

ETSI TS 133 501 V17.13.0 (2024-04)



5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 17.13.0 Release 17)

Document Preview

[ETSI TS 133 501 V17.13.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/f2fcdc3a-d7cc-416e-874f-83bb6fb3a0e2/etsi-ts-133-501-v17-13-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/f2fcdc3a-d7cc-416e-874f-83bb6fb3a0e2/etsi-ts-133-501-v17-13-0-2024-04>



ReferenceRTS/TSGS-0333501vhd0

Keywords5G

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:

<https://www.etsi.org/standards-search>

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

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

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

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

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

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 2024.
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 Web server (<https://ipr.etsi.org/>).

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™** and **LTE™** 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. (2024-04)

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

Modal verbs terminology

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

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

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
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	236
G.1	Introduction	236
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