ETSI TS 133 102 V14.1.0 (2017-03)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
3G security;
Security architecture
(3GPP TS 33.102 version 14.1.0 Release 14)

3GPP A GLOBAL INITIATIVE
GSM GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGS-0333102ve10

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

Intellectual Property Rights

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.

Foreword

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

Foreword

This Technical Specification (TS) has been produced by ETSI 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].

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".