

# ETSI TS 133 501 V19.6.0 (2026-04)



TECHNICAL SPECIFICATION

## 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 19.6.0 Release 19)

get full document from [standards.iteh.ai](https://standards.iteh.ai)



---

**Reference**

RTS/TSGS-0333501 vj60

---

**Keywords**

5G

**ETSI**

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

---

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

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

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

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

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

© ETSI 2026.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

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

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at [3GPP to ETSI numbering cross-referencing](#).

---

# Modal verbs terminology

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

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

# Contents

Intellectual Property Rights .....	2
Legal Notice .....	2
Modal verbs terminology.....	2
Foreword.....	19
1 Scope .....	20
2 References .....	20
3 Definitions and abbreviations.....	25
3.1 Definitions .....	25
3.2 Abbreviations .....	29
4 Overview of security architecture .....	31
4.1 Security domains .....	31
4.2 Security at the perimeter of the 5G Core network.....	32
4.2.0 General.....	32
4.2.1 Security Edge Protection Proxy (SEPP) .....	32
4.2.2 Inter-PLMN UP Security (IPUPS).....	32
4.3 Security entities in the 5G Core network.....	32
5 Security requirements and features .....	33
5.1 General security requirements .....	33
5.1.1 Mitigation of bidding down attacks .....	33
5.1.2 Authentication and Authorization.....	33
5.1.3 Requirements on 5GC and NG-RAN related to keys .....	33
5.2 Requirements on the UE.....	33
5.2.1 General.....	33
5.2.2 User data and signalling data confidentiality .....	34
5.2.3 User data and signalling data integrity.....	34
5.2.4 Secure storage and processing of subscription credentials .....	35
5.2.5 Subscriber privacy .....	35
5.3 Requirements on the gNB .....	36
5.3.1 General.....	36
5.3.2 User data and signalling data confidentiality .....	36
5.3.3 User data and signalling data integrity.....	36
5.3.4 Requirements for the gNB setup and configuration.....	37
5.3.5 Requirements for key management inside the gNB.....	37
5.3.6 Requirements for handling user plane data for the gNB .....	37
5.3.7 Requirements for handling control plane data for the gNB .....	37
5.3.8 Requirements for secure environment of the gNB.....	37
5.3.9 Requirements for the gNB F1 interfaces.....	38
5.3.10 Requirements for the gNB E1 interfaces .....	38
5.4 Requirements on the ng-eNB .....	38
5.5 Requirements on the AMF .....	38
5.5.1 Signalling data confidentiality .....	38
5.5.2 Signalling data integrity.....	39
5.5.3 Subscriber privacy .....	39
5.6 Requirements on the SEAF .....	39
5.7 Void.....	39
5.8 Requirements on the UDM.....	39
5.8.1 Generic requirements.....	39
5.8.2 Subscriber privacy related requirements to UDM and SIDF .....	39
5.8a Requirements on AUSF.....	40
5.8b Requirements on the UDR .....	40
5.9 Core network security .....	40
5.9.1 Trust boundaries .....	40
5.9.2 Requirements on service-based architecture.....	40

5.9.2.1	Security Requirements for service registration, discovery and authorization .....	40
5.9.2.2	NRF security requirements .....	41
5.9.2.3	NEF security requirements.....	41
5.9.2.4	Requirements on the Service Communication Proxy (SCP) .....	41
5.9.3	Requirements for e2e core network interconnection security .....	42
5.9.3.1	General .....	42
5.9.3.2	Requirements for Security Edge Protection Proxy (SEPP) .....	42
5.9.3.2a	Support for Messages generated by Roaming Intermediaries .....	44
5.9.3.3	Protection of attributes .....	44
5.9.3.4	Requirements for IPUPS functionality.....	45
5.9.3.5	Requirements for Network Functions (NF).....	45
5.9.4	Requirements for monitoring 5GC signaling traffic .....	45
5.9.4.1	Security requirements for the configuration of signalling monitoring .....	45
5.9.4.2	Security requirements for the streaming of signalling monitoring data .....	45
5.10	Visibility and configurability .....	46
5.10.1	Security visibility.....	46
5.10.2	Security configurability .....	46
5.11	Requirements for algorithms, and algorithm selection.....	46
5.11.1	Algorithm identifier values .....	46
5.11.1.1	Ciphering algorithm identifier values.....	46
5.11.1.2	Integrity algorithm identifier values.....	47
5.11.2	Requirements for algorithm selection .....	47
5.12	Requirements on 5G-RG .....	47
5.13	Requirements on NSSAAF .....	48
6	Security procedures between UE and 5G network functions .....	48
6.0	General .....	48
6.1	Primary authentication and key agreement .....	48
6.1.1	Authentication framework .....	48
6.1.1.1	General .....	48
6.1.1.2	EAP framework.....	49
6.1.1.3	Granularity of anchor key binding to serving network.....	49
6.1.1.4	Construction of the serving network name.....	50
6.1.1.4.1	Serving network name .....	50
6.1.1.4.2	Construction of the serving network name by the UE.....	50
6.1.1.4.3	Construction of the serving network name by the SEAF .....	50
6.1.2	Initiation of authentication and selection of authentication method .....	50
6.1.3	Authentication procedures .....	52
6.1.3.1	Authentication procedure for EAP-AKA' .....	52
6.1.3.2	Authentication procedure for 5G AKA .....	54
6.1.3.2.0	5G AKA .....	54
6.1.3.2.1	Void.....	57
6.1.3.2.2	RES* verification failure in SEAF or AUSF or both .....	57
6.1.3.3	Synchronization failure or MAC failure .....	57
6.1.3.3.1	Synchronization failure or MAC failure in USIM.....	57
6.1.3.3.2	Synchronization failure recovery in Home Network.....	57
6.1.4	Linking increased home control to subsequent procedures .....	58
6.1.4.1	Introduction.....	58
6.1.4.1a	Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF.....	58
6.1.4.2	Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF.....	59
6.1.5	Home network triggered primary authentication procedure .....	60
6.1.5.1	General .....	60
6.1.5.2	Security mechanisms.....	60
6.2	Key hierarchy, key derivation, and distribution scheme .....	62
6.2.1	Key hierarchy.....	62
6.2.2	Key derivation and distribution scheme.....	63
6.2.2.1	Keys in network entities .....	63
6.2.2.2	Keys in the UE .....	65
6.2.3	Handling of user-related keys .....	67
6.2.3.1	Key setting .....	67
6.2.3.2	Key identification.....	67

6.2.3.3	Key lifetimes .....	68
6.3	Security contexts .....	69
6.3.1	Distribution of security contexts .....	69
6.3.1.1	General .....	69
6.3.1.2	Distribution of subscriber identities and security data within one 5G serving network domain .....	69
6.3.1.3	Distribution of subscriber identities and security data between 5G serving network domains .....	69
6.3.1.4	Distribution of subscriber identities and security data between 5G and EPS serving network domains .....	69
6.3.2	Multiple registrations in same or different serving networks .....	70
6.3.2.0	General .....	70
6.3.2.1	Multiple registrations in different PLMNs .....	70
6.3.2.2	Multiple registrations in the same PLMN .....	70
6.4	NAS security mechanisms .....	71
6.4.1	General .....	71
6.4.2	Security for multiple NAS connections .....	71
6.4.2.1	Multiple active NAS connections with different PLMNs .....	71
6.4.2.2	Multiple active NAS connections in the same PLMN's serving network .....	71
6.4.3	NAS integrity mechanisms .....	72
6.4.3.0	General .....	72
6.4.3.1	NAS input parameters to integrity algorithm .....	72
6.4.3.2	NAS integrity activation .....	73
6.4.3.3	NAS integrity failure handling .....	73
6.4.4	NAS confidentiality mechanisms .....	73
6.4.4.0	General .....	73
6.4.4.1	NAS input parameters to confidentiality algorithm .....	73
6.4.4.2	NAS confidentiality activation .....	73
6.4.5	Handling of NAS COUNTs .....	74
6.4.6	Protection of initial NAS message .....	74
6.4.7	Security aspects of SMS over NAS .....	75
6.5	RRC security mechanisms .....	75
6.5.1	RRC integrity mechanisms .....	75
6.5.2	RRC confidentiality mechanisms .....	76
6.5.3	RRC UE capability transfer procedure .....	76
6.6	UP security mechanisms .....	76
6.6.1	UP security policy .....	76
6.6.2	UP security activation mechanism .....	77
6.6.3	UP confidentiality mechanisms .....	79
6.6.4	UP integrity mechanisms .....	79
6.6.4.1	General .....	79
6.6.4.2	UP integrity mechanisms between the UE and the gNB .....	79
6.6.4.3	UP integrity mechanisms between the UE and the ng-eNB .....	79
6.7	Security algorithm selection, key establishment and security mode command procedure .....	80
6.7.1	Procedures for NAS algorithm selection .....	80
6.7.1.1	Initial NAS security context establishment .....	80
6.7.1.2	AMF change .....	80
6.7.2	NAS security mode command procedure .....	80
6.7.3	Procedures for AS algorithm selection .....	82
6.7.3.0	Initial AS security context establishment .....	82
6.7.3.1	Xn-handover .....	82
6.7.3.2	N2-handover .....	82
6.7.3.3	Intra-gNB-CU handover/intra-ng-eNB handover .....	83
6.7.3.4	Transitions from RRC_INACTIVE to RRC_CONNECTED states .....	83
6.7.3.5	RNA Update procedure .....	83
6.7.3.6	Algorithm negotiation for unauthenticated UEs in LSM .....	83
6.7.4	AS security mode command procedure .....	84
6.8	Security handling in state transitions .....	85
6.8.1	Key handling at connection and registration state transitions .....	85
6.8.1.1	Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states .....	85
6.8.1.1.0	General .....	85
6.8.1.1.1	Transition from RM-REGISTERED to RM-DEREGISTERED .....	85
6.8.1.1.2	Transition from RM-DEREGISTERED to RM-REGISTERED .....	86
6.8.1.1.2.1	General .....	86

6.8.1.1.2.2	Full native 5G NAS security context available .....	87
6.8.1.1.2.3	Full native 5G NAS security context not available .....	87
6.8.1.1.2.4	UE registration over a second access type to the same AMF .....	88
6.8.1.2	Key handling at transitions between CM-IDLE and CM-CONNECTED states .....	88
6.8.1.2.0	General .....	88
6.8.1.2.1	Transition from CM-IDLE to CM-CONNECTED .....	88
6.8.1.2.2	Establishment of keys for cryptographically protected radio bearers in 3GPP access .....	89
6.8.1.2.3	Establishment of keys for cryptographically protected traffic in non-3GPP access .....	89
6.8.1.2.4	Transition from CM-CONNECTED to CM-IDLE .....	90
6.8.1.3	Key handling for the Registration procedure when registered in NG-RAN .....	90
6.8.2	Security handling at RRC state transitions .....	91
6.8.2.1	Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states .....	91
6.8.2.1.1	General .....	91
6.8.2.1.2	State transition from RRC_CONNECTED to RRC_INACTIVE .....	91
6.8.2.1.3	State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB .....	91
6.8.2.1.4	State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB .....	93
6.8.2.2	Key handling during mobility in RRC_INACTIVE state .....	93
6.8.2.2.1	General .....	93
6.8.2.2.2	RAN-based notification area update to a new gNB/ng-eNB .....	93
6.8.2.2.3	RAN-based notification area update to the same gNB/ng-eNB .....	93
6.9	Security handling in mobility .....	94
6.9.1	Void .....	94
6.9.2	Key handling in handover .....	94
6.9.2.1	General .....	94
6.9.2.1.1	Access stratum .....	94
6.9.2.1.2	Non access stratum .....	95
6.9.2.2	Key derivations for context modification procedure .....	95
6.9.2.3	Key derivations during handover .....	96
6.9.2.3.1	Intra-gNB-CU handover and intra-ng-eNB handover .....	96
6.9.2.3.2	Xn-handover .....	96
6.9.2.3.3	N2-Handover .....	97
6.9.2.3.4	UE handling .....	98
6.9.3	Key handling in mobility registration update .....	99
6.9.4	Key-change-on-the-fly .....	101
6.9.4.1	General .....	101
6.9.4.2	NAS key re-keying .....	101
6.9.4.3	NAS key refresh .....	101
6.9.4.4	AS key re-keying .....	102
6.9.4.5	AS key refresh .....	102
6.9.5	Rules on concurrent running of security procedures .....	103
6.9.5.1	Rules related to AS and NAS security context synchronization .....	103
6.9.5.2	Rules related to parallel NAS connections .....	103
6.9.6	Security handling in registration with AMF reallocation via direct NAS reroute .....	103
6.10	Dual connectivity .....	104
6.10.1	Introduction .....	104
6.10.1.1	General .....	104
6.10.1.2	Dual Connectivity protocol architecture for MR-DC with 5GC .....	104
6.10.2	Security mechanisms and procedures for DC .....	105
6.10.2.1	SN Addition or modification .....	105
6.10.2.2	Secondary Node key update .....	107
6.10.2.2.1	General .....	107
6.10.2.2.2	MN initiated .....	107
6.10.2.2.3	SN initiated .....	107
6.10.2.3	SN release and change .....	107
6.10.2.4	Security mechanism and procedures for SCPAC .....	107
6.10.2.4.1	General .....	107
6.10.2.4.2	Security context initialization for selective SCPAC .....	108
6.10.2.4.3	Security mechanism for UE to access target PSCell or SN .....	108
6.10.2.4.4	Security procedure for UE to access target PSCell or SN .....	108
6.10.3	Establishing the security context between the UE and SN .....	110
6.10.3.1	SN Counter maintenance .....	110
6.10.3.2	Derivation of keys .....	111

6.10.3.3	Negotiation of security algorithms .....	111
6.10.4	Protection of traffic between UE and SN.....	111
6.10.5	Handover Procedure .....	112
6.10.6	Signalling procedure for PDCP COUNT check.....	113
6.10.7	Radio link failure recovery .....	113
6.11	Security handling for RRC connection re-establishment procedure.....	113
6.12	Subscription identifier privacy .....	114
6.12.1	Subscription permanent identifier.....	114
6.12.2	Subscription concealed identifier.....	115
6.12.3	Subscription temporary identifier .....	116
6.12.4	Subscription identification procedure .....	117
6.12.5	Subscription identifier de-concealing function (SIDF).....	117
6.13	Signalling procedure for PDCP COUNT check .....	118
6.14	Steering of roaming security mechanism .....	118
6.14.1	General.....	118
6.14.2	Security mechanisms .....	119
6.14.2.1	Procedure for steering of UE in VPLMN during registration .....	119
6.14.2.2	Procedure for steering of UE in VPLMN or HPLMN after registration .....	121
6.14.2.3	SoR Counter .....	122
6.15	UE parameters update via UDM control plane procedure security mechanism .....	123
6.15.1	General.....	123
6.15.2	Security mechanisms .....	123
6.15.2.1	Procedure for UE Parameters Update .....	123
6.15.2.2	UE Parameters Update Counter .....	125
6.16	Security handling in Cellular IoT.....	125
6.16.1	Security handling in Control Plane CIoT 5GS Optimization.....	125
6.16.1.1	Security procedures for Small Data Transfer in Control Plane CIoT 5GS Optimisation.....	125
6.16.1.2	Security procedures for RRCConnectionRe-establishment Procedure in Control Plane CIoT 5GS Optimization.....	126
6.16.2.1	General .....	126
6.16.2.2	Connection Suspend.....	126
6.16.2.3	Connection Resume in CM-IDLE with Suspend to a new ng-eNB .....	127
6.16.2.4	Connection Resume in CM-IDLE with Suspend to the same ng-eNB.....	128
6.16.3	Protection of Non-IP Data Delivery (NIDD) interfaces.....	129
6.16.4	Security handling in NAS based redirection from 5GS to EPS .....	129
6.17	Security mechanism and procedures for L1/L2 Triggered Mobility .....	129
6.17.1	When DC is not configured .....	129
6.17.2	When DC is configured .....	130
7	Security for non-3GPP access to the 5G core network .....	130
7.1	General .....	130
7.1a	Determining trust relationship in the UE.....	131
7.2	Security procedures .....	131
7.2.1	Authentication for Untrusted non-3GPP Access.....	131
7A	Security for trusted non-3GPP access to the 5G core network.....	135
7A.1	General .....	135
7A.2	Security procedures .....	135
7A.2.1	Authentication for trusted non-3GPP access .....	135
7A.2.1.1	General .....	135
7A.2.1.2	Re-authentication for UE moving from one TNAP to another TNAP connecting to the same TNGF .....	138
7A.2.2	Void .....	138
7A.2.3	Key hierarchy for trusted non-3GPP access .....	138
7A.2.4	Authentication for devices that do not support 5GC NAS over WLAN access.....	139
7A.2.4.1	General .....	139
7A.2.4.2	Re-authentication for UE moving from one TNAP to another TNAP connecting to the same TWIF.....	142
7B	Security for wireline access to the 5G core network.....	142
7B.1	General .....	142
7B.2	Authentication for 5G-RG.....	142
7B.3	Authentication for FN-RG.....	144

7B.4	Authentication for UE behind 5G-RG and FN-RG .....	146
7B.5	Subscriber privacy for wireline access .....	146
7B.6	Subscriber privacy for N5CW over trusted WLAN access .....	146
7B.7	Authentication for AUN3 devices behind 5G-RG.....	146
7B.7.1	General.....	146
7B.7.2	Authentication for AUN3 devices not supporting 5G key hierarchy.....	147
7B.7.3	Authentication for AUN3 devices supporting 5G key hierarchy.....	148
8	Security of interworking.....	150
8.1	General .....	150
8.2	Registration procedure for mobility from EPS to 5GS over N26.....	150
8.3	Handover procedure from 5GS to EPS over N26.....	151
8.3.1	General.....	151
8.3.2	Procedure .....	151
8.4	Handover from EPS to 5GS over N26.....	154
8.4.1	General.....	154
8.4.2	Procedure .....	155
8.5	Idle mode mobility from 5GS to EPS over N26.....	157
8.5.1	General.....	157
8.5.2	TAU Procedure.....	158
8.6	Mapping of security contexts .....	159
8.6.1	Mapping of a 5G security context to an EPS security context.....	159
8.6.2	Mapping of an EPS security context to a 5G security context.....	159
8.7	Interworking without N26 interface in single-registration mode .....	160
9	Security procedures for non-service based interfaces .....	160
9.1	General .....	160
9.1.1	Use of NDS/IP .....	160
9.1.2	Implementation requirements .....	160
9.1.3	QoS considerations .....	160
9.2	Security mechanisms for the N2 interface.....	161
9.3	Security requirements and procedures on N3.....	161
9.4	Security mechanisms for the Xn interface.....	161
9.5	Interfaces based on DIAMETER or GTP.....	162
9.5.1	Void .....	162
9.6	Void.....	162
9.7	Void.....	162
9.8	Security mechanisms for protection of the gNB internal interfaces .....	162
9.8.1	General.....	162
9.8.2	Security mechanisms for the F1 interface.....	162
9.8.3	Security mechanisms for the E1 interface.....	163
9.9	Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs.....	163
9.10	Security mechanisms for the interface between W-5GAN and 5GC .....	164
10	Security aspects of IMS emergency session handling.....	164
10.1	General .....	164
10.2	Security procedures and their applicability .....	164
10.2.1	Authenticated IMS Emergency Sessions .....	164
10.2.1.1	General .....	164
10.2.1.2	UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services.....	165
10.2.1.3	UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services.....	165
10.2.2	Unauthenticated IMS Emergency Sessions .....	166
10.2.2.1	General .....	166
10.2.2.2	UE sets up an IMS Emergency session with emergency registration .....	166
10.2.2.3	Key generation for Unauthenticated IMS Emergency Sessions.....	167
10.2.2.3.1	General .....	167
10.2.2.3.2	Handover .....	168
11	Security procedures between UE and external data networks via the 5G Network .....	168
11.1	EAP based secondary authentication by an external DN-AAA server .....	168
11.1.1	General.....	168
11.1.2	Authentication.....	169
11.1.3	Re-Authentication.....	172

11.1.4	Secondary authentication and authorization revocation.....	173
12	Security aspects of Network Exposure Function (NEF) .....	173
12.1	General .....	173
12.2	Mutual authentication.....	173
12.3	Protection of the NEF – AF interface.....	174
12.4	Authorization of Application Function’s requests.....	174
12.5	Support for CAPIF .....	174
13	Service Based Interfaces (SBI).....	174
13.1	Protection at the network or transport layer .....	174
13.1.0	General.....	174
13.1.1	TLS protection between NF and SEPP .....	174
13.1.1.0	General .....	174
13.1.1.1	TLS protection based on telescopic FQDN and wildcard certificate .....	175
13.1.1.2	TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header.....	175
13.1.2	Protection between SEPPs .....	176
13.2	Application layer security on the N32 interface .....	177
13.2.1	General.....	177
13.2.2	N32-c connection between SEPPs .....	178
13.2.2.1	General .....	178
13.2.2.2	Procedure for Key agreement and Parameter exchange .....	179
13.2.2.3	Procedure for error detection and handling in SEPP.....	179
13.2.2.4	N32-f Context .....	180
13.2.2.4.0	N32-f parts.....	180
13.2.2.4.1	N32-f context ID.....	180
13.2.2.4.2	N32-f peer information.....	181
13.2.2.4.3	N32-f security context .....	181
13.2.2.4.4	N32-f context information .....	181
13.2.3	Protection policies for N32 application layer solution .....	182
13.2.3.1	Overview of protection policies .....	182
13.2.3.2	Data-type encryption policy .....	182
13.2.3.3	NF API data-type placement mapping .....	182
13.2.3.4	Modification policy .....	183
13.2.3.5	Provisioning of the policies in the SEPP.....	183
13.2.3.6	Precedence of policies in the SEPP.....	183
13.2.4	N32-f connection between SEPPs .....	184
13.2.4.1	General .....	184
13.2.4.2	Overall Message payload structure for message reformatting at SEPP.....	185
13.2.4.3	Message reformatting in sending SEPP .....	185
13.2.4.3.1	dataToIntegrityProtect.....	185
13.2.4.3.1.1	clearTextEncapsulatedMessage .....	185
13.2.4.3.1.2	metadata .....	185
13.2.4.3.2	dataToIntegrityProtectAndCipher .....	186
13.2.4.4	Protection using JSON Web Encryption (JWE).....	186
13.2.4.4.0	General .....	186
13.2.4.4.1	N32-f key hierarchy.....	186
13.2.4.5	Message modifications by roaming intermediary .....	188
13.2.4.5.1	modifiedDataToIntegrityProtect.....	188
13.2.4.5.2	Modifications by RIs .....	188
13.2.4.5.2a	Error messages originated by Roaming Hub .....	189
13.2.4.6	Protecting RI modifications using JSON Web Signature (JWS) .....	189
13.2.4.7	Message verification by the receiving SEPP.....	189
13.2.4.8	Procedure .....	190
13.2.4.9	JOSE profile.....	193
13.3	Authentication and static authorization .....	193
13.3.0	Static authorization .....	193
13.3.1	Authentication and authorization between network functions and NRF .....	193
13.3.1.1	Direct communication.....	193
13.3.1.2	Indirect communication .....	193
13.3.1.3	Authorization of discovery request and error handling .....	194
13.3.2	Authentication between network functions.....	194

13.3.2.1	Direct communication .....	194
13.3.2.2	Indirect communication .....	195
13.3.2.3	Inter-PLMN NF to NF communication.....	195
13.3.2.4	Error handling .....	195
13.3.3	Authentication between SEPP and network functions.....	195
13.3.4	Authentication and authorization between SEPPs .....	195
13.3.6	Authentication and static authorization between SCP and network functions.....	196
13.3.7	Authentication and static authorization between SCPs.....	196
13.3.8	Client credentials assertion based authentication.....	196
13.3.8.1	General .....	196
13.3.8.2	Client credentials assertion .....	197
13.3.8.3	Verification of Client credentials assertion .....	197
13.4	Authorization of NF service access .....	197
13.4.1	OAuth 2.0 based authorization of Network Function service access.....	197
13.4.1.0	General.....	197
13.4.1.1	Service access authorization within the PLMN.....	198
13.4.1.1.1	OAuth 2.0 roles .....	198
13.4.1.1.2	Service Request Process .....	199
13.4.1.1.3	Access token requests in deployments with several NRFs.....	203
13.4.1.1A	Service access authorization in interconnect scenarios .....	203
13.4.1.2	Service access authorization in roaming scenarios .....	204
13.4.1.2.1	OAuth 2.0 roles .....	204
13.4.1.2.2	Service Request Process .....	204
13.4.1.3	Service access authorization in indirect communication scenarios.....	208
13.4.1.3.1	Authorization for indirect communication without delegated discovery procedure.....	208
13.4.1.3.1.1	With mutual authentication between NF Service Consumer and NRF at the transport layer ..	208
13.4.1.3.1.2	Without mutual authentication between NF and NRF at the transport layer .....	209
13.4.1.3.2	Authorization for indirect communication with delegated discovery procedure.....	211
13.4.1.4	Service access authorization in inter NF mobility scenario .....	212
13.4.1.5	Service access authorization in interconnect and roaming scenarios with indirect communication ...	212
13.4.1.5.1	General .....	212
13.4.1.5.2	Authorization with NF selection at source network.....	212
13.4.1.5.2.1	General .....	212
13.4.1.5.2.2	Authorization for indirect communication with or without delegated discovery procedure .....	212
13.4.1.5.3	Authorization with NF selection at target network .....	214
13.4.1.5.3.1	General.....	214
13.4.1.5.3.2	Authorization for indirect communication without delegated discovery procedure .....	214
13.4.1.5.3.3	Authorization for indirect communication with delegated discovery procedure .....	215
13.5	Security capability negotiation between SEPPs .....	215
14	Security related services.....	217
14.1	Services provided by AUSF .....	217
14.1.1	General.....	217
14.1.2	Nausf_UEAuthentication service.....	217
14.1.2.1	Nausf_UEAuthentication_Authenticate service operation.....	217
14.1.2.2	Nausf_UEAuthentication_deregister service operation .....	217
14.1.2.3	Nausf_UEAuthentication_ProseAuthenticate service operation.....	218
14.1.3	Nausf_SoRProtection service .....	218
14.1.4	Nausf_UPUProtection service .....	218
14.1.5	Void .....	219
14.2	Services provided by UDM .....	219
14.2.1	General.....	219
14.2.2	Nudm_UEAuthentication_Get service operation .....	219
14.2.3	Nudm_UEAuthentication_ResultConfirmation service operation.....	219
14.2.4	Nudm_UEAuthentication_GetProseAv service operation.....	220
14.2.5	Nudm_UEAuthentication_GetGbaAv service operation.....	220
14.2.6	Nudm_UECM_AuthTrigger service operation.....	220
14.2.7	Nudm_UECM_Re-AuthenticationNotification service operation .....	220
14.3	Services provided by NRF .....	220
14.3.1	General.....	220
14.3.2	Nnrf_AccessToken_Get Service Operation.....	220
14.3.3	Nnrf_AccessToken_RetrieveKey Service Operation .....	221

14.4	Services provided by NSSAAF .....	221
14.4.1	Nnssaaf_NSSAA services.....	221
14.4.1.1	General .....	221
14.4.1.2	Nnssaaf_NSSAA_Authenticate service operation .....	221
14.4.1.3	Nnssaaf_NSSAA_Re-AuthenticationNotification service operation .....	222
14.4.1.4	Nnssaaf_NSSAA_RevocationNotification service operation .....	222
14.4.2	Nnssaaf_AIW services.....	222
14.4.2.1	General .....	222
14.4.2.2	Nnssaaf_AIW_Authenticate service operation .....	223
15	Management security for network slices.....	223
15.1	General .....	223
15.2	Mutual authentication.....	223
15.3	Protection of management interactions between the management service consumer and the management service producer .....	223
15.4	Authorization of management service consumer's request .....	224
16	Security procedures for network slices.....	224
16.1	General .....	224
16.2	Authorization for network slice access.....	224
16.3	Network slice specific authentication and authorization .....	225
16.4	AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.....	227
16.5	AAA Server triggered Slice-Specific Authorization Revocation .....	228
16.6	AF Authorization for network slice quota-usage information notification/retrieval .....	229
16.6.1	Introduction.....	229
16.6.2	General.....	229
16.6.3	Subscription/unsubscription procedure of NSACF notification service .....	229
17	Protection of 5GC Signalling Traffic Monitoring .....	231
17.1	General .....	231
17.2	Protection for the configuration and enabling/disabling of signalling monitoring .....	231
17.3	Protection for the streaming of signalling monitoring data .....	232
18	Protection of XRM media related information.....	232
18.1	General .....	232
18.2	Protection of media related information when using connect-UDP .....	232
18.2.1	Using Tunnelling mode .....	232
18.2.2	Security of the QUIC connection between UPF and AS proxy .....	233
18.2.3	Using Forwarded mode.....	233
18.2.4	Security parameters to be used in the Forwarded mode.....	234
18.2.5	Key derivation in the Forwarded mode.....	234
18.2.6	Nonce and counter values in the Forwarded mode .....	234
18.2.7	VCID uniqueness in the forwarding mode .....	234
18.3	Protection of Media related information when using UDP Options.....	235
<b>Annex A (normative): Key derivation functions.....</b>		<b>236</b>
A.1	KDF interface and input parameter construction .....	236
A.1.1	General .....	236
A.1.2	FC value allocations .....	236
A.2	$K_{AUSF}$ derivation function .....	236
A.3	$CK'$ and $IK'$ derivation function .....	236
A.4	$RES^*$ and $XRES^*$ derivation function .....	237
A.5	$HRES^*$ and $HXRES^*$ derivation function .....	237
A.6	$K_{SEAF}$ derivation function .....	237
A.7	$K_{AMF}$ derivation function.....	238
A.7.0	Parameters for the input S to the KDF .....	238
A.7.1	ABBA parameter values.....	238
A.8	Algorithm key derivation functions .....	238

A.9	$K_{gNB}$ , $K_{WAGF}$ , $K_{TNGF}$ , $K_{TWIF}$ and $K_{N3IWF}$ derivation function.....	239
A.10	NH derivation function.....	240
A.11	$K_{NG-RAN}^*$ derivation function for target gNB .....	240
A.12	$K_{NG-RAN}^*$ derivation function for target ng-eNB .....	240
A.13	$K_{AMF}$ to $K_{AMF}'$ derivation in mobility.....	241
A.14	$K_{AMF}$ to $K_{ASME}'$ derivation for interworking .....	241
A.14.1	Idle mode mobility .....	241
A.14.2	Handover .....	241
A.15	$K_{ASME}$ to $K_{AMF}'$ derivation for interworking .....	241
A.15.1	Idle mode mobility .....	241
A.15.2	Handover .....	242
A.16	Derivation of $K_{SN}$ for dual connectivity .....	242
A.17	SoR-MAC- $I_{AUSF}$ generation function .....	242
A.18	SoR-MAC- $I_{UE}/$ SoR-XMAC- $I_{UE}$ generation function .....	243
A.19	UPU-MAC- $I_{AUSF}$ generation function .....	243
A.20	UPU-MAC- $I_{UE}/$ UPU-XMAC- $I_{UE}$ generation function.....	243
A.21	$K_{AMF}$ to $K_{ASME\_SRVCC}$ derivation for interworking .....	244
A.22	$K_{TIPSec}$ , $K_{TNAP}$ and $K_{FT}$ derivation function.....	244
A.23	$K_{IAB}$ generation function .....	244
<b>Annex B (informative): Using additional EAP methods for primary authentication .....</b>		<b>246</b>
B.1	Introduction .....	246
B.2	Primary authentication and key agreement .....	246
B.2.1	EAP TLS .....	246
B.2.1.1	Security procedures.....	246
B.2.1.2	Privacy considerations .....	250
B.2.1.2.1	EAP TLS without subscription identifier privacy.....	250
B.2.1.2.2	EAP TLS with subscription identifier privacy .....	250
B.2.2	Revocation of subscriber certificates .....	251
B.3	Key derivation .....	251
<b>Annex C (normative): Protection schemes for concealing the subscription permanent identifier .....</b>		<b>253</b>
C.1	Introduction .....	253
C.2	Null-scheme .....	253
C.3	Elliptic Curve Integrated Encryption Scheme (ECIES) .....	254
C.3.1	General .....	254
C.3.2	Processing on UE side.....	254
C.3.3	Processing on home network side .....	255
C.3.4	ECIES profiles.....	255
C.3.4.0	General.....	255
C.3.4.1	Profile A .....	256
C.3.4.2	Profile B.....	256
C.4	Implementers' test data .....	257
C.4.1	General .....	257
C.4.2	Null-scheme .....	257
C.4.2.1	IMSI-based SUPI.....	257
C.4.2.2	Network specific identifier-based SUPI .....	257
C.4.3	ECIES Profile A.....	257
C.4.3.1	IMSI-based SUPI.....	257

C.4.3.2	Network specific identifier-based SUPI .....	258
C.4.4	ECIES Profile B .....	259
C.4.4.1	IMSI-based SUPI.....	259
C.4.4.2	Network specific identifier-based SUPI .....	260
<b>Annex D (normative): Algorithms for ciphering and integrity protection.....</b>		<b>261</b>
D.1	Null ciphering and integrity protection algorithms .....	261
D.2	Ciphering algorithms .....	261
D.2.1	128-bit Ciphering algorithms .....	261
D.2.1.1	Inputs and outputs.....	261
D.2.1.2	128-NEA1 .....	262
D.2.1.3	128-NEA2.....	262
D.2.1.4	128-NEA3.....	262
D.3	Integrity algorithms .....	262
D.3.1	128-Bit integrity algorithms .....	262
D.3.1.1	Inputs and outputs.....	262
D.3.1.2	128-NIA1 .....	263
D.3.1.3	128-NIA2.....	263
D.3.1.4	128-NIA3.....	263
D.4	Test Data for the security algorithms .....	263
D.4.1	General .....	263
D.4.2	128-NEA1 .....	263
D.4.3	128-NIA1 .....	263
D.4.4	128-NEA2 .....	263
D.4.5	128-NIA2 .....	264
D.4.6	128-NEA3 .....	264
D.4.7	128-NIA3 .....	264
<b>Annex E (informative): UE-assisted network-based detection of false base station.....</b>		<b>265</b>
E.1	Introduction .....	265
E.2	Examples of using measurement reports.....	265
<b>Annex F (normative): 3GPP 5G profile for EAP-AKA' .....</b>		<b>266</b>
F.1	Introduction .....	266
F.2	Subscriber privacy.....	266
F.3	Subscriber identity and key derivation.....	267
F.4	Void.....	267
<b>Annex G (informative): Application layer security on the N32 interface.....</b>		<b>267</b>
G.1	Introduction .....	267
G.2	Structure of HTTP Message .....	268
<b>Annex H (informative): Void.....</b>		<b>270</b>
<b>Annex I (normative): Non-public networks .....</b>		<b>271</b>
I.1	General .....	271
I.2	Authentication in standalone non-public networks .....	271
I.2.1	General .....	271
I.2.2	EAP framework, selection of authentication method, and EAP method credentials.....	271
I.2.2.1	General.....	271
I.2.2.2	Credentials holder using AAA server for primary authentication .....	272
I.2.2.2.1	General.....	272
I.2.2.2.2	Procedure .....	272
I.2.3	Key hierarchy, key derivation and key distribution.....	274

I.2.3.1	General.....	274
I.2.3.2	Credentials holder using AAA server for primary authentication .....	275
I.2.4	Credentials Holder using AUSF and UDM for primary authentication.....	275
I.3	Serving network name for standalone non-public networks .....	275
I.3.1	General .....	275
I.3.2	Definition of SN Id for standalone non-public networks .....	276
I.4	Modification of CAG ID list in the UE.....	276
I.5	SUPI privacy for standalone non-public networks.....	276
I.6	Authentication in Public Network Integrated Non-Public Networks (PNI-NPN).....	276
I.7	Authorization aspects in SNPNs .....	276
I.7.1	Credentials holder using AUSF and UDM for primary authentication .....	276
I.8	SEPP and interconnect related security procedures .....	277
I.8.1	Credentials holder using AUSF and UDM for primary authentication .....	277
I.9	Security of UE onboarding in SNPNs .....	277
I.9.1	General .....	277
I.9.2	Authentication .....	277
I.9.2.1	Requirements .....	277
I.9.2.2	Primary authentication without using DCS .....	277
I.9.2.3	Primary authentication using DCS.....	278
I.9.2.4	Secondary authentication.....	278
I.9.2.4.1	Secondary authentication using DCS.....	278
I.9.2.4.2	Secondary authentication using DN-AAA .....	278
I.10	Security for access to SNPN services via Non-3GPP access .....	278
I.10.1	General .....	278
I.10.2	Security for access to SNPN services via Untrusted non-3GPP access.....	278
I.10.2.0	General.....	278
I.10.2.1	Untrusted non-3GPP access support in SNPN without CH .....	278
I.10.2.2	Untrusted non-3GPP access support in SNPN with CH .....	279
I.10.3	Security for access to SNPN services via Trusted non-3GPP access .....	279
I.10.3.0	General.....	279
I.10.3.1	Trusted non-3GPP access support in SNPN without CH.....	280
I.10.3.2	Trusted non-3GPP access support in SNPN with CH.....	280
I.10.4	Security for access to SNPN services for N5CW devices .....	281
I.10.4.0	General.....	281
I.10.4.1	Support for N5CW devices in SNPN without CH .....	281
I.10.4.2	Support for N5CW devices in SNPN with CH .....	281
I.10.5	Security for NSW0 support in SNPN .....	282
I.10.5.1	NSWO support in SNPN using CH with AAA server .....	282
I.10.5.1.1	NSWO support in SNPN using CH with AAA server via AAA Proxies .....	282
I.10.5.1.2	NSWO support in SNPN using CH with AAA server via 5GC .....	282
I.10.5.2	NSWO support in SNPN without CH.....	283
I.10.5.3	NSWO support in SNPN using CH with AUSF/UDM.....	283
I.11	Security for accessing a localised service .....	283
<b>Annex J (normative): SRVCC from 5G to UTRAN.....</b>		<b>284</b>
J.1	SRVCC from NR to UTRAN.....	284
J.1.1	General.....	284
J.1.2	Procedure.....	284
J.2	Emergency call in SRVCC from NR to UTRAN.....	285
J.2.1	General.....	285
J.2.2	Procedure.....	285
<b>Annex K (normative): Security for 5GLAN services .....</b>		<b>286</b>
K.1	General .....	286