

ETSI TS 133 501 V15.2.0 (2018-10)



5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.2.0 Release 15)

Full standard (standards.iteh.ai/catalog/standards/sls/54931d05-e65b-44ed-a53a-5759280276a/etsi-ts-133-501-v15-2-2018-10)



Reference

RTS/TSGS-0333501vf20

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

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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>

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 2018.

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 protected for the benefit of its Members.

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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 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
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	11
1 Scope	12
2 References	12
3 Definitions and abbreviations.....	14
3.1 Definitions	14
3.2 Abbreviations	17
4 Overview of security architecture	19
4.1 Security domains	19
4.2 Security entity at the perimeter of the 5G Core network	19
4.3 Security entities in the 5G Core network.....	20
5 Security requirements and features	20
5.1 General security requirements	20
5.1.1 Mitigation of bidding down attacks	20
5.1.2 Authentication and Authorization.....	20
5.1.3 Requirements on 5GC and 5G-RAN related to keys	21
5.2 Requirements on the UE.....	21
5.2.1 General.....	21
5.2.2 User data and signalling data confidentiality.....	21
5.2.3 User data and signalling data integrity.....	21
5.2.4 Secure storage and processing of subscription credentials	22
5.2.5 Subscriber privacy	22
5.3 Requirements on the gNB	23
5.3.1 General.....	23
5.3.2 User data and signalling data confidentiality.....	23
5.3.3 User data and signalling data integrity.....	23
5.3.4 Requirements for the gNB setup and configuration.....	23
5.3.5 Requirements for key management inside the gNB.....	24
5.3.6 Requirements for handling user plane data for the gNB	24
5.3.7 Requirements for handling control plane data for the gNB	24
5.3.8 Requirements for secure environment of the gNB.....	24
5.3.9 Requirements for the gNB F1 interfaces.....	25
5.3.10 Requirements for the gNB E1 interfaces	25
5.4 Requirements on the ng-eNB	25
5.5 Requirements on the AMF	25
5.5.1 Signalling data confidentiality	25
5.5.2 Signalling data integrity.....	25
5.5.3 Subscriber privacy	26
5.6 Requirements on the SEAF	26
5.7 Void.....	26
5.8 Requirements on the UDM.....	26
5.8.1 Generic requirements.....	26
5.8.2 Subscriber privacy related requirements to UDM and SDF	26
5.8a Requirements on AUSF.....	26
5.9 Core network security	26
5.9.1 Trust boundaries	26
5.9.2 Requirements on service-based architecture.....	27
5.9.2.1 Security Requirements for service registration, discovery and authorization	27
5.9.2.2 NRF security requirements	27
5.9.2.3 NEF security requirements.....	27
5.9.3 Requirements for e2e core network interconnection security	27
5.9.3.1 General.....	27

5.9.3.2	Requirements for Security Edge Protection Proxy (SEPP)	28
5.9.3.3	Protection of attributes	28
5.10	Visibility and configurability	29
5.10.1	Security visibility	29
5.10.2	Security configurability	29
5.11	Requirements for algorithms, and algorithm selection	29
5.11.1	Algorithm identifier values	29
5.11.1.1	Ciphering algorithm identifier values	29
5.11.1.2	Integrity algorithm identifier values	30
5.11.2	Requirements for algorithm selection	30
6	Security procedures between UE and 5G network functions	31
6.1	Primary authentication and key agreement	31
6.1.1	Authentication framework	31
6.1.1.1	General	31
6.1.1.2	EAP framework	31
6.1.1.3	Granularity of anchor key binding to serving network	32
6.1.1.4	Construction of the serving network name	32
6.1.1.4.1	Serving network name	32
6.1.1.4.2	Construction of the serving network name by the UE	32
6.1.1.4.3	Construction of the serving network name by the SEAF	32
6.1.2	Initiation of authentication and selection of authentication method	33
6.1.3	Authentication procedures	34
6.1.3.1	Authentication procedure for EAP-AKA'	34
6.1.3.2	Authentication procedure for 5G AKA	36
6.1.3.2.0	5G AKA	36
6.1.3.2.1	Void	38
6.1.3.2.2	RES* verification failure in SEAF or AUSF or both	38
6.1.3.3	Synchronization failure or MAC failure	39
6.1.3.3.1	Synchronization failure or MAC failure in USIM	39
6.1.3.3.2	Synchronization failure recovery in Home Network	39
6.1.4	Linking increased home control to subsequent procedures	39
6.1.4.1	Introduction	39
6.1.4.1a	Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	40
6.1.4.2	Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	41
6.2	Key hierarchy, key derivation, and distribution scheme	41
6.2.1	Key hierarchy	41
6.2.2	Key derivation and distribution scheme	43
6.2.2.1	Keys in network entities	43
6.2.2.2	Keys in the UE	45
6.2.3	Handling of user-related keys	47
6.2.3.1	Key setting	47
6.2.3.2	Key identification	47
6.2.3.3	Key lifetimes	48
6.3	Security contexts	49
6.3.1	Distribution of security contexts	49
6.3.1.1	General	49
6.3.1.2	Distribution of subscriber identities and security data within one 5G serving network domain	49
6.3.1.3	Distribution of subscriber identities and security data between 5G serving network domains	49
6.3.1.4	Distribution of subscriber identities and security data between 5G and EPS serving network domains	49
6.3.2	Multiple registrations in same or different serving networks	50
6.3.2.0	General	50
6.3.2.1	Multiple registrations in different PLMNs	50
6.3.2.2	Multiple registrations in the same PLMN	50
6.4	NAS security mechanisms	50
6.4.1	General	50
6.4.2	Security for multiple NAS connections	50
6.4.2.1	Multiple active NAS connections with different PLMNs	50
6.4.2.2	Multiple active NAS connections in the same PLMN's serving network	51
6.4.3	NAS integrity mechanisms	51

6.4.3.0	General	51
6.4.3.1	NAS input parameters to integrity algorithm	51
6.4.3.2	NAS integrity activation	51
6.4.3.3	NAS integrity failure handling	52
6.4.4	NAS confidentiality mechanisms	52
6.4.4.0	General	52
6.4.4.1	NAS input parameters to confidentiality algorithm	52
6.4.4.2	NAS confidentiality activation	52
6.4.5	Handling of NAS COUNTs	52
6.4.6	Protection of initial NAS message	53
6.4.7	Security aspects of SMS over NAS	54
6.5	RRC security mechanisms	54
6.5.1	RRC integrity mechanisms	54
6.5.2	RRC confidentiality mechanisms	54
6.6	UP security mechanisms	54
6.6.1	UP security policy	54
6.6.2	UP security activation mechanism	55
6.6.3	UP confidentiality mechanisms	56
6.6.4	UP integrity mechanisms	57
6.7	Security algorithm selection, key establishment and security mode command procedure	57
6.7.1	Procedures for NAS algorithm selection	57
6.7.1.1	Initial NAS security context establishment	57
6.7.1.2	AMF change	57
6.7.2	NAS security mode command procedure	57
6.7.3	Procedures for AS algorithm selection	59
6.7.3.0	Initial AS security context establishment	59
6.7.3.1	Xn-handover	59
6.7.3.2	N2-handover	60
6.7.3.3	Intra-gNB-CU handover	60
6.7.3.4	Transitions from RRC-INACTIVE to RRC-CONNECTED states	60
6.7.3.5	RNA Update procedure	60
6.7.3.6	Algorithm negotiation for unauthenticated UEs in LSM	61
6.7.4	AS security mode command procedure	61
6.8	Security handling in state transitions	62
6.8.1	Key handling at connection and registration state transitions	62
6.8.1.1	Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states	62
6.8.1.1.0	General	62
6.8.1.1.1	Transition from RM-REGISTERED to RM-DEREGISTERED	62
6.8.1.1.2	Transition from RM-DEREGISTERED to RM-REGISTERED	63
6.8.1.1.2.1	General	63
6.8.1.1.2.2	Full native 5G NAS security context available	64
6.8.1.1.2.3	Full native 5G NAS security context not available	64
6.8.1.1.2.4	UE registration over a second access type to the same AMF	65
6.8.1.2	Key handling at transitions between CM-IDLE and CM-CONNECTED states	65
6.8.1.2.0	General	65
6.8.1.2.1	Transition from CM-IDLE to CM-CONNECTED	65
6.8.1.2.2	Establishment of keys for cryptographically protected radio bearers in 3GPP access	66
6.8.1.2.3	Establishment of keys for cryptographically protected traffic in non-3GPP access	66
6.8.1.2.4	Transition from CM-CONNECTED to CM-IDLE	67
6.8.1.3	Key handling for the Registration procedure when registered in 5G-RAN	67
6.8.2	Security handling at RRC state transitions	67
6.8.2.1	Security handling at transitions between RRC_INACTIVE and RRC-CONNECTED states	67
6.8.2.1.1	General	67
6.8.2.1.2	State transition from RRC_CONNECTED to RRC_INACTIVE	68
6.8.2.1.3	State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB	68
6.8.2.1.4	State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB	69
6.8.2.2	Key handling during mobility in RRC-INACTIVE state	69
6.8.2.2.1	General	69
6.8.2.2.2	RAN-based notification area update to a new gNB	69
6.8.2.2.3	RAN-based notification area update to the same gNB	70
6.9	Security handling in mobility	70
6.9.1	General	70

6.9.2	Key handling in handover.....	70
6.9.2.1	General.....	70
6.9.2.1.1	Access stratum.....	70
6.9.2.1.2	Non access stratum.....	71
6.9.2.2	Key derivations for context modification procedure.....	72
6.9.2.3	Key derivations during handover.....	72
6.9.2.3.1	Intra-gNB-CU handover.....	72
6.9.2.3.2	Xn-handover.....	72
6.9.2.3.3	N2-Handover.....	73
6.9.2.3.4	UE handling.....	74
6.9.3	Key handling in mobility registration update.....	75
6.9.4	Key-change-on-the-fly.....	77
6.9.4.1	General.....	77
6.9.4.2	NAS key re-keying.....	77
6.9.4.3	NAS key refresh.....	77
6.9.4.4	AS key re-keying.....	77
6.9.4.5	AS key refresh.....	78
6.9.5	Rules on Concurrent Running of Security Procedures.....	78
6.9.5.1	Rules related to AS and NAS security context synchronization.....	78
6.9.5.2	Rules related to parallel NAS connections.....	79
6.10	Dual connectivity.....	79
6.10.1	Introduction.....	79
6.10.1.1	General.....	79
6.10.1.2	Dual Connectivity protocol architecture for MR-DC with 5GC.....	79
6.10.2	Security mechanisms and procedures for DC.....	80
6.10.2.1	SN Addition or modification.....	80
6.10.2.2	Secondary Node key update.....	81
6.10.2.2.1	General.....	81
6.10.2.2.2	MN initiated.....	82
6.10.2.2.3	SN initiated.....	82
6.10.2.3	SN release and change.....	82
6.10.3	Establishing the security context between the UE and SN.....	82
6.10.3.1	SN Counter maintenance.....	82
6.10.3.2	Derivation of keys.....	83
6.10.3.3	Negotiation of security algorithms.....	83
6.10.4	Protection of traffic between UE and SN.....	83
6.10.5	Handover Procedure.....	83
6.10.6	Signalling procedure for PDCP COUNT check.....	83
6.10.7	Radio link failure recovery.....	84
6.11	Security handling for RRC Connection Re-establishment Procedure.....	84
6.12	Subscription identifier privacy.....	85
6.12.1	Subscription permanent identifier.....	85
6.12.2	Subscription concealed identifier.....	85
6.12.3	Subscription temporary identifier.....	86
6.12.4	Subscription identification procedure.....	87
6.12.5	Subscription identifier de-concealing function (SIDF).....	87
6.13	Signalling procedure for PDCP COUNT check.....	87
6.14	Steering of roaming security mechanism.....	88
6.14.1	General.....	88
6.14.2	Security mechanisms.....	88
6.14.2.1	Procedure for steering of UE in VPLMN during registration.....	88
6.14.2.2	Procedure for steering of UE in VPLMN after registration.....	90
6.14.2.3	SoR Counter.....	92
7	Security for non-3GPP access to the 5G core network.....	92
7.1	General.....	92
7.2	Security procedures.....	92
7.2.1	Authentication for Untrusted non-3GPP Access.....	92
8	Security of interworking.....	95
8.1	General.....	95
8.2	Registration procedure for mobility from EPS to 5GS over N26.....	95

8.3	Handover procedure from 5GS to EPS over N26.....	96
8.3.1	General.....	96
8.3.2	Procedure.....	96
8.4	Handover from EPS to 5GS over N26.....	99
8.4.1	General.....	99
8.4.2	Procedure.....	100
8.5	Idle mode mobility from 5GS to EPS over N26.....	102
8.5.1	General.....	102
8.5.2	Procedure.....	102
8.6	Mapping of security contexts.....	104
8.6.1	Mapping of a 5G security context to an EPS security context.....	104
8.6.2	Mapping of an EPS security context to a 5G security context.....	104
8.7	Interworking without N26 interface in single-registration mode.....	104
9	Security procedures for non-service based interfaces.....	104
9.1	General.....	104
9.1.1	Use of NDS/IP.....	104
9.1.2	Implementation requirements.....	105
9.1.3	QoS considerations.....	105
9.2	Security mechanisms for the N2 interface.....	105
9.3	Security requirements and procedures on N3.....	105
9.4	Security mechanisms for the Xn interface.....	106
9.5	Interfaces based on DIAMETER or GTP.....	106
9.5.1	Void.....	106
9.6	Void.....	106
9.7	Void.....	106
9.8	Security mechanisms for protection of the gNB internal interfaces.....	106
9.8.1	General.....	106
9.8.2	Security mechanisms for the F1 interface.....	106
9.8.3	Security mechanisms for the E1 interface.....	107
9.9	Security mechanisms for non-SBA interfaces internal to the 5GC.....	107
10	Security aspects of IMS emergency session handling.....	107
10.1	General.....	107
10.2	Security procedures and their applicability.....	107
10.2.1	Authenticated IMS Emergency Sessions.....	107
10.2.1.1	General.....	107
10.2.1.2	UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services.....	108
10.2.1.3	UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services.....	108
10.2.2	Unauthenticated IMS Emergency Sessions.....	109
10.2.2.1	General.....	109
10.2.2.2	UE sets up an IMS Emergency session with emergency registration.....	110
10.2.2.3	Key generation for Unauthenticated IMS Emergency Sessions.....	111
10.2.2.3.1	General.....	111
10.2.2.3.2	Handover.....	111
11	Security procedures between UE and external data networks via the 5G Network.....	111
11.1	EAP based secondary authentication by an external DN-AAA server.....	111
11.1.1	General.....	111
11.1.2	Authentication.....	112
11.1.3	Re-Authentication.....	114
12	Security aspects of Network Exposure Function (NEF).....	115
12.1	General.....	115
12.2	Mutual authentication.....	115
12.3	Protection of the NEF – AF interface.....	115
12.4	Authorization of Application Function's requests.....	115
12.5	Support for CAPIF.....	116
13	Service Based Interfaces (SBI).....	116
13.1	Protection at the network or transport layer.....	116
13.2	Application layer security on the N32 interface.....	116
13.2.1	General.....	116
13.2.2	N32-c connection between SEPPs.....	117

13.2.2.1	General	117
13.2.2.2	Procedure for Key agreement and Parameter exchange	118
13.2.2.3	Procedure for Error detection and handling in SEPP	118
13.2.2.4	N32-f Context	119
13.2.2.4.0	N32-f parts.....	119
13.2.2.4.1	N32-f context ID.....	119
13.2.2.4.2	N32-f peer information.....	119
13.2.2.4.3	N32-f security context	120
13.2.2.4.4	N32-f context information.....	120
13.2.3	Protection policies for N32 application layer solution.....	120
13.2.3.1	Overview of protection policies	120
13.2.3.2	Data-type encryption policy	120
13.2.3.3	NF API data-type placement mapping	121
13.2.3.4	Modification policy	121
13.2.3.5	Provisioning of the policies in the SEPP.....	122
13.2.4	N32-f connection between SEPPs	122
13.2.4.1	General	122
13.2.4.2	Overall Message payload structure for message reformatting at SEPP.....	122
13.2.4.3	Message reformatting in sending SEPP	123
13.2.4.3.1	dataToIntegrityProtect	123
13.2.4.3.1.1	clearTextEncapsulatedMessage	123
13.2.4.3.1.2	metadata	124
13.2.4.3.2	dataToIntegrityProtectAndCipher	124
13.2.4.4	Protection using JSON Web Encryption (JWE).....	124
13.2.4.4.1	N32-f key hierarchy.....	125
13.2.4.5	Message modifications in IPX	126
13.2.4.5.1	modifiedDataToIntegrityProtect.....	126
13.2.4.5.2	Modifications by IPX	126
13.2.4.6	Protecting IPX modifications using JSON Web Signature (JWS).....	127
13.2.4.7	Message verification by the receiving SEPP.....	127
13.2.4.8	Procedure	128
13.2.4.9	JOSE profile.....	130
13.3	Authentication and static authorization	130
13.3.1	Authentication and authorization between network functions and the NRF.....	130
13.3.2	Authentication and authorization between network functions	130
13.3.3	Authentication and authorization between SEPP and network functions	131
13.3.4	Authentication and authorization between SEPPs	131
13.4	Authorization of NF service access.....	131
13.4.1	OAuth 2.0 based authorization of Network Function service access.....	131
13.4.1.0	General	131
13.4.1.1	Service access authorization within the PLMN.....	131
13.4.1.2	Service access authorization in roaming scenarios	134
13.5	Security capability negotiation between SEPPs	136
14	Security related services.....	137
14.1	Services provided by AUSF	137
14.1.1	General.....	137
14.1.2	Nausf_UEAuthentication service.....	138
14.1.3	Nausf_SoRProtection service	138
14.2	Services provided by UDM	139
14.2.1	General.....	139
14.2.2	Nudm_UEAuthentication_Get service operation	139
14.2.3	Nudm_UEAuthentication_ResultConfirmation service operation.....	139
14.3	Services provided by NRF	139
14.3.1	General	139
14.3.2	Nnrf_AccessToken_Get Service Operation.....	139
15	Management security for network slices	140
15.1	General	140
15.2	Mutual authentication.....	140
15.3	Protection of management interactions between the management service consumer and the management service producer	140

15.4	Authorization of management service consumer's request	140
Annex A (normative):	Key derivation functions	141
A.1	KDF interface and input parameter construction	141
A.1.1	General	141
A.1.2	FC value allocations	141
A.2	K_{AUSF} derivation function	141
A.3	CK' and IK' derivation function	141
A.4	RES^* and $XRES^*$ derivation function	142
A.5	$HRES^*$ and $HXRES^*$ derivation function	142
A.6	K_{SEAF} derivation function	142
A.7	K_{AMF} derivation function	142
A.7.0	Parameters for the input S to the KDF	142
A.7.1	ABBA parameter values	143
A.8	Algorithm key derivation functions	143
A.9	K_{gNB} and K_{N3IWF} derivation function	144
A.10	NH derivation function	144
A.11	$K_{\text{NG-RAN}}^*$ derivation function for target gNB	145
A.12	$K_{\text{NG-RAN}}^*$ derivation function for target ng-eNB	145
A.13	K_{AMF} to K_{AMF}' derivation in mobility	145
A.14	K_{AMF} to K_{ASME}' derivation for interworking	146
A.14.1	Idle mode mobility	146
A.14.2	Handover	146
A.15	K_{ASME} to K_{AMF}' derivation for interworking	146
A.15.1	Idle mode mobility	146
A.15.2	Handover	146
A.16	Derivation of K_{SN} for dual connectivity	146
A.17	SoR-MAC- I_{AUSF} generation function	147
A.18	SoR-MAC- I_{UE} generation function	147
Annex B (informative):	Using additional EAP methods for primary authentication	148
B.1	Introduction	148
B.2	Primary authentication and key agreement	148
B.2.1	EAP TLS	148
B.2.1.1	Security procedures	148
B.2.1.2	Privacy considerations	151
B.2.1.2.1	EAP TLS without subscription identifier privacy	151
B.2.1.2.2	EAP TLS with subscription identifier privacy	151
B.2.2	Revocation of subscriber certificates	152
B.3	Key derivation	152
Annex C (normative):	Protection schemes for concealing the subscription permanent identifier	153
C.1	Introduction	153
C.2	Null-scheme	153
C.3	Elliptic Curve Integrated Encryption Scheme (ECIES)	153
C.3.1	General	153

C.3.2	Processing on UE side	154
C.3.3	Processing on home network side	154
C.3.4	ECIES profiles.....	155
C.3.4.0	General.....	155
C.3.4.1	Profile A	155
C.3.4.2	Profile B.....	156
Annex D (normative):	Algorithms for ciphering and integrity protection	157
D.1	Null ciphering and integrity protection algorithms	157
D.2	Ciphering algorithms	157
D.2.1	128-bit Ciphering algorithms	157
D.2.1.1	Inputs and outputs.....	157
D.2.1.2	128-NEA1.....	158
D.2.1.3	128-NEA2.....	158
D.2.1.4	128-NEA3.....	158
D.3	Integrity algorithms	158
D.3.1	128-Bit integrity algorithms	158
D.3.1.1	Inputs and outputs.....	158
D.3.1.2	128-NIA1.....	159
D.3.1.3	128-NIA2.....	159
D.3.1.4	128-NIA3.....	159
D.4	Test Data for the security algorithms	159
D.4.1	General	159
D.4.2	128-NEA1	159
D.4.3	128-NIA1	159
D.4.4	128-NEA2	159
D.4.5	128-NIA2	159
D.4.6	128-NEA3	160
D.4.7	128-NIA3	160
Annex E (informative):	UE-assisted network-based detection of false base station.....	161
E.1	Introduction	161
E.2	Examples of using measurement reports.....	161
Annex F (normative):	3GPP 5G profile for EAP-AKA'.....	162
F.1	Introduction	162
F.2	Subscriber privacy.....	162
F.3	Subscriber identity and key derivation.....	162
F.4	Void.....	163
Annex G (informative):	Application layer security on the N32 interface.....	164
G.1	Introduction	164
G.2	Structure of HTTP Message	164
Annex H (normative):	Hash functions.....	165
H.1	General	165
H.2	HASH _{AMF} and HASH _{UE}	165
Annex I (informative):	Change history	167
History		171

Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/54931d05-e65b-44ed-a53a-5759280276a/etsi-ts-133-501-v15.2.0-2018-10>

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the 5G System and the 5G Core, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 23.501: "System Architecture for the 5G System".
- [3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".
- [5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".
- [6] IETF RFC 4301: "Security Architecture for the Internet Protocol".
- [7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".
- [8] 3GPP TS 23.502: "Procedures for the 5G System".
- [9] 3GPP TS 33.102: "3G security; Security architecture".
- [10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- [11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".
- [12] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- [13] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [14] 3GPP TS 35.215: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".
- [15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".
- [16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".
- [17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".
- [18] 3GPP TS 35.221: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".
- [19] 3GPP TS 23.003: "Numbering, addressing and identification".