ETSI TS 133 401 V15.7.0 (2019-05)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP System Architecture Evolution (SAE);
Security architecture
(3GPP TS 33.401 version 15.7.0 Release 15)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f76d133c-bca2-44d3-8466-7c8508e07845/etsi-ts-133-401-v15-7-0-2019-05

A GLOBAL INITIATIVE

Reference
RTS/TSGS-0333401vf70

Keywords
GSM,LTE,SECURITY,UMTS

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 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.

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)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/d5533c-bca2-4a1-ad0f-e18508/etsi-ts-133-401-v15.7.0-2019-05

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/1e60533c-bca2-4013-8466-7c8508750784/etsi-ts-133-401-v15.7.0-2019-05

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 10
1 Scope 11
2 References 11
3 Definitions, symbols and abbreviations 13
3.1 Definitions 13
3.2 Symbols 14
3.3 Abbreviations 15
3.4 Conventions 16
4 Overview of Security Architecture 17
5 Security Features 17
5.1 User-to-Network security 17
5.1.0 General 17
5.1.1 User identity and device confidentiality 18
5.1.2 Entity authentication 18
5.1.3 User data and signalling data confidentiality 18
5.1.3.1 Ciphering requirements 18
5.1.3.2 Algorithm Identifier Values 19
5.1.4 User data and signalling data integrity 19
5.1.4.1 Integrity requirements 19
5.1.4.2 Algorithm Identifier Values 19
5.2 Security visibility and configurability 20
5.3 Security requirements on eNodeB 20
5.3.1 General 20
5.3.2 Requirements for eNB setup and configuration 20
5.3.3 Requirements for key management inside eNB 21
5.3.4 Requirements for handling User plane data for the eNB 21
5.3.4a Requirements for handling Control plane data for the eNB 21
5.3.5 Requirements for secure environment of the eNB 21
5.4 Void 22
6 Security Procedures between UE and EPC Network Elements 22
6.0 General 22
6.1 Authentication and key agreement 22
6.1.1 AKA procedure 22
6.1.2 Distribution of authentication data from HSS to serving network 23
6.1.3 User identification by a permanent identity 24
6.1.4 Distribution of IMSI and authentication data within one serving network domain 25
6.1.5 Distribution of IMSI and authentication data between different serving network domains 26
6.1.6 Distribution of IMSI and UMTS authentication vectors between MMEs or between MME and SGSN 26
6.2 EPS key hierarchy 27
6.3 EPS key identification 29
6.4 Handling of EPS security contexts 30
6.5 Handling of NAS COUNTs 31
7 Security procedures between UE and EPS access network elements 32
7.0 General 32
7.1 Mechanism for user identity confidentiality 32
7.2 Handling of user-related keys in E-UTRAN 32
7.2.1 E-UTRAN key setting during AKA 32
7.2.2 E-UTRAN key identification 32

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f760533c-bca2-4d7-84c5-3b5875078d/etsi-ts-133-401-v15.7.0-2019-05

7.2.3 E-UTRAN key lifetimes 33
7.2.4 Security mode command procedure and algorithm negotiation 33
7.2.4.1 Requirements for algorithm selection 33
7.2.4.2 Procedures for AS algorithm selection 34
7.2.4.2.1 Initial AS security context establishment 34
7.2.4.2.2 X2-handover 34
7.2.4.2.3 S1-handover 34
7.2.4.2.4 Intra-eNB handover 34
7.2.4.3 Procedures for NAS algorithm selection 34
7.2.4.3.1 Initial NAS security context establishment 34
7.2.4.3.2 MME change 35
7.2.4.4 NAS security mode command procedure 35
7.2.4.5 AS security mode command procedure 36
7.2.4a Algorithm negotiation for unauthenticated UEs in LSM 37
7.2.5 Key handling at state transitions to and away from EMM-DEREGISTERED 38
7.2.5.1 Transition to EMM-DEREGISTERED 38
7.2.5.2 Transition away from EMM-DEREGISTERED 39
7.2.5.2.1 General 39
7.2.5.2.2 With existing native EPS NAS security context 39
7.2.5.2.3 With run of EPS AKA 40
7.2.6 Key handling in ECM-IDLE to ECM-CONNECTED and ECM-CONNECTED to ECM-IDLE transitions 40
7.2.6.1 ECM-IDLE to ECM-CONNECTED transition 40
7.2.6.2 Establishment of keys for cryptographically protected radio bearers 40
7.2.6.3 ECM-CONNECTED to ECM-IDLE transition 41
7.2.7 Key handling for the TAU procedure when registered in E-UTRAN 41
7.2.8 Key handling in handover 42
7.2.8.1 General 42
7.2.8.1.1 Access stratum 42
7.2.8.1.2 Non access stratum 43
7.2.8.2 Void 43
7.2.8.3 Key derivations for context modification procedure 43
7.2.8.4 ..... Key derivations during handovers 44
7.2.8.4.1 Intra-eNB Handover 44
7.2.8.4.2 X2-handover 44
7.2.8.4.3 S1-Handover 44
7.2.8.4.4 UE handling 45
7.2.9 Key-change-on-the fly 45
7.2.9.1 General 45
7.2.9.2 K_{eNB} re-keying 45
7.2.9.3 KeNB refresh 46
7.2.9.4 NAS key re-keying 46
7.2.10 Rules on Concurrent Running of Security Procedures 46
7.2.11 Suspend and resume of RRC connection 47
7.2.11.1 General 47
7.2.11.2 RRC connection suspend 47
7.2.11.3 RRC connection resume to a new eNB 48
7.2.11.4 RRC connection resume to the same eNB 50
7.3 UP security mechanisms 50
7.3.1 UP confidentiality mechanisms 50
7.3.2 UP integrity mechanisms 50
7.4 RRC security mechanisms 51
7.4.1 RRC integrity mechanisms 51
7.4.2 RRC confidentiality mechanisms 51
7.4.3 K_{eNB}* and Token Preparation for the RRCConnectionRe-establishment Procedure 51
7.4.4 RRCConnectionRe-establishment Procedure for Control Plane CIoT EPS optimisation 52
7.5 Signalling procedure for periodic local authentication 53

8 Security mechanisms for non-access stratum signalling and data via MME 54
8.0 General 54
8.1 NAS integrity mechanisms 54

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4760d33c-b6c2-44d3-8466-7c8508750784/etsi-ts-133-401-v15.7.0-2019-05

8.1.1 NAS input parameters and mechanism 54
8.1.2 NAS integrity activation 54
8.2 NAS confidentiality mechanisms 55

9 Security interworking between E-UTRAN and UTRAN 55
9.1 RAU and TAU procedures 55
9.1.1 RAU procedures in UTRAN 55
9.1.2 TAU procedures in E-UTRAN 56
9.2 Handover 58
9.2.1 From E-UTRAN to UTRAN 58
9.2.2 From UTRAN to E-UTRAN 59
9.2.2.1 Procedure 59
9.2.2.2 Derivation of NAS keys and K_{eNB} during Handover from UTRAN to E-UTRAN 63
9.3 Recommendations on AKA at IRAT-mobility to E-UTRAN 63
9.4 Attach procedures 64
9.4.1 Attach in UTRAN 64

10 Security interworking between E-UTRAN and GERAN 64
10.1 General 64
10.2 RAU and TAU procedures 65
10.2.1 RAU procedures in GERAN 65
10.2.2 TAU procedures in E-UTRAN 65
10.3 Handover 65
10.3.1 From E-UTRAN to GERAN 65
10.3.2 From GERAN to E-UTRAN 65
10.3.2.1 Procedures 65
10.4 Recommendations on AKA at IRAT-mobility to E-UTRAN 65
10.5 Attach procedures 66
10.5.1 Attach in GERAN 66

11 Network Domain Control Plane protection 66

12 Backhaul link user plane protection 66

13 Management plane protection over the S1 interface 67

14 SRVCC between E-UTRAN and Circuit Switched UTRAN/GERAN 68
14.1 From E-UTRAN to Circuit Switched UTRAN/GERAN 68
14.2 Emergency call in SRVCC from E-UTRAN to circuit switched UTRAN/GERAN 69
14.3 SRVCC from circuit switched UTRAN/GERAN to E-UTRAN 69
14.3.1 Procedure 69

15 Security Aspects of IMS Emergency Session Handling 72
15.1 General 72
15.2 Security procedures and their applicability 73
15.2.1 Authenticated IMS Emergency Sessions 73
15.2.1.1 General 73
15.2.1.2 UE and MME share a current security context 73
15.2.2 Unauthenticated IMS Emergency Sessions 74
15.2.2.1 General 74
15.2.2.2 UE and MME share no security context 75
15.2.3 Void 76
15.2.4 Key generation procedures for unauthenticated IMS Emergency Sessions 76
15.2.4.1 General 76
15.2.4.2 Handover 76

16 Void 76

Annex A (normative): Key derivation functions 77

A.1 KDF interface and input parameter construction 77
A.1.1 General 77
A.1.2 FC value allocations 77

A.2 K_{ASME} derivation function 77

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f7e0553c-bca2-44d3-8f63-5f5f5f5f5f5f/etsi-ts-133-401-v15.7.0-2019-05

A.3 K_{eNB} derivation function 78
A.4 NH derivation function 78
A.5 K_{eNB}* derivation function 78
A.6 Void 78
A.7 Algorithm key derivation functions 79
A.8 K_{ASME} to CK', IK' derivation at handover 79
A.9 NAS token derivation for inter-RAT mobility 80
A.10 K'_{ASME} from CK, IK derivation during handover 80
A.11 K'_{ASME} from CK, IK derivation during idle mode mobility 80
A.12 K_{ASME} to CK_{SRVCC}, IK_{SRVCC} derivation 81
A.13 K_{ASME} to CK', IK' derivation at idle mobility 81
A.14 (Void) 81
A.15 Derivation of S-K_{eNB} or S-K_{gNB} for dual connectivity 81
A.16 Derivation of LWIP-PSK 81
A.17 Derivation of K_n for IOPS subscriber key separation 82
A.18 Derivation of S-K_{WT} for LWA 82
A.19 Key derivation function for key used in algorithms between UE and SgNB 82

Annex B (normative): Algorithms for ciphering and integrity protection 83

B.0 Null ciphering and integrity protection algorithms 83
B.1 128-bit ciphering algorithm 83
B.1.1 Inputs and outputs 83
B.1.2 128-EEA1 84
B.1.3 128-EEA2 84
B.1.4 128-EEA3 84
B.2 128-Bit integrity algorithm 85
B.2.1 Inputs and outputs 85
B.2.2 128-EIA1 85
B.2.3 128-EIA2 85
B.2.4 128-EIA3 86

Annex C (informative): Algorithm test data 87

C.1 128-EEA2 87
C.1.1 Test Set 1 87
C.1.2 Test Set 2 88
C.1.3 Test Set 3 89
C.1.4 Test Set 4 89
C.1.5 Test Set 5 90
C.1.6 Test Set 6 91
C.2 128-EIA2 94
C.2.1 Test Set 1 95
C.2.2 Test Set 2 96
C.2.3 Test Set 3 97
C.2.4 Test Set 4 98
C.2.5 Test Set 5 99
C.2.6 Test Set 6 100
C.2.7 Test Set 7 102
C.2.8 Test Set 8 104

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/2f60533c-bca2-44d3-8466-7e8508750784/etsi-ts-133-401-v15.7.0-2019-05

C.3 128-EEA1 116
C.4 128-EIA1 116
C.4.1 Test Set 1 116
C.4.2 Test Set 2 117
C.4.3 Test Set 3 117
C.4.4 Test Set 4 117
C.4.5 Test Set 5 118
C.4.6 Test Set 6 118
C.4.7 Test Set 7 118

Annex D (normative): Security for Relay Node Architectures 121

D.1 Introduction 121
D.2 Solution 121
D.2.1 General 121
D.2.2 Security Procedures 121
D.2.3 USIM Binding Aspects 124
D.2.4 Enrolment procedures for RNs 124
D.2.5 Secure management procedures for RNs 125
D.2.6 Certificate and subscription handling 125
D.3 Secure channel profiles 127
D.3.1 General 127
D.3.2 APDU secure channel profile 127
D.3.3 Key agreement based on certificate exchange 127
D.3.3.1 TLS profile 127
D.3.3.2 Common profile for RN and UICC certificate 127
D.3.3.3 RN certificate profile 128
D.3.3.4 UICC certificate profile 128
D.3.4 Key agreement for pre-shared key (psk) case 128
D.3.5 Identities used in key agreement 129

Annex E (normative): Dual connectivity 130

E.1 Introduction 130
E.1.1 General 130
E.1.2 Dual Connectivity architecture with an SeNB 130
E.1.3 Dual Connecivity architecture with an SgNB 131
E.2 Dual connectivity offload architecture between eNBs 132
E.2.1 Protection of the X2 reference point 132
E.2.2 Addition and modification of DRB in SeNB 132
E.2.3 Activation of encryption/decryption 133
E.2.4 Derivation of keys for the DRBs in the SeNB 134
E.2.4.1 SCG Counter maintenance 134
E.2.4.2 Security key derivation 134
E.2.4.3 Negotiation of security algorithms 135
E.2.5 S-K_{eNB} update 135
E.2.5.1 S-K_{eNB} update triggers 135
E.2.5.2 S-K_{eNB} update procedure 135
E.2.6 Handover procedures 135
E.2.7 Periodic local authentication procedure 135
E.2.8 Radio link failure recovery 136
E.2.9 Avoiding key stream reuse caused by DRB type change 136
E.3 Dual connectivity architecture between a MeNB and a SgNB 136
E.3.1 Protection of the X2 reference point 136
E.3.2 Addition and modification of DRBs and/or SRB in SgNB 136
E.3.3 Activation of encryption/decryption of DRBs and encryption/decryption/integrity protection of SRB 137
E.3.4 Derivation of keys for RBs with PDCP in the SgNB 138
E.3.4.1 SCG Counter maintenance 138
E.3.4.2 Security key derivation 138

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f7e05c3c-bca2-4d13-a56f-6e67e850875074/etsi-ts-133-401-v15.7.0-2019-05

E.3.4.3 Negotiation of security algorithms....139
E.3.5 S-K_{gNB} update....140
E.3.5.1 S-K_{gNB} update triggers....140
E.3.5.2 S-K_{gNB} update procedure....140
E.3.6 Handover procedures....140
E.3.7 Periodic local authentication procedure....140
E.3.8 Radio link failure recovery....141
E.3.9 Avoiding key stream reuse caused by DRB type change....141
E.3.10 Protection of the traffic between the UE and SgNB....141
E.3.10.1 General....141
E.3.10.2 Creating the mapped UE NR security capabilities....141

Annex F (informative): Isolated E-UTRAN Operation for Public Safety....142

F.1 General Description....142

F.2 IOPS security solution....142

F.3 Security Considerations....143
F.3.1 Malicious switching of USIM applications....143
F.3.2 Compromise of local HSSs....143

F.4 Mitigation of compromise of a local HSS....143
F.4.0 Introduction....143
F.4.1 'Subscriber key separation' mechanism....143
F.4.2 Key derivation mechanism for 'subscriber key separation'....144

F.5 Actions in case of compromise of a local HSS....145

Annex G (normative): LTE - WLAN aggregation....146

G.1 Introduction....146

G.2 LTE-WLAN aggregation security....147
G.2.1 Protection of the WLAN Link between the UE and the WT....147
G.2.2 Protection of the Xw interface....147
G.2.3 Addition, modification and release of DRBs in LWA....147
G.2.4 Derivation of keys for the DRBs in LWA....148
G.2.4.1 WT Counter maintenance....148
G.2.4.2 Security key derivation....148
G.2.5 Security key update....148
G.2.5.1 Security key update triggers....148
G.2.5.2 Security key update procedures....149
G.2.6 Handover procedures....149
G.2.7 Periodic local authentication procedure....149
G.2.8 LTE and WLAN link failure....149

G.3 Method for installing PMK....149

Annex H (normative): LTE-WLAN RAN level integration using IPsec tunnelling....152

H.1 General....152

H.2 Security of LTE-WLAN integration using IPsec Tunnelling....153
H.2.1 eNB to UE interaction for setting up the LWIP offload....153
H.2.2 UE to LWIP-SeGW interaction for setting up the LWIP offload....154
H.2.3 eNB to LWIP-SeGW interaction for setting the LWIP offload....154

H.3 Addition and modification of DRB in LTE-WLAN integration....155

H.4 Security Key for IKEv2 handshake....155
H.4.0 LWIP counter maintenance....155
H.4.1 Security Key (LWIP-PSK) Derivation....155
H.4.2 Security key (LWIP-PSK) update....155
H.5 Handover procedures....156

H.6 LWIP radio link failure....156

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f760533c-bca2-44d3-8466-7c850875f784/etsi-ts-133-401-v15.7.0-2019-05

Annex I (normative): Hash functions 157
I.1 General 157
I.2 $HASH_{MME}$ and $HASH_{UE}$ 157
I.3 $HASH_{UE\text{-}data}$ and $HASH_{eNB\text{-}data}$ 157
Annex J (informative): Change history 158
History 165

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f760533c-bca2-44d3-8466-7c8508750784/etsi-ts-133-401-v15.7.0-2019-05

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/f760533c-bca2-44d3-8466-7c85508750784/etsi-ts-133-401-v15.7.0-2019-05

1 Scope

The present document specifies the security architecture, i.e., the security features and the security mechanisms for the Evolved Packet System and the Evolved Packet Core, and the security procedures performed within the evolved Packet System (EPS) including the Evolved Packet Core (EPC) and the Evolved UTRAN (E-UTRAN).

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 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 33.102: "3G security; Security architecture".

[5] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[9] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[10] – [11] Void.

[12] 3GPP TS 36.323: "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification"

[13] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[14] 3GPP TS 35.215: "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] – [20] Void.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/4760533c-ca2-4a42-8466-7d3505f7e784/etsi-ts-133-401-v15.7.0-2019-05

[21] 3GPP TS 36.331:"Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

[22] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[23] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[24] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Resource Control (RRC); Protocol Specification ".

[25] 3GPP TS 44.060: "3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol.

[26] 3GPP TS 23.122: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[27] 3GPP TS 33.320: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[28] (void)

[29] ETSI TS 102 484 V10.0.0: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[30] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[31] 3GPP TS 31.116 "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[32] ETSI TS 102 221 V9.2.0: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[33] 3GPP TS 35.221: "Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[34] RFC 4301: "Security Architecture for the Internet Protocol".

[35] 3GPP TS 22.346: "Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1".

[36] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[37] 3GPP TS.33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[38] IETF RFC 7296: " Internet Key Exchange Protocol Version 2 (IKEv2)".

[39] IEEE 802.11, Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Std.".

[40] 3GPP TS 36.463: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and Wireless LAN (WLAN); Xw application protocol (XwAP)".

[41] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[42] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[43] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/60533c-1ea2-4d3...-7c85...-ts-133-401-v15.7.0-2019-05