

ETSI TS 133 501 V18.9.0 (2025-04)



5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 18.9.0 Release 18)

Document Preview

[ETSI TS 133 501 V18.9.0 \(2025-04\)](https://standards.iteh.ai/catalog/standards/etsi/3fcc7179-025c-4304-9274-a10e9d82509c/etsi-ts-133-501-v18-9-0-2025-04)

<https://standards.iteh.ai/catalog/standards/etsi/3fcc7179-025c-4304-9274-a10e9d82509c/etsi-ts-133-501-v18-9-0-2025-04>



ReferenceRTS/TSGS-0333501v190

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 the
[ETSI Search & Browse Standards application](#).

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

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

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

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

Copyright Notification

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

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

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

© ETSI 2025.
All rights reserved.

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables. (2025-04)

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

Modal verbs terminology

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

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

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	17
1 Scope	19
2 References	19
3 Definitions and abbreviations.....	23
3.1 Definitions	23
3.2 Abbreviations	27
4 Overview of security architecture	29
4.1 Security domains	29
4.2 Security at the perimeter of the 5G Core network.....	30
4.2.0 General.....	30
4.2.1 Security Edge Protection Proxy (SEPP)	30
4.2.2 Inter-PLMN UP Security (IPUPS).....	30
4.3 Security entities in the 5G Core network.....	30
5 Security requirements and features	31
5.1 General security requirements	31
5.1.1 Mitigation of bidding down attacks	31
5.1.2 Authentication and Authorization.....	31
5.1.3 Requirements on 5GC and NG-RAN related to keys	31
5.2 Requirements on the UE.....	31
5.2.1 General.....	31
5.2.2 User data and signalling data confidentiality	32
5.2.3 User data and signalling data integrity.....	32
5.2.4 Secure storage and processing of subscription credentials	33
5.2.5 Subscriber privacy	33
5.3 Requirements on the gNB	34
5.3.1 General.....	34
5.3.2 User data and signalling data confidentiality	34
5.3.3 User data and signalling data integrity.....	34
5.3.4 Requirements for the gNB setup and configuration.....	35
5.3.5 Requirements for key management inside the gNB.....	35
5.3.6 Requirements for handling user plane data for the gNB	35
5.3.7 Requirements for handling control plane data for the gNB	35
5.3.8 Requirements for secure environment of the gNB.....	35
5.3.9 Requirements for the gNB F1 interfaces.....	36
5.3.10 Requirements for the gNB E1 interfaces	36
5.4 Requirements on the ng-eNB	36
5.5 Requirements on the AMF	36
5.5.1 Signalling data confidentiality	36
5.5.2 Signalling data integrity.....	37
5.5.3 Subscriber privacy	37
5.6 Requirements on the SEAF	37
5.7 Void.....	37
5.8 Requirements on the UDM.....	37
5.8.1 Generic requirements.....	37
5.8.2 Subscriber privacy related requirements to UDM and SIDF	37
5.8a Requirements on AUSF.....	38
5.9 Core network security	38
5.9.1 Trust boundaries	38
5.9.2 Requirements on service-based architecture.....	38
5.9.2.1 Security Requirements for service registration, discovery and authorization	38

5.9.2.2	NRF security requirements	38
5.9.2.3	NEF security requirements.....	39
5.9.2.4	Requirements on the Service Communication Proxy (SCP)	39
5.9.3	Requirements for e2e core network interconnection security	39
5.9.3.1	General	39
5.9.3.2	Requirements for Security Edge Protection Proxy (SEPP).....	40
5.9.3.2a	Support for Messages generated by Roaming Intermediaries	42
5.9.3.3	Protection of attributes	42
5.9.3.4	Requirements for IPUPS functionality.....	43
5.9.3.5	Requirements for Network Functions (NF).....	43
5.10	Visibility and configurability	43
5.10.1	Security visibility	43
5.10.2	Security configurability	43
5.11	Requirements for algorithms, and algorithm selection.....	43
5.11.1	Algorithm identifier values	43
5.11.1.1	Ciphering algorithm identifier values.....	43
5.11.1.2	Integrity algorithm identifier values.....	44
5.11.2	Requirements for algorithm selection	44
5.12	Requirements on 5G-RG	45
5.13	Requirements on NSSAAF	45
6	Security procedures between UE and 5G network functions.....	45
6.0	General	45
6.1	Primary authentication and key agreement	45
6.1.1	Authentication framework	45
6.1.1.1	General	45
6.1.1.2	EAP framework.....	46
6.1.1.3	Granularity of anchor key binding to serving network.....	46
6.1.1.4	Construction of the serving network name.....	47
6.1.1.4.1	Serving network name	47
6.1.1.4.2	Construction of the serving network name by the UE	47
6.1.1.4.3	Construction of the serving network name by the SEAF	47
6.1.2	Initiation of authentication and selection of authentication method	48
6.1.3	Authentication procedures	49
6.1.3.1	Authentication procedure for EAP-AKA'	49
6.1.3.2	Authentication procedure for 5G AKA	52
6.1.3.2.0	5G AKA	52
6.1.3.2.1	Void.....	54
6.1.3.2.2	RES* verification failure in SEAF or AUSF or both	54
6.1.3.3	Synchronization failure or MAC failure	54
6.1.3.3.1	Synchronization failure or MAC failure in USIM.....	54
6.1.3.3.2	Synchronization failure recovery in Home Network.....	54
6.1.4	Linking increased home control to subsequent procedures	55
6.1.4.1	Introduction.....	55
6.1.4.1a	Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	56
6.1.4.2	Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	56
6.1.5	Home network triggered primary authentication procedure	57
6.1.5.1	General	57
6.1.5.2	Security mechanisms.....	57
6.2	Key hierarchy, key derivation, and distribution scheme	59
6.2.1	Key hierarchy.....	59
6.2.2	Key derivation and distribution scheme.....	61
6.2.2.1	Keys in network entities	61
6.2.2.2	Keys in the UE	63
6.2.3	Handling of user-related keys	65
6.2.3.1	Key setting	65
6.2.3.2	Key identification.....	65
6.2.3.3	Key lifetimes	66
6.3	Security contexts	67
6.3.1	Distribution of security contexts.....	67
6.3.1.1	General	67

6.3.1.2	Distribution of subscriber identities and security data within one 5G serving network domain	67
6.3.1.3	Distribution of subscriber identities and security data between 5G serving network domains	67
6.3.1.4	Distribution of subscriber identities and security data between 5G and EPS serving network domains	67
6.3.2	Multiple registrations in same or different serving networks	68
6.3.2.0	General	68
6.3.2.1	Multiple registrations in different PLMNs	68
6.3.2.2	Multiple registrations in the same PLMN	68
6.4	NAS security mechanisms	69
6.4.1	General	69
6.4.2	Security for multiple NAS connections	69
6.4.2.1	Multiple active NAS connections with different PLMNs	69
6.4.2.2	Multiple active NAS connections in the same PLMN's serving network	69
6.4.3	NAS integrity mechanisms	70
6.4.3.0	General	70
6.4.3.1	NAS input parameters to integrity algorithm	70
6.4.3.2	NAS integrity activation	71
6.4.3.3	NAS integrity failure handling	71
6.4.4	NAS confidentiality mechanisms	71
6.4.4.0	General	71
6.4.4.1	NAS input parameters to confidentiality algorithm	71
6.4.4.2	NAS confidentiality activation	71
6.4.5	Handling of NAS COUNTs	72
6.4.6	Protection of initial NAS message	72
6.4.7	Security aspects of SMS over NAS	73
6.5	RRC security mechanisms	73
6.5.1	RRC integrity mechanisms	73
6.5.2	RRC confidentiality mechanisms	74
6.5.3	RRC UE capability transfer procedure	74
6.6	UP security mechanisms	74
6.6.1	UP security policy	74
6.6.2	UP security activation mechanism	75
6.6.3	UP confidentiality mechanisms	77
6.6.4	UP integrity mechanisms	77
6.6.4.1	General	77
6.6.4.2	UP integrity mechanisms between the UE and the gNB	77
6.6.4.3	UP integrity mechanisms between the UE and the ng-eNB	77
6.7	Security algorithm selection, key establishment and security mode command procedure	78
6.7.1	Procedures for NAS algorithm selection	78
6.7.1.1	Initial NAS security context establishment	78
6.7.1.2	AMF change	78
6.7.2	NAS security mode command procedure	78
6.7.3	Procedures for AS algorithm selection	80
6.7.3.0	Initial AS security context establishment	80
6.7.3.1	Xn-handover	80
6.7.3.2	N2-handover	80
6.7.3.3	Intra-gNB-CU handover/intra-ng-eNB handover	81
6.7.3.4	Transitions from RRC_INACTIVE to RRC_CONNECTED states	81
6.7.3.5	RNA Update procedure	81
6.7.3.6	Algorithm negotiation for unauthenticated UEs in LSM	81
6.7.4	AS security mode command procedure	82
6.8	Security handling in state transitions	83
6.8.1	Key handling at connection and registration state transitions	83
6.8.1.1	Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states	83
6.8.1.1.0	General	83
6.8.1.1.1	Transition from RM-REGISTERED to RM-DEREGISTERED	83
6.8.1.1.2	Transition from RM-DEREGISTERED to RM-REGISTERED	84
6.8.1.1.2.1	General	84
6.8.1.1.2.2	Full native 5G NAS security context available	85
6.8.1.1.2.3	Full native 5G NAS security context not available	85
6.8.1.1.2.4	UE registration over a second access type to the same AMF	86
6.8.1.2	Key handling at transitions between CM-IDLE and CM-CONNECTED states	86

6.8.1.2.0	General	86
6.8.1.2.1	Transition from CM-IDLE to CM-CONNECTED	86
6.8.1.2.2	Establishment of keys for cryptographically protected radio bearers in 3GPP access	87
6.8.1.2.3	Establishment of keys for cryptographically protected traffic in non-3GPP access	87
6.8.1.2.4	Transition from CM-CONNECTED to CM-IDLE	88
6.8.1.3	Key handling for the Registration procedure when registered in NG-RAN	88
6.8.2	Security handling at RRC state transitions	89
6.8.2.1	Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states	89
6.8.2.1.1	General	89
6.8.2.1.2	State transition from RRC_CONNECTED to RRC_INACTIVE	89
6.8.2.1.3	State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB	89
6.8.2.1.4	State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB	91
6.8.2.2	Key handling during mobility in RRC_INACTIVE state	91
6.8.2.2.1	General	91
6.8.2.2.2	RAN-based notification area update to a new gNB/ng-eNB	91
6.8.2.2.3	RAN-based notification area update to the same gNB/ng-eNB	91
6.9	Security handling in mobility	92
6.9.1	Void	92
6.9.2	Key handling in handover	92
6.9.2.1	General	92
6.9.2.1.1	Access stratum	92
6.9.2.1.2	Non access stratum	93
6.9.2.2	Key derivations for context modification procedure	93
6.9.2.3	Key derivations during handover	94
6.9.2.3.1	Intra-gNB-CU handover and intra-ng-eNB handover	94
6.9.2.3.2	Xn-handover	94
6.9.2.3.3	N2-Handover	95
6.9.2.3.4	UE handling	96
6.9.3	Key handling in mobility registration update	97
6.9.4	Key-change-on-the-fly	99
6.9.4.1	General	99
6.9.4.2	NAS key re-keying	99
6.9.4.3	NAS key refresh	99
6.9.4.4	AS key re-keying	100
6.9.4.5	AS key refresh	100
6.9.5	Rules on concurrent running of security procedures	101
6.9.5.1	Rules related to AS and NAS security context synchronization	101
6.9.5.2	Rules related to parallel NAS connections	101
6.9.6	Security handling in registration with AMF reallocation via direct NAS reroute	101
6.10	Dual connectivity	102
6.10.1	Introduction	102
6.10.1.1	General	102
6.10.1.2	Dual Connectivity protocol architecture for MR-DC with 5GC	102
6.10.2	Security mechanisms and procedures for DC	103
6.10.2.1	SN Addition or modification	103
6.10.2.2	Secondary Node key update	105
6.10.2.2.1	General	105
6.10.2.2.2	MN initiated	105
6.10.2.2.3	SN initiated	105
6.10.2.3	SN release and change	105
6.10.2.4	Security mechanism and procedures for SCPAC	105
6.10.2.4.1	General	105
6.10.2.4.2	Security context initialization for selective SCPAC	106
6.10.2.4.3	Security mechanism for UE to access target PSCell or SN	106
6.10.2.4.4	Security procedure for UE to access target PSCell or SN	106
6.10.3	Establishing the security context between the UE and SN	108
6.10.3.1	SN Counter maintenance	108
6.10.3.2	Derivation of keys	109
6.10.3.3	Negotiation of security algorithms	109
6.10.4	Protection of traffic between UE and SN	109
6.10.5	Handover Procedure	110
6.10.6	Signalling procedure for PDCP COUNT check	111