

ETSI TS 133 401 V14.5.0 (2018-01)



**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 14.5.0 Release 14)**



Reference

RTS/TSGS-0333401ve50

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 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 the present document 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.....	9
1 Scope	10
2 References	10
3 Definitions, symbols and abbreviations	12
3.1 Definitions	12
3.2 Symbols.....	13
3.3 Abbreviations	14
3.4 Conventions.....	15
4 Overview of Security Architecture.....	16
5 Security Features	16
5.1 User-to-Network security	16
5.1.0 General.....	16
5.1.1 User identity and device confidentiality	17
5.1.2 Entity authentication	17
5.1.3 User data and signalling data confidentiality	17
5.1.3.1 Ciphering requirements.....	17
5.1.3.2 Algorithm Identifier Values	18
5.1.4 User data and signalling data integrity.....	18
5.1.4.1 Integrity requirements	18
5.1.4.2 Algorithm Identifier Values	18
5.2 Security visibility and configurability	19
5.3 Security requirements on eNodeB.....	19
5.3.1 General.....	19
5.3.2 Requirements for eNB setup and configuration.....	19
5.3.3 Requirements for key management inside eNB.....	20
5.3.4 Requirements for handling User plane data for the eNB	20
5.3.4a Requirements for handling Control plane data for the eNB	20
5.3.5 Requirements for secure environment of the eNB	20
5.4 Void.....	21
6 Security Procedures between UE and EPC Network Elements	21
6.0 General	21
6.1 Authentication and key agreement	21
6.1.1 AKA procedure.....	21
6.1.2 Distribution of authentication data from HSS to serving network.....	22
6.1.3 User identification by a permanent identity	23
6.1.4 Distribution of IMSI and authentication data within one serving network domain	24
6.1.5 Distribution of IMSI and authentication data between different serving network domains.....	25
6.1.6 Distribution of IMSI and UMTS authentication vectors between MMEs or between MME and SGSN	25
6.2 EPS key hierarchy	26
6.3 EPS key identification	28
6.4 Handling of EPS security contexts	29
6.5 Handling of NAS COUNTS.....	29
7 Security Procedures between UE and EPS Access Network Elements.....	31
7.0 General	31
7.1 Mechanism for user identity confidentiality	31
7.2 Handling of user-related keys in E-UTRAN	31
7.2.1 E-UTRAN key setting during AKA	31
7.2.2 E-UTRAN key identification.....	31

7.2.3	E-UTRAN key lifetimes	32
7.2.4	Security mode command procedure and algorithm negotiation.....	32
7.2.4.1	Requirements for algorithm selection	32
7.2.4.2	Procedures for AS algorithm selection.....	33
7.2.4.2.1	Initial AS security context establishment	33
7.2.4.2.2	X2-handover	33
7.2.4.2.3	S1-handover.....	33
7.2.4.2.4	Intra-eNB handover	33
7.2.4.3	Procedures for NAS algorithm selection.....	33
7.2.4.3.1	Initial NAS security context establishment	33
7.2.4.3.2	MME change	34
7.2.4.4	NAS security mode command procedure.....	34
7.2.4.5	AS security mode command procedure.....	35
7.2.4a	Algorithm negotiation for unauthenticated UEs in LSM	36
7.2.5	Key handling at state transitions to and away from EMM-DEREGISTERED	37
7.2.5.1	Transition to EMM-DEREGISTERED.....	37
7.2.5.2	Transition away from EMM-DEREGISTERED.....	38
7.2.5.2.1	General	38
7.2.5.2.2	With existing native EPS NAS security context.....	38
7.2.5.2.3	With run of EPS AKA	39
7.2.6	Key handling in ECM-IDLE to ECM-CONNECTED and ECM-CONNECTED to ECM-IDLE transitions.....	39
7.2.6.1	ECM-IDLE to ECM-CONNECTED transition.....	39
7.2.6.2	Establishment of keys for cryptographically protected radio bearers	39
7.2.6.3	ECM-CONNECTED to ECM-IDLE transition.....	40
7.2.7	Key handling for the TAU procedure when registered in E-UTRAN	40
7.2.8	Key handling in handover.....	41
7.2.8.1	General	41
7.2.8.1.1	Access stratum.....	41
7.2.8.1.2	Non access stratum	42
7.2.8.2	Void.....	42
7.2.8.3	Key derivations for context modification procedure.....	42
7.2.8.4	Key derivations during handovers.....	43
7.2.8.4.1	Intra-eNB Handover	43
7.2.8.4.2	X2-handover	43
7.2.8.4.3	S1-Handover.....	43
7.2.8.4.4	UE handling.....	44
7.2.9	Key-change-on-the fly	44
7.2.9.1	General	44
7.2.9.2	K _{eNB} re-keying.....	44
7.2.9.3	KeNB refresh	45
7.2.9.4	NAS key re-keying.....	45
7.2.10	Rules on Concurrent Running of Security Procedures	45
7.2.11	Suspend and resume of RRC connection	46
7.2.11.1	General	46
7.2.11.2	RRC connection suspend	46
7.2.11.3	RRC connection resume to a new eNB	47
7.2.11.4	RRC connection resume to the same eNB	48
7.3	UP security mechanisms	48
7.3.1	UP confidentiality mechanisms	48
7.3.2	UP integrity mechanisms	48
7.4	RRC security mechanisms.....	49
7.4.1	RRC integrity mechanisms	49
7.4.2	RRC confidentiality mechanisms	49
7.4.3	K _{eNB} * and Token Preparation for the RRCConnectionRe-establishment Procedure	49
7.4.4	RRCConnection re-establishment procedure for Control Plane CIoT EPS optimisation	50
7.5	Signalling procedure for periodic local authentication.....	51
8	Security mechanisms for non-access stratum signalling and data via MME	52
8.0	General	52
8.1	NAS integrity mechanisms.....	52
8.1.1	NAS input parameters and mechanism.....	52

8.1.2	NAS integrity activation	52
8.2	NAS confidentiality mechanisms	53
9	Security interworking between E-UTRAN and UTRAN.....	53
9.1	RAU and TAU procedures	53
9.1.1	RAU procedures in UTRAN.....	53
9.1.2	TAU procedures in E-UTRAN	54
9.2	Handover	56
9.2.1	From E-UTRAN to UTRAN	56
9.2.2	From UTRAN to E-UTRAN	57
9.2.2.1	Procedure	57
9.2.2.2	Derivation of NAS keys and K_{eNB} during Handover from UTRAN to E-UTRAN	61
9.3	Recommendations on AKA at IRAT-mobility to E-UTRAN	61
9.4	Attach procedures.....	62
9.4.1	Attach in UTRAN.....	62
10	Security interworking between E-UTRAN and GERAN.....	62
10.1	General	62
10.2	RAU and TAU procedures	63
10.2.1	RAU procedures in GERAN.....	63
10.2.2	TAU procedures in E-UTRAN	63
10.3	Handover	63
10.3.1	From E-UTRAN to GERAN	63
10.3.2	From GERAN to E-UTRAN	63
10.3.2.1	Procedures	63
10.4	Recommendations on AKA at IRAT-mobility to E-UTRAN	63
10.5	Attach procedures.....	64
10.5.1	Attach in GERAN.....	64
11	Network Domain Control Plane protection.....	64
12	Backhaul link user plane protection	64
13	Management plane protection over the S1 interface	65
14	SRVCC between E-UTRAN and Circuit Switched UTRAN/GERAN.....	66
14.1	From E-UTRAN to Circuit Switched UTRAN/GERAN	66
14.2	Emergency call in SRVCC from E-UTRAN to circuit switched UTRAN/GERAN	67
14.3	SRVCC from circuit switched UTRAN/GERAN to E-UTRAN.....	67
14.3.1	Procedure	67
15	Security Aspects of IMS Emergency Session Handling	70
15.1	General	70
15.2	Security procedures and their applicability	71
15.2.1	Authenticated IMS Emergency Sessions	71
15.2.1.1	General	71
15.2.1.2	UE and MME share a current security context	71
15.2.2	Unauthenticated IMS Emergency Sessions	72
15.2.2.1	General	72
15.2.2.2	UE and MME share no security context	73
15.2.3	Void	74
15.2.4	Key generation procedures for unauthenticated IMS Emergency Sessions	74
15.2.4.1	General	74
15.2.4.2	Handover.....	74
16	Void.....	74
Annex A (normative): Key derivation functions		75
A.1	KDF interface and input parameter construction	75
A.1.1	General	75
A.1.2	FC value allocations	75
A.2	K_{ASME} derivation function	75
A.3	K_{eNB} derivation function.....	76

A.4	NH derivation function.....	76
A.5	K_{eNB}^* derivation function.....	76
A.6	Void.....	76
A.7	Algorithm key derivation functions	77
A.8	K_{ASME} to CK', IK' derivation at handover.....	77
A.9	NAS token derivation for inter-RAT mobility	78
A.10	K'_{ASME} from CK, IK derivation during handover.....	78
A.11	K'_{ASME} from CK, IK derivation during idle mode mobility	78
A.12	K_{ASME} to CK_{SRVCC} , IK_{SRVCC} derivation	79
A.13	K_{ASME} to CK', IK' derivation at idle mobility	79
A.14	(Void)	79
A.15	Derivation of S- K_{eNB} for dual connectivity	79
A.16	Derivation of LWIP-PSK	79
A.17	Derivation of K_n for IOPS subscriber key separation.....	80
A.18	Derivation of S- K_{WT} for LWA	80
Annex B (normative): Algorithms for ciphering and integrity protection		81
B.0	Null ciphering and integrity protection algorithms	81
B.1	128-bit ciphering algorithm.....	81
B.1.1	Inputs and outputs	81
B.1.2	128-EEA1	82
B.1.3	128-EEA2.....	82
B.1.4	128-EEA3.....	82
B.2	128-Bit integrity algorithm.....	83
B.2.1	Inputs and outputs	83
B.2.2	128-EIA1	83
B.2.3	128-EIA2.....	83
B.2.4	128-EIA3.....	84
Annex C (informative): Algorithm test data		85
C.1	128-EEA2.....	85
C.1.1	Test Set 1	85
C.1.2	Test Set 2.....	86
C.1.3	Test Set 3.....	87
C.1.4	Test Set 4.....	87
C.1.5	Test Set 5.....	88
C.1.6	Test Set 6.....	89
C.2	128-EIA2.....	92
C.2.1	Test Set 1	93
C.2.2	Test Set 2.....	94
C.2.3	Test Set 3.....	95
C.2.4	Test Set 4.....	96
C.2.5	Test Set 5.....	97
C.2.6	Test Set 6.....	98
C.2.7	Test Set 7.....	100
C.2.8	Test Set 8.....	102
C.3	128-EEA1	114
C.4	128-EIA1	114
C.4.1	Test Set 1	114

C.4.2	Test Set 2.....	115
C.4.3	Test Set 3.....	115
C.4.4	Test Set 4.....	115
C.4.5	Test Set 5.....	116
C.4.6	Test Set 6.....	116
C.4.7	Test Set 7.....	116
Annex D (normative): Security for Relay Node Architectures		119
D.1	Introduction	119
D.2	Solution	119
D.2.1	General	119
D.2.2	Security Procedures	119
D.2.3	USIM Binding Aspects	122
D.2.4	Enrolment procedures for RNs.....	122
D.2.5	Secure management procedures for RNs.....	123
D.2.6	Certificate and subscription handling	123
D.3	Secure channel profiles	125
D.3.1	General	125
D.3.2	APDU secure channel profile.....	125
D.3.3	Key agreement based on certificate exchange.....	125
D.3.3.1	TLS profile.....	125
D.3.3.2	Common profile for RN and UICC certificate.....	125
D.3.3.3	RN certificate profile	126
D.3.3.4	UICC certificate profile	126
D.3.4	Key agreement for pre-shared key (psk) case.....	126
D.3.5	Identities used in key agreement	127
Annex E (normative): Dual connectivity.....		128
E.1	Introduction	128
E.2	Dual connectivity offload architecture	129
E.2.1	Protection of the X2 reference point.....	129
E.2.2	Addition and modification of DRB in SeNB.....	129
E.2.3	Activation of encryption/decryption.....	129
E.2.4	Derivation of keys for the DRBs in the SeNB.....	131
E.2.4.1	SCG Counter maintenance.....	131
E.2.4.2	Security key derivation	131
E.2.4.3	Negotiation of security algorithms.....	132
E.2.5	S-K _{eNB} update	132
E.2.5.1	S-K _{eNB} update triggers	132
E.2.5.2	S-K _{eNB} update procedure.....	132
E.2.6	Handover procedures.....	132
E.2.7	Periodic local authentication procedure	132
E.2.8	Radio link failure recovery	133
E.2.9	Avoiding key stream reuse caused by DRB type change	133
Annex F (informative): Isolated E-UTRAN Operation for Public Safety.....		134
F.1	General Description.....	134
F.2	IOPS security solution.....	134
F.3	Security Considerations.....	135
F.3.1	Malicious switching of USIM applications.....	135
F.3.2	Compromise of local HSSs	135
F.4	Mitigation of compromise of a local HSS.....	135
F.4.0	Introduction	135
F.4.1	'Subscriber key separation' mechanism	135
F.4.2	Key derivation mechanism for 'subscriber key separation'.....	136
F.5	Actions in case of compromise of a local HSS	137

Annex G (normative):	LTE - WLAN aggregation	138
G.1	Introduction	138
G.2	LTE-WLAN aggregation security	139
G.2.1	Protection of the WLAN Link between the UE and the WT	139
G.2.2	Protection of the Xw interface	139
G.2.3	Addition, modification and release of DRBs in LWA	139
G.2.4	Derivation of keys for the DRBs in LWA	140
G.2.4.1	WT Counter maintenance	140
G.2.4.2	Security key derivation	140
G.2.5	Security key update	140
G.2.5.1	Security key update triggers	140
G.2.5.2	Security key update procedures	141
G.2.6	Handover procedures	141
G.2.7	Periodic local authentication procedure	141
G.2.8	LTE and WLAN link failure	141
G.3	Method for installing PMK	141
Annex H (normative):	LTE-WLAN RAN level integration using IPsec tunnelling	144
H.1	General	144
H.2	Security of LTE-WLAN integration using IPsec Tunnelling	145
H.2.1	eNB to UE interaction for setting up the LWIP offload	145
H.2.2	UE to LWIP-SeGW interaction for setting up the LWIP offload	146
H.2.3	eNB to LWIP-SeGW interaction for setting the LWIP offload	146
H.3	Addition and modification of DRB in LTE-WLAN integration	147
H.4	Security Key for IKEv2 handshake	147
H.4.0	LWIP counter maintenance	147
H.4.1	Security Key (LWIP-PSK) Derivation	147
H.4.2	Security key (LWIP-PSK) update	147
H.5	Handover procedures	148
H.6	LWIP radio link failure	148
Annex I (normative):	Hash functions	149
I.1	General	149
I.2	HASH _{MME} and HASH _{UE}	149
Annex I (informative):	Change history	150
History	156

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.

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.