ETSI TS 133 401 V15.8.0 (2019-07)

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 15.8.0 Release 15)

Reference
RTS/TSGS-0333401vf80

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

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.

Legal Notice

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

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

The cross reference between 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

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.

[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".