

ETSI TS 133 501 V16.7.1 (2021-08)



5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.7.1 Release 16)

<https://standards.iteh.ai/catalog/standards/sist/836df603-6a86-4794-9bf2-469cf727a10/etsi-ts-133-501-v16-7-1-2021-08>



ReferenceRTS/TSGS-0333501vg71

Keywords

5G, SECURITY

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Important notice

ETSI TS 133 501 V16.7.1 (2021-08)
<https://standards.iteh.ai/catalog/standards/sist/836df603-6a86-4794-9bf2-469c8177a10f/etsi-ts-133-501-v16-7-1-2021-08>
The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the 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>

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 2021.

All rights reserved.

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.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

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

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.

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 under <http://webapp.etsi.org/key/queryform.asp>.

<https://standards.iteh.ai/catalog/standards/sist/836df603-6a86-4794-9bf2-469cdf727a10/etsi-ts-133-501-v16-7-1-2021-08>

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.....	15
1 Scope	16
2 References	16
3 Definitions and abbreviations.....	19
3.1 Definitions	19
3.2 Abbreviations	22
4 Overview of security architecture	24
4.1 Security domains	24
4.2 Security at the perimeter of the 5G Core network	25
4.2.1 Security Edge Protection Proxy (SEPP)	25
4.2.2 Inter-PLMN UP Security (IPUPS).....	25
4.3 Security entities in the 5G Core network.....	26
5 Security requirements and features	26
5.1 General security requirements	26
5.1.1 Mitigation of bidding down attacks	26
5.1.2 Authentication and Authorization	26
5.1.3 Requirements on 5GC and NG-RAN related to keys	27
5.2 Requirements on the UE.....	27
5.2.1 General.....	27
5.2.2 User data and signalling data confidentiality	27
5.2.3 User data and signalling data integrity	27
5.2.4 Secure storage and processing of subscription credentials.....	28
5.2.5 Subscriber privacy	28
5.3 Requirements on the gNB	29
5.3.1 General.....	29
5.3.2 User data and signalling data confidentiality	29
5.3.3 User data and signalling data integrity.....	29
5.3.4 Requirements for the gNB setup and configuration.....	30
5.3.5 Requirements for key management inside the gNB.....	30
5.3.6 Requirements for handling user plane data for the gNB	30
5.3.7 Requirements for handling control plane data for the gNB	30
5.3.8 Requirements for secure environment of the gNB.....	31
5.3.9 Requirements for the gNB F1 interfaces.....	31
5.3.10 Requirements for the gNB E1 interfaces	31
5.4 Requirements on the ng-eNB	31
5.5 Requirements on the AMF	31
5.5.1 Signalling data confidentiality	31
5.5.2 Signalling data integrity	32
5.5.3 Subscriber privacy	32
5.6 Requirements on the SEAF	32
5.7 Void.....	32
5.8 Requirements on the UDM.....	32
5.8.1 Generic requirements.....	32
5.8.2 Subscriber privacy related requirements to UDM and SIDF	32
5.8a Requirements on AUSF.....	33
5.9 Core network security	33
5.9.1 Trust boundaries	33
5.9.2 Requirements on service-based architecture.....	33
5.9.2.1 Security Requirements for service registration, discovery and authorization	33
5.9.2.2 NRF security requirements	33

5.9.2.3	NEF security requirements.....	34
5.9.2.4	Requirements on the Service Communication Proxy (SCP)	34
5.9.3	Requirements for e2e core network interconnection security	34
5.9.3.1	General	34
5.9.3.2	Requirements for Security Edge Protection Proxy (SEPP)	35
5.9.3.3	Protection of attributes	35
5.9.3.4	Requirements for IPUPS functionality	36
5.10	Visibility and configurability	36
5.10.1	Security visibility	36
5.10.2	Security configurability	36
5.11	Requirements for algorithms, and algorithm selection	36
5.11.1	Algorithm identifier values	36
5.11.1.1	Ciphering algorithm identifier values.....	36
5.11.1.2	Integrity algorithm identifier values.....	37
5.11.2	Requirements for algorithm selection	37
5.12	Requirements on 5G-RG	38
5.13	Requirements on NSSAAF	38
6	Security procedures between UE and 5G network functions	38
6.0	General	38
6.1	Primary authentication and key agreement	38
6.1.1	Authentication framework	38
6.1.1.1	General	38
6.1.1.2	EAP framework.....	39
6.1.1.3	Granularity of anchor key binding to serving network.....	39
6.1.1.4	Construction of the serving network name.....	40
6.1.1.4.1	Serving network name	40
6.1.1.4.2	Construction of the serving network name by the UE	40
6.1.1.4.3	Construction of the serving network name by the SEAF	40
6.1.2	Initiation of authentication and selection of authentication method	40
6.1.3	Authentication procedures	42
6.1.3.1	Authentication procedure for EAP-AKA	42
6.1.3.2	Authentication procedure for 5G AKA	44
6.1.3.2.0	5G AKA	44
6.1.3.2.1	Void	46
6.1.3.2.2	RES* verification failure in SEAF or AUSF or both	46
6.1.3.3	Synchronization failure or MAC failure	46
6.1.3.3.1	Synchronization failure or MAC failure in USIM	46
6.1.3.3.2	Synchronization failure recovery in Home Network	46
6.1.4	Linking increased home control to subsequent procedures	47
6.1.4.1	Introduction	47
6.1.4.1a	Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	48
6.1.4.2	Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	48
6.2	Key hierarchy, key derivation, and distribution scheme	49
6.2.1	Key hierarchy.....	49
6.2.2	Key derivation and distribution scheme.....	51
6.2.2.1	Keys in network entities	51
6.2.2.2	Keys in the UE	53
6.2.3	Handling of user-related keys	55
6.2.3.1	Key setting	55
6.2.3.2	Key identification.....	55
6.2.3.3	Key lifetimes	56
6.3	Security contexts	57
6.3.1	Distribution of security contexts	57
6.3.1.1	General	57
6.3.1.2	Distribution of subscriber identities and security data within one 5G serving network domain	57
6.3.1.3	Distribution of subscriber identities and security data between 5G serving network domains	57
6.3.1.4	Distribution of subscriber identities and security data between 5G and EPS serving network domains	57
6.3.2	Multiple registrations in same or different serving networks	58
6.3.2.0	General	58

6.3.2.1	Multiple registrations in different PLMNs.....	58
6.3.2.2	Multiple registrations in the same PLMN	58
6.4	NAS security mechanisms.....	58
6.4.1	General.....	58
6.4.2	Security for multiple NAS connections	59
6.4.2.1	Multiple active NAS connections with different PLMNs	59
6.4.2.2	Multiple active NAS connections in the same PLMN's serving network	59
6.4.3	NAS integrity mechanisms	60
6.4.3.0	General	60
6.4.3.1	NAS input parameters to integrity algorithm	60
6.4.3.2	NAS integrity activation	61
6.4.3.3	NAS integrity failure handling.....	61
6.4.4	NAS confidentiality mechanisms	61
6.4.4.0	General.....	61
6.4.4.1	NAS input parameters to confidentiality algorithm	61
6.4.4.2	NAS confidentiality activation.....	61
6.4.5	Handling of NAS COUNTs.....	61
6.4.6	Protection of initial NAS message	62
6.4.7	Security aspects of SMS over NAS	63
6.5	RRC security mechanisms.....	63
6.5.1	RRC integrity mechanisms	63
6.5.2	RRC confidentiality mechanisms	64
6.5.3	RRC UE capability transfer procedure	64
6.6	UP security mechanisms	64
6.6.1	UP security policy.....	64
6.6.2	UP security activation mechanism.....	65
6.6.3	UP confidentiality mechanisms.....	66
6.6.4	UP integrity mechanisms	66
6.7	Security algorithm selection, key establishment and security mode command procedure.....	67
6.7.1	Procedures for NAS algorithm selection	67
6.7.1.1	Initial NAS security context establishment	67
6.7.1.2	AMF change.....	67
6.7.2	NAS security mode command procedure.....	67
6.7.3	Procedures for AS algorithm selection.....	69
6.7.3.0	Initial AS security context establishment.....	69
6.7.3.1	Xn-handover.....	69
6.7.3.2	N2-handover.....	69
6.7.3.3	Intra-gNB-CU handover/intra-ng-eNB handover.....	70
6.7.3.4	Transitions from RRC_INACTIVE to RRC_CONNECTED states	70
6.7.3.5	RNA Update procedure.....	70
6.7.3.6	Algorithm negotiation for unauthenticated UEs in LSM	70
6.7.4	AS security mode command procedure	71
6.8	Security handling in state transitions.....	72
6.8.1	Key handling at connection and registration state transitions.....	72
6.8.1.1	Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states	72
6.8.1.1.0	General	72
6.8.1.1.1	Transition from RM-REGISTERED to RM-DEREGISTERED	72
6.8.1.1.2	Transition from RM-DEREGISTERED to RM-REGISTERED	73
6.8.1.1.2.1	General.....	73
6.8.1.1.2.2	Full native 5G NAS security context available.....	74
6.8.1.1.2.3	Full native 5G NAS security context not available.....	74
6.8.1.1.2.4	UE registration over a second access type to the same AMF	75
6.8.1.2	Key handling at transitions between CM-IDLE and CM-CONNECTED states	75
6.8.1.2.0	General	75
6.8.1.2.1	Transition from CM-IDLE to CM-CONNECTED.....	75
6.8.1.2.2	Establishment of keys for cryptographically protected radio bearers in 3GPP access	76
6.8.1.2.3	Establishment of keys for cryptographically protected traffic in non-3GPP access	76
6.8.1.2.4	Transition from CM-CONNECTED to CM-IDLE.....	77
6.8.1.3	Key handling for the Registration procedure when registered in NG-RAN.....	77
6.8.2	Security handling at RRC state transitions	78
6.8.2.1	Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states.....	78
6.8.2.1.1	General	78

6.8.2.1.2	State transition from RRC_CONNECTED to RRC_INACTIVE.....	78
6.8.2.1.3	State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB	78
6.8.2.1.4	State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB	80
6.8.2.2	Key handling during mobility in RRC_INACTIVE state	80
6.8.2.2.1	General	80
6.8.2.2.2	RAN-based notification area update to a new gNB/ng-eNB	80
6.8.2.2.3	RAN-based notification area update to the same gNB/ng-eNB	80
6.9	Security handling in mobility	81
6.9.1	Void	81
6.9.2	Key handling in handover.....	81
6.9.2.1	General	81
6.9.2.1.1	Access stratum.....	81
6.9.2.1.2	Non access stratum	82
6.9.2.2	Key derivations for context modification procedure	82
6.9.2.3	Key derivations during handover	83
6.9.2.3.1	Intra-gNB-CU handover and intra-ng-eNB handover	83
6.9.2.3.2	Xn-handover	83
6.9.2.3.3	N2-Handover	84
6.9.2.3.4	UE handling.....	85
6.9.3	Key handling in mobility registration update	86
6.9.4	Key-change-on-the-fly.....	88
6.9.4.1	General	88
6.9.4.2	NAS key re-keying.....	88
6.9.4.3	NAS key refresh.....	88
6.9.4.4	AS key re-keying	89
6.9.4.5	AS key refresh.....	89
6.9.5	Rules on concurrent running of security procedures	90
6.9.5.1	Rules related to AS and NAS security context synchronization	90
6.9.5.2	Rules related to parallel NAS connections	90
6.9.6	Security handling in registration with AMF reallocation via direct NAS reroute.....	90
6.10	Dual connectivity	91
6.10.1	Introduction.....	91
6.10.1.1	General	91
6.10.1.2	Dual Connectivity protocol architecture for MR-DC with 5GC	91
6.10.2	Security mechanisms and procedures for DC	92
6.10.2.1	SN Addition or modification.....	92
6.10.2.2	Secondary Node key update.....	93
6.10.2.2.1	General	93
6.10.2.2.2	MN initiated	93
6.10.2.2.3	SN initiated.....	93
6.10.2.3	SN release and change	94
6.10.3	Establishing the security context between the UE and SN	94
6.10.3.1	SN Counter maintenance.....	94
6.10.3.2	Derivation of keys	94
6.10.3.3	Negotiation of security algorithms.....	94
6.10.4	Protection of traffic between UE and SN.....	95
6.10.5	Handover Procedure	96
6.10.6	Signalling procedure for PDCP COUNT check.....	96
6.10.7	Radio link failure recovery	96
6.11	Security handling for RRC connection re-establishment procedure.....	96
6.12	Subscription identifier privacy	98
6.12.1	Subscription permanent identifier.....	98
6.12.2	Subscription concealed identifier.....	98
6.12.3	Subscription temporary identifier	99
6.12.4	Subscription identification procedure	100
6.12.5	Subscription identifier de-concealing function (SIDF).....	100
6.13	Signalling procedure for PDCP COUNT check	100
6.14	Steering of roaming security mechanism	101
6.14.1	General.....	101
6.14.2	Security mechanisms	102
6.14.2.1	Procedure for steering of UE in VPLMN during registration	102
6.14.2.2	Procedure for steering of UE in VPLMN or HPLMN after registration	103

6.14.2.3	SoR Counter	105
6.15	UE parameters update via UDM control plane procedure security mechanism	105
6.15.1	General	105
6.15.2	Security mechanisms	106
6.15.2.1	Procedure for UE Parameters Update	106
6.15.2.2	UE Parameters Update Counter	107
6.16	Security handling in Cellular IoT	108
6.16.1	Security handling in Control Plane CIoT 5GS Optimization	108
6.16.1.1	Security procedures for Small Data Transfer in Control Plane CIoT 5GS Optimisation	108
6.16.1.2	Security procedures for RRCConnectionRe-establishment Procedure in Control Plane CIoT 5GS Optimization	108
6.16.2.1	General	109
6.16.2.2	Connection Suspend	109
6.16.2.3	Connection Resume in CM-IDLE with Suspend to a new ng-eNB	109
6.16.2.4	Connection Resume in CM-IDLE with Suspend to the same ng-eNB	111
6.16.3	Protection of Non-IP Data Delivery (NIDD) interfaces	111
6.16.4	Security handling in NAS based redirection from 5GS to EPS	111
7	Security for non-3GPP access to the 5G core network	112
7.1	General	112
7.1a	Determining trust relationship in the UE	112
7.2	Security procedures	112
7.2.1	Authentication for Untrusted non-3GPP Access	112
7A	Security for trusted non-3GPP access to the 5G core network	115
7A.1	General	115
7A.2	Security procedures	116
7A.2.1	Authentication for trusted non-3GPP access	116
7A.2.2	Mobility handling for trusted non-3GPP access	119
7A.2.3	Key hierarchy for trusted non-3GPP access	119
7A.2.4	Authentication for devices that do not support 5GC NAS over WLAN access	119
7B	Security for wireline access to the 5G core network	122
7B.1	General	122
7B.2	Authentication for 5G-RG	122
7B.3	Authentication for FN-RG	124
7B.4	Authentication for UE behind 5G-RG and FN-RG	126
7B.5	Subscriber privacy for wireline access	126
7B.6	Subscriber privacy for N5CW over trusted WLAN access	126
8	Security of interworking	126
8.1	General	126
8.2	Registration procedure for mobility from EPS to 5GS over N26	127
8.3	Handover procedure from 5GS to EPS over N26	128
8.3.1	General	128
8.3.2	Procedure	128
8.4	Handover from EPS to 5GS over N26	131
8.4.1	General	131
8.4.2	Procedure	132
8.5	Idle mode mobility from 5GS to EPS over N26	134
8.5.1	General	134
8.5.2	TAU Procedure	135
8.6	Mapping of security contexts	136
8.6.1	Mapping of a 5G security context to an EPS security context	136
8.6.2	Mapping of an EPS security context to a 5G security context	136
8.7	Interworking without N26 interface in single-registration mode	137
9	Security procedures for non-service based interfaces	137
9.1	General	137
9.1.1	Use of NDS/IP	137
9.1.2	Implementation requirements	137
9.1.3	QoS considerations	137
9.2	Security mechanisms for the N2 interface	137
9.3	Security requirements and procedures on N3	138

9.4	Security mechanisms for the Xn interface.....	138
9.5	Interfaces based on DIAMETER or GTP.....	139
9.5.1	Void.....	139
9.6	Void.....	139
9.7	Void.....	139
9.8	Security mechanisms for protection of the gNB internal interfaces.....	139
9.8.1	General.....	139
9.8.2	Security mechanisms for the F1 interface.....	139
9.8.3	Security mechanisms for the E1 interface.....	140
9.9	Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs.....	140
9.10	Security mechanisms for the interface between W-5GAN and 5GC.....	140
10	Security aspects of IMS emergency session handling.....	141
10.1	General.....	141
10.2	Security procedures and their applicability.....	141
10.2.1	Authenticated IMS Emergency Sessions.....	141
10.2.1.1	General.....	141
10.2.1.2	UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services.....	141
10.2.1.3	UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services.....	141
10.2.2	Unauthenticated IMS Emergency Sessions.....	142
10.2.2.1	General.....	142
10.2.2.2	UE sets up an IMS Emergency session with emergency registration.....	143
10.2.2.3	Key generation for Unauthenticated IMS Emergency Sessions.....	144
10.2.2.3.1	General.....	144
10.2.2.3.2	Handover.....	144
11	Security procedures between UE and external data networks via the 5G Network.....	145
11.1	EAP based secondary authentication by an external DN-AAA server.....	145
11.1.1	General.....	145
11.1.2	Authentication.....	146
11.1.3	Re-Authentication.....	149
12	Security aspects of Network Exposure Function (NEF) (2021-08).....	150
12.1	General.....	150
12.2	Mutual authentication.....	150
12.3	Protection of the NEF – AF interface.....	150
12.4	Authorization of Application Function's requests.....	150
12.5	Support for CAPIF.....	151
13	Service Based Interfaces (SBI).....	151
13.1	Protection at the network or transport layer.....	151
13.1.0	General.....	151
13.1.1	TLS protection between NF and SEPP.....	151
13.1.1.0	General.....	151
13.1.1.1	TLS protection based on telescopic FQDN and wildcard certificate.....	151
13.1.1.2	TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header.....	152
13.1.2	Protection between SEPPs.....	152
13.2	Application layer security on the N32 interface.....	153
13.2.1	General.....	153
13.2.2	N32-c connection between SEPPs.....	154
13.2.2.1	General.....	154
13.2.2.2	Procedure for Key agreement and Parameter exchange.....	155
13.2.2.3	Procedure for error detection and handling in SEPP.....	155
13.2.2.4	N32-f Context.....	156
13.2.2.4.0	N32-f parts.....	156
13.2.2.4.1	N32-f context ID.....	156
13.2.2.4.2	N32-f peer information.....	157
13.2.2.4.3	N32-f security context.....	157
13.2.2.4.4	N32-f context information.....	157
13.2.3	Protection policies for N32 application layer solution.....	157
13.2.3.1	Overview of protection policies.....	157
13.2.3.2	Data-type encryption policy.....	158
13.2.3.3	NF API data-type placement mapping.....	158

13.2.3.4	Modification policy	158
13.2.3.5	Provisioning of the policies in the SEPP.....	159
13.2.3.6	Precedence of policies in the SEPP	159
13.2.4	N32-f connection between SEPPs	160
13.2.4.1	General	160
13.2.4.2	Overall Message payload structure for message reformatting at SEPP.....	160
13.2.4.3	Message reformatting in sending SEPP	161
13.2.4.3.1	dataToIntegrityProtect	161
13.2.4.3.1.1	clearTextEncapsulatedMessage	161
13.2.4.3.1.2	metadata	161
13.2.4.3.2	dataToIntegrityProtectAndCipher	162
13.2.4.4	Protection using JSON Web Encryption (JWE).....	162
13.2.4.4.0	General	162
13.2.4.4.1	N32-f key hierarchy.....	162
13.2.4.5	Message modifications in IPX	163
13.2.4.5.1	modifiedDataToIntegrityProtect.....	163
13.2.4.5.2	Modifications by IPX	164
13.2.4.6	Protecting IPX modifications using JSON Web Signature (JWS)	164
13.2.4.7	Message verification by the receiving SEPP.....	165
13.2.4.8	Procedure	165
13.2.4.9	JOSE profile	168
13.3	Authentication and static authorization	168
13.3.0	Static authorization	168
13.3.1	Authentication and authorization between network functions and NRF	168
13.3.1.1	Direct communication.....	168
13.3.1.2	Indirect communication	168
13.3.1.3	Authorization of discovery request and error handling	169
13.3.2	Authentication and authorization between network functions	169
13.3.2.1	Direct communication.....	169
13.3.2.2	Indirect communication	169
13.3.2.3	Inter-PLMN NF to NF communication.....	170
13.3.2.4	Error handling	170
13.3.3	Authentication and authorization between SEPP and network functions	170
13.3.4	Authentication and authorization between SEPPs	170
13.3.6	Authentication and authorization between SCP and network functions	170
13.3.7	Authentication and authorization between SCPs	171
13.3.8	Client credentials assertion based authentication.....	171
13.3.8.1	General	171
13.3.8.2	Client credentials assertion	171
13.3.8.3	Verification of Client credentials assertion	172
13.4	Authorization of NF service access	172
13.4.1	OAuth 2.0 based authorization of Network Function service access.....	172
13.4.1.0	General	172
13.4.1.1	Service access authorization within the PLMN.....	173
13.4.1.1.1	OAuth 2.0 roles	173
13.4.1.1.2	Service Request Process	173
13.4.1.2	Service access authorization in roaming scenarios	176
13.4.1.2.1	OAuth 2.0 roles	176
13.4.1.2.2	Service Request Process	176
13.4.1.3	Service access authorization in indirect communication scenarios.....	179
13.4.1.3.1	Authorization for indirect communication without delegated discovery procedure.....	179
13.4.1.3.1.1	With mutual authentication between NF Service Consumer and NRF at the transport layer ..	179
13.4.1.3.1.2	Without mutual authentication between NF and NRF at the transport layer	181
13.4.1.3.2	Authorization for indirect communication with delegated discovery procedure.....	182
13.5	Security capability negotiation between SEPPs	183
14	Security related services.....	184
14.1	Services provided by AUSF	184
14.1.1	General.....	184
14.1.2	Nausf_UEAuthentication service.....	184
14.1.3	Nausf_SoRProtection service	185
14.1.4	Nausf_UPUProtection service	185

14.1.5	Nausf_UEAuthentication_deregister service operation.....	185
14.2	Services provided by UDM.....	186
14.2.1	General.....	186
14.2.2	Nudm_UEAuthentication_Get service operation	186
14.2.3	Nudm_UEAuthentication_ResultConfirmation service operation.....	186
14.3	Services provided by NRF	186
14.3.1	General.....	186
14.3.2	Nnrf_AccessToken_Get Service Operation.....	187
14.4	Services provided by NSSAAF	187
14.4.1	Nnssaaf_NSSAA services.....	187
14.4.1.1	General	187
14.4.1.2	Nnssaaf_NSSAA_Authenticate service operation	187
14.4.1.3	Nnssaaf_NSSAA_Re-AuthenticationNotification service operation.....	188
14.4.1.4	Nnssaaf_NSSAA_RevocationNotification service operation	188
15	Management security for network slices.....	188
15.1	General	188
15.2	Mutual authentication.....	188
15.3	Protection of management interactions between the management service consumer and the management service producer	189
15.4	Authorization of management service consumer's request	189
16	Security procedures for network slices.....	189
16.1	General	189
16.2	Authorization for network slice access.....	189
16.3	Network slice specific authentication and authorization	190
16.4	AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.....	192
16.5	AAA Server triggered Slice-Specific Authorization Revocation	193
Annex A (normative):	Key derivation functions.....	195
A.1	KDF interface and input parameter construction	195
A.1.1	General	195
A.1.2	FC value allocations.....	195
A.2	K_{AUSF} derivation function.....	195
A.3	CK' and IK' derivation function	195
A.4	RES^* and XRES^* derivation function	196
A.5	HRES^* and HXRES^* derivation function	196
A.6	K_{SEAF} derivation function	196
A.7	K_{AMF} derivation function.....	197
A.7.0	Parameters for the input S to the KDF	197
A.7.1	ABBA parameter values.....	197
A.8	Algorithm key derivation functions	197
A.9	K_{gNB} , K_{WAGF} , K_{TNGF} , K_{TWIF} and K_{N3IWF} derivation function.....	198
A.10	NH derivation function.....	199
A.11	$K_{\text{NG-RAN}}^*$ derivation function for target gNB	199
A.12	$K_{\text{NG-RAN}}^*$ derivation function for target ng-eNB	199
A.13	K_{AMF} to K_{AMF}' derivation in mobility.....	200
A.14	K_{AMF} to K_{ASME}' derivation for interworking	200
A.14.1	Idle mode mobility	200
A.14.2	Handover	200
A.15	K_{ASME} to K_{AMF}' derivation for interworking	200
A.15.1	Idle mode mobility	200
A.15.2	Handover	201

A.16	Derivation of K_{SN} for dual connectivity	201
A.17	SoR-MAC- I_{AUSF} generation function	201
A.18	SoR-MAC- I_{UE} generation function	202
A.19	UPU-MAC- I_{AUSF} generation function	202
A.20	UPU-MAC- I_{UE} generation function	202
A.21	K_{AMF} to K_{ASME_SRVCC} derivation for interworking	203
A.22	K_{TIPSec} and K_{TNAP} derivation function.....	203
A.23	K_{IAB} generation function	203
Annex B (informative): Using additional EAP methods for primary authentication		204
B.1	Introduction	204
B.2	Primary authentication and key agreement	204
B.2.1	EAP TLS	204
B.2.1.1	Security procedures.....	204
B.2.1.2	Privacy considerations	207
B.2.1.2.1	EAP TLS without subscription identifier privacy	207
B.2.1.2.2	EAP TLS with subscription identifier privacy	207
B.2.2	Revocation of subscriber certificates	208
B.3	Key derivation	208
Annex C (normative): Protection schemes for concealing the subscription permanent identifier.....		210
C.1	Introduction	210
C.2	Null-scheme	210
C.3	Elliptic Curve Integrated Encryption Scheme (ECIES)	211
C.3.1	General	211
C.3.2	Processing on UE side	211
C.3.3	Processing on home network side	212
C.3.4	ECIES profiles.....	212
C.3.4.0	General.....	212
C.3.4.1	Profile A	213
C.3.4.2	Profile B.....	213
C.4	Implementers' test data	214
C.4.1	General	214
C.4.2	Null-scheme	214
C.4.2.1	IMSI-based SUPI.....	214
C.4.2.2	Network specific identifier-based SUPI	214
C.4.3	ECIES Profile A	214
C.4.3.1	IMSI-based SUPI.....	214
C.4.3.2	Network specific identifier-based SUPI	215
C.4.4	ECIES Profile B	216
C.4.4.1	IMSI-based SUPI.....	216
C.4.4.2	Network specific identifier-based SUPI	217
Annex D (normative): Algorithms for ciphering and integrity protection		218
D.1	Null ciphering and integrity protection algorithms	218
D.2	Ciphering algorithms.....	218
D.2.1	128-bit Ciphering algorithms	218
D.2.1.1	Inputs and outputs.....	218
D.2.1.2	128-NEA1.....	219
D.2.1.3	128-NEA2.....	219
D.2.1.4	128-NEA3.....	219

D.3	Integrity algorithms	219
D.3.1	128-Bit integrity algorithms	219
D.3.1.1	Inputs and outputs.....	219
D.3.1.2	128-NIA1	220
D.3.1.3	128-NIA2	220
D.3.1.4	128-NIA3	220
D.4	Test Data for the security algorithms	220
D.4.1	General	220
D.4.2	128-NEA1	220
D.4.3	128-NIA1	220
D.4.4	128-NEA2	220
D.4.5	128-NIA2	221
D.4.6	128-NEA3	221
D.4.7	128-NIA3	221
Annex E (informative):	UE-assisted network-based detection of false base station.....	222
E.1	Introduction	222
E.2	Examples of using measurement reports.....	222
Annex F (normative):	3GPP 5G profile for EAP-AKA'	223
F.1	Introduction	223
F.2	Subscriber privacy	223
F.3	Subscriber identity and key derivation.....	224
F.4	Void.....	224
Annex G (informative):	Application layer security on the N32 interface.....	225
G.1	Introduction	225
G.2	Structure of HTTP Message	225
Annex H (informative):	Void	227
Annex I (normative):	Non-public networks.....	228
I.1	General	228
I.2	Authentication in standalone non-public networks	228
I.2.1	General	228
I.2.2	EAP framework, selection of authentication method, and EAP method credentials.....	228
I.2.3	Key hierarchy, key derivation and key distribution.....	228
I.3	Serving network name for standalone non-public networks	229
I.3.1	General	229
I.3.2	Definition of SN Id for standalone non-public networks	229
I.4	Modification of CAG ID list in the UE	229
I.5	SUPI privacy for standalone non-public networks.....	230
I.6	Authentication in Public Network Integrated Non-Public Networks (PNI-NPN).....	230
Annex J (normative):	SRVCC from 5G to UTRAN.....	231
J.1	SRVCC from NR to UTRAN.....	231
J.1.1	General.....	231
J.1.2	Procedure	231
J.2	Emergency call in SRVCC from NR to UTRAN.....	232
J.2.1	General.....	232
J.2.2	Procedure	232

Annex K (normative):	Security for 5GLAN services	233
K.1	General	233
K.2	Authentication and authorization	233
K.3	Handling of UP security policy	233
Annex L (normative):	Security for TSC service.....	234
L.1	General	234
L.2	Access security for a 5GS TSC-enabled UE	234
L.3	Protection of user plane data in TSC including gTP control messages	234
Annex M (normative):	Security for Integrated Access and Backhaul (IAB).....	235
M.1	General	235
M.2	Security requirements and features	235
M.2.1	Requirements on the IAB-node (IAB-UE)	235
M.2.2	Requirements on the IAB donor.....	235
M.2.3	Requirements on the 5GC supporting IAB architecture.....	235
M.2.4	Requirements for secure environment.....	235
M.2.5	Requirements on the F1 interface.....	235
M.3	IAB-node Integration Procedure	236
M.3.1	General	236
M.3.2	Authentication and Authorization of IAB-node (Phase-1)	236
M.3.3	Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (Phase-3)	236
M.3.3.1	General.....	236
M.3.3.2	Security mechanisms for the F1 interface.....	236
M.4	Protection of management traffic between IAB-node and OAM.....	237
Annex N (normative):	Security for URLLC services.....	238
N.1	General	238
N.2	Security support on redundant transmission.....	238
N.2.1	Redundant user plane paths based on dual connectivity.....	238
N.2.1.1	Introduction.....	238
N.2.2.2	Security policy aspects.....	238
N.2.2	Redundant transmission on N3/N9 interfaces	239
Annex O (Informative):	Authentication for non-5G capable devices behind residential gateways.....	240
O.1	General	240
O.2	Baseline for using non-5G capable devices with 5GC	240
O.3	Authentication procedure	240
Annex P (informative):	Security Aspects of DNS and ICMP.....	245
P.1	General	245
P.2	Security aspects of DNS.....	245
P.3	Security aspects of ICMP	245
Annex Q (informative):	Security and privacy in 5G system location services	246
Annex R (informative):	Authorization aspects in communication models for NF/NF services interaction.....	247
Annex S (informative):	Change history	249

History258

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ETSI TS 133 501 V16.7.1 (2021-08)

<https://standards.iteh.ai/catalog/standards/sist/836df603-6a86-4794-9bf2-469cfd727a10/etsi-ts-133-501-v16-7-1-2021-08>