ETSI TS 133 501 V15.4.0 (2019-05)

TECHNICAL SPECIFICATION

5G;
Security architecture and procedures for 5G System
(3GPP TS 33.501 version 15.4.0 Release 15)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

Reference

RTS/TSGS-0333501vf40

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)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5f60009d-7fcf-4e8f-ac1c-4f0da3220412/etsi-ts-133-501-v15.4.0-2019-05

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

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 2019.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**TM 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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f569009d-71cf-48ef-acfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 12
1 Scope 13
2 References 13
3 Definitions and abbreviations 15
3.1 Definitions 15
3.2 Abbreviations 19
4 Overview of security architecture 20
4.1 Security domains 20
4.2 Security entity at the perimeter of the 5G Core network 21
4.3 Security entities in the 5G Core network 21
5 Security requirements and features 21
5.1 General security requirements 21
5.1.1 Mitigation of bidding down attacks 21
5.1.2 Authentication and Authorization 21
5.1.3 Requirements on 5GC and NG-RAN related to keys 22
5.2 Requirements on the UE 22
5.2.1 General 22
5.2.2 User data and signalling data confidentiality 22
5.2.3 User data and signalling data integrity 23
5.2.4 Secure storage and processing of subscription credentials 23
5.2.5 Subscriber privacy 23
5.3 Requirements on the gNB 24
5.3.1 General 24
5.3.2 User data and signalling data confidentiality 24
5.3.3 User data and signalling data integrity 25
5.3.4 Requirements for the gNB setup and configuration 25
5.3.5 Requirements for key management inside the gNB 25
5.3.6 Requirements for handling user plane data for the gNB 26
5.3.7 Requirements for handling control plane data for the gNB 26
5.3.8 Requirements for secure environment of the gNB 26
5.3.9 Requirements for the gNB F1 interfaces 26
5.3.10 Requirements for the gNB E1 interfaces 26
5.4 Requirements on the ng-eNB 27
5.5 Requirements on the AMF 27
5.5.1 Signalling data confidentiality 27
5.5.2 Signalling data integrity 27
5.5.3 Subscriber privacy 27
5.6 Requirements on the SEAF 27
5.7 Void 28
5.8 Requirements on the UDM 28
5.8.1 Generic requirements 28
5.8.2 Subscriber privacy related requirements to UDM and SIDF 28
5.8a Requirements on AUSF 28
5.9 Core network security 28
5.9.1 Trust boundaries 28
5.9.2 Requirements on service-based architecture 28
5.9.2.1 Security Requirements for service registration, discovery and authorization 28
5.9.2.2 NRF security requirements 29
5.9.2.3 NEF security requirements 29
5.9.3 Requirements for e2e core network interconnection security 29

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

5.9.3.1 General 29
5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP) 30
5.9.3.3 Protection of attributes 30
5.10 Visibility and configurability 31
5.10.1 Security visibility 31
5.10.2 Security configurability 31
5.11 Requirements for algorithms, and algorithm selection 31
5.11.1 Algorithm identifier values 31
5.11.1.1 Ciphering algorithm identifier values 31
5.11.1.2 Integrity algorithm identifier values 31
5.11.2 Requirements for algorithm selection 32

6 Security procedures between UE and 5G network functions 32
6.0 General 32
6.1 Primary authentication and key agreement 33
6.1.1 Authentication framework 33
6.1.1.1 General 33
6.1.1.2 EAP framework 33
6.1.1.3 Granularity of anchor key binding to serving network 34
6.1.1.4 Construction of the serving network name 34
6.1.1.4.1 Serving network name 34
6.1.1.4.2 Construction of the serving network name by the UE 34
6.1.1.4.3 Construction of the serving network name by the SEAF 34
6.1.2 Initiation of authentication and selection of authentication method 35
6.1.3 Authentication procedures 36
6.1.3.1 Authentication procedure for EAP-AKA' 36
6.1.3.2 Authentication procedure for 5G AKA 38
6.1.3.2.0 5G AKA 38
6.1.3.2.1 Void 40
6.1.3.2.2 RES* verification failure in SEAF or AUSF or both 40
6.1.3.3 Synchronization failure or MAC failure 41
6.1.3.3.1 Synchronization failure or MAC failure in USIM 41
6.1.3.3.2 Synchronization failure recovery in Home Network 41
6.1.4 Linking increased home control to subsequent procedures 42
6.1.4.1 Introduction 42
6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 42
6.1.4.2 Guidance on linking authentication confirmation to Nudm_UECM_Registration procedure from AMF 43
6.2 Key hierarchy, key derivation, and distribution scheme 44
6.2.1 Key hierarchy 44
6.2.2 Key derivation and distribution scheme 46
6.2.2.1 Keys in network entities 46
6.2.2.2 Keys in the UE 47
6.2.3 Handling of user-related keys 49
6.2.3.1 Key setting 49
6.2.3.2 Key identification 49
6.2.3.3 Key lifetimes 50
6.3 Security contexts 51
6.3.1 Distribution of security contexts 51
6.3.1.1 General 51
6.3.1.2 Distribution of subscriber identities and security data within one 5G serving network domain 51
6.3.1.3 Distribution of subscriber identities and security data between 5G serving network domains 51
6.3.1.4 Distribution of subscriber identities and security data between 5G and EPS serving network domains 51
6.3.2 Multiple registrations in same or different serving networks 52
6.3.2.0 General 52
6.3.2.1 Multiple registrations in different PLMNs 52
6.3.2.2 Multiple registrations in the same PLMN 52
6.4 NAS security mechanisms 52
6.4.1 General 52
6.4.2 Security for multiple NAS connections 52
6.4.2.1 Multiple active NAS connections with different PLMNs 52

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48e8-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

6.4.2.2 Multiple active NAS connections in the same PLMN's serving network 53
6.4.3 NAS integrity mechanisms 54
6.4.3.0 General 54
6.4.3.1 NAS input parameters to integrity algorithm 54
6.4.3.2 NAS integrity activation 54
6.4.3.3 NAS integrity failure handling 54
6.4.4 NAS confidentiality mechanisms 55
6.4.4.0 General 55
6.4.4.1 NAS input parameters to confidentiality algorithm 55
6.4.4.2 NAS confidentiality activation 55
6.4.5 Handling of NAS COUNTs 55
6.4.6 Protection of initial NAS message 55
6.4.7 Security aspects of SMS over NAS 56
6.5 RRC security mechanisms 57
6.5.1 RRC integrity mechanisms 57
6.5.2 RRC confidentiality mechanisms 57
6.6 UP security mechanisms 57
6.6.1 UP security policy 57
6.6.2 UP security activation mechanism 58
6.6.3 UP confidentiality mechanisms 60
6.6.4 UP integrity mechanisms 60
6.7 Security algorithm selection, key establishment and security mode command procedure 60
6.7.1 Procedures for NAS algorithm selection 60
6.7.1.1 Initial NAS security context establishment 60
6.7.1.2 AMF change 60
6.7.2 NAS security mode command procedure 60
6.7.3 Procedures for AS algorithm selection 62
6.7.3.0 Initial AS security context establishment 62
6.7.3.1 Xn-handover 62
6.7.3.2 N2-handover 63
6.7.3.3 Intra-gNB-CU handover/intra-ng-eNB handover 63
6.7.3.4 Transitions from RRC_INACTIVE to RRC_CONNECTED states 63
6.7.3.5 RNA Update procedure 64
6.7.3.6 Algorithm negotiation for unauthenticated UEs in LSM 64
6.7.4 AS security mode command procedure 64
6.8 Security handling in state transitions 66
6.8.1 Key handling at connection and registration state transitions 66
6.8.1.1 Key handling at transitions between RM-DEREGISTERED and RM-REGISTERED states 66
6.8.1.1.0 General 66
6.8.1.1.1 Transition from RM-REGISTERED to RM-DEREGISTERED 66
6.8.1.1.2 Transition from RM-DEREGISTERED to RM-REGISTERED 67
6.8.1.1.2.1 General 67
6.8.1.1.2.2 Full native 5G NAS security context available 67
6.8.1.1.2.3 Full native 5G NAS security context not available 68
6.8.1.1.2.4 UE registration over a second access type to the same AMF 68
6.8.1.2 Key handling at transitions between CM-IDLE and CM-CONNECTED states 69
6.8.1.2.0 General 69
6.8.1.2.1 Transition from CM-IDLE to CM-CONNECTED 69
6.8.1.2.2 Establishment of keys for cryptographically protected radio bearers in 3GPP access 69
6.8.1.2.3 Establishment of keys for cryptographically protected traffic in non-3GPP access 70
6.8.1.2.4 Transition from CM-CONNECTED to CM-IDLE 70
6.8.1.3 Key handling for the Registration procedure when registered in NG-RAN 70
6.8.2 Security handling at RRC state transitions 71
6.8.2.1 Security handling at transitions between RRC_INACTIVE and RRC_CONNECTED states 71
6.8.2.1.1 General 71
6.8.2.1.2 State transition from RRC_CONNECTED to RRC_INACTIVE 71
6.8.2.1.3 State transition from RRC_INACTIVE to RRC_CONNECTED to a new gNB/ng-eNB 72
6.8.2.1.4 State transition from RRC_INACTIVE to RRC_CONNECTED to the same gNB/ng-eNB 73
6.8.2.2 Key handling during mobility in RRC_INACTIVE state 73
6.8.2.2.1 General 73
6.8.2.2.2 RAN-based notification area update to a new gNB/ng-eNB 73
6.8.2.2.3 RAN-based notification area update to the same gNB/ng-eNB 74

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-bcfd-489da3210f3f/etsi-ts-133-501-v15.4.0-2019-05

6.9 Security handling in mobility 74
6.9.1 General......74
6.9.2 Key handling in handover......74
6.9.2.1 General......74
6.9.2.1.1 Access stratum......74
6.9.2.1.2 Non access stratum......76
6.9.2.2 Key derivations for context modification procedure......76
6.9.2.3 Key derivations during handover......76
6.9.2.3.1 Intra-gNB-CU handover and intra-ng-eNB handover......76
6.9.2.3.2 Xn-handover......77
6.9.2.3.3 N2-Handover......77
6.9.2.3.4 UE handling......79
6.9.3 Key handling in mobility registration update......80
6.9.4 Key-change-on-the-fly......81
6.9.4.1 General......81
6.9.4.2 NAS key re-keying......82
6.9.4.3 NAS key refresh......82
6.9.4.4 AS key re-keying......82
6.9.4.5 AS key refresh......83
6.9.5 Rules on concurrent running of security procedures......83
6.9.5.1 Rules related to AS and NAS security context synchronization......83
6.9.5.2 Rules related to parallel NAS connections......84
6.10 Dual connectivity......84
6.10.1 Introduction......84
6.10.1.1 General......84
6.10.1.2 Dual Connectivity protocol architecture for MR-DC with 5GC......84
6.10.2 Security mechanisms and procedures for DC......85
6.10.2.1. SN Addition or modification......85
6.10.2.2 Secondary Node key update......87
6.10.2.2.1 General......87
6.10.2.2.2 MN initiated......87
6.10.2.2.3 SN initiated......87
6.10.2.3 SN release and change......87
6.10.3 Establishing the security context between the UE and SN......87
6.10.3.1 SN Counter maintenance......87
6.10.3.2 Derivation of keys......88
6.10.3.3 Negotiation of security algorithms......88
6.10.4 Protection of traffic between UE and SN......88
6.10.5 Handover Procedure......89
6.10.6 Signalling procedure for PDCP COUNT check......89
6.10.7 Radio link failure recovery......90
6.11 Security handling for RRC connection re-establishment procedure......90
6.12 Subscription identifier privacy......91
6.12.1 Subscription permanent identifier......91
6.12.2 Subscription concealed identifier......91
6.12.3 Subscription temporary identifier......93
6.12.4 Subscription identification procedure......93
6.12.5 Subscription identifier de-concealing function (SIDF)......94
6.13 Signalling procedure for PDCP COUNT check......94
6.14 Steering of roaming security mechanism......95
6.14.1 General......95
6.14.2 Security mechanisms......95
6.14.2.1 Procedure for steering of UE in VPLMN during registration......95
6.14.2.2 Procedure for steering of UE in VPLMN after registration......96
6.14.2.3 SoR Counter......98
6.15 UE parameters update via UDM control plane procedure security mechanism......98
6.15.1 General......98
6.15.2 Security mechanisms......99
6.15.2.1 Procedure for UE Parameters Update......99
6.15.2.2 UE Parameters Update Counter......100

7 Security for non-3GPP access to the 5G core network......100

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569f09d-71cf-48ef-afd4-489da3210f45/etsi-ts-133-501-v15.4.0-2019-05

7.1 General 100
7.2 Security procedures 101
7.2.1 Authentication for Untrusted non-3GPP Access..101

8 Security of interworking...103
8.1 General 103
8.2 Registration procedure for mobility from EPS to 5GS over N26..103
8.3 Handover procedure from 5GS to EPS over N26..104
8.3.1 General...104
8.3.2 Procedure 104
8.4 Handover from EPS to 5GS over N26...107
8.4.1 General...107
8.4.2 Procedure 108
8.5 Idle mode mobility from 5GS to EPS over N26..110
8.5.1 General...110
8.5.2 Procedure 110
8.6 Mapping of security contexts 112
8.6.1 Mapping of a 5G security context to an EPS security context...112
8.6.2 Mapping of an EPS security context to a 5G security context...112
8.7 Interworking without N26 interface in single-registration mode 112

9 Security procedures for non-service based interfaces 113
9.1 General 113
9.1.1 Use of NDS/IP 113
9.1.2 Implementation requirements 113
9.1.3 QoS considerations 113
9.2 Security mechanisms for the N2 interface...113
9.3 Security requirements and procedures on N3...114
9.4 Security mechanisms for the Xn interface...114
9.5 Interfaces based on DIAMETER or GTP...114
9.5.1 Void 115
9.6 Void...115
9.7 Void...115
9.8 Security mechanisms for protection of the gNB internal interfaces 115
9.8.1 General...115
9.8.2 Security mechanisms for the F1 interface...115
9.8.3 Security mechanisms for the E1 interface...115
9.9 Security mechanisms for non-SBA interfaces internal to the 5GC 116

10 Security aspects of IMS emergency session handling..116
10.1 General 116
10.2 Security procedures and their applicability 116
10.2.1 Authenticated IMS Emergency Sessions 116
10.2.1.1 General...116
10.2.1.2 UE in RM-DEREGISTERED state requests a PDU Session for IMS Emergency services...............116
10.2.1.3 UE in RM-REGISTERED state requests a PDU Session for IMS Emergency services....................117
10.2.2 Unauthenticated IMS Emergency Sessions 118
10.2.2.1 General...118
10.2.2.2 UE sets up an IMS Emergency session with emergency registration 118
10.2.2.3 Key generation for Unauthenticated IMS Emergency Sessions..119
10.2.2.3.1 General 119
10.2.2.3.2 Handover 119

11 Security procedures between UE and external data networks via the 5G Network 120
11.1 EAP based secondary authentication by an external DN-AAA server..120
11.1.1 General...120
11.1.2 Authentication..121
11.1.3 Re-Authentication...123

12 Security aspects of Network Exposure Function (NEF) 124
12.1 General 124
12.2 Mutual authentication..124
12.3 Protection of the NEF – AF interface..124
12.4 Authorization of Application Function’s requests...125

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-49ef-bcfd-4bdda32104f3/etsi-ts-133-501-v15.4.0-2019-05

12.5 Support for CAPIF 125

13 Service Based Interfaces (SBI) 125
13.1 Protection at the network or transport layer 125
13.2 Application layer security on the N32 interface 126
13.2.1 General 126
13.2.2 N32-c connection between SEPPs 127
13.2.2.1 General 127
13.2.2.2 Procedure for Key agreement and Parameter exchange 128
13.2.2.3 Procedure for error detection and handling in SEPP 128
13.2.2.4 N32-f Context 129
13.2.2.4.0 N32-f parts 129
13.2.2.4.1 N32-f context ID 129
13.2.2.4.2 N32-f peer information 130
13.2.2.4.3 N32-f security context 130
13.2.2.4.4 N32-f context information 130
13.2.3 Protection policies for N32 application layer solution 130
13.2.3.1 Overview of protection policies 130
13.2.3.2 Data-type encryption policy 131
13.2.3.3 NF API data-type placement mapping 131
13.2.3.4 Modification policy 131
13.2.3.5 Provisioning of the policies in the SEPP 132
13.2.3.6 Precedence of policies in the SEPP 132
13.2.4 N32-f connection between SEPPs 133
13.2.4.1 General 133
13.2.4.2 Overall Message payload structure for message reformatting at SEPP 134
13.2.4.3 Message reformatting in sending SEPP 135
13.2.4.3.1 dataToIntegrityProtect 135
13.2.4.3.1.1 clearTextEncapsulatedMessage 135
13.2.4.3.1.2 metadata 135
13.2.4.3.2 dataToIntegrityProtectAndCipher 135
13.2.4.4 Protection using JSON Web Encryption (JWE) 136
13.2.4.4.0 General 136
13.2.4.4.1 N32-f key hierarchy 136
13.2.4.5 Message modifications in IPX 137
13.2.4.5.1 modifiedDataToIntegrityProtect 137
13.2.4.5.2 Modifications by IPX 138
13.2.4.6 Protecting IPX modifications using JSON Web Signature (JWS) 138
13.2.4.7 Message verification by the receiving SEPP 138
13.2.4.8 Procedure 139
13.2.4.9 JOSE profile 142
13.3 Authentication and static authorization 142
13.3.1 Authentication and authorization between network functions and the NRF 142
13.3.2 Authentication and authorization between network functions 142
13.3.3 Authentication and authorization between SEPP and network functions 143
13.3.4 Authentication and authorization between SEPPs 143
13.4 Authorization of NF service access 144
13.4.1 OAuth 2.0 based authorization of Network Function service access 144
13.4.1.0 General 144
13.4.1.1 Service access authorization within the PLMN 144
13.4.1.2 Service access authorization in roaming scenarios 146
13.5 Security capability negotiation between SEPPs 149

14 Security related services 151
14.1 Services provided by AUSF 151
14.1.1 General 151
14.1.2 Nausf_UEAuthentication service 151
14.1.3 Nausf_SoRProtection service 151
14.1.4 Nausf_UPUProtection service 152
14.2 Services provided by UDM 152
14.2.1 General 152
14.2.2 Nudm_UEAuthentication_Get service operation 152

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-b6fd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

14.2.3 Nudm_UEAuthentication_ResultConfirmation service operation 153
14.3 Services provided by NRF 153
14.3.1 General 153
14.3.2 Nnrf_AccessToken_Get Service Operation 153

15 Management security for network slices 154
15.1 General 154
15.2 Mutual authentication 154
15.3 Protection of management interactions between the management service consumer and the management service producer 154
15.4 Authorization of management service consumer’s request 154

Annex A (normative): Key derivation functions 155

A.1 KDF interface and input parameter construction 155
A.1.1 General 155
A.1.2 FC value allocations 155

A.2 K_{AUSF} derivation function 155

A.3 CK' and IK' derivation function 155

A.4 RES* and XRES* derivation function 156

A.5 HRES* and HXRES* derivation function 156

A.6 K_{SEAF} derivation function 156

A.7 K_{AMF} derivation function 157
A.7.0 Parameters for the input S to the KDF 157
A.7.1 ABBA parameter values 157

A.8 Algorithm key derivation functions 157

A.9 K_{gNB} and K_{N3IWF} derivation function 158

A.10 NH derivation function 159

A.11 K_{NG-RAN}* derivation function for target gNB 159

A.12 K_{NG-RAN}* derivation function for target ng-eNB 159

A.13 K_{AMF} to K_{AMF}' derivation in mobility 159

A.14 K_{AMF} to K_{ASME}' derivation for interworking 160
A.14.1 Idle mode mobility 160
A.14.2 Handover 160

A.15 K_{ASME} to K_{AMF}' derivation for interworking 160
A.15.1 Idle mode mobility 160
A.15.2 Handover 161

A.16 Derivation of K_{SN} for dual connectivity 161

A.17 SoR-MAC-I_{AUSF} generation function 161

A.18 SoR-MAC-I_{UE} generation function 161

A.19 UPU-MAC-I_{AUSF} generation function 162

A.20 UPU-MAC-I_{UE} generation function 162

Annex B (informative): Using additional EAP methods for primary authentication 163

B.1 Introduction 163

B.2 Primary authentication and key agreement 163
B.2.1 EAP TLS 163
B.2.1.1 Security procedures 163
B.2.1.2 Privacy considerations 166
B.2.1.2.1 EAP TLS without subscription identifier privacy 166

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-4eef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

B.2.1.2.2 EAP TLS with subscription identifier privacy 166
B.2.2 Revocation of subscriber certificates 167

B.3 Key derivation 167

Annex C (normative): Protection schemes for concealing the subscription permanent identifier....169

C.1 Introduction 169

C.2 Null-scheme 169

C.3 Elliptic Curve Integrated Encryption Scheme (ECIES) 170
C.3.1 General 170
C.3.2 Processing on UE side 170
C.3.3 Processing on home network side 171
C.3.4 ECIES profiles 171
C.3.4.0 General 171
C.3.4.1 Profile A 172
C.3.4.2 Profile B 172

Annex D (normative): Algorithms for ciphering and integrity protection 174

D.1 Null ciphering and integrity protection algorithms 174

D.2 Ciphering algorithms 174
D.2.1 128-bit Ciphering algorithms 174
D.2.1.1 Inputs and outputs 174
D.2.1.2 128-NEA1 175
D.2.1.3 128-NEA2 175
D.2.1.4 128-NEA3 175

D.3 Integrity algorithms 175
D.3.1 128-Bit integrity algorithms 175
D.3.1.1 Inputs and outputs 175
D.3.1.2 128-NIA1 176
D.3.1.3 128-NIA2 176
D.3.1.4 128-NIA3 176

D.4 Test Data for the security algorithms 176
D.4.1 General 176
D.4.2 128-NEA1 176
D.4.3 128-NIA1 176
D.4.4 128-NEA2 176
D.4.5 128-NIA2 177
D.4.6 128-NEA3 177
D.4.7 128-NIA3 177

Annex E (informative): UE-assisted network-based detection of false base station....178

E.1 Introduction 178

E.2 Examples of using measurement reports 178

Annex F (normative): 3GPP 5G profile for EAP-AKA' 179

F.1 Introduction 179

F.2 Subscriber privacy 179

F.3 Subscriber identity and key derivation 180

F.4 Void 180

Annex G (informative): Application layer security on the N32 interface 181

G.1 Introduction 181

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

G.2 Structure of HTTP Message 181

Annex H (informative): Void 183

Annex I (informative): Change history 184

History 190

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b569009d-71cf-48ef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05

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/b569009d-71cf-48ef-bcfd-489da32104f3/etsi-ts-133-501-v15.4.0-2019-05