key. The input parameters to the NAS 128-bit integrity algorithms as described in Annex D.3 shall be set as follows when calculating NAS MAC.

The calculation of NAS MAC shall be the 32-bit output of the selected NIA and shall use the following inputs:

- KEY : it shall be set to the corresponding K_{NASint};
- COUNT : it shall be set to 2^{32}-1;
- MESSAGE : it shall be set to the content of NAS Container as defined in TS 24.501 [35];
- DIRECTION : its bit shall be set to 1; and
- BEARER : it shall be set to the value of the NAS connection identifier for 3GPP access.

The use of the 2^{32}-1 as the value of the COUNT for the purpose of NAS MAC calculation/verification does not actually set the NAS COUNT to 2^{32}-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 2^{24}-1] is to avoid any possibility that the value may be reused for normal NAS messages.

Replay protection is achieved by the UE checking if the downlink NAS COUNT included in the NAS Container is replayed or not. The UE shall not accept the same downlink NAS COUNT value twice before a newly derived K_{AMF} is taken into use and the corresponding downlink NAS COUNT is set to zero. The target AMF shall increment the downlink NAS COUNT by one after creating a NASC.

The NASC is included in the NGAP HANDOVER REQUEST message to the target ng-eNB/gNB. The purpose of this NASC could be compared to a NAS SMC message. If the target AMF receives the keyAmfChangeInd, it shall further send the received {NCC, NH} pair and the New Security Context Indicator (NSCI) to the target ng-eNB/gNB within the NGAP HANDOVER REQUEST message. The target AMF shall further set the NCC to one and shall further compute a NH as specified in Annex A.10. The target AMF shall further store the {NCC=1, NH} pair.

NOTE 1a: VoidNOTE 2: The NAS Container (NASC) is defined as Intra N1 mode NAS transparent container in TS 24.501 [35].

NOTE 3: The downlink NAS COUNT is always included in the Namf_Communication_CreateUEContext Request and used by the target AMF for NAS MAC computation. This provides replay protection for NASC.

If the target AMF does not receive the keyAmfChangeInd, it shall store locally the K_{AMF} and {NH, NCC} pair received from the source AMF and then send the received {NH, NCC} pair to the target ng-eNB/gNB within the NGAP HANDOVER REQUEST message.

Upon receipt of the NGAP HANDOVER REQUEST message from the target AMF, the target ng-eNB/gNB shall compute the $K_{NG\text{-}RAN}$* to be used with the UE by performing the key derivation defined in Annex A.11 and A.12 with the {NH, NCC} pair received in the NGAP HANDOVER REQUEST message and the target PCI and its frequency ARFCN-DL/EARFCN-DL. The gNB uses the $K_{NG\text{-}RAN}$* corresponding to the selected cell as K_{gNB}. The ng-eNB uses the $K_{NG\text{-}RAN}$* corresponding to the selected cell as K_{eNB}. The target ng-eNB/gNB shall associate the NCC value received from AMF with the K_{gNB}/K_{eNB}. The target ng-eNB/gNB shall include the NCC value from the received {NH, NCC} pair, and the NASC if such was also received, into the HO Command message to the UE and remove any existing unused stored {NH, NCC} pairs. If the target ng-eNB/gNB had received the NSCI, it shall set the *keySetChangeIndicator* field in the HO Command message to true.

NOTE 4: The source AMF may be the same as the target AMF in the description in this sub-clause. If so the single AMF performs the roles of both the source and target AMF. In this case, actions related to N14 messages are handled internally in the single AMF.

6.9.2.3.4 UE handling

The UE behaviour is the same regardless if the handover is intra-gNB-CU, intra ng-eNB, Xn, or N2 with the exception that during intra-gNB-CU handover, the UE may retain the same key based on an indication from the gNB. The UE behaviour is also same in case of conditional handover, as specified in TS 38.300 [52], i.e., the UE shall use the parameters of the selected target cell in $K_{NG\text{-}RAN}$* derivations.

If the UE also receives a NASC (NAS Container) in the HO Command message, the UE shall update its NAS security context as follows:

NOTE 1: The purpose of this NASC could be compared to a NAS SMC message.

- The UE shall verify the freshness of the downlink NAS COUNT in the NASC.

- If the NASC indicates a new K_{AMF} has been calculated (i.e., K_AMF_change_flag is one),
  - The UE shall compute the horizontally derived K_{AMF} using the K_{AMF} from the current 5G NAS security context identified by the ngKSI included in the NASC and the downlink NAS COUNT in the NASC, as specified in Annex A.13.
  - The UE shall assign the ngKSI included in the NASC to the ngKSI of the new derived K_{AMF}. The UE shall further configure NAS security based on the horizontally derived K_{AMF} and the selected NAS security algorithms in the NASC.
  - The UE shall further verify the NAS MAC in the NASC as described in Clause 6.9.2.3.3 and if the verification is successful, the UE shall further set the NAS COUNTs to zero.
- If K_{AMF} change is not indicated,
  - If the verification is successful, the UE shall configure the NAS security based on the parameters included in the NASC but shall not set the NAS COUNTs to zero.
  - The UE shall verify the NAS MAC in the NASC.
  - The UE shall further set the downlink NAS COUNT value of the currently active NAS security context to the received downlink NAS COUNT value in the NASC.

If verification of the NASC fails, the UE shall abort the handover procedure. Furthermore, the UE shall discard the new NAS security context if it was derived and continue to use the existing NAS and AS security contexts.

If *keySetChangeIndicator* in the HO command is true

- If the HO Command message contained a NASC parameter with the K_AMF_change_flag set to one:
  - The UE shall use the horizontally derived K_{AMF} and the NAS COUNT value of 2^{32}-1 in the derivation of the temporary K_{gNB}. The UE shall further process this temporary key as described in subclause 6.9.4.4.
- Else:
  - The UE handling related to key derivation shall be done as defined in clause 6.9.4.4.

Else

- If the NCC value the UE received in the HO Command message from target ng-eNB/gNB via source ng-eNB/gNB is equal to the NCC value associated with the currently active K_{gNB}/K_{eNB}, the UE shall derive the K_{NG-RAN}* from the currently active K_{gNB}/K_{eNB} and the target PCI and its frequency ARFCN-DL/EARFCN-DL using the function defined in Annex A.11 and A.12.
- If the UE received an NCC value that was different from the NCC associated with the currently active K_{gNB}/K_{eNB}, the UE shall first synchronize the locally kept NH parameter by computing the function defined in Annex A.10 iteratively (and increasing the NCC value until it matches the NCC value received from the source ng-eNB/gNB via the HO command message. When the NCC values match, the UE shall compute the K_{NG-RAN}* from the synchronized NH parameter and the target PCI and its frequency ARFCN-DL/EARFCN-DL using the function defined in Annex A.11 and A.12.

The UE shall use the K_{NG-RAN}* as the K_{gNB} when communicating with the target gNB and as the K_{eNB} when communicating with the target ng-eNB.

6.9.3 Key handling in mobility registration update

The procedure shall be invoked by the target AMF after the receiving of a Registration Request message of type mobility registration update from the UE wherein the UE and the source AMF are identified by means of a temporary identifier 5G-GUTI.

The protocol steps for the source AMF and target AMF performing context transfer are as follows:

a) The target AMF sends a message to the source AMF, this message contains the 5G-GUTI, the Access Type and the received Registration Request message.

b) The source AMF searches the data of the UE in the database and checks the integrity protection on the Registration Request message. The source AMF uses the 5G NAS security context corresponding to the Access Type to perform the integrity check.

   i) If the UE is found and the integrity check succeeds, when the source AMF does not change K_{AMF} according to its local policy, the source AMF shall send a response back that:

      - shall include the SUPI, and

      - may include any current 5G security context it holds.

   ii) If the UE is found and the integrity check succeeds, when the source AMF changes K_{AMF} according to its local policy, the source AMF shall send a response back that:

      - shall include the SUPI,

      - keyAmfHDerivationInd, and

      - may include a new 5G security context it derives from the current one it holds.

      The source AMF subsequently deletes the 5G security context which it holds.

      If the UE cannot be identified or the integrity check fails, then the source AMF shall send a response indicating that the temporary identifier 5G-GUTI cannot be retrieved.

c) If the target AMF receives a response with a SUPI, it creates an entry and stores the 5G security context that may have beenreceived .

   If the target AMF receives a response indicating that the UE could not be identified, it shall initiate the subscription identification procedure described in clause 6.12.4 of the present document.

NOTE: Void.

NOTE 1: The source AMF does not have K_{SEAF} because it is deleted after K_{AMF} derivation as per clause 6.2.2.1 and therefore the context transfer from the source AMF to the target AMF does not contain K_{SEAF}.

At mobility registration update, the source AMF shall use local policy to determine whether to perform horizontal K_{AMF} derivation. If the source AMF determines not to perform horizontal K_{AMF} derivation, the source AMF shall transfer current security context to the target AMF. If the source AMF determines to perform horizontal K_{AMF} derivation, the source AMF shall derive a new key K_{AMF} from the currently active K_{AMF} and the uplink NAS COUNT value in the received Registration Request message. The ngKSI for the newly derived K_{AMF} key is defined such as the value field and the type field are taken from the ngKSI of the current K_{AMF}. The source AMF shall transfer the new K_{AMF}, the new ngKSI, the UE security capability, the keyAmfHDerivationInd to the target AMF. The key derivation of the new K_{AMF} is specified in Annex A.13. If the source AMF has derived a new key K_{AMF}, the source AMF shall not transfer the old K_{AMF} to the target AMF and the source AMF shall in this case also delete any stored non-current 5G security context, and not transfer any non-current 5G security context to the target AMF.

When the target AMF receives the new K_{AMF} together with the keyAmfHDerivationInd, then the target AMF shall decide whether to use the K_{AMF} directly according to its local policy after receiving the response from the source AMF.

If the target AMF, according to its local policy, decides to not use the K_{AMF} received from the source AMF, it can perform a re-authentication procedure to the UE to establish a new NAS security context.

If the target AMF decides to use the key K_{AMF} received from source AMF (i.e., no re-authentication), it shall send the K_AMF_change_flag set to 1 to the UE in the NAS SMC including replayed UE security capabilities, the selected NAS algorithms and the ngKSI for identifying the new K_{AMF} from which the UE shall derive a new K_{AMF} to establish a new NAS security context between the UE and target AMF.

The target AMF shall reset the NAS COUNTs to zero and derive new NAS keys (K_{NASint} and K_{NASenc}) from the new K_{AMF} using the selected NAS algorithm identifiers as input. The target AMF shall integrity protect the NAS Security Mode Command message with the new K_{NASint} key.

If the UE receives the K_AMF_change_flag set to 1 in the NAS Security Mode Command message, then the UE shall derive a new key K_{AMF} from the current active K_{AMF} identified by the received ngKSI in the NAS Security Mode Command message using the uplink NAS COUNT valuethat was sent in the Registration Request message. The UE shall assign the received ngKSI in the NAS Security Mode Command message to the ngKSI of the new derived K_{AMF}.

The UE shall derive new NAS keys (K_{NASint} and K_{NASenc}) from the new K_{AMF} and integrity check the NAS Security Mode Command message using the new K_{NASint} key.

The UE shall then derive a new initial K_{gNB} from the new K_{AMF} as specified in Annex A.9.

The UE shall associate the derived new initial K_{gNB} with a new NCC value equal to zero and reset the NAS COUNTs to zero.

After the ongoing mobility registration procedure is successfully completed, the ME shall replace the currently stored K_{AMF} and ngKSI values on both USIM and ME with the new K_{AMF} and the associated ngKSI.

6.9.4 Key-change-on-the-fly

6.9.4.1 General

Key change on-the-fly consists of key refresh or key re-keying.

Key refresh shall be possible for K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-enc}, and K_{UP-int} (if available) and shall be initiated by the gNB/ng-eNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB}. The procedure is described in clause 6.9.4.5.

Key re-keying shall be possible for the K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-enc}, and K_{UP-int} (if available). This re-keying shall be initiated by the AMF when a 5G AS security context different from the currently active one shall be activated. The procedures for doing this are described in clause 6.9.4.4.

AS Key change on-the-fly is accomplished using a procedure based on intra-cell handover. The following AS key changes on-the-fly shall be possible: local K_{gNB} refresh (performed when PDCP COUNTs are about to wrap around), K_{gNB} re-keying performed after an AKA run, activation of a native context after handover from E-UTRAN.

Key re-keying shall be possible for $K_{NAS-enc}$ and $K_{NAS-int}$. Re-keying of $K_{NAS-enc}$ and $K_{NAS-int}$ shall be initiated by the AMF when a 5G NAS security context different from the currently active one shall be activated. The procedures for doing this are described in clause 6.9.4.2.

Re-keying of the entire 5G key hierarchy including K_{AMF} shall be achieved by first re-keying K_{AMF}, then $K_{NAS-enc}$ and $K_{NAS-int}$, followed by re-keying of the K_{gNB} and derived keys. For NAS key change on-the-fly, activation of NAS keys is accomplished by a NAS SMC procedure.

6.9.4.2 NAS key re-keying

After a primary authentication has taken place, new NAS keys from a new K_{AMF} shall be derived, according to Annex A.8.

To re-activate a non-current full native 5G security context after handover from E-UTRAN the UE and the AMF take the NAS keys into use by running a NAS SMC procedure according to clause 6.7.2.

AMF shall activate fresh NAS keys from a primary authentication run or activate native security context, which has a sufficiently low NAS COUNT values, before the NAS uplink or downlink COUNT wraps around with the current security context.

6.9.4.3 NAS key refresh

If the AMF determines that NAS key refresh is required due to e.g. uplink or downlink NAS counter in the current security context is about to wrap around or based on a local operator policy to refresh the NAS keys after a certain time, the AMF may trigger a primary authentication run or may derive a new K_{AMF} key using horizontal K_{AMF} derivation upon the reception of an initial NAS message, e.g. a Registration Request or a Service Request using the uplink NAS COUNT value in the initial NAS message as described in clause 6.9.3 for mobility update registration. The AMF resets the corresponding uplink and downlink NAS counters and derive new NAS keys from the new K_{AMF} key and the algorithms in use. The AMF activates the new K_{AMF} key by running a NAS SMC with UE according to clause 6.7.2. When the new K_{AMF} key is horizontally derived, the UE shall use the uplink NAS COUNT value that was sent in the initial NAS message to derive the same K_{AMF} key as the AMF, reset the corresponding uplink and downlink NAS counters and then derive new NAS keys from the K_{AMF} and the algorithms in use.

In this case, if AS security is also established between the UE and gNB/ng-eNB, then the AMF and the UE shall derive a new initial K_{gNB} from the new K_{AMF} as specified in Annex A.9. Further, the AMF and the UE shall associate the derived new initial K_{gNB} with a new NCC value equal to zero. Further, the derived new initial K_{gNB}/K_{eNB} is sent by the AMF to the gNB/ng-eNB triggering the gNB/ng-eNB to perform the AS key re-keying as described in clause 6.9.4.4.

6.9.4.4 AS key re-keying

The K_{gNB}/K_{eNB} re-keying procedure is initiated by the AMF. It may be used under the following conditions:

- after a successful AKA run with the UE as part of activating a partial native 5G security context; or
- as part of synchronizing the NAS and the AS security contexts as a part of handover procedure, if a handover is occuring; or
- as part of re-activating a non-current full native 5G security context after handover from E-UTRAN according to clause 8.4; or
- to create a new K_{gNB} from the current K_{AMF}.

NOTE 1: To perform a key change on-the-fly of the entire key hierarchy, the AMF has to change the 5G NAS security context before changing the 5G AS security context.

In order to be able to re-key the K_{gNB}, the AMF requires a fresh uplink NAS COUNT from a successful NAS SMC procedure with the UE. In the case of creating a new K_{gNB} from the current K_{AMF} a NAS SMC procedure shall be run first to provide this fresh uplink NAS COUNT. This NAS SMC procedure does not have to change other parameters in the current EPS NAS security context. The AMF derives the new K_{gNB} using the key derivation function as specified in Annex A.9 using the K_{AMF} and the uplink NAS COUNT used in the most recent NAS Security Mode Complete message. The derived new K_{gNB} is sent to the gNB/ng-eNB in an NGAP UE CONTEXT MODIFICATION REQUEST message triggering the gNB/ng-eNB to perform the AS key re-keying. The gNB/ng-eNB runs the key change on-the-fly procedure with the UE. During this procedure the gNB/ng-eNB shall indicate to the UE that a key change on-the-fly is taking place. The procedure used is based on an intra-cell handover, and hence the same K_{gNB} derivation steps shall be taken as in a normal handover procedure. The gNB/ng-eNB shall indicate to the UE to change the current K_{gNB} in intra-cell handover during this procedure. Network-side handling of AS key re-keying that occur as a part of Xn and N2 handovers are described is defined in clauses 6.9.2.3.2 and 6.9.2.3.3 of the present document.

When the UE receives an indication that the procedure is a key change on-the-fly procedure, the UE shall derive a temporary K_{gNB} by applying the key derivation function as specified in Annex A.9 using the K_{AMF} from the current 5G NAS security context and the uplink NAS COUNT in the most recent NAS Security Mode Complete message. UE-side handling of AS key re-keying that occur as a part of Xn and N2 handovers is described in clause 6.9.2.3.4 of the present document.

From this temporary K_{gNB} the UE shall derive the $K_{NG\text{-}RAN}$* as normal (see Annex A.11/A.12). The gNB/ng-eNB shall take the K_{gNB} it received from the AMF, which is equal to the temporary K_{gNB}, as basis for its $K_{NG\text{-}RAN}$* derivations. From this step onwards, the key derivations continue as in a normal handover.

If the AS level re-keying fails, then the AMF shall complete another NAS security mode procedure before initiating a new AS level re-keying. This ensures that a fresh K_{gNB} is used.

The NH parameter shall be handled according to the following rules:

- The UE, AMF, and gNB/ng-eNB shall delete any old NH upon completion of the context modification.
- The UE and AMF shall use the K_{AMF} from the currently active 5G NAS security context for the computation of the fresh NH. The computation of NH parameter value sent in the Namf_Communication_CreateUEContext Request, NGAP HANDOVER REQUEST, and NGAP PATH SWITCH REQUEST ACKNOWLEDGE messages shall be done according to clauses 6.9.2.3.2 and 6.9.2.3.3.

6.9.4.5 AS key refresh

This procedure is based on an intra-cell handover. The K_{gNB} chaining that is performed during a handover ensures that the K_{gNB} is re-freshed with respect to the RRC and UP COUNT after the procedure. The gNB/ng-eNB shall indicate to the UE to change the current K_{gNB} in intra-cell handover during this procedure.

6.9.5 Rules on concurrent running of security procedures

6.9.5.1 Rules related to AS and NAS security context synchronization

Concurrent runs of security procedures may, in certain situations, lead to mismatches between security contexts in the network and the UE. In order to avoid such mismatches, the following rules shall be adhered to:

1. AMF shall not initiate any of the N2 procedures including a new key towards a UE if a NAS Security Mode Command procedure is ongoing with the UE.

2. The AMF shall not initiate a NAS Security Mode Command towards a UE if one of the N2 procedures including a new key is ongoing with the UE.

3. When the AMF has sent a NAS Security Mode Command to a UE in order to take a new K_{AMF} into use and receives a request for an inter-AMF handover or an inter-RAT handover from the serving gNB/ng-eNB, the AMF shall wait for the completion of the NAS SMC procedure (i.e. receiving NAS Security Mode Complete) before initiating an inter-AMF handover or initiating an inter-RAT handover.

4. When the AMF has initiated a NGAP UE Context Modification procedure in order to take a new K_{gNB} into use, and receives a request for an inter-AMF handover from the serving gNB/ng-eNB, and decides not to change the K_{AMF} for the inter-AMF handover, the AMF shall wait for the (successful or unsuccessful) completion of the UE Context Modification procedure before initiating an inter-AMF handover.

5. Once the source AMF has initiated inter-AMF handover to the target AMF, or inter-system handover to the target MME, the source AMF shall not send any downlink NAS messages to the UE until it is aware that the handover has either failed or has been cancelled.

6.9.5.2 Rules related to parallel NAS connections

Concurrent runs of security procedures in parallel over two different NAS connections when terminated in the same AMF can lead to race conditions and mismatches between the security contexts in the network and the UE. In order to avoid such mismatches, the following rules shall be followed:

1. The SEAF/AMF shall not initiate a primary authentication or NAS SMC procedure in case a primary authentication or a NAS SMC procedure is ongoing on a parallel NAS connection. Authentication procedures followed by a NAS SMC procedures taking the new 5G security context into use, shall be performed on one NAS signalling connection at a time.

2. When the AMF has sent a NAS Security Mode Command to a UE in order to take a new K_{AMF} into use and receives a context transfer request message for the UE from another AMF, the AMF shall wait for the completion of the NAS SMC procedure (e.g. receiving NAS Security Mode Complete) before transferring the context.

3. The UE shall not initiate a NAS registration over a second NAS connection to an AMF of the same network before primary authentication on the first NAS connection is complete.

6.9.6 Security handling in registration with AMF reallocation via direct NAS reroute

In registration with AMF reallocation via direct NAS reroute, the initial AMF shall send the complete Registration Request in clear text to the target AMF.

NOTE: The completeRegistration Request in clear text is obtained based on the Registration Request initially received by the initial AMF if the UE have a valid NAS sececurity context, or the Registration Request received by the initial AMF as part of the Security Mode Complete if it is executed.

In registration with AMF reallocation via direct NAS reroute, the initial AMF shall use its local policy to determine whether to perform horizontal K_{AMF} derivation on current K_{AMF}. As described in Clause 6.9.3, if the initial AMF decides not to change K_{AMF}, the initial AMF shall send the current security context to the target AMF; otherwise, the initial

AMF shall derive new security context and send to the target AMF the derived security context and the indication of horizontal K_{AMF} derivation (i.e., keyAmfHDerivationInd).

If the target AMF receives the indication of horizontal K_{AMF} derivation (i.e., keyAmfHDerivationInd) from the initial AMF, it shall initiate NAS SMC. If the target AMF does not receive keyAmfHDerivationInd, the target AMF shall use the received security context from initial AMF and send protected NAS message including protected authentication request message if authentication is needed. The target AMF decides whether to perform authentication based on local policy.

6.10 Dual connectivity

6.10.1 Introduction

6.10.1.1 General

This clause describes the security functions necessary to support a UE that is simultaneously connected to more than one NG-RAN node, i.e., Multi-Radio dual connectivity (MR-DC) with 5GC as described in TS 37.340 [51]. The security functions are described in the context of the functions controlling the dual connectivity.

6.10.1.2 Dual Connectivity protocol architecture for MR-DC with 5GC

The dual connectivity protocol architecture for MR-DC with 5GC is shown in figure 6.10.1.2-1. The TS 37.340 [51] is to be referred for further details of the architecture illustrating MCG, SCG, and Split bearers for both SRBs and DRBs. The architecture has the following variants:

- NG-RAN E-UTRA-NR Dual Connectivity (NGEN-DC) is the variant when the UE is connected to one ng-eNB that acts as a Master Node (MN) and one gNB that acts as a Secondary Node (SN). The ng-eNB is connected to the 5GC and the gNB is connected to the ng-eNB via Xn interface.

- NR-E-UTRA Dual Connectivity (NE-DC) is the variant when the UE is connected to one gNB that acts as a MN and one ng-eNB that acts as a SN. The MN (i.e., gNB) is connected to 5GC and the ng-eNB (i.e., SN) is connected to the gNB via Xn interface.

- NR-NR Dual Connectivity (NR-DC) is the variant when the UE is connected to one gNB that acts as a MN and one gNB that acts as a SN. The MN is connected to 5GC while the SN is connected to MN via Xn interface.

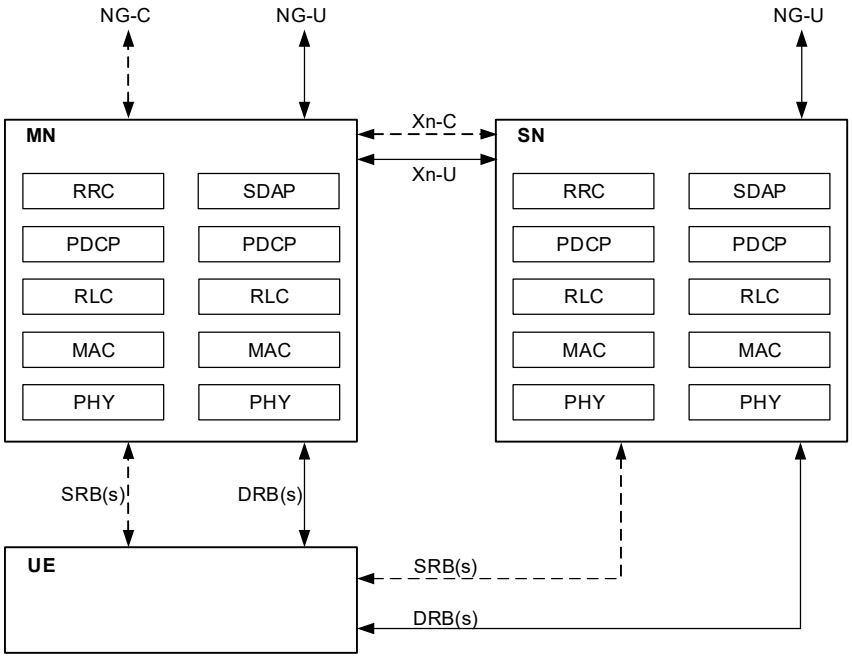


Figure 6.10.1.2-1 Multi-Radio dual connectivity (MR-DC) protocol architecture.

When the MN establishes security context between an SN and the UE for the first time for a given AS security context shared between the MN and the UE, the MN generates the K_{SN} for the SN and sends it to the SN over the Xn-C. To generate the K_{SN}, the MN associates a counter, called an SN Counter, with the current AS security context. The SN Counter is used as freshness input into K_{SN} derivations as described in the clause 6.10.3.2. The MN sends the value of the SN Counter to the UE over the RRC signalling path when it is required to generate a new K_{SN}. The K_{SN} is used to derive further RRC and UP keys that are used between the UE and SN.

6.10.2 Security mechanisms and procedures for DC

6.10.2.1 SN Addition or modification

When the MN is executing the Secondary Node Addition procedure (i.e. initial offload of one or more radio bearers to the SN), or the Secondary Node Modification procedure (as in clauses 10.2.2 and 10.3.2 in TS 37.340 [51]) which requires an update of the K_{SN}, the MN shall derive an K_{SN} as defined in clause 6.10.3.2. The MN shall maintain the SN Counter as defined in Clause 6.10.3.1. In the case of Conditional PSCell Change (CPC) and Conditional PSCell Addition (CPA) as specified in TS 37.340 [51], if there are more than one candidate SNs, for each SN, the MN shall derive a different KSN via using different SN counter as defined in clause 6.10.3.2.

When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last K_{SN} change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh K_{SN}, and then shall perform a SN Modification procedure to update the K_{SN}.

The dual connectivity procedure with activation of encryption/decryption and integrity protection follows the steps outlined on the Figure 6.10.2.1-1.

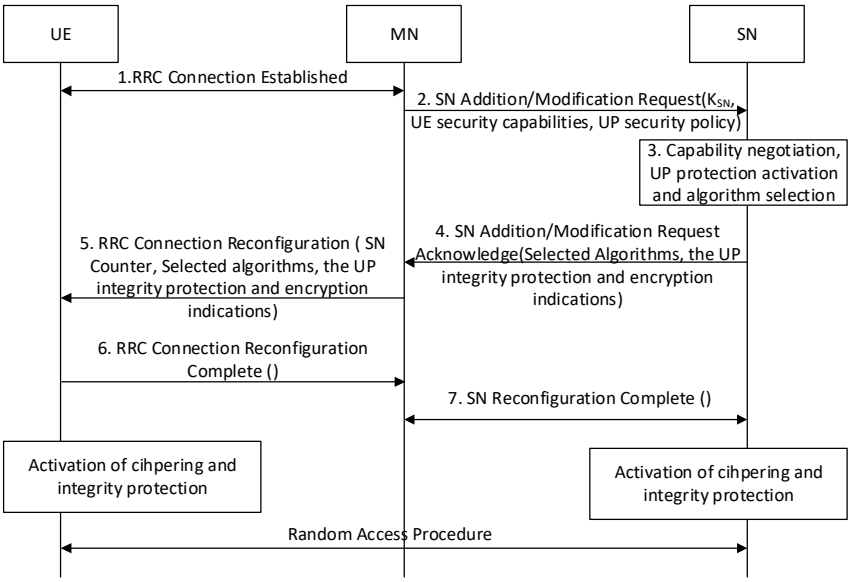


Figure 6.10.2.1-1. Security aspects in SN Addition/Modification procedures (MN initiated)

1. The UE and the MN establish the RRC connection.

2. The MN sends SN Addition/Modification Request to the SN over the Xn-C to negotiate the available resources, configuration, and algorithms at the SN. The MN computes and delivers the K_{SN} to the SN if a new key is needed. The UE security capabilities (see subclause 6.10.4) and the UP security policy received from the SMF shall also be sent to SN. In case of PDU split, UP integrity protection and ciphering activation decision from MN may be also included as described in subclause 6.10.4

   When the MN decides to configure CPA or CPC, if there are more than one candidate SNs, for each SN, the MN shall derive a different KSN and delivers the KSN to each SN via SN addition request separately..

3. The SN allocates the necessary resources and chooses the ciphering algorithm and integrity algorithm which has the highest priority from its configured list and is also present in the UE security capability. If a new K_{SN} was delivered to the SN then the SN calculates the needed RRC. The UP keys may be derived at the same time when RRC key derived. The SN shall activate the UP security policy as described in subclause 6.10.4.

4. The SN sends SN Addition/Modification Acknowledge to the MN indicating availability of requested resources and the identifiers for the selected algorithm(s) for the requested DRBs and/or SRB for the UE. The UP integrity protection and encryption indications shall be send to the MN.

5. The MN sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SN. The MN shall include the SN Counter parameter to indicate a new K_{SN} is needed and the UE shall compute the K_{SN} for the SN. The MN forwards the UE configuration parameters (which contains the algorithm identifier(s) received from the SN in step 4) , and UP integrity protection and encryption indications(received from the SN in step 4) to the UE (see subclause 6.10.3.3 for further details).

   If an SN sends more than one candidate PScell SCG configuration, the MN signals to the UE that all these configurations are associated with the same SN counter value.

NOTE 3: Since the message is sent over the RRC connection between the MN and the UE, it is integrity protected using the K_{RRCint} of the MN. Hence the SN Counter cannot be tampered with.

6. The UE accepts the RRC Connection Reconfiguration Request after validating its integrity. The UE shall compute the K_{SN} for the SN if an SN Counter parameter was included. The UE shall also compute the needed RRC and UP keys and activate the RRC and UP protection as per the indications received for the associated SRB and/or DRBs respectively. The UE sends the RRC Reconfiguration Complete to the MN. The UE activates the chosen encryption/decryption and integrity protection keys with the SN at this point.

7. MN sends SN Reconfiguration Complete to the SN over the Xn-C to inform the SN of the configuration result. On receipt of this message, SN may activate the chosen encryption/decryption and integrity protection with UE.

If SN does not activate encryption/decryption and integrity protection with the UE at this stage, SN shall activate encryption/decryption and integrity protection upon receiving the Random Access request from the UE.

6.10.2.2 Secondary Node key update

6.10.2.2.1 General

The SN shall request the Master Node to update the K_{SN} over the Xn-C, when uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB.

If the Master Node re-keys its currently active AS key in an 5G AS security context the Master Node shall update any K_{SN} associated with that 5G AS security context.

Whenever the UE or SN start using a fresh K_{SN}, they shall re-calculate the RRC and UP keys from the fresh K_{SN}.

6.10.2.2.2 MN initiated

The Master Node may update the K_{SN} for any reason. If the MN decides to update the K_{SN}, the MN shall perform a SN modification procedure to deliver the fresh K_{SN} to the SN as defined in clause 6.10.2.1. The MN shall provide the value of the SN Counter used in the derivation of the K_{SN} to the UE in an integrity protected RRC Connection Reconfiguration procedure. The UE shall derive the K_{SN} as described in clause A.16.

6.10.2.2.3 SN initiated

When uplink and/or downlink PDCP COUNTs are about to wrap around for any of the SCG DRBs or SCG SRB, the SN shall request the MN to update the K_{SN} over the Xn-C using the SN Modification procedure with MN involvement. The SN shall send the SN Modification Required message including K_{SN} key update an indication to the MN as shown in Figure 6.10.2.2.3-1. When the MN receives K_{SN} Key update indication, the MN shall derive a fresh K_{SN} and send the derived K_{SN} to the SN in the SN Modification Request message as in clause 6.10.2.1. Rest of the flows are like the call flow in Clause 6.10.2.1.

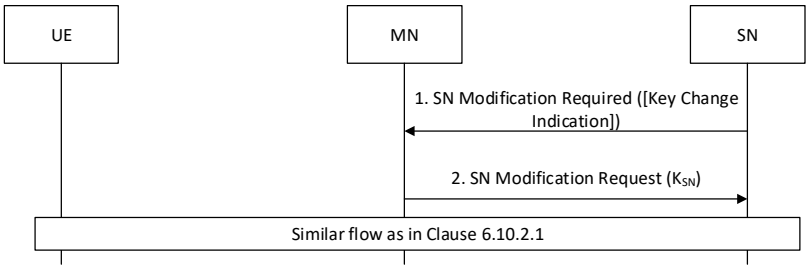


Figure 6.10.2.2.3-1. SN Key update procedure using SN Modification procedure (SN initiated with MN involvement)

6.10.2.3 SN release and change

When the SN releases the last UE radio bearer on the SN or when the SN is changed, i.e., the UE radio bearer(s) is moved from the SN, the SN and the UE shall delete the SN RRC and UP keys. The SN and UE shall also delete the K_{SN}, if it was not deleted earlier.

6.10.3 Establishing the security context between the UE and SN

6.10.3.1 SN Counter maintenance

The MN shall maintain a 16-bit counter, SN Counter, in its AS security context. The SN Counter is used when computing the K_{SN}.

The MN maintains the value of the counter SN Counter for a duration of the current 5G AS security context between UE and MN. The UE does not need to maintain the SN Counter after it has computed the K_{SN} since the MN provides the UE with the current SN Counter value when the UE needs to compute a new K_{SN}.

The SN Counter is a fresh input to K_{SN} derivation. That is, the UE assumes that the MN provides a fresh SN Counter each time and does not need to verify the freshness of the SN Counter.

NOTE: An attacker cannot, over the air modify the SN Counter and force re-use of the same SN Counter. The reason for this is that the SN Counter is delivered over the RRC connection between the MN and the UE, and this connection is both integrity protected and protected from replay.

The MN shall set the SN Counter to '0' when a new AS root key, $K_{NG\text{-}RAN}$, in the associated 5G AS security context is established. The MN shall set the SN Counter to '1' after the first calculated K_{SN}, and monotonically increment it for each additional calculated K_{SN}. The SN Counter value '0' is used to calculate the first K_{SN}.

If the MN decides to release the offloaded connections to the SN and later decides to re-start the offloading to the same SN, the SN Counter value shall keep increasing, thus keeping the computed K_{SN} fresh.

The MN shall refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. Refreshing the root key is done using intra cell handover as described in subclause 6.7.3.3 of the present document. When the root key is refreshed, the SN Counter is reset to '0' as defined above.

6.10.3.2 Derivation of keys

The UE and MN shall derive the security key K_{SN} of the SN as defined in Annex A.16 of the present document.

The SN RRC and UP keys shall be derived from the K_{SN} both at the SN and the UE using the function given in Annex A.7 of TS 33.401 [10] if the SN is a ng-eNB or using the function given in Annex A.8 of the present specification if the SN is a gNB.

Once all the SN RRC and UP keys have been derived from the K_{SN}, the SN and UE may delete the K_{SN}.

6.10.3.3 Negotiation of security algorithms

The MN shall receive the UE security capabilities from the AMF or the previous NG-RAN node. These security capabilities include both LTE and NR security capabilities.

When establishing one or more DRBs and/or SRBs for a UE at the SN, as shown on Figure 6.10.2.1-1, the MN shall provide the UE security capabilities of the UE to the SN in the SN Addition/Modification Request message.

Upon receipt of this message, the SN shall select the algorithms with highest priority in its locally configured list of algorithms that are also present in the received UE security capabilities and include the selected algorithms in SN Addition/Modification Request Acknowledge.

The MN shall provide the selected algorithms to the UE during the RRCConnectionReconfiguration procedure that configures the DRBs and/or SRB with the SN for the UE. The UE shall use the indicated algorithms for the DRBs and/or SRB whose PDCP terminates on the SN.

NOTE: The algorithms that the UE uses with the MN can be the same or different to the algorithms used with the SN.

6.10.4 Protection of traffic between UE and SN

This subclause provides the details of the needed SN RRC and UP keys and the algorithms used to protect the traffic whose PDCP terminates on the SN. The UE and SN may either calculate all the SN RRC and UP keys at once or as there are required to be used. The RRC and UP keys are K_{RRCenc} and K_{RRCint} for the SRB whose PDCP terminates on the SN and K_{UPenc} for the DRBs whose PDCP terminate on the SN.

When the SN is a gNB, the RRC traffic protection directly between the UE and SN is done using the mechanism described in subclause 6.5 of the present document with the algorithms specified in Annex D of the present document.

When the SN is a gNB, the UP traffic protection and activation is done using the mechanism described in subclauses 6.6 of the present document using the algorithms specified in Annex D of the present document. The UP security

activation procedure for MR-DC (meaning NR-DC, NE-DC and NGEN-DC) scenarios use the mechanism described in sublcause 6.10.2.1 with the following additional procedures:

In the case of split PDU session where some of the DRB(s) is terminated at the MN and some DRB(s) is terminated at the SN, the MN shall ensure that all DRBs which belong to the same PDU session have the same UP integrity protection and ciphering activation. To achieve this, the MN shall inform the SN with its UP integrity protection and ciphering activation decision of any DRB that is offloaded and to be terminated at the SN. The SN shall activate the UP integrity protection and ciphering based on the MN decision.

For UP Integrity Protection, if the UE does not indicate that it supports the use of integrity protection with ng-eNB:

Case 1: UP security policy indicates UP Integrity Protection "required":

In NGEN-DC scenario, the MN shall reject the PDU session.

In NE-DC scenario, if the MN decides to activate the UP integrity protection for this PDU session, the MN shall not offload any DRB of the PDU session to the SN.

In NR-DC scenario, the MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.

Case 2: UP security policy indicates UP Integrity Protection "preferred":

In NGEN-DC scenario, the MN shall always deactivate UP integrity protection. In this case, the SN shall always deactivate the UP integrity protection of any PDU session terminated at the SN.

In NE-DC scenario, if the MN has activated any of this PDU session DRBs with UP integrity protection "on", the MN shall not offload any DRB of this PDU session to the SN. However, if the MN has activated all DRBs of this PDU session with integrity protection "off", the MN may offload DRBs of this PDU session to the SN. In this case, the SN shall not activate the UP integrity protection and shall always set the UP integrity protection indication to "off".

In NR-DC scenario, the MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.

Case 3: UP security policy indicates UP Integrity Protection "not needed":

In all MR-DC scenarios, the MN and SN shall always deactivate UP integrity protection.

For UP integrity protection, if the UE indicates that it supports use of integrity protection with ng-eNB, in all 5GC-based MR-DC scenarios, the MN and SN shall make a decision on UP integrity protection according to the UP security policy for PDU sessions which terminate at the MN and SN, respectively, where all DRBs belonging to the same PDU session shall have the integrity protection either "on" or "off".

For UP Ciphering Protection:

In all MR-DC scenario, the MN and SN shall make a decision on UP ciphering protection according to the UP security policy for PDU sessions which terminate at the MN and SN, respectively, where all DRBs belonging to the same PDU session shall have the ciphering protection either "on" or "off".

NOTE 1: A UE that is Rel-16 or prior does not support UP integrity protection with ng-eNB. Therefore, explicit indication, as specified in clause 6.6.4.3, that the UE supports use of UP integrity protection with ng-eNB is required.

In all scenarios of MR-DC, the SN shall send the UP integrity protection and encryption indications to the MN in the SN Addition/Modification Request Acknowledgement message. The MN shall forward the UP integrity protection and encryption indications to the UE in RRC Connection Reconfiguration message. The UE activate the UP security protection with the SN based on the UP integrity protection and encryption indications using the scheme described in subclause 6.6.2. If the MN has not activated the RRC security before sending the RRC Connection Reconfiguration message, the MN shall perform AS SMC procedure first.

When the SN is a ng-eNB, the RRC and UP traffic is protected using the mechanism described in subclauses 7.4 and 7.3 respectively of TS 33.401 [10] with the algorithms specified in Annex C of TS 33.401 [10]. Additionally, the UP traffic is integrity protected based on the UP security policy and the indication that the UE supports the use of UP integrity protection with ng-eNB.

NOTE: Void.

6.10.5 Handover Procedure

During N2 and Xn handover, the DRB and/or SRB connections between the UE and the SN shall be released, and the SN and the UE shall delete the SN RRC and UP keys since they shall be refreshed by the new K_{SN} derived by the target-MN.

6.10.6 Signalling procedure for PDCP COUNT check

SN may request the MN to execute a counter check procedure specified in Clause 6.13 of this specification to verify the value of the PDCP COUNT(s) associated with DRB(s) offloaded to the SN. To accomplish this, the SN shall communicate this request, including the expected values of PDCP COUNT(s) and associated radio bearer identities to the MN over the Xn-C.

If the MN receives a RRC counter check response from the UE that contains one or several PDCP COUNT values (possibly associated with both MN and SN), the MN may release the connection or report the difference of the PDCP COUNT values to the serving AMF or O&M server for further traffic analysis, e.g., detecting the attacker.

6.10.7 Radio link failure recovery

Since the MN holds the control plane functions in MR-DC as in clause 6.10.1.2, the UE runs the RRC re-establishment procedure with the MN as specified in Clause 6.11 of the present document. During the RRC re-establishment procedure, the radio bearers between the UE and the SN shall be released.

6.11 Security handling for RRC connection re-establishment procedure

NOTE: This clause applies only to the gNB. Inter-RAT RRC Connection Re-establishment (i.e., between gNB and ng-eNB) is not supported. The RRC Connection Re-establishment procedure for the ng-eNB is specified in TS 33.401 [10].

The $K_{NG\text{-}RAN}$* and token calculation at handover preparation are cell specific instead of gNB specific. During the handover procedure, at potential RRC connection reestablishment (e.g., in handover failure case), the UE may select a cell different from the target cell to initiate the reestablishment procedure. To ensure that the UE RRC connection re-establishment attempt is successful when the UE selects another cell under the control of the target gNB at handover preparation, the source gNB may prepare multiple $K_{NG\text{-}RAN}$* keys and tokens for multiple cells which are under the control of the target gNB. The source gNB may prepare for multiple cells belonging to the serving gNB itself.

The preparation of these cells includes sending security context containing $K_{NG\text{-}RAN}$* keys and tokens for each cell to be prepared, as well as the corresponding NCC, the UE 5G security capabilities, and the security algorithms used in the source cell for computing the token, to the target gNB. The source gNB shall derive the $K_{NG\text{-}RAN}$* keys as described in Annex A.11/A.12 based on the corresponding target cell's physical cell ID and frequency ARFCN-DL.

In order to calculate the token, the source gNB shall use the negotiated NIA-algorithm from the 5G AS Security context from the source gNB with the following inputs: source C-RNTI, source PCI and target Cell-ID, where source PCI and source C-RNTI are associated with the cell the UE last had an active RRC connection with and target Cell-ID is the identity of the target cell where the RRCReestablishmentRequest is sent to.

- KEY shall be set to K_{RRCint} of the source cell;
- all BEARER bits shall be set to 1;
- DIRECTION bit shall be set to 1;
- all COUNT bits shall be set to 1.

The token shall be the 16 least significant bits of the output of the used integrity algorithm.

In order to avoid UE's inability to perform the RRC re-establishment procedure due to a failure during a handover or a connection re-establishment, the UE shall keep the K_{gNB} used in the source cell until the handover or a connection re-establishment has been completed successfully or until the UE has deleted the K_{gNB} for other reasons (e.g., due to transitioning to CM-IDLE).

For Xn handover, the target gNB shall use the received multiple $K_{NG\text{-}RAN}$* keys. But for N2 handover, the target gNB discards the multiple $K_{NG\text{-}RAN}$* keys received from the source gNB, and derives the $K_{NG\text{-}RAN}$* keys as described in Annex A.11/A.12 based on the received fresh {NH, NCC} pair from AMF for forward security purpose.

When an RRCReestablishmentRequest is initiated by the UE, the RRCReestablishmentRequest shall contain the token corresponding to the cell the UE tries to reconnect to. This message is transmitted over SRB0 and hence not integrity protected.

If the target gNB receiving the RRCReestablishmentRequest has a prepared $K_{NG\text{-}RAN}$* key and token for the specific cell, the target gNB receiving the RRCReestablishmentRequest shall validate the token received in the RRCReestablishmentRequest. However, if the target gNB has not prepared token for the cell, the target gNB extracts the C-RNTI and PCI from the RRCReestablishmentRequest message. The target gNB contacts the source gNB based on PCI by sending an Xn-AP Retrieve UE Context Request message with the following included: C-RNTI, PCI, the token and target Cell-ID, in order to allow the source gNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.

The source gNB retrieves the stored UE context including the UE 5G AS security context from its database using the C-RNTI. The source gNB verifies the token. If the verification is successful, then the source gNB calculates $K_{NG\text{-}RAN}$* using the target cell PCI, target ARFCN-DL and the K_{gNB}/NH in the current UE 5G AS security context based on either a horizontal key derivation or a vertical key derivation according to whether the source gNB has an unused pair of {NCC, NH} as described in Annex A.11. The source gNB can obtain the target PCI and target ARFCN-DL from a cell configuration database by means of the target Cell-ID which was received from the target gNB. Then the source gNB shall respond with an Xn-AP Retrieve UE Context Response message to the target gNB including the UE context that contains the UE 5G AS security context.

After successful verification of token by either target gNB or source gNB, the target gNB shall check whether it supports ciphering and integrity algorithms that the UE was using with the last source cell, if supports and these algorithms are the chosen algorithms or they are not the chosen algorithms by the target gNB, the target gNB shall use the $K_{NG\text{-}RAN}$* corresponding to the selected cell as K_{gNB} and derive new RRC keys (new K_{RRCint} and new K_{RRCenc}) based on the K_{gNB} and the AS algorithms used in source cell.

Then, the target gNB shall respond with an RRCReestablishment message containing the NCC received during the preparation phase or context fetch phase. This RRCReestablishment message is sent on SRB1 and is integrity protected in PDCP layer using the newly calculated K_{RRCint}.

If verification of the token is failed by either target gNB or source gNB, or the target gNB does not support the ciphering and integrity algorithms used in source cell, the target gNB shall reply with an RRCSetup message. The RRCSetup message is sent on SRB0 and hence not integrity protected.

Next the target gNB and UE shall do the following: The UE shall firstly synchronize the locally kept NH parameter as defined in Annex A.10 if the received NCC value is different from the current NCC value in the UE itself. Then the UE shall derive $K_{NG\text{-}RAN}$* as described in Annex A.11/A.12 based on the selected cell's physical cell ID and its frequency ARFCN-DL. The UE shall use this $K_{NG\text{-}RAN}$* as K_{gNB}. The gNB uses the $K_{NG\text{-}RAN}$* corresponding to the selected cell as K_{gNB}. The UE shall derive the new RRC keys from the K_{gNB} and the AS algorithms (ciphering and integrity algorithms) the UE was using with the source cell. The UE shall verify the integrity of the RRCReestablishment message by verifying the PDCP MAC-I using the newly derived K_{RRCint}.

NOTE: Void.

If the UE successfully validate the integrity of the received RRCReestablishment message, the UE shall respond with an RRCReestablishmentComplete on SRB1 while being integrity protected and ciphered using the new RRC keys. The RRCConnectionReconfiguration procedure used to re-establish the remaining radio bearers shall only include integrity protected and ciphered messages.

When the UE receives RRCSetup message, the UE shall perform the RRC connection establishment procedure as if the UE was in RRC_IDLE.

6.12 Subscription identifier privacy

6.12.1 Subscription permanent identifier

In the 5G system, the globally unique 5G subscription permanent identifier is called SUPI as defined in 3GPP TS 23.501 [2]. The SUCI is a privacy preserving identifier containing the concealed SUPI.

The SUPI is privacy protected over-the-air by using the SUCI which is described in clause 6.12.2. Handling of SUPI and privacy provisioning related to concealing the SUPI shall be done according to the requirements specified in clause 5 and details provided in clause 6.12.2.

6.12.2 Subscription concealed identifier

The SUbscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI.

The UE shall generate a SUCI using a protection scheme with the raw public key, i.e. the Home Network Public Key, that was securely provisioned in control of the home network. The protection schemes shall be the ones specified in Annex C of this document or the ones specified by the HPLMN.

The UE shall construct a scheme-input from the subscription identifier part of the SUPI as follows:

- For SUPIs containing IMSI, the subscription identifier part of the SUPI includes the MSIN of the IMSI as defined in TS 23.003 [19].
- For SUPIs taking the form of a NAI, the subscription identifier part of the SUPI includes the "username" portion of the NAI as defined in NAI RFC 7542 [57].

The UE shall execute the protection scheme with the constructed scheme-input as input and take the output as the Scheme Output.

The UE shall not conceal the Home Network Identifier and the Routing Indicator.

For SUPIs containing IMSI, the UE shall construct the SUCI with the following data fields:

- The SUPI Type as defined in TS 23.003 [19] identifies the type of the SUPI concealed in the SUCI.
- The Home Network Identifier is set to the MCC and MNC of the IMSI as specified in 23.003 [19].
- The Routing Indicator as specified in TS 23.003 [19].
- The Protection Scheme Identifier as specified in Annex C of this specification.
- The Home Network Public Key Identifier as specified in this document and detailed in TS 23.003 [19].
- The Scheme Output as specified in this document and detailed in TS 23.003 [19].

For SUPIs containing Network Specific Identifier, the UE shall construct the SUCI in NAI format with the following data fields:

- realm part of the SUCI is set to the realm part of the SUPI.
- username part of the SUCI is formatted as specified in TS 23.003 [19] using the SUPI Type, Routing Indicator, the Protection Scheme Identifier, the Home Network Public Key Identifier and the Scheme Output.

NOTE 1: The format of the SUPI protection scheme identifiers is defined in Annex C.

NOTE 2: The identifier and the format of the Scheme Output are defined by the protection schemes in Annex C. In case of non-null-schemes, the freshness and randomness of the SUCI will be taken care of by the corresponding SUPI protection schemes.

NOTE 2a: In case of null-scheme being used, the Home Network Public Key Identifier is set to a default value as described in TS 23.003 [19].

The UE shall include a SUCI only in the following 5G NAS messages:

- if the UE is sending a Registration Request message of type "initial registration" to a PLMN for which the UE does not already have a 5G-GUTI, the UE shall include a SUCI to the Registration Request message, or

- if the UE responds to an Identity Request message by which the network requests the UE to provide its permanent identifier, the UE includes a SUCI in the Identity Response message as specified in clause 6.12.4.

- if the UE is sending a De-Registration Request message to a PLMN during an initial registration procedure for which the UE did not receive the registration accept message with 5G-GUTI, the UE shall include the SUCI used in the initial registration to the De-Registration Request message.

NOTE 3: In response to the Identity Request message, the UE never sends the SUPI.

The UE shall generate a SUCI using "null-scheme" only in the following cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen PLMN, or

- if the home network has configured "null-scheme" to be used, or

- if the home network has not provisioned the public key needed to generate a SUCI.

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier. The operator should use proprietary identifier for protection schemes if the operator chooses that the calculation of the SUCI shall be done in USIM.

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision in the USIM an ordered priority list of the protection scheme identifiers that the operator allows. The priority list of protection scheme identifiers in the USIM shall only contain protection scheme identifiers specified in Annex C, and the list may contain one or more protection schemes identifiers. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the SUPI Type, the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the list of protection scheme identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list are obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the Home Network Public Key or the priority list are not provisioned in the USIM.

NOTE 4: The above feature is introduced since additional protection schemes could be specified in the future for a release newer than the ME release. In this case, the protection scheme selected by older MEs may not be the protection scheme with the highest priority in the list of the USIM.

6.12.3 Subscription temporary identifier

A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [19].

Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE in the registration procedure.

Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the N1 NAS signalling connection is suspended.

Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM-IDLE mode with suspend indication in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released or the suspension of the N1 NAS signalling connection.

NOTE 1: It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above, for example after a Service Request message from the UE not triggered by the network.

NOTE 2: It is left to implementation to generate 5G-GUTI containing 5G-TMSI that uniquely identifies the UE within the AMF.

5G-TMSI generation should be following the best practices of unpredictable identifier generation.

A new I-RNTI shall be sent to a UE only after a successful activation of AS security.

On transition of UE to RRC INACTIVE state requested by gNB during RRC Resume procedure or RNAU procedure, the gNB shall assign a new I-RNTI to the UE.

6.12.4 Subscription identification procedure

The subscriber identification mechanism may be invoked by the serving network when the UE cannot be identified by means of a temporary identity (5G-GUTI). In particular, it should be used when the serving network cannot retrieve the SUPI based on the 5G-GUTI by which the subscriber identifies itself on the radio path.

The mechanism described in figure 6.12.4-1 allows the identification of a UE on the radio path by means of the SUCI.

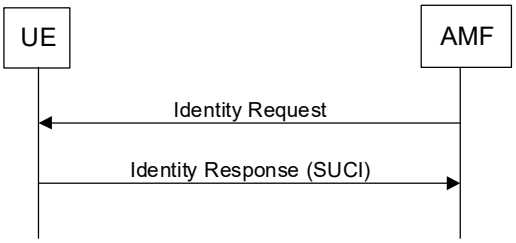


Figure 6.12.4-1: Subscription identifier query

The mechanism is initiated by the AMF that requests the UE to send its SUCI.

The UE shall calculate a fresh SUCI from SUPI using the Home Network Public Key, and respond with Identity Response carrying the SUCI. The UE shall implement a mechanism to limit the frequency at which the UE responds with a fresh SUCI to an Identity Request for a given 5G-GUTI.

NOTE 1: If the UE is using any other scheme than the null-scheme, the SUCI does not reveal the SUPI.

AMF may initiate authentication with AUSF to receive SUPI as specified in clause 6.1.3.

In case the UE registers for Emergency Services and receives an Identity Request, the UE shall use the null-scheme for generating the SUCI in the Identity Response.

NOTE 2: Registration for Emergency does not provide subscription identifier confidentiality.

6.12.5 Subscription identifier de-concealing function (SIDF)

SIDF is responsible for de-concealing the SUPI from the SUCI. When the Home Network Public Key is used for encryption of SUPI, the SIDF shall use the Home Network Private Key that is securely stored in the home operator's network to decrypt the SUCI. The de-concealment shall take place at the UDM. Access rights to the SIDF shall be defined, such that only a network element of the home network is allowed to request SIDF.

NOTE: One UDM can comprise several UDM instances. The Routing Indicator in the SUCI can be used to identify the right UDM instance that is capable of serving a subscriber.

6.13 Signalling procedure for PDCP COUNT check

The following procedure is used optionally by the gNB to periodically perform a local authentication. At the same time, the amount of data sent during the AS connection is periodically checked by the gNB and the UE for both up and down streams. If UE receives the Counter Check request, it shall respond with Counter Check Response message.

NOTE: The PDCP COUNT check is used to detect maliciously inserted packets. Packet insertion is detected automatically in integrity protected DRBs; therefore, the PDCP COUNT check procedure is superfluous for integrity protected bearers.

The gNB is monitoring the PDCP COUNT values associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

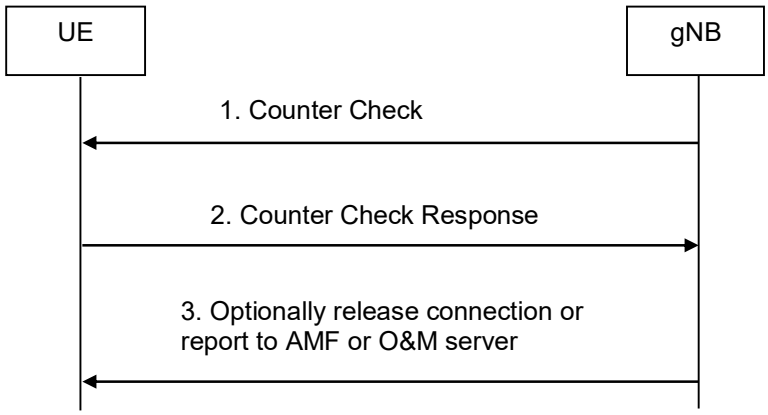


Figure 6.13-1: gNB periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the gNB. The Counter Check message contains the most significant parts of the PDCP COUNT values (which reflect amount of data sent and received) from each active radio bearer.

2. The UE compares the PDCP COUNT values received in the Counter Check message with the values of its radio bearers. Different UE PDCP COUNT values are included within the Counter Check Response message.

3. If the gNB receives a counter check response message that does not contain any PDCP COUNT values, the procedure ends. If the gNB receives a counter check response that contains one or several PDCP COUNT values, the gNB may release the connection or report the difference of the PDCP COUNT values for the serving AMF or O&M server for further traffic analysis for e.g. detecting the attacker.

6.14 Steering of roaming security mechanism

6.14.1 General

This clause describes the security functions necessary to support steering of the UE in the VPLMN during registration procedure and also after registration as described in TS 23.122 [53] Annex C. The security functions are described in the context of the functions supporting the control plane solution for steering of roaming in 5GS.

If the control plane solution for Steering of Roaming is supported by the HPLMN, the AUSF shall store the latest K_{AUSF} after the completion of the latest primary authentication.

The content of the Steering List as well as the conditions for sending it to the UE are described in TS 23.122 [53] Annex C. The Steering List includes either a list of preferred PLMN/access technology combinations, a secured packet or the HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'.

NOTE: The Steering of Roaming Information is defined in clause 1.2 of TS 23.122 [53]. It contains thus the ACK indication, the Steering List and the integrity protection information.

6.14.2 Security mechanisms

6.14.2.1 Procedure for steering of UE in VPLMN during registration

The security procedure for the case where the UE registers with VPLMN AMF is described below in figure 6.14.2.1-1:

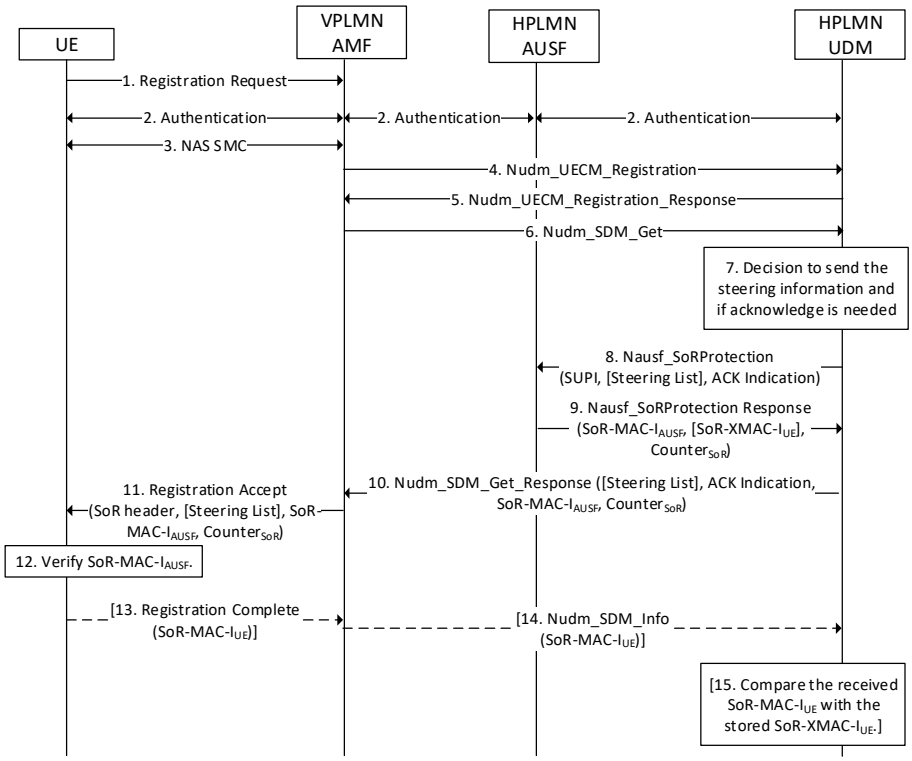


Figure 6.14.2.1-1: Procedure for providing list of preferred PLMN/access technology combinations during registration in VPLMN

1) The UE initiates registration by sending Registration Request message to the VPLMN AMF.

2-3) The VPLMN AMF executes the registration procedure as defined in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]. As part of the registration procedure, the VPLMN AMF executes primary authentication of the UE and then initiates the NAS SMC procedure, after the authentication is successful.

4-5) The VPLMN AMF invokes the Nudm_UECM_Registration message to the UDM and registers access with the UDM as per step 14a in sub-clause 4.2.2.2.2 of 3GPP TS 23.502[8].

6) The VPLMN AMF invokes Nudm_SDM_Get service operation message to the UDM to get amongst other information the Access and Mobility Subscription data for the UE (see step 14b in sub-clause 4.2.2.2.2 of 3GPP TS 23.502 [8]).

7) The UDM decides to send the Steering of Roaming Information, and obtains a list of preferred PLMN/access technology combinations and optional additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator), or a secured packet list as described in TS 23.122 [53].

NOTE 1: Additional SoR information (e.g. SOR-CMCI and the "Store the SOR-CMCI in the ME" indicator) can only be added when the AMF supports SoR transparent container.

If the UDM determines that the UE is configured to not expect to receive Steering of Roaming Information at initial registration and if the UDM determines that no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed, then the UDM may not piggyback Steering of Roaming Information at all in the Nudm_SDM_Get response and hence the following steps are omitted.

8-9) The UDM shall invoke Nausf_SoRProtection service operation message to the AUSF to get SoR-MAC-I_{AUSF} and $Counter_{SoR}$ as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest K_{AUSF} of the UE.

If the HPLMN decides that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-I_{UE}, as specified in sub-clause 14.1.3 of this document.

NOTE 2: At reception of Nausf_SoRProtection_Protect request from the UDM, if the SoR header is not included in the request, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and list of preferred PLMN/access technology combinations or secured packet (if provided); otherwise, if the SoR header is contained in the request, the AUSF uses the received SoR header in the calculation of SoR-MAC-I_{AUSF}..

The details of the $Counter_{SoR}$ are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SoR header in the calculation of SoR-MAC-I_{AUSF} allows the UE to verify that the received Steering of Roaming Information is not tampered with or removed by the VPLMN. The expected SoR-XMAC-I_{UE} allows the UDM to verify that the UE received the Steering of Roaming Information.

10) The UDM responds to the Nudm_SDM_Get service operation to the VPLMN AMF, which shall include the SoR transparent container as specified in clause 6.1.6.3.2 of TS 29.503 [93] if the VPLMN AMF support SoR transparent container, or shall include individual IEs comprising the ACK Indication, the list of preferred PLMN/access technology combinations or secured packet (if provided), SoR-MAC-I_{AUSF} and $Counter_{SoR}$ within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-I_{UE}.

11) If the SoR transparent container is received from the UDM, the VPLMN AMF shall include the received SoR transparent container in the Registration Accept message and send it to the UE. If the individual IEs are received from the UDM, the VPLMN AMF shall construct the SOR header based on the ACK Indication and the list of preferred PLMN/access technology combinations or secured packet (if provided) received from the UDM and include it in the SOR transparent container as specified in clause 9.11.3.51 of TS 24.501 [35]. The vPLMN shall also include SoR-MAC-$I_{AUSF}$and $Counter_{SoR}$(both also received from the UDM) in the constructed SoR transparent container, and convey the constructed SoR transparent container to the UE in the Registration Accept message.

12) On receiving the Registration Accept message with the SoR transparent container from the AMF the UE shall calculate the SoR-MAC-I_{AUSF} in the same way as the AUSF (as specified in Annex A.17) on the SoR transparent container, including the $Counter_{SoR}$ and the SoR header, and verifies whether it matches the SoR-MAC-I_{AUSF} value received in the Registration Accept message. Based on the SoR-MAC-I_{AUSF} verification outcome, the behaviour of the UE is specified in TS 23.122 [53].

13) If the UDM has requested an acknowledgement from the UE and the UE verified that the SoR transparent container received in step 12 has been provided by the HPLMN, then the UE shall send the Registration Complete message to the serving AMF. The UE shall generate the SoR-MAC-I_{UE} as specified in Annex A.18 and includes the generated SoR-MAC-I_{UE} in a SOR transparent container in the Registration Complete message.

14) The AMF sends a Nudm_SDM_Info request message to the UDM. If a transparent container with the SoR-MAC-I_{UE} was received in the Registration Complete message, then if the AMF supports SoR transparent container, the AMF shall include the received SoR transparent container in SoR transparent container in the Nudm_SDM_Info request message, otherwise, the AMF shall include the SoR-MAC-I_{UE} in the received SoR transparent container in the Nudm_SDM_Info request message.

15) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information in step 10, then the UDM shall compare the received SoR-MAC-I_{UE} with the expected SoR-XMAC-I_{UE} that the UDM stored temporarily in step 10.

6.14.2.2 Procedure for steering of UE in VPLMN or HPLMN after registration

The security procedure for the steering of UE in VPLMN after registration is described below in figure 6.14.2.2-1:

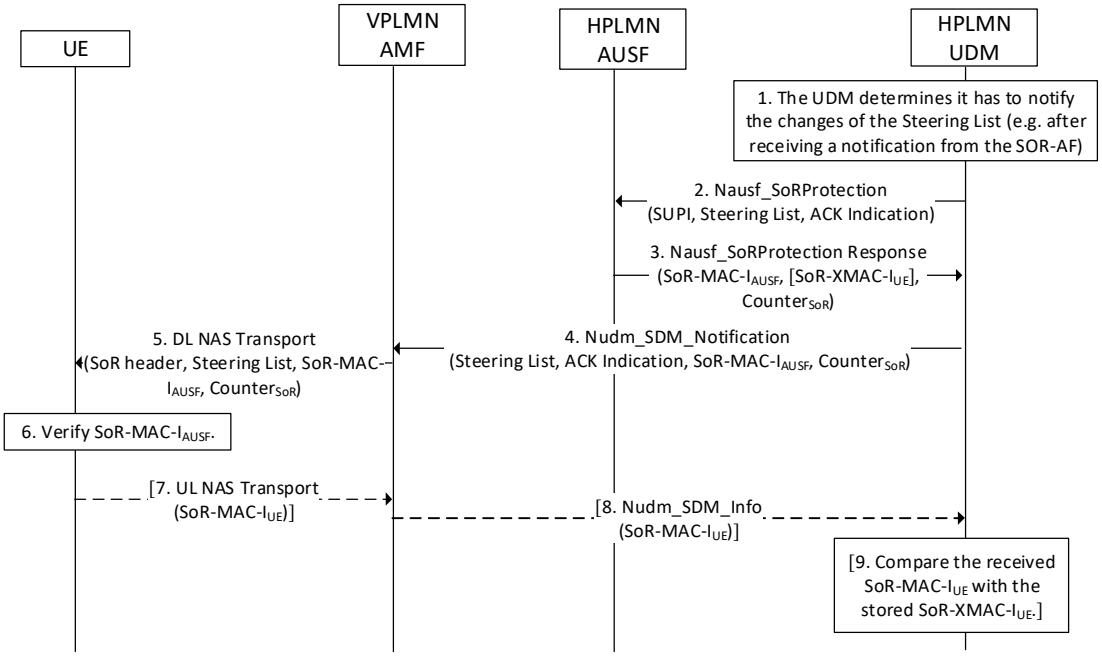


Figure 6.14.2.2-1: Procedure for providing list of preferred PLMN/access technology combinations after registration

1) The UDM decides to notify the UE of the changes to the Steering of Roaming Information by the means of invoking Nudm_SDM_Notification service operation.

2-3) The UDM shall invoke Nausf_SoRProtection service operation message by including the ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packet or SoR transparent container (only if transparent container is supported by the AMF) to the AUSF to get SoR-MAC-I_{AUSF} and $Counter_{SoR}$ as specified in sub-clause 14.1.3 of this document. The UDM shall select the AUSF that holds the latest K_{AUSF} of the UE.

If the HPLMN decided that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall set accordingly the ACK Indication included in the Nausf_SoRProtection service operation message to signal that it also needs the expected SoR-XMAC-I_{UE}, as specified in sub-clause 14.1.3 of this document.

NOTE: At reception of Nausf_SoRProtection_Protect request from the UDM, if the SoR header is not included in the request, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the UDM, i.e. ACK Indication and optionally the list of preferred PLMN/access technology combinations or secured packet; otherwise, if the SoR header in contained in the request, the AUSF uses the received SoR header in the calculation of SoR-MAC-$I_{AUSF.}$.

The details of the $Counter_{SoR}$ are specified in sub-clause 6.14.2.3 of this document. The inclusion of the Steering List and the SOR header in the calculation of SoR-MAC-I_{AUSF} allows the UE to verify that the Steering of Roaming Information received is not tampered with or removed by the VPLMN. The inclusion of these information in the calculation of the expected SoR-XMAC-I_{UE} allows the UDM to verify that the UE received the Steering of Roaming Information.

4) The UDM shall invoke Nudm_SDM_Notification service operation, which contains the SoR transaprent container as specified in clause 6.1.6.3.2 of TS 29.503 [93] if the VPMN AMF support SOR transparent container, or contains individual IEs including an optional the list of preferred PLMN/access technology combinations or secured packet, the ACK Indication, SoR-MAC-I_{AUSF}, and $Counter_{SoR}$ within the Access and

Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected SoR-XMAC-I_{UE}.

5) Upon receiving the Nudm_SDM_Notification message, if the SoR transparent container is included in the message, the AMF shall send a DL NAS Transport message to the served UE. including the received SoR transparent container; otherwise, the AMF shall construct the SOR transparent container (including the SOR header) as specified in clause 9.11.3.51 of 3GPP TS 24.501 [35] based on the ACK Indication, the Steering List, SoR-MAC-I_{AUSF} and $Counter_{SoR}$ received from the UDM, and send the constructed SoR transparent container included to the served UE in a DL NAS Transport message.

6) On receiving the DL NAS Transport message, the UE shall calculate the SoR-MAC-I_{AUSF} in the same way as the AUSF (as specified in Annex A.17) on the received SoR transparent container, including the $Counter_{SoR}$ and the SoR header and verify whether it matches the SoR-MAC-I_{AUSF} value received in the DL NAS Transport message.

7) If the UDM has requested an acknowledgement from the UE and the UE verified that the Steering Information has been provided by the HPLMN, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the SoR-MAC-I_{UE} as specified in Annex A.18 and includes the generated SoR-MAC-I_{UE} in a SOR transparent container in the UL NAS Transport message.

8) The AMF shall send a Nudm_SDM_Info request message to the UDM. If a SOR transparent container with the SoR-MAC-I_{UE} was received in the UL NAS Transport message, the AMF shall include the received SoR transparent container in the Nudm_SDM_Info request message if the AMF supports SoR transparent container, otherwise, the AMF shall include the SoR-MAC-I_{UE} in the Nudm_SDM_Info request message.

9) If the HPLMN indicated that the UE is to acknowledge the successful security check of the received Steering of Roaming Information, then the UDM shall compare the received SoR-MAC-I_{UE} with the expected SoR-XMAC-I_{UE} that the UDM stored temporarily in step 4.

6.14.2.3 SoR Counter

The AUSF and the UE shall associate a 16-bit counter, $Counter_{SoR}$, with the key K_{AUSF}.

The UE shall initialize the $Counter_{SoR}$ to 0x00 0x00 when the newly derived K_{AUSF} is stored (see clause 6.2.2.2). The UE shall store the SoR counter. If the USIM supports both 5G parameters storage and 5G parameters extended storage, then CounterSoR shall be stored in the USIM. Otherwise, CounterSoR shall be stored in the non-volatile memory of the ME

To generate the SoR-MAC-I_{AUSF}, the AUSF shall use the $Counter_{SoR}$. The $Counter_{SoR}$ shall be incremented by the AUSF for every new computation of the SoR-MAC-I_{AUSF}. The $Counter_{SoR}$ is used as freshness input into SoR-MAC-I_{AUSF} and SoR-MAC-I_{UE} derivations as described in the Annex A.17 and Annex A.18 respectively, to mitigate the replay attack. The AUSF shall send the value of the $Counter_{SoR}$ (used to generate the SoR-MAC-I_{AUSF}) along with the SoR-MAC-I_{AUSF} to the UE. The UE shall only accept $Counter_{SoR}$ value that is greater than stored $Counter_{SoR}$ value. The UE shall store the received $Counter_{SoR,}$ only if the verification of the received SoR-MAC-I_{AUSF} is successful. The UE shall use the stored $Counter_{SoR}$ received from the HPLMN, when deriving the SoR-MAC-I_{UE} for the SoR acknowledgement.

The AUSF and the UE shall maintain the $Counter_{SoR}$ for lifetime of the K_{AUSF}.

The AUSF that supports the control plane solution for steering of roaming shall initialize the $Counter_{SoR}$ to 0x00 0x01 when the newly derived K_{AUSF} is stored (see clause 6.2.2.1). The AUSF shall set the $Counter_{SoR}$ to 0x00 0x02 after the first calculated SoR-MAC-I_{AUSF}, and monotonically increment it for each additional calculated SoR-MAC-I_{AUSF}. The SoR Counter value of 0x00 0x00 shall not be used to calculate the SoR-MAC-I_{AUSF} and SoR-MAC-I_{UE}.

The AUSF shall suspend the SoR protection service for the UE, if the $Counter_{SoR}$ associated with the K_{AUSF} of the UE, is about to wrap around. When a fresh K_{AUSF} is generated for the UE, the $Counter_{SoR}$ at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume the SoR protection service for the UE.

6.15 UE parameters update via UDM control plane procedure security mechanism

6.15.1 General

This clause describes the security functions necessary to update the UE parameters using the UDM control plane procedure specified in TS 23.502 [8]. The security functions are described in the context of the functions supporting the delivery of UE Parameters Update Data from the UDM to the UE after the UE has successfully registered to the 5G network.

If the control plane procedure for UE parameters update is supported by the UDM, the AUSF shall store the latest K_{AUSF} after the completion of the latest primary authentication.

The content of UE Parameters Update Data and the conditions for sending it to the UE as well as how it is handled at the UE are specified in TS 24.501 [35].

NOTE : The home network relies on the serving network to deliver the UE parameters update.

6.15.2 Security mechanisms

6.15.2.1 Procedure for UE Parameters Update

The UDM may decide to perform UE parameters update anytime after the UE has been successfully authenticated and registered to the 5G system. The security procedure for the UE parameters update is described below in figure 6.15.2.1-1:

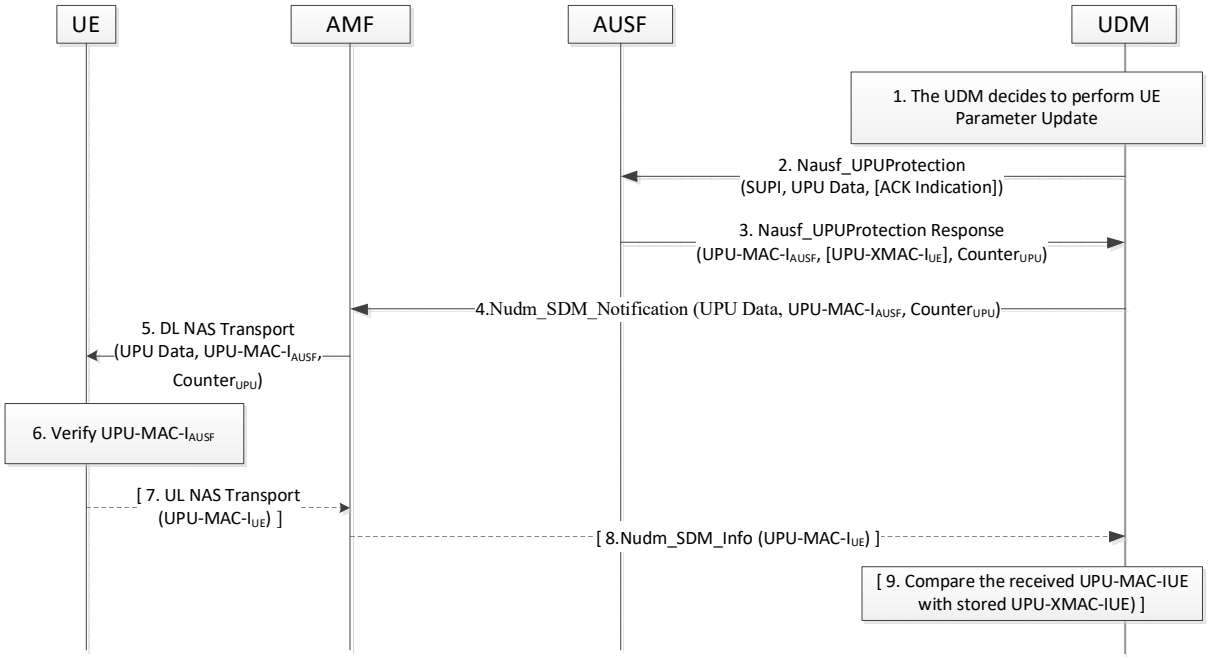


Figure 6.15.2.1-1: Procedure for UE Parameters Update

1) The UDM decides to perform the UE Parameters Update (UPU) using the control plane procedure while the UE is registered to the 5G system. If the final consumer of any of the UE parameters to be updated (e.g., the updated Routing ID Data) is the USIM, the UDM shall protect these parameters using a secured packet mechanism (see 3GPP TS 31.115 [65]) to update the parameters stored on the USIM. The UDM shall then prepare the UE Parameters Update Data (UPU Data) by including the parameters protected by the secured packet, if any, as well as any UE parameters for which final consumer is the ME (see TS 24.501 [35]).

2-3) The UDM shall invoke Nausf_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-I_{AUSF} and $Counter_{UPU}$ as specified in sub-clause 14.1.4 of this document. The UDM shall select the AUSF that holds the latest K_{AUSF} of the UE.

If the UDM decided that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall include the ACK Indication in the Nausf_UPUProtection service operation message to signal that it also needs the expected UPU-XMAC-I_{UE}, as specified in sub-clause 14.1.4 of this document.

The details of the CounterUPU is specified in sub-clause 6.15.2.2 of this document. The inclusion of UE Parameters Update Data in the calculation of UPU-MAC-IAUSF allows the UE to verify that it has not been tampered by any intermediary. The expected UPU-XMAC-I_{UE} allows the UDM to verify that the UE received the UE Parameters Update Data correctly.

4) The UDM shall invoke Nudm_SDM_Notification service operation, which includes the UPU transparent container if the AMF supports UPU transparent container, or includes individual IEs comprising the UE Parameters Update Data, UPU-MAC-I_{AUSF}, $Counter_{UPU}$ within the Access and Mobility Subscription data. If the UDM requests an acknowledgement, it shall temporarily store the expected UPU-XMAC-I_{UE}.

5) Upon receiving the Nudm_SDM_Notification message, the AMF shall send a DL NAS Transport message to the served UE. The AMF shall include in the DL NAS Transport message the transparent container if received from the UDM in step 4. Otherwise, if the UDM provided individual IEs in step 4, then the AMF shall construct a UPU transparent container.

6) On receiving the DL NAS Transport message, the UE shall calculate the UPU-MAC-I_{AUSF} in the same way as the AUSF (as specified in Annex A.19) on the received UE Parameters Update Data and the $Counter_{UPU}$ and verify whether it matches the UPU-MAC-I_{AUSF} value received within the UPU transparent container in the DL NAS Transport message. If the verification of UPU-MAC-I_{AUSF} is successful and the UPU Data contains any parameters that is protected by secured packet (see 3GPP TS 31.115 [65]), the ME shall forward the secured packet to the USIM using procedures in 3GPP TS 31.111 [66]. If the verification of UPU-MAC-I_{AUSF} is successful and the UPU Data contains any parameters that is not protected by secure packet, the ME shall update its stored parameters with the received parameters in UDM Updata Data.

7) If the UDM has requested an acknowledgement from the UE and the UE has successfully verified and updated the UE Parameters Update Data provided by the UDM, then the UE shall send the UL NAS Transport message to the serving AMF. The UE shall generate the UPU-MAC-I_{UE} as specified in Annex A.20 and include the generated UPU-MAC-I_{UE} in a transparent container in the UL NAS Transport message.

8) If a transparent container with the UPU-MAC-I_{UE} was received in the UL NAS Transport message, the AMF shall send a Nudm_SDM_Info request message with the transparent container to the UDM.

9) If the UDM indicated that the UE is to acknowledge the successful security check of the received UE Parameters Update Data, then the UDM shall compare the received UPU-MAC-I_{UE} with the expected UPU-XMAC-I_{UE} that the UDM stored temporarily in step 4.

6.15.2.2 UE Parameters Update Counter

The AUSF and the UE shall associate a 16-bit counter, $Counter_{UPU}$, with the key K_{AUSF}.

The UE shall initialize the $Counter_{UPU}$ to 0x00 0x00 when the newly derived K_{AUSF} is stored (see clause 6.2.2.2). The UE shall store the UPU counter . If the USIM supports both 5G parameters storage and 5G parameters extended storage, then $Counter_{UPU}$ shall be stored in the USIM. Otherwise, $Counter_{UPU}$ shall be stored in the non-volatile memory of the ME.

To generate the UPU-MAC-I_{AUSF}, the AUSF shall use the $Counter_{UPU}$. The $Counter_{UPU}$ shall be incremented by the AUSF for every new computation of the UPU-MAC-I_{AUSF}. The $Counter_{UPU}$ is used as freshness input into UPU-MAC-I_{AUSF} and UPU-MAC-I_{UE} derivations as described in the Annex A.19 and Annex A.20 respectively, to mitigate the replay attack. The AUSF shall send the value of the $Counter_{UPU}$ (used to generate the UPU-MAC-I_{AUSF}) along with the UPU-MAC-I_{AUSF} to the UE. The UE shall only accept $Counter_{UPU}$ value that is greater than stored $Counter_{UPU}$ value. The UE shall update the stored $Counter_{UPU}$ with the received $Counter_{UPU,}$ only if the verification of the received UPU-MAC-I_{AUSF} is successful. The UE shall use the $Counter_{UPU}$ received from the UDM, when deriving the UPU-MAC-I_{UE} for the UE Parameters Upadate Data acknowledgement.

The AUSF and the UE shall maintain the $Counter_{UPU}$ for lifetime of the K_{AUSF}.

The AUSF that supports the UE parameters update using control plane procedure shall initialize the $Counter_{UPU}$ to 0x00 0x01 when the newly derived K_{AUSF} is stored (see clause 6.2.2.1). The AUSF shall set the $Counter_{UPU}$ to 0x00 0x02 after the first calculated UPU-MAC-I_{AUSF}, and monotonically increment it for each additional calculated UPU-MAC-I_{AUSF}. The UPU Counter value of 0x00 0x00 shall not be used to calculate the UPU-MAC-I_{AUSF} and UPU-MAC-I_{UE}.

The AUSF shall suspend the UE Parameters Update protection service for the UE, if the $Counter_{UPU}$ associated with the K_{AUSF} of the UE, is about to wrap around. When a fresh K_{AUSF} is generated for the UE, the $Counter_{UPU}$ at the AUSF is reset to 0x00 0x01 as defined above and the AUSF shall resume theUE Parameters Update protection service for the UE.

6.16 Security handling in Cellular IoT

6.16.1 Security handling in Control Plane CIoT 5GS Optimization

6.16.1.1 Security procedures for Small Data Transfer in Control Plane CIoT 5GS Optimisation

The Control Plane Optimisation for 5GS CIoT is used to exchange small user data or SMS as payload of a NAS message in both uplink and downlink directions. The UE and the AMF perform integrity protection and ciphering for the small user data or SMS using NAS security context specific to the NAS connection.

If UE uses Control Plane optimisation for 5GS CIoT for Mobile Originated data transport, the UE sends a Control Plane Service Request message including a container for small user data or SMS transport. The Control Plane Service Request message shall be partially ciphered (i.e. the container including uplink user data or SMS is ciphered, and non-cleartext remains unciphered) and integrity protected by the current 5G NAS security context specific to the NAS connection if such exists as depicted in TS 24.501 [35]. Upon reception of the Control Plane Service Request message with the ciphered container for small user data or SMS transport, the AMF shall verify integrity of the whole Control Plane Service Request message and decipher the ciphered container to obtain the small user data or SMS. When applying NAS ciphering/deciphering mechanism for the container, the LENGTH value shall be set to the length of the container contents.

Additionally, if UE uses Control Plane optimisation for 5GS CIoT for Mobile Originated data transport, the UE in CM-CONNECTED mode sends small user data or SMS in UL NAS transport message to the AMF. The UL NAS transport message shall be ciphered and integrity protected with the current 5G NAS security context specific to the NAS connection. Upon reception of the UL NAS transport message for small user data or SMS transport, the AMF shall verify integrity and decipher the UL NAS transport message to obtain the small user data or SMS.

If UE uses Control Plane optimisation for 5GS CIoT for Mobile Terminated data transport, the UE obtains small user data or SMS in DL NAS transport message from the AMF. The DL NAS transport message shall be ciphered and integrity protected with the current 5G NAS security context specific to the NAS connection. Upon reception of the DL NAS transport message for small user data or SMS transport, the UE shall verify integrity and decipher the DL NAS transport message to obtain the small user data or SMS.

6.16.1.2 Security procedures for RRCConnectionRe-establishment Procedure in Control Plane CIoT 5GS Optimization

If the UE experience a RLF when using Control Plane CIoT 5GS optimisation only, the AS layer of the UE may trigger an RRCConnectionReestablishment procedure. As there is no AS security available, this procedure can not be protected as described in subclause 6.11.

In order to protect the the re-establishment procedure, the AS part of the UE triggers the NAS part of the UE to provide the UL_NAS_MAC and XDL_NAS_MAC. These parameter are used to show that the UE is requesting the re-establishment and that the UE is talking to a genuine network respectively.

The UE calculates a UL_NAS_MAC and XDL_NAS_MAC by using the curently used NAS integrity algorithm with the following inputs, K_{NASint} as the key, the uplink NAS COUNT that would be used for the next uplink NAS message, the DIRECTION bit set to 0 and the target Cell-ID as the message to be protected to calculate NAS-MAC (see Annex D.3.1).

The uplink NAS COUNT is increased by the UE in exactly the same way as if it had sent a NAS message. The first 16 bits of NAS-MAC form UL_NAS_MAC and the last 16 bits form XDL_NAS_MAC, which is stored by the UE.

The UE shall send the RRCConnectionRestablishmentRequest message to the target ng-eNB and shall include the Truncated 5G-S-TMSI (as described in TS 23.501 [2], TS 23.003 [19] and TS 36.331 [69]), the 5 least significant bits (LSB) of the NAS COUNT that was used to calculate NAS-MAC and UL_NAS_MAC in the message.

The target ng-eNB recognises the RRCConnectionRestablishmentRequest message sent by a UE relates to the Control Plane CIoT 5GS optimisation based on the presence of the Truncated 5G-S-TMSI in the message. The target ng-eNB shall recreate the 5G-S-TMSI from the Truncated 5G-S-TMSI (as described in TS 23.501 [2], TS 23.003 [19] and TS 36.331 [69]). The target ng-eNB shall send the 5G-S-TMSI, LSB of NAS COUNT, UL_NAS_MAC and target Cell-ID in the CP Relocation Indication message to the AMF that is serving the UE (this can be deteremined by the S-TMSI).

The AMF uses LSB of NAS COUNT to estimate the full uplink NAS COUNT and calculates XNAS-MAC (see Annex D.3.1) using the same inputs (i.e. estimated uplink NAS COUNT, DIRECTION bit set to 0 and the target Cell-ID as the message) as the UE used for calculating NAS-MAC. The AMF then compares the received UL_NAS_MAC with the first 16 bits of XNAS-MAC and if these are equal the network is sure that the geniune UE sent the RRCConnectionRestablishmentRequest message. The stored uplink NAS COUNT in the AMF is set as though the AMF received a sucessfully protected NAS message using that NAS COUNT.

The AMF shall set DL_NAS_MAC to the last 16 bits of already calculated XNAS-MAC and send DL_NAS_MAC to the target ng-eNB in the Connection Establishment Indication message. The target ng-eNB shall send the DL_NAS_MAC to the UE in the RRCConnectionReestablisment message. The UE shall check that the received DL_NAS_MAC equal to the stored XDL_NAS_MAC. If so, the UE shall complete the re-establishment procedure.

6.16.2 Security handling in User Plane CIoT 5GS Optimization

6.16.2.1 General

The purpose of this procedure is to allow the ng-eNB to suspend an RRC connection to be resumed by the UE using User Plane CIoT 5GS Optimisation at a later time. The UE may resume the RRC connection in the same or different ng-eNB where the suspend took place. The UE and ng-eNB store the AS security context at suspend and reactivate the AS security context at resume.

The UE and the ng-eNB may also use EDT (Early Data Transmission) or PUR (Preconfigured Uplink Resource) feature in this procedure, as defined in TS 36.300 [88] and TS 36.331 [69].

6.16.2.2 Connection Suspend

When the ng-eNB initiates the Connection Suspend procedure, it sends N2 Suspend Request message to the AMF. Upon reception of the N2 Suspend Request message, the AMF shall check its local policy. If the local policy indicates that a new NH derivation is needed, the AMF shall increase its locally kept NCC value by one and compute a fresh NH from its stored data using the function defined in Annex A.10. The AMF shall store that fresh {NH, NCC} pair and send it to the ng-eNB in the N2 Suspend Response message.

Upon receipt of the N2 Suspend Response message from the AMF and if the message includes a {NH, NCC} pair, the ng-eNB shall store the fresh {NH, NCC} pair in the N2 Suspend Response message and remove any existing unused stored {NH, NCC} pairs.

The ng-eNB shall send to the UE an RRC Release with *releaseCause set to rrc-suspend* message that is ciphered and integrity protected in PDCP layer using current AS security context. The ng-eNB shall include a fresh I-RNTI, and an NCC in that RRC Release message. The I-RNTI is used for context identification, and the UE ID part of the I-RNTI assigned by the ng-eNB shall be different in consecutive suspends of the same UE. This is to avoid tracking of UEs based on the I-RNTI. If the ng-eNB has a fresh and unused pair of {NCC, NH}, the ng-eNB shall include the NCC in the RRC Release message. Otherwise, the ng-eNB shall include the same NCC associated with the current K_{gNB} in the RRC Release message. The NCC is used for AS security.

The ng-eNB shall delete the current AS keys K_{RRCenc}, K_{UPenc} (if available), and K_{UPint} (if available) after sending the RRC Release message to the UE, but shall keep the current AS key K_{RRCint}. If the sent NCC value is fresh and belongs to an unused pair of {NCC, NH}, the ng-eNB shall save the pair of {NCC, NH} in the current UE AS security context and shall delete the current AS key K_{gNB}. If the sent NCC value is equal to the NCC value associated with the current

K_{gNB}, the ng-eNB shall keep the current AS key K_{gNB} and NCC. The ng-eNB shall store the sent I-RNTI together with the current UE context including the remainder of the AS security context.

Upon receiving the RRC Release with *releaseCause set to rrc-suspend* message from the ng-eNB, the UE shall decrypt the RRC Release message using the K_{RRCenc} key and verify that the integrity of the received the RRC Release message is correct by checking the PDCP MAC-I. If this verification is successful, then the UE shall take the received NCC value and save it as stored NCC with the current UE context.

6.16.2.3 Connection Resume in CM-IDLE with Suspend to a new ng-eNB

When the UE using user plane CIoT 5GS Optimization decides to resume the RRC connection in CM-IDLE with suspend, the UE sends the RRC Resume Request message on SRB0 (i.e. it is not integrity protected). The UE shall include I-RNTI and a ShortResumeMAC-I in RRC Resume Request message. The I-RNTI is used for context identification and its value shall be the same as the I-RNTI that the UE had received from the source ng-eNB in the RRC Release with *releaseCause set to rrc-suspend* message in the source cell. The ShortResumeMAC-I is a 16-bit message authentication token, the UE shall calculate it using the integrity algorithm (EIA) in the stored AS security context, which was negotiated between the UE and the source ng-eNB and the current K_{RRCint} with the following inputs:

- KEY : it shall be set to current K_{RRCint};
- BEARER : all its bits shall be set to 1.
- DIRECTION : its bit shall be set to 1;
- COUNT : all its bits shall be set to 1;
- MESSAGE : it shall be set to VarShortResumeMAC-Input as defined in TS 36.331 [69] for ng-eNB with the following inputs:

  source C-RNTI, source PCI, resume constant, target Cell-ID.

The source PCI and source C-RNTI are associated with the cell where the UE was suspended. The target Cell-ID is the identity of the target cell where the UE sends the RRC Resume Request message. The resume constant allows differentiation of *VarShortResumeMAC* from *VarShortMAC*.

For protection of all RRC messages except RRC Reject message following the sent RRC Resume Request message, the UE shall derive a $K_{NG\text{-}RAN}$* using the target PCI, target EARFCN-DL and the K_{gNB}/NH based on either a horizontal key derivation or a vertical key derivation as defined in clause 6.9.2.1.1 and Annex A.12. The UE shall further derive K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived $K_{NG\text{-}RAN}$*. Then the UE resets all PDCP COUNTs to 0 and activates the new AS keys in PDCP layer.

When the target ng-eNB receives the RRC Resume Request message from the UE, the target ng-eNB extracts the I-RNTI from the RRC Resume Request message. The target ng-eNB contacts the source ng-eNB based on the information in the I-RNTI by sending an Xn-AP Retrieve UE Context Request message with the following included: I-RNTI, ShortResumeMAC-I and target Cell-ID, in order to allow the source ng-eNB to validate the UE request and to retrieve the UE context including the UE 5G AS security context.

The source ng-eNB retrieves the stored UE context including the UE 5G AS security context from its database using the I-RNTI. The source ng-eNB verifies the shortResumeMAC-I using the current K_{RRCint} key stored in the retrieved UE 5G AS security context (calculating the shortResumeMAC-I in the same way as described above). If the verification of the shortResumeMAC-I is successful, then the source ng-eNB calculates $K_{NG\text{-}RAN}$* using the target cell PCI, target EARFCN-DL and the K_{gNB}/NH in the current UE 5G AS security context based on either a horizontal key derivation or a vertical key derivation according to whether the source ng-eNB has an unused pair of {NCC, NH} as described in Annex A.12. The source ng-eNB can obtain the target PCI and target EARFCN-DL from a cell configuration database by means of the target Cell-ID which was received from the target ng-eNB. Then the source ng-eNB shall respond with an Xn-AP Retrieve UE Context Response message to the target ng-eNB including the UE context that contains the UE 5G AS security context. The UE 5G AS security context sent to the target ng-eNB shall include the newly derived $K_{NG\text{-}RAN}$*, the NCC associated to the $K_{NG\text{-}RAN}$*, the UE EPS security capabilities, UP security policy, the UP security activation status, and the ciphering and integrity algorithms used by the UE with the source cell.

The target ng-eNB shall check if it supports the ciphering and integrity algorithms the UE used with the last source cell. If the target ng-eNB does not support the ciphering and integrity algorithms used in the last source cell or if the target ng-eNB prefers to use different algorithms than the source ng-eNB, then the target ng-eNB shall send an RRC Setup

message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC_IDLE (i.e., a fallback procedure).

If the target ng-eNB supports the ciphering and integrity algorithms used with the last source cell and these algorithms are the chosen algorithms by the target ng-eNB, the target ng-eNB shall derive new AS keys (RRC integrity key, RRC encryption key and UP keys) using the algorithms the UE used with the source cell and the received $K_{NG\text{-}RAN}$*. The target ng-eNB shall reset all PDCP COUNTs to 0 and activate the new keys in PDCP layer. The target ng-eNB shall respond to the UE with an RRC Resume message on SRB1 which is integrity protected and ciphered in PDCP layer using the new RRC keys.

If the UP security activation status can be supported in the target ng-eNB, the target ng-eNB shall use the UP security activations that the UE used at the last source cell.

When the UE receives the RRC Resume message, the UE shall decrypt the message using the K_{RRCenc} that was derived based on the newly derived $K_{NG\text{-}RAN}$*. The UE shall also verify the RRC Resume message by verifying the PDCP MAC-I using the K_{RRCint} that was derived from the newly derived $K_{NG\text{-}RAN}$* If verification of the RRC Resume message is successful, the UE shall delete the current K_{RRCint} key and the UE shall save the K_{RRCint}, K_{RRCenc}, K_{UPenc} (optionally), and K_{UPint} (optionally) from the newly derived $K_{NG\text{-}RAN}$* as part of the UE current AS security context. In this case, the UE shall send the RRC Resume Complete message both integrity protected and ciphered to the target ng-eNB on SRB1 using the current K_{RRCint} and K_{RRCenc}. The UE shall use the UP security activations status to protect the UP data.

If the UE receives RRC Reject message from the target ng-eNB in response to the RRC Resume Request message, the UE shall delete newly derived AS keys used for connection resumption attempt, including newly derived $K_{NG\text{-}RAN}$*, newly derived RRC integrity key, RRC encryption key and UP keys, and keep the current K_{RRCint} and the K_{gNB}/NH in its current AS context. In that case, for the next resume to any target ng-eNB, the UE shall start with the same AS security context as it had when it was suspended originally, i.e., same K_{gNB}/NH shall act as base key for derivation of new $K_{NG\text{-}RAN}$*.

After a successful resume, the target ng-eNB shall perform Path Switch procedure with the AMF as is done in case of X2-handover. The AMF shall verify the UE security capability as described in the clause 6.7.3.1, and the SMF shall verify the UE's UP security policy as described in the clause 6.6.1.

When EDT or PUR feature is used, the UE shall use newly derived K_{UPenc} to encrypt the UL UP data according to the UP security activations before transmitting the RRC Resume Request message, and send the encrypted UL UP data in the PDCP layer with RRC Resume Request message to the target ng-eNB. The target ng-eNB shall use newly derived K_{UPenc} key to get the UL UP data according to the UP security activations after retrieving UE context from the source ng-eNB. The UE and the target eNB shall use the same K_{UPenc} key and UP security activation to protect the DL data (if included) in PDCP layer in the RRC Release or RRC Resume message.

NOTE: UP security policy is only applicable for UP ciphering as UP integrity protection is not supported.

6.16.2.4 Connection Resume in CM-IDLE with Suspend to the same ng-eNB

The target ng-eNB may be the same as the source ng-eNB in the description in the previous subclause. If so the single ng-eNB performs the roles of both the source and target ng-eNB. In particular, a new $K_{NG\text{-}RAN}$* shall be derived even if the UE is resuming to the same cell from where it was suspended. However, there is the following difference.

After a successful resume, the ng-eNB shall send N2 Resume Request message to the AMF. Upon reception of the N2 Resume Request message, the AMF shall check its local policy. If the local policy in the AMF indicates that a new NH derivation is needed, the AMF shall increase its locally kept NCC value by one and compute a fresh NH from its stored data using the function defined in Annex A.10. The AMF shall store that fresh pair and send it to the ng-eNB in the N2 Resume Response message.

Upon receipt of the N2 Resume Response message from the AMF and if the message includes a {NH, NCC} pair, the ng-eNB shall store the {NH, NCC} pair in the N2 Resume Response message and remove any existing unused stored {NH, NCC} pairs. The {NH, NCC} pair may be used in the next suspend/resume or Xn handover procedures.

6.16.3 Protection of Non-IP Data Delivery (NIDD) interfaces

Functions for NIDD may be used to handle Mobile Originated (MO) and Mobile Terminated (MT) communication with UEs, where the data used for the communication is considered unstructured (which is also referred as Non-IP).

Since the NEF exposes the NIDD API, TLS protection mechanism defined in clause 12 shall be used for protection of NIDD interfaces.

6.16.4 Security handling in NAS based redirection from 5GS to EPS

When a UE initiates registration procedure with the AMF, the AMF may redirect the UE from 5GC to EPC by including a EMM cause indicating to the UE that it shall not use 5GC, as described in clause 5.31.3 in TS 23.501 [2]. The following requirements apply to Registration Reject message with an EMM cause which indicates to the UE that the UE shall not use 5GC:

- the AMF shall only send such a Registration Reject message once NAS security has been established between the AMF and the UE; and
- the UE shall only act upon such Registration Reject message if received integrity protected and if UE has verified the integrity of the Registration Reject message successfully.

NOTE: This solution does not apply to unauthenticated emergency calls.

7 Security for non-3GPP access to the 5G core network

7.1 General

Security for untrusted non-3GPP access to the 5G Core network is achieved by a procedure using IKEv2 as defined in RFC 7296 [25] to set up one or more IPsec ESP [4] security associations. The role of IKE initiator (or client) is taken by the UE, and the role of IKE responder (or server) is taken by the N3IWF.

During this procedure, the AMF delivers a key K_{N3IWF} to the N3IWF. The AMF derives the key K_{N3IWF} from the key K_{AMF}. The key K_{N3IWF} is then used by UE and N3IWF to complete authentication within IKEv2.

Security for trusted non-3GPP access to 5G Core network is defined in clause 7A.

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

Whether a non-3GPP IP access network is trusted or untrusted is not a characteristic of the access network.

In non-roaming scenario it is the HPLMN's operator decision if a non-3GPP IP access network is used as trusted or untrusted non-3GPP access Network. When one or more of the security feature groups provided by the non-3GPP access network are considered not sufficiently secure by the home operator, the non-3GPP access may be identified as an untrusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

In roaming scenario, the UDM in HPLMN makes the final decision of whether a non-3GPP IP access network is used as trusted or untrusted non-3GPP access network based on the identities of the access network and the visited network. The UDM may take the VPLMN's policy and capability returned from the AMF or roaming agreement into account

For supporting multiple DNs, the same trust relationship shall apply to all the DNs the UE connects to from a certain non-3GPP access network, i.e. it shall not be possible to access one DN using the non-3GPP access network as trusted, while access to another DN using the same non-3GPP access network as untrusted.

7.1a Determining trust relationship in the UE

There are various possibilities to determine the trust relationship in the UE as it is described in TS 23.501 [2]. For example, the non-3GPP access networks, which are trusted, can be pre-configured in the UE. If the USIM supports non-3GPP access networks service, the home network operator may configure in the USIM a list of trusted non-3GPP access networks. In case of pre-configured information in the UE, the list of trusted non-3GPP access networks pre-

configured by the home network operator in the USIM shall take precedence over information pre-configured in the ME.

7.2 Security procedures

7.2.1 Authentication for Untrusted non-3GPP Access

This clause specifies how a UE is authenticated to 5G network via an untrusted non-3GPP access network. It uses a vendor-specific EAP method called "EAP-5G", utilizing the "Expanded" EAP type and the existing 3GPP Vendor-Id, registered with IANA under the SMI Private Enterprise Code registry. The "EAP-5G" method is used between the UE and the N3IWF and is utilized for encapsulating NAS messages. If the UE needs to be authenticated by the 3GPP home network, any of the authentication methods as described in clause 6.1.3 can be used. The method is executed between the UE and AUSF as shown below.

When possible, the UE shall be authenticated by reusing the existing UE NAS security context in AMF.

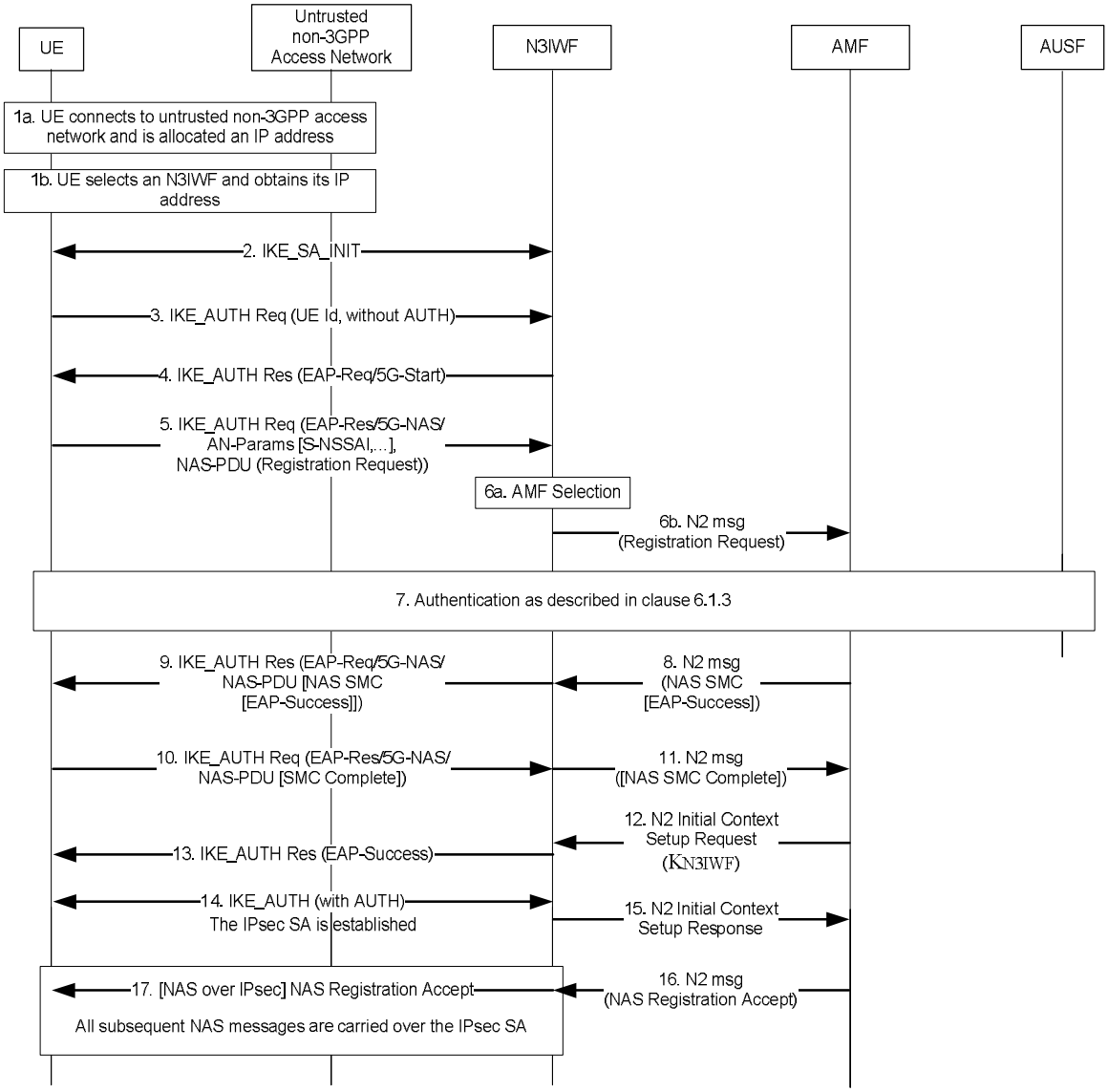


Figure 7.2.1-1: Authentication for untrusted non-3GPP access

1. The UE connects to an untrusted non-3GPP access network with procedures outside the scope of 3GPP. When the UE decides to attach to 5GC network, the UE selects an N3IWF in a 5G PLMN, as described in TS 23.501 [2] clause 6.3.6.

2. The UE proceeds with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange according to RFC 7296 [25]. After step 2 all subsequent IKE messages are encrypted and integrity protected by using the IKE SA established in this step.

3. The UE shall initiate an IKE_AUTH exchange by sending an IKE_AUTH request message. The AUTH payload is not included in the IKE_AUTH request message, which indicates that the IKE_AUTH exchange shall use EAP signalling (in this case EAP-5G signalling). As per the RFC 7296 [25], in the IDi the UE shall set the ID type as ID_KEY-ID in this message and set its value equal to any random number. The UE shall not use its GUTI/SUCI/SUPI as the Id in this step. If the UE is provisioned with the N3IWF root certificate, it shall include the CERTREQ payload within the IKE_AUTH request message to request N3IWF's certificate.

4. The N3IWF responds with an IKE_AUTH response message which includes the N3IWF identity, the AUTH payload to protect the previous message it sent to the UE (in the IKE_SA_INIT exchange) and an EAP-Request/5G-Start packet. The EAP-Request/5G-Start packet informs the UE to initiate an EAP-5G session, i.e. to start sending NAS messages encapsulated within EAP-5G packets. If the UE has sent a CERTREQ payload in step 3, the N3IWF shall also include the CERT payload including N3IWF certificate.

5. The UE shall validate the N3IWF certificate and shall confirm that the N3IWF identity matches the N3IWF selected by the UE. An absence of the certificate from the N3IWF if the UE had requested the certificate or unsuccessful identity confirmation shall result in a connection failure. The UE shall send an IKE_AUTH request which includes an EAP-Response/5G-NAS packet that contains a Registration Request message containing UE security capabilities and the SUCI. If UE is already with the 5GC over 3GPP access and there is an available security context, the UE shall integrity protect the Registration Request message and shall send the 5G-GUTI instead of SUCI. The N3IWF shall refrain from sending an EAP-Identity request. The UE may ignore an EAP Identity request or respond with the SUCI it sent in the Registration Request. If the UE has registrated to the same AMF through 3GPP access, and if this is the first time that the UE connects to the 5GC through non-3GPP access, the value of corresponding UL NAS COUNT used for integrity protection is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity protection

NOTE: The N3IWF does not send an EAP-Identity request because the UE includes its identity in the IKE_AUTH request in message 5. This is in line with RFC 7296 [25], clause 3.16.

6. The N3IWF shall select an AMF as specified in TS 23.501 [2], clause 6.5.3. The N3IWF forwards the Registration Request received from the UE to the AMF.

7. If the AMF receives a 5G-GUTI and the Registration is integrity protected, it may use the security context to verify the integrity protection as describe in clause 6.4.6. If the UE has registrated to the same AMF through 3GPP access, and if this is the first time that the AMF receives UE's NAS signalling through non-3GPP access, the value of corresponding UL NAS COUNT used for integrity verification is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity verification. If integrity is verified successfully, it indicates that UE is authenticated by AMF.If integrity is verified successfully and no newer security context has been activated over the 3GPP access, then step 8 to step 11 may be skipped. If integrity is verified successfully and a newer security context has been activated over the 3GPP access then authentication may be skipped but the AMF shall activate the newer context with a NAS SMC procedure as described in step 8 and onwards. Otherwise, the AMF shall authenticate the UE.

   If the AMF decides to authenticate the UE, it shall use one of the methods from clause 6.1.3. In this case, the AMF shall send a key request to the AUSF. The AUSF may initiate an authentication procedure as specified in clause 6.1.3. Between AMF and UE, the authentication packets are encapsulated within NAS authentication messages and the NAS authentication messages are carried in N2 signalling between the AMF and N3IWF, and then are encapsulated within EAP-5G/5G-NAS packets between the N3IWF and the UE.

   In the final authentication message from the home network, the AUSF shall send the anchor key K_{SEAF} derived from K_{AUSF} to the SEAF. The SEAF shall derive the K_{AMF} from K_{SEAF} and send it to the AMF which is used by the AMF to derive NAS security keys. If EAP-AKA' is used for authentication as described in clause 6.1.3.1, then the AUSF shall include the EAP-Success. The UE also derives the anchor key K_{SEAF} and from that key it derives the K_{AMF} followed by NAS security keys. The NAS COUNTs associated with NAS connection identifier "0x02" are set at the UE and AMF.

8. The AMF shall send a Security Mode Command (SMC) to the UE in order to activate NAS security associated with NAS connection identifier "0x02". This message is first sent to N3IWF (within an N2 message). If EAP-AKA' is used for authentication, the AMF shall encapsulate the EAP-Success received from AUSF within the SMC message.

9. The N3IWF shall forward the NAS SMC to UE within an EAP-Request/5G-NAS packet.

10. The UE completes the authentication (if initiated in step 7) and creates a NAS security context or activates another one based on the received ngKSI in the NAS SMC. UE shall respond to the NAS SMC it received from the AMF based on the selected algorithms and parameters as described in clause 6.7.2. The UE shall encapsulate the NAS SMC Complete in the EAP-5G Response.

11. The N3IWF shall forward the NAS packet containing NAS SMC Complete to the AMF over the N2 interface.

12. The AMF upon reception of the NAS SMC Complete from the UE or upon success of integrity protection verification, initiates the NGAP procedure to set up the AN context. AMF shall compute the N3IWF key, K_{N3IWF}, using the uplink NAS COUNT associated with NAS connection identifier "0x02" as defined in Annex A.9 for the establishment of the IPsec SA between the UE and the N3IWF and shall include it in the NGAP Initial Context Setup Request sent to the N3IWF.

13. N3IWF sends an EAP-Success/EAP-5G to the UE upon reception of the NGAP Initial Context Setup Request containing the N3IWF key, KN3IWF. This completes the EAP-5G session and no further EAP-5G packets are exchanged. If the N3IWF does not receive the K_{N3IWF} from AMF, the N3IWF shall respond with an EAP-Failure

14. The IPsec SA is established between the UE and N3IWF by using the N3IWF key K_{N3IWF} that was created in the UE using the uplink NAS COUNT associated with NAS connection identifier "0x02" as defined in Annex A.9 and was received by N3IWF from the AMF in step 12.

15. Upon successful establishment of the IPsec SA between the UE and the N3IWF, the N3IWF shall send the NGAP Initial Context Setup Response message to the AMF.

16. When NGAP Initial Context Setup Response for the UE is received by the AMF, AMF shall send the NAS Registration Accept message for the UE over the N2 towards the N3IWF.

17. Upon receiving the NAS Registration Accept message from the AMF, the N3IWF shall forward it to the UE over the established IPsec SA. All further NAS messages between the UE and the N3IWF shall be sent over the established IPsec SA.

7A Security for trusted non-3GPP access to the 5G core network

7A.1 General

Security for trusted non-3GPP access to the 5G Core network is achieved when the UE registers to the 5GC via the TNAN. The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-5G procedure, similar to the one used with the registration procedure for untrusted non-3GPP access.

The link between the UE and the TNAN can be any data link (L2) that supports EAP encapsulation. The requirement on the Ta interface between the TNAP and TNGF can be found in clause 4.2.8.3.2 of TS 23.501[2]. The TNGF terminates the EAP-5G signalling andfowards the NAS message to the 5GC when the UE attempts to register to 5GC via the TNAN. The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling. However, integrity protection would be provided.

NOTE: The encryption protection over Layer-2 between UE and TNAP is assumed to be enabled.

Separate IPSec SAs may be used for NAS transport and PDU Sessions. At the end of the UE's registration to 5GC, an IPSec SA (NWt) is established between the UE and TNGF. This is used to protect NAS messages between the UE and TNGF. Later when the UE initiates a PDU session establishment, the TNGF initiates establishment of one or more

IPSec child SAs per PDU session. This results in additional IPSec SA's (NWt) to be setup between the UE and TNGF-UP which are then for user plane transport between the two.

Clause 7A.2.4 describes how WLAN UEs that do not support 5GC NAS (N5CW) register via trusted non-3GPP access. Those N5CW devices are able to authenticate to the network with 3GPP credentials and register with the help of an interworking function (TWIF) that provides the 5GC NAS protocol stack towards the AMF.

As defined in clause 7.1, it is the home operator policy decision if a non-3GPP access network is treated as trusted non-3GPP access network. When all of the security domains in clause 4.1 of the present specification related to the non-3GPP access network are considered sufficiently secure by the home operator, the non-3GPP access may be identified as a trusted non-3GPP access for that operator. However, this policy decision may additionally be based on reasons not related to security feature groups.

NOTE: It is specified in clause 7.1a of the current document how the UE gets the operator policy and how it will behave accordingly.

7A.2 Security procedures

7A.2.1 Authentication for trusted non-3GPP access

This clause specifies how a UE is authenticated to 5G network via a trusted non-3GPP access network.

This is based on the specified procedure in TS 23.502 [8] clause 4.12a.2.2 "Registration procedure for trusted non-3GPP access". The authentication procedure is similar to the authentication procedure for trusted non-3GPP access defined in clause 7.2.1 with few differences, which are mentioned below:

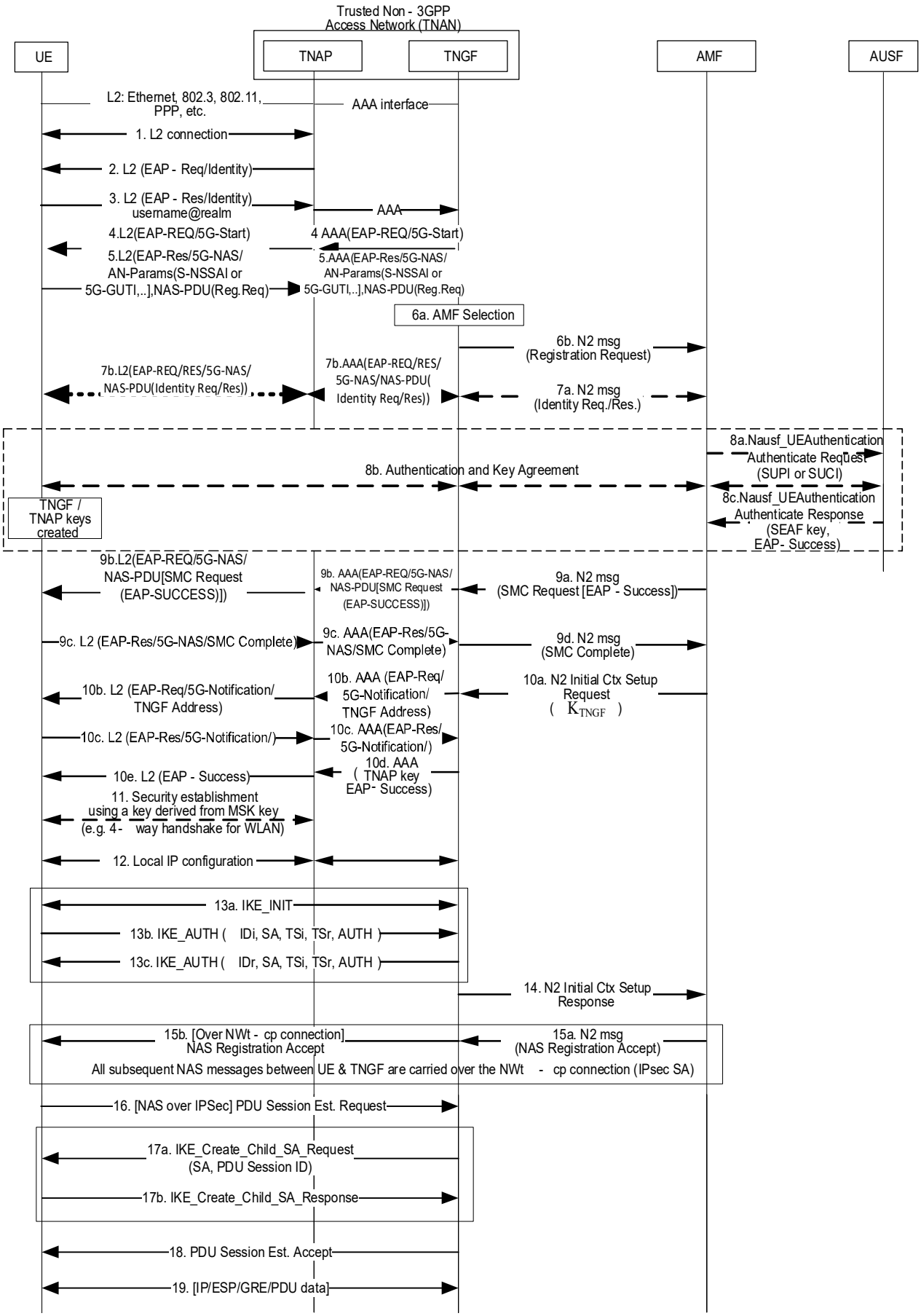

Trusted Non - 3GPP Access Network (TNAN)
UE
TNAP
TNGF
AMF
AUSF
L2: Ethernet, 802.3, 802.11, PPP, etc.
AAA interface
1. L2 connection
2. L2 (EAP - Req/Identity)
3. L2 (EAP - Res/Identity) username@realm
AAA
4.L2(EAP-REQ/5G-Start)
4 AAA(EAP-REQ/5G-Start)
5.L2(EAP-Res/5G-NAS/ AN-Params(S-NSSAI or 5G-GUTI,..],NAS-PDU(Reg.Req)
5.AAA(EAP-Res/5G-NAS/ AN-Params(S-NSSAI or 5G-GUTI,..],NAS-PDU(Reg.Req)
6a. AMF Selection
6b. N2 msg (Registration Request)
7b.L2(EAP-REQ/RES/5G-NAS/ NAS-PDU(Identity Req/Res))
7b.AAA(EAP-REQ/RES/ 5G-NAS/NAS-PDU(Identity Req/Res))
7a. N2 msg (Identity Req./Res.)
8a.Nausf_UEAuthentication Authenticate Request (SUPI or SUCI)
8b. Authentication and Key Agreement
8c.Nausf_UEAuthentication Authenticate Response (SEAF key, EAP- Success)
TNGF / TNAP keys created
9b.L2(EAP-REQ/5G-NAS/ NAS-PDU[SMC Request (EAP-SUCCESS)])
9b. AAA(EAP-REQ/5G-NAS/ NAS-PDU[SMC Request (EAP-SUCCESS)])
9a. N2 msg (SMC Request [EAP - Success])
9c. L2 (EAP-Res/5G-NAS/SMC Complete)
9c. AAA(EAP-Res/5G-NAS/SMC Complete)
9d. N2 msg (SMC Complete)
10b. L2 (EAP-Req/5G-Notification/ TNGF Address)
10b. AAA (EAP-Req/ 5G-Notification/ TNGF Address)
10a. N2 Initial Ctx Setup Request (K-TNGF)
10c. L2 (EAP-Res/5G-Notification/)
10c. AAA(EAP-Res/ 5G-Notification/)
10d. AAA (TNAP key EAP- Success)
10e. L2 (EAP - Success)
11. Security establishment using a key derived from MSK key (e.g. 4- way handshake for WLAN)
12. Local IP configuration
13a. IKE_INIT
13b. IKE_AUTH (IDi, SA, TSi, TSr, AUTH)
13c. IKE_AUTH (IDr, SA, TSi, TSr, AUTH)
14. N2 Initial Ctx Setup Response
15b. [Over NWt - cp connection] NAS Registration Accept
15a. N2 msg (NAS Registration Accept)
All subsequent NAS messages between UE & TNGF are carried over the NWt - cp connection (IPsec SA)
16. [NAS over IPSec] PDU Session Est. Request
17a. IKE_Create_Child_SA_Request (SA, PDU Session ID)
17b. IKE_Create_Child_SA_Response
18. PDU Session Est. Accept
19. [IP/ESP/GRE/PDU data]

Figure 7A.2.1-1: Registration \ Authentication and PDU Session establishment for trusted non-3GPP access

0. The UE selects a PLMN and a TNAN for connecting to this PLMN by using the Trusted Non-3GPP Access Network selection procedure specified in TS 23.501 [2] clause 6.3.12. During this procedure, the UE discovers the PLMNs with which the TNAN supports trusted connectivity (e.g. "5G connectivity").

1. A layer-2 connection is established between the UE and the TNAP. In case of IEEE 802.11 [80], this step corresponds to an 802.11 [80] Association. In case of PPP, this step corresponds to a PPP LCP negotiation. In other types of non-3GPP access (e.g. Ethernet), this step may not be required.

2-3. An EAP authentication procedure is initiated. EAP messages shall be encapsulated into layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc. The UE provides a NAI that triggers the TNAP to send an AAA request to a TNGF. Between the TNAP and TNGF the EAP packets are encapsulated into AAA messages.

4-10. An EAP-5G procedure is executed as specified in clause 7.2.1with the following modifications:

- The EAP-5G packets shall not be encapsulated into IKEv2 packets. The UE shall also include a UE Id in the AN parameters, e.g. a 5G-GUTI if available from a prior registration to the same PLMN.

- A K_{TNGF} as specified in clause Annex A.9 (equivalent to K_{N3IWF}) is created in the UE and in the AMF after the successful authentication. The K_{TNGF} is transferred from the AMF to TNGF in step 10a (within the N2 Initial Context Setup Request).

- The TNAP is a trusted entity. The TNGF shall generate the K_{TNAP} as specified in Annex A.22 and transfers it from TNGF to TNAP in step 10b (within an AAA message).

- After receiving the TNGF key from AMF in step 10a, the TNGF shall send to UE an EAP-Request/5G-Notification packet containing the "TNGF Contact Info", which includes the IP address of TNGF. After receiving an EAP-Response/5G-Notification packet from the UE, the TNGF shall send message 10d containing the EAP-Success packet.

11. The common TNAP key is used by the UE and TNAP to derive security keys according to the applied non-3GPP technology and to establish a security association to protect all subsequent traffic. In case of IEEE 802.11 [80], the K_{TNAP} is the Pairwise Master Key (PMK) and a 4-way handshake is executed (see IEEE 802.11 [80]) which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air. All messages between UE and TNAP are encrypted and integrity protected from this step onwards.

NOTE 1: whether step 11 is performed out of the scope of this document. The current procedure assumes the encryption protection over Layer-2 between UE and TNAP is to be enabled.

12. The UE receives IP configuration from the TNAN, e.g. with DHCP.

13. The UE shall initiate an IKE_INIT exchange with the TNGF. The UE has received the IP address of TNGF during the EAP-5G signalling in step 9b, subsequently, the UE shall initiate an IKE_AUTH exchange and shall include the same UE Id (i.e. SUCI or 5G-GUTI) as in the UE Id provided in step 5. The common K_{TIPSe} is used for mutual authentication. The key K_{TIPSec} is derived as specified in Annex A.22.NULL encryption is negotiated as specified in RFC 2410 [81]. After step 13c, an IPsec SA is established between the UE and TNGF (i.e. a NWt connection) and it is used to transfer all subsequent NAS messages. This IPsec SA does not apply encryption but only apply integrity protection.

14. After the NWtp connection is successfully established, the TNGF responds to AMF with an N2 Initial Context Setup Response message.

15. Finally, the NAS Registration Accept message is sent by the AMF and is forwarded to UE via the established NWt connection.

16-18. The UE initiates a PDU session establishment. This is carried out exactly as specified in TS 23.502 [8] clause 4.12a.5. The TNGF may establish one or more IPSec child SA's per PDU session.

19. User plane data for the established PDU session is transported between the UE and TNGF inside the established IPSec child SA.

7A.2.2 Void

7A.2.3 Key hierarchy for trusted non-3GPP access

The key hierarchy described in clause 6.2.1 applies, with the following changes:

The key derived for non-3GPP access is called K_{TNGF} in the context of trusted access.

The key K_{TNGF} received from AMF is used for two different purposes; to setup IPSec SAs between the UE and the TNGF and to create WLAN keys between the UE and the TNAP.

To separate the keys for these purposes, the key hierarchy in Figure 7A.2.3-1 shall be used. The K_{TIPSec} key is used to setup IPSec SAs and the K_{TNAP} key is used to setup access security.

The keys K_{TIPSec} and K_{TNAP} are derived as described in Clause A.22.

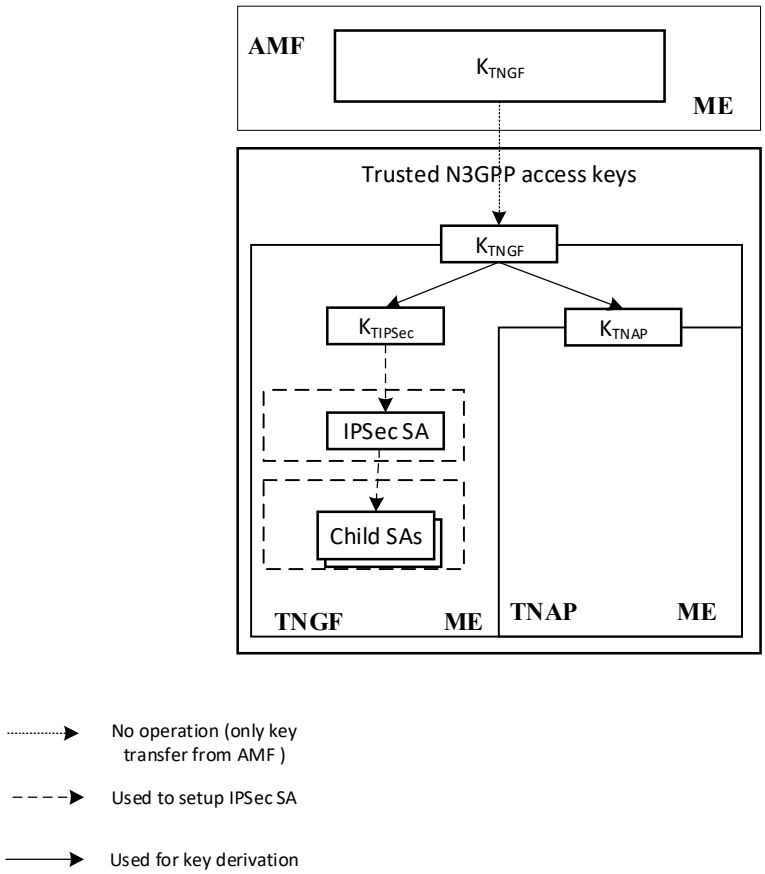


Figure 7A.2.3-1 Key hierarchy for trusted non-3GPP access

7A.2.4 Authentication for devices that do not support 5GC NAS over WLAN access

A N5CW device is capable to register to 5GC with 3GPP credentials and to establish 5GC connectivity via a trusted WLAN access network. The reference architecture is captured in clause 4.2.8.5.2 of TS 23.501[2]. The 3GPP credentials are stored as defined in clause 6.1.1.1. The Trusted WLAN Interworking Function (TWIF) provides interworking functionality that enables connectivity with 5GC and implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device. A single EAP-AKA' authentication procedure is executed for connecting the N5CW device both to the trusted WLAN access network and to the 5G core network.

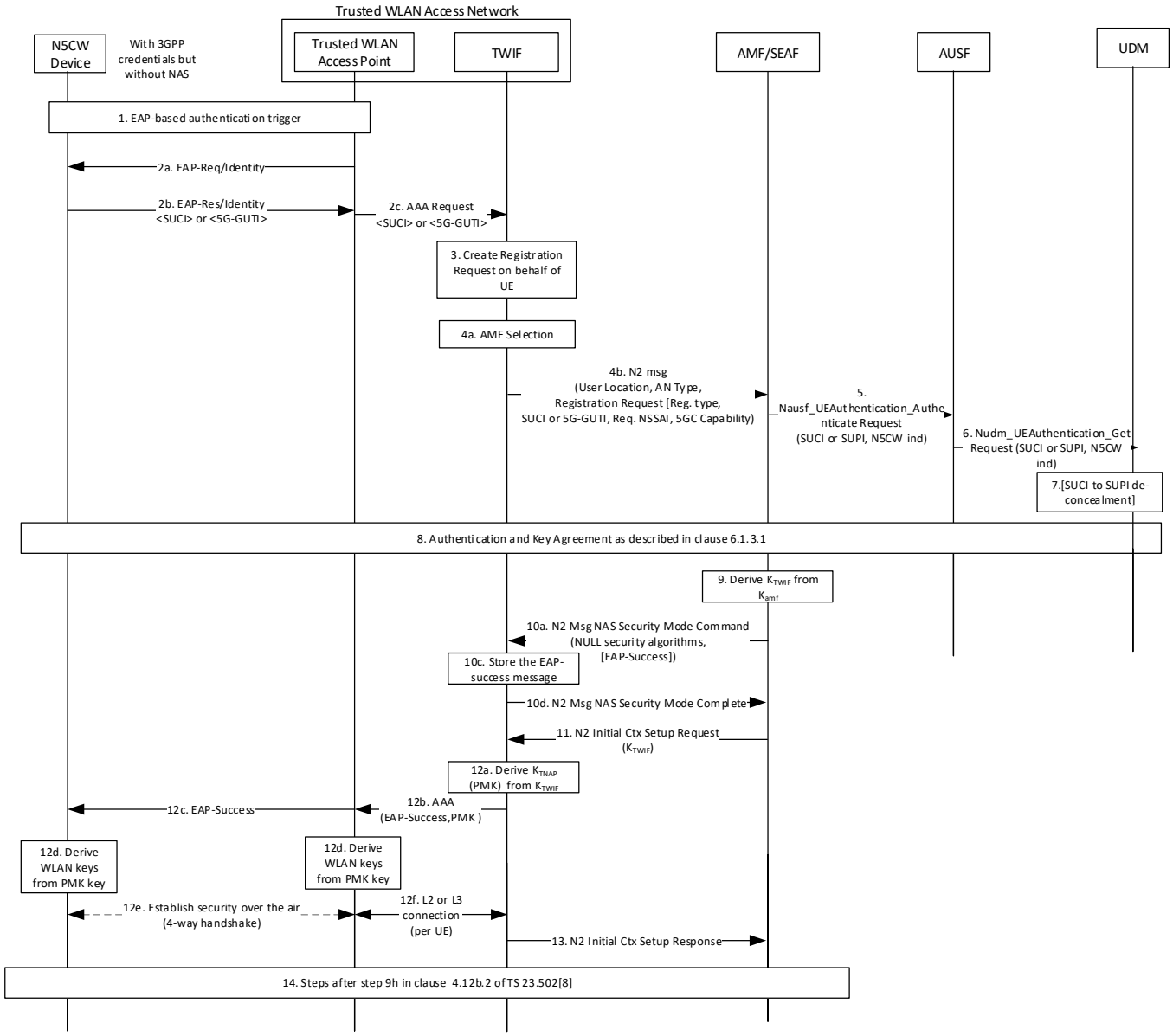


Figure 7A.2.4-1: Authentication Procedure for N5CW

0. The N5CW device selects a PLMN and a trusted WLAN that supports "5G connectivity-without-NAS" to this PLMN by using the procedure specified in TS 23.501 [2] clause 6.3.12a, "Access Network selection for devices that do not support 5GC NAS over WLAN".

Steps 1-10: Initial registration to 5GC.

1. The N5CW device associates with the trusted WLAN network and the EAP-AKA' authentication procedure is initiated.

2. The N5CW device shall provide its Network Access Identity (NAI) The Trusted WLAN Access Point (TWAP) selects a Trusted WLAN Interworking Function (TWIF), e.g. based on the received realm, and sends an AAA request to the selected TWIF.

   If the N5CW device registers to 5GC over 3GPP access for the first time when the above procedure is initiated, then the NAI shall include the SUCI. The SUCI shall be constructed as specified in clause 6.12.2.

If the N5CW device has registered to 5GC over 3GPP access when the above procedure is initiated, then the NAI includes the 5G-GUTI assigned to the N5CW device over 3GPP access. This enables the TWIF in step 4a below to select the same AMF as the one serving the N5CW device over 3GPP access.

3. The TWIF shall create a 5GC Registration Request message on behalf of the N5CW device. The TWIF shall use default values to populate the parameters in the Registration Request message, which are the same for all N5CW devices that do not support 5G NAS. The Registration type indicates "Initial Registration".

4. The TWIF shall select an AMF (e.g. by using the 5G-GUTI in the NAI, if provided by the N5CW device) and shall send an N2 message to the AMF including the Registration Request, the User Location and an AN Type.

5. In case the AMF triggers an authentication procedure, it sends a request to AUSF by sending Nausf_UEAuthentication_Authenticate Request message. The Nausf_UEAuthentication_Authenticate Request message contains SUCI or SUPI (in case of a valid 5G-GUTI is received by the AMF). The request message contains also an indication that the request is from a N5CW device.

   Even if the AMF already has a security context identified by 5G-GUTI, the AMF shall initiate the primary authentication.

NOTE 1: To avoid key stream reuse when deriving K_{TWIF} from K_{AMF}, the K_{AMF} always needs to be refreshed by a renewed primary authentication.

6. The AUSF shall send Nudm_UEAuthentication_Get Request to the UDM including SUCI or SUPI and the N5CW indication.

7. Upon reception of the Nudm_UEAuthentication_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. The UDM may select an authentication method based on the "realm" part of the SUPI, the N5CW device indicator, a combination of the "realm" part and the N5CW device indicator, or the UDM local policy.

8. The EAP-AKA' procedure will be trigged to perform mutual authentication between the N5CW device and the home network as specified in clause 6.1.3.1.

   EAP-AKA' takes place between the N5CW device and AUSF. Over the N2 interface, the EAP messages are encapsulated within NAS Authentication messages. The EAP-AKA' messages exchanged between the N5CW Device and the TWIF shall be encapsulated into the layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc.

9. The NAS security context is not required in this scenario. The AMF shall derive an K_{TWIF} key from the received K_{AMF} key as specified in Annex A.9. NAS security between AMF and TWIF is established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

NOTE 2: N5CW device does not support NAS; therefore, using the NAS counter is not possible on N5CW device.

10a. The AMF shall send NAS Security Mode Command to the TWIF. The NAS Security Mode Command shall contain the EAP-Success message and the NULL security algorithms.

10b. The TWIF shall not forward the EAP-Success to the N5CW directly, instead, it shall store the EAP-Success message and wait for K_{TWIF}.

10c. The TWIF shall send the NAS Security Mode Complete message to the AMF.

11. The AMF sends an N2 Initial Context Setup Request and provides the K_{TWIF} key to TWIF.

12. The TWIF shall derive a TNAP key, K_{TNAP}, from the K_{TWIF} key as specified in Appendix A.22 and send the TNAP key and the EAP-Success message to the Trusted WLAN Access Point, which forwards the EAP-Success to the N5CW device. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication according to IEEE 802.11 [80]. A layer-2 or layer-3 connection is established between the Trusted WLAN Access Point and the TWIF for transporting all user-plane traffic of the N5CW device to TWIF. This connection is later bound to an N3 connection that is created for this N5CW device.

13. The TWIF shall send N2 Initial Context Setup Response message to the AMF.

14. The following steps are captured in clause 4.12b.2 of TS 23.502[8].

7B Security for wireline access to the 5G core network

7B.1 General

To support Wireless and Wireline Convergence for the 5G system, two new network entities, 5G-RG and FN-RG, are introduced in the architecture specificaction TS 23.501[2].

The 5G-RG acts as a 5G UE and can connect to 5GC via wireline access network (W-5GAN) or via Fixed Wireless Access (FWA). Existing security procedures defined in this document are reused.

The FN-RG can connect to 5GC via wireline access network (W-5GAN). The W-AGF performs the registration procedure on behalf of the FN-RG. It acts as end point of N1 and provides the NAS signalling connection to the 5GC on behalf of the FN-RG.

A 5G -capable UE can connect to 5GC through an RG that's connected to the 5GC via wireline access network (W-5GAN) or NG-RAN. The UE supports untrusted non-3GPP access and/or trusted non-3GPP access.

NOTE: Roaming of FN-RG and 5G-RG are not supported.

NOTE: Informative Annex X provides an example of how N5GC devices behind a residential gateway in private or in isolated scenarios with wireline access make use of additional EAP methods for authentication.

7B.2 Authentication for 5G-RG

The 5G-RG can be connected to 5GC via W-5GAN, NG RAN or via both accesses. The registration procedure for the 5G-RG connecting to 5GC via NG-RAN is specified in TS 23.316 [79] clause 4.11. The registration procedure for the 5G-RG connecting to 5GC via W-5GAN is specified in TS 23.316 [79] clause 7.2.1.

The Untrusted non-3GPP access procedure defined in clause 7.2.1 is used as the basis for registration of the 5G-RG. The 5G-RG shall support both 5G-AKA and EAP-AKA' and it shall be authenticated by the 3GPP home network. The 5G-RG is equivalent to a normal UE.

As 5G-RG is a UE from 5GC point of view, the authentication framework defined in clause 6.1.3 shall be used to authenticate the 5G-RG.

In case of 5G-RG connects to 5GC via 5G-RAN, comparing to clause 6.1, the difference is:

- UE is replaced by 5G-RG.

In case of 5G-RG connects to 5GC via W-5GAN, a W-CP protocol stack message shall be used between the 5G-RG and the W-5GAN for encapsulating NAS message. The authentication method is executed between the 5G-RG and AUSF as shown below.

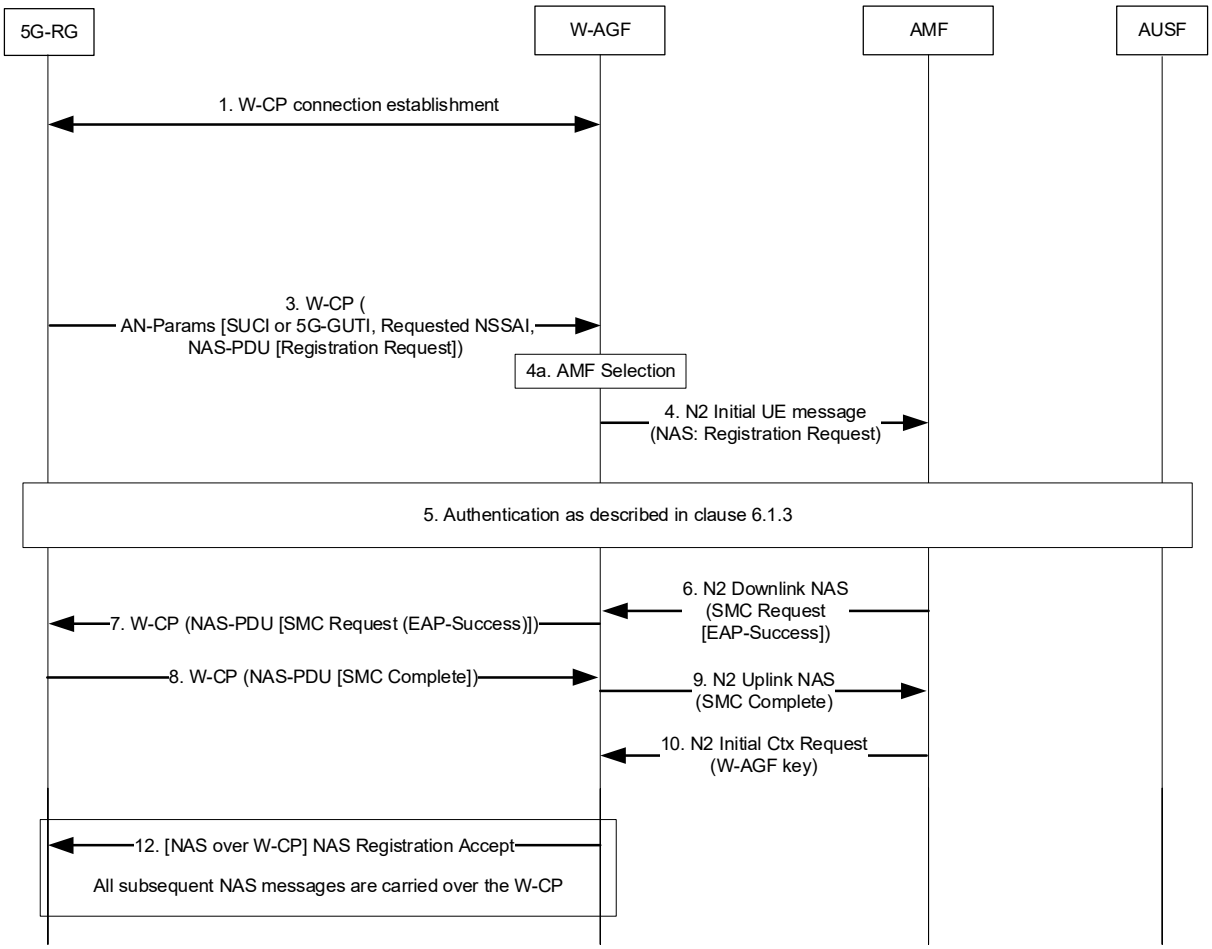


Figure 7B.2-1 5G-RG authentication procedure

1. 5G-RG establishes a W-CP connection with a W-5GAN. The detail of connection is out of the scope of 3GPP.

2. (void)

3. The 5G-RG shall send a message using W-CP protocol stack that contains a Registration message containing UE security capabilities and the SUCI. If there is an available security context, the 5G-RG shall integrity protect the Registration Request message and shall send the 5G-GUTI instead of SUCI. If the 5G-RG has registered to the same AMF through NG RAN, and if this is the first time that the 5G-RG connects to the 5GC throughW-5GAN, the value of corresponding UL NAS COUNT used for integrity protection is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity protection.

NOTE: Since the 5G-RG will not use non-3GPP access, and to avoid to create new category of security context, so the non-3GPP specific security context is used to refer to the security context that 5G-RG is used through wireline access.

4. The W-AGF shall select an AMF as specified in TS 23.316[79]. The W-AGF shall then forward the Registration Request received from the UE to the selected AMF within an N2 initial UE message

5. If the AMF receives a 5G-GUTI and the Registration is integrity protected, it may use the security context to verify the integrity protection as describe in clause 6.4.6. If the 5G-RG has registered to the same AMF through NG RAN, and if this is the first time that the AMF receives UE's NAS signalling through wireline access, the value of corresponding UL NAS COUNT used for integrity verification is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity verification. If integrity is verified successfully, it indicates that 5G-RG is authenticated by AMF. If integrity is verified successfully and no newer security context has been activated over the NG RAN, then step 8 to step 11 may be skipped. If integrity is verified successfully and a newer security context has been activated over the NG RAN then authentication may be skipped but the AMF

shall activate the newer context with a NAS SMC procedure as described in step 8 and onwards. Otherwise, the AMF shall authenticate the 5G-RG.

If the AMF decides to authenticate the 5G-RG, it shall use one of the methods from clause 6.1.3. In this case, the AMF shall send a key request to the AUSF. The AUSF may initiate an authentication procedure as specified in clause 6.1.3. Between AMF and UE (5G-RG), the authentication packets are encapsulated within NAS authentication messages and the NAS authentication messages are carried in N2 signalling between the AMF and W-AGF, and then are encapsulated using W-CP protocol stack message between the W-AGF and the UE (5G-RG).

In the final authentication message from the home network, the AUSF shall send the anchor key K_{SEAF} derived from K_{AUSF} to the SEAF. The SEAF shall derive the K_{AMF} from K_{SEAF} and send it to the AMF which is used by the AMF to derive NAS security keys. If EAP-AKA' is used for authentication as described in clause 6.1.3.1, then the AUSF shall include the EAP-Success. The 5G-RG also derives the anchor key K_{SEAF} and from that key it derives the K_{AMF} followed by NAS security keys. The NAS COUNTs associated with NAS connection identifier "0x02" are set at the 5G-RG and AMF.

6. The AMF shall send a Security Mode Command (SMC) to the UE (5G-RG) in order to activate NAS security associated with NAS connection identifier "0x02". This message is first sent to W-AGF (within an N2 message). If EAP-AKA' is used for authentication, the AMF shall encapsulate the EAP-Success received from AUSF within the SMC message.

7. The W-AGF shall forward the NAS SMC to 5G-RG.

8. The W-AGF shall forward the NAS packet containing NAS SMC Complete to the AMF over the N2 interface.

9. The AMF upon reception of the NAS SMC Complete from the UE (5G-RG) or upon success of integrity protection verification, initiates the NGAP procedure to set up the AN context. AMF shall compute the W-AGF key, K_{WAGF} that is an equivalent to key K_{N3IWF}, using the uplink NAS COUNT associated with NAS connection identifier "0x02" as defined in Annex A.9.

10. Upon receiving NAS Security Mode Complete, the AMF shall send an N2 Initial Context Setup Request message to the W-AGF. The message contains the $K_{WAGF.}$

NOTE: Whether the key K_{WAGF} is used by the 5G-RG and W-AGF is out of the scope of 3GPP.

11. (void)

12. Upon receiving the NAS Registration Accept message from the AMF, the W-AGF shall forward it to the 5G-RG over the established W-CP. All further NAS messages between the UE and the W-AGF shall be sent over the established W-CP.

7B.3 Authentication for FN-RG

The FN-RG connects to 5GC via W-5GAN, which has the W-AGF function that provides connectivity to the 5GC via N2 and N3 reference points. Since the FN-RG is a non-wireless entity defined by BBF or CableLabs, it doesn't support N1. The W-AGF provides N1 connectivity on behalf of the FN-RG. The authentication method is executed between the FN-RG and AUSF as shown in Figure 7B.c.

The W-AGF may authenticate the FN-RG; this is controlled by local policies.

It is assumed that there is a trust relationship between the wireline operator that manages the W-5GAN and the PLMN operator managing the 5GC. The AMF trusts the W-5GAN based on mutual authentication executed when security is established on the interface between the two using NDS/IP or DTLS.

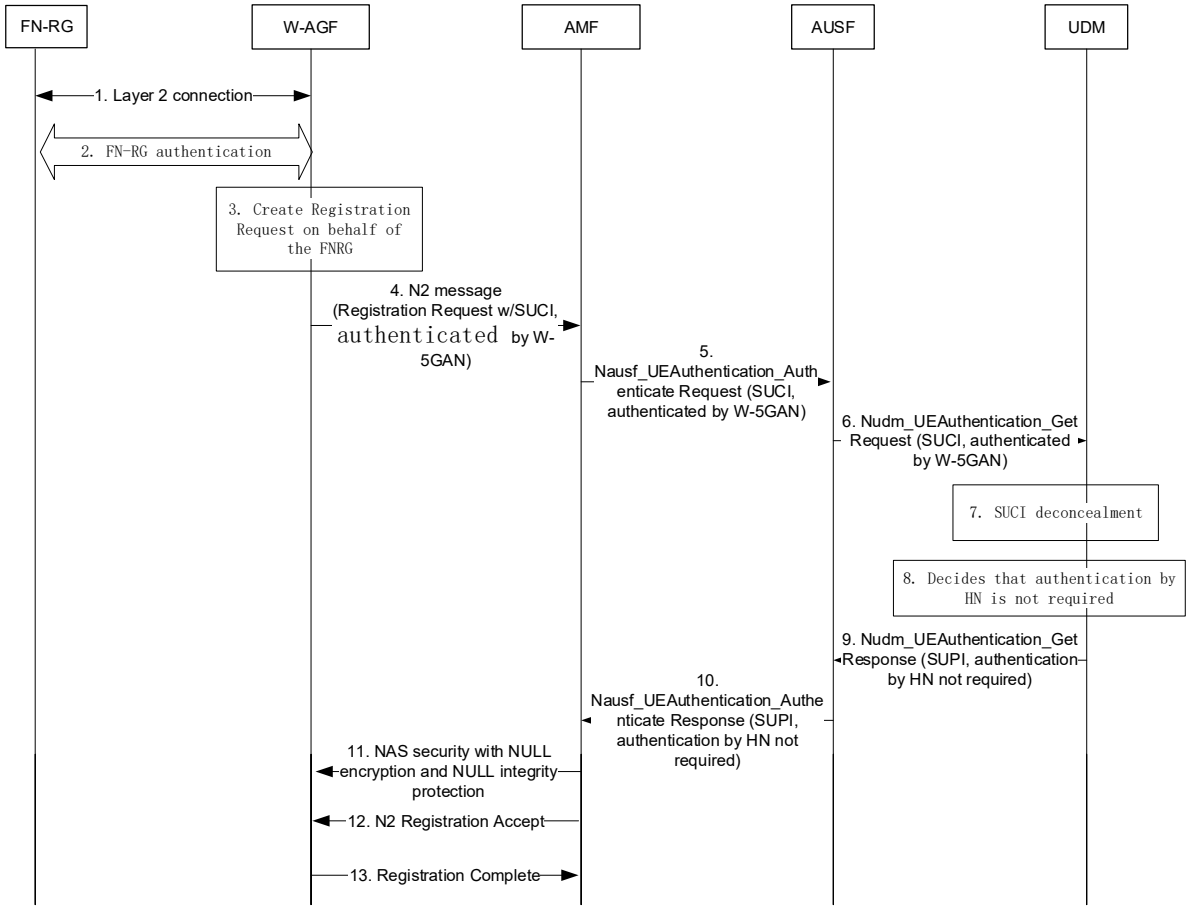


Figure7B.c FN-RG authentication procedure

1. A layer-2 (L2) connection is established between the FN-RG and the FAGF function in the W-AGF.

2. The FN-RG is authenticated by the W-AGF. Authentication method used for FN-RG is defined by BBF or CableLabs and out of scope of 3GPP.

3-4. The W-AGF shall perform initial registration on behalf of the FN-RG. The W-AGF shall generate a Registration Request message and send it to the AMF over N2. The Registration Request message contains the SUCI of the FN-RG. The N2 message contains an indication that the W-AGF has authenticated the FN-RG.

5. The AMF shall select an AUSF based on the received SUCI. The AMF shall send a Nausf_UEAuthentication_Authenticate Request message to the AUSF. It contains the SUCI of the FN-RG. It also contains the authenticated indication generated by the W-AGF.

6. The AUSF shall send a Nudm_UEAuthentication_Get Request to the UDM. It contains the SUCI of the FN-RG and the authenticated indication.

7. The UDM shall invoke the SIDF and maps the SUCI to the SUPI.

8. The UDM decides, based on the subscription profile of the SUPI and the authenticated indication that authentication has been completed by the W-5GAN, that authentication by the home network is not required for the FN-RG.

9. The UDM shall send a Nudm_UEAuthentication_Get Response to the AUSF. It contains the SUPI of the FN-RG and an indication that authentication by the home network is not required.

10. After checking the indication set by the UDM, The AUSF shall not perform authentication and shall send a Nausf_UEAuthentication_Authenticate Response to the AMF. It contains the SUPI of the FN-RG and the indication that authentication by the home network is not required set by the UDM.

This response from AUSF indicates that authentication is not required, and no K_{SEAF} is included.

11. After checking the indication to make sure that the authentication by the home network is not required, the AMF shall estabilish the NAS security between AMF and W-AGF with NULL encryption and NULL integrity protection.

12. The AMF shall send Registration Accept message to the W-AGF. This message contains 5G-GUTI and other parameters.

13. The W-AGF shall send a Registration Complete message back to the AMF. The W-AGF shall store the 5G-GUTI for use in later NAS procedures.

7B.4 Authentication for UE behind 5G-RG and FN-RG

A UE that is connected to a 5G-RG or FN-RG, can access the 5GC via the N3IWF or via the TNGF.

A UE behind a FN-RG can use the untrusted non-3GPP access procedure as defined in TS 23.502[8] clause 4.12.2.2 to access the 5GC via the N3IWF.

A UE behind a 5G-RG can use either the untrusted non-3GPP access as defined in TS 23.502[8] clause 4.12.2.2, or trusted N3GPP-access as defined in TS 23.502 [8] clause 4.12a.2.2.

When the UE uses untrusted non-3GPP access, the authentication of the UE is as specified in clause 7.2.1.

When the UE uses trusted non-3GPP access, the authentication of the UE is as specified in clause 7A.2.1.

7B.5 Subscriber privacy for wireline access

The requirements and procedures on the UE related to subscriber privacy in clauses 5.2.5, 6.12 and Annex C are applicable for the 5G-RG.

NOTE 1: The requirements and procedures on the UE related to subscriber privacy in clauses 5.2.5, 6.12 and Annex C are not applicable for the FG-RG.

NOTE 2: When the SUPI contains a GCI, the 5G-CRG can use the null scheme to construct the SUCI.

For a W-AGF representing an FN-RG, the null scheme shall be used to construct the SUCI as described in clauses 4.7.3 and 4.7.4 in TS 23.316 [79].

7B.6 Subscriber privacy for N5CW over trusted WLAN access

The requirements and procedures on the UE related to subscriber privacy in clauses 5.2.5, 6.12 and Annex C are applicable for the N5CW.

8 Security of interworking

8.1 General

As described in TS 23.501 [2], in order to interwork with EPC, the UE can operate in Single Registration or Dual Registration mode.

When operating in Dual Registration mode, the UE shall independently maintain and use two different security contexts, an EPS security context to interact with the Evolved Packet System and a 5G security context to interact with the 5G System. Therefore, during inter-system mobility, when the target system is EPS, the UE shall take into use the EPS security context and hence all the security mechanisms described in TS 33.401 [10] are applicable. In the other direction, i.e. when the target system is the 5GC, the UE shall take into use the 5G security context and hence all the security mechanisms described in the present document are applicable.

When operating in Single Registration mode, there are two cases depending on the support of the N26 interface between the AMF and the MME. In both cases the security mechanisms described in all the subsequent sub-clauses are applicable.

8.2 Registration procedure for mobility from EPS to 5GS over N26

During mobility from EPS to 5GS, the security handling described below shall apply.

When the UE performs idle mode mobility from EPS to 5GS, and if the UE has a native non-current 5G context, then the UE shall make the native non-current 5G context as the current one. The UE shall discard any mapped 5G security context.

The UE shall include the UE 5G security capability alongside the mapped 5G GUTI in the Registration Request message. The UE shall also include the 5G GUTI and the ngKSI that identify a current 5G security context if available, e.g. established during an earlier visit to 5G, and integrity protect the Registration Request using the selected security algorithms in the current 5G NAS security context as it is performed for a 5G NAS message over a 3GPP access. If the UE has no current 5G security context then the UE shall send the Registration Request message without integrity protection.The Registration Request shall contain the TAU request integrity protected using the EPS NAS security context shared with the source MME as it is performed for a LTE NAS message, then the UE shall increment its stored uplink EPS NAS COUNT value by one.

NOTE: The enclosed TAU request in the Registration Request contains a complete TAU Request.

Upon receipt of the Registration Request, the AMF shall interact with the MME identified by the mapped 5G GUTI to retrieve the UE context. The AMF shall include the enclosed TAU request in the Context Request message to the MME. The MME shall verify the TAU request using the stored UE security context and if the verification is successful, the MME shall send the UE context to the AMF.

The AMF shall verify the integrity of the Registration Request message if the AMF obtained the 5G security context identified by the 5G GUTI. In case the verification succeeds then the AMF shall then dispose of any EPS security parameters received from the source MME in the Context Response message. In case the verification fails or the 5G UE context is not available then the AMF shall treat the Registration Request message as if it was unprotected. In such case, the AMF may either derive a mapped 5G security context from the EPS context received from the source MME as described in clause 8.6.2 or initiate a primary authentication procedure to create a new native 5G security context.

If the AMF derives a mapped 5G security context from the EPS security context, then the ngKSI associated with the newly derived mapped 5G security context and the uplink and downlink 5G NAS COUNTs are defined and set as described in clause 8.6.2. If the Registration Request contains a TAU Request message, the network shall use the uplink EPS NAS COUNT corresponding to the TAU Request message for deriving the KAMF' from the KASME. The AMF shall use and include the ngKSI to the UE in NAS SMC procedure, for the UE to identify the EPS security context used for the derivation of a mapped 5G security context. If a mapped 5G security context is created or the native 5G security context has been changed (e.g., due to a new K_{AMF}' derivation or NAS algorithm change), the AMF shall activate the resulting 5G security context by a NAS SMC procedure. When a mapped 5G security context is created, the AMF shall store the selected EPS NAS security algorithms in the mapped 5G security context and include them in the NAS Security Mode Command.

If the AMF wants to continue to use the native 5G security context used by the UE to protect the Registration Request, the AMF may skip the NAS SMC procedure and send the Registration Accept message protected using the native 5G security context identified by the 5G-GUTI and the ngKSI included in the Registration Request message.

In case the type value in the received ngKSI in NAS SMC indicates a mapped security context, then the UE shall use the value field in the received ngKSI to identify the EPS security context from which the UE derives the mapped 5G security context as described in clause 8.6.2. The UE shall activate the mapped 5G security context to verify the integrity protection of the NAS SMC as it is performed for a 5G NAS message over a 3GPP access.

The Registration Accept message shall be protected by the new mapped 5G security context (if a mapped 5G security context was activated by NAS SMC) or by the new native 5G security context (if a new native 5G security context was activated by NAS SMC) as it is performed for a 5G NAS message over a 3GPP access. Otherwise, the current native 5G security context shall be used. If the AMF chooses to derive an initial K_{gNB} from a new K_{AMF} key (either the mapped K_{AMF}' key or the native K_{AMF} key), then the initial K_{gNB} is derived as specified in Annex A.9 using the start value of the uplink 5G NAS COUNT protecting the NAS Security Mode Command Complete message and an access type

distinguisher set to "3GPP access". If the UE receives an AS SMC message, then the UE shall derive an initial K_{gNB} from a new K_{AMF} key in the same way as the AMF.

8.3 Handover procedure from 5GS to EPS over N26

8.3.1 General

This subclause covers the case of handover from 5GS to EPS, as defined in TS 23.502 [8].

8.3.2 Procedure

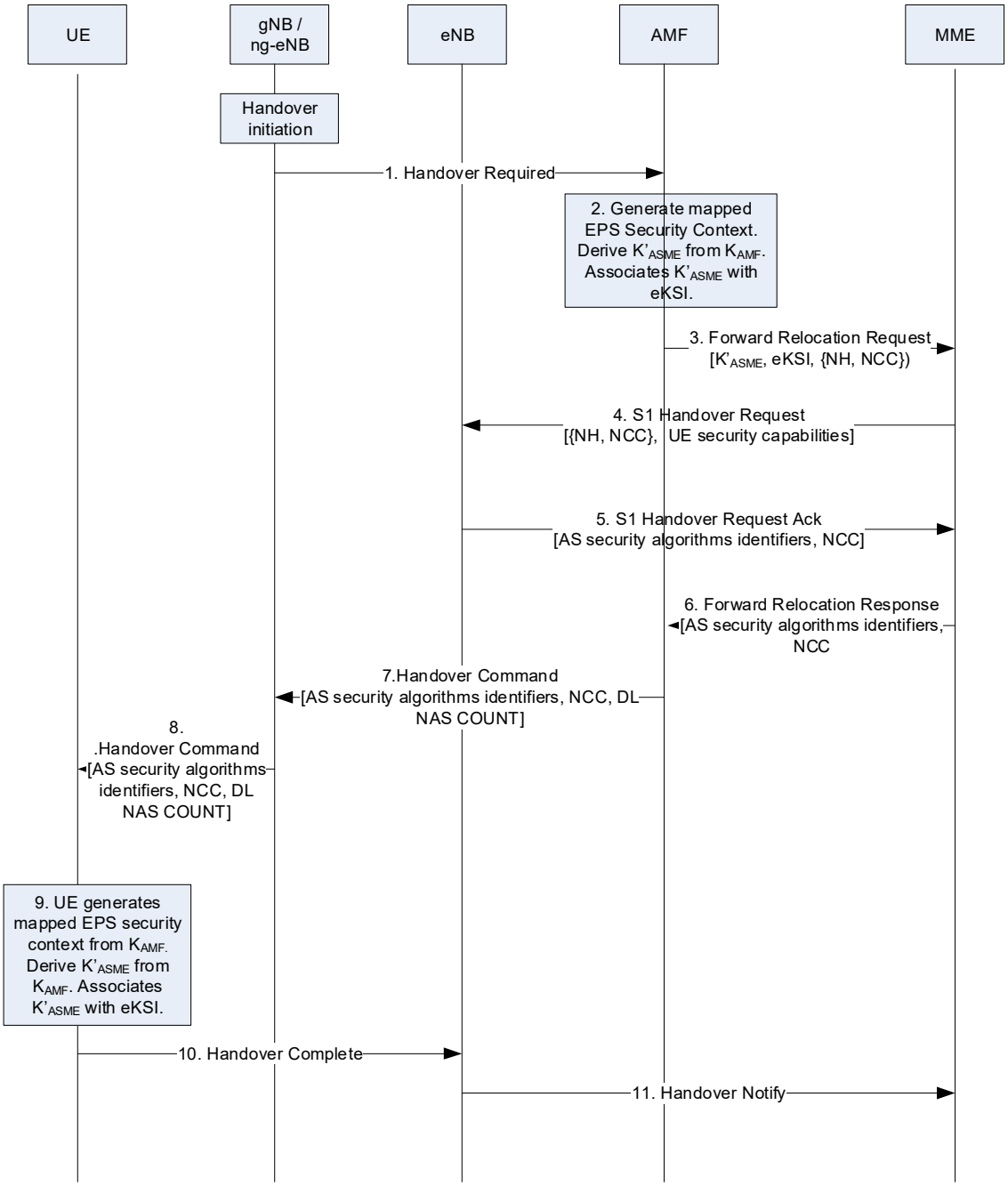


Figure 8.3.2-1 Handover from 5GS to EPC over N26

NOTE 1: This procedure is based on clause 4.11.1.2.1 in TS 23.502 and only includes steps and description that are relevant to security.

If the UE is initially registered and connected to the 5GC, the 5GC has a current security context for the UE. The current 5G security context may be a mapped 5G security context resulting from a previous mobility from EPC, or a native 5G security context resulting from a primary authentication with the 5GC.

1. The gNB/ng-eNB sends a Handover Required message to the AMF, including UE's identity .

2. When the source AMF performs a handover procedure to the EPC, after checking the UE's access rights and security capabilities, the source AMF shall prepare a UE context including a mapped EPS security context for the target MME. To construct the mapped EPS security context, the source AMF shall derive a K'_{ASME} using the

K_{AMF} key and the current downlink 5G NAS COUNT of the current 5G security context as described in clause 8.6.1 and then increments its stored downlink 5G NAS COUNT value by one.

The source AMF shall select the EPS NAS algorithms identifiers (it has stored) to be used in the target MME at interworking handover to EPS, for encryption and integrity protection.

NOTE 2: A legacy target MME is expecting to receive the selected EPS NAS algorithms identifiers over N26 from the source AMF as the target MME believes the source AMF is another MME. The source AMF has therefore provisioned the EPS NAS security algorithms identifiers to be used at interworking handover to EPS to the UE in the 5G NAS SMC in 5G access as described in clause 6.7.2. The target MME could re-select different EPS NAS algorithms though to be used with the UE by running a NAS SMC in the following Tracking Area Update procedure.

The uplink and downlink EPS NAS COUNT associated with the newly derived K_{ASME}' key are set to the values as described in clause 8.6.1. The eKSI for the newly derived K_{ASME}' key is defined as described in clause 8.6.1.

The source AMF shall also derive the initial K_{eNB} key from the K_{ASME}' key and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 2^{32}-1 as the value of the uplink NAS COUNT parameter.

NOTE 3: The source AMF and the UE only uses the 2^{32}-1 as the value of the uplink NAS COUNT for the purpose of deriving K_{eNB} and do not actually set the uplink NAS COUNT to 2^{32}-1. The reason for choosing such a value not in the normal NAS COUNT range, i.e., [0, 2^{24}-1] is to avoid any possibility that the value may be used to derive the same K_{eNB} again.

The source AMF subsequently derives NH two times as specified in clause A.4 of TS 33.401 [10]. The {NH, NCC=2} pair is provided to the target MME as a part of UE security context in the Forward Relocation Request message.

3. The source AMF shall transfer the UE security context (including new K_{ASME}', eKSI, uplink and downlink EPS NAS COUNT's, UE EPS security capabilities, selected EPS NAS algorithms identifiers) to the target MME in the Forward Relocation Request message. The UE NR security capabilities may be sent by the source AMF as well.

4. When the target MME receives Forward Relocation Request message from source AMF, then the target MME shall derive EPS NAS keys (i.e., K_{NASenc} and K_{NASint}) from the received K_{ASME}' key with the received EPS NAS security algorithm identifiers as input, to be used in EPC as described in Annex A.7 in TS 33.401 [10]. The target MME needs to include the {NH, NCC=2} pair and the UE security capabilities in the S1 HANDOVER REQUEST message to the target LTE eNB. The UE security capabilities include the UE EPS security capabilities received from the source AMF.

5. Upon receipt of the S1 HANDOVER REQUEST from the target MME, the target LTE eNB selects AS security algorithmsfrom the UE EPS security capabilities as described in clause 7.2.4.2.3 in TS 33.401 [10] and computes the KeNB to be used with the UE and proceed as described in clause 7.2.8.4.3 in TS 33.401[10]. The target LTE eNB then sends the selected AS security algorithms in the target to source transparent container in the S1 Handover Request Ack Message to the target MME.

6. The target MME shall include the target to source transparent container received from the target LTE eNB in the Forward Relocation Response message sent to the source AMF.

7. The source AMF shall include the target to source transparent container and the 8 LSB of the downlink NAS COUNT value used in K_{ASME}' derivation in step 2, in the Handover command sent to the source gNB/ng-eNB.

8. The source gNB/ng-eNB shall include the target to source transparent container and the 8 LSB of the downlink NAS COUNT value in the Handover command sent to the UE.

   Upon the reception of the Handover Command message, the UE shall estimate the downlink NAS COUNT value using the received 8 LSB of the downlink NAS COUNT value and its stored downlink NAS COUNT value. The UE shall ensure that the estimated downlink NAS COUNT value is greater than the stored downlink NAS COUNT value. Then, the UE shall derive the mapped EPS security context, i.e. derive K_{ASME}' from K_{AMF} as described in clause 8.6.1 using the estimated downlink 5G NAS COUNT value. After the derivation the UE shall set the downlink NAS COUNT value in the 5G NAS security context to the received downlink NAS COUNT value.

9. The eKSI for the newly derived K_{ASME}' key is defined as described in clause 8.6.1. The UE shall also derive the EPS NAS keys (i.e. K_{NASenc} and K_{NASint}) as the MME did in step 4 using the EPS NAS security algorithms identifiers stored in the ME and provisioned by the AMF to the UE in 5G NAS SMC in earlier 5G access. The UE shall also derive the initial K_{eNB} from the K_{ASME}' and the uplink NAS COUNT as specified in Annex A.3 of TS 33.401 [10] using 2^{32}-1 as the value of the uplink NAS COUNT parameter.

The UE shall also derive the {NH, NCC=2} pair as described in A.4 of TS 33.401 [10] and further derive the K_{eNB} to be used with the UE by performing the key derivation defined in Annex A.5 in TS 33.401[10]. The UE shall derive the AS RRC keys and the AS UP keys based on the K_{eNB} and the received AS EPS security algorithms identifiers selected by the target eNB as described in Annex A.7 in TS 33.401 [10]. The uplink and downlink EPS NAS COUNT associated with the derived EPS NAS keys are set to the values as described in clause 8.6.1. The UE shall immediately take into use the newly created mapped EPS security context, both for NAS and AS communication.

10. The UE sends the Handover Complete message to the target LTE eNB. The UE shall cipher and integrity protect this message using the newly created mapped EPS security context.

11. The target LTE eNB notifies the target MME with a Handover Notify message.

After successful completion of the Handover procedure, the UE shall delete any mapped 5G security context.

After deleting the mapped 5G security context, if the UE has a full non-current native 5G NAS security context then the UE shall make the non-current native 5G NAS security context the current one.

8.4 Handover from EPS to 5GS over N26

8.4.1 General

This clause covers the case of handoff from EPS to 5GS, as defined in TS 23.502 [8].

8.4.2 Procedure

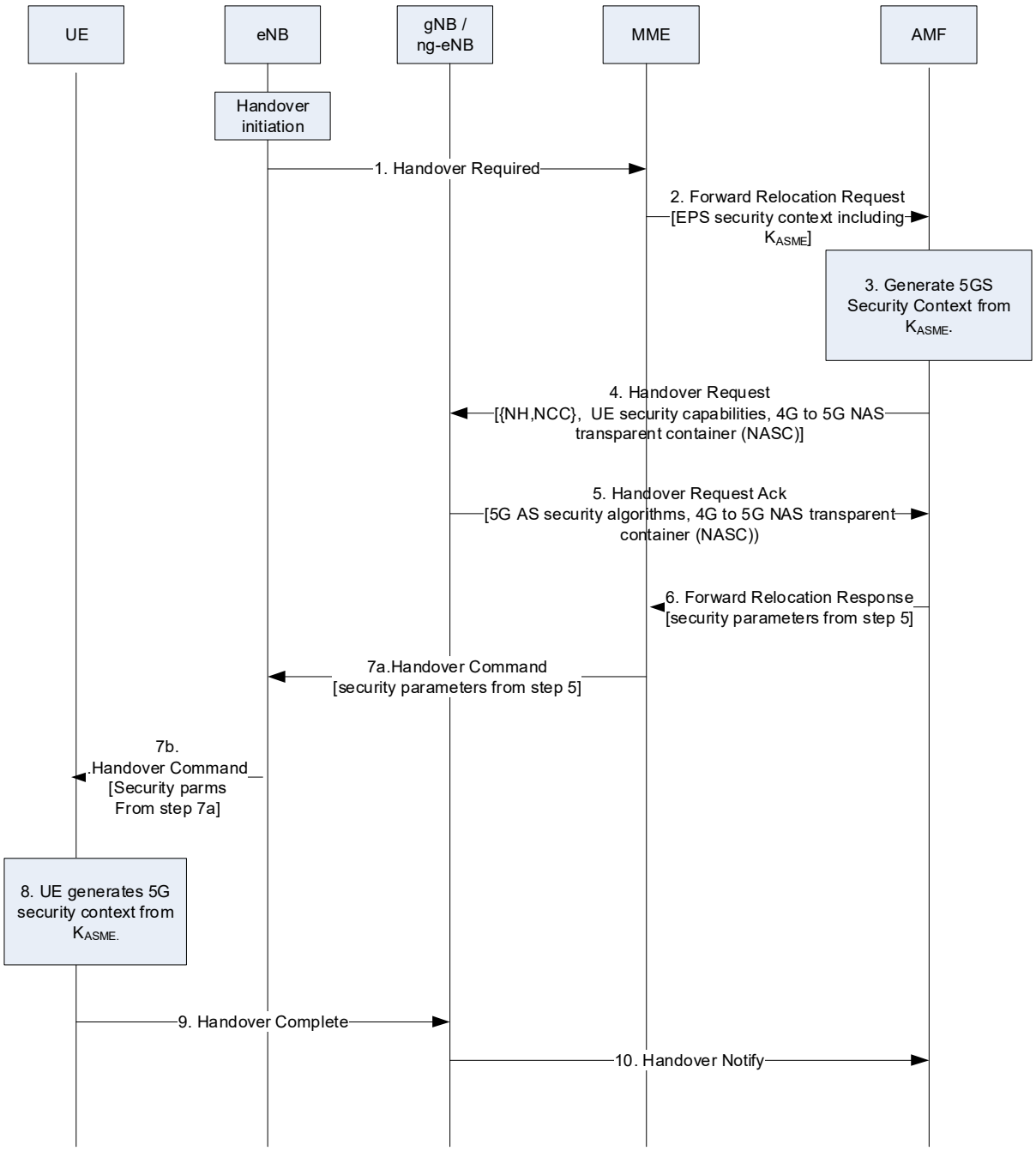


Figure 8.4.2-1: Handover from EPS to 5GS over N26

NOTE 1: This procedure is based on clause 4.11.1.2.2 in TS 23.502 [8] and only includes steps and description that are relevant to security.

As the UE is connected to the EPS, the source MME has a current EPS security context for the UE. The current EPS security context may be a mapped EPS security context resulting from a previous mobility from 5GC, or a native EPS security context resulting from a primary authentication with the EPS.

1. The source eNB sends a Handover Required message to the source MME, including UE's identity .

NOTE 2: The source MME checks whether the UE's security capabilities and access rights are valid in order to decide whether it can initiate handover to 5GS.

2. The source MME selects the target AMF and sends a Forward Relocation Request to the selected target AMF. The source MME includes UE's EPS security context including K_{ASME}, eKSI, UE EPS security capabilities, selected EPS NAS algorithm identifiers, uplink and downlink EPS NAS COUNTs, {NH, NCC} pair, in this message. If the source MME has the UE NR security capabilities stored, then it will forward the UE NR security capabilities as well to the target AMF.

3. The target AMF shall construct a mapped 5G security context from the EPS security context received from the source MME. The target AMF shall derive a mapped K_{AMF}' key from the received K_{ASME} and the NH value in the EPS security context received from the source MME as described in clause 8.6.2.

   If the target AMF receives the UE 5G security capabilities, then the target AMF shall select the 5G NAS security algorithms (to be used in the target AMF for encryption and integrity protection) which have the highest priority from its configured list.

   If the target AMF does not receive the UE 5G security capabilities from the source MME, then the target AMF shall assume that the following default set of 5G security algorithms are supported by the UE (and shall set the UE 5G security capabilities in the mapped 5G NAS security context according to this default set):

   a. NEA0, 128-NEA1 and 128-NEA2 for NAS signalling ciphering, RRC signalling ciphering and UP ciphering;

   b. 128-NIA1 and 128-NIA2 for NAS signalling integrity protection, RRC signalling integrity protection and UP integrity protection.

   The target AMF then derives the complete mapped 5G security context. The target AMF shall derive the 5G NAS keys (i.e., K_{NASenc} and K_{NASint}) from the new K_{AMF}' with the selected 5G NAS security algorithm identifiers as input, to be used in AMF as described in clause A.8. The uplink and downlink 5G NAS COUNTs associated with the derived 5G NAS keys are set to the value as described in clause 8.6. 2. The ngKSI for the newly derived K_{AMF}' key is defined such as the value is taken from the eKSI of the K_{ASME} key (i.e. included in the received EPS security context) and the type is set to indicate a mapped security context. The target AMF shall store the EPS NAS security algorithms received from the source MME in the mapped 5G security context. Similar to N2-Handover defined in Clause 6.9.2.3.3, the target AMF shall also set the NCC to zero and shall further derive the temporary K_{gNB} using the mapped K_{AMF}' key and the uplink NAS COUNT value of 2^{32}-1 as specified in Annex A.9.

   The target AMF associates this mapped 5G Security context with ngKSI.

NOTE 3: The target AMF derives a temporary K_{gNB} using the mapped K_{AMF}' instead of using the {NH, NCC} pair received from the MME. The uplink NAS COUNT value for the initial K_{gNB} derivation is set to 2^{32}-1. The reason for choosing such a value is to avoid any possibility that the value may be used to derive the same K_{gNB} again.

   The target AMF shall create a NAS Container to signal the necessary security parameters to the UE. The NAS Container shall include a NAS MAC, the selected 5G NAS security algorithms, the ngKSI associated with the derived K_{AMF}' and the NCC value associated with the NH parameter used in the derivation of the K_{AMF}'. The target AMF shall calculate the NAS MAC as described in clause 6.9.2.3.3. with the COUNT parameter set to the maximal value of 2^{32}-1.

   The target AMF shall increment the downlink NAS COUNT by one after creating a NAS Container.

4. The target AMF requests the target gNB/ng-eNB to establish the bearer(s) by sending the Handover Request message.

   The target AMF sends the NAS Container created in step 3 along with, the {NCC=0, NH=derived temporary K_{gNB}}, the New Security Context Indicator (NSCI), and the UE security capabilities in the Handover Request message to the target gNB/ng-eNB. The target AMF shall further set the NCC to one and shall further compute a NH as specified in Annex A.10. The target AMF shall further store the {NCC=1, NH} pair.

5. The target gNB/ng-eNB shall selects the 5G AS security algorithms from the list in the UE security capabilities

   The target gNB/ng-eNB shall compute the K_{gNB} to be used with the UE by performing the key derivation defined in Annex A.11 with the {NCC, NH} pair received in the Handover Request message and the target PCI and its frequency ARFCN-DL. The target gNB/ng-eNB shall associate the NCC value received from AMF with the K_{gNB}.The target gNB /ng-eNB shall then derive the 5G AS security context, by deriving the 5G AS keys (K_{RRCint}, K_{RRCenc}, K_{UPint}, and K_{UPenc}) from the K_{gNB} and the selected 5G AS security algorithm identifiers as described in Annex A.8 for gNB and in Annex A.7 in TS 33.401[10].

The target gNB/ng-eNB sends a Handover Request Ack message to the target AMF. Included in the Handover Request Ack message is the Target to Source Container, which contains the selected 5G AS algorithms, the *keySetChangeIndicator*, the NCC value from the received {NH, NCC} pair, and the NAS Container received from the target AMF. If the target gNB/ng-eNB had received the NSCI, it shall set the *keySetChangeIndicator* field to true, otherwise it shall set the *keySetChangeIndicator* field to false.

6. The target AMF sends the Forward Relocation Response message to the source MME. The required security parameters obtained from gNB/ng-eNB in step 5 as the Target to Source Container are forwarded to the source MME.

7. The source MME sends the Handover Command to the source eNB. The source eNB commands the UE to handover to the target 5G network by sending the Handover Command. This message includes all the security related parameters in the NAS Container obtained from the target AMF in step 6.

8. The UE derives a mapped K_{AMF}' key from the K_{ASME} in the same way the AMF did in step 3. It shall also derive the 5G NAS keys and K_{gNB} corresponding to the AMF and the target gNB/ng-eNB in step 3 and step 5. The UE shall further set the selected EPS NAS security algorithms in the 5G security context to the NAS security algorithms used with the source MME. It associates this mapped 5G security context with the ngKSI included in the NAS Container. The UE shall verify the NAS MAC in the NAS Container.

   If verification of the NAS MAC fails, the UE shall abort the handover procedure. Furthermore, the UE shall discard the new NAS security context if it was derived and continue to use the existing NAS and AS security contexts.

NOTE 4: Void.

   The mapped 5G security context shall become the current 5G security context.

9. The UE sends the Handover Complete message to the target gNB/ng-eNB. This shall be ciphered and integrity protected by the AS keys in the current 5G security context.

10. The target gNB/ng-eNB notifies the target AMF with a Handover Notify message.

    If the UE has a native 5G security context established during the previous visit to 5GS, then the UE shall provide the associated the 5G GUTI as an additional GUTI in the Registration Request following the handover procedure. The UE shall use the mapped 5G security context to protect the subsequent Registration Request message over 3GPP access. The target AMF shall validate the integrity of the Registration Request message using the mapped security context. Upon successful validation, the target AMF shall send a context request message to the old AMF and shall include the additional GUTI and an indication that the UE is validated. Upon receiving the context request message with the indication that the UE is validated, the old AMF shall skip the integrity check and transfer the native 5G security context to the target AMF.The AMF shall retrieve the native security context using the 5G GUTI. If the AMF determines to activate the native security context, the AMF shall perform a NAS SMC procedure.

NOTE 5: It is up to AMF when to activate the native 5G security context.

   If the handover is not completed successfully, the new mapped 5G security context cannot be used in the future. In this case, the AMF shall delete the new mapped 5G security context.

   If the AMF has no native 5G security context available when the UE performs the Registration Request (protected by the mapped 5G security context) following the handover procedure, then the AMF via the SEAF should run a primary authentication depending on local operator policy.

The handling of security contexts in the case of multiple active NAS connections in the same PLMN's serving network is given in clasue 6.4.2.2.

8.5 Idle mode mobility from 5GS to EPS over N26

8.5.1 General

This clause covers the case of idle mode mobility from 5GS to EPS over N26, as defined in TS 23.502 [8].The UE performs either Tracking Area Update (TAU) procedure or Initial Attach procedure in this scenario.

8.5.2 TAU Procedure

NOTE: This procedure is based on clause 4.11.1.3.2 in TS 23.502 [8] and only includes steps and descriptions that are relevant to security.

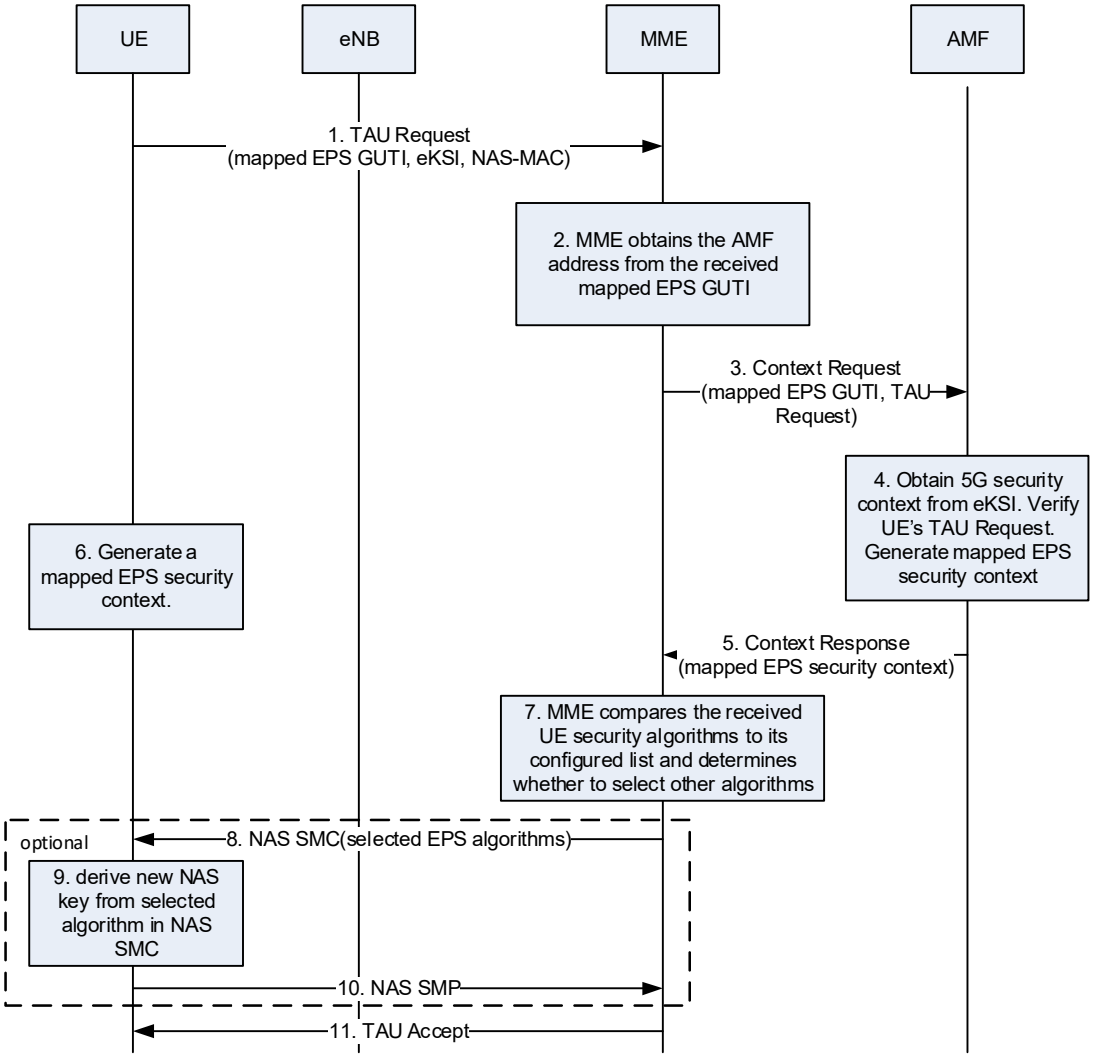


Figure 8.5.2-1: Idle mode mobility from 5G to 4G

1. The UE initiates the TAU procedure by sending a TAU Request to the MME with a mapped EPS GUTI derived from the 5G GUTI and its EPS security capabilities. The mapped EPS GUTI contains the information of the AMF that has the latest UE context in the 5G network.

   The UE integrity protects the TAU Request message using the current 5G NAS security context identified by the 5G GUTI used to derive the mapped EPS GUTI. More precisely, the UE shall compute the NAS MAC for the TAU request as it is done for a 5G NAS message over a 3GPP access. The NAS Uplink COUNT for integrity protection of the TAU request shall use the same value as the 5G NAS Uplink COUNT. Consequently, this results in an increase of the stored NAS Uplink COUNT value in the NAS COUNT pair associated with the 3GPP access. The corresponding ngKSI value of the 5G Security context is included in the eKSI parameter of the TAU Request message.

2. Upon receipt of the TAU Request, the MME obtains the AMF address from the mapped EPS GUTI value.

3. The MME forwards the complete TAU Request message including the eKSI, NAS-MAC and mapped EPS GUTI in the Context Request message.

4. The AMF shall use the eKSI value field to identify the 5G NAS security context and use it to verify the TAU Request message as if it was a 5G NAS message received over 3GPP access.

5. If the verification is successful, the AMF shall derive a mapped EPS NAS security context as described in clause 8.6.1. The AMF shall set the EPS NAS algorithms to the ones indicated earlier to the UE in a NAS SMC as described in clause 6.7.2.

   The AMF shall include the mapped EPS NAS security context in the Context Response message it sends to the MME. The AMF shall never transfer 5G security parameters to an entity outside the 5G system.

6. The UE shall derive a mapped EPS NAS security context as described in clause 8.6.1. The UE shall select the EPS algorithms using the ones received in an earlier NAS SMC from the AMF as described in clause 6.7.2. The UE shall immediately activate the mapped EPS security context and be ready to use it for the processing of the TAU Accept message in step 7.

7. The MME compares the UE security algorithms to its configured list after it receives the Context Response message. If an algorithm change is required, the MME shall select the NAS algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities and initiate an NAS SMC to the UE. Otherwise, step 8~10 shall be skipped.

8 - 10. The MME and the UE performs an NAS SMC to derive new NAS keys with the new algorithms as described in Clause 7.2.8.1.2 of TS 33.401[10].

11. The MME completes the procedure with a TAU Accept message.

After successful completion of the TAU procedure, the UE shall delete any mapped 5G security context. After deleting the mapped 5G security context, if the UE has a full non-current native 5G NAS security context then the UE shall make the non-current native 5G NAS security context the current one.

8.5.3 Initial Attach Procedure

NOTE: This procedure is based on clause 4.11.1.5.2 in TS 23.502 [8].

The Initial Attach procedure shall use the security mechanism for the TAU procedure in clause 8.5.2.

8.6 Mapping of security contexts

8.6.1 Mapping of a 5G security context to an EPS security context

The derivation of a mapped EPS security context from a 5G security context is done as described below:

- The K_{ASME}' key, taken as the K_{ASME}, shall be derived from the K_{AMF} using the 5G NAS Uplink COUNT value derived from the TAU Request message or Attach Request message in idle mode mobility or the 5G NAS Downlink COUNT value in handovers as described in Annex A.14.

- The eKSI for the newly derived K_{ASME} key shall be defined such as the value field is taken from the ngKSI and the type field is set to indicate a mapped security context.

- The EPS uplink and downlink NAS COUNT values in the mapped context shall be set to the uplink and downlink NAS COUNT values of the current 5G security context respectively.

- The selected EPS NAS algorithms shall be set to the EPS algorithms signalled to the UE by the AMF during an early authentication procedure followed by a NAS SMC as described in clause 6.7.2.

NOTE: Whenever an algorithm change is required, the target MME initiates an NAS SMC to select other algorithms as described in TS 33.401 [10].

8.6.2 Mapping of an EPS security context to a 5G security context

The derivation of a mapped 5G security context from an EPS security is done as described below.

- The K_{AMF}' key, taken as the K_{AMF}, shall be derived from the K_{ASME} using the EPS NAS Uplink COUNT of the TAU message included in the Registration Request message in idle mode mobility or the NH value in handovers as described in clause A.15.

- The ngKSI for the newly derived K_{AMF} key shall be defined such as the value field is taken from the eKSI and the type field is set to indicate a mapped security context.

- The 5G NAS COUNT values in the mapped 5G security context shall be set to 0.

NOTE: The selection of the 5G NAS algorithms is performed by the AMF and signalled to the UE either in the NAS Container during handovers as described in clause 8.4, or in a NAS SMC during idle mode mobility as described in clause 8.2.

8.7 Interworking without N26 interface in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure without N26 interface:

- For mobility from 5GC to EPC, if the UE has a current EPS NAS security context, the UE shall start using the EPS security context as defined in TS 33.401 [10].

- For mobility from EPC to 5GC, if the UE has a current 5G NAS security context, the UE shall start using the 5G NAS security context as defined in the present document.

9 Security procedures for non-service based interfaces

9.1 General

9.1.1 Use of NDS/IP

The protection of IP based interfaces for 5GC and 5G-AN according to NDS/IP is specified in TS 33.210 [3]. Traffic on interfaces carrying control plane signalling can be both integrity and confidentiality protected according to NDS/IP.

NOTE 1: Void.

9.1.2 Implementation requirements

IPsec ESP implementation shall be done according to RFC 4303 [4] as profiled by TS 33.210 [3]. For IPsec implementation, tunnel mode is mandatory to support while transport mode is optional.

IKEv2 certificate-based authentication implementation shall be done according to TS 33.310 [5]. The certificates shall be supported according to the profile described by TS 33.310 [5]. IKEv2 shall be supported conforming to the IKEv2 profile described in TS 33.310 [5].

9.1.3 QoS considerations

If the sender of IPsec traffic uses DiffServ Code Points (DSCPs) to distinguish different QoS classes, either by copying DSCP from the inner IP header or directly setting the encapsulating IP header's DSCP, the resulting traffic may be reordered to the point where the receiving node's anti-replay check discards the packet. If different DSCPs are used on the encapsulating IP header, then to avoid packet discard under one IKE SA and with the same set of traffic selectors, distinct Child-SAs should be established for each of the traffic classes (using the DSCPs as classifiers) as specified in RFC 4301 [6].

9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the N2 interface between the AMF and the 5G-AN using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect N2 is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

9.3 Security requirements and procedures on N3

N3 is the reference point between the 5G-AN and UPF. It is used to carry user plane data from the UE to the UPF.

The transport of user data over N3 shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

NOTE: The use of cryptographic solutions to protect N3 is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

9.4 Security mechanisms for the Xn interface

Xn is the interface connecting NG-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gNB and ng-eNB.

In addition to IPsec, for the Xn-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the Xn interface between the NG-RAN nodes using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding..

NOTE 2: The use of cryptographic solutions to protect Xn is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

9.5 Interfaces based on DIAMETER or GTP

This clause applies to all DIAMETER or GTP-based interfaces between the 5G Core and other network entities that are not part of the 5G System. These includes the Rx interface between the PCF and the IMS System and the N26 interface between the AMF and the MME.

The protection of these interfaces shall be supported according to NDS/IP as specified in TS 33.210 [3], unless security is provided by other means, e.g. physical security. If (D)TLS is used, implementation and usage shall follow the profile given in clause 6.2 of TS 33.210 [3] and clause 6.1.3a of TS 33.310 [5]. The cipher suites in RFC 6733 shall not be supported. A SEG may be used to terminate the NDS/IP IPsec tunnels.

9.5.1 Void

9.6 Void

9.7 Void

9.8 Security mechanisms for protection of the gNB internal interfaces

9.8.1 General

The following clause applies to the gNB supporting the split architecture.

9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. The security mechanisms for the F1 interface connecting the IAB-node to the IAB-donor-CU are detailed in clause M.3.3 of this document.

In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks..

Mutual authentication shall be supported over the F1-C interface between the gNB-CU and the gNB-DU using DTLS and/or IKEv2.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect F1 is an operator's decision. In case the gNB or the IAB-node has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB or the IAB-node.

NOTE 3: The security considerations for DTLS over SCTP are documented in RFC 6083 [58].

NOTE 4: The support of DTLS (with mutual authentication) for F1-C, between the IAB-node (gNB-DU) and the IAB-donor-CU, is optional for the IAB-node and the IAB-donor-CU.

9.8.3 Security mechanisms for the E1 interface

The E1 interface connects the gNB-CU-CP to the gNB-CU-UP. It is only used for the transport of signalling data.

In order to protect the traffic on the E1 interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

Mutual authentication shall be supported over the E1interface between the gNB-CU-CP and the gNB-CU-UP using DTLS and/or IKEv2.

IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect E1 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs

Non-SBA interfaces internal to the 5G Core such as N4 and N9 can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, these interfaces shall be confidentiality, integrity, and replay protected.

Roaming interfaces between PLMNs except for N32, shall be confidentiality, integrity, and replay protected. Protection for the N32 interface is specified in clauses 13.1 and 13.2..

For the protection of the above mentioned non-SBA internal and roaming interfaces except N32, IPsec ESP and IKEv2 certificate-based authentication shall be supported as specified in sub-clauses 9.1.2 of the present document with confidentiality, integrity and replay protection. This security mechanism shall be used,, unless security is provided by other means, e.g. physical security. A SEG may be used to terminate the IPsec tunnels.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

NOTE: It is up to the operator choice to use cryptographic solutions or other mechanisms to protect internal non-SBA interfaces such as N4 and N9.

9.10 Security mechanisms for the interface between W-5GAN and 5GC

The W-AGF function in Wireline 5G Access network (W-5GAN) terminates the following interfaces:

- N2 interface between the W-5GAN and the AMF.

-N3 interface between the W-5GAN and the UPF.

The security of the N2 interface between the W-5GAN and the AMF is as defined in clause 9.2 of the present document.

The security of the N3 interface between the W-5GAN and the UPF is as defined in clause 9.3 of the present document.

On the W-AGF side a SEG may be used to terminate the IPsec tunnels.

NOTE: Clauses 9.2 and 9.3 require that the N2 and N3 interfaces are integrity, confidentiality, and replay protected. The same protection can be achieved by placing the AGF in the same trust domain as the AMF and the SMF.

10 Security aspects of IMS emergency session handling

10.1 General

This clause addresses security procedures for IMS emergency session handling.

10.2 Security procedures and their applicability

10.2.1 Authenticated IMS Emergency Sessions

10.2.1.1 General

Authenticated emergency services are provided to UEs in the following scenarios:

a) A UE in RM-DEREGISTERED state requests IMS Emergency services

   In this scenario, the UE has a valid subscription and is authenticated when it registers with the network.

b) A UE in RM-REGISTERED state initiates a PDU Session request to setup an IMS Emergency Session

   In this scenario, the UE is already registered with the network and share a security context with the AMF. The UE initiates a session management message to setup a new bearer for emergency services. The request for emergency services is sent protected by the current security context. The AMF may decide to re-authenticate the UE.

If there is a redirection of the UE to EUTRAN for IMS Emergency services, the redirect command from the gNB to the UE shall be protected by the UE's AS security context. The AMF shall send the 'NG AP UE Initial Context setup' message to enable the AS security context set up.

10.2.1.2 UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services

The UE shall first initiate a normal initial registration procedure to register with the 5G network. Upon successful normal registration, the UE initiates the UE requested PDU session establishment procedure to establish a PDU Session to receive emergency services as specified in TS 23.502 [8].

At the time of registration, the security mode control procedure shall be applied to authenticate the UE and setup NAS and AS security. Thus, integrity protection (and optionally ciphering) shall be applied to the emergency bearers as for normal bearers.

If authentication fails for any reason, it shall be treated the same way as any registration. Once the IMS Emergency Session is in progress with NAS and AS integrity protection (and optionally ciphering) applied, failure of integrity checking or ciphering (for both NAS and AS) is an unusual circumstance and shall be treated as in the case of a normal bearer.

10.2.1.3 UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services

The UE initiates the UE requested PDU session establishment procedure to receive emergency services as specified in clause 5.16.4 in TS 23.501 [2]. Since the UE already has a current 5G security context when it attempts to set up an IMS Emergency Session, the UE shall use this 5G security context to protect NAS, RRC and UP traffic. If the AMF successfully validates the PDU Session request for emergency bearer services using the current 5G security context, the AMF may accept this request and setup a PDU session.

If the AMF attempts to re-authenticate the UE after receiving a correctly integrity protected request for emergency bearer services based on the current NAS security context and the authentication failed and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as for the initial registration error scenario as described in clause 6.1.3.

If the AMF attempts to re-authenticate the UE after receiving a correctly integrity protected request for emergency bearer services based on the current NAS security context and the authentication failed and the serving network policy allows unauthenticated IMS Emergency Sessions, then the set up of the emergency bearers shall proceed in one of the two ways:

a) The set-up proceeds according to clause 10.2.2. In this case, there is no need for the UE to re-attach, and the AMF requests the use of the NULL ciphering and integrity algorithms in the same way as described in clause 10.2.2.2 for the case of Emergency registration by UEs in limited service state.

NOTE 1: If the authentication failure is detected in the AMF then the UE is not aware of the failure in the AMF, but still needs to be prepared, according to the conditions specified in TS 24.301, to accept a NAS SMC from the AMF requesting the use of the NULL ciphering and integrity algorithms.

NOTE 2: Regardless of if the authentication failed in the UE or in the AMF, the AMF can assume that the UE will accept that NULL integrity and ciphering algorithms are selected in the security mode control procedure

b) The UE and the AMF continues using the current security context as described below for the case when primary authentication is executed while setting up a PDU session for emergency services.

If primary authentication procedure is executed while setting up a PDU Session for emergency bearer services, the AMF and UE shall behave as follows:

UE behavior:

- Upon successful authentication verification in the UE, the UE shall continue using the current security context.
- Alternatively, upon authentication verification failure in the UE, the UE shall send a failure message to the AMF and shall continue using the current security context. If the UE receives a NAS security mode command selecting NULL integrity and ciphering algorithms, the UE shall accept this as long as the IMS Emergency session progresses.

AMF behavior:

- If the serving network policy allows unauthenticated IMS Emergency Sessions, the AMF, after the unsuccessful authentication verification of the UE, should not send a reject an Authentication Reject message and continue using the current security context with the UE.
- After receiving both, the EC Indication and the failure message from the UE, the AMF shall continue using the current security context with the UE for establishing an emergency bearer.

10.2.2 Unauthenticated IMS Emergency Sessions

10.2.2.1 General

There are many scenarios when an unauthenticated Emergency Session may be established without the network having to authenticate the UE or apply ciphering or integrity protection for either AS or NAS. For example:

a) UEs that are in Limited service state UEs, as specified in clause 3.5 in TS 23.122

b) UEs that have valid subscription but SN cannot complete authentication because of network failure or other reasons

TS 23.401 clause 4.3.12.1 identifies four possible network behaviours of emergency bearer support. Amongst these, the following two cases are applicable for unauthenticated emergency sessions:

a. **IMSI required, authentication optional**. These UEs shall have a SUPI. If authentication fails, the UE is granted access and the unauthenticated SUPI retained in the network for recording purposes. The PEI is used in the network as the UE identifier. PEI only UEs will be rejected (e.g. UICCless UEs).

b. **All UEs are allowed**. Along with authenticated UEs, this includes UEs with a SUPI that cannot be authenticated and UEs with only an PEI. If an unauthenticated SUPI is provided by the UE, the unauthenticated SUPI is retained in the network for recording purposes. The PEI is used in the network to identify the UE.

The network policy is configured to one of the above, and accordingly determine how emergency requests from the UE are treated.

If the ME receives a NAS SMC selecting NIA0 (NULL integrity) for integrity protection, and NEA0 (NULL ciphering) for encryption protection, then:

- the ME shall mark any stored native 5G NAS security context on the USIM /non-volatile ME memory as invalid; and

- the ME shall not update the USIM/non-volatile ME memory with the current 5G NAS security context.

These two rules override all other rules regarding updating the 5G NAS security context on the USIM/non-volatile ME memory, in the present document.

If NIA0 is used, and the NAS COUNT values wrap around, and a new K_{AMF} has not been established before the NAS COUNT wrap around, the NAS connection shall be kept.

NOTE: For unauthenticated IMS emergency sessions, NIA0, i.e., null integrity algorithm, is used for integrity protection. Additionally, as the NAS COUNT values can wrap around, the initialization of the NAS COUNT values are not crucial. Uplink and downlink NAS COUNT are incremented for NAS message that use NIA0, as for any other NAS messages.

A UE without a valid 5G subscription shall at an IRAT handover to 5G, when an IMS Emergency Service is active, be considered by the AMF to be unauthenticated. In such a scenario, NIA0 shall be used in 5G after handover if the target network policy allows unauthenticated IMS Emergency Sessions.

A handover from 5G to another RAT, of an unauthenticated IMS Emergency Session, shall result in an unauthenticated IMS Emergency Session in the other RAT.

10.2.2.2 UE sets up an IMS Emergency session with emergency registration

UEs that are in limited service state (LSM) request emergency services by initiating the Registration procedure with the indication that the registration is to receive emergency services, referred to as Emergency Registration.

UEs that had earlier registered for normal services but now cannot be authenticated by the serving network, shall initiate Emergency Registration procedure to request emergency services.

It shall be possible to configure whether the network allows or rejects an emergency registration request and whether it allows unauthenticated UEs to establish bearers for unauthenticated IMS emergency sessions or not.

The AMF may attempt to authenticate the UE after receiving the emergency registration request.

If authentication failed in the UE during an emergency registration request, the UE shall wait for a NAS SMC command to set up an unauthenticated emergency bearer.

If authentication failed in the serving network and if the serving network policy does not allow unauthenticated IMS Emergency Sessions, the UE and AMF shall proceed as with the normal initial registration requests. The AMF shall reject the unauthenticated emergency bearer setup request from the UE.

If authentication failed in the serving network and if the serving network policy allow unauthenticated IMS Emergency Sessions, then the AMF shall support unauthenticated emergency bearer setup and the behaviours of the UE and the AMF are as described below.

a) UE behaviour:

After sending Emergency Registration request to the serving network the UE shall know of its own intent to establish an unauthenticated IMS Emergency Session.

The UE shall proceed as specified for the non-emergency case in except that the UE shall accept a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF. If the UE accepts a NAS SMC selecting NEA0 and NIA0 algorithms from the AMF as part of Emergency Registration request, then the primary authentication performed if any shall be considered as unsuccessful and the newly generated K_{AUSF} is not stored.

NOTE: In case of authentication success the AMF will send a NAS SMC selecting algorithms with a non-NULL integrity algorithm, and the UE will accept it.

b) AMF behavior:

After receiving Emergency Registration request from the UE, the AMF knows of that UE's intent to establish an unauthenticated IMS Emergency Session.

- If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.
- After the unsuccessful verification of the UE, the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.
- If both, the Emergency Registration request and an AUTHENTICATION FAILURE message with error code as defined in 24.501 [35] clauses 5.4.1.2.4.5 (for EAP based authentication) or 5.4.1.3.7 (for 5G AKA based authentication) are received by the AMF from the UE, then the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.

If the UE has initiated a PDU session establishment procedure to establish bearers for unauthenticated IMS emergency sessions and the AMF has indicated to the SMF that this is an unauthenticated emergency call, then the SMF shall indicate 'Not Needed' in the UP security policy for both UP confidentiality and UP integrity protection to the ng-eNB/gNB.

10.2.2.3 Key generation for Unauthenticated IMS Emergency Sessions

10.2.2.3.1 General

An unauthenticated UE does not share a complete 5G NAS security context with the network as there has been no successful primary authentication run between the UE and the AMF. When the UE and the AMF does not share the security context the only possibility for an AMF that allows unauthenticated IMS Emergency Sessions is to run with the NULL integrity algorithm NIA0 and the NULL ciphering algorithm NEA0.

When there has been no successful run of Primary authentication of the UE, the UE and the AMF independently generate the K_{AMF} in an implementation defined way and populate the 5G NAS security context with this K_{AMF} to be used when activating a 5G NAS security context. All key derivations proceed as if they were based on a K_{AMF} generated from a successful Primary authentication run.

Even if no confidentiality or integrity protection is provided by NIA0 and NEA0, the UE and the network treat the 5G security context with the independently generated K_{AMF} as if it contained a normally generated K_{AMF}.

10.2.2.3.2 Handover

When UE attempts to make Xn/N2 handover, UE and gNB derive and transfer the keys as normal to re-use the normal handover mechanism. Since the derived keys have no ability to affect the output of the NULL algorithms it is irrelevant that the network and the UE derive different keys. This implies that source gNB will forward UE 5G security capability which contains NIA0 and NEA0 to target gNB. So the target gNB can only select NIA0 for integrity protection and NEA0 for confidential protection. If the UE does not receive any selection of new AS security algorithms during a intra-gNB-CU handover, the UE continues to use the same algorithms as before the handover (see TS 38.331 [22]).

11 Security procedures between UE and external data networks via the 5G Network

11.1 EAP based secondary authentication by an external DN-AAA server

11.1.1 General

This sub-clause specifies support for optional to use secondary authentication between the UE and an external data network (DN).

The EAP framework specified in RFC 3748 [27] shall be used for authentication between the UE and a DN-AAA server in the external data network. The SMF shall perform the role of the EAP Authenticator. In the non-roaming scenario, the SMF shall perform the role of EAP Authenticator. And In the local break out scenario, the V-SMF of visited nework shall perform the role of EAP Authenticator. In the Home Routed deployment scenario, the H-SMF shall perform the role of the EAP Authenticator and the V-SMF shall transport the EAP messages exchanged between the UE and H-SMF. It shall rely on the external DN-AAA server to authenticate and authorize the UE's request for the establishment of PDU sessions.

Between the UE and the SMF, EAP messages shall be sent in the SM NAS message. This message is received at the AMF over N1 and delivered to the SMF over N11 using either the Nsmf_PDUSession_CreateSMContext service operation or the Nsmf_PDUSession_Update SM Context service operation, as specified in TS23.502 [8]. The SMF that takes the role of the EAP authenticator communicates with the external DN-AAA over N4 and N6 via the UPF.

The SMF invokes the Namf_Communication_N1N2MessageTransfer service operation to transfer the N1 NAS message containing the EAP message, towards the UE via the AMF.

Following clauses describe the procedures for initial Authentication and Re-Authentication with the external DN-AAA server.

11.1.2 Authentication

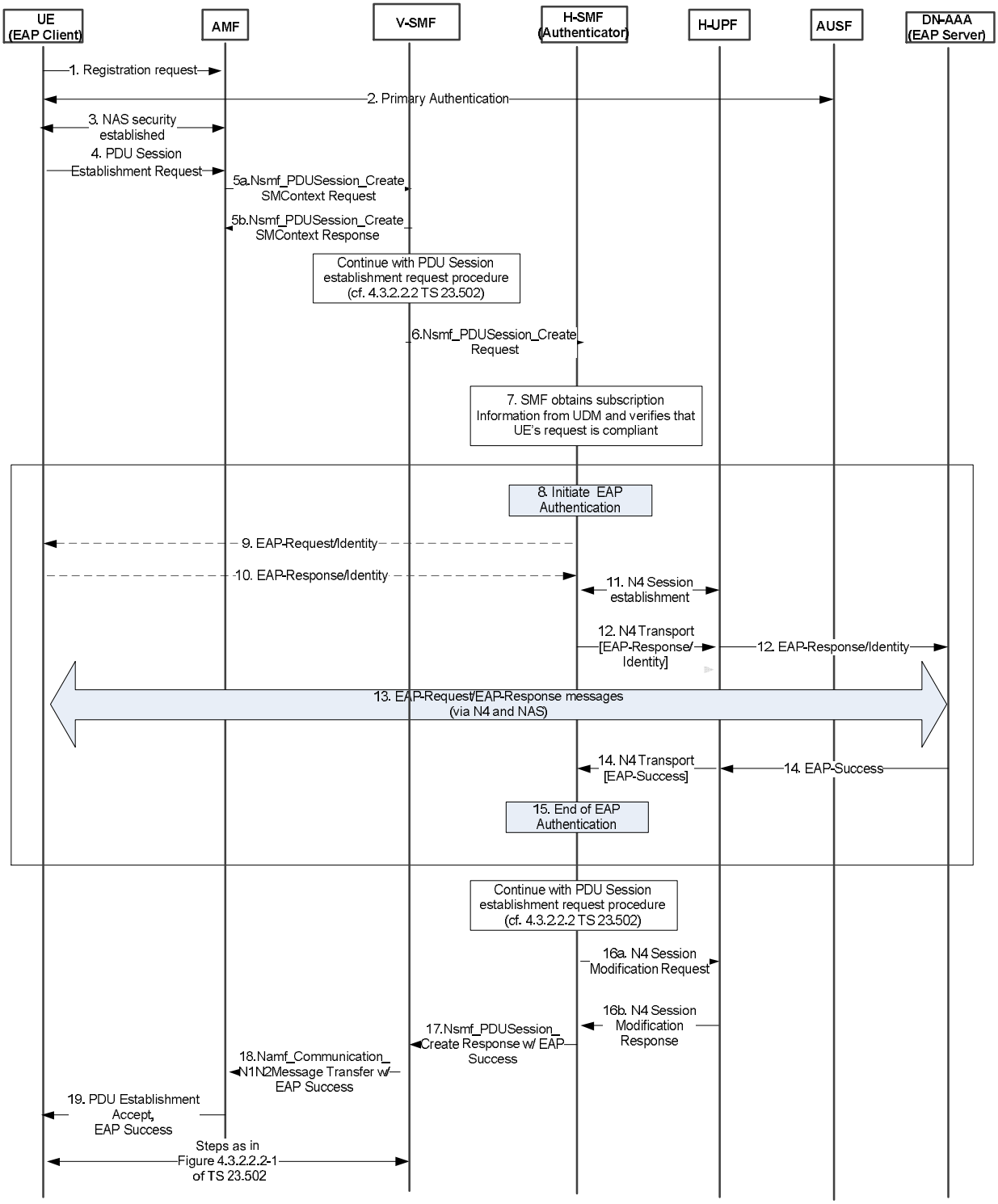


Figure 11.1.2-1: Initial EAP Authentication with an external AAA server

This procedure concerns both roaming and non-roaming scenarios. In the non-roaming case, the V-SMF is not involved. In the HR roaming case, the V-SMF shall proxy the signalling between the AMF in the VPLMN and the H-SMF in the HPLMN. In the LBO roaming case, only one SMF in VPLMN is involved.

The following procedure is based on sub-clauses 4.2.2.2.2, 4.3.2.2.1 and 4.3.2.3 in TS 23.502 [8].

NOTE 1: Steps 1-6 are borrowed from clause 4.2.2.2.2 and 4.3.2.2.1 TS 23.502 [8] and are for information only. Steps 7 to 15are related to authentication and are normative text.

1-3. The NG-UE registers with the network performing primary authentication with the AUSF/ARPF based on its network access credentials and establishes a NAS security context with the AMF.

4. The UE initiates establishment of a new PDU Session by sending a NAS message containing a PDU Session Establishment Request within the N1 SM container, slice information (identified by S-NSSAI) , PDU session ID and the PDN it would like to connect to (identified by DNN).

   The PDU Session Establishment Request may contain SM PDU DN Request Container IE containing information for the PDU session authorization by the external DN.

5a. The AMF selects a V-SMF and sends either Nsmf_PDUSession_CreateSMContext Request or Nsmf_PDUSession_UpdateSMContext Request with the N1 SM container as one of its payload. It also forwards SUPI PDU Session ID, the received S-NSSAI, and the DNN.

5b. The V-SMF sends an Nsmf_PDUSession_CreateSMContext Responseor Nsmf_PDUSession_UpdateSMContext Response correspondingly to the AMF.

In case of a single SMF being involved in the PDU session setup, e.g. non-roaming or local breakout, that single SMF takes the role of both V-SMF and H-SMF. In this case, steps 6 and 17 are skipped.

6. The V-SMF sends an Nsmf_PDUSession_Create Request to the H-SMF.

7. The H-SMF obtains subscription data from the UDM for the given SUPI obtained from the AMF in step 5. The SMF checks the subscription data whether the secondary authentication is required and whether the UE request is allowed according to the user subscription and local policies. If not allowed, the H-SMF will reject UE's request via SM-NAS signalling and skip rest of the procedure. If secondary authentication is required, the SMF may also check whether the UE has been authenticated and/or authorized by the same DN, as indicated DNN in step 5, or the same AAA server in a previous PDU session establishment. The SMF may skip steps 8 to 15 if positive.

NOTE 2: The information on a successful authentication/authorization between a UE and an SMF may be saved in SMF and/or UDM.

8. The H-SMF shall trigger EAP Authentication to obtain authorization from an external DN-AAA server. If there is no existing N4 session, the H-SMF selects a UPF and establishes an N4 Session with it. The H-SMF notifies the DN-AAA server with the GPSI, if available, and the IP address(es) of the UE allocated to the PDU Session if the PDU session is of IP PDU type or the MAC address if the PDU session is of Ethernet PDU type.

9. The H-SMF may send an EAP Request/Identity message to the UE.

10. The UE may send an EAP Response/Identity message contained within t a NAS message. The DN-specific identity shall comply with Network Access Identifier (NAI) format.

To avoid the additional round-trip in steps 9 and 10, the secondary authentication DN-specific identity may be sent by the UE in step 4. In this case, H-SMF forms an EAP Response/Identity message that contains the identity.

11. If there is no existing N4 session, the H-SMF selects a UPF and establishes an N4 Session with it.

12. The DN-specific identity, if provided by the UE, is forwarded to the UPF. The H-SMF identifies the DN AAA server based on the DN-specific identity provided by the UE and on local configuration.

    The UPF shall forward the DN-specific identity within an EAP Response/Identity message to the DN AAA Server.

13. The DN AAA server and the UE shall exchange EAP messages, as required by the EAP method. In addition, it may send additional authorization information as defined in TS 23.501 clause 5.6.6.

14. After the successful completion of the authentication procedure, DN AAA server shall send EAP Success message to the H-SMF.

15. This completes the authentication procedure at the SMF. The SMF may save the DN-specific ID and DNN (or DN's AAA server ID if available) in a list for successful authentication/authorization between UE and an SMF. Alternatively, the SMF may update the list in UDM.

If the authorization is successful, PDU Session Establishment proceeds further starting at step 7a of Figure 4.3.2.2.1-1 in TS 23.502 [8].

16a-16b. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 10a and 10b of Fig 4.3.2.2.1-1 in TS 23.502 [8].

17. The H-SMF sends an Nsmf_PDUSession_Create Response to the V-SMF. This message shall include EAP Success to be sent to the UE to V-SMF.

18. The V-SMF sends Namf_Communication_N1N2MessageTransfer to the AMF as in step 11 of Figure 4.3.2.2.1-1 in TS 23.502 [8]. This message shall include EAP Success to be sent to the UE within the NAS SM PDU Session Establishment Accept message.

19. The AMF forwards NAS SM PDU Session Establishment Accept message along with EAP Success to the UE as described in steps 12 and step 13 of Figure 4.3.2.2.1-1 in TS 23.502 [8].

The UE-requested PDU Session Establishment authentication/authorization by a DN-AAA server proceeds further as described in sub-clause 4.3.2.3 in TS 23.502 [8].

11.1.3 Re-Authentication

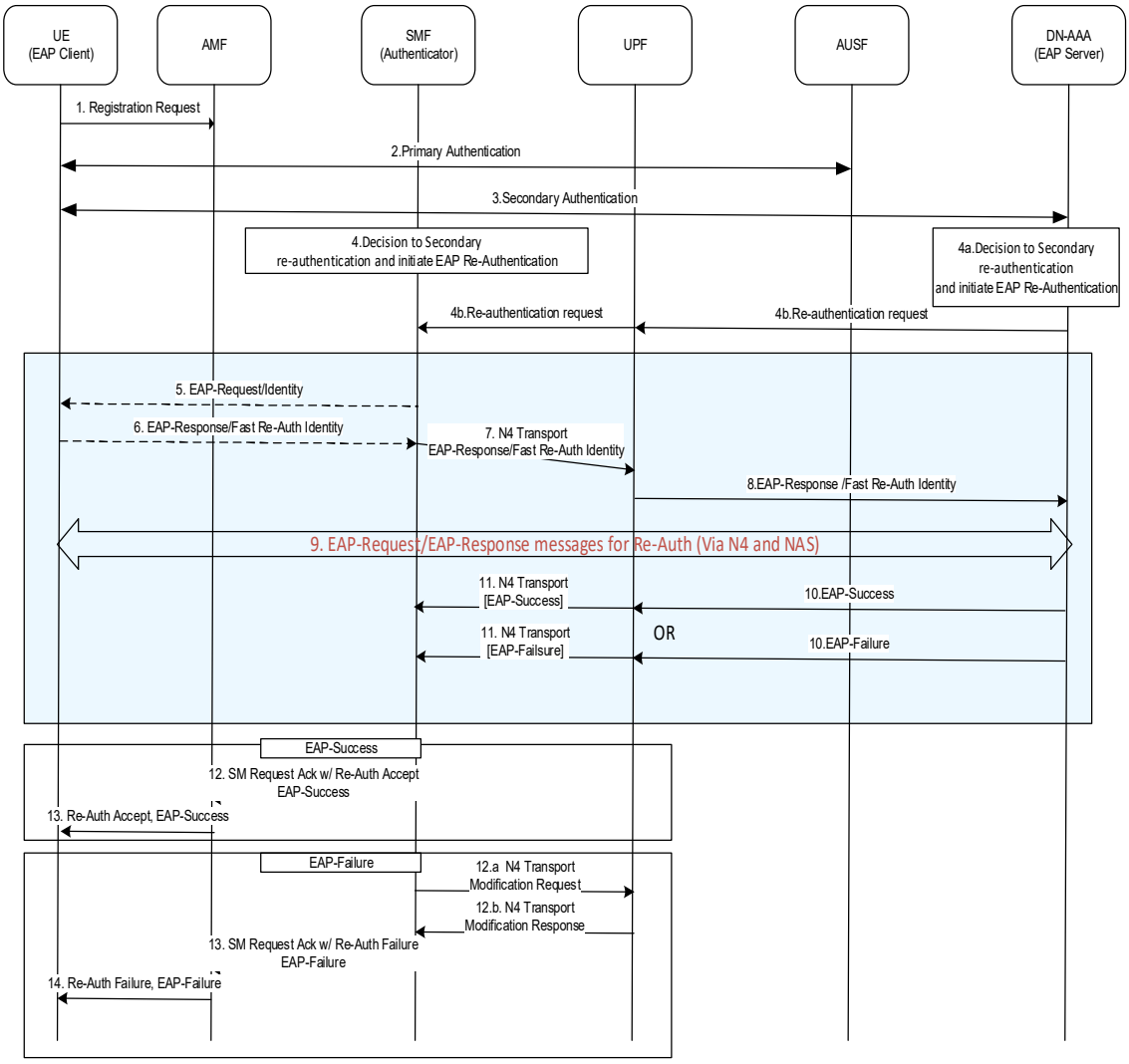


Figure 11.1.3-1: EAP Re-Authentication with an external AAA server

This procedure concerns both roaming and non-roaming scenarios. In the non-roaming and LBO roaming cases, only one SMF is involved. In the HR roaming case, the V-SMF shall proxy the signalling between the AMF in the VPLMN and the H-SMF in the HPLMN.

1-3 Secondary Authentication has been established according to procedures specified in clause 11.1.2, Initial EAP Authentication with an external AAA server.

Secondary Re-authentication may either be initiated by SMF or the external DN/AAA server. If Re-authentication is initiated by SMF, the procedure proceeds with step 4 (skipping steps 4a and 4b). If Re-authentication is initiated by the external DN/AAA server, the procedure proceeds with the alternative steps 4a and 4b.

4. The SMF decides to initiate Secondary Re-Authentication.

4a. The DN AAA server decides to initiate Secondary Re-Authentication.

4b. The DN AAA shall send a Secondary Re-Authentication request to UPF, and the UPF forwards it to SMF. The Secondary Re-authentication request contains the GPSI, if available, and the IP/MAC address of the UE allocated to the PDU Session and the MAC address if the PDU session is of Ethernet PDU type.

5. The SMF shall send an EAP Request/Identity message to the UE.

6. The UE shall respond with an EAP Response/Identity message (with Fast-Reauth Identity).
7. The SMF forwards the EAP Response/Identity to UPF, selected during initial authentication, over N4 interface.

   This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.
8. The UPF shall forward the EAP Response/Identity message to the DN AAA Server.
9. The DN AAA server and the UE shall exchange EAP messages as required by the EAP method.
10. After the completion of the authentication procedure, DN AAA server either sends EAP Success or EAP Failure message to the SMF.
11. This completes the Re-authentication procedure at the SMF.

12-13. If the authentication is successful, EAP-Success shall be sent to UE.

12-14. If authentication is not successful, the SMF notifies failure to UPF. Upon completion of a N4 Session Modification procedure with the selected UPF, SMF sends EAP-Failure to UE via AMF.

11.1.4 Secondary authentication and authorization revocation

At any time, a DN-AAA server may revoke the authentication and authorization for a PDU Session and according to the request from the DN-AAA server, the SMF may release the PDU Session as specified in sub-clause 4.3.4 of TS 23.502 [8].

12 Security aspects of Network Exposure Function (NEF)

12.1 General

In the 5G system, the Network Functions securely expose capabilities and events to 3rd party Application Functions (AF) via NEF. The NEF also enable secure provision of information in the 3GPP network by authenticated and authorized AFs.

NOTE: If a token is generated for AF authorization, such a token can include specific information depending on the procedure, e.g. clause 16.6.3.

Requirements on security aspects of NEF are captured in clause 5.9.2.3.

12.2 Mutual authentication

For authentication between NEF and an AF that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates shall be performed between the NEF and AF using TLS.

Certificate based authentication shall follow the profiles given in 3GPP TS 33.310 [5], clause 6.1.3a. The identities in the end entity certificates shall be used for authentication and policy checks. The structure of the PKI used for the certificate is out of scope of the present document.

12.3 Protection of the NEF – AF interface

TLS shall be used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the AF. The support of TLS is mandatory.

Security profiles for TLS implementation and usage shall follow the provisions given in clause 6.2 of TS 33.210 [3].

12.4 Authorization of Application Function's requests

After the authentication, NEF determines whether theAF is authorized to send requests for the 3GPP Network Entity. The NEF shall authorize the requests from AF using OAuth-based authorization mechanism, the specific authorization mechanisms shall follow the provisions given in RFC 6749 [43].

12.5 Support for CAPIF

When the NEF supports CAPIF for external exposure as specified in clause 6.2.5.1 in TS 23.501[2], then CAPIF core function shall choose the appropriate CAPIF-2e security method as defined in the sub-clause 6.5.2 in TS 33.122[53] for mutual authentication and protection of the NEF – AF interface.

13 Service Based Interfaces (SBI)

13.1 Protection at the network or transport layer

13.1.0 General

All network functions shall support mutually authenticated TLS and HTTPS as specified in RFC 7540 [47] and RFC 2818 [90]. The identities in the end entity certificates shall be used for authentication and policy checks. Network functions shall support both server-side and client-side certificates. TLS client and server certificates shall be compliant with the SBA certificate profile specified in clause 6.1.3c of TS 33.310 [5].

The TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [3] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47]. TLS clients shall include the SNI extension as specified in RFC 7540 [47].

TLS shall be used for transport protection within a PLMN unless network security is provided by other means.

NOTE 1: Regardless of whether TLS is used or not, NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5] can be used for network layer protection.

NOTE 2: If interfaces are trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to use cryptographic protection.

NOTE 3: It is a vendor implementation decision how the SNI extension is being used in TLS servers.

13.1.1 TLS protection between NF and SEPP

13.1.1.0 General

To allow for TLS protection between the SEPP and Network Functions or SCPs within a PLMN, the SEPP shall support:

- TLS wildcard certificate for its domain name and generation of telescopic FQDN based on an FQDN obtained from the received N32-f message as specified in clause 13.1.1.1.
- using the custom HTTP header 3gpp-Sbi-Target-apiRoot, defined in clause 5.2.3.2.4 of TS 29.500[74], in the HTTP request originated by the NF within the SEPP's PLMN, to forward the protected HTTP Request message towards the remote PLMN as specified in clause 13.1.1.2.

NOTE: Whether the SEPP and NFs within the SEPP's PLMN use telescopic FQDN or the custom HTTP header is based on PLMN operator's policy.

13.1.1.1 TLS protection based on telescopic FQDN and wildcard certificate

A telescopic FQDN is an FQDN with a single label as the first element and the SEPP's domain as the trailer component. The label uniquely represents the original FQDN.

NOTE 3: The structure of telescopic FQDN is defined in 3GPP TS 23.003 [19], clause 28.5.2.

The SEPP shall generate a telescopic FQDN for the following messages received over N32-f:

a. Nnrf_NFDiscovery_Get response HTTP message with FQDNs of a set of the discovered NF or NF service instance(s) (see TS 29.510 [68]). The cSEPP generates a telescopic FQDN for each target Network Function FQDN in the Discovery response, rewrites the original FQDN with the telescopic FQDN and forwards the modified Discovery response to the NRF.

b. Subscription message with the Callback URI in the payload of the message (see TS 29.501 [94]). The pSEPP generates a telescopic FQDN from the Callback URI in the Subscription message, rewrites the original FQDN in the callback URI, and forwards the modified Subscription message to the producer Network Function.

c. Nsmf_PDUSession_POST HTTP message from a V-SMF with PduSessionCreateData containing the URI representing the PDU session in the V-SMF (see TS 29.502 [95]). The pSEPP generates a telescopic FQDN from the Callback URI in the message, rewrites the original FQDN in the callback URI, and forwards the modified message to the target H-SMF.

The following procedure illustrates how SEPPs use telescopic FQDN and wildcard certificate to establish a TLS connection between a Network Function or a SCP and the SEPP:

1. When the SEPP receives one of the messages identified in a-c above, it shall rewrite the FQDN from the received message with a telescopic FQDN and it forwards the modified HTTP message to the target Network Function or SCP inside the PLMN.

2. When the Network Function or SCP that received the telescopic FQDN in step 1 is ready to communicate with the target Network Function or SCP in another PLMN, it uses the telescopic FQDN in the Request URI of the HTTP Request. When communication between the Network Function or SCP and the SEPP that generated the telescopic FQDN is based on using the 3gpp-Sbi-Target-apiRoot custom HTTP header as specified in TS 29.500 [74], clause 5.2.3.2.4, the Network Function or SCP uses the telescopic FQDN in the 3gpp-Sbi-Target-apiRoot custom HTTP header of the HTTP Request. During TLS setup between the Network Function and the SEPP, the SEPP shall authenticate towards the Network Function or SCP using the wildcard certificate.

3. When the SEPP receives a HTTP request from the Network Function or SCP, the SEPP shall rewrite the telescopic FQDN with the original FQDN by replacing the unique delimiter in the label with the period character and removing its own suffix part.

13.1.1.2 TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header

The NF uses the 3gpp-Sbi-Target-apiRoot HTTP header in the HTTP Request to convey the target FQDN to the SEPPs.

If PRINS is used on the N32-f interface, the following applies: The sending SEPP shall use the 3gpp-Sbi-Target-apiRoot header to obtain the apiRoot to be used in the request URI of the protected HTTP Request. It removes the 3gpp-Sbi-Target-apiRoot header before forwarding the protected HTTP Request on the N32-f interface.

If TLS is used on the N32 interface, the following applies: The sending SEPP shall replace the authority header in the HTTP Request with the FQDN of the receiving SEPP before forwarding the protected HTTP Request on the N32 interface. The sending SEPP shall not change the 3gpp-Sbi-Target-apiRoot header.

NOTE: This solution does not require the SEPP to support TLS wildcard certificate for its domain name during TLS setup, nor the SEPP to generate a telescopic FQDN for the target FQDN.

13.1.2 Protection between SEPPs

TLS shall be used for N32-c connections between the SEPPs.

The SEPP shall maintain a set of trust anchors, each consisting of a list of trusted root certificates and a list of corresponding PLMN-IDs. Any given PLMN-ID shall appear in at most one trust anchor. During N32-c connection setup, the SEPP shall map the PLMN-ID of the remote SEPP leaf (server or client) certificate to the associated trust

anchor for the purposes of certificate chain verification. Only the root certificates in the associated list shall be treated as trusted during certificate chain verification. If the remote SEPP certificate contains multiple PLMN-IDs that are mapped to different trust anchors, then that certificate shall be rejected.

Operator Group Roaming Hubs SEPPs are equivalent to a network operator SEPP when they are in the same security domain and are not considered IPX providers as detailed in this clause. The communication between a group network operator's SBA network border element and the Operator Group Roaming Hub SEPP is out of scope of the present document.

If there are no IPX providers between the SEPPs, TLS shall be used for N32-f connections between the SEPPs. Different TLS connections are used for N32-c and N32-f. If there are IPX providers which only offer IP routing service between SEPPs, either TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

If TLS is selected, the SEPP shall correlate the N32-f TLS connection with the N32-c connection. If the peer network is a PLMN, the SEPP compares the PLMN-IDs contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections. Specifically, if the certificate used for N32-f contains one or more PLMN-IDs that are not contained in the TLS certificate used for the corresponding N32-c, the N32-f certificate shall be rejected. If the peer network is an SNPN, the SEPP compares the SNPN-ID contained in the SEPP TLS certificates used to establish the N32-c and N32-f connections.

If there are IPX providers which, in addition to IP routing, offer other services that require modification or observation of the information and/or additions to the information sent between the SEPPs, PRINS shall be used for protection of N32-f connections between the SEPPs.

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs allows SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32, and provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.

If PRINS is used on the N32-f interface, one of the following additional transport protection methods should be applied between SEPP and IPX provider for confidentiality and integrity protection:

- NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5], or
- TLS VPN with mutual authentication following the profile given in clause 6.2 of TS 33.210 [3] and clause clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

NOTE 1: Void

NOTE 2: Void.

13.2 Application layer security on the N32 interface

13.2.1 General

The internetwork interconnect allows secure communication between service-consuming and a service-producing NFs in different PLMNs. Security is enabled by the Security Edge Protection Proxies of both networks, henceforth called cSEPP and pSEPP respectively. The SEPPs enforce protection policies regarding application layer security thereby ensuring integrity and confidentiality protection for those elements to be protected.

It is assumed that there are interconnect providers between cSEPP and pSEPP. The interconnect provider the cSEPP's operator has a business relationship with is called cIPX, while the interconnect provider the pSEPP's operator has a business relationship with is called pIPX. There could be further interconnect providers in between cIPX and pIPX, but they are assumed to be transparent and simply forward the communication.

The SEPPs use JSON Web Encryption (JWE, specified in RFC 7516 [59]) for protecting messages on the N32-f interface, and the IPX providers use JSON Web Signatures (JWS, specified in RFC 7515 [45]) for signing their modifications needed for their mediation services.

For illustration, consider the case where a service-consuming NF sends a message to a service-producing NF. If this communication is across PLMN operators over the N32-f interface, as shown in Figure 13.2.1-1 below, the cSEPP

receives the message and applies symmetric key based application layer protection, as defined in clause 13.2 of the present document. The resulting JWE object is forwarded to intermediaries. The pIPX and cIPX can offer services that require modifications of the messages transported over the interconnect (N32) interface. These modifications are appended to the message as digitally signed JWS objects which contain the desired changes. The pSEPP, which receives the message from pIPX, validates the JWE object, extracts the original message sent by the NF, validates the signature in the JWS object and applies patches corresponding to the modifications by intermediaries. The pSEPP then forwards the message to the destination NF.

The N32 interface consists of:

- N32-c connection, for management of the N32 interface, and
- N32-f connection, for sending of JWE and JWS protected messages between the SEPPs.

The application layer security protocol for the N32 interface described in clause 13.2 of the present document is called PRINS.

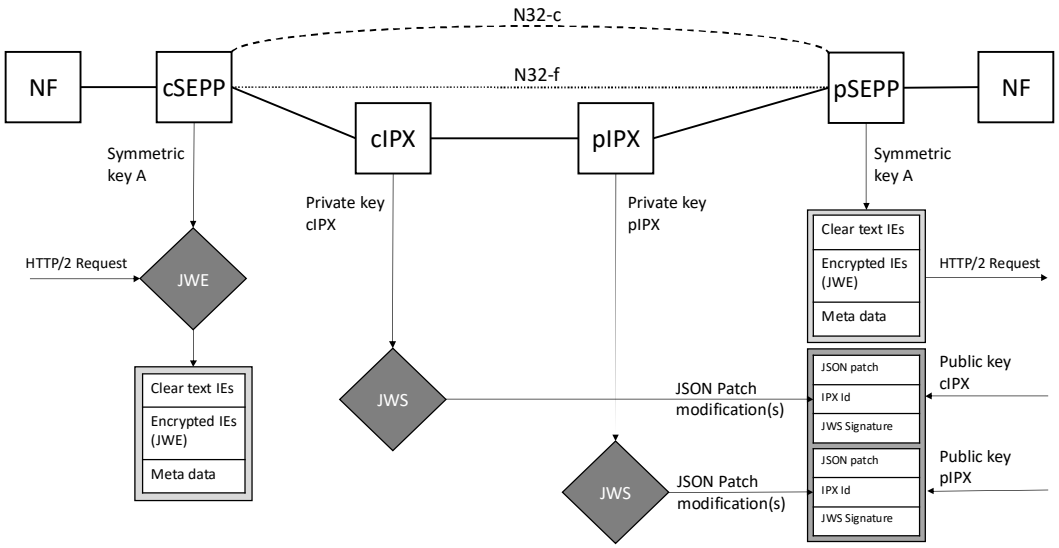


Figure 13.2.1-1: Overview of PRINS

13.2.2 N32-c connection between SEPPs

13.2.2.1 General

When the negotiated security mechanism to use over N32, according to the procedure in clause 13.5, is PRINS (described in clause 13.2), the SEPPs use the established TLS connection (henceforth referred to as N32-c connection) to negotiate the N32-f specific associated security configuration parameters required to enforce application layer security on HTTP messages exchanged between the SEPPs. A second N32-c connection is established by the receiving SEPP to enable it to not only receive but also send HTTP Requests.

The N32-c connection is used for the following purposes:

- Key agreement: The SEPPs independently export keying material associated with the first N32-c connection between them and use it as the pre-shared key for generating the shared session key required.
- Parameter exchange: The SEPPs exchange security related configuration parameters that they need to protect HTTP messages exchanged between the two Network Functions (NF) in their respective networks.
- Error handling: The receiving SEPP sends an error signalling message to the peer SEPP when it detects an error on the N32-f interface.

The following security related configuration parameters may be exchanged between the two SEPPs:

a. Modification policy. A modification policy, as specified in clause 13.2.3.4, indicates which IEs can be modified by an IPX provider of the sending SEPP.

b. Data-type encryption policy. A data-type encryption policy, as specified in 13.2.3.2, indicates which types of data will be encrypted by the sending SEPP.

c. Cipher suites for confidentiality and integrity protection, when application layer security is used to protect HTTP messages between them.

d. N32-f context ID. As specified in clause 13.2.2.4.1, N32-f context ID identifies the set of security related configuration parameters applicable to a protected message received from a SEPP in a different PLMN.

13.2.2.2 Procedure for Key agreement and Parameter exchange

1. The two SEPPs shall perform the following cipher suite negotiation to agree on a cipher suite to use for protecting NF service related signalling over N32-f.

   1a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP's supported cipher suites. The cipher suites shall be ordered in initiating SEPP's priority order. The SEPP shall provide an initiating SEPP's N32-f context ID for the responding SEPP.

   1b. The responding SEPP shall compare the received cipher suites to its own supported cipher suites and shall select, based on its local policy, a cipher suite, which is supported by both initiating SEPP and responding SEPP.

   1c. The responding SEPP shall send a Security Parameter Exchange Response message to the initiating SEPP including the selected cipher suite for protecting the NF service related signalling over N32. The responding SEPP shall provide a responding SEPP's N32-f context ID for the initiating SEPP.

2. The two SEPPs may perform the following exchange of Data-type encryption policies and Modification policies. Both SEPPs shall store protection policies sent by the peer SEPP:

   2a. The SEPP which initiated the first N32-c connection shall send a Security Parameter Exchange Request message to the responding SEPP including the initiating SEPP's Data-type encryption policies, as described in clause 13.2.3.2, and Modification policies, as described in clause 13.2.3.4.

   2b. The responding SEPP shall store the policies if sent by the initiating SEPP.

   2c. The responding SEPP shall send a Security Parameter Negotiation Response message to the initiating SEPP with the responding SEPP's suite of protection policies.

   2d. The initiating SEPP shall store the protection policy information if sent by the responding SEPP.

3. The two SEPPs shall exchange IPX security information lists that contain information on IPX public keys or certificates that are needed to verify IPX modifications at the receiving SEPP.

4. The two SEPPs shall export keying material from the TLS session established between them using the TLS export function. For TLS 1.2, the exporter specified in RFC 5705 [61] shall be used. For TLS 1.3, the exporter described in section 7.5 of RFC 8446 [60] shall be used. The exported key shall be used as the master key to derive session keys and IVs for the N32-f context as specified in clause 13.2.4.4.1.

5. When the responding SEPP needs to initiate traffic, e.g., error reporting, in the reverse direction to the sending SEPP, the responding SEPP in the first N32-c connection shall now setup a second N32-c connection by establishing a mutually authenticated TLS connection with the peer SEPP.

NOTE: The second N32-c connection setup by the responding SEPP does not perform the negotiation of steps 1-4.

6. The two SEPPs start exchanging NF to NF service related signalling over N32-f and tear down the N32-c connection. The SEPPs may initiate new N32-c TLS sessions for any further N32-c communication that may occur over time while application layer security is applied to N32-f.

13.2.2.3 Procedure for error detection and handling in SEPP

Errors can occur on an active N32-c connection or on one or more N32-f connections between two SEPPs.

When an error is detected, the SEPP shall map the error to an appropriate cause code. The SEPP shall create a signalling message to inform the peer SEPP, with cause code as one of its parameters.

The SEPP shall use the N32-c connection to send the signalling message to the peer SEPP. If the old N32-c connection has been terminated, it uses a new N32-c connection instead.

If the error occurred in the processing of the one or more N32-f message(s), the SEPP shall include the corresponding message ID (s), obtained from the metadata section of the N32-f message, as a parameter in the signalling message. This allows the peer SEPP to identify the source message(s) (HTTP Request or Response) on which the other SEPP found the error.

NOTE: Local action taken by either SEPP is out of 3GPP scope.

13.2.2.4 N32-f Context

13.2.2.4.0 N32-f parts

The N32-f context consists of the following main parts as illustrated in Figure 13.2.2.4.0-1:

1. N32-f context ID
2. N32-f peer information
3. N32-f security context
4. N32-f context information

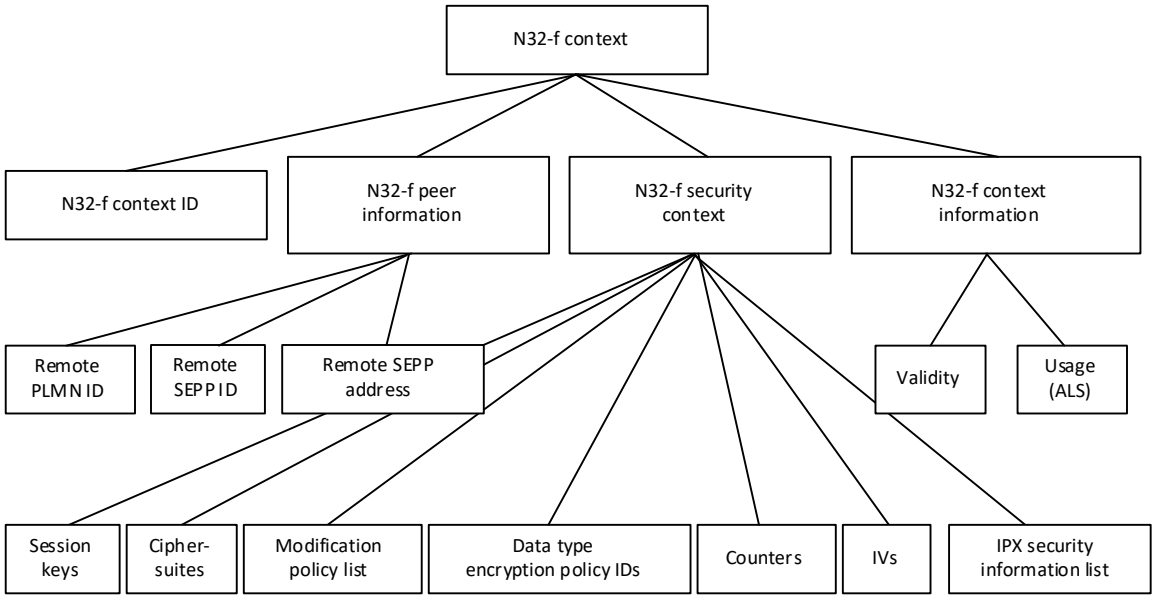


Figure 13.2.2.4.0-1: N32-f context overview

13.2.2.4.1 N32-f context ID

The N32-f context ID is used to refer to an N32-f context. The SEPPs shall create the N32-f context ID during the N32-c negotiation and use it over N32-f to inform the receiving peer which security context to use for decryption of a received message.

The initiating SEPP shall send the initiating SEPP's N32-f context ID to the responding SEPP which the responding SEPP shall use to identify the N32-f connection with this initiating SEPP. Vice versa, the responding SEPP shall send the responding SEPP's N32-f context ID to the initiating SEPP which the initiating SEPP shall use to identify the N32-f connection with this responding SEPP. To avoid collision of the N32-f context ID value, the SEPPs shall select the N32-f context ID as a random value during the exchange over N32-c.

During transfer of application data over N32-f, the SEPP shall include the N32-f context ID in a separate IE in the metadata part of the JSON structure, see clause 13.2.4.2. The receiving SEPP shall use this information to apply the correct key and parameters during decryption and validation.

13.2.2.4.2 N32-f peer information

The N32-f connection between SEPPs is bidirectional and consists of the two SEPP endpoints and possibly up to two IPX providers. The SEPPs are identified by the PLMN ID and additionally a SEPP ID to distinguish between several SEPPs in the same PLMN. The remote SEPP address is necessary for routing the messages to the correct destination.

The N32-f peer information shall consist of the following parameters:

- Remote PLMN ID;
- Remote SEPP ID;
- Remote SEPP address.

13.2.2.4.3 N32-f security context

The N32-c initial handshake described in clause 13.2.2.2 establishes session keys, IVs and negotiated cipher suites. Counters are used for replay protection. Modification policies are identified by modification policy IDs, to be able to verify received messages that have undergone IPX modifications.

The N32-f security context shall consist of the following parameters:

- Session keys
- Negotiated cipher suites
- Data type encryption policy IDs
- Modification policy list (if IPXs are used)
    - Modification policy IDs
    - IPX provider identifier
- Counters
- IVs
- List of security information of the IPX providers connected to the SEPPs (IPX security information list)
    - IPX provider identifier
    - List of raw public keys or certificates for that IPX

13.2.2.4.4 N32-f context information

The N32-f context information shall consist of the following parameters:

- Validity.

- Usage (PRINS).

13.2.3 Protection policies for N32 application layer solution

13.2.3.1 Overview of protection policies

The protection policy suite is comprised of a data-type encryption policy and a modification policy. Together, these policies determine which part of a certain message shall be confidentiality protected and which part of a certain message shall be modifiable by IPX providers. The SEPP shall apply the protection policies for application layer protection of messages on the N32-f interface.

There are two types of protection policies, namely:

- Data-type encryption policy: specifies which data types need to be confidentiality protected;
- Modification policy: specifies which IEs are modifiable by intermediaries.

In addition, there is a mapping between the data-types in the data-type encryption policy and the IEs in NF API descriptions which is given in a NF-API data-type placement mapping.

13.2.3.2 Data-type encryption policy

The SEPP shall contain an operator-controlled protection policy that specifies which types of data shall be encrypted. The data-types defined are the following:

- Data of the type 'SUPI';
- Data of the type 'authentication vector';
- Data of the type 'location data';
- Data of the type 'cryptographic material';
- Data of the type 'authorization token'.

The policy shall be specific per roaming partner. The policy shall contain a policy identifier and a release number referring to the release it is applicable for.

The data-type encryption policies in the two partner SEPPs shall be equal to enforce a consistent ciphering of IEs on N32-f.

13.2.3.3 NF API data-type placement mapping

Each NF API data-type placement mapping shall contain the following:

- Which IEs contain data of the type 'SUPI' or type 'NAI'.
- Which IEs contain data of the type 'authentication vector’.
- Which IEs contain data of the type 'location data'.
- Which IEs contain data of the type 'cryptographic material'.
- Which IEs contain data of the type 'authorization token'.

The location of the IEs refers to the location of the IEs after the SEPP has rewritten the message for transmission over N32-f.

An NF API data-type placement mapping shall furthermore contain data that identifies the NF API, namely

- The name of the NF;
- The API version;
- An identifier for the NF API data-type placement mapping;

- The NF's 3GPP Release version.

NOTE: Larger networks can contain multiple NFs with the same API, e.g. three AMFs. The NF API policy applies to all NFs with the same API.

The NF API data-type placement mapping shall reside in the SEPP.

13.2.3.4 Modification policy

The SEPP shall contain an operator-controlled policy that specifies which IEs can be modified by the IPX provider directly related to this particular SEPP. These IEs refer to the IEs after the sending SEPP has rewritten the message.

Each PLMN-operator shall agree the modification policy with the IPX provider it has a business relationship with prior to establishment of an N32 connection. Each modification policy applies to one individual relation between PLMN-operator and IPX provider. To cover the whole N32 connection, both involved roaming partners shall exchange their modification policies.

NOTE 1: In order to validate modifications for messages received on the N32-f interface, the operator's roaming partners will have to know the overall modification policy.

NOTE 2: Modification includes removal and addition of new IE. IEs therefore may not be present in the rewritten message.

The IEs that the IPX is allowed to modify shall be specified in a list giving an enumeration of JSON paths within the JSON object created by the SEPP. Wildcards may be used to specify paths.

This policy shall be specific per roaming partner and per IPX provider that is used for the specific roaming partner.

The modification policy shall reside in the SEPP.

For each roaming parter, the SEPP shall be able to store a policy for receiving.

The following basic validation rules shall always be applied irrespective of the policy exchanged between two roaming partners:

- IEs requiring encryption shall not be inserted at a different location in the JSON object.

13.2.3.5 Provisioning of the policies in the SEPP

The SEPP shall contain an interface that the operator can use to manually configure the protection policies in the SEPP.

The SEPP shall be able to store and process the following policies for outgoing messages:

- A generic data-type encryption policy;
- Roaming partner specific data-type encryption policies that will take precedence over a generic data-type encryption policy if present;
- NF API data-type placement mappings;
- Multiple modification policies, to handle modifications that are specific per IPX provider and modification policies that are specific per IPX provider and roaming partner.

The SEPP shall also be able to store and process the following policies for incoming messages during the initial connection establishment via N32-c:

- Roaming partner specific data-type encryption policies;
- Roaming partner specific modification policies that specify which fields can be modified by which of its IPX providers.

13.2.3.6 Precedence of policies in the SEPP

This clause specifies the order of precedence of data-type encryption policies and modification policies available in a SEPP.

In increasing order of precedence, the following policies apply for a message to be sent on N32:

1. The set of default rules specified in the present specification:

   - For the data-type encryption policy, the rules on data-types that are mandatory to be encrypted according to clause 5.9.3.3.

   - For the modification policy, the basic validation rules defined in clause 13.2.3.4.

2. Manually configured policies:

   - For the data-type encryption policy: rules according to clause 13.2.3.2, on a per roaming partner basis.

   - For the modification policy: rules according to clause 13.2.3.4, per roaming partner and per IPX provider that is used for the specific roaming partner.

NOTE 1: It is assumed that operators agree both data-type encryption and modification policy in advance, for example as part of their bilateral roaming agreement. The protection policies exchanged via N32-c during the initial connection establishment only serve the purpose of detecting possible misconfigurations.

NOTE 2: It is assumed that the default rules and manually configured policies do not overlap or contradict each other. The manually configured policies are used to extend the protection by the default rules in the present document and are applied on top of them.

When a SEPP receives a data-type encryption or modification policy on N32-c as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and IPX provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy:

- Send the error message as specified in TS 29.573 [73], clause 6.1.4.3.2, to the peer SEPP.

- Create a local warning.

13.2.4 N32-f connection between SEPPs

13.2.4.1 General

The SEPP receives HTTP/2 request/response messages from the Network Function. It shall perform the following actions on these messages before they are sent on the N32-f interface to the SEPP in the other PLMN:

a) It parses the incoming message and, if present, rewrites the telescopic FQDN of the receiving NF to obtain the original FQDN as described in clause 13.1.

b) It reformats the message to produce the input to JSON Web Encryption (JWE) [59] as described in clause 13.2.4.3.

c) It applies JWE to the input created in b) to protect the reformatted message as described in clause 13.2.4.4.

d) It encapsulates the resulting JWE object into a HTTP/2 message (as the body of the message) and sends the HTTP/2 message to the SEPP in the other PLMN over the N32-f interface.

The message may be routed via the cIPX and pIPX nodes. These IPX nodes may modify messages as follows:

a) The IPX node recovers the cleartext part of the HTTP message from the JWE object, modifies it according to the modification policy, and calculates an "operations" JSON Patch object. It then creates a temporary JSON object with the "operators" JSON Patch object and some other parameters for replay protection etc. as described in clause 13.2.4.5.1.

b) The IPX node uses the temporary JSON object as input into JSON Web Signature (JWS) [45] to create a JWS object, as described in clause 13.2.4.5.2.

c) The IPX node appends the JWS object to the received message and sends it to the next hop.

The JWS objects generated by the two IPX providers form an auditable chain of modifications that to the receiving SEPP shall apply to the parsed message after verifying that the patches conform to the modification policy.

Encryption of IEs shall take place end to end between cSEPP and pSEPP.

A SEPP shall not include IEs in the clear that are encrypted elsewhere in the JSON object.

A SEPP shall verify that an intermediate IPX has not moved or copied an encrypted IE to a location that would be reflected from the producer NF in an IE without encryption.

13.2.4.2 Overall Message payload structure for message reformatting at SEPP

The SEPP reformats an HTTP message received from an internal Network Function into two temporary JSON objects that will be intput to JWE:

a. The **dataToIntegrityProtect**, containing information that is only integrity protected. It consists of the following:

- clearTextEncapsulationMessage: contains the complete original HTTP message, excluding attribute values which require encryption and, including the pseudo-header fields, HTTP headers and HTTP message body.

- metadata: contains SEPP generated information i.e. authorizedIPX ID, N32-f message ID and N32-f context ID.

b. The **dataToIntegrityProtectAndCipher**: contains attribute values of the original message that require both encryption and integrity protection.

For the details of JSON representation of a reformatted HTTP message, refer to TS 29.573 [92].

13.2.4.3 Message reformatting in sending SEPP

13.2.4.3.1 dataToIntegrityProtect

13.2.4.3.1.1 clearTextEncapsulatedMessage

The clearTextEncapsulatedMessage is a JSON object that contains the non-encrypted portion of the original message.Specifically, it consists of the following objects:

1.a) Pseudo_Headers – the JSON object that includes all the Pseudo Headers in the message.

- For HTTP Request messages, the object contains one entry for each of the ":method", ":path", ":scheme" and ":authority" pseudo headers. If the ":path" pseudoheader contains multiple parts separated by a slash (/) or includes a query parameter (following a "?"), an array is used to represent :path, with one element per part of the path (i.e. per "directory").

NOTE: This enables encryption of individual elements of the path (e.g. if SUPI is passed).

- For HTTP Response messages, the object contains the ":status" pseudo header.

1.b) HTTP_Headers – the JSON object that includes all the Headers in the message.

All the headers of the request are put into a JSON array called HTTP_Headers.Each entry contains a header name and value, where the value part can be an encoded index to the dataToIntegrityProtectAndCipher block, if the header value is encrypted.

1.c) Payload – the JSON object that includes the content of the payload of the HTTP message.

Each attribute or IE in the payload shall form a single entry in the Payload JSON object. If there is any attribute value that requires encryption, it shall be moved into the dataToIntegrityProtectAndCipher JSON object (clause 13.2.4.2), and the original value in this element shall be replaced by the index in the form {"encBlockIdx": <num>} where "num" is the index of the corresponding entry in the dataToIntegrityProtectAndCipher array.

13.2.4.3.1.2 metadata

The JSON object containing information added by the sending SEPP. It shall contain:

a) N32-f **message ID**: Unique identifier (64-bit integer) representing a HTTP Request/Response transaction between two SEPPs. The N32-f message ID is generated by the sending SEPP and included in the HTTP Request sent over the N32 interface. The receiving SEPP uses the same N32-f message ID when it responds back with a HTTP Response. The N32-f message ID is included in the metadata portion of the JSON structure.

b) **authorizedIPX ID**: String identifying the first hop IPX (cIPX or pIPX) that is authorized to update the message. This field shall always be present. When there is no IPX that is authorized to update, the value of this field is set to null. The sending SEPP selects one of the IPX providers from the list exchanged with the other SEPP during parameter exchange over N32-c and includes its identifier value in this field.

c) **N32-f context ID**: Unique identifier representing the N32-f context information used for protecting the message. This is exchanged during parameter exchange over N32-c (clause 13.2.2.4.1).

13.2.4.3.2 dataToIntegrityProtectAndCipher

The dataToIntegrityProtectAndCipher is a JSON patch document as per RFC 6902 [64] that contains all the attribute values that require both encryption and integrity protection. Attribute values may come from any part of the original HTTP message – Pseudo_Headers, HTTP_Headers and Payload.

The JSON array shall contain one array entry per attribute value that needs encryption. Each array entry represents the value of the attribute to be protected, and the index in the array is used to reference the protected value within the dataToIntegrityProtect block. This associates each attribute in the dataToIntegrityProtectAndCipher block with the original attribute in the dataToIntegrityProtect block. This is needed to reassemble the original message at the receiving SEPP.

13.2.4.4 Protection using JSON Web Encryption (JWE)

13.2.4.4.0 General

The SEPP shall use JSON Web Encryption (JWE) as specified in RFC 7516 [59] for the protection of reformatted HTTP messages between the SEPPs. All encryption methods supported by JWE are AEAD methods, i.e. methods that encrypt and integrity protect in one single operation and can additionally integrity protect additional data.

The dataToIntegrityProtectAndCipher and dataToIntegrityProtect blocks shall be input to JWE as plaintext and JWE Additional Authenticated Data (AAD) respectively. The JWE AEAD algorithm generates JWE encrypted text (ciphertext) and a JWE Authentication Tag (Message Authentication Code). The ciphertext is the output from symmetrically encrypting the plaintext, while the authentication tag is a value that verifies the integrity of both the generated ciphertext and the Additional Authenticated Data.

The Flattened JWE JSON Serialization syntax shall be used to represent JWE as a JSON object.

The session key shared between the two SEPPs, as specified in clause 13.2.4.4.1, shall be used as the Content Encryption Key (CEK) value to the algorithm indicated in the Encryption algorithm ("enc") parameter in the JOSE header. The algorithm ("alg") parameter in the JOSE header denoting the key exchange method shall be set to "dir", i.e. "Direct use of a shared symmetric key as the CEK".

The 3GPP profile for supported cipher suites in the "enc" parameter is described in clause 13.2.4.9.

The generated JWE object shall be transmitted on the N32-f interface in the payload body of a SEPP to SEPP HTTP/2 message.

13.2.4.4.1 N32-f key hierarchy

The N32-f key hierarchy is based on the N32-f master key generated during the N32-c initial handshake by TLS key export. The N32-f key hierarchy consists of two pairs of session keys and two pairs of IV salts, which are used in two different HTTP/2 sessions. In one Session the N32-c initiator acts as the HTTP client and in the second the N32-c responder acts as the client.

If the exported master secret is reused to set up multiple HTTP sessions or to set up new HTTP sessions on stream ID exhaustion, a new, unique, N32-f Context ID shall be generated to avoid key and IV re-use.

The master key shall be obtained from the TLS exporter. The export function takes 3 arguments: Label, Context, Length (in octets) of the desired output. For the N32 Master key derivation, the Label shall be the IANA registered label "EXPORTER_3GPP_N32_MASTER" [89], the Context shall be "" (the empty string) and the Length shall be 64.

The N32 key derivation function N32-KDF shall be based on HKDF [62] and shall use only the HKDF-Expand function as the initial key material has been generated securely:

N32-KDF (label, L) = HKDF-Expand (N32-f master key, "N32" || N32-Context-ID || label, L),

where

- label is a string used for key separation,
- L is the length of output keying material in octets.

Each run of N32-KDF (label, L) produces either one session key or one IV salt.

There are two pairs of session keys and IV salts to be derived.

NOTE: In AES-GCM re-use of one IV may reveal the integrity key (Joux's Forbidden attack). The binding of session keys and IV salts to N32-f context IDs and labels is essential to protect against inadvertent use of the same key with a repeated IV.

The labels for the JWE keys are:

- "parallel_request_key"
- "parallel_response_key"
- "reverse_request_key", and
- "reverse_response_key".

The keys derived with labels starting parallel shall be used for request/responses in an HTTP session with the N32-c initiating SEPP acting as the client (i.e. in parallel to the N32-c connection). The keys derived with the labels starting reverse shall be used for an HTTP session with the N32-c responding SEPP acting as the client.

To generate the IV salts, the length is 8 and the labels are:

- "parallel_request_iv_salt",
- "parallel_response_iv_salt",
- "reverse_request_iv_salt", and
- "reverse_response_iv_salt".

The 96-bit nonce for AES_GCM shall be constructed as the concatenation of the IV salt (8 octets, 64-bits) and the sequence counter, SEQ, following section 8.2.1 of NIST Special Publication 800-38D [63]:

Nonce = IV salt || SEQ.

The sequence counter shall be a 32-bit unsigned integer that starts at zero and is incremented for each invocation of the encryption. A different sequence counter shall be maintained for each IV salt.

13.2.4.5 Message modifications in IPX

13.2.4.5.1 modifiedDataToIntegrityProtect

```
modifiedDataToIntegrityProtect =
{
   ”Operations” : JSON Patch that captures
         IPX provider modifications,
   ”Identity” : ”IPX1",
   ”Tag” : JWE Tag generated by sending
         SEPP
}
```

Figure 13.2.4.5.1-1 Example of JSON representation of IPX provider modifications

This is a temporary JSON object generated by an IPX provider as it modifies the original message. It shall contain the following:

a) **Operations** – This is a JSON patch document that captures IPX modifications based on RFC 6902 [64]. If no patch is required, the operations element shall be set to null.

b) **Identity** – This is the identity of the IPX performing the modification.

c) **Tag** – A JSON string element to capture the “tag” value (JWE Authentication tag) in the JWE object generated by the sending SEPP. This is required for replay protection.

NOTE: Since there is no central registry that can ensure unique IPX Identities, it is expected that an IPX will include its Fully Quantified Domain Name (FQDN) in the JSON modification object.

13.2.4.5.2 Modifications by IPX

NOTE 1: It is assumed that operators act as a certification authority for IPX providers they have a direct business relationship with. In order to authorize N32-f message modifications, operators sign a digital certificate for each of these IPX providers and provide it to both the IPX provider itself as well as their roaming partners to enable them to validate any modifications by this IPX provider.

Only cIPX and pIPX shall be able to modify messages between cSEPP and pSEPP. In cases of messages from cSEPP to pSEPP, the cIPX is the first intermediary, while the pIPX is the second intermediary. In cases of messages from pSEPP to cSEPP the pIPX is the first intermediary, while the cIPX is the second intermediary.

The first intermediary shall parse the encapsulated request (i.e. the clearTextEncapsulationMsg in the dataToIntegrityProtect block) and determine which changes are required. The first intermediary creates an Operations JSON patch document to describe the differences between received and desired message, using the syntax and semantic from RFC 6902 [64], such that, when applying the JSON patch to the encapsulated request the result will be the desired request. If no patch is required, the operations element is null.

NOTE 2: It is necessary to create a JWS object even if no patch is required to prevent deletion of modifications.

The first intermediary shall create a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.4.5.1. The JSON object shall include the intermediary’s identity and the JWE authentication tag, which associates this update by the intermediary with the JWE object created by the sending SEPP.

The first intermediary shall use the modifiedDataToIntegrityProtect JSON object as input to JWS to create a JWS object. The first intermediary shall append the generated JWS object to the payload in the HTTP message and then send the messageto the next hop.

The second intermediary shall parse the encapsulated request, apply the modifications described in the JSON patch appended by the first intermediary and determine further modifications required for obtaining the desired request. The second intermediary shall record these modifications in an additional JSON patch against the JSON object resulting from application of the first intermediary's JSON patch. If no patch is required, the operations element for the second JSON patch is null.

The second intermediary shall create a modifiedDataToIntegrityProtect JSON object as described in clause 13.2.4.5.1. It shall include its identity and the JWE authentication tag, which associates this update by the second intermediary with the JWE object created by the sending SEPP.

The second intermediary shall use the modifiedDataToIntegrityProtect JSON object as input to JWS to create a JWS object. The second intermediary shall append the generated JWS object to the payload in the HTTP message and then send the message to the receiving SEPP.

13.2.4.6 Protecting IPX modifications using JSON Web Signature (JWS)

The IPX providers shall use JSON Web Signature (JWS) as specified in RFC 7515 [45] for the protection of IPX provider modified attributes. The mechanism described in this clause uses signatures, i.e. asymmetric methods, with private/public key pairs.

More specifically, when an IPX node modifies one or more attributes of the original HTTP message and creates a modifiedDataToIntegrityProtect object to record its modifications, it shall use JWS to integrity protect the modifiedDataToIntegrityProtect object.

The IPX provider shall use its private key as input to JWS for generating the signature representing the contents of the modifiedDataToIntegrityProtect object.

The "alg" parameter in the JOSE header indicates the chosen signature algorithm. The 3GPP profile for supported algorithms is described in clause 13.2.4.9.

The Flattened JWS JSON Serialization syntax shall be used to represent JWS as a JSON object.

13.2.4.7 Message verification by the receiving SEPP

The receiving SEPP shall decrypt the JWE ciphertext using the shared session key and the following parameters obtained from the JWE object – Initialization Vector, Additional Authenticated Data value (clearTextEncapsulatedMessage in "aad") and JWE Authentication Tag ("tag").

The receiving SEPP shall check the integrity and authenticity of the clearTextEncapsulatedMessage and the encrypted text by verifying the JWE Authentication Tag in the JWE object with the JWE AAD algorithm. The algorithm returns the decrypted plaintext (dataToIntegrityProtectAndCipher) only if the JWE Authentication Tag is correct.

The receiving SEPP refers to the NF API data-type placement mapping table to re-construct the original reformatted message by updating corresponding entries in clearTextEncapsulatedMessage with values in the dataToIntegrityProtectAndCipher array.

The receiving SEPP shall next verify IPX provider updates, if included, by verifying the JWS signatures added by the intermediaries. The SEPP shall verify the JWS signature, using the corresponding raw public key or certificate that is contained in the IPX provider's security information list obtained during parameter exchange in the related N32-c connection setup or, alternatively, has been configured for the particular peer SEPP. It shall then check that the raw public key or certificate of the JWS signature IPX's Identity in the modifiedDataToIntegrity block matches to the IPX provider referred to in the "authorizedIPX ID" field added by the sending SEPP, based on the information given in the IPX provider security information list.

The receiving SEPP shall check whether the modifications performed by the intermediaries were permitted by the respective modification policies. The receiving SEPP shall use the modification policy of the cIPX obtained during parameter exchange in the related N32-c connection setup, and use the modification policy of pIPX configured within the receiving SEPP.

If this is the case, the receiving SEPP shall apply the patches in the Operations field in order, perform plausibility checks, and create a new HTTP request according to the "patched" clearTextEncapsulatedMessage.

The receiving SEPP shall verify that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context.

13.2.4.8 Procedure

The following clause illustrates the message flow between the two SEPPs with modifications from cIPX and pIPX.

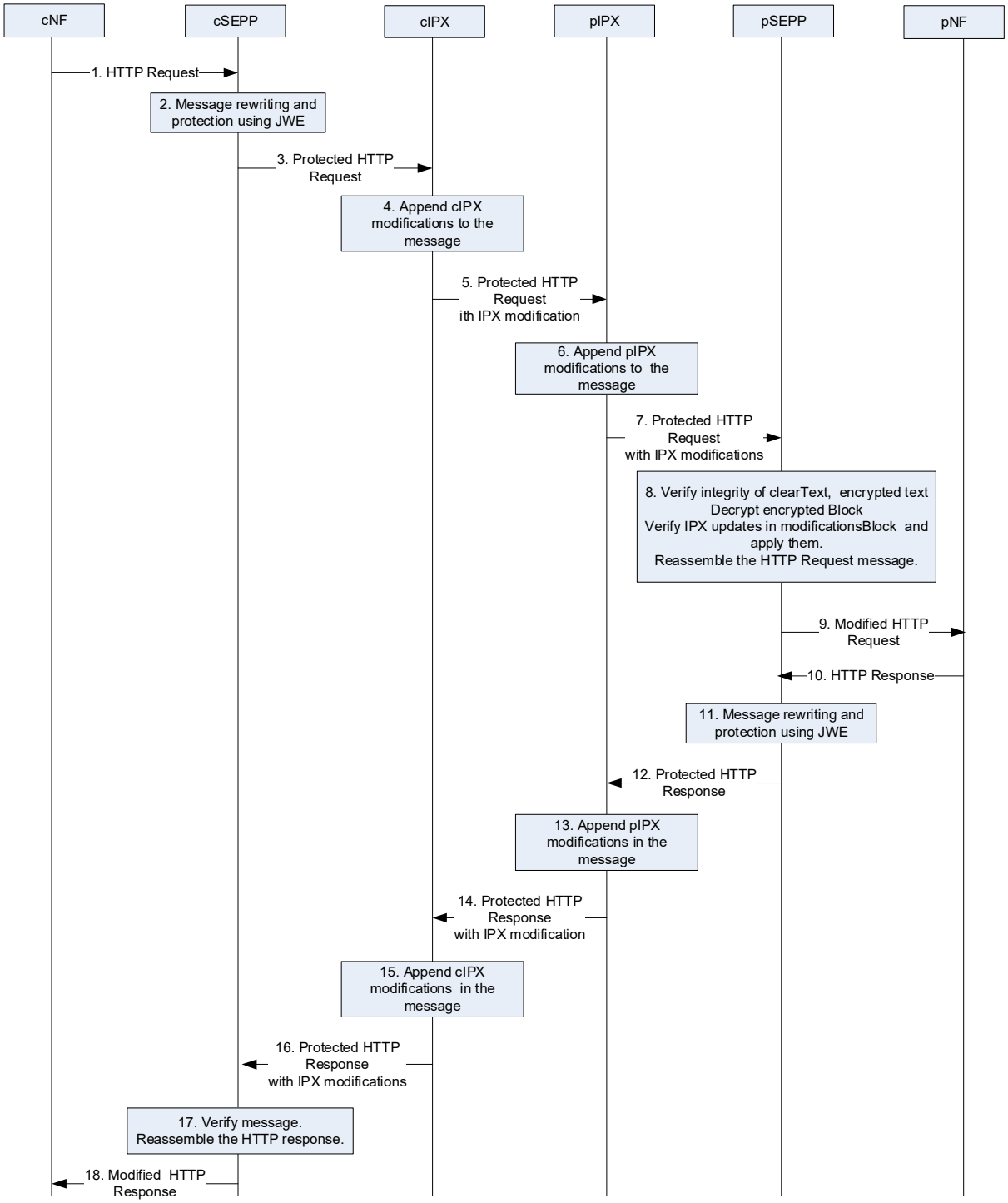


Figure 13.2.4.8-1 Message flow between two SEPPs

1. The cSEPP receives an HTTP request message from a network function. If the message contains a telescopic FQDN, the cSEPP removes its domain name from this FQDN to obtain the original FQDN as described in clause 13.1.

2. The cSEPP shall reformate the HTTP Request message as follows:

   a. The cSEPP shall generate blocks (JSON objects) for integrity protected data and encrypted data, and protecting them:

The cSEPP shall encapsulate the HTTP request into a clearTextEncapsulatedMessage block containing the following child JSON objects:

- Pseudo_Headers
- HTTP_Headers with one element per header of the original request.
- Payload that contains the message body of the original request.

For each attribute that require end-to-end encryption between the two SEPPs, the attribute value is copied into a dataToIntegrityProtectAndCipher JSON object and the attribute's value in the clearTextEncapsulatedMessage is replaced by the index of attribute value in the dataToIntegrityProtectAndCipher block.

The cSEPP shall create a metadata block that contains the N32-f context ID, message ID generated by the cSEPP for this request/response transaction and next hop identity.

The cSEPP shall protect the dataToIntegrityProtect block and the dataToIntegrityProtectAndCipher block as per clause 13.2.4.4. This results in a single JWE object representing the protected HTTP Request message.

b. The cSEPP shall generate payload for the SEPP to SEPP HTTP message:

The JWE object becomes the payload of the new HTTP message generated by cSEPP.

3. The cSEPP shall use HTTP POST to send the HTTP message to the first intermediary.

4. The first intermediary (e.g. visited network's IPX provider) shall create a new modifiedDataToIntegrityProtect JSON object with three elements:

   a. The Operations JSON patch document contains modifications performed by the first intermediary as per RFC 6902 [64].

   b. The first intermediary shall include its own identity in the Identity field of the modifiedDataToIntegrityProtect.

   c. The first intermediary shall copy the "tag" element, present in the JWE object generated by the cSEPP, into the modifiedDataToIntegrityProtect object. This acts as a replay protection for updates made by the first intermediary.

The intermediary shall execute JWS on the modifiedDataToIntegrityProtect JSON object and append the resulting JWS object to the message.

5. The first intermediary shall send the modified HTTP message request to the second intermediary (e.g. home network's IPX) as in step 3.

6. The second intermediary shall perform further modifications as in step 4 if required. The second intermediary shall further execute JWS on the modifiedDataToIntegrityProtect JSON object and shall append the resulting JWS object to the message.

7. The second intermediary shall send the modified HTTP message to the pSEPP as in step 3.

NOTE 1: The behaviour of the intermediaries is not normative, but the pSEPP assumes that behaviour for processing the resulting request.

8. The pSEPP receives the message and shall perform the following actions:

   - The pSEPP extracts the serialized values from the components of the JWE object.
   - The pSEPP invokes the JWE AEAD algorithm to check the integrity of the message and decrypt the dataToIntegrityProtectAndCipher block. This results in entries in the encrypted block becoming visible in cleartext.
   - The pSEPP updates the clearTextEncapsulationMessage block in the message by replacing the references to the dataToIntegrityProtectAndCipher block with the referenced decrypted values from the dataToIntegrityProtectAndCipher block.
   - The pSEPP then verifies IPX provider updates of the attributes in the modificationsArray. It checks whether the modifications performed by the intermediaries were permitted by policy.

The pSEPP further verifies that the PLMN-ID contained in the message is equal to the "Remote PLMN-ID" in the related N32-f context.

- The pSEPP updates the modified values of the attributes in the clearTextEncapsulationMessage in order.

The pSEPP shall re-assemble the full HTTP Request from the contents of the clearTextEncapsulationMessage.

9. The pSEPP shall send the HTTP request resulting from step 8 to the home network's NF.

10.-18.These steps are analogous to steps 1.-9.

13.2.4.9 JOSE profile

SEPPs shall follow the JWE profile defined in TS 33.210 [3] with the restriction that it shall only use AES GCM with a 128-bit or 256-bit key. The security considerations for the use of AES GCM in section 8.4 of RFC 7518 [59] shall be taken into account. In particular, the same key shall not be used more than 2^{32} times and an IV value shall not be used more than once with the same key.

SEPPs and IPXs shall follow the JWS profile as defined in TS 33.210 [3] with the restriction that they shall only use ES256 algorithm.

13.3 Authentication and static authorization

13.3.0 Static authorization

Static authorization is based on local authorization policy at the NRF and the NF Service Producer. It can be used when token-based authorization is not used.

During the Nnrf_NFDiscovery procedure, the NRF ensures that the NF Service Consumer is authorized to discover the NF Service Producer service(s) as specified in clause 13.3.1.3 of this document.

If token-based authorization is not used within one PLMN and the NF Service Producer receives a service request, the NF Service Producer shall check authorization of the NF Service Consumer based on its local policy. If the NF Service Consumer is authorized to receive the service requested, the NF Service Producer shall grant the NF Service Consumer access to the service API.

13.3.1 Authentication and authorization between network functions and NRF

13.3.1.1 Direct communication

NRF and NF shall authenticate each other during discovery, registration, and access token request.

In direct communication, NF and NRF shall use one of the following methods for authentication:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.

- If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

13.3.1.2 Indirect communication

In indirect communication, NF and NRF shall use one of the following methods for authentication:

- Mutual authentication between NF and NRF provided by the transport layer protection solution.

- Client credentials assertion (CCA) based authentication as specified in clause 13.3.8.

NOTE 1: Client credentials assertion authentication is based on a CCA token sent by the NF Service Consumer to the NRF via an intermediate such as the SCP. CCA based authentication does not provide authentication of the NRF towards the NF Service Consumer or protection of the service request sent by the NF Service Consumer to the NRF.

- Implicit, i.e. by relying on authentication between NF Service Consumer and SCP, and between SCP and NRF, provided by the hop-by-hop security protection at the transport layer, NDS/IP, or physical security.

NOTE 2: Mutual authentication between NF Service Consumer and NRF is not achieved with hop-by-hop security.

NOTE 3: If only hop-by-hop security is used in a PLMN, the NRF is not able to verify that an access token request sent by SCP on behalf of a certain NF Service Consumer, is actually authorized by this consumer.

13.3.1.3 Authorization of discovery request and error handling

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf_NFDiscovery_Request based on the profile of the expected NF/NF service and the type of the NF Service Consumer, as described in clause 4.17.4 of TS23.502 [8].

In the roaming scenario, the NRF of the NF Service Producer shall authorize the Nnrf_NFDiscovery_Request based on the profile of the expected NF/NF Service, the type of the NF Service Consumer and the serving network ID.

If the NRF finds NF Service Consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

NOTE 1: Void.

When a NF consumes the Nnrf_NFManagement or the Nnrf_NFDiscovery services provided by the NRF, the usage of the OAuth 2.0 access token for authorization between the NF and the NRF is optional.

13.3.2 Authentication and authorization between network functions

13.3.2.1 Direct communication

In direct communication, authentication between network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between NFs.

- If the PLMN does not use protection at the transport layer, authentication between NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

13.3.2.2 Indirect communication

In indirect communication scenarios, the NF Service Producer and NF Service Consumer shall use implicit authentication by relying on authentication between NF Service Consumer and SCP, and between SCP and NF Service Producer, provided by the transport layer protection solution, NDS/IP, or physical security.

NOTE 0: Mutual authentication between NF Service Consumer and NF Service Producer is not achieved with hop-by-hop security.

If the PLMN uses token-based authorization as specified by clause 13.4.1.2 and the PLMN's policy mandates that the NRF authenticates the NF Service Consumer before granting an access token, the access token indicates to the NF Service Producer that the NF Service Consumer has been authenticated by the NRF.

If additional authentication of the NF Service Consumer is required, the NF Service Producer authenticates the NF Service Consumer at the application layer using CCA based authentication as specified in clause 13.3.8.

The NF Service Consumer authentication based on CCA based authentication is optional to use, and based on operator policy.

13.3.2.3 Inter-PLMN NF to NF communication

NOTE 1: Void

NOTE 2: Void

The Inter-PLMN UP Security functionality (IPUPS) as described in clauses 4.2.2 and 5.9.3.4 provide a standardised solution for binding 5G SBA REST Service Operations between the PLMN V-SMF and H-SMF over N16 / N32 to GTP-U over N9 in roaming scenarios.

13.3.2.4 Error handling

When an NF receives a message from an unauthenticated NF, the receiving NF shall support error handling, and may send back an error message.

13.3.3 Authentication and authorization between SEPP and network functions

NOTE 1: This clause also describes authentication and authorization between SEPP and NRF, because the NRF is a network function.

Authentication between SEPP and network functions within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between SEPP and NFs.

- If the PLMN does not use protection at the transport layer, authentication between SEPP and NFs within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

A network function and the SEPP shall mutually authenticate before the SEPP forwards messages sent by the network function to network functions in other PLMN, and before the SEPP forwards messages sent by other network functions in other PLMN to the network function.

13.3.4 Authentication and authorization between SEPPs

Authentication and authorization between SEPPs in different PLMNs is defined in clause 13.2.

13.3.5 Authentication between SEPP and SCP

Authentication between SEPP and SCP within one PLMN shall use one of the following methods:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for authentication between SEPP and SCP.

- If the PLMN does not use protection at the transport layer, authentication between SEPP and SCP within one PLMN may be implicit by NDS/IP or physical security (see clause 13.1).

A SCP and the SEPP shall mutually authenticate before forwarding incoming or outgoing requests.

13.3.6 Authentication and authorization between SCP and network functions

The SCP and network functions shall use one of the following methods described in clause 13.1 to mutually authenticate each other before service layer messages can be exchanged on that interface:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for mutual authentication of the SCP and the network functions.
- If the PLMN does not use protection at the transport layer, mutual authentication of the SCP and network functions may be implicit by NDS/IP or physical security.

Authentication between the SCP and the Network Function may be implicit by co-location.

Authorization between the SCP and NFs is based on local authorization policy. Regarding the authorization of access token requests sent by an SCP on behalf of an NF Service Consumer, NOTE 3 in clause 13.3.1.2 applies.

13.3.7 Authentication and authorization between SCPs

SCPs shall use one of the following methods as described in 13.1 to mutually authenticate each other before service layer messages can be exchanged on that interface:

- If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for mutual authentication of the SCPs.
- If the PLMN does not use protection at the transport layer, mutual authentication of the two SCPs may be implicit by NDS/IP or physical security.

Authorization between SCPs is based on local authorization policy.

13.3.8 Client credentials assertion based authentication

13.3.8.1 General

The Client credentials assertion (CCA) is a token signed by the NF Service Consumer. It enables the NF Service Consumer to authenticate towards the receiving end point (NRF, NF Service Producer) by including the signed token in a service request.

It includes the NF Service Consumer's NF Instance ID that can be checked against the certificate by the NF Service Producer. The CCA includes a timestamp as basis for restriction of its lifetime.

CCAs are expected to be more short-lived than NRF generated access tokens. So, they can be used in deployments with requirements for tokens with shorter lifetime for NF-NF communication. There is a trade-off that when the lifetime of the CCA is too short, it requires the NF Service Consumer to generate a new CCA for every new service request.

The CCA cannot be used in the roaming case, as the NF Service Producer in the home PLMN will not be able to verify the signature of the NF Service Consumer in the visited PLMN unless cross-certification process is established between the two PLMNs through one of the mechanisms specified in TS 33.310.

CCA does not provide integrity protection on the full service request. Neither does it provide a mechanism for the NF Service Consumer to authenticate the NF Service Producer.

In this clause, CCAs are described generally for both NF-NRF communication and NF-NF communication.

13.3.8.2 Client credentials assertion

CCAs shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures based on JSON Web Signature (JWS) as described in RFC 7515 [45].

The CCA shall include:

- the NF instance ID of the NF Service Consumer (subject);
- A timestamp (iat) and an expiration time (exp), and
- The NF type of the expected audience (audience), i.e. the type "NRF" and/or the NF type of the NF Service Producer.

The NF Service Consumer shall digitally sign the generated CCA based on its private key as described in RFC 7515 [45]. The signed CCA shall include one of the following fields:

- the X.509 URL (x5u) to refer to a resource for the X.509 public key certificate or certificate chain used for signing the client authentication assertion, or
- the X.509 Certificate Chain (x5c) include the X.509 public key certificate or certificate chain used for signing the client authentication assertion.

13.3.8.3 Verification of Client credentials assertion

The verification of the CCA shall be performed by the receiving node, i.e., NRF or NF Service Producer in the following way:

- It validates the signature of the JWS as described in RFC 7515 [45].
- It validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519 [44].

  If the receiving node is the NRF, the NRF validates the timestamp (iat) and the expiration time (exp).

  If the receiving node is the NF Service Producer, the NF Service Producer validates the expiration time and it may validate the timestamp.
- It checks that the audience claim in the the CCA matches its own type.
- It verifies that the NF instance ID of the NFc in the CCA matches the NF instance ID in the public key certificate used for signing the CCA.

13.4 Authorization of NF service access

13.4.1 OAuth 2.0 based authorization of Network Function service access

13.4.1.0 General

The authorization framework described in clause 13.4.1 allows NF Service Producers to authorize the requests from NF Service requestors.

The authorization framework uses the OAuth 2.0 framework as specified in RFC 6749 [43]. Grants shall be of the type Client Credentials Grant, as described in clause 4.4 of RFC 6749 [43]. Access tokens shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45].

NOTE 1a: Securing the access token using Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a pairwise pre-shared symmetric key between the NRF and the NF Service Producer. The provisioning of such pre-shared symmetric key is outside the scope of this document.

The basic extent provided by the authorization token is at service level (i.e. the "scope" claim includes allowed services per NF type). Depending on the NF Service Producer configuration, higher level of granularity for the authorization token can be defined adding "additional scope" information within the token e.g. to authorize specific service operations and/or resources/data sets within service operations per NF Service Consumer type.

NOTE 1: The additional scope(s) included within the access token add additional security checks at the NF Service Producer that authorizes the services operations, resources and NF Service Consumer type related to the additional scope(s).

The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.

13.4.1.1 Service access authorization within the PLMN

13.4.1.1.1 OAuth 2.0 roles

OAuth 2.0 roles, as defined in clause 1.1 of RFC 6749 [43], are as follows:

a. The Network Repository Function (NRF) shall be the OAuth 2.0 Authorization server.

b. The NF Service Consumer shall be the OAuth 2.0 client.

c. The NF Service Producer shall be the OAuth 2.0 resource server.

OAuth 2.0 client (NF Service Consumer) registration with the OAuth 2.0 authorization server (NRF)

The NF Service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], may be used to register the OAuth 2.0 client (NF Service Consumer) with the OAuth 2.0 Authorization server (NRF), as described in clause 2.0 of RFC 6749 [43]. The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF.

A Network Function that does not implement this option shall be able to get an access token from the NRF as long as the NRF is able to authenticate and authorize the Network Function during the NF access token get service request.

OAuth 2.0 resource server (NF Service Producer) registration with the OAuth 2.0 authorization server (NRF)

The NF Service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], shall be used to register the OAuth 2.0 resource server (NF Service Producer) with the OAuth 2.0 Authorization server (NRF). The NF Service Producer, as part of its NF profile, may include "additional scope" information related to the allowed service operations and resources per NF Service Consumer type.

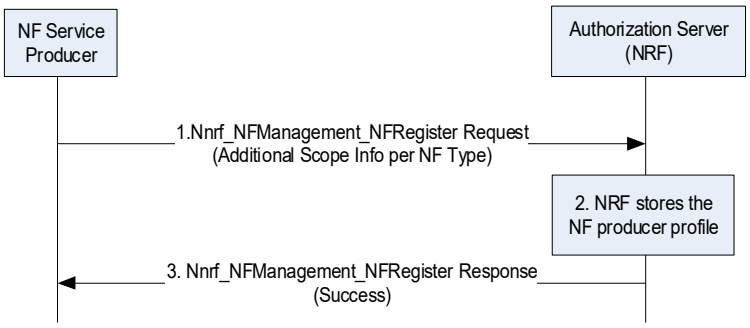


Figure 13.4.1.1-1b NF Service Producer registers in NRF

1) The NF Service Producer registers as OAuth 2.0 resource server in the NRF. The NF profile configuration data of the NF Service Producer may include the "additional scope". The "additional scope" information indicates the resources and the actions (service operations) that are allowed on these resources for the NF Service Consumer. These resources may be per NF type of the NF Service Consumer or per NF instance ID of the NF Service Consumer.

2-3) After storing the NF Profile, NRF responds successfully.

13.4.1.1.2 Service Request Process

The complete service request is a two-step process including requesting an access token by NF Service Consumer (Step 1, i.e. 1a or 1b), and then verification of the access token by NF Service Producer (Step 2).

NOTE: The service request process regarding the enabler for network automation is specified in Annex X.

Step 1: Access token request

Pre-requisite:

- The NF Service consumer (OAuth2.0 client) is registered with the NRF (Authorization Server).

- The NF Service Producer (OAuth2.0 resource server) is registered with the NRF (Authorization Server) with optionally "additional scope" information per NF type.

- The NRF and NF Service Producer share the required credentials.

- The NRF and NF have mutually authenticated each other.

1a. Access token request for accessing services of NF Service Producers of a specific NF type

The following procedure describes how the NF Service Consumer obtains an access token before service access to NF Service Producers of a specific NF type.

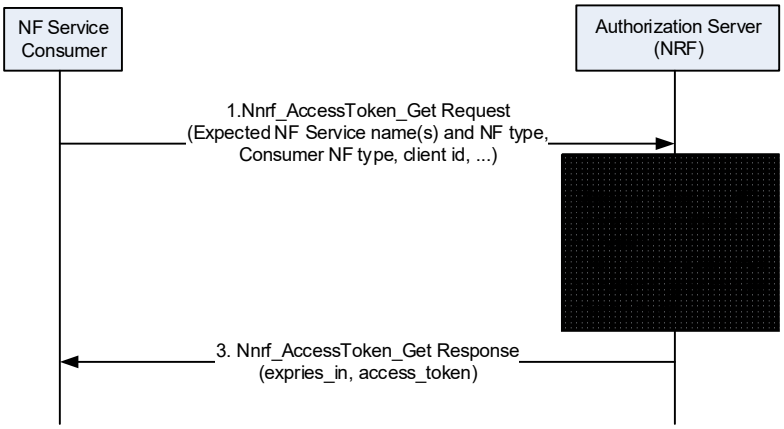


Figure 13.4.1.1.2-1: NF Service Consumer obtaining access token before NF Service access

1. The NF Service Consumer shall request an access token from the NRF in the same PLMN using the Nnrf_AccessToken_Get request operation. The message shall include the NF Instance Id(s) of the NF Service Consumer, the requested "scope" including the expected NF Service name(s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF type of the expected NF Service Producer instance and NF Service Consumer. The NF Service Consumer may also include a list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances.
   The message may include the NF Set ID and/or NF Service Set Id of the expected NF Service Producer instances.
   The message may include a list of S-NSSAIs of the NF Service Consumer.

2. The NRF may verify that the input parameters (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF Service Consumer or those in the NF profile of the NF Service Consumer. The NRF checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the NRF shall then generate an access token with appropriate claims included. The NRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

   The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer (subject), NF type of the NF Service Producer (audience), expected service name(s), (scope), expiration time (expiration) and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources). The claims may include a list of NSSAIs or NSI IDs for the expected NF Service Producer instances. The claims may include the NF Set ID and/or NF Service Set Id of the expected NF Service Producer instances.

3. If the authorization is successful, the NRF shall send access token to the NF Service Consumer in the Nnrf_AccessToken_Get response operation, otherwise it shall reply based on Oauth 2.0 error response defined in

RFC 6749 [43]. The other parameters (e.g., the expiration time, allowed scope) sent by NRF in addition to the access token are described in TS 29.510 [68].

The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Service Producer NF type listed in claims (scope, audience) during their validity time.

1b. Access token request for accessing services of a specific NF Service Producer instance / NF Service Producer service instance

The following steps describes how the NF Service Consumer obtains an access token before service access to a specific NF Service Producer instance / NF Service Producer service instance. 1. The NF Service Consumer shall request an access token from the NRF for a specific NF Service Producer instance / NF Service Producer service instance. The request shall include the NF Instance Id(s) of the requested NF Service Producer, the expected NF Service name, optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources) and NF Instance Id of the NF Service Consumer.

2.The NRF checks whether the NF Service Consumer is authorized to use the requested NF Service Producer instance/NF Service Producer service instance, and then proceeds to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer (subject), NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer (audience), expected service name(s) (scope), optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources), and expiration time (expiration).

3. The token shall be included in the Nnrf_AccessToken_Get response sent to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer instance listed in claims (scope, audience) during their validity time.

Step 2: Service access request based on token verification

The following figure and procedure describe how authorization is performed during Service request of the NF Service Consumer. Prior to the request, the NF Service Consumer may perform Nnrf_NFDiscovery_Request operation with the requested additional scopes to select a suitable NF Service Producer (resource server) which is able to authorize the Service Access request.

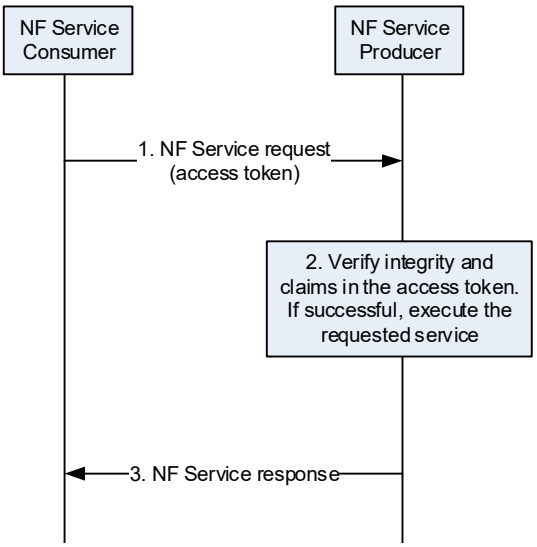


Figure 13.4.1.1.2-2: NF Service Consumer requesting service access with an access token

Pre-requisite: The NF Service Consumer is in possession of a valid access token before requesting service access from the NF Service Producer.

1. The NF Service Consumer requests service from the NF Service Producer. The NF Service Consumer shall include the access token.

   The NF Service Consumer and NF Service Producer shall authenticate each other following clause 13.3.

2. The NF Service Producer shall verify the token as follows:

   - The NF Service Producer ensures the integrity of the token by verifying the signature using NRF's public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service Producer shall verify the claims in the token as follows:

NOTE: Void.

   - It checks that the audience claim in the access token matches its own identity or the type of NF Service Producer. If a list of NSSAIs or list of NSI IDs is present, the NF Service Producer shall check that it serves the corresponding slice(s).

   - If an NF Set ID present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.

     If an NF Service Set ID present, the NF Service Producer shall check if the NF Service Consumer is authorized to access the requested service according to NF Service Producer Service Set ID in the access token claim.

   - If scope is present, it checks that the scope matches the requested service operation.

   - If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.

   - It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

   - If the CCA is present in the service request, it may verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.

3. If the verification is successful, the NF Service Producer shall execute the requested service and responds back to the NF Service Consumer. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43].

13.4.1.1A Service access authorization in interconnect scenarios

In the inter-PLMN interconnect scenario, OAuth 2.0 roles are as follows:

a. The NF Service Consumer's Network Repository Function (cNRF) shall be the OAuth 2.0 Authorization server for the PLMN of the NF Service Consumer (cPLMN) and authenticates the NF Service Consumer.

b. The NF Service Producer's Network Repository Function (pNRF) shall be OAuth 2.0 Authorization server for the PLMN of the NF Service Producer (pPLMN) and generates the access token.

c. The NF Service Consumer in the cPLMN shall be the OAuth 2.0 client.

d. The NF Service Producer in the pPLMN shall be the OAuth 2.0 resource server.

As an example of the inter-PLMN interconnect use case, service access authorization in the roaming scenario where the service consumer NF is located in the visited PLMN and the service producer NF is located in the home PLMN is specified in clause 13.4.1.2.

13.4.1.2 Service access authorization in roaming scenarios

13.4.1.2.1 OAuth 2.0 roles

In the roaming scenario, OAuth 2.0 roles are as follows:

a. The visited Network Repository Function (vNRF) shall be the OAuth 2.0 Authorization server for vPLMN and authenticates the NF Service Consumer.

b. The home Network Repository Function (hNRF) shall be OAuth 2.0 Authorization server for hPLMN and generates the access token.

c. The NF Service Consumer in the visited PLMN shall be the OAuth 2.0 client.

d. The NF Service Producer in the home PLMN shall be the OAuth 2.0 resource server.

OAuth 2.0 client (NF Service Consumer) registration with the OAuth 2.0 authorization server (NRF) in the vPLMN

Same as in the non-roaming scenario in 13.4.1.1.

OAuth 2.0 resource server (NF Service Producer) registration with the OAuth 2.0 authorization server (NRF) in the hPLMN

Same as in the non-roaming scenario in 13.4.1.1.

13.4.1.2.2 Service Request Process

The complete service request is two-step process including requesting an access token by NF Service Consumer (Step 1, i.e. 1a or 1b), and then verification of the access token by NF Service Producer (Step 2).

Step 1: Access token request

Pre-requisite:

- The NF Service consumer (OAuth2.0 client) is registered with the vNRF (Authorization Server in the vPLMN).

- The hNRF and NF Service Producer share the required credentials. Additionally, the NF Service Producer (OAuth2.0 resource server) is registered with the hNRF (Authorization Server in the hPLMN) with optionally "additional scope" information per NF type.

- The two NRFs are implicitly authenticated via N32 mutual authentication of SEPPs.

NOTE: vSEPP to hSEPP communication is secured via N32. Only transitive trust between vNRF and hNRF can be achieved: The vNRF and vSEPP mutually authenticate, the vSEPP and hSEPP mutually authenticate, and the hSEPP and hNRF mutually authenticate. Hence, vNRF and hNRF can only implicitly authenticate each other.

- The NRF in the visited PLMN (vNRF) has authenticated the NF Service Consumer.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Consumer and the vNRF are located in the SNPN while the hNRF is located in the Credentials Holder.

1a. Access token request for accessing services of NF Service Producers of a specific NF type

The following procedure describes how the NF Service Consumer obtains an access token for NF Service Producers of a specific NF type for use in the roaming scenario.

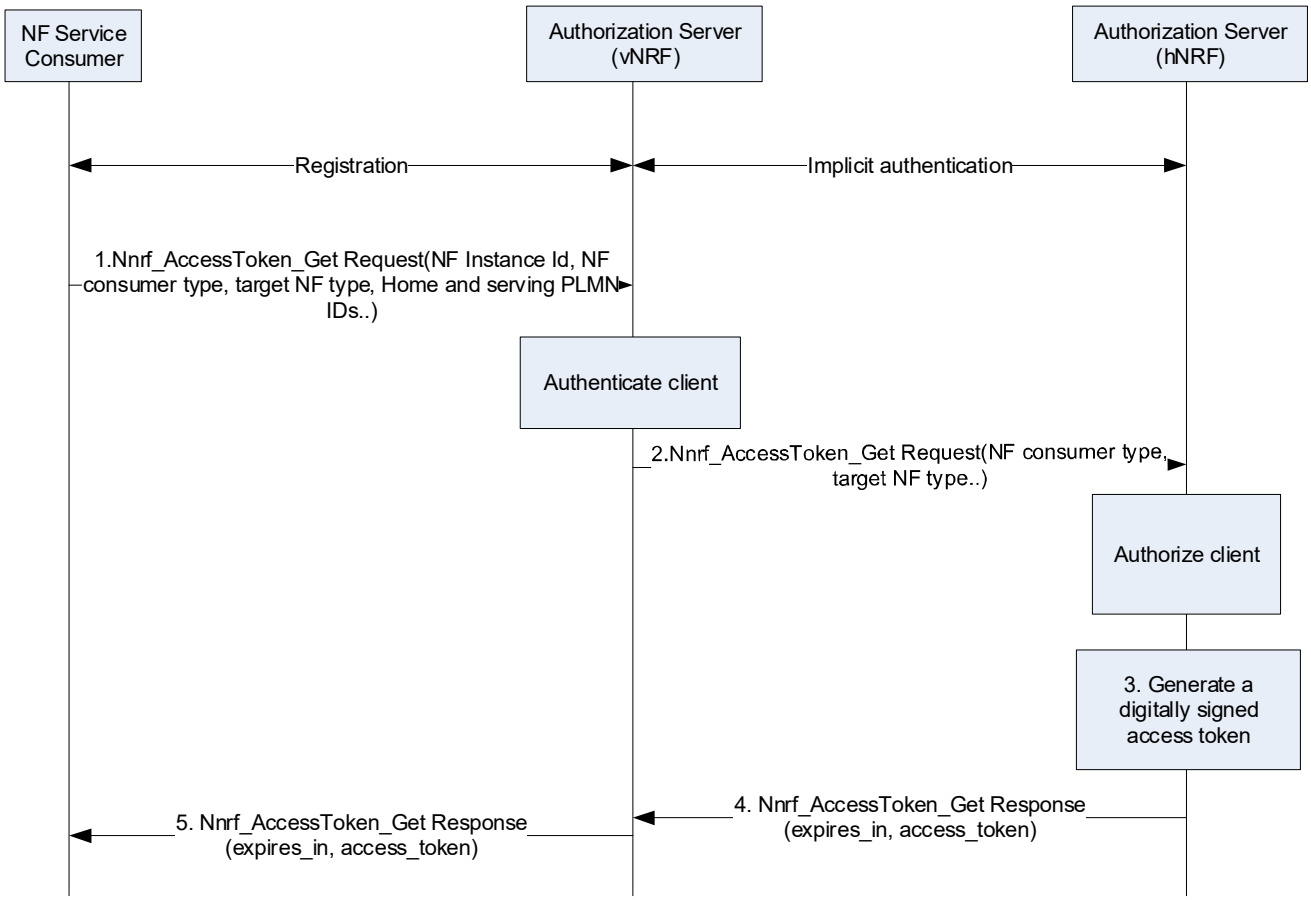


Figure 13.4.1.2.2-1: NF Service Consumer obtaining access token before NF Service access (roaming)

1. The NF Service Consumer shall invoke Nnrf_AccessToken_Get Request (NF Instance Id of the NF Service Consumer, the requested "scope" including the expected NF Service Name (s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF Type of the expected NF Service Producer instance, NF type of the NF Service Consumer, home and serving PLMN IDs, optionally list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances, optionally NF Set ID and/or the NF Service Set ID of the expected NF Service Producer) from NRF in the same PLMN.

   For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the serving PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the home PLMN ID.

2. The NRF in visited PLMN shall identify the NRF in home PLMN (hNRF) based on the home PLMN ID, and request an access token from hNRF as described in clause 4.17.5 of TS 23.502 [8]. The vNRF shall forward the parameters it obtained from the NF Service Consumer, including NF Service Consumer type, to the hNRF.

3. The hNRF checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the hNRF shall generate an access token with appropriate claims included as defined in clause 13.4.1.1. The hNRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. If the NF service consumer is not authorized, the hNRF shall not issue an access token to the NF Service Consumer.

   The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer appended with its PLMN ID (subject), NF type of the NF Service Producer appended with its PLMN ID (audience), expected services name(s), (scope) and expiration time (expiration), and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources). The claims may include a list of NSSAIs or NSI IDs for the expected NF Service Producer instances. The claims may include the NF Set ID and/or the NF Service Set ID of the expected NF Service Producer instances.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

4. If the authorization is successful, the access token shall be included in Nnrf_AccessToken_Get Response message to the vNRF. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43].

5. The vNRF shall forward the Nnrf_AccessToken_Get Response or error message to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Service Producer NF type listed in claims (scope, audience) during their validity time. The other parameters (e.g., the expiration time, allowed scope) sent by NRF in addition to the access token are described in TS 29.510 [68].

1b. Obtain access token for accessing services of a specific NF Service Producer instance / NF Service Producer service instance

The following steps describes how the NF Service Consumer obtains an access token before service access to a specific NF Service Producer instance / NF Service Producer service instance.

1. The NF Service Consumer shall request an access token from the NRF for a specific NF Service Producer instance / NF Service Producer service instance. The request shall include the NF Instance Id of the requested NF Service Producer, appended with its PLMN ID, the expected NF service name and NF Instance Id of the NF Service Consumer, appended with its PLMN ID.

   For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

2. The NRF in the visited PLMN shall forward the request to the NRF in the home PLMN.

3. The NRF in the home PLMN checks whether the NF Service Consumer is authorized to use the requested NF Service Producer instance/NF Service Producer service instance and shall then proceed to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF in the home PLMN shall not issue an access token to the NF Service Consumer.

   The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer appended with its PLMN ID (subject), NF Instance Id of the requested NF Service Producer appended with its PLMN ID (audience), expected service name(s) (scope) and expiration time (expiration).

   For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

4. The token shall be included in the Nnrf_AccessToken_Get response sent to the NRF in the visited PLMN.

5. The NRF in the visited PLMN shall forward the Nnrf_AccessToken_Get response message to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer listed in claims (scope, audience) during their validity time.

Step 2: Service access request based on token verification

In addition to the steps described in the non-roaming scenario in 13.4.1.1, the NF Service Producer shall verify that the PLMN-ID (or SNPN ID) contained in the API request is equal to the one inside the access token.

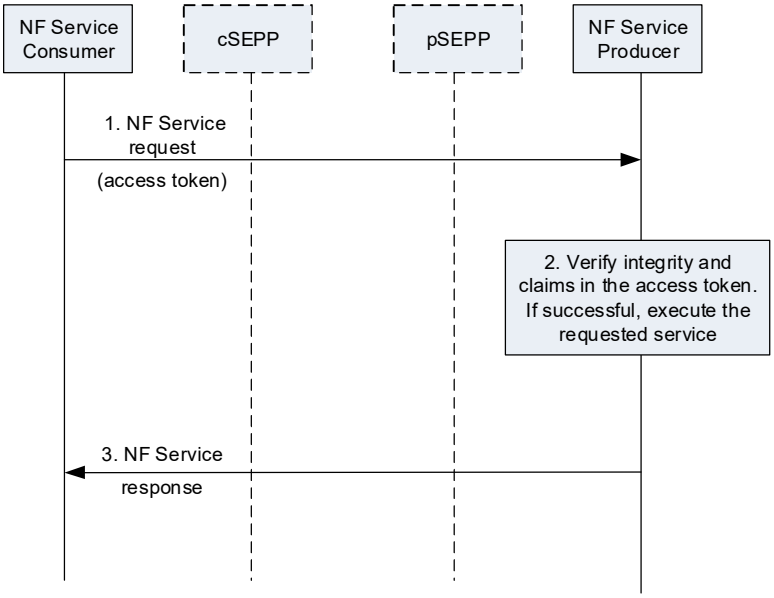


Figure 13.4.1.2.2-2: NF Service Consumer requesting service access with an access token in roaming case

The NF Service Producer shall check that the home PLMN ID of audience claim in the access token matches its own PLMN identity.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Producer verifies the SNPN ID of the serving SNPN contained in the API request instead of the PLMN-ID, and the SNPN ID or the PLMN ID of the Credentials Holder instead of the home PLMN ID.

The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID. If PRINS is used, this can be achieved by the pSEPP checking the PLMN ID of the serving network in the access token against the PLMN ID(s) in the N32-f context.

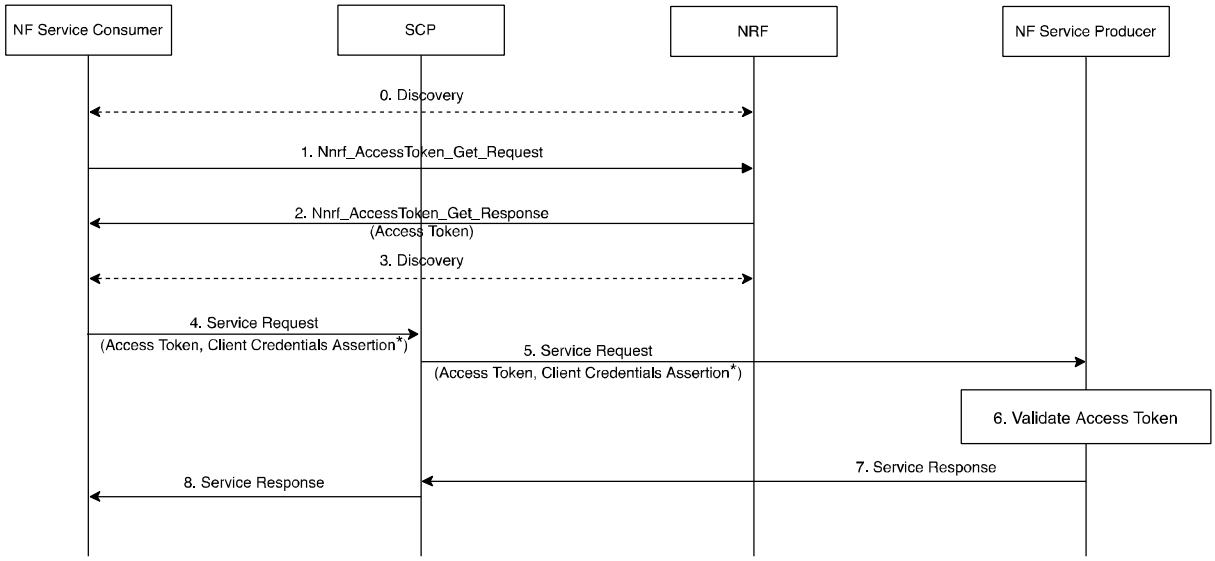
If the peer network is an SNPN, the pSEPP shall check that the SNPN ID of the NF Service Consumer in the access token matches the SNPN ID of the peer network.

13.4.1.3 Service access authorization in indirect communication scenarios

13.4.1.3.1 Authorization for indirect communication without delegated discovery procedure

13.4.1.3.1.1 With mutual authentication between NF Service Consumer and NRF at the transport layer

This clause covers the scenario where the NF Service Consumer and the NRF are connected over a mutually authenticated TLS connection.



* indicates that Client Credentials Assertion is optional in this step.

Figure 13.4.1.3.1.1-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, with mutual authentication between NF and NRF at the transport layer

Discovery of the NF Service Producer:

0. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer. E.g. if the NF Service Consumer has not yet discovered the NF Service Producer, then it may run the discovery procedure.

NF Service Consumer authorization:

1-2.

After mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer and NRF perform the "Access token request before service access" procedure as described in clause 13.4.1.1. If the NF Service Consumer has already discovered the NF Service Producer, it can also perform the "Access token request for a specific NF Service Producer/NF Service Producer instance" procedure as described in clause 13.4.1.1.

Service request:

The NF Service Consumer, SCP, NRF and NF Service Producer perform the procedure "Indirect Communication without delegated discovery Procedure" described in clause 4.17.11 of TS 23.502 [8]. The following steps describe how the access token received from steps 1 and 2 is used in this procedure.

3. If no cached data is available, the NF Service Consumer discovers the NF Service Producer via the SCP.

4. The NF Service Consumer sends a service request for the specific service to the SCP. The service request includes the access token as received in step 2, and may include the NF Service Consumer CCA as defined in clause 13.3.8.

   If the CCA is included, the NF type of the expected audience in the CCA shall contain "NF Service Producer".

   If the NF Service Consumer allows reselection of a target NF Service Producer by the SCP, the expected audience in the CCA shall also contain NF type "NRF".

NOTE: In the same deployment, the NF Service Consumer can delegate the reselection of the target NF Service Producer to the SCP for some requests, and not for other requests.

5. The SCP selects a NF Service Producer instance, performs the API root modifications and forwards the received request to the selected NF Service Producer instance. The request contains the access token and may contain the NF Service Consumer CCA if received in step 4.

6. To authorize the access, the NF Service Producer authenticates the service consumer NF using one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1 by verifying the signature and checking if the requested service is part of the token's scope.

7. If the checks in step 6 are successful, the NF Service Producer processes the service request and provides a service response.

8. The SCP performs reverse API root modifications and forwards the service response.

13.4.1.3.1.2 Without mutual authentication between NF and NRF at the transport layer

When there is no mutual authentication between NF Service Consumer and NRF at the transport layer, the NF Service Consumer performs the following procedure to obtain the access token from NRF and uses it for service access at the NF Service Producer. In this clause, the authentication of NF Service Consumer by the NRF and by the NF Service Producer is based on any of the methods described in clauses 13.3.1.2 and 13.3.2.2.

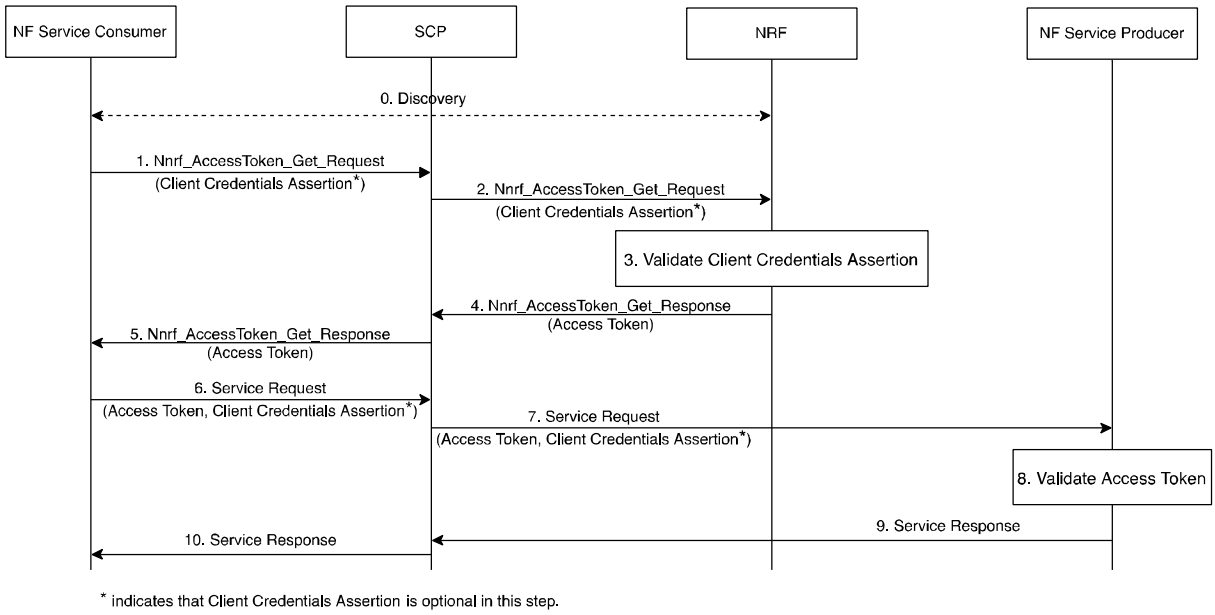


Figure 13.4.1.3.1.2-1: Authorization and service invocation procedure, for indirect communication without delegated discovery, without mutual authentication between NF and NRF at the transport layer

0. Optionally, the NF Service Consumer may discover the NF Service Producer before requesting authorization to invoke the services of the NF Service Producer.

1. The NF Service Consumer sends an access token request (Nnrf_AccessToken_Get Request) to the SCP with parameters as specified in 13.4.1.1. The access token request may additionally include the NF Service Consumer CCA as defined in clause 13.3.8.

   If the CCA is included, the NF type of the expected audience in CCA shall contain "NRF".

2. The SCP forwards the access token request (Nnrf_AccessToken_Get Request) to the NRF. The request may include the NF Service Consumer CCA if received in step 1.

3. The NRF authenticates the service consumer NF using one of the methods described in clause 13.3.1.2. If the NF Service Consumer authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer NF Instance ID as the subject of the access token.

4. The NRF sends the access token to the SCP in an access token response (Nnrf_AccessToken_Get Response).

5. The SCP forwards the access token response (Nnrf_AccessToken_Get Response) to the NF Service Consumer, including the access token.

6. The NF Service Consumer sends the service request to the SCP. The service request includes the access token received in Step 5 and may include the NF Service Consumer CCA.

   If the CCA is included, the NF type of the expected audience in CCA shall contain "NF Service Producer".

   If the NF Service Consumer allows reselection of a target NF Service Producer by the SCP, the expected audience in the CCA shall also contain NF type "NRF".

NOTE: In the same deployment, the NF Service Consumer can delegate the reselection of the target NF Service Producer to the SCP for some requests, and not for other requests.

7. The SCP forwards the service request to the NF Service Producer. The service request includes the access token received in step 6, and may include the NF Service Consumer CCA if received in step 6.

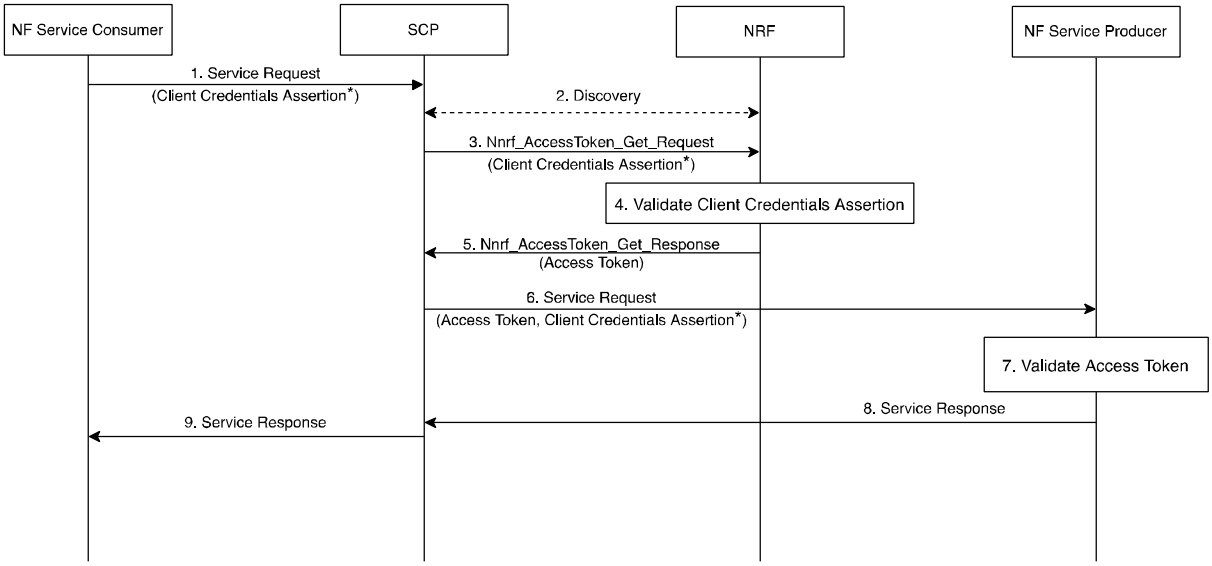
8. The NF Service Producer authenticates the NF Service Consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

9. If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

10. The SCP forwards the service response to the NF Service Consumer.

13.4.1.3.2 Authorization for indirect communication with delegated discovery procedure

This clause covers the scenario where the NF Service Consumer use the SCP to discover and select the NF Service Producer instance that can process the service request.



* indicates that Client Credentials Assertion is optional in this step.

Figure 13.4.1.3.2-1: Authorization and service invocation procedure, for indirect communication with delegated discovery

1. The NF Service Consumer sends a service request to the SCP. The service request may include the NF Service Consumer's CCA as defined in clause 13.3.8.The NF Service Consumer may include an access token in the service request if it has received an access token in a previous service response. If a previously received access token has expired, the NF Service Consumer may include discovery parameters as specified in TS 29.500 [74] clause 5.2.3.2.7 in the service request.

If the CCA is included, the NF type of the expected audience in CCA shall contain "NRF" and "NF Service Producer".

2. The SCP may perform a service discovery with the NRF. If NF Service Consumer has included an access token in step 1, or if the SCP has a cached granted access token, then SCP may reuse the access token and proceeds to step 6.

3. The SCP sends an access token request (Nnrf_AccessToken_Get Request) to the NRF. The access token request includes parameters as defined in clause 13.4.1.1. The access token request may include the NF Service Consumer's CCA if received in Step 1.

4. The NRF authenticates the NF Service Consumer using one of the methods described in clause 13.3.1.2. If NF Service Consumer authentication is successful and the NF Service Consumer is authorized based on the NRF policy, the NRF issues an access token as described in clause 13.4.1.1. The NRF uses the NF Service Consumer instance ID as the subject of the access token.

5. The NRF sends the access token to the SCP in an access token response (Nnrf_AccessToken_Get Response).

6. The SCP sends the service request to the NF Service Producer. The service request includes an access token (i.e., received in Step 1, received in Step 5, or previously cached), and may include the NF Service Consumer's CCA if received in Step 1.

7. The NF Service Producer authenticates the NF Service Consumer by one of the methods described in clause 13.3.2.2 and if successful, it validates the access token as described in clause 13.4.1.1.

8. If the validation of the access token is successful, the NF Service Producer sends the service response to the SCP.

9. The SCP forwards the service response to the NF Service Consumer. The SCP may include the access token in the service response to NF Service Consumer for possible re-use in subsequent service requests.

13.5 Security capability negotiation between SEPPs

The security capability negotiation over N32-c allows the SEPPs to negotiate which security mechanism to use for protecting NF service-related signalling over N32-f. There shall be an agreed security mechanism between a pair of SEPPs before conveying NF service-related signalling over N32-f.

When a SEPP notices that it does not have an agreed security mechanism for N32-f protection with a peer SEPP or if the security capabilities of the SEPP have been updated, the SEPP shall perform security capability negotiation with the peer SEPP over N32-c in order to determine, which security mechanism to use for protecting NF service-related signalling over N32-f. Certificate based authentication shall follow the profiles given in 3GPP TS 33.210 [3], clause 6.2.

A mutually authenticated TLS connection as defined in clause 13.1 shall be used for protecting security capability negotiation over N32-c. The TLS connection shall provide integrity, confidentiality and replay protection.

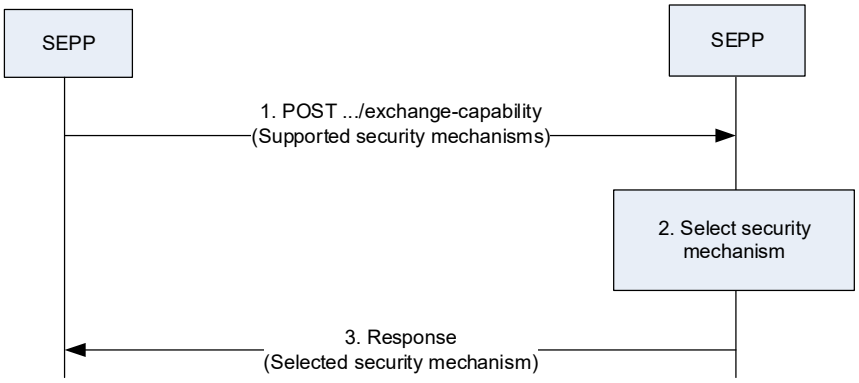


Figure 13.5-1 Security capability negotiation

1. The SEPP which initiated the TLS connection shall issue a POST request to the exchange-capability resource of the responding SEPP including the initiating SEPP's supported security mechanisms for protecting the NF service-related signalling over N32-f (see table Table 13.5-1). The security mechanisms shall be ordered in the initiating SEPP's priority order.

2. The responding SEPP shall compare the received security capabilities to its own supported security capabilities and selects, based on its local policy (e.g. based on whether there are IPX providers on the path between the SEPPs), a security mechanism, which is supported by both initiating SEPP and responding SEPP.

3. The responding SEPP shall respond to the initiating SEPP with the selected security mechanism for protecting the NF service-related signalling over N32.

Table 13.5-1: NF service-related signalling traffic protection mechanisms over N32

N32-f protection mechanism	Description
Mechanism 1	PRINS (described in clause 13.2)
Mechanism 2	TLS
Mechanism n	Reserved

If the selected security mechanism is PRINS, the SEPPs shall behave as specified in clause 13.2.

If the selected security mechanism is TLS, the SEPPs shall behave as specified in clause 13.1.2, tear down the N32-c connection and forward the NF service related signalling over N32-f using a TLS connection.

If the selected security mechanism is a mechanism other than the ones specified in Table 13.5-1, the two SEPPs shall terminate the N32-c TLS connection.

14 Security related services

14.1 Services provided by AUSF

14.1.1 General

The AUSF provides UE authentication service to the requester NF by Nausf_UEAuthentication. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. Clause 14.1.2

describes the Nausf_UEAuthentication service. The service operations listed here are used in procedures that are described in clause 6 of the present document and in TS 33.503 [109].

Clause 14.1.3 describes the Nausf_SoRProtection service used in procedures that are described in clause 6.14 of the present document.

Clause 14.1.4 describes the Nausf_UPUProtection service used in procedures that are described in clause 6.15 of the present document.

Since AUSF is completely security-related, all service operations are described in the present document. TS 23.501 [2], clause 7.2.7, only lists the services and TS 23.502 [8], clause 5.2.10, provides the reference to the present document.

14.1.2 Nausf_UEAuthentication service

14.1.2.1 Nausf_UEAuthentication_Authenticate service operation

Service operation name: Nausf_UEAuthentication_authenticate.

Description: Authenticate the UE and provides related keying material.

Input, Required: One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.
2. In the subsequent authentication requests depending on the authentication method:
   a. 5G AKA: Authentication confirmation message with RES* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS).
   b. EAP-AKA': EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

Input, Optional: Disaster Roaming service indication, NSWO indicator.

NOTE: If NSWO indicator is present then the serving network name contains "5G:NSWO".

Output, Required: One of the options below.

1. Depending on the authentication method:
   a. 5G AKA: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.
   b. EAP-AKA': EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.
2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

Output, Optional: SUPI if the authentication was initiated with SUCI, MSK if NSWO indicator was received as input.

14.1.2.2 Nausf_UEAuthentication_deregister service operation

Service operation name: Nausf_UEAuthentication_deregister

Description: Deletion of stale security parameters (K_{AUSF}, SOR counter and UE parameter update counter) in AUSF. UDM uses this service operation to request the AUSF to clear the stale security parameters, after the UE has been successfully (re)authenticated in different AUSF Instance.

Input, Required: SUPI

Input, Optional: None

Output, Required: None

Output, Optional: None

14.1.2.3 Nausf_UEAuthentication_ProseAuthenticate service operation

See TS 33.503 [109].

14.1.3 Nausf_SoRProtection service

The following table illustrates the security related services for SoR that AUSF provides.

Table 14.1.3-1: NF services for SoR provided by AUSF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nausf_SoRProtection	Protect	Request/Response	UDM

Service operation name: Nausf_SoRProtection.

Description: The AUSF calculates the SoR-MAC-I_{AUSF} as specified in the Annex A.17 of this document using UE specific home key (K_{AUSF}), the Steering Information List and ACK Indication received from the requester NF and delivers the SoR-MAC-I_{AUSF} and $Counter_{SoR}$ to the requester NF. If the ACK Indication input is set to indicate that the acknowledgement is requested, then the AUSF shall compute the SoR-XMAC-I_{UE} as specified in Annex A.18 of the present document, and return it in the response.

NOTE: At reception of Nausf_SoRProtection_Protect request from the UDM, the AUSF constructs the SOR header, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the requester NF, i.e. ACK Indication and list of preferred PLMN/access technology combinations or a secured packet (if provided).

Input, Required: Requester ID, SUPI, service name, ACK Indication.

Input, Optional: list of preferred PLMN/access technology combinations or secured packet or SoR transparent container.

Output, Required: SoR-MAC-I_{AUSF}, $Counter_{SoR}$ or error (counter_wrap).

Output, Optional: SoR-XMAC-I_{UE} (if the ACK Indication input is set to indicate that the acknowledgement is requested, then the SoR-XMAC-I_{UE} shall be computed and returned).

14.1.4 Nausf_UPUProtection service

The following table illustrates the security related services for UE Parameters Update that AUSF provides.

Table 14.1.4-1: NF services for UE Parameters Update provided by AUSF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nausf_UPUProtection	Protect	Request/Response	UDM

Service operation name: Nausf_UPUProtection.

Description: The AUSF calculates the UPU-MAC-I_{AUSF} as specified in the Annex A.19 of this document using UE specific home key (K_{AUSF}) along with the UE Parameters Update Data received from the requester NF (see clause A.19) and delivers the UPU-MAC-I_{AUSF} and $Counter_{UPU}$ to the requester NF. If the ACK Indication input is present, then the AUSF shall compute the UPU-XMAC-I_{UE} and return the computed UPU-XMAC-I_{UE} as specified in Annex A.20 of the present document, in the response. The details of the UE Parameters Update Data is specified in TS 24.501 [35].

Input, Required: Requester ID, SUPI, service name, UE Parameters Update Data.

Input, Optional: ACK Indication.

Output, Required: UPU-MAC-I_{AUSF}, $Counter_{UPU}$ or error (counter_wrap).

Output, Optional: UPU-XMAC-I_{UE} (if the ACK Indication input is present, then the UPU-XMAC-I_{UE} shall be computed and returned).

14.1.5 Void

14.2 Services provided by UDM

14.2.1 General

UDM provides within Nudm_UEAuthentication service all authentication-related service operations, which are Nudm_UEAuthentication_Get (clause 14.2.2) , Nudm_UEAuthentication_ResultConfirmation (clause 14.2.3), Nudm_UEAuthentication_GetProseAv (clause 14.2.4) and Nudm_UEAuthentication_GetGbaAv (clause 14.2.5).

The complete list of UDM services is defined in TS 23.501 [2], clause 7.2.5, and further refined in TS 23.502 [8], clause 5.2.3.1.

14.2.2 Nudm_UEAuthentication_Get service operation

Service operation name: Nudm_UEAuthentication_Get

Description: Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

Inputs, Required: SUPI or SUCI, serving network name.

Inputs, Optional: Synchronization Failure indication and related information (i.e. RAND/AUTS) , Disaster Roaming service indication, NSWO indicator.

NOTE: If NSWO indicator is present then the serving network name contains "5G:NSWO".

Outputs, Required: Authentication method

Outputs, Optional**:** SUPI if SUCI was used as input. Depending on the authentication method, authentication data (e.g. AKA authentication vector) for the SUPI. AKMA Indication and Routing indicator, if the subscriber has an AKMA subscription (see TS 33.535 [91]).

14.2.3 Nudm_UEAuthentication_ResultConfirmation service operation

Service operation name: UEAuthentication_ResultConfirmation

Description: Requester NF informs UDM about the result of an authentication procedure with a UE.

Inputs, Required: SUPI, timestamp of the authentication, the authentication type (e.g. EAP method or 5G-AKA), and the serving network name.

Inputs, Optional: None.

Outputs, Required: None.

Outputs, Optional: None.

14.2.4 Nudm_UEAuthentication_GetProseAv service operation

See TS 33.503 [109].

14.2.5 Nudm_UEAuthentication_GetGbaAv service operation

See TS 33.220 [28], Annex N.

14.3 Services provided by NRF

14.3.1 General

The following table illustrates the security related services for OAuth 2.0 that NRF provides. OAuth 2.0 based authorization is described in clause 13.4.1.

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnrf_AccessToken	Get	Request/Response	AMF, SMF, PCF, NEF, NSSF, SMSF, AUSF

The complete list of NRF services is defined in TS 23.501 [2], clause 7.2.6, and further refined in TS 23.502 [8], clause 5.2.7.

14.3.2 Nnrf_AccessToken_Get Service Operation

Service Operation name: Nnrf_AccessToken_Get.

Description: NF Service Consumer requests NRF to provide an Access Token.

Inputs, Required: the NF Instance Id of the NF Service Consumer, the requested "scope" including the expected NF service name(s).

Inputs, Optional: PLMN ID (or SNPN ID) of the requester NF Service Consumer, PLMN ID (or SNPN ID) of the requested NF Service Producer, NF Instance Id(s) of the requested NF Service Producer, NF type of the expected NF Service Producer instance and NF Service Consumer, "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances, NF Set ID of the expected NF Service Producer instances, list of S-NSSAIs of the NF Service Consumer.

Outputs, Required: Access Token with appropriate claims, where the claims shall include NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer potentially appended with its PLMN ID (or SNPN ID) (subject), NF type of the NF Service Producers or NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer, potentially appended with PLMN ID (or SNPN ID) (audience), expected service name (scope), optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources) and expiration time (expiration), may include list of NSSAIs or NSI IDs for the expected NF Service Producer instances, and may include the NF Set ID of the expected NF Service Producer instances.

Outputs, Optional: None.

14.4 Services provided by NSSAAF

14.4.1 Nnssaaf_NSSAA services

14.4.1.1 General

The following table illustrates the security related services for Network Slice Specific Authentication and Authorisation that NSSAAF provides.

Table 14.4.1.1-1: NF services for the NSSAA service provided by NSSAAF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnssaaf_NSSAA	Authenticate	Request/Response	AMF
	Re-AuthenticationNotification	Notify	AMF
	RevocationNotification	Notify	AMF

14.4.1.2 Nnssaaf_NSSAA_Authenticate service operation

Service operation name: Nnssaaf_NSSAA_Authenticate

Description: NF consumer requires the NSSAAF to relay Network Slice specific authentication messages towards the corresponding AAA-S handling the Network Slice specific authentication for the requested S-NSSAI (see clause 16).

Input, Required:

1) In the initial NSSAA requests: EAP ID Response, GPSI, S-NSSAI

2) In subsequent NSSAA requests: EAP message, GPSI, S-NSSAI

Input, Optional: None

Output, Required: EAP message, GPSI, S-NSSAI

Output, Optional: None

14.4.1.3 Nnssaaf_NSSAA_Re-AuthenticationNotification service operation

Service operation name: Nnssaaf_NSSAA_Re-AuthenticationNotification

Description: NSSAAF notifies the NF consumer to trigger a Network Slice specific reauthentication procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nnssaaf_NSSAA_Re-authenticationNotification service operation.

Input, Required: GPSI, S-NSSAI

Input, Optional: None

Output, Required: None

Output, Optional: None

14.4.1.4 Nnssaaf_NSSAA_RevocationNotification service operation

Service operation name: Nnssaaf_NSSAA_RevocationNotification

Description: NSSAAF notifies the NF consumer to trigger a Network Slice specific revocation procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nnssaaf_NSSAA_RevocationNotification service operation.

Input, Required: GPSI, S-NSSAI

Input, Optional: None

Output, Required: None

Output, Optional: None

14.4.2 Nnssaaf_AIW services

14.4.2.1 General

The following table illustrates the security related services provided by the NSSAAF for primary authentication in SNPN with Credentials holder using AAA server (see clause I.2.2.2).

Table 14.4.2.1-1: NF services for CH using AAA for primary authentication provided by NSSAAF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnssaaf_AIW	Authenticate	Request/Response	AUSF

14.4.2.2 Nnssaaf_AIW_Authenticate service operation

Service operation name: Nnssaaf_AIW_Authenticate

Description: The NSSAAF provides Authentication and Authorization service to the consumer NF by relaying EAP or EAP-TTLS inner method messages towards a AAA Server and performing related protocol conversion as needed.
Input, Required:

1) In EAP Authentication:

   a) In the initial authentication request: SUPI.

   b) In subsequent authentication requests: EAP message.

2) In case EAP-TTLS mechanisms are implemented: inner method container.

Input, Optional: None

Output, Required:

1) In EAP authentication: EAP message, authentication result and if success MSK and SUPI.

2) In case EAP-TTLS mechanisms are implemented: inner method container.

Output, Optional: None

15 Management security for network slices

15.1 General

The creation, modification, and termination of a Network Slice Instance (NSI) is part of the Management Services provided by the 5G management systems. A management service is accessed by management service consumers via standardized service interfaces given in 3GPP TS 28.533 [54]. The typical service consumers for the above NSI provisioning and NSI provisioning exposure are operators and vertical industry respecitively, as described in 3GPP TS 28.531 [55]. These management services are securely protected through mutual authentication and authorization below.

15.2 Mutual authentication

If a management service consumer resides outside the 3GPP operator's trust domain, mutual authentication shall be performed between the management service consumer and the management service producer using TLS. TLS shall follow, the profile given in TS 33.210 [3], clause 6.2 and either 1) the client and server certificates with the profiles given in 3GPP TS 33.310 [5], clause 6.1.3a or 2) pre-shared keys following RFC 5489for TLS 1.2 and RFC 8446 [60] for TLS 1.3. The structure of the PKI used for the certificates is out of scope of the present document. The identities in the end entity certificates shall be used for authentication and policy checks. The key distribution of pre-shared keys for TLS is up to the operator's security policy and out of scope of the present document.

15.3 Protection of management interactions between the management service consumer and the management service producer

TLS shall be used to provide mutual authentication, integrity protection, replay protection and confidentiality protection for the interface between the management service producer and the management service consumer residing outside the 3GPP operator's trust domain. Security profiles for TLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

15.4 Authorization of management service consumer's request

After the mutual authentication, the management service producer determines whether the management service consumer is authorized to send requests to the management service producer. The management service producer shall authorize the requests from the management service consumer using the one of the following two options: 1) OAuth-based authorization mechanism following RFC 6749 [43]; 2) based on the local policy of the management service producer.

16 Security procedures for network slices

16.1 General

This clause specifies the security procedures for network slices.

16.2 Authorization for network slice access

This clause specifies the relationship between primary authentication (as described in Clause 6.1) and authorization for network slice access (as described in TS 23.502 [8]) for a UE. Authorization from a home/serving PLMN is required for a UE to gain access to a network slice, identified by an S-NSSAI. An authorized S-NSSAI (i.e. allowed S-NSSAI) shall be granted to a UE only after the UE has completed successfully primary authentication. At the end of the primary authentication, the AMF and UE may receive a list of allowed S-NSSAI, which the UE is authorized to access.

For certain S-NSSAIs, additional Network Slice Specific Authentication and Authorization (NSSAA) is required. This clause in addition specifies the pre-requisite for an NSSAA procedure that is described in clause 16.3, with reference to the following figure 16.2-1.

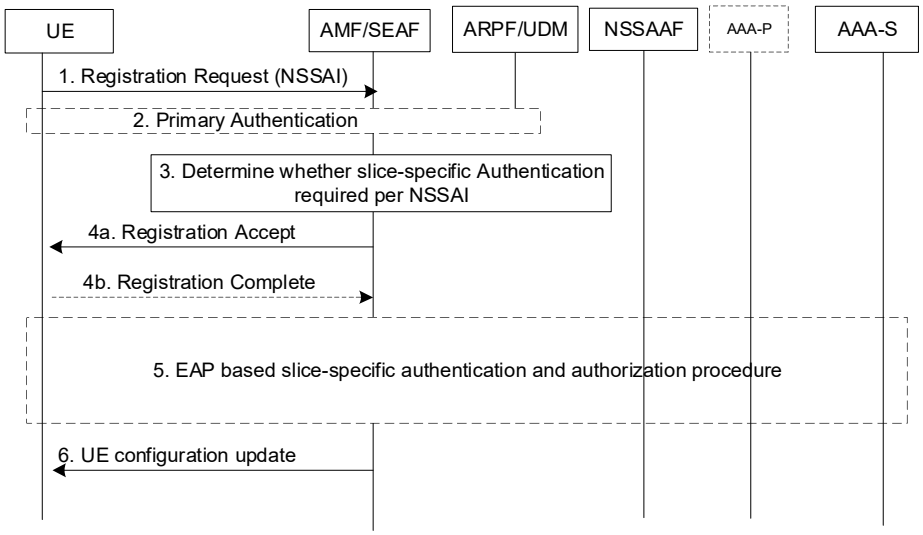


Figure 16.2-1: Relationship between primary authentication and NSSAA

1. UE sends a Registration Request with a list of S-NSSAIs. UE shall not include those S-NSSAIs for which NSSAA procedures are ongoing, regardless of access types (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2).

2. For an initial Registration Request, the AMF/SEAF shall invoke Primary authentication as described in clause 6.1.2 of the present document. For a subsequent Registration Request, the Primary authentication may be skipped if the UE has already been authenticated and the AMF has valid security context.

3. AMF shall determine whether NSSAA is required for each of S-NSSAIs, based on information stored locally or from UDM. For example, the NSSAA for an S-NSSAI may be omitted

   1) if it is not required based on the subscription information,

   2) if UE has previously performed NSSAA successfully, regardless of access type and the result is still valid, or

   3) NSSAA for UE is ongoing

4. AMF sends the Registration Accept message to the UE (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2, step 21). Optionally UE sends a Registration Complete.

5. The EAP based NSSAA procedure for each S-NSSAI if required, as determined in step 3, is executed in this step.

6. Based on the results of step 5, AMF sends UE Configuration Update to update the requested S-NSSAI status based on the NSSAA results.

The procedure for step 5, i.e., the NSSAA procedure is specified in clause 16.3.

16.3 Network slice specific authentication and authorization

This clause specifies the optional-to-use NSSAA between a UE and an AAA server (AAA-S) which may be owned by an external 3rd party enterprise. NSSAA uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication.

The EAP framework specified in RFC 3748 [27] shall be used for NSSAA between the UE and the AAA server. The SEAF/AMF shall perform the role of the EAP Authenticator and communicates with the AAA-S via the NSSAAF. The NSSAAF undertakes any AAA protocol interworking with the AAA-S. Multiple EAP methods are possible for NSSAA. If the AAA-S belongs to a third party the NSSAAF contacts the AAA-S via a AAA-P. The NSSAAF and the AAA-P may be co-located.

To protect privacy of the EAP ID used for the EAP based NSSAA, a privacy-protection capable EAP method is recommended, if privacy protection is required.

The steps involved in NSSAA are described below.

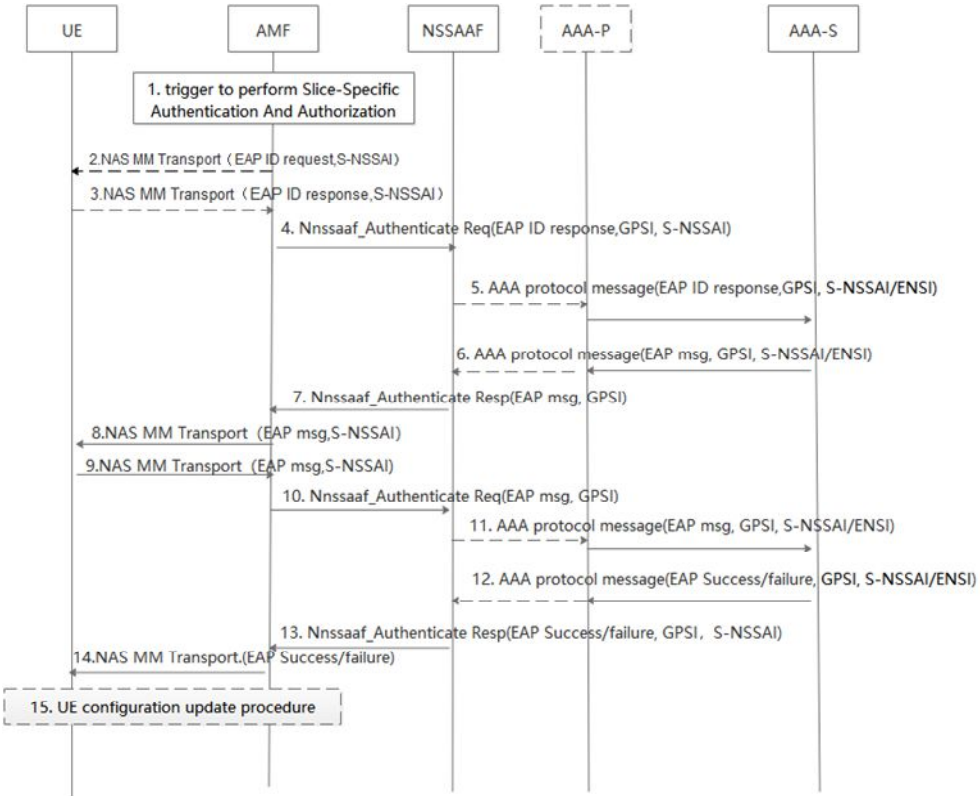


Figure 16.3-1: NSSAA procedure

1. For S-NSSAIs that are requiring NSSAA, based on change of subscription information, or triggered by the AAA-S, the AMF may trigger the start of the NSSAA procedure.

   If NSSAA is triggered as a result of Registration procedure, the AMF may determine, based on UE Context in the AMF, that for some or all S-NSSAI(s) subject to NSSAA, the UE has already been authenticated following a Registration procedure on a first access. Depending on NSSAA result (e.g. success/failure) from the previous Registration, the AMF may decide, based on Network policies, to skip NSSAA for these S-NSSAIs during the Registration on a second access.

   If the NSSAA procedure corresponds to a re-authentication and re-authorization procedure triggered as a result of AAA Server-triggered UE re-authentication and re-authorization for one or more S-NSSAIs, as described in clause 16.4, or triggered by the AMF based on operator policy or a subscription change and if S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization are included in the Allowed NSSAI for each Access Type, the AMF selects an Access Type to be used to perform the NSSAA procedure based on network policies.

2. The AMF may request the UE User ID for EAP authentication (EAP ID) for the S-NSSAI in a NAS MM Transport message including the S-NSSAI.

3. The UE provides the EAP ID for the S-NSSAI alongside the S-NSSAI in an NAS MM Transport message towards the AMF.

4. The AMF sends the EAP ID to the NSSAAF which provides interface with the AAA, in an Nnssaaf_NSSAA_Authenticate Request (EAP ID Response, GPSI, S-NSSAI).

5. If the AAA-P is present (e.g. because the AAA-S belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF forwards the EAP ID Response message to the AAA-P, otherwise the

NSSAAF forwards the message directly to the AAA-S. NSSAAF routes to the AAA-S based on the S-NSSAI. The NSSAAF/AAA-P forwards the EAP Identity message to the AAA-S together with S-NSSAI and GPSI. The AAA-S stores the GPSI to create an association with the EAP ID in the EAP ID response message so the AAA-S can later use it to revoke authorisation or to trigger reauthentication. The AAA-S uses the EAP-ID and S-NSSAI to identify for which UE and slice authorisation is requested.

NOTE : If the AAA-S belongs to the 3rd party, the NSSAAF optionally maps the S-NSSAI to External Network Slice Information (ENSI), and forwards the EAP Identity message to the AAA-S together with ENSI and GPSI. In this case, the AAA-S uses the EAP-ID and ENSI to identify the UE for which slice authorisation is requested.

6 -11. EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

12. EAP authentication completes. An EAP-Success/Failure message is delivered to the NSSAAF/AAA-P along with GPSI and S-NSSAI/ENSI.

13. The NSSAAF sends the Nnssaaf_NSSAA_Authenticate Response (EAP-Success/Failure, S-NSSAI, GPSI) to the AMF.

14. The AMF transmits a NAS MM Transport message (EAP-Success/Failure) to the UE.

15. Based on the result of Slice specific authentication (EAP-Success/Failure), if a new Allowed NSSAI or new Rejected NSSAIs needs to be delivered to the UE, or if the AMF re-allocation is required, the AMF initiates the UE Configuration Update procedure, for each Access Type, as described in clause 4.2.4.2 of TS 23.502 [8].

If the NSSAA procedure can not be completed (e.g. due to server error or UE becoming unreachable), the AMF sets the status of the corresponding S-NSSAI subject to Network Slice-Specific Authentication and Authorization in the UE context as defined in TS 29.526 [96], so that an NSSAA is executed next time the UE requests to register with the S-NSSAI.

16.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure

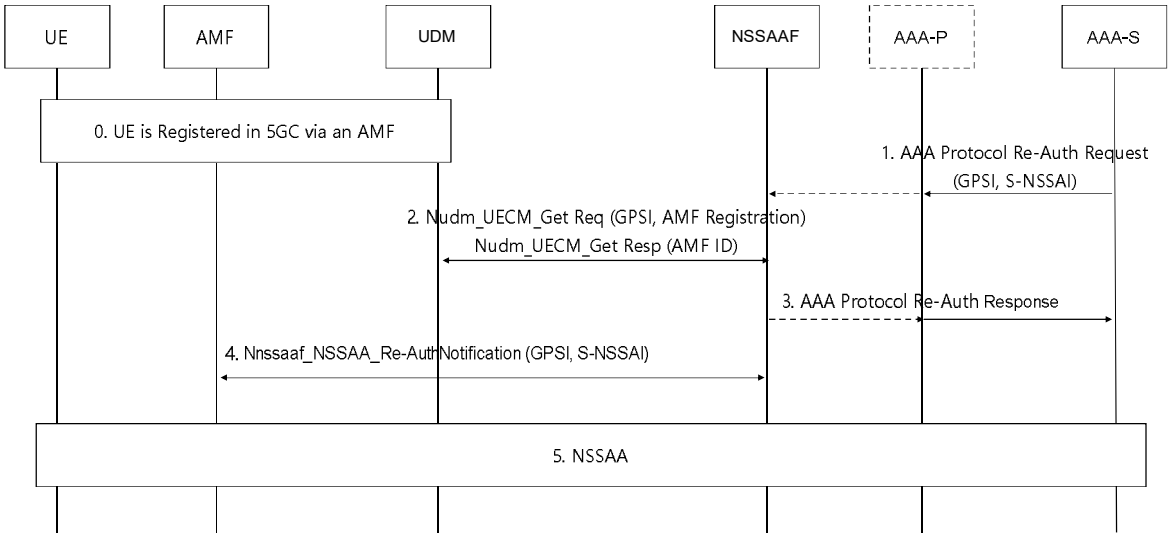


Figure 16.4-1: AAA Server initiated Network Slice-Specific Re-authentication and Re-authorization procedure

0. The UE is registered in 5GC via an AMF. The AMF ID is stored in the UDM.

1. The AAA-S requests the re-authentication and re-authorization for the Network Slice specified by the S-NSSAI/ENSI in the Re-Auth Request message, for the UE identified by the GPSI in this message. This message

is sent to an AAA-P, if the AAA-P is used (e.g. the AAA Server belongs to a third party), otherwise it may be sent directly to the NSSAAF. If an AAA-P is present, the AAA-P relays the Reauthentication Request to the NSSAAF.

2. The NSSAAF checks whether the AAA-S is authorized to request the re-authentication and re-authorization by checking the local configuration of AAA-S address per S-NSSAI. If success,the NSSAAF requests UDM for the AMF serving the UE using the Nudm_UECM_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE.

3. The NSSAAF provides an acknowledgement to the AAA protocol Re-Auth Request message. If the AMF is not registered in UDM the procedure is stopped here.

4. If the AMF is registered in UDM, the NSSAAF requests the relevant AMF to re-authenticate/re-authorize the S-NSSAI for the UE using the Nnssaaf_NSSAA_Re-authenticationNotification service operation. The AMF is implicitly subscribed to receive Nnssaaf_NSSAA_Re-authenticationNotification service operations. The NSSAAF may discover the Callback URI for the Nnssaaf_NSSAA_Re-authenticationNotification service operation exposed by the AMF via the NRF.

   The AMF acknowledges the notification of Re-authentication request.

5. If the UE is registered with the S-NSSAI in the Mapping Of Allowed NSSAI, the AMF triggers the NSSAA procedure defined in clause 16.3 for the UE identified by the GPSI and the Network Slice identified by the S-NSSAI received from the NSSAAF.

   If the UE is registered but the S-NSSAI is not in the Mapping Of Allowed NSSAI, the AMF removes any status of the corresponding S-NSSAI subject to Network Slice-Specific Authentication and Authorization in the UE context it may have kept, so that an NSSAA is executed next time the UE requests to register with the S-NSSAI.

16.5 AAA Server triggered Slice-Specific Authorization Revocation

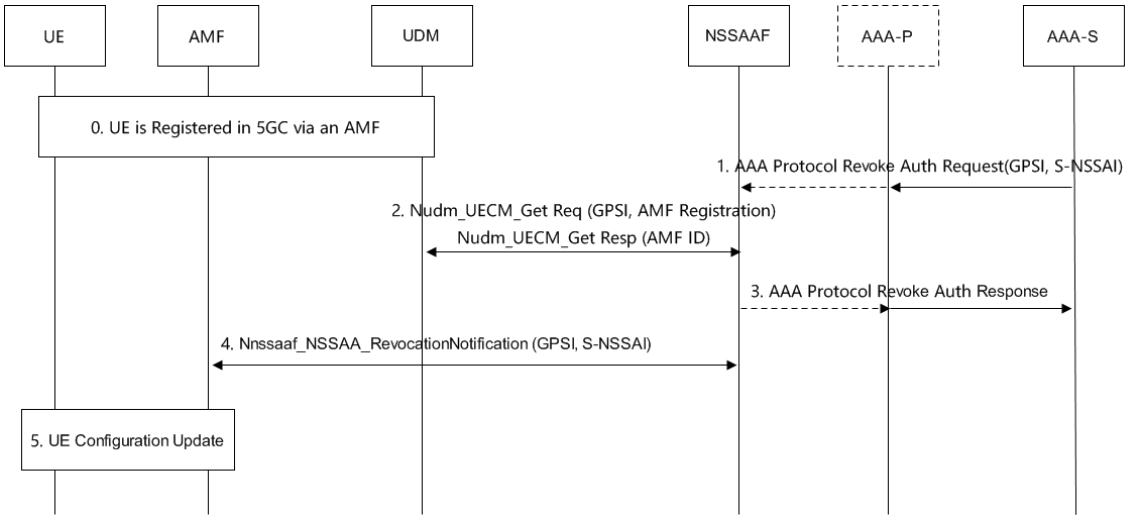


Figure 16.5-1: AAA Server-initiated Network Slice-Specific Authorization Revocation procedure

0. The UE is registered in 5GC via an AMF. The AMF ID is stored in the UDM.

1. The slice specific AAA-S requests the revocation of authorization for the Network Slice identified by the GPSI in the AAA Protocol Revoke Authorization Request message. This message is sent to NSSAAF instance interfacing with AAA-S or AAA-P if it is used.

   The AAA-P, if present, relays the request to the NSSAAF.

2. The NSSAAF checks whether the AAA-S is authorized to request the revocation by checking the local configuration of AAA-S address per S-NSSAI. If success,the NSSAAF requests UDM for the AMF serving the UE using the Nudm_UECM_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE.

3. The NSSAAF sends an acknowledgement to the the AAA-S/AAA-P with AAA Protocol Revoke Authorization Response message. If the AMF is not registered in UDM the procedure is stopped here.

4. If the AMF is registered in UDM, the NSSAAF request the relevant AMF to revoke the S-NSSAI authorization for the UE using the Nnssaaf_NSSAA_RevocationNotification service operation.

   The AMF is implicitly subscribed to receive Nnssaaf_NSSAA_RevocationNotification service operations. The NSSAAF may discover the Callback URI for the Nnssaaf_NSSAA_RevocationNotification service operation exposed by the AMF via the NRF. The AMF acknowledges the Notification of Revocation request.

5. The AMF removes any status it may have kept of the corresponding S-NSSAI subject to Network Slice-Specific Authentication and Authorisation in the UE context and sends the UE Configuration Update message to revoke the S-NSSAI from the current Allowed NSSAI, for any Access Type for which NSSAA had been successfully run on this S-NSSAI. The AMF provides a new Allowed NSSAI to the UE by removing the S-NSSAI for which authorization has been revoked. The AMF provides new rejected NSSAIs to the UE including the S-NSSAI for which authorization has been revoked. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and a Default NSSAI exists that requires no NSSAA or for which a NSSAA did not previously fail over this access, then the AMF may provide a new Allowed NSSAI to the UE containing the Default NSSAI. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

16.6 AF Authorization for network slice quota-usage information notification/retrieval

16.6.1 Introduction

This clause specifies the AF Authorization procedures when AF subscribes/unsubscribes to network slice quota-usage information and when AF retrieves network slice quota-usage information.

16.6.2 General

If an AF is deployed within the 3GPP operator domain, an S-NSSAI is allowed to be sent to the AF. The baseline procedure for notifying the AF slice usage information (e.g. number of UEs and PDU Sessions in the slice indicated by the S-NSSAI) and the procedure for retrieving slice usage information by the AF are defined in TS 23.502 [8].

If an AF is deployed outside the 3GPP operator domain, an S-NSSAI is not allowed to be sent to the AF as required in clasue 5.9.2.3. The procedure for notifying the AF slice usage information (e.g. number of UEs and PDU Sessions in the slice indicated by the S-NSSAI) and the procedure for retrieving slice usage information by the AF are described in clause 16.6.3.

16.6.3 Subscription/unsubscription procedure of NSACF notification service

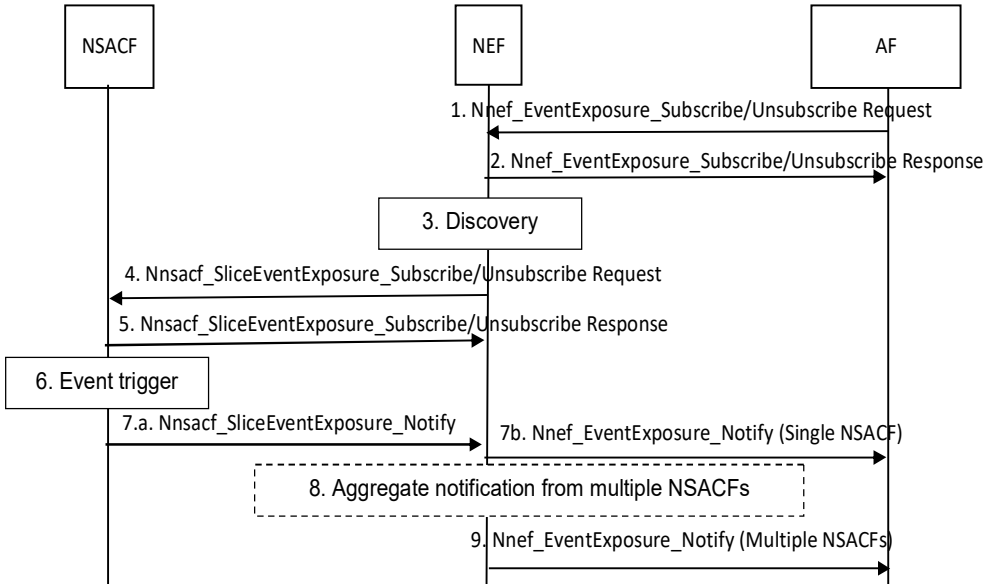


Figure 16.6.3-1: Subscription/unsubscription of NSACF notification procedure

0. Authentication of the AF: the AF is authenticated based on the description in clause 13 or clause 12. The AF authorization is based on clause 13 or clause 12 or local configuration at the NEF. If a token based authorization mechanism is used, a token is generated for theAF after authentication and authorization.

1. To subscribe or unsubscribe for the number of UEs or the number of PDU Sessions per network slice notification with the NSACF, the AF sends Nnef_EventExposure_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information) message to the NEF as described in TS 23.502 [8]. The Event Filter parameter shall be AF-Service-Identifier for an AF deployed outside the 3GPP operator domain. Other parameters are specified in TS 23.502 [8].

2. The NEF confirms with Nnef_ SliceStatusEventExposure _Subscribe/Unsubscribe Response message to the AF.

The Event Filter parameter is the mapped AF-Service-Identifier for the AF deployed outside the 3GPP operator domain.

3. The NEF checks whether the AF is authorised for the requested subscription based on the AF token. It needs to check whether the token claims match the AF's identity and the Event Filter parameter. If authorised, the NEF may query the NRF to find the NSACF responsible for the requested S-NSSAI (NEF needs to map to S-NSSAI based on AF-Service-Identifier for the AF deployed outside the 3GPP operator domain).

4. The NEF forwards the request to the NSACF with Nnsacf_SliceEventExposure_Subscribe/Unsubscribe Request (Event ID, Event Filter, Event Reporting information). The Event Filter parameter shall be the mapped S-NSSAI for the AF deployed outside the 3GPP operator domain.

5. The NSACF confirms with Nnsacf_SliceEventExposure_Subscribe/Usubscribe Response message to the NEF as in TS 23.502 [8].

6-7a. The NSACF triggers a notification towards the AF and sends the Nnsacf_SliceEvent Exposure_Notify (Event ID, Event Filter, Event Reporting information) message to the NEF as described in TS 23.502 [8].

7b-9. The NEF forwards the message to the AF for single NSACF or aggregates reporting information for multiple NSACFs in the Nnef_EventExposure_Notify (Event ID, Event Filter, Event Reporting information) message as described in TS 23.502 [8]. The Event Filter parameter shall be the mapped AF-Service-Identifier from the S-NSSAI for the AF deployed outside the 3GPP operator domain.

Annex A (normative): Key derivation functions

A.1 KDF interface and input parameter construction

A.1.1 General

All key derivations (including input parameter encoding) for 5GC shall be performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220 [28].

This clause specifies how to construct the input string, S, and the input key, KEY, for each distinct use of the KDF. Note that "KEY" is denoted "Key" in TS 33.220 [28].

A.1.2 FC value allocations

The FC number space used is controlled by TS 33.220 [28], FC values allocated for the present document are in range of 0x69 – 0x79, 0x7B – 0x7D and 0x83-0x84.

A.2 K_{AUSF} derivation function

This clause applies to 5G AKA only.

When deriving a K_{AUSF} from CK, IK and the serving network name when producing authentication vectors, and when the UE computes K_{AUSF} during 5G AKA, the following parameters shall be used to form the input S to the KDF:

- FC = 0x6A;
- P0 = serving network name;
- L0 = length of the serving network name (variable length as specified in 24.501 [35]);
- P1 = SQN ⊕ AK,
- L1 = length of SQN ⊕ AK (i.e. 0x00 0x06).

The XOR of the Sequence Number (SQN) and the Anonymity Key (AK) is sent to the UE as a part of the Authentication Token (AUTN), see TS 33.102. If AK is not used, AK shall be treated in accordance with TS 33.102, i.e. as 000…0.

The serving network name shall be constructed as specified in clause 6.1.1.4.

The input key KEY shall be equal to the concatenation CK || IK of CK and IK.

A.3 CK' and IK' derivation function

When deriving CK' and IK' then the KDF of TS 33.402 [11] clause A.2 shall be used with the following exception: the serving network name (specified in clause 6.1.1.4) shall be used as the value of access network identity (P0).

A.4 RES* and XRES* derivation function

When deriving RES* from RES, RAND, and serving network name in the UE and when deriving XRES* from XRES, RAND, and the serving network name in the ARPF, the following parameters shall be used to form the input S to the KDF.

- FC = 0x6B,
- P0 = serving network name,
- L0 = length of the serving network name (variable length as specified in 24.501 [35]),
- P1 = RAND,
- L1 = length of RAND (i.e. 0x00 0x10),
- P2 = RES or XRES,
- L2 = length RES or XRES (i.e. variable length between 0x00 0x04 and 0x00 0x10).

The input key KEY shall be equal to the concatenation CK || IK of CK and IK.

The serving network name shall be constructed as specified in clause 6.1.1.4.

The (X)RES* is identified with the 128 least significant bits of the output of the KDF.

A.5 HRES* and HXRES* derivation function

When deriving HRES* from RES* in the SEAF and when deriving HXRES* from XRES* in the AUSF the following parameters shall be used to form the input S to the SHA-256 hashing algorithm:

- P0 = RAND,
- P1 = RES* or XRES*,

The input S shall be equal to the concatenation P0||P1 of the P0 and P1.

The H(X)RES* is identified with the 128 least significant bits of the output of the SHA-256 function.

A.6 K_{SEAF} derivation function

When deriving a K_{SEAF} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF:

- FC = 0x6C,
- P0 = <serving network name>,
- L0 = length of <serving network name>.

The input key KEY shall be K_{AUSF}.

The serving network name shall be constructed as specified in clause 6.1.1.4.

A.7 K_{AMF} derivation function

A.7.0 Parameters for the input S to the KDF

When deriving a K_{AMF} from K_{SEAF} the following parameters shall be used to form the input S to the KDF.

- FC = 0x6D
- P0 = IMSI or NAI or GCI or GLI
- L0 = P0 length - number of octets in P0
- P1 = ABBA parameter
- L1 = P1 length - number of octets in P1

The input key KEY shall be the 256-bit K_{SEAF}.

For P0, when the SUPI type is IMSI, P0 shall be set to IMSI as defined in clause 2.2 of TS 23.003 [19]. For P0, when the SUPI type is network specific identifier, the P0 shall be set to Network Access Identifier (NAI) as defined in clause 28.7.2 of TS 23.003 [19]. When the SUPI type is GLI, P0 shall be set to GLI taking format of NAI as defined in clause 28.16.2 of TS 23.003 [19]. When the SUPI type is GCI, P0 shall be set to GCI taking format of NAI as defined in clause 28.15.2 of TS 23.003 [19]. P0 shall be represented as a character string as specified in B.2.1.2 of TS 33.220 [28], for both SUPI types.

For ABBA parameter values please refer to clause A.7.1.

A.7.1 ABBA parameter values

ABBA parameter is provided to the UE from SEAF and shall be used as an input parameter for K_{AMF} derivation. To support flexible set of security features ABBA parameter is defined when security features change. To ensure forward compatibility, the ABBA parameter is a variable length parameter.

The SEAF shall set the ABBA parameter to 0x0000. The UE shall use the ABBA parameter provided by the SEAF in the calculation of K_{AMF}.

The following values have been defined for this parameter.

ABBA parameter value	**Description**
0x0000	Initial set of security features defined for 5GS.

Table A.7.1-1: ABBA parameter definitions

A.8 Algorithm key derivation functions

When deriving keys for NAS integrity and NAS encryption algorithms from K_{AMF} in the AMF and UE or ciphering and integrity keys from K_{gNB}/ K_{SN} in the gNB and UE, the following parameters shall be used to form the string S.

- FC = 0x69
- P0 = algorithm type distinguisher
- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)
- P1 = algorithm identity
- L1 = length of algorithm identity (i.e. 0x00 0x01)

The algorithm type distinguisher shall be N-NAS-enc-alg for NAS encryption algorithms and N-NAS-int-alg for NAS integrity protection algorithms. The algorithm type distinguisher shall be N-RRC-enc-alg for RRC encryption algorithms, N-RRC-int-alg for RRC integrity protection algorithms, N-UP-enc-alg for UP encryption algorithms and N-UP-int-alg for UP integrity protection algorithms (see table A.8-1). The values 0x00 and 0x07 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

Table A.8-1: Algorithm type distinguishers

Algorithm distinguisher	Value
N-NAS-enc-alg	0x01
N-NAS-int-alg	0x02
N-RRC-enc-alg	0x03
N-RRC-int-alg	0x04
N-UP-enc-alg	0x05
N-UP-int-alg	0x06

The algorithm identity (as specified in clause 5) shall be put in the four least significant bits of the octet. The two least significant bits of the four most significant bits are reserved for future use, and the two most significant bits of the most significant nibble are reserved for private use. The entire four most significant bits shall be set to all zeros.

For the derivation of integrity and ciphering keys used between the UE and gNB, the input key shall be the 256-bit K_{gNB}// K_{SN}. For the derivation of integrity and ciphering keys used between the UE and AMF, the input key shall be the 256-bit K_{AMF}.

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

A.9 K_{gNB}, K_{WAGF}, K_{TNGF}, K_{TWIF} and K_{N3IWF} derivation function

When deriving the keys K_{gNB}, K_{WAGF}, K_{TNGF}, K_{TWIF} and K_{N3IWF} from K_{AMF} and the uplink NAS COUNT in the UE and the AMF the following parameters shall be used to form the input S to the KDF.

- FC = 0x6E
- P0 = Uplink NAS COUNT
- L0 = length of uplink NAS COUNT (i.e. 0x00 0x04)
- P1 = Access type distinguisher
- L1 = length of Access type distinguisher (i.e. 0x00 0x01)

The values for the access type distinguisher are defined in table A.9-1. The values 0x00 and 0x03 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

The access type distinguisher shall be set to the value for 3GPP (0x01) when deriving KgNB. The access type distinguisher shall be set to the value for non-3GPP (0x02) when deriving K_{N3IWF}, K_{WAGF}, K_{TWIF} or K_{TNGF}..

Table A.9-1: Access type distinguishers

Access type distinguisher	Value
3GPP access	0x01
Non 3GPP access	0x02

The input key KEY shall be the 256-bit K_{AMF}.

This function is applied when cryptographically protected 5G radio bearers are established and when a key change on-the-fly is performed.

As N5CW devices do not support NAS over non-3GPP access, the Uplink NAS COUNT shall be set to 0 for K_{TWIF} key generation, see clause 7A.2.4.

A.10 NH derivation function

When deriving a NH from K_{AMF} the following parameters shall be used to form the input S to the KDF.

- FC = 0x6F
- P0 = SYNC-input
- L0 = length of SYNC-input (i.e. 0x00 0x20)

The SYNC-input parameter shall be the newly derived K_{gNB} for the initial NH derivation, and the previous NH for all subsequent derivations. This results in a NH chain, where the next NH is always fresh and derived from the previous NH.

The input key KEY shall be the 256-bit K_{AMF}.

A.11 $K_{NG\text{-}RAN}$* derivation function for target gNB

When deriving a $K_{NG\text{-}RAN}$* from current K_{gNB} or from fresh NH and the target physical cell ID in the UE and NG-RAN for handover purposes and transition from RRC_INACTIVE to RRC_CONNECTED states the following parameters shall be used to form the input S to the KDF.

- FC = 0x70
- P0 = PCI (target physical cell id)
- L0 = length of PCI (i.e. 0x00 0x02)
- P1 = ARFCN-DL (the absolute frequency of SSB of the target PCell as specified in clause 13.3 of TS 38.300 [52])
- L1 = length of ARFCN-DL (i.e. 0x00 0x03)

The input key KEY shall be the 256-bit NH when the index NCC in the handover increases, otherwise the current 256-bit K_{gNB}(when source is gNB) or K_{eNB} (when source is ng-eNB).

A.12 $K_{NG\text{-}RAN}$* derivation function for target ng-eNB

When deriving a $K_{NG\text{-}RAN}$* from current K_{gNB} or from fresh NH and the target physical cell ID in the UE and NG-RAN for handover purposes and transition from RRC_INACTIVE to RRC_CONNECTED states the following parameters shall be used to form the input S to the KDF.

- FC = 0x71
- P0 = PCI (target physical cell id)
- L0 = length of PCI (i.e. 0x00 0x02)
- P1 = EARFCN-DL (target physical cell downlink frequency)
- L1 = length of EARFCN-DL (i.e. 0x00 0x03)

The input key KEY shall be the 256-bit NH when the index NCC in the handover increases, otherwise the current 256-bit K_{gNB} (when source is gNB) or K_{eNB} (when source is ng-eNB).

A.13 K_{AMF} to K_{AMF}' derivation in mobility

Derivation of K_{AMF}' from K_{AMF} during mobility shall use the following input parameters.

- FC = 0x72
- P0 = DIRECTION
- L0 = length of DIRECTION (i.e. 0x00 0x01)
- P1 = COUNT,
- L1 = length of COUNT (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

When K_{AMF}' is derived in handover, DIRECTION shall be 0x01 and COUNT shall be the downlink NAS COUNT of the 3GPP access.

When K_{AMF}' is derived in idle mode mobility (i.e., mobility registration update), DIRECTION shall be 0x00 and COUNT shall be the uplink NAS COUNT of the 3GPP access used in the Registration Request.

A.14 K_{AMF} to K_{ASME}' derivation for interworking

A.14.1 Idle mode mobility

This input string is used when there is a need to derive K'_{ASME} from K_{AMF} during mapping of security contexts from 5G to EPS at idle mode mobility. The following input parameters shall be used.

- FC = 0x73
- P0 = NAS Uplink COUNT value
- L0 = length of NAS Uplink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

A.14.2 Handover

This input string is used when there is a need to derive K_{ASME}' from K_{AMF} during mapping of security contexts from 5G to EPS at handovers. The following input parameters shall be used.

- FC = 0x74
- P0 = NAS Downlink COUNT value
- L0 = length of NAS Downlink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

A.15 K_{ASME} to K_{AMF}' derivation for interworking

A.15.1 Idle mode mobility

This input string is used when there is a need to derive K_{AMF}' from K_{ASME} during mapping of security contexts from EPS to 5G at idle mode mobility. The following input parameters shall be used.

- FC = 0x75
- P0 = NAS Uplink COUNT value of the TAU message included in the Registration Request message
- L0 = length of NAS Uplink COUNT value of the TAU message included in the Registration Request message (i.e. 0x00 0x04)

The input key KEY shall be K_{ASME}.

A.15.2 Handover

This input string is used when there is a need to derive K_{AMF}' from K_{ASME} during mapping of security contexts from EPS to 5G at handovers. The following input parameters shall be used.

- FC = 0x76
- P0 = NH value
- L0 = length of NH value (i.e. 0x00 0x20)

The input key KEY shall be K_{ASME}.

A.16 Derivation of K_{SN} for dual connectivity

This input string is used when the MN and UE derive K_{SN} during dual connectivity. The following input parameters shall be used:

- FC =0x79,
- P0 = Value of the SN Counter as a non-negative integer,
- L0 = length of the SN Counter value (i.e. 0x00 0x02).

The input key KEY shall be K_{eNB} when the MN is an ng-eNB and K_{gNB} when the MN is a gNB.

A.17 SoR-MAC-I_{AUSF} generation function

When deriving a SoR-MAC-I_{AUSF} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x77,
- P0 = SoR header,
- L0 = length of SoR header,
- P1 = $Counter_{SoR}$,
- L1 = length of $Counter_{SoR}$,
- P2 = octets included in SoR transparent container (in clause 9.11.3.51 of TS 24.501 [35]) beyond (and not including) octet 22,
- L2 = length of list data included in P2

The input key KEY shall be K_{AUSF}.

The selection of parameters included in P2 shall be the same as the selection of input to the Nausf_SoRProtection service operation. If none of these parameters are included in Nausf_SoRProtection service operation, P2 and L2 are not included for SoR-MAC-I_{AUSF} generation.

The SOR header is either received from the requester NF (e.g UDM), or constructed by the AUSF, as described in clause 9.11.3.51 of TS 24.501 [35], based on the information received from the requester NF (e.g. UDM), i.e. ACK Indication and List of preferred PLMN/access technology combinations or secured packet (if provided).

The SoR-MAC-I_{AUSF} is identified with the 128 least significant bits of the output of the KDF.

A.18 SoR-MAC-I_{UE}/SoR-XMAC-I_{UE} generation function

When deriving a SoR-MAC-I_{UE}/SoR-XMAC-I_{UE} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x78,
- P0 = 0x01 (SoR Acknowledgement: Verified the Steering of Roaming Information successfully),
- L0 = length of SoR Acknowledgement (i.e. 0x00 0x01),
- P1 = $Counter_{SoR}$,
- L1 = length of $Counter_{SoR}$.

The input key KEY shall be K_{AUSF}.

The SoR-MAC-I_{UE}/SoR-XMAC-I_{UE} is identified with the 128 least significant bits of the output of the KDF.

A.19 UPU-MAC-I_{AUSF} generation function

When deriving a UPU-MAC-I_{AUSF} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x7B,
- P0 = UE Parameters Update Data, i.e. UE parameters update list as given in clause 9.11.3.53A of TS 24.501 [35] (starting from octet 23),
- L0 = length of UE Parameters Update Data
- P1 = $Counter_{UPU}$
- L1 = length of $Counter_{UPU}$

The input key Key shall be K_{AUSF}.

The UPU-MAC-I_{AUSF} is identified with the 128 least significant bits of the output of the KDF.

A.20 UPU-MAC-I_{UE}/UPU-XMAC-I_{UE} generation function

When deriving a UPU-MAC-I_{UE}/UPU-XMAC-I_{UE} from K_{AUSF}, the following parameters shall be used to form the input S to the KDF.

- FC = 0x7C,
- P0 = 0x01 (UPU Acknowledgement: Verified the UE Parameters Update Data successfully)
- L0 = length of UPU Acknowledgement (i.e. 0x00 0x01)
- P1 = $Counter_{UPU}$
- L1 = length of $Counter_{UPU}$

The input key Key shall be K_{AUSF}.

The UPU-MAC-I_{UE}/UPU-XMAC-I_{UE} is identified with the 128 least significant bits of the output of the KDF.

A.21 K_{AMF} to K_{ASME_SRVCC} derivation for interworking

This input string is used when there is a need to derive K_{ASME_SRVCC} from K_{AMF} during SRVCC from 5G to UTRAN CS. The following input parameters shall be used.

- FC = 0x7D
- P0 = NAS Downlink COUNT value
- L0 = length of NAS Downlink COUNT value (i.e. 0x00 0x04)

The input key KEY shall be K_{AMF}.

A.22 K_{TIPSec} and K_{TNAP} derivation function

When deriving a K_{TIPSec} from K_{TNGF} and when deriving a K_{TNAP} from K_{TWIF} or K_{TNGF} the following parameters shall be used to form the input S to the KDF.

- FC = 0x84
- P0 = Usage type distinguisher
- L0 = length of Usage type distinguisher (i.e. 0x00 0x01)

The values for the Usage type distinguisher are defined in table A.22-1. The values 0x00 and 0x03 to 0xf0 are reserved for future use, and the values 0xf1 to 0xff are reserved for private use.

The Usage type distinguisher shall be set to the value for IPSec (0x01) when deriving K_{TIPSec}. The Usage type distinguisher shall be set to the value for TNAP (0x02) when deriving K_{TNAP}.

The input key KEY shall be the 256-bit K_{TNGF} or K_{TWIF}.

Table A.22-1: Usage type distinguishers

Usage type distinguisher	Value
IPSec	0x01
TNAP	0x02

A.23 K_{IAB} generation function

This input string is used when the IAB-node and the IAB-donor derive K_{IAB} (PSK) for establishment of secure F1 interface. The following parameters shall be used to form the input S to the KDF:

- FC = 0x83,
- P0 = IAB-donor-CU IP address,
- L0 = length of IAB-donor-CU IP address,
- P1 = IAB-node DU IP address,
- L1 = length of IAB-node DU IP address.

The input key KEY shall be $K_{gNB,}$ if the key K_{gNB} is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU (also when acts as MN for NR-DC scenario), after the IAB-UE setup procedure (Phase-1).

The input key KEY shall be S-K_{gNB}, if the key S-K_{gNB} is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU (acts as a SN for EN-DC scenario), after dual connectivity procedure.

The input key KEY shall be K_{SN}, if the key K_{SN} is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU (acts as a SN for NR-DC scenario), after dual connectivity procedure.

For P0, in case of CP-UP separation of IAB-donor-CU,

- P0 shall be set to IAB-donor-CU-CP IP address for deriving $K_{IAB\text{-}CU\text{-}CP}$.
- P0 shall be set to IAB-donor-CU-UP IP address for deriving $K_{IAB\text{-}CU\text{-}UP}$.

The entire output of the KDF (256 bits) is used as the K_{IAB} or $K_{IAB\text{-}CU\text{-}CP}$ or $K_{IAB\text{-}CU\text{-}UP}$..

Annex B (informative): Using additional EAP methods for primary authentication

B.1 Introduction

The present annex describes an example of the usage of additional EAP methods for primary authentication in private networks using the 5G system as specified in TS 22.261 [7]. It is provided as an example on how the 5G authentication framework for primary authentication can be applied to EAP methods other than EAP-AKA' The additional EAP methods are only intended for private networks or with IoT devices in isolated deployment scenarios, i.e. roaming is not considered, as specified in TS 22.261 [7].

When the 5G system is deployed in private networks, the SUPI and SUCI should be encoded using the NAI format as specified in TS 23.501 [2]. UE always includes the realm part in the NAI for routing to the correct UDM.

B.2 Primary authentication and key agreement

B.2.1 EAP TLS

B.2.1.1 Security procedures

EAP-TLS is a mutual authentication EAP method that can be used by the EAP peer and the EAP server to authenticate each other. It is specified in RFC 5216 [38] and draft-ietf-emu-eap-tls13 [76]. The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [3]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [5].

EAP-TLS supports several TLS versions, and the negotiation of the TLS version is part of EAP-TLS. The main principle of negotiation goes as follows. The EAP server indicates the support for EAP-TLS in the EAP-Request. If the peer chooses EAP-TLS, it responds with an EAP-Response indicating in the ClientHello message which TLS versions the peer supports. The EAP server chooses the TLS version, and indicates the chosen version in the ServerHello message.

The TLS procedure described in the RFC 5216 [38] is applicable to TLS 1.2 defined in RFC 5246 [40]. The TLS procedure described in the draft-ietf-emu-eap-tls13 [76] is applicable to TLS 1.3 defined in RFC 8446 [77].

The procedure below is based on the unified authentication framework from the present document, procedures from TS 23.502 [8] and RFC 5216 [38]. The procedure for EAP-TLS with TLS 1.2 is presented here as an example, and other potential procedures are possible, e.g. if TLS resumption is used.

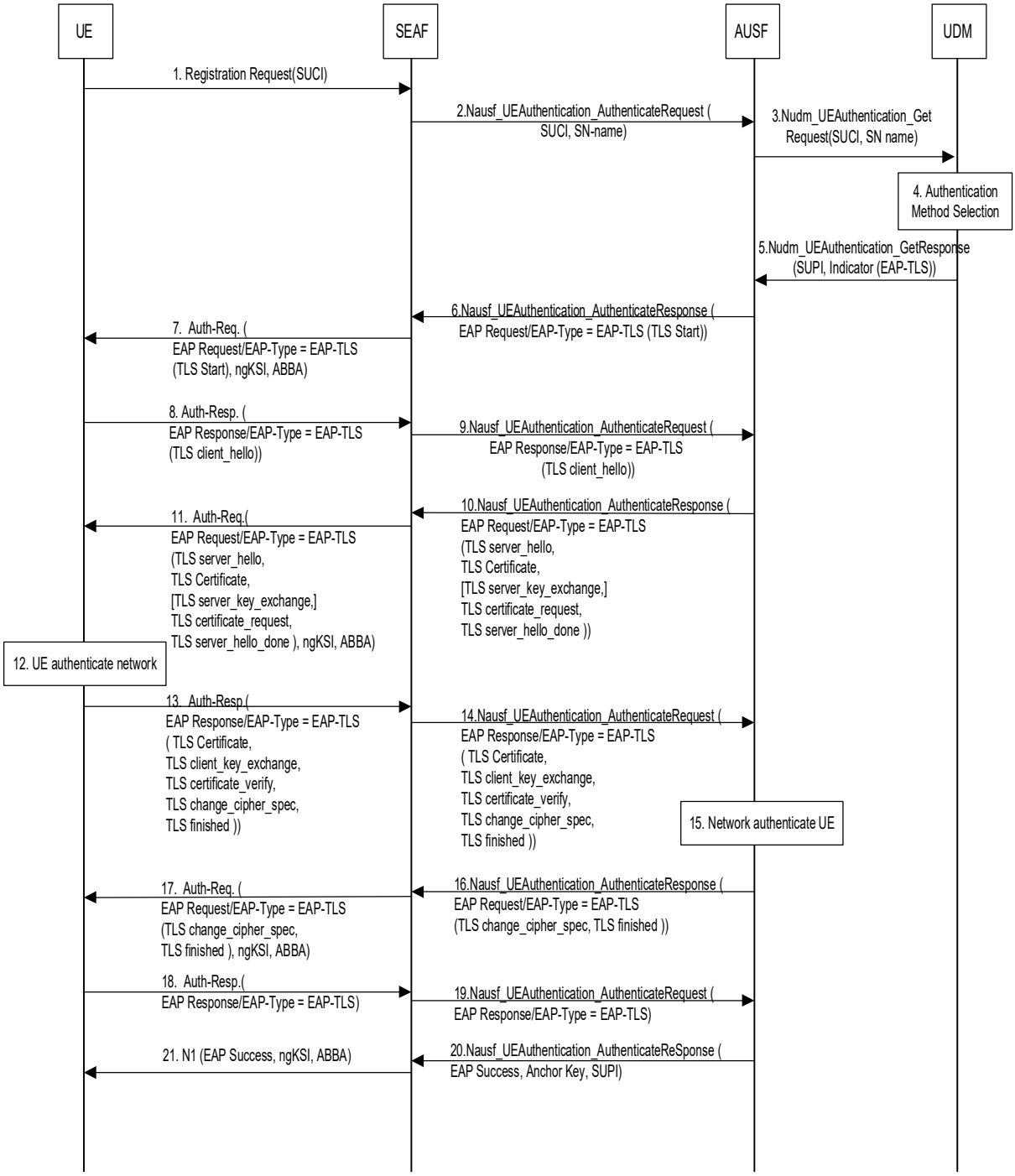


Figure B.2.1.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial authentication

1. The UE sends the Registration Request message to the SEAF, containing SUCI. If the SUPI is in NAI format, only the username part of the NAI is encrypted using the selected protection scheme and included in the SUCI, together with the realm part in the NAI needed for UDM routing.

   Privacy considerations are described in Clause B.2.2.

2. The SEAF sends Nausf_UEAuthentication_Authenticate Request message to the AUSF. The SUCI and the serving network name (as described in clause 6.1.1.4) are included in the message.

3. AUSF sends the the Nudm_UEAuthentication_Get Request, containing SUCI and the serving network name, to UDM. The general rules for UDM selection apply.

4. The SIDF located within the UDM de-conceals the SUCI to SUPI if SUCI is received in the message. The UDM then selects the primary authentication method.

5. If the UDM chooses to use EAP-TLS, it sends the SUPI and an indicator to choose EAP-TLS to AUSF in the Nudm_UEAuthentication_Get Response.

6. With the received SUPI and the indicator, the AUSF chooses EAP-TLS as the authentication method. The AUSF sends thea Nausf_UEAuthentication_Authenticate Response message containing EAP-Request/EAP-TLS [TLS start] message to the SEAF.

7. The SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the UE. This message also includes the ngKSI and the ABBA parameter. In fact, the SEAF shall always include the ngKSI and ABBA parameter in all EAP-Authentication request message. ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. During an EAP authentication, the value of the ngKSI and the ABBA parameter sent by the SEAF to the UE shall not be changed.

8. After receiving the EAP-TLS [TLS-start] message from SEAF, the UE replies with an EAP-Response/EAP-TLS [client_hello] to the SEAF in the Authentication Response message. The contents of TLS client_hello are defined in the TLS specification of the TLS version in use.

NOTE1: The EAP framework supports negotiation of EAP methods. If the UE does not support EAP-TLS, it should follow the rule described in RFC 3748 [27] to negotiate another EAP method. In 5G system, UDM typically knows which EAP method and credentials are supported by the subscriber, and consequently EAP based negotiation may never be used.

9. The SEAF forwards the EAP-Response/EAP-TLS [client hello] message to AUSF in the Nausf_UEAuthentication_Authenticate Request.

10. The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf_UEAuthentication_Authenticate Response, which further includes information elements such as server_hello, server_certificate, server_key_exchange, certificate_request, server_hello_done. These information elements are defined in the RFCs for the corresponding TLS version in use.

11. The SEAF forwards the EAP-Request/EAP-TLS message with server_hello and other information elements to the UE through Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

12. The UE authenticates the server with the received message from step 11.

NOTE 2: The UE is required to be pre-configured with a UE certificate and also certificates that can be used to verify server certificates.

13. If the TLS server authentication is successful, then the UE replies with EAP-Response/EAP-TLS in Authentication Response message, which further contains information element such as client_certificate, client_key_exchange, client_certificate_verify, change_cipher_spec, client_finished etc. Privacy considerations are described in Clause B.2.1.2.

14. The SEAF forwards the message with EAP-Response/EAP-TLS message with client_certificate and other information elements to the AUSF in the Nausf_UEAuthentication_Authenticate Request.

15. The AUSF authenticates the UE based on the message received. The AUSF verifies that the client certificate provided by the UE belongs to the subscriber identified by the SUPI. If there is a miss-match in the subscriber identifiers in the SUPI, the AUSF does not accept the client certificate. If the AUSF has successfully verified this message, the AUSF continues to step 16, otherwise it returns an EAP-failure.

NOTE 2: The AUSF is required to be pre-configured with the root or any intermediary CA certificates that can be used to verify UE certificates. Deployment of certificate revocation lists (CRLs) and online certificate status protocol (OCSP) are described in clause B.2.2.

16. The AUSF sends EAP-Request/EAP-TLS message with change_cipher_spec and server_finished to the SEAF in the Nausf_UEAuthentication_Authenticate Response.

17. The SEAF forwards EAP-Request/EAP-TLS message from step 16 to the UE with Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

18. The UE sends an empty EAP-TLS message to the SEAF in Authentication Response message.

19. The SEAF further forwards the EAP-Response/EAP-TLS message to the AUSF in the Nausf_UEAuthentication_Authenticate Request.

20. The AUSF uses the most significant 256 bits of EMSK as the K_{AUSF} and then calculates K_{SEAF} from K_{AUSF} as described in Annex A.6. The AUSF sends an EAP-Success message to the SEAF together with the SUPI and the derived anchor key in the Nausf_UEAuthentication_Authenticate Response.

21. The SEAF forwards the EAP-Success message to the UE and the authentication procedure is finished. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. Then the SEAF derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7, and provides the ngKSI and the K_{AMF} to the AMF.

    On receiving the EAP-Success message, the UE derives EMSK and uses the most significant 256 bits of the EMSK as the K_{AUSF} and then calculates K_{SEAF} in the same way as the AUSF. The UE derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 3: Step 21 could be NAS Security Mode Command or Authentication Result.

NOTE 4: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

NOTE 5: As an implementation option, the UE creates the temporary security context as described in step 21 after receiving the EAP message that allows EMSK to be calculated. The UE turns this temporary security context into a partial security context when it receives the EAP Success. The UE removes the temporary security context if the EAP authentication fails.

B.2.1.2 Privacy considerations

B.2.1.2.1 EAP TLS without subscription identifier privacy

For EAP TLS, if the operator determines to not provide subscription identifier privacy for the UE in TLS layer (e.g., in TLS 1.2 without privacy option), the subscription identifier protection in NAS layer, i.e., in Step 1 of Figure B.2.1-1, becomes ineffective privacy-wise. Therefore, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer. However, the operator may anyway use other than null-schemes (e.g., one of ECIES schemes) for simplification of having single scheme for all UEs in NAS layer even though privacy is not enhanced in this particular case.

The operator could also determine not to provide subscription identifier privacy for the UE in NAS layer even though the TLS layer inherently provides subscription identifier privacy (e.g., in TLS 1.3). In such case, the operator may just choose that UE uses "null-scheme" for calculation of SUCI which is sent in NAS layer.

B.2.1.2.2 EAP TLS with subscription identifier privacy

For EAP TLS, if the operator determines to provide subscription identifier privacy for the UE in TLS layer, the the EAP TLS server needs to support privacy either inherently (e.g., in TLS 1.3) or via separate privacy option (e.g., in TLS 1.2). If privacy is an option in TLS layer, then the operator needs to configure UE with the information that privacy-on-TLS layer is enabled. Further, following considerations need to be taken.

In Step 1 of Figure B.2.1-1, it is important that calculation of SUCI, which is sent in NAS layer, is done using schemes other than "null-scheme". Otherwise, the subscription identifier protection provided by TLS layer becomes ineffective privacy-wise. Nevertheless, the "null-scheme" could be used in NAS layer while still preserving subscription identifier privacy, by omitting the username part from NAI as described in RFC 4282 clause 2.3 [y]. It would be analogous to using anonymous identifier in EAP, meaning that only realm part from NAI is included in SUCI which is sent in NAS layer. Thus formed SUCI can still be used to route the authentication request to AUSF.

In Step 13 and 14 of Figure B.2.1-1, when TLS 1.2 is used, the UE would need to behave as described in "Section 2.1.4. Privacy" of RFC 5216 [38] where instead of sending the client certificate in cleartext over the air, the UE first sends TLS certificate (no cert) and only later sends TLS certificate after a TLS is setup.

B.2.2 Revocation of subscriber certificates

Subscriber certificates that are used with EAP-TLS typically include static validity times. A certificate revocation list (CRL) as specified in RFC 5280 [48] and online certificate status protocol (OCSP) as specified in RFC 6960 [49] are means for the issuing certificate authority (CA) to revoke the certificates before their scheduled expiration date. In 5G security architecture, the UDM/ARPF is responsible for such subscriber status information. EAP-TLS peers and servers may also support Certificate Status Requests (OCSP stapling) as specified in RFC6066 [50] which allows peers to request the server's copy of the current status of certificates.

The deployment of CRLs is demonstrated in figure B.2.2-1. When the UDM/ARPF maintains the CRLs, the lists may be periodically updated to AUSFs, and stored locally in AUSF.

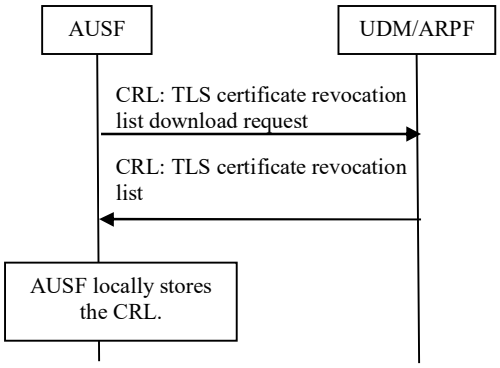


Figure B.2.2-1: AUSF requests CRL from UDM/ARPF

The deployment of OSCP is demonstrated in figure B.2.2-2. When the UDM/ARPF supports OCSP, the AUSF may check the certificate status online.

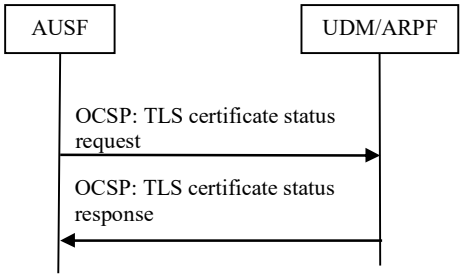


Figure B.2.2-2: AUSF requests the status of TLS certificate from UDM/ARPF

B.3 Key derivation

When EAP methods are used with 5G system, the serving network name is always bound to the anchor key derivation as required in clause 6.1.1.3.

When SEAF acts as a pass-through EAP authenticator, it always includes the serving network name (constructed as specified in clause 6.1.1.4) into the authentication request to the AUSFduring the initial authentication procedure as

specified in clause 6.1.2. The AUSF verifies that the SEAF is authorized to use the serving network name, before it uses the serving network name to calculate the K_{SEAF} from the K_{AUSF} as described in Annex A.6. The AUSF always uses the most significant 256 bits of EMSK as the K_{AUSF}.

When EAP-TLS as specified in RFC 5216 [38] and draft-ietf-emu-eap-tls13 [76] is used for authentication, key materials are derived during authentication and key agreement procedure, which are further split into MSK and EMSK. Both UE and AUSF share a 512 bits EMSK key and use the most significant 256 bits of the EMSK as the K_{AUSF}. The K_{SEAF} is derived based on the rules specified in Annex A.6.

Annex C (normative): Protection schemes for concealing the subscription permanent identifier

C.1 Introduction

The present Annex specifies the protection schemes for concealing the subscription permanent identifier. Each protection scheme is identified by a Protection Scheme Identifier. The Protection Scheme Identifiers are as follows:

null-scheme 0x0;

Profile <A> 0x1;

Profile <B> 0x2.

The values 0x3 - 0xB are reserved for future standardized protection schemes. The values 0xC - 0xF are reserved for proprietary protection schemes specified by the home operator.

Care should be taken when using unique schemes for small groups of users, as this may impact the effectiveness of the privacy scheme for these users.

The size of the Scheme Output of the protection schemes is as follows:

null-scheme size of input, i.e., size of username used in case of NAI format or MSIN in case of IMSI;

Profile <A> total of 256-bit public key, 64-bit MAC, plus size of input;

Profile <B> total of 264-bit public key, 64-bit MAC, plus size of input.

The maximum size of a Scheme Output for proprietary protection schemes shall be total of 3000 octets plus size of input .

NOTE 1: The maximum size of scheme-output was chosen to allow the introduction of quantum-resistant protection schemes.

The UE shall not send, and the network may reject SUCIs larger than the maximum size of scheme-output.

C.2 Null-scheme

The null-scheme shall be implemented such that it returns the same output as the input, which applies to both encryption and decryption.

When using the null-scheme, the SUCI does not conceal the SUPI and therefore the newly generated SUCIs do not need to be fresh.

NOTE 1: The reason for mentioning the non-freshness is that, normally, in order to attain unlinkability (i.e., to make it infeasible for over-the-air attacker to link SUCIs together), it is necessary for newly generated SUCIs to be fresh. But, in case of the null-scheme, the SUCI does not conceal the SUPI. So unlinkability is irrelevant.

NOTE 2: The null-scheme provides no privacy protection.

C.3 Elliptic Curve Integrated Encryption Scheme (ECIES)

C.3.1 General

The use of ECIES for concealment of the SUPI shall adhere to the SECG specifications [29] and [30]. Processing on UE side and home network side are described in high level in clauses C.3.2 and C.3.3.

When the SUPI is of type IMSI, the subscription identifier part of the IMSI (i.e., MSIN) that is used to construct the scheme-input shall be coded as hexadecimal digits using packed BCD coding where the order of digits within an octet is same as the order of MSIN digits specified in Figure 9.11.3.4.3a of TS 24.501 [35]. If the MSIN is composed of an odd number of digits, then the bits 5 to 8 of final octet shall be coded as "1111".

When the SUPI is of type network specific identifier, the subscription identifier part of the SUPI that is used to construct the scheme-input shall follow the encoding rules specified in Annex B.2.1.2 of TS 33.220 [28].

C.3.2 Processing on UE side

The ECIES scheme shall be implemented such that for computing a fresh SUCI, the UE shall use the provisioned public key of the home network and freshly generated ECC (elliptic curve cryptography) ephemeral public/private key pair according to the ECIES parameters provisioned by home network. The processing on UE side shall be done according to the encryption operation defined in [29]. with the following changes to Section 3.8 and step 5 and 6 of Section 5.1.3.

- generate keying data K of length *enckeylen* + *icblen* + *mackeylen*.
- Parse the leftmost enckeylen octets of K as an encryption key EK, the middle icblen octets of K as an ICB, and the rightmost mackeylen octets of K as a MAC key MK.

The final output shall be the concatenation of the ECC ephemeral public key, the ciphertext value, the MAC tag value, and any other parameters, if applicable.

NOTE: The reason for mentioning "any other parameter, if applicable" in the final output is to allow cases, e.g. to enable the sender to send additional sign indication when point compression is used.

The Figure C.3.2-1 illustrates the UE's steps.

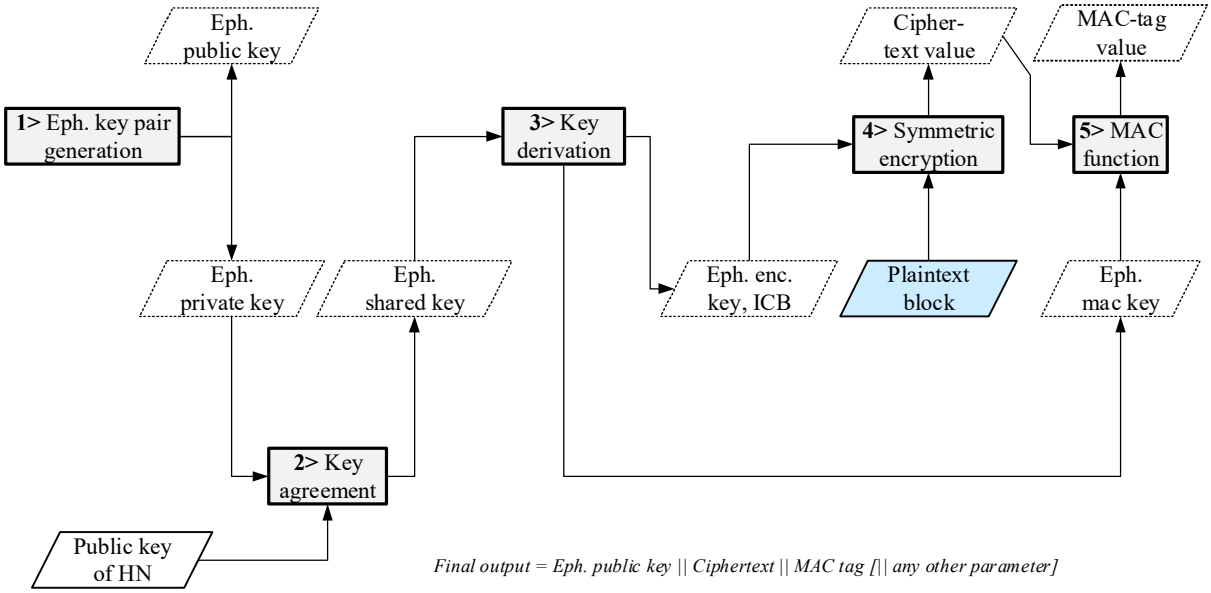


Figure C.3.2-1: Encryption based on ECIES at UE

C.3.3 Processing on home network side

The ECIES scheme shall be implemented such that for deconcealing a SUCI, the home network shall use the received ECC ephemeral public key of the UE and the private key of the home network. The processing on home network side shall be done according to the decryption operation defined in [29]. with the following changes to Section 3.8 and step 6 and 7 of Section 5.1.4.

- generate keying data K of length *enckeylen* + *icblen* + *mackeylen.*
  - Parse the leftmost *enckeylen* octets of *K* as an encryption key *EK*, the middle *icblen* octets of *K* as an ICB, and the rightmost *mackeylen* octets of *K* as a MAC key *MK*.

NOTE: Unlike the UE, the home network does not need to perform a fresh ephemeral key pair generation for each decryption. How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.

The Figure C.3.3-1 illustrates the home network's steps.

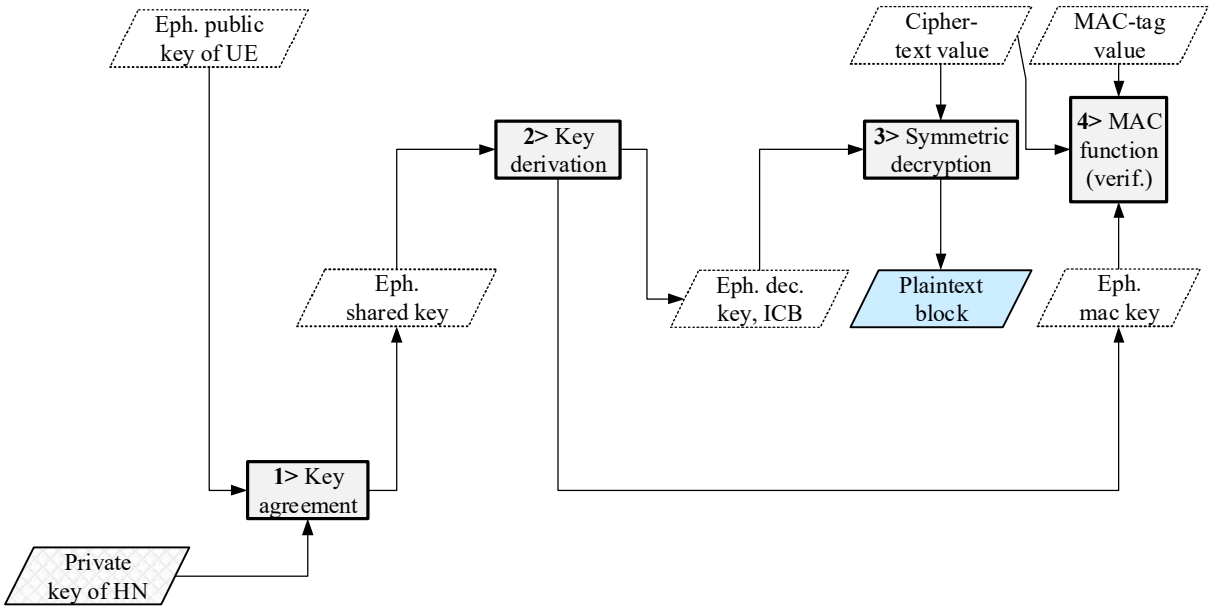


Figure C.3.3-1: Decryption based on ECIES at home network

C.3.4 ECIES profiles

C.3.4.0 General

Unless otherwise stated, the ECIES profiles follow the terminology and processing specified in SECG version 2 [29] and [30]. The profiles shall use "named curves" over prime fields.

For generating successive counter blocks from the initial counter block (ICB) in CTR mode, the profiles shall use the standard incrementing function in section B.1 of NIST Special Publication 800-38A [16] with m = 32 bits. The ICB corresponds to T_1 in section 6.5 of [16].

The value of the *MAC tag* in ECIES, shall be the *L* most significant octets of the output generated by the HMAC function, where *L* equals to the maclen.

Profile A shall use its own standardized processing for key generation (section 6 of RFC 7748 [46]) and shared secret calculation (section 5 of RFC 7748 [46]). The Diffie-Hellman primitive X25519 (section 5 of RFC 7748 [46]) takes two random octet strings as input, decodes them as scalar and coordinate, performs multiplication, and encodes the result as an octet string. The shared secret output octet string from X25519 shall be used as the input Z in the ECIES KDF

(section 3.6.1 of [29]). As the point compression is not applied for profile A, the prefix rule for compression type defined in [29] section 5.1.3 shall not be used in profile A, i.e., there shall be no prefix for the ephemeral public key of Profile A.

Profile B shall use point compression to save overhead and shall use the Elliptic Curve Cofactor Diffie-Hellman Primitive (section 3.3.2 of [29]) to enable future addition of profiles with cofactor $h \neq 1$. For curves with cofactor $h = 1$ the two primitives (section 3.3.1 and 3.3.2 of [29]) are equal.

The profiles shall not use backwards compatibility mode (therefore are not compatible with version 1 of SECG).

C.3.4.1 Profile A

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters : Curve25519 [46]
- EC Diffie-Hellman primitive : X25519 [46]
- point compression : N/A
- KDF : ANSI-X9.63-KDF [29]
- Hash : SHA-256
- SharedInfo_1 : $\overline{R}$(the ephemeral public key octet string – see [29] section 5.1.3)
- MAC : HMAC–SHA-256
- mackeylen : 32 octets (256 bits)
- maclen : 8 octets (64 bits)
- SharedInfo_2 : the empty string
- ENC : AES–128 in CTR mode
- enckeylen : 16 octets (128 bits)
- icblen : 16 octets (128 bits)
- backwards compatibility mode : false

C.3.4.2 Profile B

The ME and SIDF shall implement this profile. The ECIES parameters for this profile shall be the following:

- EC domain parameters : secp256r1 [30]
- EC Diffie-Hellman primitive : Elliptic Curve Cofactor Diffie-Hellman Primitive [29]
- point compression : true
- KDF : ANSI-X9.63-KDF [29]
- Hash : SHA-256
- SharedInfo1 : $\overline{R}$ (the ephemeral public key octet string – see [29] section 5.1.3)
- MAC : HMAC–SHA-256
- mackeylen : 32 octets (256 bits)
- maclen : 8 octets (64 bits)
- SharedInfo2 : the empty string

- ENC : AES–128 in CTR mode
- enckeylen : 16 octets (128 bits)
- icblen : 16 octets (128 bits)
- backwards compatibility mode : false

C.4 Implementers' test data

C.4.1 General

The test data sets presented here are for encryption based on ECIES at UE with protection schemes defined in this clause.

C.4.2 Null-scheme

C.4.2.1 IMSI-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for IMSI-based SUPI and null-scheme.

```
IMSI consists of MCC|MNC: '274012' and MSIN: '001002086'
```

ECIES Scheme Input

```
Scheme Input: '00012080F6'
```

ECIES Scheme Output

```
Scheme Output: '00012080F6'
```

C.4.2.2 Network specific identifier-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for network specific identifier-based SUPI and null-scheme.

```
SUPI is: verylongusername1@3gpp.com
```

ECIES Scheme Input

```
Scheme Input: '766572796C6F6E67757365726E616D6531'
```

ECIES Scheme Output

```
Scheme Output: useridverylongusername1
```

C.4.3 ECIES Profile A

C.4.3.1 IMSI-based SUPI

The following test data set corresponds to SUCI computation in the UE for IMSI-based SUPI and ECIES Profile A.

```
IMSI consists of MCC|MNC: '274012' and MSIN: '001002086'
```

ECIES test data

The ECIES Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with the following data

```
Home Network Private Key:
'c53c22208b61860b06c62e5406a7b330c2b577aa5558981510d128247d38bd1d'

Home Network Public Key:
'5a8d38864820197c3394b92613b20b91633cbd897119273bf8e4a6f4eec0a650'

Eph. Private Key:
'c80949f13ebe61af4ebdbd293ea4f942696b9e815d7e8f0096bbf6ed7de62256'

Eph. Public Key:
'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457d'

Eph. Shared Key:
'028ddf890ec83cdf163947ce45f6ec1a0e3070ea5fe57e2b1f05139f3e82422a'

Eph. Enc. Key:
'2ba342cabd2b3b1e5e4e890da11b65f6'

ICB:
'e2622cb0cdd08204e721c8ea9b95a7c6'

Plaintext block:
'00012080f6'

Cipher-text vaue:
'cb02352410'

Eph. mac key:
'd9846966fb7cf5fcf11266c5957dea60b83fff2b7c940690a4bfe57b1eb52bd2'

MAC-tag value:
'cddd9e730ef3fa87'

Scheme Output:
'b2e92f836055a255837debf850b528997ce0201cb82adfe4be1f587d07d8457dcb02352410cddd9e730ef3fa
87’
```

C.4.3.2 Network specific identifier-based SUPI

The following test data set corresponds to SUCI computation in the UE for network specific identifier-based SUPI and ECIES Profile A.

```
SUPI is: verylongusername1@3gpp.com
```

ECIES test data

The ECIES Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with the following data

```
Home Network Private Key:
'C53C22208B61860B06C62E5406A7B330C2B577AA5558981510D128247D38BD1D'

Home Network Public Key:
'5A8D38864820197C3394B92613B20B91633CBD897119273BF8e4A6f4EEC0A650'

Eph. Private Key:
'BE9EFF3E9F22A4B42A3D236E7A6C500B3F2E7E0C7449988BA800D664BF4FCD97'

Eph. Public Key:
'977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222'

Eph. Shared Key:
'511C1DF473BB88317F923501F8BA944FD3B667D25699DCB552DBCEF60BBDC56D'

Eph. Enc. Key:
```

```
'FE77B87D87F40428EDD71BCA69D79059'

Plaintext block:
'766572796C6F6E67757365726E616D6531'

Cipher-text vaue:
'8E358A1582ADB15322C10E515141D2039A'

Eph. mac key:
'D87B69F4FE8CD6B211264EA5E69F682F151A82252684CDB15A047E6EF0595028'

MAC-tag value:
'12E1D7783A97F1AC'

Scheme Output:
ecckey977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222.cip8E358A1582ADB15
322C10E515141D2039A.mac12E1D7783A97F1AC
```

C.4.4 ECIES Profile B

C.4.4.1 IMSI-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for IMSI-based SUPI and ECIES Profile B.

```
IMSI consists of MCC|MNC: '274012' and MSIN: '001002086'
```

ECIES test data

The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data:

```
Home Network Public Key:
uncompressed:
'0472DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD15A7DED52FCBB097A4ED250
E036C7B9C8C7004C4EEDC4F068CD7BF8D3F900E3B4',

if compressed: '0272DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD1'


Home Network Private Key (Not available in the UE, provided here only for test purposes):
'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key:
If compressed: '039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1'
uncompressed:
'049AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D1D1F44EA1C87AA7478B9545
37BDE79951E748A43294A4F4CF86EAFF1789C9C81F'
If point compression applied (scheme output for Profile B always applies point
compression for Eph. public key as specified in clause C.3.4.2 above)
Eph. Private Key: '99798858A1DC6A2C68637149A4B1DBFD1FDFF5ADDD62A2142F06699ED7602529'

Eph. Shared Key: '6C7E6518980025B982FBB2FF746E3C2E85A196D252099A7AD23EA7B4C0959CAE'

Eph. Enc. Key: '  8A65C3AED80295C12BD55087E965702A'

ICB: 'EF285B4061C3BAEE858AB6EC68487DAE'

Scheme-input corresponding to the plaintext-block: '00012080F6'

Cipher-text vaue: '46A33FC271'

Eph. mac key: : 'A5EBAC0BC48D9CF7AE5CE39CD840AC6C761AEC04078FAB954D634F923E901C64'

MAC-tag value:'6AC7DAE96AA30A4D'

Scheme Output:
```

```
'039AAB8376597021E855679A9778EA0B67396E68C66DF32C0F41E9ACCA2DA9B9D146A33FC2716AC7DAE96AA3
0A4D'
```

C.4.4.2 Network specific identifier-based SUPI

The following test data set corresponds to ECIES-based encryption in the UE for network specific identifier-based SUPI and ECIES Profile B.

```
SUPI is: verylongusername1@3gpp.com
```

ECIES test data

The Scheme Output is computed in the UE as defined in Figure C.3.2-1 of clause C.3.2 with following data:

```
Home Network Public Key:

uncompressed:
'0472DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD15A7DED52FCBB097A4ED250
E036C7B9C8C7004C4EEDC4F068CD7BF8D3F900E3B4',
if compressed: '0272DA71976234CE833A6907425867B82E074D44EF907DFB4B3E21C1C2256EBCD1'

Home Network Private Key (Not available in the UE, provided here only for test purposes):
'F1AB1074477EBCC7F554EA1C5FC368B1616730155E0041AC447D6301975FECDA'

Eph. Public Key(scheme output for Profile B always applies point compression for Eph.
public key as specified in clause C.3.4.2 above):
compressed: '03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B'

Eph. Private Key: '90A5898BD29FFA3F261E00E980067C70A2B1B992A21F5B4FEF6D4DF69FE804AD'

Eph. Shared Key: 'BC3529ED79541CF8C007CE9806330F4A5FF15064D7CF4B16943EF8F007597872'

Eph. Enc. Key: '84F9A78995D39E6968047547ECC12C4F'

Scheme-input corresponding to the plaintext-block: '766572796C6F6E67757365726E616D6531'

Cipher-text vaue: 'BE22D8B9F856A52ED381CD7EAF4CF2D525'

Eph. mac key: '39D5517E965F8E1252B61345ED45226C5F1A8C69F03D6C91437591F0B8E48FA0'

MAC-tag value: '3CDDC61A0A7882EB'

Scheme Output:
ecckey03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B39399218B244B.cipBE22D8B9F856A
52ED381CD7EAF4CF2D525.mac3CDDC61A0A7882EB
```

Annex D (normative): Algorithms for ciphering and integrity protection

D.1 Null ciphering and integrity protection algorithms

The NEA0 algorithm shall be implemented such that it generates a KEYSTREAM of all zeroes (see sub-clause D.2.1). The length of the KEYSTREAM generated shall be equal to the LENGTH input parameter. The generated KEYSTREAM requires no other input parameters but the LENGTH. Apart from this, all processing performed in association with ciphering shall be exactly the same as with any of the ciphering algorithms specified in this Annex.

The NIA0 algorithm shall be implemented in such way that it shall generate a 32 bit MAC-I/NAS-MAC and XMAC-I/XNAS-MAC of all zeroes (see sub-clause D.3.1). Replay protection shall not be activated when NIA0 is activated. All processing performed in association with integrity (except for replay protection) shall be exactly the same as with any of the integrity algorithms specified in this annex except that the receiver does not check the received MAC.

NOTE 1: The reason for mentioning the replay protection here is that replay protection is associated with integrity.

The NIA0 shall not be used for signalling radio bearers (SRBs) except for unauthenticated emergency sessions for unauthenticated UEs in LSM.

The NIA0 shall not be used for data radio bearers (DRBs).

NOTE 2: A UE with a 2G SIM is considered to be in LSM in NR.

NOTE 3: NEA0 and NIA0 provide no security.

D.2 Ciphering algorithms

D.2.1 128-bit Ciphering algorithms

D.2.1.1 Inputs and outputs

The input parameters to the ciphering algorithm are a 128-bit cipher key named KEY, a 32-bit COUNT, a 5-bit bearer identity BEARER, the 1-bit direction of the transmission i.e. DIRECTION, and the length of the keystream required i.e. LENGTH. The DIRECTION bit shall be 0 for uplink and 1 for downlink.

Figure D.2.1.1-1 illustrates the use of the ciphering algorithm NEA to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

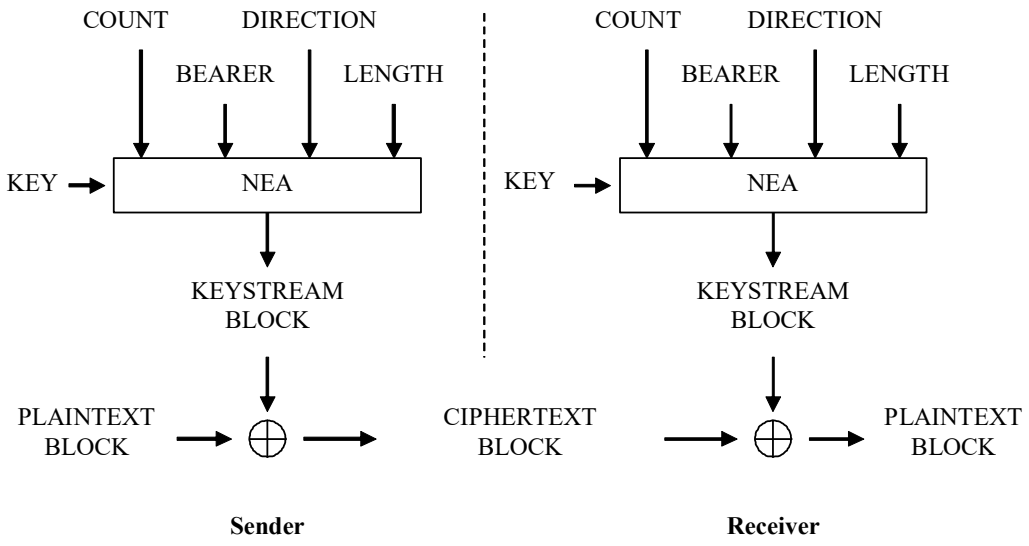


Figure D.2.1.1-1: Ciphering of data

Based on the input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

D.2.1.2 128-NEA1

128-NEA1 is identical to 128-EEA1 as specified in Annex B of TS 33.401 [10].

D.2.1.3 128-NEA2

128-NEA2 is identical to 128-EEA2 as specified in Annex B of TS 33.401 [10].

D.2.1.4 128-NEA3

128-NEA3 is identical to 128-EEA3 as specified in Annex B of TS 33.401 [10].

D.3 Integrity algorithms

D.3.1 128-Bit integrity algorithms

D.3.1.1 Inputs and outputs

The input parameters to the integrity algorithm are a 128-bit integrity key named KEY, a 32-bit COUNT, a 5-bit bearer identity called BEARER, the 1-bit direction of the transmission i.e. DIRECTION, and the message itself i.e. MESSAGE. The DIRECTION bit shall be 0 for uplink and 1 for downlink. The bit length of the MESSAGE is LENGTH.

Figure D.3.1.1-1 illustrates the use of the integrity algorithm NIA to authenticate the integrity of messages.

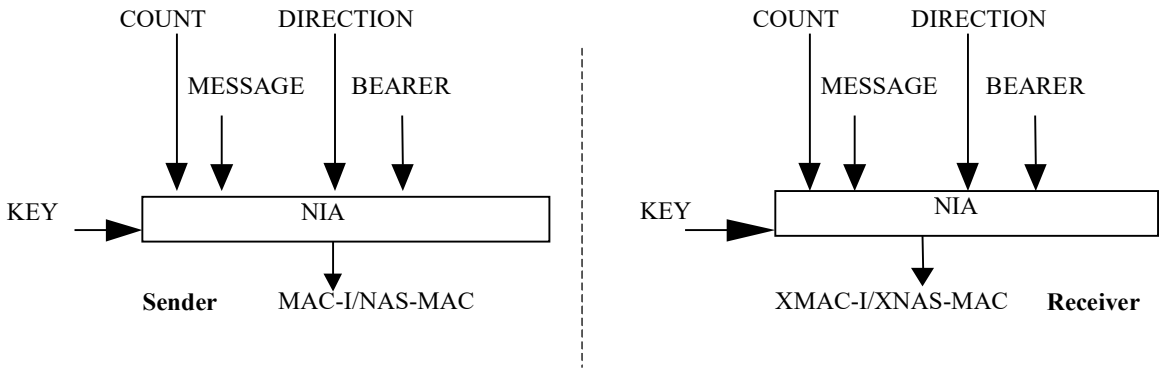


Figure D.3.1.1-1: Derivation of MAC-I/NAS-MAC (or XMAC-I/XNAS-MAC)

Based on these input parameters the sender computes a 32-bit message authentication code (MAC-I/NAS-MAC) using the integrity algorithm NIA. The message authentication code is then appended to the message when sent. For integrity protection algorithms, the receiver computes the expected message authentication code (XMAC-I/XNAS-MAC) on the message received in the same way as the sender computed its message authentication code on the message sent and verifies the data integrity of the message by comparing it to the received message authentication code, i.e. MAC-I/NAS-MAC.

D.3.1.2 128-NIA1

128-NIA1 is identical to 128-EIA1 as specified in Annex B of TS 33.401 [10].

D.3.1.3 128-NIA2

128-NIA2 is identical to 128-EIA2 as specified in Annex B of TS 33.401 [10].

D.3.1.4 128-NIA3

128-NIA3 is identical to 128-EIA3 as specified in Annex B of TS 33.401 [10].

D.4 Test Data for the security algorithms

D.4.1 General

Annex D.4 contains references to the test data for each of the specified algorithms.

D.4.2 128-NEA1

For 128-NEA1 is the test data for UEA2 in TS 35.217 [36] can be reused directly as there is an exact, one-to-one mapping between UEA2 inputs and 128-NEA1 inputs.

D.4.3 128-NIA1

For 128-NIA1 is the test data for 128-EIA1 in clause C.4 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EIA1 inputs and 128-NIA1 inputs.

D.4.4 128-NEA2

For 128-NEA2 is the test data for 128-EEA2 in clause C.1 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EEA2 inputs and 128-NEA2 inputs.

D.4.5 128-NIA2

For 128-NIA2 is the test data for 128-EIA2 in clause C.2 of TS 33.401 [10] can be reused directly as there is an exact, one-to-one mapping between 128-EIA2 inputs and 128-NIA2 inputs.

D.4.6 128-NEA3

For 128-NEA3 is the test data for 128-EEA3 in TS 35.223 [37] can be reused directly as there is an exact, one-to-one mapping between 128-EEA3 inputs and 128-NEA3 inputs.

D.4.7 128-NIA3

For 128-NIA3 is the test data for 128-EIA3 in TS 35.223 [37] can be reused directly as there is an exact, one-to-one mapping between 128-EIA3 inputs and 128-NIA3 inputs.

Annex E (informative): UE-assisted network-based detection of false base station

E.1 Introduction

The UE in RRC_CONNECTED mode sends measurement reports to the network in accordance with the measurement configuration provided by the network. These measurement reports have security values in being useful for detection of false base stations or SUPI/5G-GUTI catchers. The network, in an implementation specific way, could choose UEs or tracking areas or duration for which the measurement reports are to be analysed for detection of false base station. The present Annex gives examples of how measurement reports from UEs could be used for detection of false base station, and some actions thereafter.

E.2 Examples of using measurement reports

The received-signal strength and location information in measurement reports can be used to detect a false base station which attract the UEs by transmitting signal with higher power. They can also be used to detect a false base station which replays the genuine MIB/SIB without modification.

In order to detect a false base station which replays modified version of broadcast information to prevent victim UEs from switching back and forth between itself and genuine base stations (e.g. modifying neighbouring cells, cell reselection criteria, registration timers, etc. to avoid the so called ping-pong effect), information on broadcast information can be used to detect inconsistency from the deployment information.

Further, a false base station which uses inconsistent cell identifier or operates in inconsistent frequency than the deployment of the genuine base stations, can be detected respectively by using the cell identifier or the frequency information in the measurement reports.

Measurement reports collected from multiple UEs can be used to filter out incorrect reports sent by a potential rogue UE.

Upon detection of the false base station, the operator can take further actions, e.g. informing legal authorities or contacting the victim UE.

Annex F (normative): 3GPP 5G profile for EAP-AKA'

F.1 Introduction

The present annex describes the 3GPP 5G profile for EAP-AKA' described in RFC 5448 [12], and RFC 4187 [21].

NOTE: RFC 5448 [12] was specified for the needs of LTE and it does not take into account nor refer to 5G specifications. EAP-AKA' identity handling, when it comes to 5G, is specified in the present Annex F. RFC 5448 [12] has been updated in RFC 9048 [67] to align with the 5G specifications and especially with Annex F. Otherwise RFC 9048 [67] is technically backwards compatible with RFC 5448 [12] . The present document uses RFC 5448 [12] as the normative reference and in case of technical discrepancy, RFC 5448 [12] and the present document take precedence over RFC 9048 [67].

F.2 Subscriber privacy

EAP-AKA' includes optional support for identity privacy mechanism that protects the privacy against passive eavesdropping. The mechanism is described in RFC 4187 [21] clause 4.1.1.2, and it uses pseudonyms that are delivered from the EAP server to the peer as part of an EAP-AKA exchange. The privacy mechanism described in [21] corresponds to the privacy provided by 5G-GUTI, however, assignment of 5G-GUTI is done outside the EAP framework in 5GS.

TS 33.501 assumes that the SUCI is sent outside the EAP messages, however, the peer may still receive EAP-Request/Identity or EAP-Request/AKA-Identity messages. Table F.2-1 specifies how the 5G UE shall behave when receiving such requests.

Table F.2-1: 5G UE behaviour when receiving EAP identity requests

REQUEST	5G UE RESPONSE
EAP-Request/Identity	EAP-Response/Identity SUCI[1)]
EAP-Request/AKA-Identity AT_PERMANENT_REQ	EAP-Response/AKA-Client-Error with the error code "unable to process packet" [2)]
EAP-Request/AKA-Identity AT_FULLAUTH_REQ	EAP-Response/AKA-Identity AT_IDENTITY=SUCI [3)]
EAP-Request/AKA-Identity AT_ANY_ID_REQ	EAP-Response/AKA-Identity AT_IDENTITY=fast re-auth identity OR AT_IDENTITY=SUCI [4)]

1) RFC 3748 [27] allows the peer to respond with abbreviated Identity Response where the peer-name portion of the NAI has been omitted. The 5G UE responds with SUCI in the same format as sent in the Registration Request, where the peer name has been encrypted.

2) RFC 4187 [21] allows the peer to respond with a pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). The 5G UE follows the "conservative" policy that has been described in RFC 4187 [21] clause 4.1.6 (Attacks against Identity Privacy) for the pseudonym based privacy, i.e. the peer shall not reveal its permanent identity. Instead, the peer shall send the EAP-Response/AKA-Client-Error packet with the error code "unable to process packet", and the authentication exchange terminates. The peer assumes that the EAP-Request/AKA-Identity originates from an attacker that impersonates the network, and for this reason refuses to send the cleartext SUPI.

3) RFC 4187 [21] allows the peer to respond with a pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). The 5G UE responds with SUCI.

4) RFC 4187 [21] allows the peer to respond with a fast re-authentication identity, pseudonym (cf. 5G-GUTI) or the permanent identity (i.e. SUPI). If the 5G UE supports fast re-authentication, it responds with the fast re-authentication identity, and if the 5G UE does not support fast re-authentication, it responds with SUCI.

F.3 Subscriber identity and key derivation

EAP-AKA' uses the subscriber identity (Identity) as an input to the key derivation when the key derivation function has value 1 (i.e. MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)). RFC 4187 [21] clause 7 describes that the Identity is taken from the EAP-Response/Identity or EAP-Response/AKA-Identity AT_IDENTITY attribute sent by the peer. This principle is not applied to the 5GS.

If the AT_KDF_INPUT parameter contains the prefix "5G:", the AT_KDF parameter has the value 1 and the authentication is not related to fast re-authentication, then the UE shall set as the Identity for key derivation. When the SUPI Type is IMSI, the Identity shall be set to IMSI as defined in clause 2.2 of TS 23.003 [19]. When the SUPI type is network specific identifier, the Identity shall be set to Network Access Identifier (NAI) as defined in clause 28.7.2 of TS 23.003 [19]. When the SUPI type is GLI, the Identity shall be set to GLI taking format of NAI as defined in clause 28.15.2 of TS 23.003 [19]. When the SUPI type is GCI, the Identity shall be set to GLI taking format of NAI as defined in clause 28.16.2 of TS 23.003 [19]. This principle applies to all full EAP-AKA' authentications, even if the UE sent SUCI in NAS protocol or if the UE sent SUCI in the respose to the EAP identity requests as described in Table F.2-1 or if no identity was sent because the network performed re-authentication. The only exception is fast re-authentication when the UE follows the key derivation as described in RFC 5448 [12] for fast re-authentication.

NOTE 1: The fast re-authentication is not supported in 5GS.

NOTE 2: The prefix "5G:" is part of serving network name as specified in clause 6.1.1.4.

F.4 Void

Annex G (informative): Application layer security on the N32 interface

G.1 Introduction

The SEPP as described in clause 4.2.1 is the entity that sits at the perimeter of the network and performs application layer security on the HTTP message before it is sent externally over the roaming interface.

The application layer traffic comprises all the IEs in the HTTP message payload, sensitive information in HTTP message header and Request URI. Not all the IEs get the same security treatment in SEPP. Some IEs require e2e encryption, some only require e2e integrity protection, while other IEs may require e2e integrity protection but modifiable by intermediate IPX provider while in-transit.

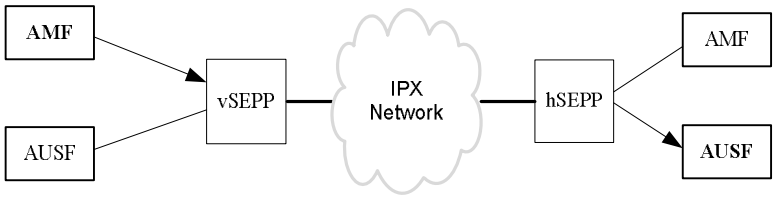


Figure G.1-1: Signaling message from AMF (vPLMN) to AUSF (hPLMN) traversing the respective SEPPs

In the above figure, an example is shown where the AMF NF in the visited PLM network (vPLMN) invokes an API request on the AUSF NF in the home PLM network (hPLMN) using the following message flow:

- The AMF NF first sends the HTTP Request message to its local SEPP (i.e. vSEPP).

- The vSEPP applies application layer security (PRINS) and sends the secure message on the N32 interface to AUSF NF of the hPLMN.

- The hSEPP at the edge of the hPLMN, receives all incoming HTTP messages from its roaming partners. It verifies the message, removes the protection mechanism applied at the application layer, and forwards the resulting HTTP message to the corresponding AUSF NF.

To allow for the trusted intermediary IPX nodes to see and possibly modify specific IEs in the HTTP message, while completely protecting all sensitive information end to end between SEPPs, the SEPP implements application layer security in such a way that:

- Sensitive information such as authentication vectors are fully e2e confidentiality protected between two SEPPs. This ensures that no node in the IPX network shall be able to view such information while in-transit.

- IEs that are subject to modification by intermediary IPX nodes are integrity protected and can only be modified in a verifiable way by authorized IPX nodes.

- Receiving SEPP can detect modification by unauthorized IPX nodes.

G.2 Structure of HTTP Message

Following is a typical structure of the HTTP Message:

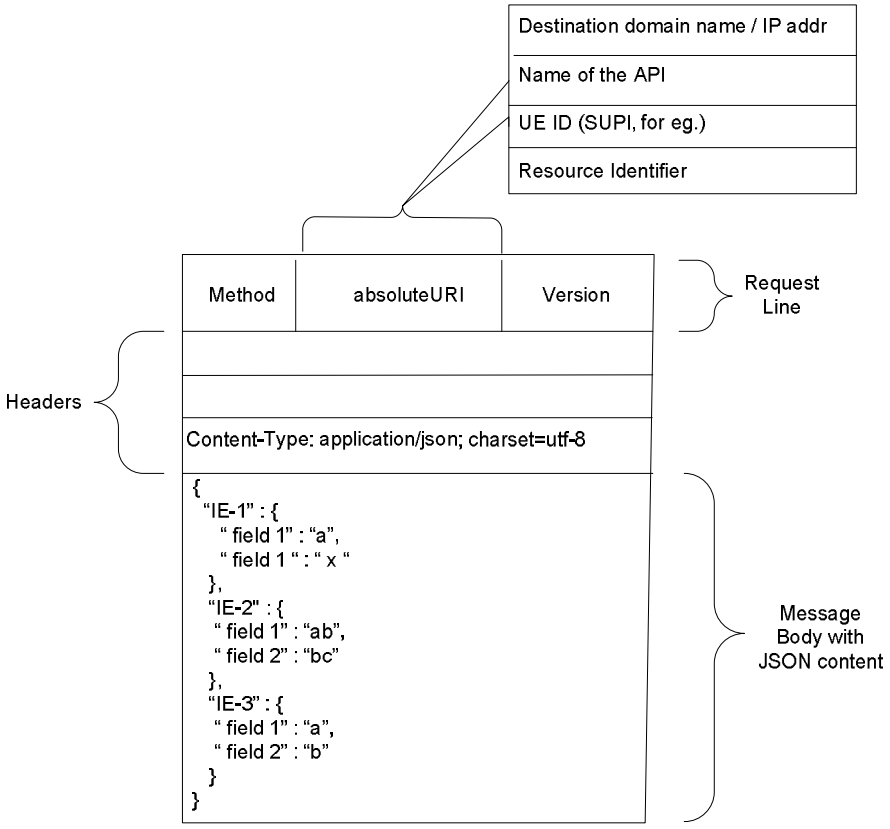


Figure G.2-1 Typical structure of the HTTP message received by SEPP

It consists of:

- HTTP Message payload with JSON based IEs

- HTTP Headers with or without sensitive elements

- HTTP Request-URI with or without sensitive elements such as SUPI.

In the outgoing direction, i.e. towards the N32 interface, the SEPP shall parse the HTTP message fully and apply protection on each part as required.

In the incoming direction, i.e. towards the Network Function, the SEPP shall verify the message, and if successful reassemble the original message and send it to the destined Network Function.

Annex H (informative):
Void

Annex I (normative): Non-public networks

I.1 General

This Annex provides details on security for non-public networks. Most of the security procedures are the same as public networks so this annex only summarizes and specifies where there are exceptions to the normal procedures.

The feature for support of non-public networks (NPN) by 5GS is described in clause 5.30 of 23.501 [2].

I.2 Authentication in standalone non-public networks

I.2.1 General

One of the major differences of non-public networks is that authentication methods other than AKA based ones may be used in a standalone non-public network (SNPN). When an AKA-based authentication method is used, clause 6.1 shall apply. When an authentication method other than 5G AKA or EAP-AKA' is used, only the non-AKA specific parts of clause 6.1 shall apply. An example of running such an authentication method is given in Annex B with EAP-TLS.

The choice of the supported authentication methods for access to SNPNs follows the principles described in clauses I.2.2 and I.2.3.

The authentication server can be an internal authentication server or an external authentication server. The internal authentication server is the AUSF, and the authentication method can be 5G-AKA or EAP-AKA´ as described in clause 6.1, or can be EAP-TLS as described in Annex B. When external authentication server is the AAA, the primary authentication procedure is described in Annex I.2.2.2.2. When external authentication server is an AUSF, then the primary authentication procedure is described in Annex I.2.4. The UDM decides to run primary authentication with internal authentication server or external authentication server.

I.2.2 EAP framework, selection of authentication method, and EAP method credentials

I.2.2.1 General

The EAP authentication framework is supported by the 5GS as described in clause 6.1.1.2.

The UE and the SNPN may support 5G AKA, EAP-AKA', or any other key-generating EAP authentication method.

Selection of the authentication methods is dependent on NPN configuration.

NOTE 1: For EAP-AKA' (as well as 5G AKA), the selection is described in clause 6.1.2. For authentication, that is not using EAP-AKA' (or 5G AKA), the selection is NPN operator deployment specific and out of scope of this specification.

When an EAP authentication method other than EAP-AKA' is selected, the chosen method determines the credentials needed in the UE and network. These credentials, called the EAP-method credentials, shall be used for authentication.

NOTE 2: How credentials for EAP methods other than EAP-AKA' are stored and processed within the UE is out of the scope for standalone non-public networks.

NOTE 3: Storage and processing of credentials for EAP-AKA' (as well as 5G AKA) is described in clause 6 of the present document.

I.2.2.2 Credentials holder using AAA server for primary authentication

I.2.2.2.1 General

The procedures described in this clause enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN.

In this scenario the authentication server role is taken by the AAA Server. The AUSF acts as EAP authenticator and interacts with the AAA Server to execute the primary authentication procedure.

The architecture for SNPN access using credentials from a Credentials Holder using AAA Server is described in clause 5.30.2.9.2 of TS 23.501 [2].

I.2.2.2.2 Procedure

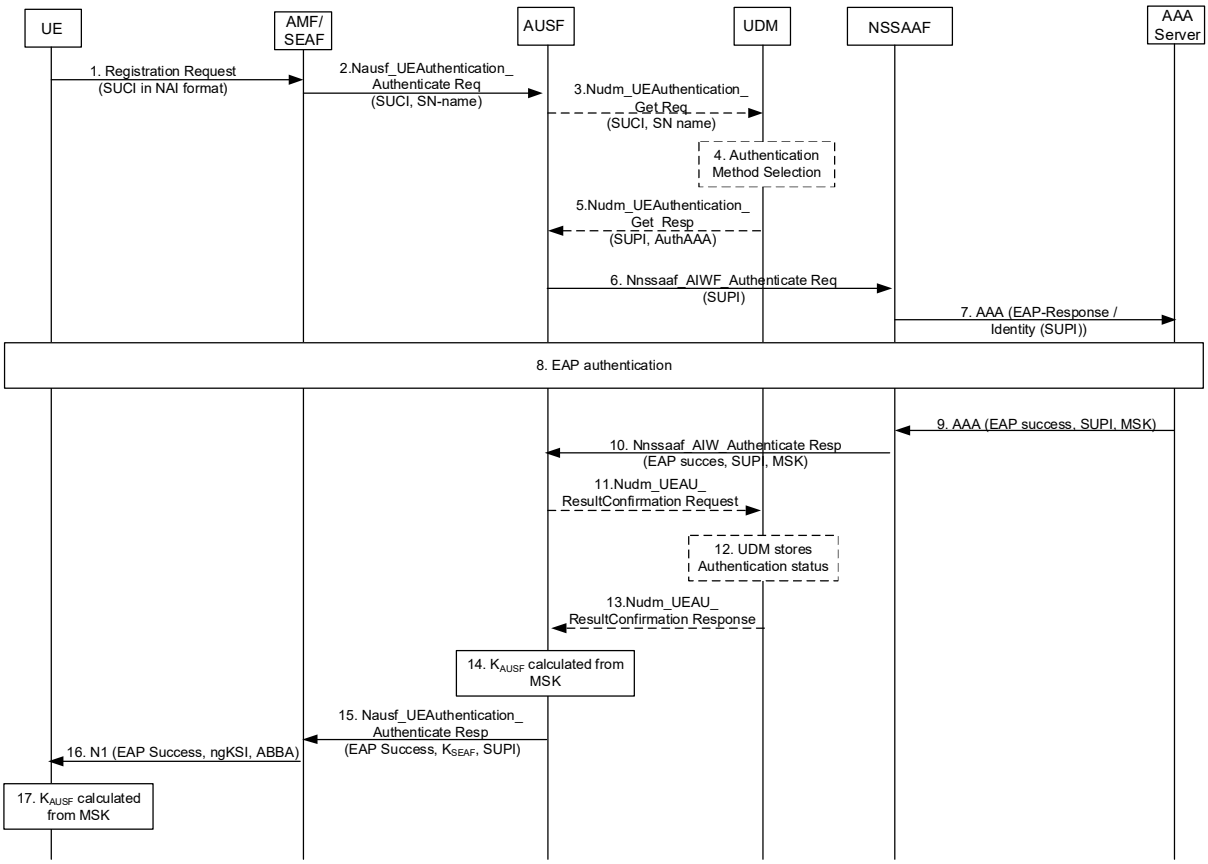


Figure: I.2.2.2.2-1: Primary authentication with external domain

0. The UE shall be configured with credentials from the Credentials holder e.g. SUPI containing a network-specific identifier and credentials for the key-generating EAP-method used. As part of configuration of the credentials, the UE shall also be configured with an indication that the UE shall use MSK for the derivation of K_{AUSF} after the success of the primary authentication. The exact procedures used to configure the UE are not specified in the present document.

   It is further assumed that there exists a trust relation between the SNPN and the Credentials holder AAA Server. These entities need to be mutually authenticated, and the information transferred on the interface need to be confidentiality, integrity and replay protected.

When the procedures of this clause are used for onboarding purposes, the onboarding specific adaptations includes: the 'credentials' used is 'Default credentials', the 'SUPI' used is 'onboarding SUPI', the 'SUCI' used is 'onboarding SUCI' respectively.

1. The UE shall select the SNPN and initiate UE registration in the SNPN.

   For construction of the SUCI, existing methods in clause 6.12 can be used. Otherwise, if the EAP method supports SUPI privacy, the UE may send an anonymous value SUCI based on configuration.

2. The AMF within the SNPN shall initiate a primary authentication for the UE using a Nausf_UEAuthentication_Authenticate service operation with the AUSF. The AMF shall discover and select an AUSF based on criterions specified in TS 23.501 [2] clause 5.30.2.9.2.

3. In the case of onboarding, steps 3-5 are omitted. If steps 3-5 are not omitted, the AUSF shall initiate a Nudm_UEAuthentication_Get service operation. The AUSF shall discover and select a UDM based on criterions specified in TS 23.501 [2] clause 5.30.2.9.

NOTE 1: SUPI will be used instead of SUCI in the case of a re-authentication.

4. In case the UDM receives a SUCI, the UDM shall resolve the SUCI to the SUPI before checking the authentication method applicable for the SUPI. The UDM decides to run primary authentication with an external entity based on subscription data.

   In case the UDM receives an anonymous SUCI, the UDM decides to run primary authentication with an external entity based the realm part of the SUPI in NAI format.

NOTE 1a: The UDM needs to be configured with a list of realms and the intended authentication server

   In case the UDM receives an anonymous SUCI that does not contain the realm part, the UDM shall abort the procedure. Otherwise, the UDM authorizes the UE based on realm part of SUCI and send the anonymous SUPI and the indicator to the AUSF as described in step5.

   The anonymous SUPI shall be a NAI format.

5. In case the UDM received a SUCI in previous steps, the UDM shall provide the AUSF with the SUPI or anonymous SUPI and shall indicate to the AUSF to run primary authentication with a AAA Server in an external Credentials holder.

   When a Credentials Holder using AAA Server is used for primary authentication, the AUSF uses the MSK to derive K_{AUSF}. It is strongly recommended that the same credentials that are used for authentication between UE and the 5G SNPN are not used for the authentication between the UE and a non-5G network, assuming that 5G SNPN and non-5G network are in different security domains.

NOTE 2: MSKs obtained from the non-5G network could be used to impersonate the 5G SNPN towards the UE.

6. Based on the indication from the UDM, the AUSF shall select an NSSAAF as defined in TS 23.501 [2] and initiate a Nnssaaf_AIWF_Authenticate service operation towards that NSSAAF as defined in clause 14.4.2.

7. The NSSAAF shall select AAA Server based on the domain name corresponding to the realm part of the SUPI. The NSSAAF shall perform related protocol conversion and relay EAP messages to the AAA Server.

NOTE 3: The interface and protocol between NSSAAF and AAA is out of scope of the present document and existing AAA protocols such as RADIUS or Diameter can be used.

8. The UE and AAA Server shall perform mutual authentication. The AAA Server shall act as the EAP Server for the purpose of primary authentication. The EAP Identity received by the AAA Server in the EAP-Response/Identity message in step 7 may contain anonymised SUPI. In such cases, AAA Server uses the EAP-method specific EAP Identity request/response messages to obtain the UE identifier as part of the EAP authentication between the UE and the AAA Server.

9. After successful authentication, the MSK and the SUPI (i.e., the UE identifier that is used for the successful EAP authentication) shall be provided from the AAA Server to the NSSAAF.

10. The NSSAAF returns the MSK and the SUPI to the AUSF using the Nnssaaf_AIWF_Authenticate service operation response message. The SUPI received from the AAA shall be used when deriving 5G keys (e.g., K_{AMF}) that requires SUPI as an input for the key derivation.

11-13. In case of onboarding or SUCI received in step 2 is not anonymous, steps 11-13 are omitted. Otherwise, the AUSF verifies that the SUPI corresponds to a valid subscription in the SNPN by informing the UDM about the authentication result for the received SUPI using a Nudm_UEAuthentication_ResultConfirmation service operation. The UDM stores the authentication state for the SUPI and if there is not a subscription corresponding to the SUPI, the UDM shall return an error.

If the verification of the SUPI is not successful, then the AUSF rejects the UE access to the SNPN.

NOTE 4: If the above failure happens, the error is no failed authentication but lacking subscription in the SNPN.

14. The AUSF shall use the most significant 256 bits of MSK as the K_{AUSF}. The AUSF shall also derive K_{SEAF} from the K_{AUSF} as defined in Annex A.6.

15. The AUSF shall send the successful indication together with the SUPI of the UE to the AMF/SEAF together with the resulting K_{SEAF}.

16. The AMF shall send the EAP success in a NAS message.

17. The UE shall derive the K_{AUSF} from MSK as described in step 11 according to the pre-configured indication as described in step 0.

I.2.3 Key hierarchy, key derivation and key distribution

I.2.3.1 General

The text in clauses 6.2.1 and 6.2.2 cannot apply directly for an EAP authentication method other than EAP-AKA' as these clauses assume that an AKA-based authentication method is used. The major differences are the way in which K_{AUSF} is calculated and that the UDM/ARPF is not necessarily involved in the key derivation or distribution.

Depending on the selected authentication method, the K_{AUSF} is generated as follows:

- For 5G AKA and EAP-AKA' refer to clause 6.2.1.
- When using a key-generating EAP authentication method other than EAP-AKA', the key derivation of K_{AUSF} is based on the EAP-method credentials in the UE and AUSF and shall be done as shown in Figure I.2.3-1.

NOTE: For EAP authentication methods other than EAP-AKA', this key derivation replaces clauses 6.2.1 and 6.2.2 for the generation of K_{AUSF} .

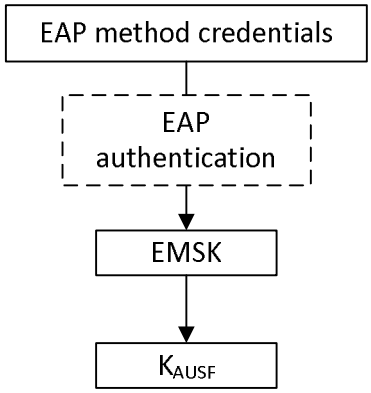


Figure I.2.3.1-1: K_{AUSF} derivation for key-generating EAP authentication methods other than EAP-AKA'

K_{AUSF} shall be derived by the AUSF and UE from the EMSK created by the EAP authentication as for EAP-AKA'.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the K_{AUSF} downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from K_{AUSF} (e.g. K_{SEAF}, K_{AMF}, K_{gNB} etc) apply without modification.

I.2.3.2 Credentials holder using AAA server for primary authentication

When running primary authentication towards an external Credentials holder using AAA server for authentication as specified in clause I.2.2.2 the derivation of K_{AUSF} is based on the EAP-method credentials in the UE and AAA-S and shall be done as shown in Figure I.2.3.2-1.

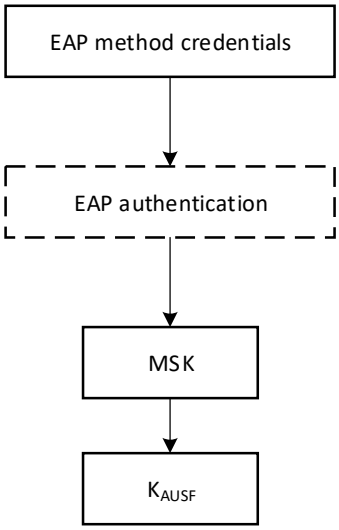


Figure I.2.3.2-1: K_{AUSF} derivation for primary authentication towards an external Credentials holder using AAA server

K_{AUSF} shall be derived by the AUSF and UE from the MSK derived during the EAP authentication as specified in clause I.2.2.2.1.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the K_{AUSF} downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from K_{AUSF} (e.g. K_{SEAF}, K_{AMF}, K_{gNB} etc) apply without modification.

I.2.4 Credentials Holder using AUSF and UDM for primary authentication

The 5G System architecture for SNPN with Credentials Holder using AUSF and UDM for primary authentication and authorization is described in clause 5.30.2.9.3 of TS 23.501 [2].

The requirements and procedures for primary authentication using AUSF and UDM as described in the present document apply, for 5G AKA, EAP-AKA', EAP-TLS or any other key-generating EAP method.

I.3 Serving network name for standalone non-public networks

I.3.1 General

The identification of standalone non-public networks uses Network Identifier (NID) in addition to PLMN ID. This means the definition of SN Id in clause 6.1.1.4.1 for the derivation of K_{SEAF} for all authentication methods, CK' and IK' for EAP-AKA', and K_{AUSF} and (X)RES* for 5G AKA needs modification for standalone non-public networks.

I.3.2 Definition of SN Id for standalone non-public networks

For standalone non-public networks, the SN Id (used in the input for various key/parameter derivations) identifies the serving SNPN.

It is defined as follows:

SN Id = PLMN ID:NID

and is specified in detail in TS 24.501 [35].

I.4 Modification of CAG ID list in the UE

The following requirements apply to NAS messages that modify the list of CAG IDs stored in the UE:

- the AMF shall only send such a NAS message once NAS security has been established; and
- the UE shall only modify its list of CAG IDs after successful integrity verification of the integrity protected NAS message requesting such a modification.

I.5 SUPI privacy for standalone non-public networks

The UE shall support SUPI privacy as defined in clause 6.12 with the following exception. When using an authentication method other than 5G AKA or EAP-AKA', the location of the functionality related to SUPI privacy in the UE is out of scope.

In scenarios where the EAP-method supports privacy, the UE may send an anonymous SUCI based on configuration.

Furthermore, the privacy considerations for EAP TLS (given in Annex B.2.1.2) should be taken into account when using an authentication method other than 5G AKA or EAP-AKA'.

I.6 Authentication in Public Network Integrated Non-Public Networks (PNI-NPN)

For public network integrated NPN (PNI-NPN), the primary authentication shall be performed with the public network as described in clause 6.1. Secondary authentication as described in clause 11 and slice-specific authentication as described in the main body can take place after a successful primary authentication.

I.7 Authorization aspects in SNPNs

I.7.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, service authorization as specified in clause 13.4.1.2 applies.

I.8 SEPP and interconnect related security procedures

I.8.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, clause 5.30.2.9.3 of TS 23.501 [2] states that the UE is not considered to be roaming, however SNPN and Credentials Holder communicate via SEPPs.

The following requirements and procedures related to SEPPs and interconnect security apply for SNPNs with Credentials Holder using AUSF and UDM for primary authentication:

- Requirements for Security Edge Protection Proxy (SEPP), clause 5.9.3.2
- Protection between SEPPs, clause 13.1.2.

NOTE: IPX providers are not expected to be used between SNPN and Credentials holder using AUSF and UDM for primary authentication.

I.9 Security of UE onboarding in SNPNs

I.9.1 General

Onboarding of UEs for SNPNs is specified in clause 5.30.2.10 of TS 23.501 [2].

Onboarding of UEs for SNPNs allows the UE to access an Onboarding Network (ONN) based on Default UE credentials for the purpose of provisioning the UE with SNPN credentials and any other necessary information. The Default UE credentials are pre-configured on the UE. Default UE credentials consist of credentials for primary authentication and optionally credentials for secondary authentication.

To provision SNPN credentials in a UE that is configured with Default UE credentials, the UE selects an SNPN as ONN and establishes a secure connection with that SNPN referred to as Onboarding SNPN (ON-SNPN).

The present clause specifies security of UE onboarding.

I.9.2 Authentication

I.9.2.1 Requirements

The primary authentication shall be performed before UE onboarding is allowed. For primary authentication, the UE shall use Default UE credentials for primary authentication. Credentials or means used to authenticate the UE based on Default UE credentials for primary authentication may be stored within the ON-SNPN or in a Default Credentials Server (DCS) that is external to the ON-SNPN.

The UE shall use Onboarding SUPI and Onboarding SUCI as specified in TS 24.501 [35] during Onboarding Registration.

I.9.2.2 Primary authentication without using DCS

When the primary authentication is performed between the UE and the ON-SNPN, any one of the existing authentication methods defined in the present document may be used, i.e., 5G AKA, EAP-AKA' or any other key-generating EAP authentication method (e.g., EAP-TLS).

The choice of primary authentication method used is left to the decision of the ON-SNPN.

Credentials required to authenticate the UE using default UE credentials for primary authentication, are provisioned at the AUSF or AUSF/UDM of the ON-SNPN. The provisioning of this information is out of scope of this document.

I.9.2.3 Primary authentication using DCS

When the primary authentication is performed between the UE and the DCS, the authentication requirements and procedures defined in clause I.2 for Credential Holder shall apply with the DCS taking the role of the Credentials Holder. When the DCS uses AAA Server for primary authentication, AUSF directly selects the NSSAAF as specified in 23.501 [2]. In this case, the UDM is not involved in the procedure defined in clause I.2.2.2.2, and the step 3 to step 5 shall be skipped. When 5G AKA or EAP-AKA' is used, the DCS shall act as a AUSF/UDM.

The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.

When the primary authentication is performed between the UE and the DCS via the AUSF using EAP-TTLS, Annex U can be used.

I.9.2.4 Secondary authentication

I.9.2.4.1 Secondary authentication using DCS

After successful primary authentication as described in I.9.2.2 (i.e. primary authentication without using DCS), upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials for secondary authentication, as described in clause 11.1.

NOTE: If both primary and secondary authentication use a certificate-based authentication method like e.g. EAP-TLS, and if required by the use case, it is possible to configure the UE with the same client certificates for Default UE credentials for secondary authentication as for the Default UE credentials for primary authentication.

I.9.2.4.2 Secondary authentication using DN-AAA

After successful primary authentication as described in I.9.2.2 or I.9.2.3, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with a DN-AAA server using Default UE credentials for secondary authentication, as described in clause 11.1.

Annex J (normative): SRVCC from 5G to UTRAN

J.1 SRVCC from NR to UTRAN

J.1.1 General

5G Single Radio Voice Call Continuity (SRVCC) is specified in 3GPP TS 23.216 [72], TS 23.501 [2] and TS 23.502 [8]. This clause specifies the security aspect to support SRVCC from 5G to UTRAN. SRVCC from UTRAN to 5G shall not be allowed. After a 5G to UTRAN SRVCC session has terminated, a UE shall run a successfully (re)authentication in 5GS before allowed to access 5G.

During SRVCC from 5G to UTRAN CS, the MSC server should never know the K_{AMF} nor should the K_{AMF} be revealed to an entity other than an AMF.

The AMF derives new key(s) to create a mapped SRVCC security context for the MSC server instead of sending K_{AMF} to the MSC server.

J.1.2 Procedure

As described in TS 23.216[72], there is no direct interface between the AMF in 5G and the MSC in UTRAN to support SRVCC, so the keys used to protect the SRVCC session once the UE is handed over to UTRAN are derived by MME based on security context mapping from 5G to E-UTRAN and then forwarded to the MSC during the HO procedure.

The procedure is initiated when the gNB wants to trigger a 5G SRVCC handover to UTRAN.

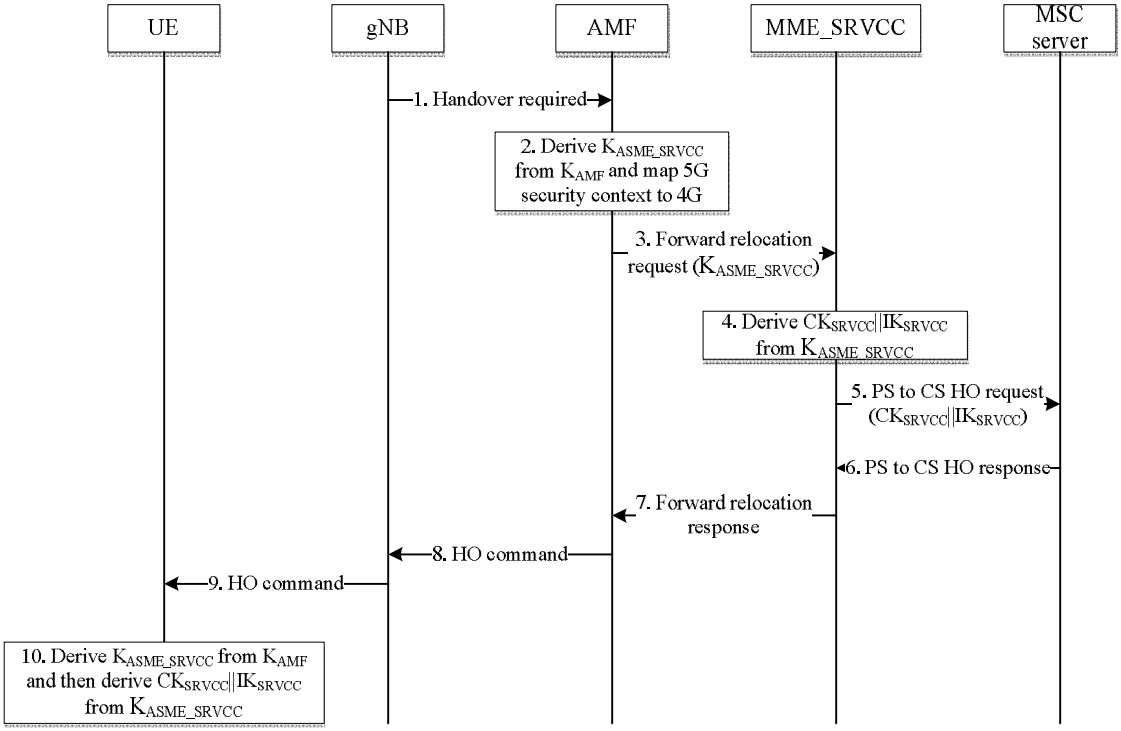


Figure J.1.2-1: Key derivation of 5G SRVCC from NR to UTRAN

1. The gNB sends Handover required message to the AMF.

2. The AMF shall derive a new K_{ASME_SRVCC} key using the K_{AMF} key and the current downlink 5G NAS COUNT of the current 5G security context as described in clause A.21. The AMF increases the downlink 5G NAS COUNT by one.

3. The AMF shall assign the value of ngKSI to the eKSI (maps ngKSI to eKSI) and shall transfer the new K_{ASME_SRVCC} key and the UE security capability to the MME_SRVCC via Forward relocation request message.

4. The MME_SRVCC shall derive the CK_{SRVCC}, IK_{SRVCC} based on the new K_{ASME_SRVCC} key as in clause A.12 in TS 33.401 [10] using a downlink NAS COUNT of zero.

5. The MME_SRVCC assigns the value of eKSI to KSI_{SRVCC} (maps eKSI to KSI_{SRVCC}) and transfers CK_{SRVCC}, IK_{SRVCC} with KSI_{SRVCC} and the UE security capability to the MSC server in PS to CS HO request message.

6. The MSC server sends the PS to CS HO response message to the MME_SRVCC.

7. The MME_SRVCC sends the Forward relocation response message to the AMF.

8. The AMF sends the HO command to the gNB, in which the AMF shall include the 4 LSBs of the downlink NAS COUNT used to calculate K_{ASME_SRVCC}.

9. The gNB sends the HO command to the UE, in which the gNB shall include the 4 LSB of the downlink NAS COUNT received from the AMF.

10. When the UE receives the message, the UE shall derive the new K_{ASME_SRVCC} key as described in Annex A.21 using the K_{AMF} key and the downlink 5G NAS COUNT estimated from the 4 LSB received form the AMF. The UE shall further derive CK_{SRVCC}, IK_{SRVCC} based on the new K_{ASME_SRVCC} key as described in the clause A.12 in TS 33.401 [10] using a downlink NAS COUNT of zero. The UE shall identify the CK_{SRVCC} and IK_{SRVCC} from eKSI (= ngKSI) as the MME_SRVCC does.

If the SRVCC handover is not completed successfully, the new mapped CK_{SRVCC}, IK_{SRVCC} and KSI_{SRVCC} cannot be used. In this case, the MSC server enhanced for SRVCC shall delete the newly mapped SRVCC security context for the UE, including CK_{SRVCC}, IK_{SRVCC} and KSI_{SRVCC}.

J.2 Emergency call in SRVCC from NR to UTRAN

J.2.1 General

IMS Emergency Sessions can be authenticated or unauthenticated depending on the serving network policy (or regulatory requirements) if unauthenticated IMS Emergency Sessions are allowed. Any behaviour not explicitly specified as being special to IMS Emergency Sessions is handled in accordance to normal procedures.

J.2.2 Procedure

When the SVRCC is for an emergency session, the security procedure in clause J.1.2 is applied.

However, in the case when the SRVCC is for an unauthenticated emergency session, since the derived keys have no ability to affect the output of the NULL algorithms, call set up needs to continue even though the network and the UE derive different keys.

Annex K (normative): Security for 5GLAN services

K.1 General

5GLAN services are described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [8].

K.2 Authentication and authorization

For authentication and authorization of a UE in 5G LAN communication, the secondary authentication procedures between UE and external data networks via the 5G Network as described in clause 11 shall apply.

K.3 Handling of UP security policy

To reduce incremental complexity added by security, all PDU sessions associated with a specific 5G LAN group should have the same UP security policy.

Annex L (normative): Security for TSC service

L.1 General

The 5G TSC service is described in 3GPP TS 23.501 [2]. It allows the 5G System to be integrated transparently as a bridge in an IEEE TSN network [75], where the 5GS system acts as one or more TSN Bridges of a TSN network.

L.2 Access security for a 5GS TSC-enabled UE

A 5GS TSC-enabled UE accesses the 5G network as described in this document except where differences are provided in the following clauses.

L.3 Protection of user plane data in TSC including (g)PTP control messages in bridge mode

After the 5GS TSC-enabled UE is authenticated and data connection is set up, any data received from a TSC bridge or another 5GS TSC-enabled UE shall be transported between DS-TT (in the UE) and NW-TT (in the UPF) in a protected way using the mechanisms for UP security as described in clause 6.6.

The UP security enforcement information shall be set to "required" for data transferred from gNB to a 5GS TSC-enabled UE. This is also applicable to the (g)PTP messages sent in the user plane.

L.4 Exposure of time synchronisation

Any AF that has knowledge of deterministic application requirements is able to request TSC services from the 5GS by interfacing with NEF, and as authorized, can be notified of pertinent network events. The security solution as described in clause 12 shall apply.

Annex M (normative): Security for Integrated Access and Backhaul (IAB)

M.1 General

This Annex provides the security procedures applied to NR IAB architecture and functional entities for supporting wireless backhauling of NR base stations.

The overall stage 2 description for IAB architecture and functional entities are described in 3GPP TS 23.501 [2] and 3GPP TS 38.401 [78].

The security requirements and security procedures applied to IAB in EN-DC architecture are defined in both TS 33.401 [10] and in the present document. The security requirements and security procedures between the IAB-node and the MeNB (i.e., when the IAB-node connects via E-UTRA to a MeNB), are defined in TS 33.401 [10] and between the IAB-node and the SgNB (F1 interface) are defined in this clause.

M.2 Security requirements and features

M.2.1 Requirements on the IAB-node (IAB-UE)

The IAB-node (IAB-UE) shall support ciphering, integrity protection and replay protection of NAS-signalling between the IAB-node (IAB-UE) and the 5GC supporting IAB architecture.

The IAB-node (IAB-UE) shall support ciphering, integrity protection and replay protection of RRC-signalling between the IAB-node (IAB-UE) and the IAB donor.

Mutual authentication between the IAB-node (IAB-UE) and the 5GC supporting IAB architecture shall be supported.

M.2.2 Requirements on the IAB donor

The IAB donor shall support ciphering, integrity protection and replay protection of RRC-signalling between the IAB donor and the IAB-node (IAB-UE).

M.2.3 Requirements on the 5GC supporting IAB architecture

The 5GC supporting IAB architecture shall support ciphering, integrity protection and replay protection of NAS-signalling between the 5GC supporting IAB architecture and the IAB-node (IAB-UE).

Mutual authentication between the 5GC supporting IAB architecture and the IAB-node (IAB-UE) shall be supported.

The 5GC shall decide whether the IAB-node is authorized to operate as IAB-node (gNB-DU).

M.2.4 Requirements for secure environment

The security requirements for secure environment of the IAB-node (gNB-DU) and the IAB-donor are described in clause 5.3.8 of this document.

M.2.5 Requirements on the F1 interface

The security requirements on the F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU are described in clause 5.3.9 of this document.

M.3 IAB-node Integration Procedure

M.3.1 General

IAB-node, consists of a UE function (referred to as IAB-UE) and gNB-DU function [2]. IAB integration procedure consists of 3 phases detailed in TS 38.401 [78].

Phase-1: IAB-UE part setup:

The IAB-UE performs registration procedure to the network as a UE as described in TS 23.501 [2] and TS 23.502 [8] in order to register to the 5GC and consequently, the NAS and AS security are established between the IAB-node and 5GC.

Phase-2: BH RLC channel establishment and routing update:

The BH RLC channels and the BAP layer are established and configured in the IAB-node by the IAB-donor using the secured RRC signalling to support routing between the IAB-node and the IAB-donor.

Phase-3: gNB -DU part setup:

F1 security establishment for IAB is performed over the RLC channel.

The Phase-1 results in IAB-UE registration and consequently, AS security establishment between the IAB donor and IAB-node, Phase-2 results in configuration of the IAB-node securely using the established AS security and Phase-3 results in the establishment of secure F1 interface between the IAB-donor and IAB-node.

M.3.2 Authentication and Authorization of IAB-node (Phase-1)

The IAB-UE function shall behave as a UE, and shall reuse the UE procedures specified in this document for the primary authentication (see clause 6), key derivation and distribution scheme, subscription credential(s) storage requirements, NAS security and AS security.

NOTE 1: For isolated deployment scenarios, Annex B describes how additional EAP methods can be used.

NOTE 2: Storage of subscription credentials for EAP AKA' and 5G AKA is described in clause 6 of the present document.

Authorization of IAB-nodes shall be performed by the 5G core network supporting IAB architecture as described in TS 23.501 [2].

M.3.3 Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (Phase-3)

M.3.3.1 General

The following clause applies to F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU.

M.3.3.2 Security mechanisms for the F1 interface

The F1 interface connects the IAB-node (gNB-DU) to the IAB-donor-CU. It consists of the F1-C for control plane and the F1-U for the user plane.

F1 security for IAB is established using the security mechanisms for the F1 interface as specified in clause 9.8.2 of the present document, with IAB node taking the role of gNB-DU and IAB-donor-CU taking the role of gNB-CU.

In addition to the security mechanisms specified in clause 9.8.2 of the present document for the F1 interface, the IKEv2 Pre-shared Secret Key (PSK) authentication shall be supported. When IKEv2 performs a PSK authentication, in the IKE_AUTH request message, the IAB node shall set the ID type to ID_KEY-ID and set its value to PSK ID.

NOTE 1: The PSK and PSK ID (for IKEv2 PSK authentication) can be preconfigured at the IAB node and IAB donor. Pre-configuration of the PSK(s) is out of the scope of the present document.

Additionally, to support a flexible plug and play of IAB-node and IAB-donor without a pre-configuration of the PSK(s), dynamic PSK computation for IKEv2 PSK authentication may also be supported. When dynamic PSK is used, the IAB-node and the IAB-donor shall calculate the PSK (K_{IAB}) as specified in the Annex A.23 of this document. The IAB-donor shall uniquely identify the IAB-node's security context (K_{gNB}) using the IAB-node DU IP address. The IAB-donor shall use K_{IAB} as PSK for IKEv2 between IAB-node and the IAB-donor. K_{IAB} is stored in the IAB-node and in the IAB-donor. This key K_{IAB} and the IPsec SA cryptographic keys are taken into use with the establishment of IPsec Security Association (SA) between the IAB-node and the IAB-donor. K_{IAB} remains valid as long as the IAB-node is connected to the IAB-donor or until the IAB-node is re-authenticated. The KIAB is associated with the IAB-node DU IP address in the IAB-donor. In the IKE_AUTH request message, the IAB node shall set the ID type to ID_IPV4_ADDR/ID_IPV6_ADDR and set its value to the IAB-node DU IP address in the Idi payload. In case of CP-UP separation of IAB-donor-CU (IAB-donor-CU contains IAB-donor-CU-CP and IAB-donor-CU-UP that use different IP address) then, IAB-donor-CU-CP and IAB-node DU shall generate $K_{IAB\text{-}CU\text{-}CP}$ and $K_{IAB\text{-}CU\text{-}UP}$ as specified in the Annex A.23 of this document. The key $K_{IAB\text{-}CU\text{-}CP}$ shall be used for establishment of secure F1 interface between the IAB-node DU and IAB-donor-CU-CP. The IAB-donor-CU-CP shall provide $K_{IAB\text{-}CU\text{-}UP}$ to the IAB-donor-CU-UP via E1 interface and $K_{IAB\text{-}CU\text{-}UP}$ shall be used for establishment of secure F1 interface between the IAB-node DU and IAB-donor-CU-UP.

NOTE 2: K_{IAB} is used as the PSK for IKEv2 authentication, the interface between the IAB-donor-CU and the SEG to provision the key K_{IAB} in the SEG is implementation specific and out of the scope of the present document.

M.4 Protection of management traffic between IAB-node and OAM

If management traffic uses the user plane via PDU session, it shall be protected using the user plane security mechanism as specified in clause 6.6.

M.5 IAB inter-CU topology adaptation and backhaul RLF recovery procedure

In case of the inter-CU migration as specified in TS 38.401 [78], the IAB-MT is migrated from a source IAB-donor-CU to a target IAB-donor-CU. The migrating IAB-node becomes a boundary IAB-node since its IAB-DU retains F1AP with the source IAB-donor-CU after its IAB-MT obtains RRC connectivity with the target IAB-donor-CU (c.f. TS 38.401 [78]).

In case IPsec tunnel mode is used for F1 interface protection, the migrating/descendant/recovery IAB-node may use MOBIKE (IETF RFC 4555 [110]) to migrate the IPsec tunnel to the new IP outer addresses as specified in TS 38.401 [78].

In IPsec transport mode for the non-dynamic PSK case, the establishment of the IPsec SAs follows the procedures in Annex M.3.3.2 of the present document. In IPsec transport mode for the dynamic PSK case, the establishment of the IPsec SAs may be performed by initiating new IKEv2 procedure using the stored K_{IAB} associated with the old IP address as the PSK for the corresponding new IP address. The identical mapping between the old IP address with the new IP address between the IAB-node and the IAB-donor-CU is performed using the old IP address present in the IDi payload and the new IP address in the IP header of the IKEv2_AUTH request message. In case of multiple IP addresses for IAB-node, the IKEv2 procedure is performed for each IP address. Once the IKEv2 authentication is successful, the K_{IAB} is associated with the new IAB-node DU IP address in the IAB-donor.

Annex N (normative): Security for URLLC services

N.1 General

This clause describes the security requirements, procedures and handling for Ultra-Reliable Low-Latency Communication (URLLC). The procedures and handling include the enforcing the security policy for data transmission. The general features for URLLC are described in 23.501 [2], 38.300 [52] and TS 23.502 [8].

N.2 Security support on redundant transmission

N.2.1 Redundant user plane paths based on dual connectivity

N.2.1.1 Introduction

In order to support URLLC services, a UE sets up two redundant PDU sessions over the 5G network, such that the 5GS sets up the user plane paths of the two redundant PDU Sessions to be disjoint as described in clause 5.33 in TS 23.501 [2]. However, NG-RAN may realize redundant user plane resources for the two PDU sessions with a single NG-RAN node, or by Dual Connectivity with two NG-RAN nodes, i.e. one PDU session spans from the UE via the MN to a first UPF and the second PDU session spans from the same UE via the SN to a second UPF. Based on the two PDU sessions, the redundant data sent between the UE and the DN takes different paths in the 3GPP network.

The security aspects for redundant PDU sessions transmission by Dual Connectivity are based on the security procedures and description described in clause 6.10 of the present specification. This clause only describes the additional security features.

N.2.2.2 Security policy aspects

When dual connectivity is used for redundant transmission, both of the two PDU sessions are initially established via the MN. The SMF(s) shall provide a UP security policy for each of the two PDU sessions to the MN during the PDU session establishment procedure as described in clause 6.6.1. The UP security policy from the SMF(s) for the two PDU sessions used for redundant data transmission shall have the same setting for encryption and for integrity protection. The network (UDM and/or SMF) shall ensure that all the redundant PDU sessions based on the information sent by the UE as described in TS 23.501 [2] shall have same UP security policy setting.

The MN shall be preconfigured or shall have access to the supported security capabilities in the available SN(s), (i.e. to whether UP integrity protection is supported in the SN or not). The MN shall take the received UP security policy into account when selecting the SN.

MN shall ensure that the first and the redundant PDU sessions shall have the same UP security activation status. If the "Preferred" option of the UP security policy is not allowed to be used for URLLC service at the SMF or UDM, which means the SMF or UDM can guaranteethe UP security policy for the first and the redundant PDU sessions are the same and only contains "Not needed", or "Required", then the MN shall forward the UP security policy to the SN as described in clause 6.10.

If the "Preferred" option of the UP security policy is allowed to be used for URLLC services, the following enhancements for the mechanism as described in clause 6.10 for Dual Connectivity shall be applied:

- The MN shall make the decision on UP encryption protection and integrity protection according to the UP security policy for these two redundant data transmissions. The MN shall store the applied UP security activation status used for the DRB's established for the first PDU session between the MN and the UE. Then, the MN shall provide the UP security activation status applied for the first PDU session to the SN, when offloading the DRB's for the second PDU session to the SN.

- The SN shall use the UP security activation status received from the MN to activate the UP security for the DRB's established for the redundant PDU session between the SN and the UE.

N.2.2 Redundant transmission on N3/N9 interfaces

If the user data redundancy is fulfilled by means of two duplicated N3 tunnels, the redundant packets will be transferred between UPF and RAN via two independent N3 tunnels, which are associated with a single PDU Session, over different transport layer path to enhance the reliability of service.

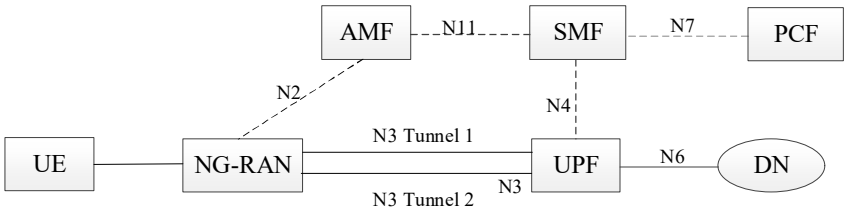


Figure N.2.2-1: Redundant transmission with two N3 tunnels between the UPF and a single NG-RAN node

In order to protect the redundant traffic on the N3 reference point, the current mechanism defined in clause 9.3 of the present document shall be reused. The added path for redundancy shall provide equal level of security compared to single path.

In case two N9 tunnels are involved to fulfil the redundancy for one NG-RAN, the security mechanism defined in clause 9.9 shall be used for protecting the redundant data transferring via two N9 tunnels as described above.

Annex O (Informative): Authentication for non-5G capable devices behind residential gateways

O.1 General

This annex describes the authentication procedure, using EAP-TLS as an example, for Non-5G Capable (N5GC) devices behind Residential Gateways (RGs) in private networks or in isolated deployment scenarios (i.e., roaming is not considered) with wireline access. The registration procedure of N5GC devices behind Cable RGs is described in clause 4.10a of TS 23.316 [79].

O.2 Baseline for using non-5G capable devices with 5GC

N5GC devices lack some key 5G capabilities, including NAS and the derivation of 5G key hierarchy. Those devices exist in wireline networks and need to be able to access the converged 5G core. The authentication of N5GC devices can be based on additional EAP methods other than EAP-AKA'. The procedure in O.3 uses EAP-TLS as in Annex B as an example, but it differs from the Annex B in the following:

a) the W-AGF creates the registration request on behalf of the N5GC device,

b) 5G related parameters (including ngKSI and ABBA) are not sent to the N5GC device. When received from the AMF, these parameters are ignored by the W-AGF, and

c) Neither the N5GC device nor the AUSF derives any 5G related keys after EAP authentication.

O.3 Authentication procedure

Figure O.3-1 shows the details of the authentication procedure as part of the initial registration procedure specified in clause 4.10a of TS 23.316 [79] following the principles listed in clause O.2. It uses EAP-TLS as an example, but other EAP methods can also be supported. The W-AGF acts on behalf of the N5GC device during the registration process. The link between the N5GC device and the RG, and between the RG and the W-AGF can be any data link (L2) that supports EAP encapsulation.

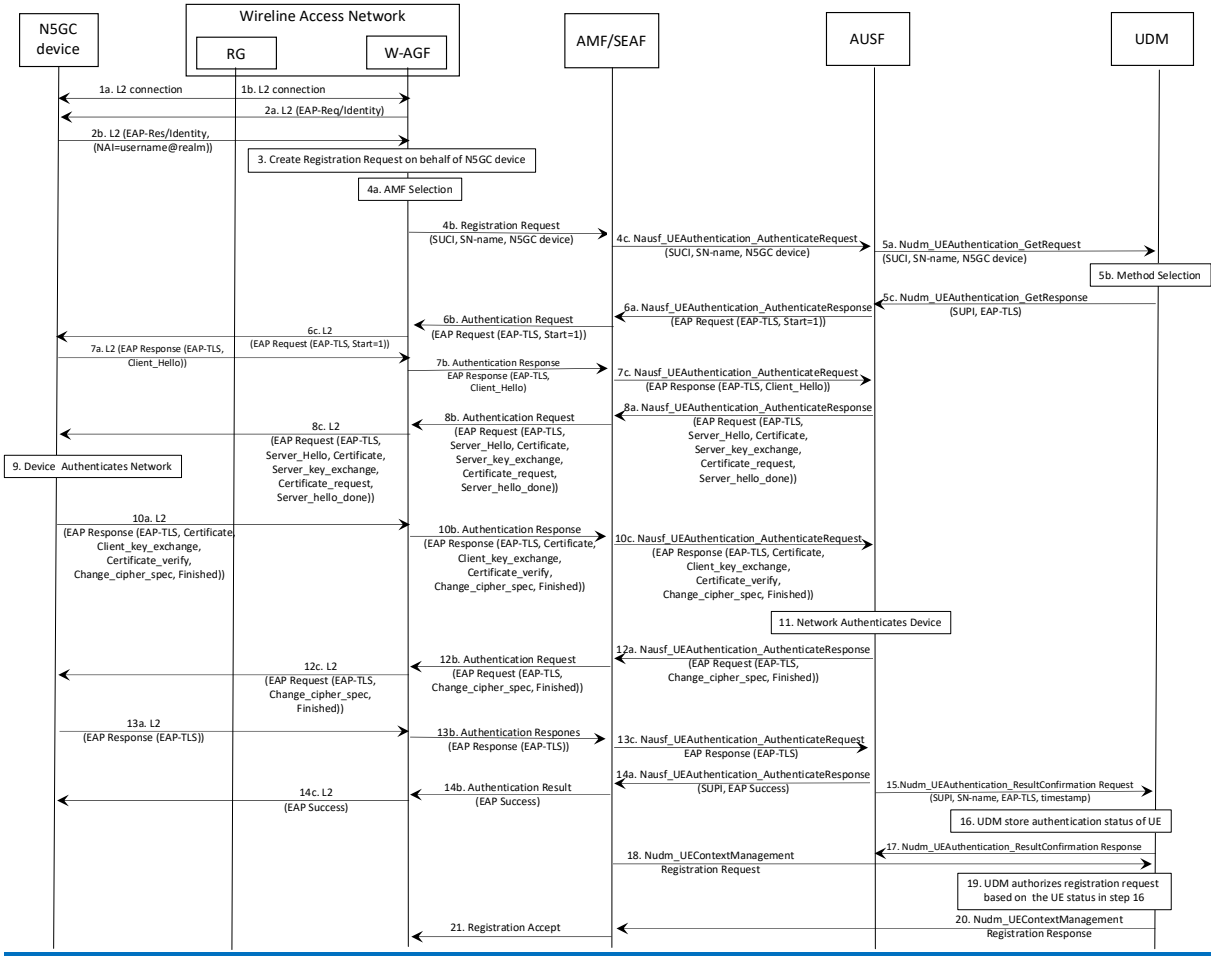


Figure O.3-1: Registration and authentication of a non-5G capable device to the 5GC

In the following, the procedure for registration and authentication of an N5GC device to the 5GC is described:

1. The N5GC device connects to the W-AGF via a RG which is configured as a layer 2 bridge. The W-AGF is associated with a 5GC and acts on behalf of the N5GC device during its registration process.

2a. The W-AGF initiates the EAP authentication procedure by sending an EAP request/Identity to the N5GC device via the RG, which acts as an L2 bridge device and forwards the ethernet frame to the N5GC device. The EAP message is encapsualted inside an L2 frame (e.g., EAPOL).

2b. In response, the N5GC device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

NOTE 1: If TLS subscription identifier privacy protection is supported , as in "Section 2.1.4. Privacy" of RFC 5216 [38] for TLS 1.2 or in RFC 8446 [60] for TLS 1.3, the "username" part must be is either omitted or "anonymous".

3. The W-AGF creates a registration request on behalf of the N5GC device with an indication that the registration is on behalf of an N5GC device. The SUPI of the N5GC device is the NAI as received from the device, and the W-AGF constructs the SUCI from this SUPI using the NULL scheme.

4a. The W-AGF selects the AMF/SEAF.

4b. The W-AGF sends to the AMF/SEAF a registration request on behalf of the N5GC device. The registration request includes the NAI SUCI, wireline network name if available, and a device capability indicator (e.g., the device is non-5G capable).

4c. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf_UEAuthentication_Authenticate Request message to the AUSF. It contains the SUCI of the N5GC device, and an indicator that the request is on behalf of the N5GC device.

5a. The AUSF sends a Nudm_UEAuthentication_Get Request to the UDM. It contains the SUCI of the N5GC device and the N5GC device indicator.

5b. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method, e.g., EAP-TLS, based on the SUPI. When the "username" part of the SUPI is "anonymous" or omitted, the UDM may select an authentication method based on the “realm” part of the SUPI, the N5GC device indicator, a combination of the "realm" part and the N5GC device indicator, or the UDM local policy.

5c. The UDM sends a Nudm_UEAuthentication_Get Response to the AUSF, which contains the SUPI of the N5GC device and an indicator of the selected authentication method, e.g., EAP-TLS.

NOTE 2: Steps 6a-14c describe the exchange of EAP-TLS between the AUSF and the N5GC device, based on TLS 1.2 without subscription identifier privacy protection. If the operator determines to provide subscription identifier privacy for the N5GC in TLS layer, the EAP TLS server needs to support privacy either inherently (e.g., in TLS 1.3) or via separate privacy option (e.g., in TLS 1.2). When TLS 1.2 is used, the N5GC device would need to behave as described in "Section 2.1.4. Privacy" of RFC 5216 [38] where instead of sending the client certificate in cleartext over the air, the N5GC device sends TLS certificate (no cert) during the first TLS handshake and sends TLS certificate (client certificate) during the second TLS handshake within the TLS session negotiated form the first TLS handshake.

6a. The AUSF starts EAP-TLS by sending to the AMF/SEAF a Nausf_UEAuthentication_Authenticate Response message containing an EAP-Request message of EAP-type=EAP-TLS with the Start (S) bit set, denoted as EAP-Request/EAP-TLS [TLS start].

6b. The AMF/SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the W-AGF.

6c. After receiving the EAP-Request/EAP-TLS [TLS start] message from AMF/SEAF, the W-AGF forwards the EAP-Request/EAP-TLS [TLS start] message to the N5GC device in an L2 message, leaving out the ABBA and ngKSI parameters.

7a. After receiving the EAP-Request/EAP-TLS [TLS start] message from the W-AGF, the N5GC device replies to the W-AGF with an EAP-Response/EAP-TLS message whose data field encapsulates a TLS client_hello message. Such EAP-Response message, denoted as EAP-Response/EAP-TLS [client_hello], is encapsulated in an L2 message.

7b. The W-AGF forwards the EAP-Response/EAP-TLS [client_hello] to the AMF/SEAF in an Authentication Response message.

7c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [client_hello] message to the AUSF in a Nausf_UEAuthentication_Authenticate Request message.

8a. The AUSF replies to the AMF/SEAF with EAP-Request/EAP-TLS message whose data field encapsulates a TLS server_hello message, a TLS server certificate message, a TLS server_key_exchange message, a TLS client certificate_request message, and a TLS server_hello_done message. Such EAP-Request message, denoted as EAP-Request/EAP-TLS [server_hello], is encapsulated in a Nausf_UEAuthentication_Authenticate Response message.

8b. The AMF/SEAF forwards the EAP-Request/EAP-TLS [server_hello] message to the W-AGF in an Authentication Request message.

8c. The W-AGF forwards the EAP-Request/EAP-TLS [server_hello] to the N5GC device in an L2 message.

9. The N5GC device authenticates the AUSF by validating the server certificate included in the EAP-Request/EAP-TLS [server_hello] message received in step 8c. The N5GC device needs to be provisioned with certificates of a trust anchor to validate the AUSF server certificate. In addition, the N5GC device also needs to be provisioned with its own client certificate.

10a. If the TLS server authentication is successful, then the N5GC device replies to the W-AGF with EAP-Response/EAP-TLS in an L2 message. The data field of the EAP-Response/EAP-TLS message contains a TLS client certificate message, a TLS client_key_exchange message, a TLS certificate_verify message, a TLS

change_cipher_spec message, and TLS finished message. This EAP-Response message is denoted as EAP-Response/EAP-TLS [client_certificate].

10b. The W-AGF forwards to the AMF/SEAF the EAP-Response/EAP-TLS [client_certificate] in an Authentication Response message.

10c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [client_certificate] message to the AUSF in a Nausf_UEAuthentication_Authenticate Request message.

11. The AUSF authenticates the N5GC device by verifying the client certificate received in the EAP-Response/EAP-TLS [client_certificate] message. Among other validations, the AUSF verifies that the client certificate is issued by a certificate authority trusted by the AUSF. If the client certificate is verified successfully, the AUSF continues to step 12a. Otherwise the AUSF returns an EAP-failure message. The AUSF needs to be provisioned with certificates of trust anchor to verify client certificates.

12a. The AUSF sends to the AMF/SEAF an EAP-Request/EAP-TLS message with its data field encapsulating a TLS change_cipher_spec message and a TLS server finished. This EAP-Request message, denoted as EAP-Request/EAP-TLS [server_finished], is encapsulated in a Nausf_UEAuthentication_Authenticate Response message.

12b. The AMF/SEAF forwards EAP-Request/EAP-TLS [server_finished] message to the W-AGF in an Authentication Request message.

12c. The W-AGF forwards EAP-Request/EAP-TLS [server_finished] message to the N5GC device in an L2 message.

13a. The N5GC sends to the W-AGF an EAP-Response/EAP-TLS message with its data field set to empty, denoted as EAP-Response/EAP-TLS [empty], in an L2 message

13b. The W-AGF forwards to the AMF/SEAF the EAP-Response/EAP-TLS [empty] message in an Authentication Response message.

13c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [empty] message to the AUSF in a Nausf_UEAuthentication_Authenticate Request message.

14a. The AUSF sends to the AMF/SEAF an EAP-Success message along with the SUPI in a Nausf_UEAuthentication_Authenticate Response message. If the SUPI received from the UDM in step 5c is anonymous, the AUSF derives the SUPI from the client identifier in the TLS client certificate. AUSF does not perform the derivation of K_{AUSF} nor K_{SEAF} based on the indicator of an N5GC device received in step 4c, nor sends K_{SEAF} to AMF/SEAF.

NOTE 2a: It is left to implementation if the AUSF verifies that the SUPI derived from the client certificate belongs to a valid susbcription in the network and returns an EAP-failure message if there is a miss-match.

14b. The AMF/SEAF forwards to the W-AGF the EAP-Success message in an Authentication Result message or a Security Mode Command message.

14c. The W-AGF forwards to the N5GC device the EAP-Success message in an L2 message, and the authentication procedure is finished.

NOTE 3: Neither the AUSF nor the N5GC device performs further 5G related key derivation from EMSK, since neither 5G AS nor 5G NAS security is used in this setting.

15. The AUSF sends a UDM_Nudm_UEAuthentication_ResultConfirmation Request message to the UDM, including the SUPI obtained from the TLS client certificate, SN-name, the authentication method (i.e., EAP-TLS), the authentication result, and a timestamp.

16. The UDM stores the authentication result accordingly.

17. The UDM sends a UDM_Nudm_UEAuthentication_ResultConfirmation Response message to the AUSF.

18. The AMF sends a Nudm_UEContextManagement_Registration Request message to the UDM.

19. The UDM authorizes the registration request based on authentication result stored in step 16 and other information (e.g., UE subscription profile).

20. The UDM sends a Nudm_UEContextManagement_Registration Response message to the AMF.

21. The AMF sends Registration Accept message to the W-AGF

Annex P (informative): Security aspects of DNS and ICMP

P.1 General

This annex specifies security measures to protect DNS and ICMP messages. These security measures are intended when integrity protection over the user plane can not be used.

P.2 Security aspects of DNS

It is recommended that the UE and DNS server(s) support DNS over (D)TLS as specified in RFC 7858 [83] and RFC 8310 [84]. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The UE can be pre-configured with the DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number, etc.), or the core network can configure the DNS server security information to the UE.

NOTE: The use of DNS over (D)TLS with DNS server(s) that are deployed outside the 3GPP network is outside the scope of this document.

When DNS over (D)TLS is used, a TLS cipher suite that supports integrity protection needs to be negotiated.

P.3 Security aspects of ICMP

ICMP (Internet Control Message Protocol) is part of the internet protocol (IP) suite. The lack of security in ICMP may be exploited to launch further attacks on the 3GPP system. To mitigate such attacks, it is recommended that the use of ICMP is restricted in the UE and the UPF (e.g., by default, use of ICMP is not allowed). In scenarios where the use of ICMP is required, it is recommended that one or more of following mitigations be enforced:

- Disable the UE from responding to ICMP requests received over 3GPP network interface(s).
- Install IP filter(s) at the UPF in order to block ICMP messages. This filter can be activated either on a per N4 Session basis or on a UPF basis. For ICMPv6, the recommendations in RFC 4890 [85] can be used for filtering ICMPv6 messages.
- Limit the maximum size of ICMP messages (e.g., to 64 bytes). Any ICMP messages that are greater than this limit needs to be dropped by the UE as well as by the UPF.

Annex Q (informative): Security and privacy in 5G system location services

Q.1 General

For security and privacy in 5GS LCS (5G System Location Services), the mechanisms defined in TS 23.273 [86] and TS 38.305 [87] apply.

Annex R (informative): Authorization aspects in communication models for NF/NF services interaction

TS 23.501 [2], Annex E, summarizes the different communication models that NF and NF services can use to interact with each other.

Figures R-1 and R-2 provide an overview of the authorization aspects in the different models, as described in detail in clause 13.

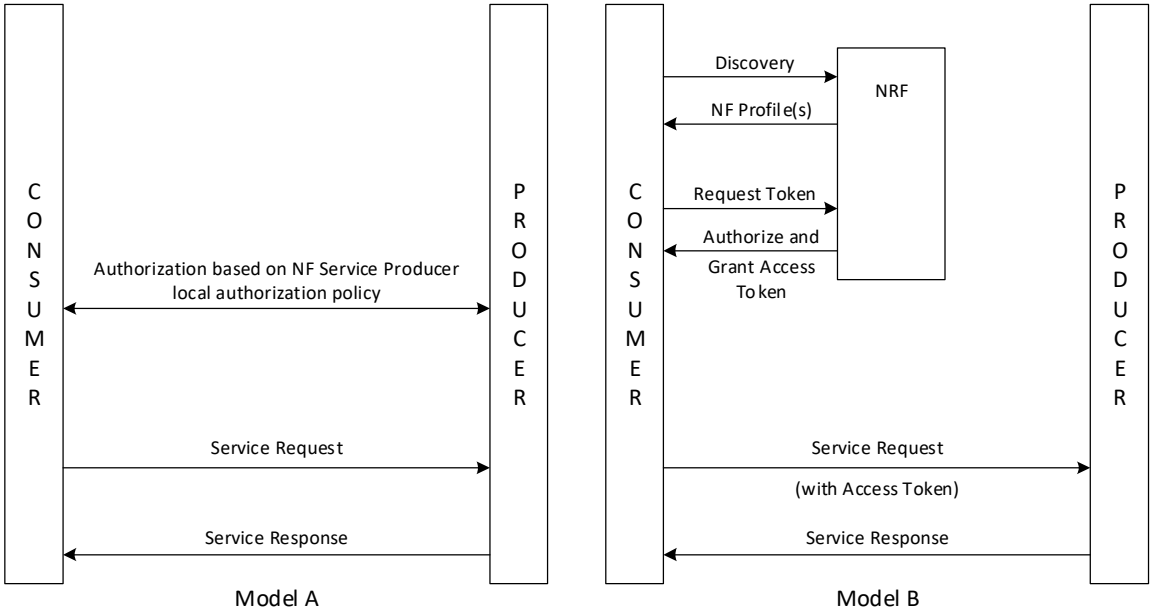


Figure R-1: Illustration of authorization aspects in direct deployment models

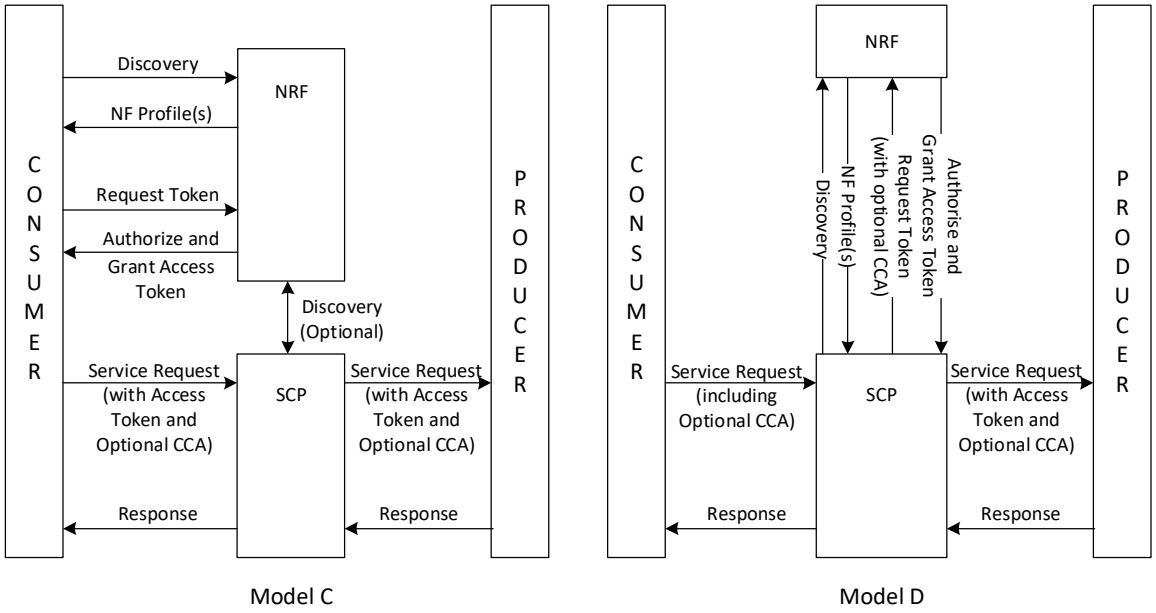


Figure R-2: Illustration of authorization aspects in indirect deployment models

Annex S (normative): Support for Non-seamless WLAN offload (NSWO) in 5GS

S.1 Introduction

Non-seamless WLAN offload (NSWO) is an optional capability of a UE supporting WLAN radio access. A UE supporting non-seamless WLAN offload may, while connected to WLAN access, route specific IP flows via the WLAN access without traversing the 3GPP core network.

The present annex specifies the support for authentication for NSWO in 5GS (5G NSWO).

S.2 General

5G NSWO shall use EAP-AKA', as specified in RFC 5448 [12], for authentication. The EAP-AKA' implementations shall comply with the EAP-AKA' profile specified in Annex F of the present document.

A new network function, called NSWOF, is introduced to support authentication for NSWO in 5GS. The NSWOF interfaces to the WLAN access network using SWa interface and interfaces to the AUSF using Service Based Interface (SBI).

S.3 Authentication procedure

S.3.1 5G NSWO co-existence with EPS NSWO

An HPLMN that supports 5G NWSO and wants the UE to use 5G NSWO shall configure the UE to use 5G NSWO. This configuration shall be either on the USIM or ME, with configuration on the USIM taking precedence over the ME.

A UE that supports 5G NSWO and is configured to use 5G NSWO shall always use 5G NSWO as described in clause S.3.2 (i.e., it shall not use EPS NSWO defined in TS 23.402[97]). Otherwise, the UE may use EPS NSWO (e.g., UE does not support 5G NSWO or not configured to use 5G NSWO).

NOTE: Such a configuration ensures that the UE supporting 5G NSWO cannot be downgraded to use EPS NSWO.

The network may support both 5G NSWO and EPS NSWO. In such a case, the routing of the AAA messages is determined by the network based on the realm part of the UE Identity (e.g., realm contains epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org (EPS NSWO) or 5gc-nswo.mnc<MNC>.mcc<MCC>.3gppnetwork.org (5G NSWO)). Which entities in the network perform this routing decision is dependent on the network configuration.

S.3.2 5G NSWO procedures

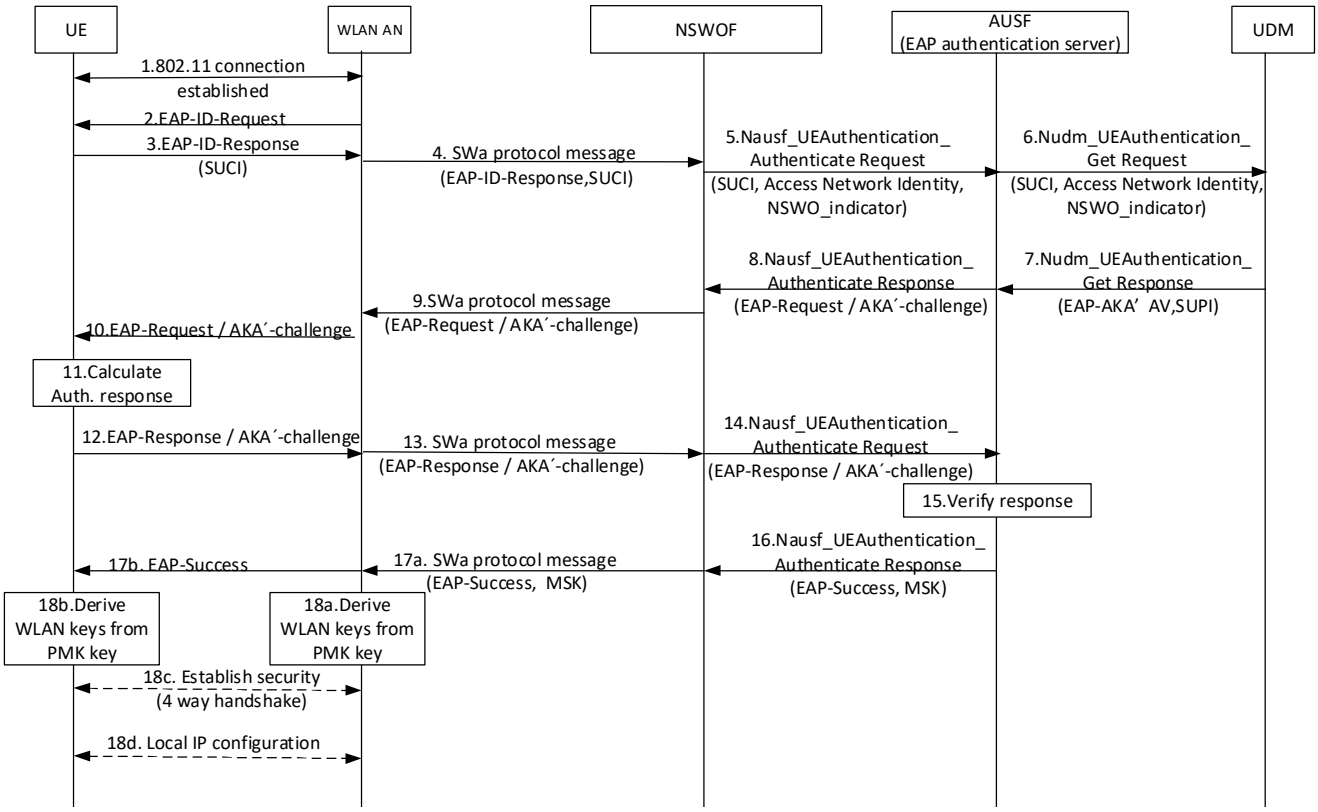


Figure: S.3-1: Authentication procedure for NSWO in 5GS

1. The UE establishes a WLAN connection between the UE and the WLAN Access Network (AN), using procedures specified in IEEE 802.11[80].

2. The WLAN AN sends an EAP Identity/Request to the UE.

3. The UE sends an EAP Response/Identity message. If the UE determines to use the NSWO service, the UE shall use the SUCI in NAI format (as specified in TS 23.003 [19], clause 28.7.12 and clause 28.7.9.2) as its identity irrespective of whether SUPI Type configured on the USIM is IMSI or NAI. If the SUPI Type configured on the USIM is IMSI, the UE shall construct the SUCI in NAI format with username containing the encrypted MSIN and the realm part containing the MCC/MNC.

4. The EAP Response/Identity message shall be routed over the SWa interface towards the NSWOF based on the realm part of the SUCI.

NOTE 1: NSWOF acts as SBI/AAA proxy between the AUSF and the WLAN Access Network.

5. The NSWOF shall send the message Nausf_UEAuthentication_Authenticate Request with SUCI, Access Network Identity and NSWO indicator towards the AUSF. NSWO_indicator is used to indicate to the AUSF that the authentication request is for Non-seamless WLAN offload purposes. The NSWOF shall set the Access Network Identity to "5G:NSWO".

6. Based on the NSWO_indicator, the AUSF (acting as the EAP authentication server) shall send a Nudm_UEAuthentication_Get Request to the UDM, including SUCI and the Access Network Identity and NSWO indicator.

7. Upon reception of the Nudm_UEAuthentication_Get Request, the UDM shall invoke SIDF. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. Based on the NSWO indicator and if NSWO is allowed based on the UE subscription data, the UDM/ARPF shall select the EAP-AKA´ authentication method and generate an authentication vector using the Access Network Identity as the KDF input parameter. The UDM

shall include the EAP-AKA' authentication vector (RAND, AUTN, XRES, CK´ and IK´) and may include SUPI to AUSF in a Nudm_UEAuthentication_Get Response message.

8. The AUSF shall store XRES for future verification. The AUSF shall send the EAP-Request/AKA'-Challenge message to the NSWOF in a Nausf_UEAuthentication_Authenticate Response message.

NOTE: The Access Network Identity is carried in the AT_KDF_INPUT attribute in EAP-AKA' as defined in RFC 5448 [12].

9. The NSWOF shall send the EAP-Request/AKA'-Challenge message to the WLAN AN over the SWa interface.

10. The WLAN AN forwards the EAP-Request/AKA'-Challenge message to the UE.

11. At receipt of the RAND and AUTN in the EAP-Request/AKA'-Challenge message, the ME shall obtain the Access Network Identity from the EAP signalling and the USIM in the UE shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [9]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' using the Access Network Identity as the KDF input parameter. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3.3. The UE may derive MSK from CK' and IK' as per Annex F and as described in RFC 5448[12]. When the UE is performing NSWO authentication, the K_{AUSF} shall not be generated by the UE.

12. The UE shall send the EAP-Response/AKA'-Challenge message to the WLAN AN.

13. The WLAN AN forwards the EAP-Response/AKA'-Challenge message over the SWa interface to the NSWOF.

14. The NSWOF shall send the Nausf_UEAuthentication_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.

15. The AUSF shall verify if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it continues as follows to step 16, otherwise it returns an error to the NSWOF. The AUSF shall derive the required MSK key from CK' and IK' as per Annex F and as described in RFC 5448[12], based on the NSWO indicator received in step 5. The AUSF shall not generate the K_{AUSF}.

16. The AUSF shall send Nausf_UEAuthentication_Authenticate Response message with EAP-Success and MSK key to NSWOF. The AUSF may optionally provide the SUPI to NSWOF. The AUSF/UDM shall not perform the linking increased home control to subsequent procedures (as stated in present document clause 6.1.4).

17. The NSWOF shall send the EAP-success and MSK to WLAN AN over the SWa interface. The EAP-Success message is forwarded from WLAN AN to the UE.

18. Upon receiving the EAP-Success message, the UE derives the MSK as specified in step 11, if it has not derived the MSK earlier. The UE uses the first 256-bit of MSK as PMK to perform 4-way handshake to establish a secure connection with the WLAN AN.

S.4 Roaming

The HPLMN may have a roaming agreement with a VPLMN for NSWO roaming. A roaming UE configured by the HPLMN to use 5G NSWO may try to register onto a WLAN AN that may advertise the HPLMN or a VPLMN (with which the HPLMN has a roaming agreement for NSWO roaming). The roaming architecture options are described in clause 4.2.15 in TS 23.501 [2].

NOTE: Void

Annex T (normative): Security for edge computing

T.1 General

The 5G Edge computing service is described in 3GPP TS 23.548 [98]. It defines the enhancements of 5G System to support Edge Computing.

T.2 Security of network exposure to edge application server

It is defined in the TS 23.548 [98] clause 6.4 that the network could expose network information to the local AF with two scenarios, i.e.

- Case 1: L-PSA UPF may expose the network information to local AF via Local NEF,
- Case 2: or L-PSA UPF may expose the network information to local AF directly. However, How to deliver the information on N6 is out of scope of the present document.

For the Case 1, the Security aspects of Network Exposure Function specified in clause 12 shall be used for the network information exposure.

T.3 Security of EAS discovery procedure via EASDF in non-roaming Scenario

DNS over TLS as specified in IETF RFC 7858 [83] and RFC 8310 [84] shall be supported by the UE and the EASDF. The DNS connection shall be authenticated and encrypted.

NOTE 1: Other DNS protection mechanisms are subject to implementation.

The security information of the EASDF can be preconfigured in the UE by using out of band mechanisms or if the core network is used to configure the security information, the SMF is preconfigured with the EASDF security information (authentication information, supported security mechanisms, port number, etc.) and provides the security information to the UE as follows:

The SMF provides the EASDF security information to the UE via PCO.

According to the clause 6.4.1.3 of TS 24.501 [35], upon receiving the DNS server security information, the UE passes it to the upper layer. The UE uses this information to send the DNS over TLS. Additionally, the clause 10.5.6.3 of TS 24.008 [111] provides the configuration of the different options of DNS over TLS specified in the RFC 7858 [83].

Annex U (informative): Primary authentication using EAP-TTLS in SNPNs

U.1 Introduction

In SNPN, when a credential holder is located outside of the 5GC of the SNPN, EAP-TTLS can be used to authenticate the UE. EAP-TTLS consists of two phases of authentication. In the first phase, a TLS tunnel is established between the UE and the EAP-TTLS server on AUSF. In the second phase, a legacy authentication protocol can be run between the UE and the credential holder (namely AAA) through the established TLS tunnel.

After the successful completion of EAP-TTLS, the AUSF and the UE derive the K_{AUSF} from the EMSK.

UE is provisioned with a trust anchor to enable verification of the EAP-TTLS server certificate. The provisioning of trust anchor on the UE is outside the scope of this document.

U.2 Procedure

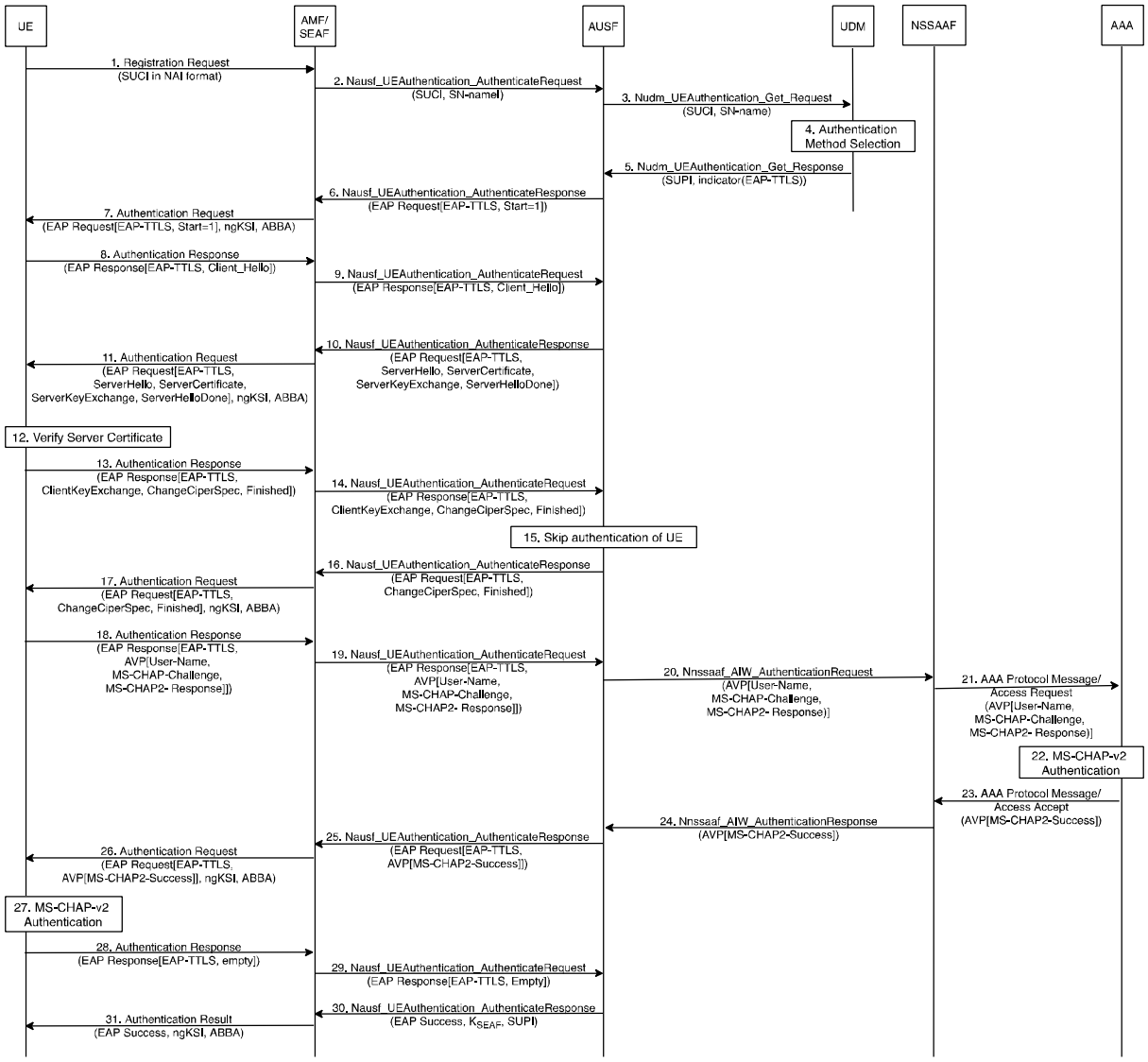


Figure: U.2-1: Primary authentication using EAP-TTLS and AAA

0. The UE is configured with the trust anchor needed to authenticate the certificate of the EAP-TTLS server running on the AUSF. Further, the UE is configured with the credentials required to authenticate with the AAA server.

Steps 1-17 are same as the steps 1-17 in clause B.2.2.1 in Annex B, except in the following steps:

1. The SUPI in the NAI format, i.e., username@realm, is used.

5. EAP-TTLS is selected by the UDM as the authentication method.

6-17. EAP-TTLS phase 1 is executed between the AUSF and the UE. EAP-Type is set to EAP-TTLS and the authentication of the UE using TLS client certificate is skipped. Since TLS client certificate is not used in EAP-TTLS, the UE need not be configured with UE certificate.

18-27. After EAP-TTLS phase 1 is successfully completed, the UE runs EAP-TTLS phase 2 authentication with the AAA as specified in RFC 5281 [99] via NSSAAF. The phase 2 authentication method used is outside the scope of the present document but MS-CHAPv2 is depicted here as an example to show that the Nnssaaf_AIW_Authentication service offered by NSSAAF carries AVPs if the phase 2 authentication method is non-EAP.NOTE: As referenced in section 14.1.11 of RFC 5281 [99], allowing the use of phase 2 (inner) authentication method outside of tunnelled protocol leads to Man-in-the-Middle (MitM) vulnerability. Thus, it is assumed that the UE does not allow the use of phase 2 authentication method outside of TLS tunnel (i.e., the UE does not respond to requests for phase 2 authentication outside of the TLS tunnel). In environments where the use of phase 2 authentication outside of the tunnelled protocol cannot be prevented, EAP-TTLS implementations need to address this vulnerability by using EAP channel binding or cryptographic binding described in RFC 6678 [100].

28-31. After EAP-TTLS phase 2 authentication is successfully completed, the rest of the procedures are same as steps 18- 21 described in clause B.2.1.1, except that the EAP-Type is set to EAP-TTLS in the EAP Response message from the UE to the AUSF.

Annex V (normative): User consent requirements and mechanisms

V.1 General

V.1.1 Scope

User consent can be required for 3GPP features depending on local regulations. Therefore, this annex describes the generic security requirements and procedures to support user consent enforcement in 3GPP services. While the use cases can differ, the annex focuses on the common and generic aspects related to the storage, checking and revocation of the user consent.

The user consent related requirements and mechanism in the present document are applicable only when it is required by regional regulations or operator's local policy, not otherwise.

The term *data processing* in this annex is used to convey the same meaning as in [101].

V.1.2 Relationship between end-users and subscriber

It is assumed that the user consent is obtained from the end-users. The end-user(s) is the subscriber itself or authorize the subscriber to provide consent on behalf of the end-users. Alternatively, the end-users are authorized by the subscriber to provide the consent. That means user consent is always tied to the subscription information. How authorization is provided between the subscriber and the end-users is out-of-scope of this specification.

NOTE: The term end-user is defined in TR 21.905 [1].

V.2 Requirements

The UDM shall support the following services related to the user consent.

- Retrieval of user consent parameters.
- Notification of user consent parameters change.

The user consent parameters shall be stored in the UDM/UDR as subscription data.

The user consent parameters shall be bound to a SUPI/GPSI.

The user consent parameters shall be bound to the purpose of data processing.

The user consent parameters shall include whether the user consent is granted or not.

The user consent shall be effective only after the point in time that user consent was given.The user consent shall be effective until revoked. It means that there is no expiry/validity timer for the user consent parameters stored in the subscription data.

NOTE: UDM does not provide user consent revocation service, it only provides notifications of user consent parameter changes.

V.3 User consent check

Any NF that is deemed an enforcement point for user consent shall support to retrieve the user consent parameters from the UDM.

Any NF that is deemed an enforcement point for user consent shall not accept any services or requests for data processing unless user consent is granted.

Any NF that is deemed an enforcement point for user consent shall determine the purpose of data processing prior to the data processing. If the purpose of data processing is not implicitly known from the service request, the user consent enforcement point shall request it or otherwise deny the service.

NFs obtaining or checking the user consent parameters shall consider the user consent parameters as effective until revoked.

V.4 User consent revocation

Any NF that is deemed an enforcement point for user consent shall support subscription to the user consent parameter change notification provided by the UDM.

Consumer NFs (processing the data pertaining to user consent) shall subscribe to UDM for user consent parameter change notification, except if the consent enforcement NF that is deemed an enforcement point is tracking of those NFs and is actively informing those consumer NFs in case of user consent revocation.

NOTE: When authorization consumer NFs for data processing subject to user consent, care needs to be taken to not authorize requests by those consumers that do not support the necessary services or related parameters for revocation. This is important because the user consent may change in the future.

Upon notification of user consent revocation, any NF that is deemed an enforcement point for user consent shall no longer accept any service request for data processing subject to a revoked user consent.

Upon notification of user consent revocation, any NF that is deemed an enforcement point for user consent may notify other NFs to halt the processing of the data subject to the revoked user consent.

Upon notification of user consent revocation, NFs (processing the data pertaining to the revoked consent) shall halt processing and collection of the data.

Upon notification of user consent revocation, NFs may delete, quarantine, or temporarily retain the data pertaining to the revoked user consent based on local policies and legal constraints.

Annex W (normative): Security for multicast/broadcast service for 3GPP service

W.1 General

This clause describes the security requirements, procedures and handling for 5G Multicast/Broadcast Service (MBS).The general features for 5G MBS are described in TS 23.247 [103].

NOTE: Security for Multicast-broadcast service for roaming is not supported.

W.2 Security requirements

W.2.1 Requirements of MBSF

The security requirements on the NEF described in clause 5.9.2.3 of present document also apply to MBSF.

W.2.2 Requirements of MBSTF

The security requirements on the NEF described in clause 5.9.2.3 of present document also apply to MBSTF.

W.3 Security mechanisms for xMB-C/MB2-C and xMB-U/MB2-U interface

The security aspects defined in clause 12 in present document is applicable for both MBSF and MBSTF. TLS based solution are reused to protect the interface xMB-C/MB2-C and xMB-U/MB2-U between AF and 5GC in MBS.

W.4 Security mechanisms for MBS traffic transmission

W.4.1 Key derivation, management and distribution

W.4.1.1 General

If the security protection of MBS traffic is required, confidentiality and integrity protection as specified in clause 5.3 of TS 33.246 [102] apply. The control-plane procedure and user-plane procedure are optionally supported in service layer. The control-plane procedure is only applicable for multicast sessions, while the user-plane procedure is applicable for both multicast sessions and broadcast sessions. The user plane security between UE and RAN shall be deactivated when 5GC shared MBS traffic delivery method for MBS data transmission is used to avoid redundant protection.

The MBS Security Function (MBSSF) is a logical function, which needs to be collocated with either MBSF or MBSTF and the according interfaces are up to the implementation of the deployment options. In case of the control-plane procedure, the key derivation, management and distribution in MBSF and MBSTF can be achieved in MBSSF.

W.4.1.2 Control-plane procedure

The multicast session security context consists of the MBS session ID, MBS keys and the corresponding key ID. The MBS keys include MBS Service Key (MSK) and MBS Traffic Key (MTK). MBS traffic is protected with the MTK. The MSK is used to protect the MTK when the MTK is delivered to the UE. The identification for every MSK and MTK are determined as specified in Clause 6.3.2.1 and clause 6.3.3.1 of TS 33.246 [102].

The MBSF determines whether security protection to be applied or not for the MBS session based on locally configured policy or based on the information provided by the AF. If security protection to be applied, then the MBSF shall create the multicast session security context by generating the MSK and its key ID for a MBS session. Afterwards, the MBSF distributes the MSK with MBS session ID and its key ID to the MB-SMF and MBSTF. The MBSF shall also distribute them to MB-SMF either upon request by the MB-SMF (i.e., pull) or when a new MSK is generated (i.e., push). The MBSF may also include the MSK lifetime when it distributes the MSK to MBSTF.

Upon receiving the MSK from the MBSF, the MBSTF generates the MTK and its key ID for the MBS traffic protection. A new MTK may be generated based on the MBS session security policy. When the MBSTF generates a new MTK, the MBSTF shall multicast the MTK and its key ID after protecting it using the MSK as specified in TS 33.246 [102]. The MBSTF shall also provide the new MTK and its key ID to the MBSF.

During the MBS session creation for multicast communication as specified in clause 7.1.1 of TS 23.247 [103], after receiving the description for an MBS session from the AF of content provider, the MBSF shall create the multicast session security context by generating an MSK and acquiring an MTK from the MBSTF. Afterwards, the MBSF distributes the muticast session security context to the MB-SMF via the Nmbsmf_MBSSession_Create Request message.

In the multicast session join and session establishment procedure, the SMF interacts with the MB-SMF to obtain the multicast session security context with Nmbsmf_MBSSession_ContextStatusSubscribe service. Absence of the multicast security context indicates that security protection is not applied for the MBS session. The SMF shall provide the multicast session security context in the N1 SM container (PDU Session Modification Command) to the UE if received from the MB-SMF and the UE is authorized to use the required multicast service. The UE shall use the MTK in the received multicast session security context, to process the protected MBS traffic until it receives a new MTK update over the user-plane.

The MSK update may be triggered by MB-SMF based on the request from AS or based on the local policy (e.g., key lifetime expiration). When the MSK is updated, the MBSF shall send the new MSK with MBS session ID and its key ID to the MB-SMF and then the MB-SMF shall trigger the session update as specified in clause 7.2.6 in TS 23.247 [103]. The MSK with MBS session ID and the corresponding key ID are delivered to the UEs that has joined the multicast session. The MBSF shall also send the new MSK with MBS session ID and its key ID to the MBSTF. The MBSTF may request a MSK to the MBSF when it does not have a valid MSK (e.g., due to the current MSK expiration).

NOTE 1: For an inactive MBS session, MBSTF defers MSK distribution until the MBS session is re-activated.

The MTK may be updated based on the change of the authorization information or based on the local policy (e.g. key lifetime expiration). In such cases, the MBSF or MB-SMF may trigger the MTK update to the MBSTF. The key update request message shall include the MBS session ID. If the MBSTF has generated a new MTK, the MBSTF shall provide the new MTK to the MBSF. To improve the efficiency of MTK update, the updated MTK is delivered from MBSTF to the UE using MIKEY over UDP as specified in clause 6.3.3.2 in TS 33.246 [102]. The MSK is used to protect the updated MTK. The UE shall not send an error message to the MBSTF as a result of receiving an MTK message.

NOTE 2: For an inactive MBS session, MBSTF defers the MTK distribution until the session in re-activated.

W.4.1.3 User-plane procedure

The UE registers to the MBS service and receives the MBS traffic as specified in TS 33.246 [102] with the following changes.

- MBSSF takes the role of the BM-SC in TS 33.246 [102].
- The UE authenticates to the MBSSF (i.e. MBSF or MBSTF) based on the GBA as in MBMS security (see TS 33.246 [102]) or based on the AKMA (see TS 33.535 [104]). When the AKMA is used, the MRK is derived from the K_{AF} as specified in Annex F of TS 33.246 [102] by replacing the Ks_NAF for the GBA_ME run with K_{AF}. Furthermore, when the AKMA is used, the MUK is set to K_{AF}. When the authorization of MBS service to the UE is required, the user id (e.g., GPSI) provided to the MBSSF by the AAnF shall be used.

NOTE a: Void

- The identifier(s) of MBS user service(s) in TS 26.502[108] is included in local configuration in MBSSF or in UDM as part of MBS subscription data for a UE, which identifies the user service(s) that the UE is allowed to join. After receiving the HTTP POST message (see clause 6.3.2 of TS 33.246 [102]) that] includes the identifier(s) of MBS user service(s), MBSSF shall authorize the UE based on local configuration if available. If no local configuration is available, the MBSSF should send verification request with user id (e.g., IMPI in GBA

or GPSI in AKMA) and identifier(s) of MBS user service(s) to UDM to acquire the authorization result. If the UE is authorized, the MBSSF registers the UE to the MBS user service(s).

NOTE: the local configuration in MBSSF may be preconfigured or provided by AF.

W.4.2 Protection of the traffic transmission

The traffic may require some protection depending on the sensitivity of the data being transmitted. For example, it is possible that the data being transmitted is actually protected by the application layer security and hence might not require additional protection. However, the protection in service layer is independent of application layer security.

The service protection description in the Service Announcement implies the protection requirement of the traffic transmission in case the security protection is provided in service layer. It may include indications for which security procedures are supported by the network: control-plane procedure or user-plane procedure. If the support for user-plane procedure is indicated then the description should include also an indication of whether GBA or/and AKMA is supported.

NOTE: If the security protection in service layer is not required, the service protection description is not present in the Service Announcement. If the UE does not support the network selected MBS security procedure at the service layer, then the UE can obtain the service via unicast delivery method.

The actual method of protection may vary depending on the type of data being transmitted, e.g. media streaming application or file download. Clause 6.6.2 and clause 6.6.3 in TS 33.246 [102] apply to the protection of streaming data and protection of download data, respectively.

W.4.3 Authentication and authorization aspects for the multicast session

The support for the optional-to-use authentication and authorization procedure for a 5G multicast session is specified in this clause.

AKMA/GBA is supported for authentication and authorization in user-plane procedure for security protection of MBS traffic, as specified in clause W.4.1.3 of the present document.

W.5 Security protection for interworking between 5MBS and eMBMS

Interworking between 5G MBS and eMBMS is supported at service layer. The procedures for inter system mobility with interworking at service layer is specified in clause 7.4 in TS 23.247 [103].

The joint BM-SC+MBSF/MBSTF functionality provides the security protection for MBS traffic. During inter-system mobility, when the target system is EPS, the security protection specified in TS 33.246 [102] applies. The security protection specified in present document applies to the case when the target system is 5GS.

Annex X (normative): Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2

X.1 General

This Annex provides security requirements and procedures for the Network Automation features.

The feature for enablers for Network Automation by 5GS is described in 3GPP TS23.501[2] and 3GPP TS23.288 [105].

X.2 Authorization of NF Service Consumers for data access via DCCF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF is depicted in Figure X.2-1:

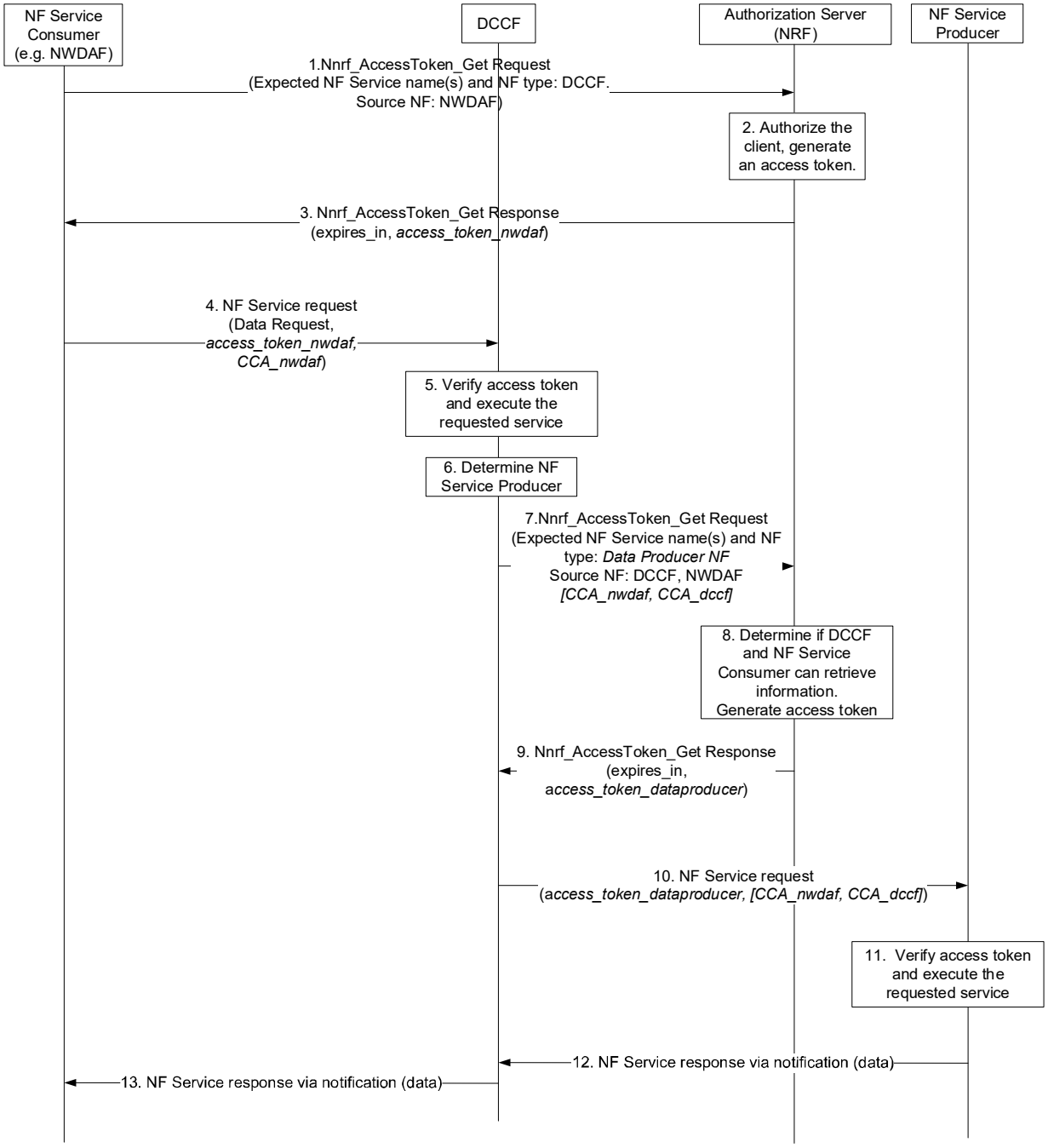


Figure X.2-1: NF Service Consumer Authorization to receive data from NF Service Producers via DCCF

1-3. NF Service Consumer shall send a request to the NRF to receive an access token to request services of DCCF, to be used for data collection request. NRF after verifying shall generate access token and sends it to the NF Service Consumer.

4. The NF Service Consumer initiates a NF service request to the DCCF which includes the access_token_nwdaf. The NF Service Consumer shall also generate a Client Credentials Assertion (CCA) token (CCA_NWDAF) as described in the clause 13.3.8 and includes it in the request message in order to authenticate itself towards the NF Service Producers.

NOTE 0: The procedure of NF Service Consumer (e.g. NWDAF) requesting the services provided by NF Service Producer via DCCF is defined in Clause 6.2.6.3 of TS 23.288 [105].

5. The DCCF shall verify if the access_token_nwdaf is valid and executes the service. If the NRF does not support authorization of the source NF (e.g. NWDAF) for data access via the DCCF (e.g. if the NRF is Rel-16), the DCCF authorizes the data access of the NF Service Consumer.

6. The DCCF determines the NF Service Producer(s) from where the data is to be collected (as specified in Clause 6.2.6.3.2 in TS 23.288[105]).

NOTE 1: If the NF Service Consumer sends the NF Service Producer information (i.e. NF Service Producer type and Instance ID) along with the service request in Step 4, then DCCF does not determine the NF Service Producer, but requests an access token from the NRF using the NF Service Producer details sent by the NF Service Consumer (as described in Step 7.)

7. The DCCF sends a Nnrf_AccessToken_Get request to NRF including the information to identify the target NF (NF Service Producer), the source NF (NF Service Consumer e.g. NWDAF), the NF Instance ID of DCCF and the CCA_NWDAF provided by the NF Service Consumer. The nfInstanceId IE attribute in the access token request (Nnrf_AccessToken_Get) indicates the NF instance ID of the DCCF as intermediate NF Service Consumer, whereas the sourceNfInstanceId IE attribute indicates the source NF instance ID (NF Service Consumer e.g., NWDAF).

NOTE 1a: Void

8. The NRF shall check whether the DCCF and the NF Service Consumer (e.g. NWDAF) are allowed to access the service provided by the identified NF Service Producers , and the DCCF as the proxy is allowed to request the service from the identified NF Service Producers on behalf the NF Service Consumer. NRF authenticates both DCCF and NWDAF based on one of the SBA methods described in clause 13.3.1.2.

NOTE 2: A Rel-16 NRF only authenticates and authorizes the DCCF, i.e., after the NRF receives Nnrf_AccessToken_Get request, the NRF validates whether the intermediate NF Service Consumer (e.g., DCCF) is authorized to receive the requested service from the NF Service Producer. The NRF from Rel-16 or earlier does not validate whether the source NF Service Consumer (e.g., NWDAF) is authorized to receive the requested service.

NOTE 3: Void

9. The NRF after successful verification then generates and provides an access token to the DCCF as described in the clause 13.4.1.1.2, with NF Instance ID of the DCCF (subject), and an additional access token claim containing the identity of the source NF Service Consumer, in order to authorize both NF DCCF and Service Consumer (e.g.. NWDAF) to consume the services of NF Service Producer.

NOTE 4: In the case the NRF is from Rel-16 or earlier, the NRF generates an OAuth2.0 access token with "subject" claim mapped to the intermediate NF Service Consumer, i.e., in this case DCCF, and no additional claim for the source NF Service Consumer (e.g., NWDAF) identity is added.

10. The DCCF requests service from the NF Service Producer. The request also contains the content of the CCA_NWDAF, so that the NF Service Producer(s) authenticates the NF Service Consumer (e.g. NWDAF) , i.e.,the NF Service Producer shall check the subject claim of CCA_NWDAF with the access token claim conveying the source NF Instance ID, when this claim is present in the access token.

11. The NF Service Producer(s) authenticates the NF Service Consumer and ensures that the source NF Service Consumer identity is included as an access token additional claim. The NF Service Producer authenticates and authorizes the DCCF following clauses 13.3.2 and 13.4.1. After authentication and authorization is successful, the NF Service Producer(s) executes the service.

NOTE 5: Rel-16 NF Service Producer only authenticates and authorizes the DCCF.

12. The NF Service Producer(s) shall provide requested data to the DCCF.

13. The DCCF forwards the received data to the NF Service Consumer(s).

NOTE 6: In the case a new NF Service Consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-10 apply. When the request is received by the NF Service Producer (i.e. the data producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to DCCF the access token verification response. DCCF based upon the response received, either updates the subscription info to include the new NF Service Consumer as well and sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288 [105]), or in the case of access token verification failure, the DCCF rejects the request received by the NF Service Consumer.

NOTE 7: Void

X.3 Authorization of NF Service Consumers for data access via DCCF when notification sent via MFAF

The detailed procedure for NF Service Consumer to receive data from Service Producers via DCCF when notification is sent via MFAF is depicted in Figure X.3-1:

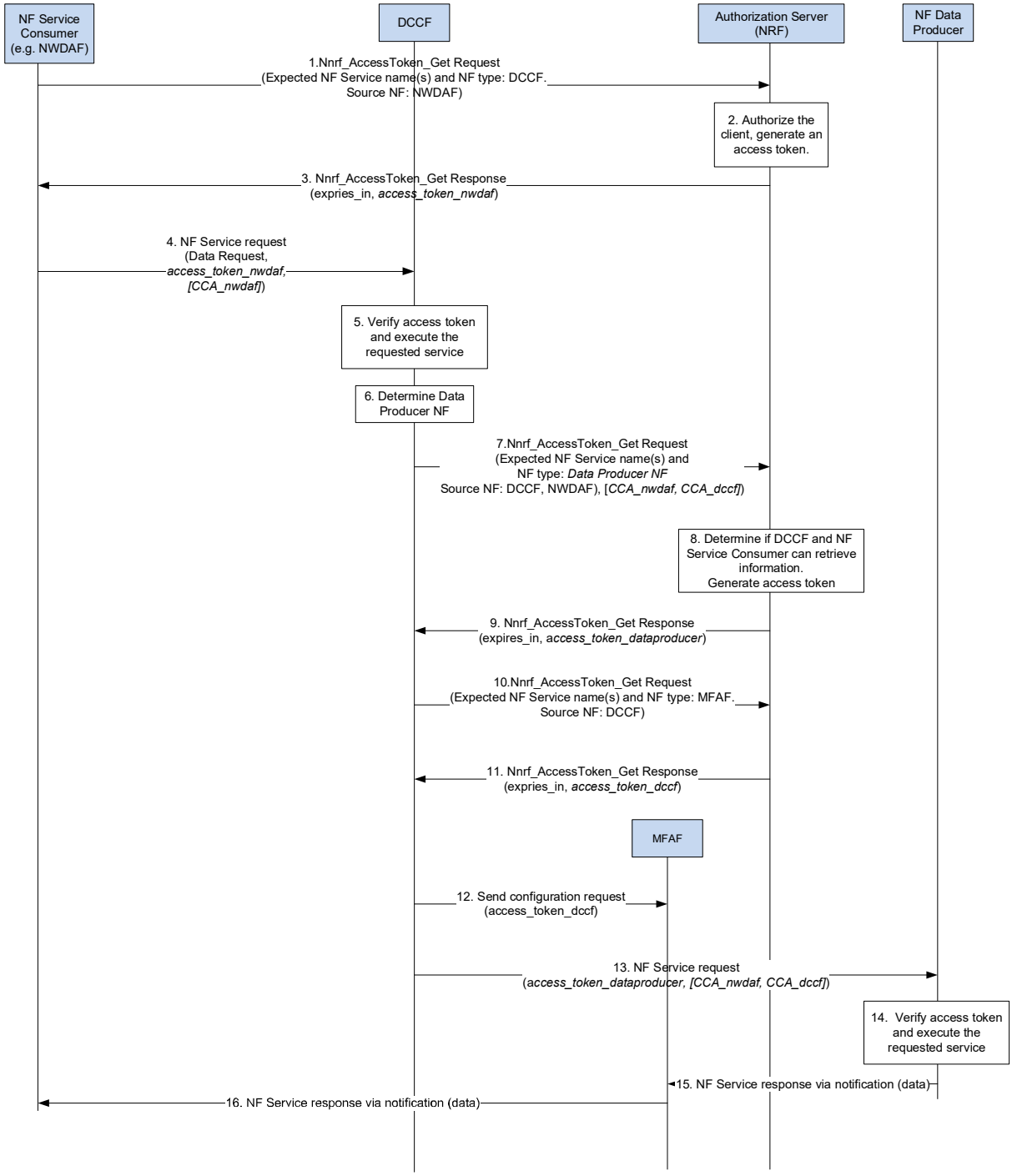


Figure X.3-1: Service Consumer Authorization to receive data from Service Producers via MFAF

Steps 1-9 are same as Steps 1 – 9 of Annex X.2

10-11. The DCCF sends an access token request to the NRF to request service from MFAF. NRF after verifying sends access_token_dccf to DCCF to consume the services of MFAF.

12. DCCF shall then send the Nmfaf_3daDataManagement_Configure request to MFAF (as specified in the Clause 6.2.6.3.2 in TS 23.288[105]) along with the access_token_dccf.

Steps 13 – 14 are same as Steps 10 – 11 of Annex X.2

15. The NF Service Producer(s) shall provide requested data to the MFAF.

16. The MFAF forwards the received data to the data consumer(s).

NOTE 1: In the case a new data consumer comes at a later stage to request the data, which is already being collected by DCCF, steps 1-9 and 13 apply. When the request is received by the NF Service Producer (i.e. the data producer), it authenticates the NF Service Consumer and verifies the access token provided along with the service request and sends to DCCF the access token verification response. DCCF based upon the response received, either updates the subscription info at the MFAF to include the new data consumer as well and MFAF sends the data to both the consumers (as specified in Clause 6.2.6.3.2 in TS 23.288 [105]), or in the case of access token verification failure, the DCCF rejects the request received by the data consumer and does not update the subscription at the MFAF.

NOTE 2: Void

X.4 Security protection of data via Messaging Framework

The transfer of the data between the data source and data consumer via the messaging framework shall be confidentiality, integrity, and replay protected.

Confidentiality protection, integrity protection, and replay-protection shall be supported on the new interfaces between 3GPP entities and MFAF by reusing the existing security mechanism defined for SBA in Clause 13.

X.5 Protection of data transferred between AF and NWDAF

As specified in TS 23.288[105], the NWDAF may interact with an AF to collect data from UE Application(s) as an input for analytics generation. The AF can be in the MNO domain or an AF external to MNO domain. To enhance the 5GS to support collection and utilisation of UE related data for providing the inputs to generate analytics information (to be consumed by other NFs), the communication between AF and NWDAF needs to be secured.

The NWDAF interacts with the 5GC NFs and the AF using Service-based Interfaces. The existing 5G security mechanism can be reused for the transfer of UE data over the SBA interface between AF and NWDAF. When the AF is located in the operator's network, the NWDAF uses Service-Based Interface as depicted in clause 13 to communicate with the AF directly. When the AF is located outside the operator's network, the NEF is used to exchange the messages between the AF and the NWDAF. The security aspects of NEF is specified in clause 12.

X.6 Protection of UE data in transit between NFs

According to clause 13.1.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

NFs shall obtain an access token from NRF for requesting analytics from an analytics function or providing analytics data to the analytics function.

X.7 User consent requirements

The user consent requirements for enablers of network automation shall comply with Annex V of the present document and TS 23.288 [105].

Annex Y (normative): Security aspects of the Message Service for MIoT over the 5G System (MSGin5G)

Y.1 General

This Annex specifies the security aspects of Message Service for MIoT over the 5G System (MSGin5G). The general features of MSGin5G are described in 23.554 [106], 22.262 [107].

Y.2 Authentication and authorization between MSGin5G client and MSGin5G Server

The Authentication and authorization between MSGin5G Client and MSGin5G Server shall be based on AKMA, which is specified in TS 33.535 [91]. Before initiating communication with MSGin5G Server, the UE needs to have performed primary authentication and registered with the 5GC, resulting in the successful generation of K_{AKMA} and A-KID at both MSGin5G Client and the 5GC as specified in clause 6.1, TS 33.535 [91].

Once the UE is registered in 5GC, the MSGin5G Client in the UE and the MSGin5G Server may use TLS for authentication as specified in Annex B of TS 33.535 [91] with the MSGin5G Server taking the role of AKMA AF.

Methods other than TLS with AKMA may be used for authentication between the MSGin5G Client and MSGin5G Server, depending on the Ua* protocols.

When MSGin5G service is used with SEAL, the application architecture described in TS 23.554 [106] is followed. In this case, authorization of the MSGin5G UE by the MSGin5G server is performed by validating the association between the UE service ID and UE ID (SUPI/GPSI). The UE service ID is acquired via the MSGin5G registration request, as specified in TS 23.554 [106]. The Configuration Management server or MSGin5G Configuration Function maintains association of the assigned UE service ID with the UE ID. The MSGin5G server retrieves the association from the Configuration Management server or MSGin5G Configuration Function using the UE ID received from the AAnF and verifies whether the UE service ID received in the registration request message is associated with the UE ID in the retrieved association information.

Y.3 Transport security protection for MSGin5G interfaces

The MSGin5G-1 interface may be protected by TLS based on K_{AF} established by AKMA as specified in TS 33.535 [91]. The MSGin5G Client and the MSGin5G Server establish the TLS session following the procedures defined in Annex B of TS 33.535 [91].

The MSGin5G-1 interface may be protected using mechanisms other than TLS with AKMA, depending on the Ua* protocols.

For the data protection over MSGin5G-3 interface between MSGin5G Server and Application Server, if the Application Server is inside the operator domain, the transport security protection on SBI interface shall be reused as specified in clause 13. If the Application Server is outside the operator domain, the Application Server shall connect to the MSGin5G Server via NEF, clause 12.3 in the present document is applicable with the Appplication Server taking the role of the AF.

For MSGin5G-2, MSGin5G-4 and MSGin5G-7 interfaces, TLS shall be used for transport protection unless network security is provided by other means.

Y.4 Authentication and Authorization between Application Server and MSGin5G Server

The authentication and authorization between Application Server and MSGin5G is based on the transport security protection. TLS should be used as specified in TS 33.210 [3].

Y.5 Authentication and Authorization between message Gateway and MSGin5G Server

The authentication and authorization between Message Gateway and the MSGin5G Server can reuse the authentication and authorization between network functions in 13.3.2 in this document.

In direct communication, authentication between message gateway and MSGin5GServer shall use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for authentication between message gateway and MSGin5GServer.

- If the PLMN does not use protection at the transport layer, authentication between message gateway and MSGin5GServer may be implicit by NDS/IP or physical security.

If the PLMN uses token-based authorization, the network shall use protection at the transport layer as described in clause 13.1.

In indirect communication scenarios, 13.3.2 in this document also applies.

Annex Z (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-06	SA#80	SP-180452	0004	1	B	Rules on concurrent running of authentication and NAS SMC procedure	15.1.0
2018-06	SA#80	SP-180452	0007	2	F	Remove EN for initial NAS message protection	15.1.0
2018-06	SA#80	SP-180452	0012	1	F	Modification on UE's subscribe privacy requirement	15.1.0
2018-06	SA#80	SP-180452	0018	-	D	Editorial modification on reference	15.1.0
2018-06	SA#80	SP-180452	0030	1	F	Add condition for reset NAS COUNTs	15.1.0
2018-06	SA#80	SP-180452	0038	2	F	Editorials to 33.501	15.1.0
2018-06	SA#80	SP-180454	0046	2	B	The granularity of NF service discovery	15.1.0
2018-06	SA#80	SP-180452	0053	2	F	CR for Clause Security algorithm selection, key establishment and security mode command procedure	15.1.0
2018-06	SA#80	SP-180452	0064	4	F	Corrections to secondary authentication procedure	15.1.0
2018-06	SA#80	SP-180454	0066	2	F	Clarifications to clause UP security mechanisms	15.1.0
2018-06	SA#80	SP-180452	0075	1	C	F1-C Protection	15.1.0
2018-06	SA#80	SP-180452	0080	1	F	Corrections related to authentication related services	15.1.0
2018-06	SA#80	SP-180452	0081	1	F	Clarifications to: Linking increased home control to subsequent procedures	15.1.0
2018-06	SA#80	SP-180452	0084	1	F	Clarifications to: Initiation of authentication and selection of authentication method	15.1.0
2018-06	SA#80	SP-180452	0090	1	F	Clarifications to Idle mode mobility from 5GS to EPS	15.1.0
2018-06	SA#80	SP-180452	0095	2	F	Multiple NAS connections	15.1.0
2018-06	SA#80	SP-180452	0097	2	F	Clarifications to Mapping of Security Contexts	15.1.0
2018-06	SA#80	SP-180452	0104	1	F	KeNB derivation in 5GS to EPS handover	15.1.0
2018-06	SA#80	SP-180455	0105	3	F	Corrections and clarifications to Handover from EPS to 5GS over N26	15.1.0
2018-06	SA#80	SP-180455	0107	-	F	Delete Editor's Note in C.3.4.3	15.1.0
2018-06	SA#80	SP-180454	0111	2	F	Misleading title given to clause 6.13	15.1.0
2018-06	SA#80	SP-180455	0115	3	F	Clarifications to: Authentication procedures	15.1.0
2018-06	SA#80	SP-180453	0118	3	F	Clarifications to: Using additional EAP methods for primary authentication	15.1.0
2018-06	SA#80	SP-180454	0120	1	F	Clarifications on unused 5G authentication vectors, and remaning authentication data	15.1.0
2018-06	SA#80	SP-180453	0125	3	F	Generalization of key derivation in NG-RAN to cover both gNBs and ng-eNBs	15.1.0
2018-06	SA#80	SP-180455	0128	1		Emergency call redirection scenarios	15.1.0
2018-06	SA#80	SP-180453	0135	1	C	TS 33.501 Resolving Editors notes 5.10.1 Security Visibility	15.1.0
2018-06	SA#80	SP-180453	0143	3	F	Clarifications to: Key hierarchy, key derivation, and distribution scheme	15.1.0
2018-06	SA#80	SP-180455	0145	5	B	Clarification to Subscription identifier privacy	15.1.0
2018-06	SA#80	SP-180453	0147	3	B	Clarifications to: Protection at the network or transport layer, Authorization and authentication between network functions and the NRF	15.1.0
2018-06	SA#80	SP-180453	0149	3	F	Corrections in clause 6	15.1.0
2018-06	SA#80	SP-180453	0150	1	F	Reference corrections in clause 8	15.1.0
2018-06	SA#80	SP-180453	0152	3	F	Clarifications to: Definitions and Abbreviations	15.1.0
2018-06	SA#80	SP-180453	0153	1	F	Editorial changes to claus 10 and 12	15.1.0
2018-06	SA#80	SP-180453	0155	2	F	Clarifications to Annex A : Key derivation functions	15.1.0
2018-06	SA#80	SP-180453	0156	2	F	Clarifications to: Security contexts	15.1.0
2018-06	SA#80	SP-180453	0157	1	F	Clarifications to: Security handling in state transitions	15.1.0
2018-06	SA#80	SP-180455	0160	-	F	Corrections to Authentication Framework	15.1.0
2018-06	SA#80	SP-180453	0161	1	B	Clarifications to security requirements and features (clause 5)	15.1.0
2018-06	SA#80	SP-180453	0162	2	F	Corrections on SUCI protection schemes	15.1.0
2018-06	SA#80	SP-180453	0163	3	F	Clarifications to: Security handling in mobility	15.1.0
2018-06	SA#80	SP-180453	0164	-	F	Corrections on clause 6.5	15.1.0
2018-06	SA#80	SP-180453	0165	1	F	Clarifications on clause 7.2	15.1.0
2018-06	SA#80	SP-180455	0170	2	F	Correction for TS 33.501 subclause 4.1	15.1.0
2018-06	SA#80	SP-180455	0172	1	F	Correction for TS 33.501 subclause 5.11.2	15.1.0
2018-06	SA#80	SP-180455	0183	1	B	Security Negotiation for RRC INACTIVE	15.1.0
2018-06	SA#80	SP-180455	0184	1	B	Key handling at RRC-INACTIVE state transitions	15.1.0
2018-06	SA#80	SP-180454	0185	1	F	Security Procedures for Dual Connectivity	15.1.0
2018-06	SA#80	SP-180455	0189	1	F	Editorial correction to clause 6.12.5 on SIDF	15.1.0
2018-06	SA#80	SP-180454	0192	1	F	Correction to: 3GPP 5G profile for EAP-AKA'	15.1.0
2018-06	SA#80	SP-180455	0194	-	F	Corrections to section 4.1 Security domains	15.1.0
2018-06	SA#80	SP-180455	0196	1	F	Corrections to section 13.4.1.1	
2018-06	SA#80	SP-180454	0200	-	F	Resolving Editor's Note on USIM	15.1.0
2018-06	SA#80	SP-180455	0201	1	C	Addition of SBA security requirements for SEPP and NF	
2018-06	SA#80	SP-180454	0208	1	F	Clarification of the IPsec implementation requirements	15.1.0
2018-06	SA#80	SP-180454	0209	1	B	Protection of internal gNB interfaces	15.1.0
2018-06	SA#80	SP-180454	0210	1	B	Introduction of DTLS for protection of Xn-C and N2 interfaces	15.1.0
2018-06	SA#80	SP-180454	0211	-	F	Corrections of references to sub-clauses	15.1.0

2018-06	SA#80	SP-180454	0212	-	F	Corrections and clarifications to idle mode mobility from EPS to 5GS over N26	15.1.0
2018-06	SA#80	SP-180454	0213	-	F	Authorization of Application Function's requests	15.1.0
2018-06	SA#80	SP-180454	0214	1	B	Security Mechanism for Steering of Roaming	15.1.0
2018-06	SA#80	SP-180448	0215	-	B	CAPIF support for NEF external exposure interface	15.1.0
2018-06	SA#80	SP-180454	0216	-	F	Clarfication to 6.4.1 NAS security general	15.1.0
2018-06	SA#80	SP-180454	0217	-	F	Clarifications to Annex D.3 Integrity algorithms	15.1.0
2018-09	SA#81	SP-180709	0154	3	D	Editorial changes to clause 9	15.2.0
2018-09	SA#81	SP-180708	0221	1	F	Generic description of 5G security elements	15.2.0
2018-09	SA#81	SP-180708	0223	2	F	Update on SEAF requirements	15.2.0
2018-09	SA#81	SP-180708	0230	1	F	Clause 5.2.5 - Modification on subscriber privacy	15.2.0
2018-09	SA#81	SP-180706	0236	-	D	Clause 6.4.5 - Editorial modification on NAS COUNT handling	15.2.0
2018-09	SA#81	SP-180709	0238	1	F	Clause 6.6.2 - Modification on UP security activation mechanism	15.2.0
2018-09	SA#81	SP-180708	0239	1	F	Clause 6.7.3.2 - Modification on algorithm selection during N2 handover	15.2.0
2018-09	SA#81	SP-180706	0240	-	F	Clause 6.7.3.5 - Correct reference for RNA update procedure	15.2.0
2018-09	SA#81	SP-180708	0242	1	F	Mobility - Correcting AS re-keying and NAS re-keying in N2-handover	15.2.0
2018-09	SA#81	SP-180709	0249	1	F	Add rule for concurrent running of security procedures	15.2.0
2018-09	SA#81	SP-180709	0250	1	F	Modify rule for concurrent running of security procedures	15.2.0
2018-09	SA#81	SP-180708	0251	1	F	Annex C clarification on 'username'	15.2.0
2018-09	SA#81	SP-180706	0252	-	F	Deletion of Requester ID from 'Nausf_UEAuthentication_authenticate'	15.2.0
2018-09	SA#81	SP-180707	0253	1	F	Removal of KSEAF storage restriction	15.2.0
2018-09	SA#81	SP-180709	0257	1	F	Deletion of ENs in Clause 5.3 Requirements on the gNB	15.2.0
2018-09	SA#81	SP-180706	0258	-	F	Align NAS connection identifier with access type identifier	15.2.0
2018-09	SA#81	SP-180706	0259	-	F	Correct the encryption key in confidentiality clause	15.2.0
2018-09	SA#81	SP-180706	0260	-	F	Deletion of Editor Note in Annex D.2.1 Ciphering algorithm	15.2.0
2018-09	SA#81	SP-180709	0261	1	F	Add definition and values for ABBA parameter	15.2.0
2018-09	SA#81	SP-180706	0262	-	F	Deletion of EN in Caluse 10.2.1 Authenticated IMS Emergency Sessions	15.2.0
2018-09	SA#81	SP-180706	0268	-	F	Reference corrections in clause 6.10	15.2.0
2018-09	SA#81	SP-180709	0270	1	F	Algorithm Negotiation for Unauthenticated UEs in LSM	15.2.0
2018-09	SA#81	SP-180706	0272		F	AS SMC Handling Update	15.2.0
2018-09	SA#81	SP-180709	0273	1	F	Other security procedures for DC	15.2.0
2018-09	SA#81	SP-180707	0275	1	F	N32 related definitions	15.2.0
2018-09	SA#81	SP-180708	0276	1	F	Access Token Request updates	15.2.0
2018-09	SA#81	SP-180708	0277	1	F	Access Token Request for a specific NF service producer	15.2.0
2018-09	SA#81	SP-180709	0278	1	F	Editorial corrections to TS 33.501	15.2.0
2018-09	SA#81	SP-180709	0279	1	F	Corrections on primary authentication	15.2.0
2018-09	SA#81	SP-180706	0280	-	F	Delay the transmission of kseaf after home network verifies the RES	15.2.0
2018-09	SA#81	SP-180709	0284	1	F	Align AS SMC procedure with SA2 and RAN3	15.2.0
2018-09	SA#81	SP-180707	0287	1	F	Remove Editor's Note on additional claims in the access token	15.2.0
2018-09	SA#81	SP-180707	0288	1	F	Remove Editor's Note on additional parameters that may be required in step 1 of Figure 13.4.1.1-2	15.2.0
2018-09	SA#81	SP-180706	0290	-	B	CR-slice-management-security	15.2.0
2018-09	SA#81	SP-180706	0292	-	F	Authentication for token-based authorization	15.2.0
2018-09	SA#81	SP-180709	0295	1	F	DC - definition corrections	15.2.0
2018-09	SA#81	SP-180706	0301	-	F	DC - correcting reference	15.2.0
2018-09	SA#81	SP-180709	0302	1	F	Mobility - Clarification in intra-gNB-CU handover	15.2.0
2018-09	SA#81	SP-180708	0305	1	F	Mobility - Resolving EN and corrections in AS re-keying	15.2.0
2018-09	SA#81	SP-180708	0306	1	F	Mobility - Corrections for usage of local policy at AMF	15.2.0
2018-09	SA#81	SP-180708	0307	1	F	Mobility - Rectification of NAS MAC calculation for NAS Container	15.2.0
2018-09	SA#81	SP-180706	0309	-	F	Mobility - Correction of NAS COUNTs in N2-handover	15.2.0
2018-09	SA#81	SP-180706	0310	-	F	Mobility - Removing an EN in Xn-handover	15.2.0
2018-09	SA#81	SP-180706	0311	-	F	Mobility - Rectification of UE security capabilities in NAS Container	15.2.0
2018-09	SA#81	SP-180707	0313	1	F	Privacy - adding missing details to SUCI content and format	15.2.0
2018-09	SA#81	SP-180707	0314	1	F	Privacy - addressing ENs	15.2.0
2018-09	SA#81	SP-180709	0315	1	F	Update of definition of 5G AS security context for 3GPP access	15.2.0
2018-09	SA#81	SP-180708	0316	1	F	Use the old KRRCint for calculation of the security token in MSG3	15.2.0
2018-09	SA#81	SP-180707	0319	1	F	Removal of token validation by NRF	15.2.0
2018-09	SA#81	SP-180707	0323	-	F	Clarification of ngKSI and ABBA parameter in 5G-AKA	15.2.0
2018-09	SA#81	SP-180707	0324	1	F	Clarification for ngksi and ABBA parameter for EAP-AKA'	15.2.0
2018-09	SA#81	SP-180708	0327	1	F	Corrections and clarifications to interworking clauses	15.2.0
2018-09	SA#81	SP-180708	0328	1	F	Removal of editor's note on harmonization between inter and intra system handovers	15.2.0
2018-09	SA#81	SP-180708	0329	1	F	Clarifications related to the NAS Container calculation during inter system handover	15.2.0
2018-09	SA#81	SP-180706	0330	-	F	Addition of missing reference to RFC on DTLS over SCTP	15.2.0
2018-09	SA#81	SP-180709	0331	1	F	Correction of Note on physical protection for NDS/IP use	15.2.0

2018-09	SA#81	SP-180709	0334	1	F	Multiple NAS connections: taking a new security context into use on non-3GPP access	15.2.0
2018-09	SA#81	SP-180706	0336	-	F	Correction to Clause 5.11.2 Requirements for algorithm selection	15.2.0
2018-09	SA#81	SP-180709	0337	1	F	Removal of Note 2a on Kausf use case restriction	15.2.0
2018-09	SA#81	SP-180706	0339	-	D	Editorial correction to TS 33.501	15.2.0
2018-09	SA#81	SP-180707	0341	1	F	Clarification to key hierarchy	15.2.0
2018-09	SA#81	SP-180707	0342	1	F	Collection of editorial changes	15.2.0
2018-09	SA#81	SP-180708	0343	1	F	Addition of definitions and corrections to references	15.2.0
2018-09	SA#81	SP-180707	0344	1	F	Corrections to references and update on authentication vector text	15.2.0
2018-09	SA#81	SP-180707	0347	2	F	Error handling for SBA authentication and authorization in service layer	15.2.0
2018-09	SA#81	SP-180707	0348	1	F	Clarification on authentication and authorization in SBA	15.2.0
2018-09	SA#81	SP-180709	0349	1	F	Adding OAuth related authorization services for SBA security	15.2.0
2018-09	SA#81	SP-180707	0354	1	F	Clarifications and editorials to clause 13.1 (Transport security for service based interfaces)	15.2.0
2018-09	SA#81	SP-180707	0355	-	F	Updates on Security Mechanism for Steering of Roaming	15.2.0
2018-09	SA#81	SP-180708	0360	1	F	Simplification of the UE handling of keys at handover	15.2.0
2018-09	SA#81	SP-180707	0362	1	F	CR on the registration procedure for mobility from EPS to 5GS	15.2.0
2018-09	SA#81	SP-180708	0363	1	F	CR on adding KAMF change flag in NAS SMC	15.2.0
2018-09	SA#81	SP-180708	0364	1	F	CR on corrections on the UP security policy confirmation	15.2.0
2018-09	SA#81	SP-180708	0365	1	F	CR on corrections on the UP security policy confirmation	15.2.0
2018-09	SA#81	SP-180708	0366	1	F	CR on corrections on the 5GS to EPS handover procedure	15.2.0
2018-09	SA#81	SP-180707	0367	-	F	Handling of initial value of CounterSoR	15.2.0
2018-09	SA#81	SP-180707	0368	-	F	Update on InactiveMAC-I calculation	15.2.0
2018-09	SA#81	SP-180707	0370	1	F	Clarification to the protection of attributes by the SEPP	15.2.0
2018-09	SA#81	SP-180707	0373	-	D	Editorial correction to 6.7.2 of 33.501	15.2.0
2018-09	SA#81	SP-180709	0374	-	B	Security mechanisms for non-SBA interfaces in 5GC	15.2.0
2018-09	SA#81	SP-180709	0375	-	F	Clarifications to 13.5	15.2.0
2018-09	SA#81	SP-180709	0376	-	B	Application layer security on the N32 interface	15.2.0
2018-12	SA#82	SP-181022	0377	-	F	Intra-gNB-CU term synchronization	15.3.0
2018-12	SA#82	SP-181022	0378	-	F	Update RNA Update Procedure Security	15.3.0
2018-12	SA#82	SP-181022	0379	-	F	N2 HO: Handling source algorithms for RRC Reestablishment procedure	15.3.0
2018-12	SA#82	SP-181022	0380	1	F	Handling of UP security policy in MR-DC	15.3.0
2018-12	SA#82	SP-181022	0381	-	F	Delete EN in SBA Requirements	15.3.0
2018-12	SA#82	SP-181022	0382	-	F	Clarifications on AccessToken_Get Response message	15.3.0
2018-12	SA#82	SP-181022	0383	-	F	Editorial corrections on Authorization of NF service access	15.3.0
2018-12	SA#82	SP-181022	0384	-	F	Add discover procedure as a pre-requisite for obtaining access token	15.3.0
2018-12	SA#82	SP-181022	0385	-	F	correction on the mobility from 5G to 4G	15.3.0
2018-12	SA#82	SP-181022	0387	-	F	Editorial corrections on the 5GS to EPS handover procedure	15.3.0
2018-12	SA#82	SP-181022	0388	-	F	Editorial corrections on the 5GS to EPS handover procedure	15.3.0
2018-12	SA#82	SP-181022	0389	-	F	Multiple NAS connections: clarification on the action of MAC verification in registration request over non-3gpp access	15.3.0
2018-12	SA#82	SP-181022	0390	1	F	Interworking - correcting keying material in HO request message (EPS to 5GS)	15.3.0
2018-12	SA#82	SP-181022	0391	-	F	Length of IV salt and sequence counter	15.3.0
2018-12	SA#82	SP-181022	0392	-	F	Correction to the Security Service for Steering of Roaming	15.3.0
2018-12	SA#82	SP-181022	0393	-	F	Mobility - Clarification of downlink NAS COUNT in N2 handover	15.3.0
2018-12	SA#82	SP-181022	0394	-	F	NAS key refresh	15.3.0
2018-12	SA#82	SP-181023	0395	-	F	Caching access tokens	15.3.0
2018-12	SA#82	SP-181023	0396	-	F	Addition of multiple instance IDs to OAuth2.0 access token claims	15.3.0
2018-12	SA#82	SP-181023	0397	-	F	Corrections to references for security related service in clause 14	15.3.0
2018-12	SA#82	SP-181023	0398	-	F	Correction to Nudm_UEAuthentication_ResultConfirmation service	15.3.0
2018-12	SA#82	SP-181023	0399	-	F	Correction to 5G AKA procedure - no need for SUPI or SUCI (in step 10)	15.3.0
2018-12	SA#82	SP-181023	0401	-	F	Acknowledging possibility of early calculation of EMSK	15.3.0
2018-12	SA#82	SP-181023	0402	-	F	Precedence of protection policies on the N32 interface	15.3.0
2018-12	SA#82	SP-181023	0403	-	F	Handling of encrypted IEs on the N32 interface	15.3.0
2018-12	SA#82	SP-181023	0404	-	F	Reference correction and editiorial clarification	15.3.0
2018-12	SA#82	SP-181023	0405	-	F	Removing mandatory text from note	15.3.0
2018-12	SA#82	SP-181023	0406	-	F	Clarification on first bits of EMSK	15.3.0
2018-12	SA#82	SP-181023	0407	-	F	Misleading text with reference regarding serving network name	15.3.0
2018-12	SA#82	SP-181023	0408	-	F	Alignment regarding KEY reference to 33.220	15.3.0
2018-12	SA#82	SP-181023	0409	-	F	Clarification to support of authentication methods	15.3.0
2018-12	SA#82	SP-181023	0410	-	F	Clarification to AUSF key derivation	15.3.0
2018-12	SA#82	SP-181023	0411	-	F	Corrections and addtions to definition clause	15.3.0
2018-12	SA#82	SP-181023	0412	-	F	Remove EN in 13.2	15.3.0
2018-12	SA#82	SP-181023	0413	-	F	Clarifications to clause 13.2.1	15.3.0
2018-12	SA#82	SP-181023	0414	-	F	Remove EN in 13.2.2.1	15.3.0
2018-12	SA#82	SP-181023	0415	-	F	Correction in step 2 of 13.2.2.2	15.3.0
2018-12	SA#82	SP-181023	0416	-	F	Corrections in 13.2.2.4 on N32-f context ID	15.3.0

2018-12	SA#82	SP-181023	0417	-	F	Clarifications and corrections in clause 13.2.4	15.3.0
2018-12	SA#82	SP-181024	0418	-	F	Multiple NAS Connection: Correcting NAS link identifier	15.3.0
2018-12	SA#82	SP-181024	0419	3	F	Replace 5G-RAN with NG-RAN in TS 33.501	15.3.0
2018-12	SA#82	SP-181024	0424	-	F	Editorial modification on gNB requirement	15.3.0
2018-12	SA#82	SP-181024	0425	1	F	AS subscription temperary identifier privacy	15.3.0
2018-12	SA#82	SP-181024	0426	1	F	Proposal about improvement of the UP security policy	15.3.0
2018-12	SA#82	SP-181024	0427	1	F	Corrections to definition of 5G AS security context for 3GPP access	15.3.0
2018-12	SA#82	SP-181024	0428	1	F	SUPI format in KAMF computation	15.3.0
2018-12	SA#82	SP-181024	0429	1	F	Editorial corrections in 6.9.2.3	15.3.0
2018-12	SA#82	SP-181024	0430	1	F	Update RRC reestablishment security procedure based on RAN2 agreement	15.3.0
2018-12	SA#82	SP-181024	0431	1	F	Adding UP security policy in SN Addition/modification Request message	15.3.0
2018-12	SA#82	SP-181024	0433	1	F	Clarification: AMF confirming UE SUPI in case NAS SMC failed	15.3.0
2018-12	SA#82	SP-181024	0437	-	F	Corrections to 5.2 Requirements on the UE	15.3.0
2018-12	SA#82	SP-181024	0438	-	F	Corrections to 5.3 Requirements on the gNB	15.3.0
2018-12	SA#82	SP-181024	0439	-	F	Corrections to 9. Security procedures for non-service based interfaces	15.3.0
2018-12	SA#82	SP-181024	0441	-	F	Correction on handover procedure from 5G to 4G	15.3.0
2018-12	SA#82	SP-181024	0442	-	F	Editorial corrections on the UP integrity mechanisms	15.3.0
2018-12	SA#82	SP-181024	0443	-	F	Editorial corrections on the SN Addition/Modification procedure	15.3.0
2018-12	SA#82	SP-181024	0446	1	F	CR to TS33.501-Registration related text correction	15.3.0
2018-12	SA#82	SP-181024	0448	1	F	Corrections to N32 Protection policies	15.3.0
2018-12	SA#82	SP-181024	0450	1	F	Adopting a more normative language in clause 13	15.3.0
2018-12	SA#82	SP-181024	0451	1	F	Amendment to secondary re-authentication procedure	15.3.0
2018-12	SA#82	SP-181025	0454	1	F	Clarification on interworking	15.3.0
2018-12	SA#82	SP-181025	0455	1	F	Update on access token in roaming scenario	15.3.0
2018-12	SA#82	SP-181025	0457	-	F	Corrections of N32-f key hierarchy	15.3.0
2018-12	SA#82	SP-181025	0458	1	F	Shift of text from SEPP intro to subclause	15.3.0
2018-12	SA#82	SP-181025	0459	1	F	Clarification to protection scheme identifier	15.3.0
2018-12	SA#82	SP-181025	0460	-	F	Clarification to the transfer of the authentication success result to UDM	15.3.0
2018-12	SA#82	SP-181025	0463	-	F	Correction of formatting errors	15.3.0
2018-12	SA#82	SP-181025	0464	1	F	Alignment on Home Network Public Key	15.3.0
2018-12	SA#82	SP-181025	0465	1	F	N32: remove redundant references to encrypted IEs	15.3.0
2018-12	SA#82	SP-181025	0466	-	F	pSEPP-pNF authentication	15.3.0
2018-12	SA#82	SP-181025	0467	1	F	Editorial corrections in clauses in 13.2	15.3.0
2018-12	SA#82	SP-181025	0468	1	F	Security between SEPP and IPX	15.3.0
2018-12	SA#82	SP-181025	0469	1	F	Two parallel N32-c connections between SEPPs	15.3.0
2018-12	SA#82	SP-181025	0470	1	F	Correction to Key hierarchy diagram	15.3.0
2018-12	SA#82	SP-181025	0471	-	F	Corrections to KSEAF derivation in Key distribution and derivation	15.3.0
2018-12	SA#82	SP-181025	0473	1	F	Handling of NAS COUNTs	15.3.0
2018-12	SA#82	SP-181025	0474	2	F	NG-RAN - clause 6.9.2.2	15.3.0
2018-12	SA#82	SP-181026	0475	2	F	NG-RAN - clause 6.9.2.3.3	15.3.0
2018-12	SA#82	SP-181026	0476	2	F	NG-RAN - clause 6.9.2.3.4	15.3.0
2018-12	SA#82	SP-181026	0479	-	F	Corrections on the number of bits of downlink NAS COUNT value to be delivered in the 5GS to EPS handover procedure	15.3.0
2018-12	SA#82	SP-181026	0480	-	F	Clarification on storing the selected EPS NAS algorithms	15.3.0
2018-12	SA#82	SP-181026	0481	1	F	Clarification on RRC Inactive procedure support by ng-eNB	15.3.0
2018-12	SA#82	SP-181026	0483	-	F	KgNB derivation in N2 handover	15.3.0
2018-12	SA#82	SP-181026	0484	1	B	Security mechanism for UE Parameters Update via UDM Control Plane Procedure	15.3.0
2018-12	SA#82	SP-181026	0488	-	F	Aligning the description of the initial NAS security procedures based on the CT1 agreements	15.3.0
2018-12	SA#82	SP-181026	0489	-	F	Inter PLMN Routing	15.3.0
2018-12	SA#82	SP-181026	0490	-	F	Verification of the PLMN-ID by the receiving SEPP	15.3.0
2018-12	SA#82	SP-181026	0491	-	F	Maximum output size of SUPI concealment schemes	15.3.0
2018-12	SA#82	SP-181026	0492	-	F	Support of UP security policy in ng-eNB	15.3.0
2018-12	SA#82	SP-181026	0493	-	F	Update of EAP-AKA' reference to make it compatible with 5G	15.3.0
2018-12	SA#82	SP-181026	0494	-	F	Clarifications to SUPI and SUCI	15.3.0
2018-12	SA#82	SP-181026	0495	-	F	KgNB derivation in EPS to 5GS handover	15.3.0
2018-12	SA#82					Version including all implementing CRs	15.3.1
2018-09	SA#83	SP-190095	0498	-	F	Clarification and correct clause reference for RNAU w/o context relocation	15.4.0
2018-09	SA#83	SP-190095	0501	-	F	Editorials and minor clarifications for clause 13.1	15.4.0
2018-09	SA#83	SP-190095	0502	1	F	Editorials and minor clarifications for clause 13.2	15.4.0
2018-09	SA#83	SP-190095	0503	-	F	Name correction of the Nudm_SDM_Notification service operation	15.4.0
2018-09	SA#83	SP-190095	0515	1	F	Clarification for clause 6.10.2.1	15.4.0
2018-09	SA#83	SP-190095	0516	1	F	Clarification for UP security in dual connectivity	15.4.0
2018-09	SA#83	SP-190095	0517	1	F	Clarification on interworking case	15.4.0

2018-09	SA#83	SP-190095	0518	1	F	Clarification on NAS key activation in multi-NAS connection	15.4.0
2018-09	SA#83	SP-190095	0519	1	F	Clarification on the UE selecting the 4G or 5G security protection method	15.4.0
2018-09	SA#83	SP-190095	0520	1	F	Corrections on ng-ran keys for EUTRA connected to 5GC	15.4.0
2018-09	SA#83	SP-190095	0524	1	F	NAS counter clarification on interworking	15.4.0
2018-09	SA#83	SP-190095	0525	-	F	Update on the token verification	15.4.0
2018-09	SA#83	SP-190095	0526	2	F	Clarification on service authorization and token verification	15.4.0
2018-09	SA#83	SP-190095	0528	1	F	Clarification on the Use of the SUPI in the Kamf Derivation	15.4.0
2018-09	SA#83	SP-190095	0529	2	F	Clarification on the allocation of 5G-GUTI	15.4.0
2018-09	SA#83	SP-190095	0530	1	F	Corrections to RRC Inactive procedure.and RAN-based notification area update procedure.	15.4.0
2018-09	SA#83	SP-190095	0531	1	F	EUTRA connected to 5GC: clause 6.6.2	15.4.0
2018-09	SA#83	SP-190095	0532	1	F	EUTRA connected to 5GC: clause 6.7.3	15.4.0
2018-09	SA#83	SP-190095	0533	1	F	EUTRA connected to 5GC: clause 6.7.4	15.4.0
2018-09	SA#83	SP-190095	0534	1	F	EUTRA connected to 5GC: clause 6.8.1	15.4.0
2018-09	SA#83	SP-190095	0535	1	F	EUTRA connected to 5GC: clause 6.8.2	15.4.0
2018-09	SA#83	SP-190096	0536	1	F	EUTRA connected to 5GC: clause 6.9.2.1	15.4.0
2018-09	SA#83	SP-190096	0538	1	F	EUTRA connected to 5GC: clauses 6.9.3 and 6.9.4	15.4.0
2018-09	SA#83	SP-190096	0539	1	F	EUTRA connected to 5GC: clause 6.9.5	15.4.0
2018-09	SA#83	SP-190096	0540	-	F	EUTRA connected to 5GC: clause 6.11	15.4.0
2018-09	SA#83	SP-190096	0541	-	F	EUTRA connected to 5GC: clause 8 and Annex A	15.4.0
2018-09	SA#83	SP-190096	0542	-	F	Clarification to AKA parameter derivation	15.4.0
2018-09	SA#83	SP-190096	0544	1	F	Multiple active NAS connections in the same PLMN's serving network: common algorithm identifiers	15.4.0
2018-09	SA#83	SP-190096	0545	-	F	Clarification to the implementation requirement for the protection of the backhaul and sidehaul interfaces	15.4.0
2018-09	SA#83	SP-190096	0546	-	F	Clarification to idle mode mobility from EPS to 5GS	15.4.0
2018-09	SA#83	SP-190096	0547	1	F	Allocating new 5G-GUTI during the MO service request procedure	15.4.0
2018-09	SA#83	SP-190096	0548	-	F	Correction to clause 14.2.1	15.4.0
2018-09	SA#83	SP-190096	0550	1	F	Correction on RRC states terminology usage	15.4.0
2018-09	SA#83	SP-190096	0551	1	F	Non-3GPP Access: Correcting Connection Identifier	15.4.0
2018-09	SA#83	SP-190096	0553	-	F	NAS connection identifier in NAS MAC calculation	15.4.0
2018-09	SA#83	SP-190096	0554	1	F	Clarification on N2 Handover procedure	15.4.0
2018-09	SA#83	SP-190096	0555	-	F	Clarification on KgNB derivation	15.4.0
2018-09	SA#83	SP-190096	0557	1	F	Input encoding for ECIES protection schemes	15.4.0
2018-09	SA#83	SP-190096	0558	-	F	User Plane Security for 5GC Roaming	15.4.0
2018-09	SA#83	SP-190197	0559	1	F	Clarification and definition for the term SN Id SNN input in KDFs	15.4.0
2019-06	SA#84	SP-190359	0560	1	F	Essential clarification of MSIN coding for the ECIES protection shemes	15.5.0
2019-06	SA#84	SP-190359	0561	1	F	Addition of missing SEPP requirement on JOSE-patch validation	15.5.0
2019-06	SA#84	SP-190359	0564	1	F	Aligning the storage timing of KAUSF in 5G AKA with EAP-AKA'	15.5.0
2019-06	SA#84	SP-190359	0565	1	F	Subscriber privacy: test data for ECIES-based encryption in the UE	15.5.0
2019-06	SA#84	SP-190359	0567	2	F	Clarification on Subscription Identifier mechanism for De-registration.	15.5.0
2019-06	SA#84	SP-190359	0569	1	F	Addition of AMF/SMF requirement on security logging	15.5.0
2019-06	SA#84	SP-190359	0572	1	F	Modification on Use of SUCI in NAS signalling	15.5.0
2019-06	SA#84	SP-190359	0573	-	F	Various corrections to security protocols and cryptography	15.5.0
2019-06	SA#84	SP-190359	0575	1	F	Slice information for token-based authorization	15.5.0
2019-06	SA#84	SP-190359	0576	-	F	CR to TS33.501 - NAS SMC figure correction	15.5.0
2019-06	SA#84	SP-190359	0577	1	F	Clarification on the UP integrity mechanisms	15.5.0
2019-06	SA#84	SP-190359	0578	1	F	Add details on handling UP security in RRC inactive scenario	15.5.0
2019-06	SA#84	SP-190359	0581	1	F	Clarification for initial NAS message protection	15.5.0
2019-06	SA#84	SP-190359	0583	1	F	Essential clarification on securing the procedure of idle mobility from 5GS to EPS over N26 interface	15.5.0
2019-06	SA#84	SP-190359	0587	1	F	Clarification on the SUCI computation	15.5.0
2019-06	SA#84	SP-190359	0593	1	F	Rectifying incorrect limitation for horiz/vert key derivation	15.5.0
2019-06	SA#84	SP-190359	0594	1	F	UP policy handling in case of unauthenticated emergency calls	15.5.0
2019-06	SA#84	SP-190359	0600	1	F	Missing privacy parameters	15.5.0
2019-06	SA#84	SP-190359	0602	1	F	Correction to the handling of security context in the multi-NAS scenario	15.5.0
2019-06	SA#84	SP-190359	0604	1	F	Clarification for the NAS MAC failure case in N2 HO	15.5.0
2019-06	SA#84	SP-190359	0605	1	F	Clarification for the NAS MAC failure case in interworking	15.5.0
2019-06	SA#84	SP-190359	0608	-	F	Clarification for N32 security	15.5.0
2019-09	SA#85	SP-190686	0609	3	F	Alignment with 29.505	15.6.0
2019-09	SA#85	SP-190686	0610	-	F	Missing security context handling during registration procedures	15.6.0
2019-09	SA#85	SP-190686	0611	1	F	NAS Count values in the mapped EPS security context in 5GS to EPS change	15.6.0
2019-09	SA#85	SP-190686	0614	-	F	length of ARFCN-DL	15.6.0
2019-09	SA#85	SP-190686	0616	1	F	uplink NAS Count for Kasme derivation in idle mode mobility to EPS	15.6.0

2019-09	SA#85	SP-190686	0617	3	F	Definition of authentication subscription data and update to UDM requirement	15.6.0
2019-09	SA#85	SP-190686	0618	1	F	Recommendation to run primary authentication after IW HO from 4G to 5G	15.6.0
2019-09	SA#85	SP-190686	0622	2	F	Update on ARPF	15.6.0
2019-09	SA#85	SP-190686	0627	1	F	Correction of Reference	15.6.0
2019-09	SA#85	SP-190686	0634	-	F	Changes on handover from EPS to 5GS over N26	15.6.0
2019-09	SA#85	SP-190686	0640	1	F	Correction of text on access authentication for untrusted access	15.6.0
2019-09	SA#85	SP-190686	0642	2	F	General NDS/IP SEG support for non-SBA interfaces	15.6.0
2019-09	SA#85	SP-190686	0644	1	F	Correcting references	15.6.0
2019-09	SA#85	SP-190686	0645	1	F	Removing editor notes	15.6.0
2019-09	SA#85	SP-190686	0646	1	F	Correction of handling of 5G security contexts during EPS to 5GS idle mode mobility	15.6.0
2019-09	SA#85	SP-190686	0647	1	F	Add missing message flow for Procedure for steering of UE	15.6.0
2019-09	SA#85	SP-190686	0648	1	F	Security context transfer following the handover from EPS to 5GS	15.6.0
2019-09	SA#85	SP-190686	0650	3	F	Clarification on UE context transfer in registration with AMF reallocation via direct NAS reroute	15.6.0
2019-09	SA#85	SP-190686	0652	1	F	Changes on handover from 5GS to EPS over N26	15.6.0
2019-09	SA#85	SP-190686	0653	-	F	Clarification for Secondary Authentication	15.6.0
2019-09	SA#85	SP-190686	0655	1	F	Adjust the proceudure of GPSI and IP/MAC notification	15.6.0
2019-09	SA#85	SP-190686	0656	-	F	Security of RRC UE capability transfer procedure in 5GS	15.6.0
2019-09	SA#85	SP-190686	0659	-	F	Aligning KAUSF storage at the UE with SoR and UPU procedures	15.6.0
2019-09	SA#85	SP-190685	0636	1	B	Clarification to Initial NAS message protection	16.0.0
2019-09	SA#85	SP-190687	0641	1	B	Security for non-public networks	16.0.0
2019-09	SA#85	SP-190682	0660	-	B	Security for SRVCC for 5G to UTRAN CS	16.0.0
2019-12	SA#86	SP-191132	0668	-	A	Mirror for Adding Missing Procedure for Security Handling for RRCConnectionRe-establishment Procedure	16.1.0
2019-12	SA#86	SP-191132	0673	1	A	Clarification on primary authentication in direct NAS reroute for Rel-16	16.1.0
2019-12	SA#86	SP-191131	0675	1	B	Security for roaming interfaces in indirect communication	16.1.0
2019-12	SA#86	SP-191141	0684	1	F	Removing editor's note on capturing all the details for alternative authentication methods	16.1.0
2019-12	SA#86	SP-191132	0686	-	A	Clarification on ARFCN for KNG-RAN derivation	16.1.0
2019-12	SA#86	SP-191132	0691	1	A	Updates to Counter Check Procedure	16.1.0
2019-12	SA#86	SP-191131	0692	1	B	Security requirements for SeCoP	16.1.0
2019-12	SA#86	SP-191131	0693		B	Authentication and authorization between SeCoP and network functions	16.1.0
2019-12	SA#86	SP-191131	0694		B	Authentication and authorization between SeCoPs	16.1.0
2019-12	SA#86	SP-191131	0696	1	B	TLS between NF and SEPP based on custom HTTP header	16.1.0
2019-12	SA#86	SP-191141	0701	-	F	Some corrections/clarification for non-public networks	16.1.0
2019-12	SA#86	SP-191141	0702	-	F	Removal of Editor's Note on conformance tests	16.1.0
2019-12	SA#86	SP-191141	0704	1	B	Security for 5GLAN services	16.1.0
2019-12	SA#86	SP-191141	0705	-	B	Intro to Security Annex for TSC service	16.1.0
2019-12	SA#86	SP-191141	0706	1	B	Access security for a TSC-enabled UE	16.1.0
2019-12	SA#86	SP-191141	0707	2	B	UP security in TSC	16.1.0
2019-12	SA#86	SP-191132	0708	-	F	Correction of handling of 5G security contexts during EPS to 5GS idle mode mobility	16.1.0
2019-12	SA#86	SP-191141	0709	-	D	Adding TSC abbreviation	16.1.0
2019-12	SA#86	SP-191131	0710	-	B	Service access authorization of a NF Set	16.1.0
2020-03	SA#87E	SP-200255	0689	3	B	Protection of N9 interface	16.2.0
2020-03	SA#87E	SP-200139	0745	-	F	UE handling on CHO key derivation for NR	16.2.0
2020-03	SA#87E	SP-200140	0747	-	F	Authentication in PNI-NPN	16.2.0
2020-03	SA#87E	SP-200255	0754	1	B	Security requirements for Inter-PLMN User Plane Security (IPUPS) Function	16.2.0
2020-03	SA#87E	SP-200133	0755	1	B	Resource Level Authorization using Access Tokens	16.2.0
2020-03	SA#87E	SP-200133	0756	1	F	3gpp-Sbi_Target-apiRoot header and TLS on N32	16.2.0
2020-03	SA#87E	SP-200143	0757	-	B	Using EAP-TLS with TLS 1.3	16.2.0
2020-03	SA#87E	SP-200139	0759	1	C	Key derivation for CHO (NR R16)	16.2.0
2020-03	SA#87E	SP-200134	0760	1	A	Clarification on native security context activation in handover from EPS to 5GS	16.2.0
2020-03	SA#87E	SP-200223	0765	-	F	Editoral Change on reference clauses	16.2.0
2020-03	SA#87E	SP-200140	0766	1	B	UP security policy enforcement in 5GLAN	
2020-03	SA#87E	SP-200140	0767	1	F	Referencing Annex for use of authentication methods	16.2.0
2020-03	SA#87E	SP-200140	0768	1	D	Clarifications on authentication methods selection and key derivation	16.2.0
2020-03	SA#87E	SP-200140	0769	-	F	Modification of CAG ID list	16.2.0
2020-03	SA#87E	SP-200140	0770	-	C	Definition of SN Id for standalone non-public networks	16.2.0
2020-03	SA#87E	SP-200140	0771	1	D	UP integrity enforcement for gPTP messages	16.2.0
2020-03	SA#87E	SP-200144	0782	-	B	Solution for IAB Architecture - 5GC	16.2.0
2020-03	SA#87E	SP-200142	0783	-	B	Security of 5G URLLC	16.2.0
2020-03	SA#87E	SP-200145	0784	-	B	5G security for 5WWC	16.2.0

2020-07	SA#88E	SP-200630	0762	3	A	Clarification on the use of SUPI as the Identity in EAP-AKA' key derivation	16.3.0
2020-07	SA#88E	SP-200369	0804	1	F	AKMA key generation indication	16.3.0
2020-07	SA#88E	SP-200368	0805	-	F	Adding a definition for IAB-UE	16.3.0
2020-07	SA#88E	SP-200365	0806	-	D	Aligning abbreviation of Service Communication Proxy with TS 23.501	16.3.0
2020-07	SA#88E	SP-200365	0807	-	F	Clarification on SEPP role regarding the 3gpp-Sbi-Target-apiRoot HTTP header	16.3.0
2020-07	SA#88E	SP-200365	0808	1	B	Authentication in indirect communication scenarios	16.3.0
2020-07	SA#88E	SP-200370	0824	-	F	Clarification on SUCI computation	16.3.0
2020-07	SA#88E	SP-200370	0828	1	A	Correction to security capability negotiation between SEPPs	16.3.0
2020-07	SA#88E	SP-200370	0830	-	A	Correction to initial EAP Authentication with an external AAA server	16.3.0
2020-07	SA#88E	SP-200370	0832	-	A	Editorial changes to TS 33.501 R16	16.3.0
2020-07	SA#88E	SP-200371	0833	1	F	Security entities at the perimeter of the 5G Core network	16.3.0
2020-07	SA#88E	SP-200356	0838	-	D	Several corrections to spec text	16.3.0
2020-07	SA#88E	SP-200370	0840		A	shortResumeMAC-I calculation	16.3.0
2020-07	SA#88E	SP-200367	0841	2	B	Security Aspects of DNS and ICMP	16.3.0
2020-07	SA#88E	SP-200368	0844	1	B	F1 interface security set-up procedure	16.3.0
2020-07	SA#88E	SP-200372	0846	-	B	UE pre-configuration for non-3GPP access networks	16.3.0
2020-07	SA#88E	SP-200356	0847		B	SUCI computation: implementers' test data for network specific identifier-based SUPI	16.3.0
2020-07	SA#88E	SP-200368	0848	-	F	Editorial change to the security for IAB	16.3.0
2020-07	SA#88E	SP-200372	0849	-	F	CR of 5WWC	16.3.0
2020-07	SA#88E	SP-200373	0850	2	B	5GS LCS work	16.3.0
2020-07	SA#88E	SP-200366	0851	1	B	Normative text for supporting 5G CIoT security	16.3.0
2020-07	SA#88E	SP-200628	0852	1	C	Update to User Plane Integrity Protection	16.3.0
2020-07	SA#88E	SP-200553	0853	-	B	Network slice specific authentication and authorization clauses	16.3.0
2020-07	SA#88E	SP-200584	0854	-	B	Token-based authorization in indirect communication scenarios	16.3.0
2020-09	SA#89E	SP-200709	0834	3	A	Clarification to 5G AV	16.4.0
2020-09	SA#89E	SP-200709	0858	-	A	Resolution of editor's note in clause 6.3.2.1 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0860	-	A	Resolution of editor's notes in clause 6.8.1.2.0 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0862	-	A	Resolution of editor's note in clause 6.8.1.2.2 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0864	-	A	Resolution of editor's note in clause 6.8.1.2.4 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0866	-	A	Resolution of editor's note in clause 6.9.1 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0868	-	A	Resolution of editor's note in clause 6.9.4.1 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0870	-	A	Resolution of editor's note in clause 6.9.4.2 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0872	-	A	Resolution of editor's note in clause 6.9.4.3 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0874	1	A	Resolution of editor's note in clause 10.2.2.2 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0876	-	A	Resolution of editor's note in clause 13.2.4.4.1 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0878	-	A	Resolution of editor's note in clause 13.5 - R16 mirror	16.4.0
2020-09	SA#89E	SP-200709	0879	-	A	Access Token Signature using MAC with symmetric key	16.4.0
2020-09	SA#89E	SP-200706	0880	1	F	Static authorization details	16.4.0
2020-09	SA#89E	SP-200710	0882	-	F	Removing rel-15 text relating to N9 roaming UP	16.4.0
2020-09	SA#89E	SP-200773	0883	1	F	Deletion of confusing text on KSEAF	16.4.0
2020-09	SA#89E	SP-200773	0885	1	F	Clarification of ECIES Profile B uncompressed mode text	16.4.0
2020-09	SA#89E	SP-200773	0888	1	A	Editorials on 13.4.1.2 Service access authorization in roaming scenarios-R15	16.4.0
2020-09	SA#89E	SP-200706	0900	1	F	Alignment and clarifications to SBA network or transport layer protocol	16.4.0
2020-09	SA#89E	SP-200773	0901	2	A	N32 interface	16.4.0
2020-09	SA#89E	SP-200706	0903	1	F	Authentication and static authorization	16.4.0
2020-09	SA#89E	SP-200706	0904	1	F	Overview clause on communication models	16.4.0
2020-09	SA#89E	SP-200706	0905	2	F	Authorization of NF service access	16.4.0
2020-09	SA#89E	SP-200716	0909	-	F	Modification on AAA Server triggered Slice-Specific Authorization Revocation procedure	16.4.0
2020-09	SA#89E	SP-200716	0913	1	F	Editorial changes to Clause 16	16.4.0
2020-09	SA#89E	SP-200773	0915	1	A	Mirror: change the long-lived TLS connection of N32-C to the short-lived	16.4.0
2020-09	SA#89E	SP-200773	0917	1	A	Update the N32-f context ID negotiation procedure	16.4.0
2020-09	SA#89E	SP-200773	0921	1	A	Mirror: Clarification on AMF reallocation with direct NAS reroute	16.4.0
2020-09	SA#89E	SP-200773	0924	-	F	Correction to Clause 6.10.2.1. SN Addition or modification	16.4.0
2020-09	SA#89E	SP-200773	0926	-	A	Correction of the full form of the abbreviation NRF	16.4.0
2020-09	SA#89E	SP-200707	0937	1	F	Allocation of FC values for KIAB derivation function	16.4.0
2020-09	SA#89E	SP-200773	0944	1	A	Clarifications to SoR integrity protection mechanism	16.4.0
2020-09	SA#89E	SP-200773	0947	-	A	Error handling by the receiving NF	16.4.0
2020-09	SA#89E	SP-200773	0951	-	A	NF Service Producer authorization	16.4.0
2020-12	SA#90e	SP-201012	0835	3	A	Clarification to SEAF	16.5.0
2020-12	SA#90e	SP-201011	0907	2	F	Re-using of access token in indirect communication with delegated discovery	16.5.0
2020-12	SA#90e	SP-201012	0955	1	A	NRF authorization during NF service consumer Access Token Get Request	16.5.0

2020-12	SA#90e	SP-201007	0958	-	F	Removal of AKMA related changes to TS 33.501 in Rel-16	16.5.0
2020-12	SA#90e	SP-201115	0960	3	F	Error correction and clarification of Annex O	16.5.0
2020-12	SA#90e	SP-201009	0961	1	F	Storage of 5G security context for each access type during multiple PLMN registration	16.5.0
2020-12	SA#90e	SP-201012	0968	1	A	Secondary authentication/authorization revocation	16.5.0
2020-12	SA#90e	SP-201013	0970	-	F	Correction to Nnssaaf_NSSAA services	16.5.0
2020-12	SA#90e	SP-201013	0971	-	F	Clean up to the Nnssaaf_NSSAA services	16.5.0
2020-12	SA#90e	SP-201011	0972	1	F	Input parameters of access token request addition and verification	16.5.0
2020-12	SA#90e	SP-201009	0976	-	F	Modification policy clarification in Rel16	16.5.0
2020-12	SA#90e	SP-201012	0984	1	A	Corrections for the NRF token request service	16.5.0
2020-12	SA#90e	SP-201011	0987	1	F	Resolving Editor's Note on SCP performing token-based authorization on behalf of Network Functions	16.5.0
2020-12	SA#90e	SP-201012	0998	-	A	NFc and NFp alignment in static authorization	16.5.0
2020-12	SA#90e	SP-201012	1002	-	A	Authorization of NF service access - removal of ambigious terminology	16.5.0
2020-12	SA#90e	SP-201012	1004	1	A	Authorization of NF service access - service request process steps	16.5.0
2020-12	SA#90e	SP-201011	1005	-	F	NF Service Consumer authentication	16.5.0
2020-12	SA#90e	SP-201011	1006	1	F	Authorization between NFs and SCP	16.5.0
2020-12	SA#90e	SP-201012	1011	-	A	[Mirror]Correction to derivation of KSN for dual connectivity	16.5.0
2020-12	SA#90e	SP-201009	1013	1	F	Support for mutual authentication between network entities	16.5.0
2020-12	SA#90e	SP-201009	1017	1	F	Correcting use of (D)TLS in 33.501	16.5.0
2020-12	SA#90e	SP-201008	0959	1	B	CR for AKMA changes to TS 33.501 in Rel-17	17.0.0
2021-03	SA#91e	SP-210113	1019	1	A	Resolving editor's note on encryption policy mismatch between SEPPs	17.1.0
2021-03	SA#91e	SP-210111	1022	1	A	NF Service Consumer and Producer in Service Request Process	17.1.0
2021-03	SA#91e	SP-210111	1023	1	A	Access token misuse prevention	17.1.0
2021-03	SA#91e	SP-210109	1035	1	A	Correction to access token storage in NF service consumer	17.1.0
2021-03	SA#91e	SP-210111	1037	2	A	Correction to service request process in OAuth 2.0 based authorization	17.1.0
2021-03	SA#91e	SP-210114	1044	-	A	Authentication method selection for N5CW	17.1.0
2021-03	SA#91e	SP-210113	1048	1	A	Mirror: align the JSON format on encryption IE with CT4 in Rel17	17.1.0
2021-03	SA#91e	SP-210109	1051	1	A	Adding the security requirement with encBlockIndex in Rel17	17.1.0
2021-03	SA#91e	SP-210111	1055	-	A	Corrections for the NRF token request service	17.1.0
2021-03	SA#91e	SP-210116	1073	-	B	Extend UPIP support in 5GS for all 5GC connected RAN architecture (NG-RAN) options	17.1.0
2021-03	SA#91e	SP-210109	1074	-	A	Correcting notation used for inter-AMF mobility key derivation	17.1.0
2021-03	SA#91e	SP-210109	1075	-	A	Correct NAS uplink COUNT for KgNB/KeNB derivation	17.1.0
2021-03	SA#91e	SP-210109	1076	-	A	Correct current uplink EPS NAS COUNT used at derivation of a mapped 5G security context	17.1.0
2021-03	SA#91e	SP-210115	1077	-	A	5G GUTI re-allocation	17.1.0
2021-03	SA#91e	SP-210115	1078	-	A	5G CIoT KNG-RAN derivation	17.1.0
2021-03	SA#91e	SP-210109	1079	1	A	Mirror_Clarification on security protection in AMF reallocation	17.1.0
2021-06	SA#92e	SP-210433	1081	1	A	Clarification on the number of PLMN IDuse by SEPP over N32	17.2.0
2021-06	SA#92e	SP-210435	1090	1	A	Assign FC Value for KTIPSec and KTNAP Derivation in R17	17.2.0
2021-06	SA#92e	SP-210441	1091	1	F	Change the procedure of network slice re-authentication and revocation by AAA-S	17.2.0
2021-06	SA#92e	SP-210441	1094	-	A	Addressing impersonate attack from AAA-S	17.2.0
2021-06	SA#92e	SP-210434	1107	1	A	Clarify the usage of TLS and PRINS between SEPPs	17.2.0
2021-06	SA#92e	SP-210433	1109	-	A	Correction to JOSE profile Reference	17.2.0
2021-06	SA#92e	SP-210434	1112	-	A	Downlink NAS COUNT handling after creating NAS container in EPS to 5GS Handover	17.2.0
2021-06	SA#92e	SP-210451	1114	-	A	Clarifying the support for authentication methods in an SNPN	17.2.0
2021-06	SA#92e	SP-210450	1120	1	F	Clarification on AMF transparency for SoR	17.2.0
2021-06	SA#92e	SP-210451	1123		A	Editor's note of the security of 5GLAN services removal in R17	17.2.0
2021-06	SA#92e	SP-210433	1128	1	A	N32-c and N32-f clarification	17.2.0
2021-06	SA#92e	SP-210433	1130	1	A	Deployment models	17.2.0
2021-06	SA#92e	SP-210434	1135	1	A	Removal of ENs for draft-ietf-emu-rfc5448bis- Rel-17	17.2.0
2021-06	SA#92e	SP-210449	1138	1	A	Handling of KAUSF upon successful primary authentication	17.2.0
2021-06	SA#92e	SP-210439	1140	-	B	PTP aspects	17.2.0
2021-06	SA#92e	SP-210439	1141	-	B	NEF-AF aspects	17.2.0
2021-06	SA#92e	SP-210441	1142	-	A	Slice privacy protection in NSSAA related procedures (Rel-17)	17.2.0
2021-06	SA#92e	SP-210449	1143	-	A	Solving misalignment on mapped security derivation	17.2.0
2021-06	SA#92e					Editorial fix on KAUSF to make it subscript.	17.2.1
2021-09	SA#93e	SP-210851	1150	1	A	Rel17 Align KAUSF handling for 5G AKA and EAP-AKA' for Release 17	17.3.0
2021-09	SA#93e	SP-210842	1151	-	F	Add Routing indicator into the Nudm_UEAuthentication_Get Response	17.3.0
2021-09	SA#93e	SP-210852	1158	1	F	Clairfication on AS key generation after runing NAS SMC	17.3.0
2021-09	SA#93e	SP-210851	1159	1	A	Clarification on Kausf storage in multi-NAS connection	17.3.0
2021-09	SA#93e	SP-210850	1164	-	A	Add missing reference	17.3.0
2021-09	SA#93e	SP-210852	1168		F	Clarification on transparent SoR container	17.3.0
2021-09	SA#93e	SP-210851	1170	2	A	Editorial Clarifications for Trusted non-3GPP Access using TNGF	17.3.0

2021-09	SA#93e	SP-210852	1174	1	F	Clarification on AMF transparency for UPU	17.3.0
2021-09	SA#93e	SP-210851	1176	-	A	Correction of UDM behaviour	17.3.0
2021-09	SA#93e	SP-210852	1182	3	F	Security context handling in IRAT	17.3.0
2021-09	SA#93e	SP-210850	1187	1	A	NRF service definition	17.3.0
2021-09	SA#93e	SP-210840	1191	1	A	Oauth2.0 misalignment	17.3.0
2021-12	SA#94e	SP-211359	1202	1	B	Support for NSWO in 5GS	17.4.0
2021-12	SA#94e	SP-211378	1210	-	F	Integrity check during context transfer scenario 1	17.4.0
2021-12	SA#94e	SP-211381	1214	1	A	Correction to Authorization for indirect communication	17.4.0
2021-12	SA#94e	SP-211389	1222	1	B	New Annex for Edge computing security	17.4.0
2021-12	SA#94e	SP-211381	1232	1	A	Mutual authentiation NRF-NRF in roaming	17.4.0
2021-12	SA#94e	SP-211381	1238	1	A	N32 for interconnect security	17.4.0
2021-12	SA#94e	SP-211380	1241	--	A	[Rel-17]Clarification on KIAB generation for CP-UP separation	17.4.0
2021-12	SA#94e	SP-211378	1242	--	B	KIAB generation for NR-DC scenario	17.4.0
2021-12	SA#94e	SP-211381	1246	-	A	Clarification on the audience of CCA	17.4.0
2021-12	SA#94e	SP-211383	1252	-	B	Security aspects of eNPN	17.4.0
2021-12	SA#94e	SP-211384	1253	-	B	User Plane Integrity Protection Policy Handling in IW handover from EPS to 5GS	17.4.0
2021-12	SA#94e	SP-211385	1254		B	UC3S in TS 33.501	17.4.0
2021-12	SA#94e	SP-211386	1255	-	B	Security aspects of 5MBS	17.4.0
2021-12	SA#94e	SP-211388	1256	-	B	Security aspects of eNA	17.4.0
2021-12	SA#94e	SP-211390	1257	-	B	Security aspects of MSGin5G	17.4.0
2022-01						Editorial change for the headers of annex U and V	17.4.1
2022-01						Removing wrongly implemented CR1219 (which was sent back to SA3 in SA)	17.4.2
2022-03	SA#95e	SP-220203	1261	1	A	Clarification when the responder SEPP establish a second N32-C connection	17.5.0
2022-03	SA#95e	SP-220223	1262	1	F	Editor note removal from Annex S	17.5.0
2022-03	SA#95e	SP-220210	1267	-	F	Delete EN on defining EIA7 in clause 6.6.4.3	17.5.0
2022-03	SA#95e	SP-220216	1269	1	B	AF Authorization for accessing network slice quota-usage information	17.5.0
2022-03	SA#95e	SP-220223	1273	1	F	Clarification and corrections to NSWO SBI Interface methods	17.5.0
2022-03	SA#95e	SP-220228	1274	1	F	Resolution of authorization issue	17.5.0
2022-03	SA#95e	SP-220228	1276	1	F	Corrections and clarifications in the security mechanisms for MBS	17.5.0
2022-03	SA#95e	SP-220225	1279	1	F	Delete Editor's Note in UC3S	17.5.0
2022-03	SA#95e	SP-220214	1283	1	F	Refer to User Consent Requirements for eNA	17.5.0
2022-03	SA#95e	SP-220215	1289	1	F	Removing Editor's note on SUPI sent to AAA	17.5.0
2022-03	SA#95e	SP-220194	1293	-	B	Security aspects on MINT feature	17.5.0
2022-03	SA#95e	SP-220228	1294	1	F	Clarification on AS security aspect in 5MBS	17.5.0
2022-03	SA#95e	SP-220212	1295	1	A	Editorial correction on clause 11.1.3 and 11.1.4	17.5.0
2022-03	SA#95e	SP-220227	1304	-	A	Removing Editor's Note on PNi-NPN security aspects	17.5.0
2022-03	SA#95e	SP-220215	1307	-	F	Removing Editor's note on Credentials Holder using AUSF and UDM for primary authentication	17.5.0
2022-03	SA#95e	SP-220215	1309	-	F	Editorial for the Figure on key hierarchy for Credentials Holder using AAA	17.5.0
2022-03	SA#95e	SP-220206	1312	-	A	Updating reference to RFC 9048 (EAP-AKA')	17.5.0
2022-03	SA#95e	SP-220223	1317	-	F	Usage of AN ID for NSWO authentication	17.5.0
2022-03	SA#95e	SP-220205	1319	1	F	Resolving EN on authorization in MSGin5G	17.5.0
2022-03	SA#95e	SP-220228	1322	1	B	Security indication in MBS security context	17.5.0
2022-03	SA#95e	SP-220222	1323	-	F	Clarification to IAB in EN-DC architecture	17.5.0
2022-03	SA#95e	SP-220215	1326	1	F	Clarification and corrections to UE Onboarding in SNPNs	17.5.0
2022-03	SA#95e	SP-220223	1327	1	F	Co-existence with EPS NSWO	17.5.0
2022-03	SA#95e	SP-220223	1328	1	B	5G NSWO roaming aspects	17.5.0
2022-03	SA#95e	SP-220204	1329	1	B	SBA service operations for Prose L3 U2N security CP solution	17.5.0
2022-03	SA#95e	SP-220210	1336	-	F	SEPP reference	17.5.0
2022-03	SA#95e	SP-220213	1338	1	A	Reference to N5CW and key derivation correction	17.5.0
2022-03	SA#95e	SP-220219	1343	-	F	Update of references for the GBA related UDM service operations	17.5.0
2022-03	SA#95e	SP-220210	1344	1	F	Clarification of the Registration Request handling for the direct AMF re-allocation	17.5.0
2022-03	SA#95e	SP-220210	1345	1	C	Protect additional SoR information (CPSOR-CMCI) (future proof alternative)	17.5.0
2022-03	SA#95e	SP-220215	1347	1	F	Resolution of editor's note related to NSSAAF and AUSF selection	17.5.0
2022-03	SA#95e	SP-220215	1349	1	F	Resolution of editor notes related UDM selection	17.5.0
2022-03	SA#95e	SP-220215	1350	1	F	Resolution of editor notes related to protocol between NSSAAF and AAA	17.5.0
2022-03	SA#95e	SP-220206	1356	-	A	Remove ambiguous phrase for rekeying error scenario in clause 6.9.2.3.2.	17.5.0
2022-06	SA#96	SP-220542	1334	2	A	Clarification on separate handling of N32-c and N32-f	17.6.0
2022-06	SA#96	SP-220559	1359	1	A	Clarifications to secondary authentication PDU Session Container	17.6.0
2022-06	SA#96	SP-220554	1363	1	F	NSWO alignment with SA2 specs	17.6.0
2022-06	SA#96	SP-220543	1365	1	A	Clarification on N32-f connection establishment with TLS	17.6.0
2022-06	SA#96	SP-220557	1373	1	F	Removing the Editor's Note and add clarifications in the security mechanisms for MBS	17.6.0

2022-06	SA#96	SP-220557	1374	1	F	Clarifications on the control-plane and user-plane procedures	17.6.0
2022-06	SA#96	SP-220557	1375	1	F	Enhancement for the service announcement	17.6.0
2022-06	SA#96	SP-220557	1379	1	F	Clarifications on the multicast security context handling in session creation procedure	17.6.0
2022-06	SA#96	SP-220551	1380	1	F	Configuration of Anonymous SUCI	17.6.0
2022-06	SA#96	SP-220551	1381	1	F	UDM interaction for Anonymous SUCI	17.6.0
2022-06	SA#96	SP-220550	1386	-	F	eNA - Editorial corrections and clarification to 33.501	17.6.0
2022-06	SA#96	SP-220551	1387	-	F	Terminology correction for security of UE onboarding	17.6.0
2022-06	SA#96	SP-220551	1388	1	F	Corrections and clarifications to secondary authentication during UE onboarding	17.6.0
2022-06	SA#96	SP-220551	1391	-	F	Implementation correction of CR1309	17.6.0
2022-06	SA#96	SP-220551	1397	1	F	Resolving Editor's note on using only null-scheme SUCI	17.6.0
2022-06	SA#96	SP-220551	1401	1	F	Resolution of inconsistency in SUCI usage during UE onboarding.	17.6.0
2022-06	SA#96	SP-220551	1402	1	F	Resolving Editor's Note related to UE onboarding	17.6.0
2022-06	SA#96	SP-220543	1412	-	A	Editorial changes for ENSI	17.6.0
2022-06	SA#96	SP-220556	1413	1	F	Clarification on the NSWO in the UE side	17.6.0
2022-06	SA#96	SP-220544	1414	1	F	Resolving the EN on the authorization between SCPs	17.6.0
2022-09	SA#97e	SP-220877	1427	-	F	NSWO alignment for MSK and PMK	17.7.0
2022-09	SA#97e	SP-220877	1428	1	F	Correction in AUSF api related to NSWO	17.7.0
2022-09	SA#97e	SP-220881	1436	1	F	pSEPP authorization for PLM ID in access token claim	17.7.0
2022-09	SA#97e	SP-220884	1444	1	A	Alignment of NAS transport protocol for 5G-RG over Wireline	17.7.0
2022-09	SA#97e	SP-220878	1445		F	Clarification on the authorzation of NF Service Consumers for data access via DCCF	17.7.0
2022-09	SA#97e	SP-220881	1446	-	F	Confidentiality protection of SMS content over N32	17.7.0
2022-09	SA#97e	SP-220881	1447	1	F	Clarification of SNI usage for NF clients and servers	17.7.0
2022-09	SA#97e	SP-220877	1459	1	F	Clarification on Authentication for UE behind 5G-RG and FN-RG	17.7.0
2022-09	SA#97e	SP-220882	1465	-	A	Revise the subject that performs verificaiton of access token(mirror)	17.7.0
2022-09	SA#97e	SP-220892	1468	1	F	Address EN for UC3S	17.7.0
2022-09	SA#97e	SP-220889	1469	1	F	clarification on the internal authentication and an external authentication	17.7.0
2022-09	SA#97e	SP-220890	1471	1	F	Correction of Transport security protection for MSGin5G interfaces	17.7.0
2022-09	SA#97e	SP-220882	1482	-	A	Clarification on OAuth2.0 in interconnect and roaming scenarios	17.7.0
2022-12	SA#98e	SP-221155	1430	2	F	User plane security for Non-SBA based interfaces	17.8.0
2022-12	SA#98e	SP-221155	1434	2	F	NF Service Set ID alignment	17.8.0
2022-12	SA#98e	SP-221155	1435	2	F	Clarification on N32-f connection establishment with TLS	17.8.0
2022-12	SA#98e	SP-221154	1491	-	A	Revise the pre-requisite of access token request(mirror)	17.8.0
2022-12	SA#98e	SP-221155	1500	1	F	Authentication in user plane procedure in MBS	17.8.0
2022-12	SA#98e	SP-221155	1501	1	F	Clarification on SNPN ID verification	17.8.0
2022-12	SA#98e	SP-221155	1512	-	F	Remove the redundant part of Figure I.2.3.2-1	17.8.0
2022-12	SA#98e	SP-221155	1513	1	F	Update A.17 for SoR transparent container	17.8.0
2022-12	SA#98e	SP-221155	1514	1	F	Update A.18 to define SoR-XMAC-IUE	17.8.0
2022-12	SA#98e	SP-221155	1515	1	F	Update A.20 to define UPU-XMAC-IUE	17.8.0
2022-12	SA#98e	SP-221155	1516	-	F	Update step 15 of clause I.2.2.2.1	17.8.0
2023-03	SA#99	SP-230140	1527	1	A	Support for multiple lists of root CA certificates	17.9.0
2023-03	SA#99	SP-230144	1547	1	F	Including SNPN ID in SBA and N32 related descriptions	17.9.0
2023-03	SA#99	SP-230144	1561	1	F	control-plane procedure in MBS	17.9.0
2023-03	SA#99	SP-230144	1562	2	F	Addition of Operator Roaming Hub definition in R17	17.9.0
2023-03	SA#99	SP-230144	1572	1	F	SEPP to include and verify the source PLMN-ID	17.9.0
2023-03	SA#99	SP-230144	1576	1	F	SCP requirements update related to source PLMN-ID	17.9.0
2023-06	SA#100	SP-230614	1488	3	A	Clarification to the UPU procedures	17.10.0
2023-06	SA#100	SP-230597	1605	1	A	Correction in N5CW device authentication	17.10.0
2023-06	SA#100	SP-230676	1619	1	F	Control-plane procedure in MBS	17.10.0
2023-06	SA#100	SP-230616	1624	1	F	Security for EAS discovery in non-roaming case	17.10.0
2023-06	SA#100	SP-230598	1628	1	F	Security of CPAC	17.10.0
2023-06	SA#100	SP-230596	1637	1	F	Authorization of NF service consumers for data access via DCCF	17.10.0
2023-06	SA#100	SP-230595	1645	1	A	Correction of procedures for N3GPP trusted access	17.10.0
2023-06	SA#100	SP-230598	1654	1	F	Clarification on AF authorization and architecture aligement for the NSACF notification procedure	17.10.0
2023-09	SA#101	SP-230908	1704	-	A	Correction on the Kamf derivation parameter	17.11.0
2023-09	SA#101	SP-230909	1736	1	F	Clarification on AF authorization in clause 12	17.11.0
2023-09	SA#101	SP-230877	1750	1	F	5MBS Annex W	17.11.0
2023-09	SA#101	SP-230899	1754	1	F	Correction of NAI format for 5G NSWO	17.11.0
2023-09	SA#101	SP-230873	1763	-	A	Deletion of 'N32-f precontext ID'	17.11.0
2023-09	SA#101	SP-230909	1773	1	F	IAB inter-CU topology adaptation procedure	17.11.0
2023-10						Re-issue due to corruption of the original file	17.11.1
2023-12	SA#102	SP-231329	1807	1	F	Conveying the CCA of the source NF service consumer	17.12.0
2023-12	SA#102	SP-231342	1826	-	F	Update the abbreviation list to include CPA and CPC R17	17.12.0
2023-12	SA#102	SP-231319	1841	-	A	Use visited PLMN in the roaming description	17.12.0
2023-12	SA#102	SP-231342	1873	-	F	Handling of 3gpp-Sbi-Originating-Network-Id header in the SNPN case	17.12.0
2023-12	SA#102	SP-231342	1875	-	F	Verification of the serving network name by the AUSF	17.12.0

2023-12	SA#102	SP-231342	1878	1	F	[IAB][Rel-17] IAB inter-CU topology adaptation procedure	17.12.0
2023-12	SA#102	SP-231323	1882	1	F	5MBS Annex W.4.2	17.12.0
2024-03	SA#103	SP-240348	1932	1	F	Details of the DNS security mechanism in EDGE computing (non-roaming)	17.13.0
2024-03	SA#103	SP-240351	1941	1	F	Resolution of EN concerning indication from UDM to AUSF to select authentication with external credential holder	17.13.0
2024-03	SA#103	SP-240346	1949	-	A	Voiding Reference to TLS 1.1	17.13.0
2024-03	SA#103	SP-240342	1965	-	A	Mirror of Correction of UDM service naming	17.13.0
2024-06	SA#104	SP-240657	1982	1	F	Clarification in TNGF and N3IWF procedures	17.14.0
2024-06	SA#104	SP-240657	1984	-	F	TWIF procedure correction	17.14.0
2024-06	SA#104	SP-240657	1986	1	F	UDR control flag for NSWO	17.14.0
2024-06	SA#104	SP-240657	2007	1	F	Correction on unauthenticated IMS emergency sessions - R17	17.14.0
2024-06	SA#104	SP-240657	2011	1	F	Serving Network Name check at AUSF	17.14.0
2024-06	SA#104	SP-240655	2020	-	F	Correcting incorrect reference in Section 33.501 Annex S.3.2	17.14.0