ETSI TS 133 102 V16.0.0 (2020-08)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
3G security;
Security architecture
(3GPP TS 33.102 version 16.0.0 Release 16)

3GPP A GLOBAL INITIATIVE
GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference

RTS/TSGS-0333102vg00

Keywords

GSM,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

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 (TS) 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

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (TS 21.133 [1]) and implement the security objectives and principles described in TS 33.120 [2]. A security mechanism is an element that is used to realise a security feature. All security features and security mechanisms taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e. intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the MS are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

GSM security functions are defined in the TS 43.020 [36].

NOTE: The usage of the authentication management field (AMF) is specified in Annex H and applies for the third (UMTS), fourth (LTE) and fifth (5G system) generation of mobile telecommunication systems.

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 TS 21.133: "3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] 3GPP TS 43.020: "Security related network functions".

[9] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol specification".

[18] 3GPP TS 25.321: "Medium Access Control (MAC) protocol specification".

[19] 3GPP TS 25.322: "Radio Link Control (RLC) protocol specification".

[20] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] 3GPP TS 23.195: "Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".

[23] 3GPP TS 43.129: "Packed-switched handover for GERAN A/Gb mode; Stage 2".

[24] 3GPP TS 35.215: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[25] 3GPP TS 35.216: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification".

[26] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[27] 3GPP TS 35.218: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 4: Design conformance test data".

[28] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security architecture".

[29] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non 3GPP accesses".

[30] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[31] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[32] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[33] 3GPP TS 22.101: "Service aspects; Service principles".

[34] 3GPP TS 23.167: " IP Multimedia Subsystem (IMS) emergency sessions".

[35] 3GPP TS 24.008: " Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[36] 3GPP TS 43.020: "Security related network functions".

[37] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[38] 3GPP TS 25.420: "UTRAN Iur interface general aspects and principles".

[39] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[40] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

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

[42] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

3 Definitions, symbols abbreviations and conventions

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101 [21], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905 [3]. 'User Equipment', 'USIM', 'SIM' and 'IC Card' have been defined in TS 22.101 [21].

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in 3GPP TS 43.020.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5).

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA or as a result of inter RAT mobility from E-UTRAN [28] to UTRAN or GERAN. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.

Rel4- ME: Refers to a ME that conforms to Rel-4 or R99 specifications.

Rel5+ ME: Refers to a ME that conforms to Rel-5 or later specifications.

ME capable of UMTS AKA: either a Rel4- ME that does support USIM-ME interface or a Rel5+ ME.

ME not capable of UMTS AKA: a Rel4- ME that does not support USIM-ME interface or a R98- ME.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MAC-S
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK in normal procedures
f5*	Key generating function used to compute AK in re-synchronisation procedures
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], for the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
DSCP	Differentiated Services Code Point
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
GERAN	GSM/EDGE Radio Access Network
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
Kc	64-bit GSM ciphering key
Kc_{128}	128-bit GSM ciphering key
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre

PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
SQN	Sequence number
SQN_{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN_{MS}	The highest sequence number the USIM has accepted
SRVCC	Single Radio Voice Call Continuity
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VLR	Visitor Location Register
XRES	Expected Response

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

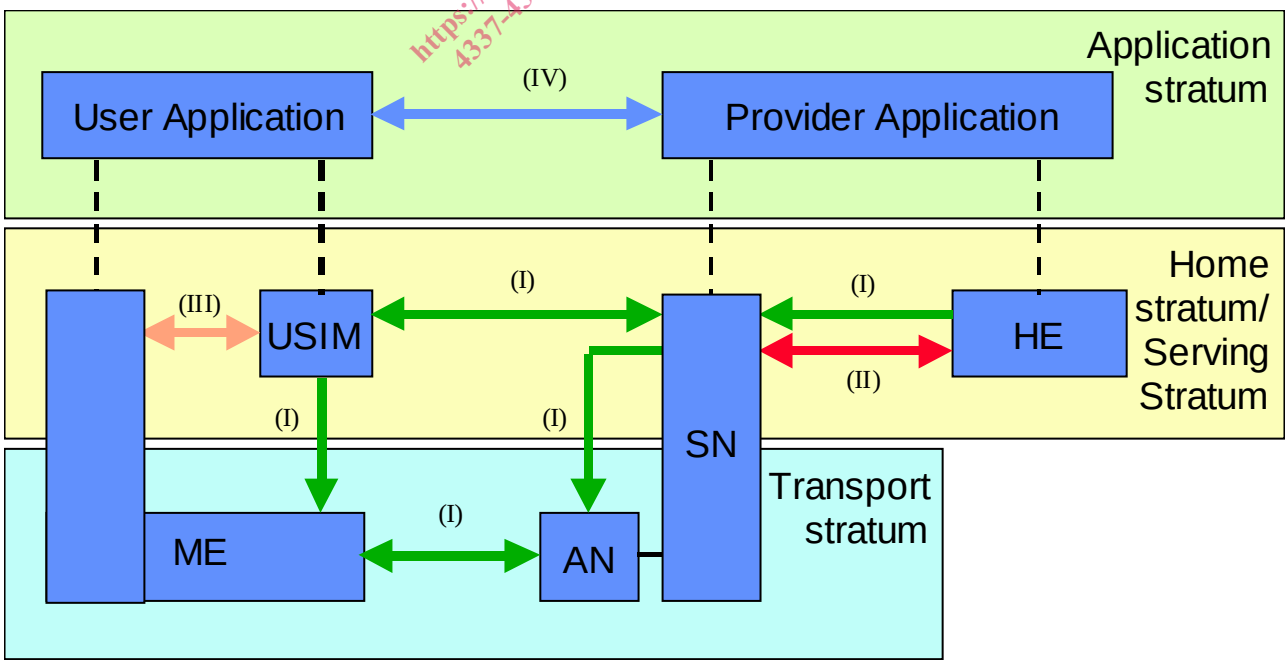

Figure 1: Overview of the security architecture