ETSI TS 133 501 V17.7.0 (2022-09)

TECHNICAL SPECIFICATION

5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 17.7.0 Release 17)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

Reference

RTS/TSGS-0333501vh70

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 - 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:
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/CommiteeSupportStaff.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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/[illegible]-4264-9b01-
[illegible]/etsi-ts-133-501-v17-7-0-2022-09

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 2022.
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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Legal Notice

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

ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1134/etsi-ts-133-501-v17-7-0-2022-09

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.

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 26
4.1 Security domains 26
4.2 Security at the perimeter of the 5G Core network 27
4.2.0 General 27
4.2.1 Security Edge Protection Proxy (SEPP) 27
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 29
5.2.4 Secure storage and processing of subscription credentials 30
5.2.5 Subscriber privacy 30
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 31
5.3.4 Requirements for the gNB setup and configuration 32
5.3.5 Requirements for key management inside the gNB 32
5.3.6 Requirements for handling user plane data for the gNB 32
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 33
5.4 Requirements on the ng-eNB 33
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 34
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 35
5.9.2.1 Security Requirements for service registration, discovery and authorization 35

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

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 36
5.9.3.1 General 36
5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP) 37
5.9.3.3 Protection of attributes 38
5.9.3.4 Requirements for IPUPS functionality 38
5.10 Visibility and configurability 38
5.10.1 Security visibility 38
5.10.2 Security configurability 39
5.11 Requirements for algorithms, and algorithm selection 39
5.11.1 Algorithm identifier values 39
5.11.1.1 Ciphering algorithm identifier values 39
5.11.1.2 Integrity algorithm identifier values 39
5.11.2 Requirements for algorithm selection 39
5.12 Requirements on 5G-RG 40
5.13 Requirements on NSSAAF 40

6 Security procedures between UE and 5G network functions 40
6.0 General 40
6.1 Primary authentication and key agreement 41
6.1.1 Authentication framework 41
6.1.1.1 General 41
6.1.1.2 EAP framework 42
6.1.1.3 Granularity of anchor key binding to serving network 42
6.1.1.4 Construction of the serving network name 42
6.1.1.4.1 Serving network name 42
6.1.1.4.2 Construction of the serving network name by the UE 42
6.1.1.4.3 Construction of the serving network name by the SEAF 43
6.1.2 Initiation of authentication and selection of authentication method 43
6.1.3 Authentication procedures 44
6.1.3.1 Authentication procedure for EAP-AKA' 44
6.1.3.2 Authentication procedure for 5G AKA 47
6.1.3.2.0 5G AKA 47
6.1.3.2.1 Void 49
6.1.3.2.2 RES* verification failure in SEAF or AUSF or both 49
6.1.3.3 Synchronization failure or MAC failure 49
6.1.3.3.1 Synchronization failure or MAC failure in USIM 49
6.1.3.3.2 Synchronization failure recovery in Home Network 49
6.1.4 Linking increased home control to subsequent procedures 50
6.1.4.1 Introduction 50
6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 51
6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 51
6.2 Key hierarchy, key derivation, and distribution scheme 52
6.2.1 Key hierarchy 52
6.2.2 Key derivation and distribution scheme 54
6.2.2.1 Keys in network entities 54
6.2.2.2 Keys in the UE 56
6.2.3 Handling of user-related keys 58
6.2.3.1 Key setting 58
6.2.3.2 Key identification 58
6.2.3.3 Key lifetimes 59
6.3 Security contexts 60
6.3.1 Distribution of security contexts 60
6.3.1.1 General 60
6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain 60
6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains 60
6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains 60
6.3.2 Multiple registrations in same or different serving networks 61

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/9d3db86e-1ec0-4204-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

6.3.2.0 General 61
6.3.2.1 Multiple registrations in different PLMNs 61
6.3.2.2 Multiple registrations in the same PLMN 61
6.4 NAS security mechanisms 62
6.4.1 General 62
6.4.2 Security for multiple NAS connections 62
6.4.2.1 Multiple active NAS connections with different PLMNs 62
6.4.2.2 Multiple active NAS connections in the same PLMN's serving network 62
6.4.3 NAS integrity mechanisms 63
6.4.3.0 General 63
6.4.3.1 NAS input parameters to integrity algorithm 63
6.4.3.2 NAS integrity activation 64
6.4.3.3 NAS integrity failure handling 64
6.4.4 NAS confidentiality mechanisms 64
6.4.4.0 General 64
6.4.4.1 NAS input parameters to confidentiality algorithm 64
6.4.4.2 NAS confidentiality activation 64
6.4.5 Handling of NAS COUNTs 64
6.4.6 Protection of initial NAS message 65
6.4.7 Security aspects of SMS over NAS 66
6.5 RRC security mechanisms 66
6.5.1 RRC integrity mechanisms 66
6.5.2 RRC confidentiality mechanisms 67
6.5.3 RRC UE capability transfer procedure 67
6.6 UP security mechanisms 67
6.6.1 UP security policy 67
6.6.2 UP security activation mechanism 68
6.6.3 UP confidentiality mechanisms 70
6.6.4 UP integrity mechanisms 70
6.6.4.1 General 70
6.6.4.2 UP integrity mechanisms between the UE and the gNB 70
6.6.4.3 UP integrity mechanisms between the UE and the ng-eNB 70
6.7 Security algorithm selection, key establishment and security mode command procedure 71
6.7.1 Procedures for NAS algorithm selection 71
6.7.1.1 Initial NAS security context establishment 71
6.7.1.2 AMF change 71
6.7.2 NAS security mode command procedure 71
6.7.3 Procedures for AS algorithm selection 73
6.7.3.0 Initial AS security context establishment 73
6.7.3.1 Xn-handover 73
6.7.3.2 N2-handover 73
6.7.3.3 Intra-gNB-CU handover/intra-ng-eNB handover 74
6.7.3.4 Transitions from RRC_INACTIVE to RRC_CONNECTED states 74
6.7.3.5 RNA Update procedure 74
6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM 74
6.7.4 AS security mode command procedure 75
6.8 Security handling in state transitions 76
6.8.1 Key handling at connection and registration state transitions 76
6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states 76
6.8.1.1.0 General 76
6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED 76
6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED 77
6.8.1.1.2.1 General 77
6.8.1.1.2.2 Full native 5G NAS security context available 78
6.8.1.1.2.3 Full native 5G NAS security context not available 78
6.8.1.1.2.4 UE registration over a second access type to the same AMF 79
6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states 79
6.8.1.2.0 General 79
6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED 79
6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access 80
6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access 80
6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE 81

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-

6.8.1.3 Key handling for the Registration procedure when registered in NG-RAN ... 81
6.8.2 Security handling at RRC state transitions ... 82
6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states ... 82
6.8.2.1.1 General ... 82
6.8.2.1.2 State transition from RRC_CONNECTED to RRC_INACTIVE ... 82
6.8.2.1.3 State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB ... 82
6.8.2.1.4 State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB ... 84
6.8.2.2 Key handling during mobility in RRC_INACTIVE state ... 84
6.8.2.2.1 General ... 84
6.8.2.2.2 RAN-based notification area update to a new gNB/ng-eNB ... 84
6.8.2.2.3 RAN-based notification area update to the same gNB/ng-eNB ... 84
6.9 Security handling in mobility ... 85
6.9.1 Void ... 85
6.9.2 Key handling in handover ... 85
6.9.2.1 General ... 85
6.9.2.1.1 Access stratum ... 85
6.9.2.1.2 Non access stratum ... 86
6.9.2.2 Key derivations for context modification procedure ... 86
6.9.2.3 Key derivations during handover ... 87
6.9.2.3.1 Intra-gNB-CU handover and intra-ng-eNB handover ... 87
6.9.2.3.2 Xn-handover ... 87
6.9.2.3.3 N2-Handover ... 88
6.9.2.3.4 UE handling ... 89
6.9.3 Key handling in mobility registration update ... 90
6.9.4 Key-change-on-the-fly ... 92
6.9.4.1 General ... 92
6.9.4.2 NAS key re-keying ... 92
6.9.4.3 NAS key refresh ... 92
6.9.4.4 AS key re-keying ... 93
6.9.4.5 AS key refresh ... 93
6.9.5 Rules on concurrent running of security procedures ... 94
6.9.5.1 Rules related to AS and NAS security context synchronization ... 94
6.9.5.2 Rules related to parallel NAS connections ... 94
6.9.6 Security handling in registration with AMF reallocation via direct NAS reroute ... 94
6.10 Dual connectivity ... 95
6.10.1 Introduction ... 95
6.10.1.1 General ... 95
6.10.1.2 Dual Connectivity protocol architecture for MR-DC with 5GC ... 95
6.10.2 Security mechanisms and procedures for DC ... 96
6.10.2.1 SN Addition or modification ... 96
6.10.2.2 Secondary Node key update ... 98
6.10.2.2.1 General ... 98
6.10.2.2.2 MN initiated ... 98
6.10.2.2.3 SN initiated ... 98
6.10.2.3 SN release and change ... 98
6.10.3 Establishing the security context between the UE and SN ... 98
6.10.3.1 SN Counter maintenance ... 98
6.10.3.2 Derivation of keys ... 99
6.10.3.3 Negotiation of security algorithms ... 99
6.10.4 Protection of traffic between UE and SN ... 99
6.10.5 Handover Procedure ... 101
6.10.6 Signalling procedure for PDCP COUNT check ... 101
6.10.7 Radio link failure recovery ... 101
6.11 Security handling for RRC connection re-establishment procedure ... 101
6.12 Subscription identifier privacy ... 103
6.12.1 Subscription permanent identifier ... 103
6.12.2 Subscription concealed identifier ... 103
6.12.3 Subscription temporary identifier ... 104
6.12.4 Subscription identification procedure ... 105
6.12.5 Subscription identifier de-concealing function (SIDF) ... 105
6.13 Signalling procedure for PDCP COUNT check ... 105
6.14 Steering of roaming security mechanism ... 106

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
0c0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

6.14.1 General 106
6.14.2 Security mechanisms 107
6.14.2.1 Procedure for steering of UE in VPLMN during registration 107
6.14.2.2 Procedure for steering of UE in VPLMN or HPLMN after registration 108
6.14.2.3 SoR Counter 110
6.15 UE parameters update via UDM control plane procedure security mechanism 111
6.15.1 General 111
6.15.2 Security mechanisms 111
6.15.2.1 Procedure for UE Parameters Update 111
6.15.2.2 UE Parameters Update Counter 112
6.16 Security handling in Cellular IoT 113
6.16.1 Security handling in Control Plane CIoT 5GS Optimization 113
6.16.1.1 Security procedures for Small Data Transfer in Control Plane CIoT 5GS Optimisation 113
6.16.1.2 Security procedures for RRCConnectionRe-establishment Procedure in Control Plane CIoT 5GS Optimization 113
6.16.2.1 General 114
6.16.2.2 Connection Suspend 114
6.16.2.3 Connection Resume in CM-IDLE with Suspend to a new ng-eNB 115
6.16.2.4 Connection Resume in CM-IDLE with Suspend to the same ng-eNB 116
6.16.3 Protection of Non-IP Data Delivery (NIDD) interfaces 116
6.16.4 Security handling in NAS based redirection from 5GS to EPS 117

7 Security for non-3GPP access to the 5G core network 117
7.1 General 117
7.1a Determining trust relationship in the UE 117
7.2 Security procedures 118
7.2.1 Authentication for Untrusted non-3GPP Access 118

7A Security for trusted non-3GPP access to the 5G core network 120
7A.1 General 120
7A.2 Security procedures 121
7A.2.1 Authentication for trusted non-3GPP access 121
7A.2.2 Void 124
7A.2.3 Key hierarchy for trusted non-3GPP access 124
7A.2.4 Authentication for devices that do not support 5GC NAS over WLAN access 124

7B Security for wireline access to the 5G core network 127
7B.1 General 127
7B.2 Authentication for 5G-RG 127
7B.3 Authentication for FN-RG 129
7B.4 Authentication for UE behind 5G-RG and FN-RG 131
7B.5 Subscriber privacy for wireline access 131
7B.6 Subscriber privacy for N5CW over trusted WLAN access 131

8 Security of interworking 131
8.1 General 131
8.2 Registration procedure for mobility from EPS to 5GS over N26 132
8.3 Handover procedure from 5GS to EPS over N26 133
8.3.1 General 133
8.3.2 Procedure 133
8.4 Handover from EPS to 5GS over N26 136
8.4.1 General 136
8.4.2 Procedure 137
8.5 Idle mode mobility from 5GS to EPS over N26 139
8.5.1 General 139
8.5.2 TAU Procedure 140
8.6 Mapping of security contexts 141
8.6.1 Mapping of a 5G security context to an EPS security context 141
8.6.2 Mapping of an EPS security context to a 5G security context 141
8.7 Interworking without N26 interface in single-registration mode 142

9 Security procedures for non-service based interfaces 142
9.1 General 142
9.1.1 Use of NDS/IP 142

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

9.1.2 Implementation requirements 142
9.1.3 QoS considerations 142
9.2 Security mechanisms for the N2 interface 143
9.3 Security requirements and procedures on N3 143
9.4 Security mechanisms for the Xn interface 143
9.5 Interfaces based on DIAMETER or GTP 144
9.5.1 Void 144
9.6 Void 144
9.7 Void 144
9.8 Security mechanisms for protection of the gNB internal interfaces 144
9.8.1 General 144
9.8.2 Security mechanisms for the F1 interface 144
9.8.3 Security mechanisms for the E1 interface 145
9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs 145
9.10 Security mechanisms for the interface between W-5GAN and 5GC 145
10 Security aspects of IMS emergency session handling 146
10.1 General 146
10.2 Security procedures and their applicability 146
10.2.1 Authenticated IMS Emergency Sessions 146
10.2.1.1 General 146
10.2.1.2 UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services 146
10.2.1.3 UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services 147
10.2.2 Unauthenticated IMS Emergency Sessions 147
10.2.2.1 General 147
10.2.2.2 UE sets up an IMS Emergency session with emergency registration 148
10.2.2.3 Key generation for Unauthenticated IMS Emergency Sessions 149
10.2.2.3.1 General 149
10.2.2.3.2 Handover 149
11 Security procedures between UE and external data networks via the 5G Network 150
11.1 EAP based secondary authentication by an external DN-AAA server 150
11.1.1 General 150
11.1.2 Authentication 151
11.1.3 Re-Authentication 154
11.1.4 Secondary authentication and authorization revocation 155
12 Security aspects of Network Exposure Function (NEF) 155
12.1 General 155
12.2 Mutual authentication 155
12.3 Protection of the NEF – AF interface 155
12.4 Authorization of Application Function’s requests 156
12.5 Support for CAPIF 156
13 Service Based Interfaces (SBI) 156
13.1 Protection at the network or transport layer 156
13.1.0 General 156
13.1.1 TLS protection between NF and SEPP 156
13.1.1.0 General 156
13.1.1.1 TLS protection based on telescopic FQDN and wildcard certificate 157
13.1.1.2 TLS protection based on 3gpp-Sbi-Target-apiRoot HTTP header 157
13.1.2 Protection between SEPPs 157
13.2 Application layer security on the N32 interface 158
13.2.1 General 158
13.2.2 N32-c connection between SEPPs 159
13.2.2.1 General 159
13.2.2.2 Procedure for Key agreement and Parameter exchange 160
13.2.2.3 Procedure for error detection and handling in SEPP 160
13.2.2.4 N32-f Context 161
13.2.2.4.0 N32-f parts 161
13.2.2.4.1 N32-f context ID 161
13.2.2.4.2 N32-f peer information 162
13.2.2.4.3 N32-f security context 162

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-9c0874ed1154/etsi-ts-133-501-v17-7-0-2022-09

13.2.2.4.4 N32-f context information 162
13.2.3 Protection policies for N32 application layer solution 162
13.2.3.1 Overview of protection policies 162
13.2.3.2 Data-type encryption policy 163
13.2.3.3 NF API data-type placement mapping 163
13.2.3.4 Modification policy 163
13.2.3.5 Provisioning of the policies in the SEPP 164
13.2.3.6 Precedence of policies in the SEPP 164
13.2.4 N32-f connection between SEPPs 165
13.2.4.1 General 165
13.2.4.2 Overall Message payload structure for message reformatting at SEPP 165
13.2.4.3 Message reformatting in sending SEPP 166
13.2.4.3.1 dataToIntegrityProtect 166
13.2.4.3.1.1 clearTextEncapsulatedMessage 166
13.2.4.3.1.2 metadata 166
13.2.4.3.2 dataToIntegrityProtectAndCipher 167
13.2.4.4 Protection using JSON Web Encryption (JWE) 167
13.2.4.4.0 General 167
13.2.4.4.1 N32-f key hierarchy 167
13.2.4.5 Message modifications in IPX 168
13.2.4.5.1 modifiedDataToIntegrityProtect 168
13.2.4.5.2 Modifications by IPX 169
13.2.4.6 Protecting IPX modifications using JSON Web Signature (JWS) 169
13.2.4.7 Message verification by the receiving SEPP 170
13.2.4.8 Procedure 170
13.2.4.9 JOSE profile 173
13.3 Authentication and static authorization 173
13.3.0 Static authorization 173
13.3.1 Authentication and authorization between network functions and NRF 173
13.3.1.1 Direct communication 173
13.3.1.2 Indirect communication 173
13.3.1.3 Authorization of discovery request and error handling 174
13.3.2 Authentication and authorization between network functions 174
13.3.2.1 Direct communication 174
13.3.2.2 Indirect communication 174
13.3.2.3 Inter-PLMN NF to NF communication 175
13.3.2.4 Error handling 175
13.3.3 Authentication and authorization between SEPP and network functions 175
13.3.4 Authentication and authorization between SEPPs 175
13.3.6 Authentication and authorization between SCP and network functions 175
13.3.7 Authentication and authorization between SCPs 176
13.3.8 Client credentials assertion based authentication 176
13.3.8.1 General 176
13.3.8.2 Client credentials assertion 176
13.3.8.3 Verification of Client credentials assertion 177
13.4 Authorization of NF service access 177
13.4.1 OAuth 2.0 based authorization of Network Function service access 177
13.4.1.0 General 177
13.4.1.1 Service access authorization within the PLMN 178
13.4.1.1.1 OAuth 2.0 roles 178
13.4.1.1.2 Service Request Process 178
13.4.1.1A Service access authorization in interconnect scenarios 181
13.4.1.2 Service access authorization in roaming scenarios 181
13.4.1.2.1 OAuth 2.0 roles 181
13.4.1.2.2 Service Request Process 182
13.4.1.3 Service access authorization in indirect communication scenarios 185
13.4.1.3.1 Authorization for indirect communication without delegated discovery procedure 185
13.4.1.3.1.1 With mutual authentication between NF Service Consumer and NRF at the transport layer .. 185
13.4.1.3.1.2 Without mutual authentication between NF and NRF at the transport layer 187
13.4.1.3.2 Authorization for indirect communication with delegated discovery procedure 188
13.5 Security capability negotiation between SEPPs 189

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-6e0f74ed1154/etsi-ts-133-501-v17-7-0-2022-09

14 Security related services 190
14.1 Services provided by AUSF 190
14.1.1 General 190
14.1.2 Nausf_UEAuthentication service 191
14.1.2.1 Nausf_UEAuthentication_Authenticate service operation 191
14.1.2.2 Nausf_UEAuthentication_deregister service operation 191
14.1.2.3 Nausf_UEAuthentication_ProseAuthenticate service operation 192
14.1.3 Nausf_SoRProtection service 192
14.1.4 Nausf_UPUProtection service 192
14.1.5 Void 193
14.2 Services provided by UDM 193
14.2.1 General 193
14.2.2 Nudm_UEAuthentication_Get service operation 193
14.2.3 Nudm_UEAuthentication_ResultConfirmation service operation 193
14.2.4 Nudm_UEAuthentication_GetProseAv service operation 193
14.2.5 Nudm_UEAuthentication_GetGbaAv service operation 193
14.3 Services provided by NRF 194
14.3.1 General 194
14.3.2 Nnrf_AccessToken_Get Service Operation 194
14.4 Services provided by NSSAAF 194
14.4.1 Nnssaaf_NSSAA services 194
14.4.1.1 General 194
14.4.1.2 Nnssaaf_NSSAA_Authenticate service operation 195
14.4.1.3 Nnssaaf_NSSAA_Re-AuthenticationNotification service operation 195
14.4.1.4 Nnssaaf_NSSAA_RevocationNotification service operation 195
14.4.2 Nnssaaf_AIW services 195
14.4.2.1 General 195
14.4.2.2 Nnssaaf_AIW_Authenticate service operation 196

15 Management security for network slices 196
15.1 General 196
15.2 Mutual authentication 196
15.3 Protection of management interactions between the management service consumer and the management service producer 197
15.4 Authorization of management service consumer’s request 197

16 Security procedures for network slices 197
16.1 General 197
16.2 Authorization for network slice access 197
16.3 Network slice specific authentication and authorization 198
16.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure 200
16.5 AAA Server triggered Slice-Specific Authorization Revocation 201
16.6 AF Authorization for network slice quota-usage information notification/retrieval 202
16.6.1 Introduction 202
16.6.2 General 202
16.6.3 Subscription/unsubscription procedure of NSACF notification service 202

Annex A (normative): Key derivation functions 204

A.1 KDF interface and input parameter construction 204
A.1.1 General 204
A.1.2 FC value allocations 204

A.2 K_{AUSF} derivation function 204

A.3 CK' and IK' derivation function 204

A.4 RES* and XRES* derivation function 205

A.5 HRES* and HXRES* derivation function 205

A.6 K_{SEAF} derivation function 205

A.7 K_{AMF} derivation function 206
A.7.0 Parameters for the input S to the KDF 206

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ec6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

A.7.1 ABBA parameter values 206

A.8 Algorithm key derivation functions 206

A.9 $K_{gNB,}$ $K_{WAGF,}$ $K_{TNGF,}$ K_{TWIF} and K_{N3IWF} derivation function 207

A.10 NH derivation function 208

A.11 K_{NG-RAN}* derivation function for target gNB 208

A.12 K_{NG-RAN}* derivation function for target ng-eNB 208

A.13 K_{AMF} to K_{AMF}' derivation in mobility 209

A.14 K_{AMF} to K_{ASME}' derivation for interworking 209
A.14.1 Idle mode mobility 209
A.14.2 Handover 209

A.15 K_{ASME} to K_{AMF}' derivation for interworking 209
A.15.1 Idle mode mobility 209
A.15.2 Handover 210

A.16 Derivation of K_{SN} for dual connectivity 210

A.17 SoR-MAC-I_{AUSF} generation function 210

A.18 SoR-MAC-I_{UE} generation function 211

A.19 UPU-MAC-I_{AUSF} generation function 211

A.20 UPU-MAC-I_{UE} generation function 211

A.21 K_{AMF} to K_{ASME_SRVCC} derivation for interworking 212

A.22 K_{TIPSec} and K_{TNAP} derivation function 212

A.23 K_{IAB} generation function 212

Annex B (informative): Using additional EAP methods for primary authentication 214

B.1 Introduction 214

B.2 Primary authentication and key agreement 214
B.2.1 EAP TLS 214
B.2.1.1 Security procedures 214
B.2.1.2 Privacy considerations 217
B.2.1.2.1 EAP TLS without subscription identifier privacy 217
B.2.1.2.2 EAP TLS with subscription identifier privacy 217
B.2.2 Revocation of subscriber certificates 218

B.3 Key derivation 218

Annex C (normative): Protection schemes for concealing the subscription permanent identifier 220

C.1 Introduction 220

C.2 Null-scheme 220

C.3 Elliptic Curve Integrated Encryption Scheme (ECIES) 221
C.3.1 General 221
C.3.2 Processing on UE side 221
C.3.3 Processing on home network side 222
C.3.4 ECIES profiles 222
C.3.4.0 General 222
C.3.4.1 Profile A 223
C.3.4.2 Profile B 223

C.4 Implementers' test data 224
C.4.1 General 224

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

C.4.2 Null-scheme ... 224
C.4.2.1 IMSI-based SUPI ... 224
C.4.2.2 Network specific identifier-based SUPI ... 224
C.4.3 ECIES Profile A ... 224
C.4.3.1 IMSI-based SUPI ... 224
C.4.3.2 Network specific identifier-based SUPI ... 225
C.4.4 ECIES Profile B ... 226
C.4.4.1 IMSI-based SUPI ... 226
C.4.4.2 Network specific identifier-based SUPI ... 227

Annex D (normative): Algorithms for ciphering and integrity protection ... 228

D.1 Null ciphering and integrity protection algorithms ... 228

D.2 Ciphering algorithms ... 228
D.2.1 128-bit Ciphering algorithms ... 228
D.2.1.1 Inputs and outputs ... 228
D.2.1.2 128-NEA1 ... 229
D.2.1.3 128-NEA2 ... 229
D.2.1.4 128-NEA3 ... 229

D.3 Integrity algorithms ... 229
D.3.1 128-Bit integrity algorithms ... 229
D.3.1.1 Inputs and outputs ... 229
D.3.1.2 128-NIA1 ... 230
D.3.1.3 128-NIA2 ... 230
D.3.1.4 128-NIA3 ... 230

D.4 Test Data for the security algorithms ... 230
D.4.1 General ... 230
D.4.2 128-NEA1 ... 230
D.4.3 128-NIA1 ... 230
D.4.4 128-NEA2 ... 230
D.4.5 128-NIA2 ... 231
D.4.6 128-NEA3 ... 231
D.4.7 128-NIA3 ... 231

Annex E (informative): UE-assisted network-based detection of false base station ... 232

E.1 Introduction ... 232

E.2 Examples of using measurement reports ... 232

Annex F (normative): 3GPP 5G profile for EAP-AKA' ... 233

F.1 Introduction ... 233

F.2 Subscriber privacy ... 233

F.3 Subscriber identity and key derivation ... 234

F.4 Void ... 234

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

G.1 Introduction ... 235

G.2 Structure of HTTP Message ... 235

Annex H (informative): Void ... 237

Annex I (normative): Non-public networks ... 238

I.1 General ... 238

I.2 Authentication in standalone non-public networks ... 238
I.2.1 General ... 238
I.2.2 EAP framework, selection of authentication method, and EAP method credentials ... 238

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

I.2.2.1 General 238
I.2.2.2 Credentials holder using AAA server for primary authentication 239
I.2.2.2.1 General 239
I.2.2.2.2 Procedure 239
I.2.3 Key hierarchy, key derivation and key distribution 241
I.2.3.1 General 241
I.2.3.2 Credentials holder using AAA server for primary authentication 242
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 243

I.4 Modification of CAG ID list in the UE 243

I.5 SUPI privacy for standalone non-public networks 243

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 244
I.8.1 Credentials holder using AUSF and UDM for primary authentication 244

I.9 Security of UE onboarding in SNPNs 244
I.9.1 General 244
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 245
I.9.2.4 Secondary authentication 245
I.9.2.4.1 Secondary authentication using DCS 245
I.9.2.4.2 Secondary authentication using DN-AAA 245

Annex J (normative): SRVCC from 5G to UTRAN **246**

J.1 SRVCC from NR to UTRAN 246
J.1.1 General 246
J.1.2 Procedure 246

J.2 Emergency call in SRVCC from NR to UTRAN 247
J.2.1 General 247
J.2.2 Procedure 247

Annex K (normative): Security for 5GLAN services **248**

K.1 General 248

K.2 Authentication and authorization 248

K.3 Handling of UP security policy 248

Annex L (normative): Security for TSC service **249**

L.1 General 249

L.2 Access security for a 5GS TSC-enabled UE 249

L.3 Protection of user plane data in TSC including (g)PTP control messages in bridge mode 249

L.4 Exposure of time synchronisation 249

Annex M (normative): Security for Integrated Access and Backhaul (IAB) **250**

M.1 General 250

M.2 Security requirements and features 250
M.2.1 Requirements on the IAB-node (IAB-UE) 250

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86e-1ee6-4264-9b01-0e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09

M.2.2 Requirements on the IAB donor 250
M.2.3 Requirements on the 5GC supporting IAB architecture 250
M.2.4 Requirements for secure environment 250
M.2.5 Requirements on the F1 interface 250

M.3 IAB-node Integration Procedure 251
M.3.1 General 251
M.3.2 Authentication and Authorization of IAB-node (Phase-1) 251
M.3.3 Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (Phase-3) 251
M.3.3.1 General..251
M.3.3.2 Security mechanisms for the F1 interface 251

M.4 Protection of management traffic between IAB-node and OAM..252

Annex N (normative): Security for URLLC services 253

N.1 General 253

N.2 Security support on redundant transmission..253
N.2.1 Redundant user plane paths based on dual connectivity..253
N.2.1.1 Introduction..253
N.2.2.2 Security policy aspects..253
N.2.2 Redundant transmission on N3/N9 interfaces 254

Annex O (Informative): Authentication for non-5G capable devices behind residential gateways 255

O.1 General 255

O.2 Baseline for using non-5G capable devices with 5GC 255

O.3 Authentication procedure 255

Annex P (informative): Security Aspects of DNS and ICMP..260

P.1 General 260

P.2 Security aspects of DNS..260

P.3 Security aspects of ICMP 260

Annex Q (informative): Security and privacy in 5G system location services 261

Annex R (informative): Authorization aspects in communication models for NF/NF services interaction..262

Annex S (normative): Support for Non-seamless WLAN offload (NSWO) in 5GS 264

S.1 Introduction 264

S.2 General 264

S.3 Authentication procedure 264
S.3.1 5G NSWO co-existence with EPS NSWO..264
S.3.2 5G NSWO procedures..265

S.4 Roaming 266

Annex T (normative): Security for edge computing 267

T.1 General 267

T.2 Security of network exposure to edge application server..267

Annex U (informative): Primary authentication using EAP-TTLS in SNPNs 268

U.1 Introduction 268

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 133 501 V17.7.0 (2022-09)
https://standards.iteh.ai/catalog/standards/sist/5d3db86c-1ec6-4264-9b01-9e0f74cd1154/etsi-ts-133-501-v17-7-0-2022-09