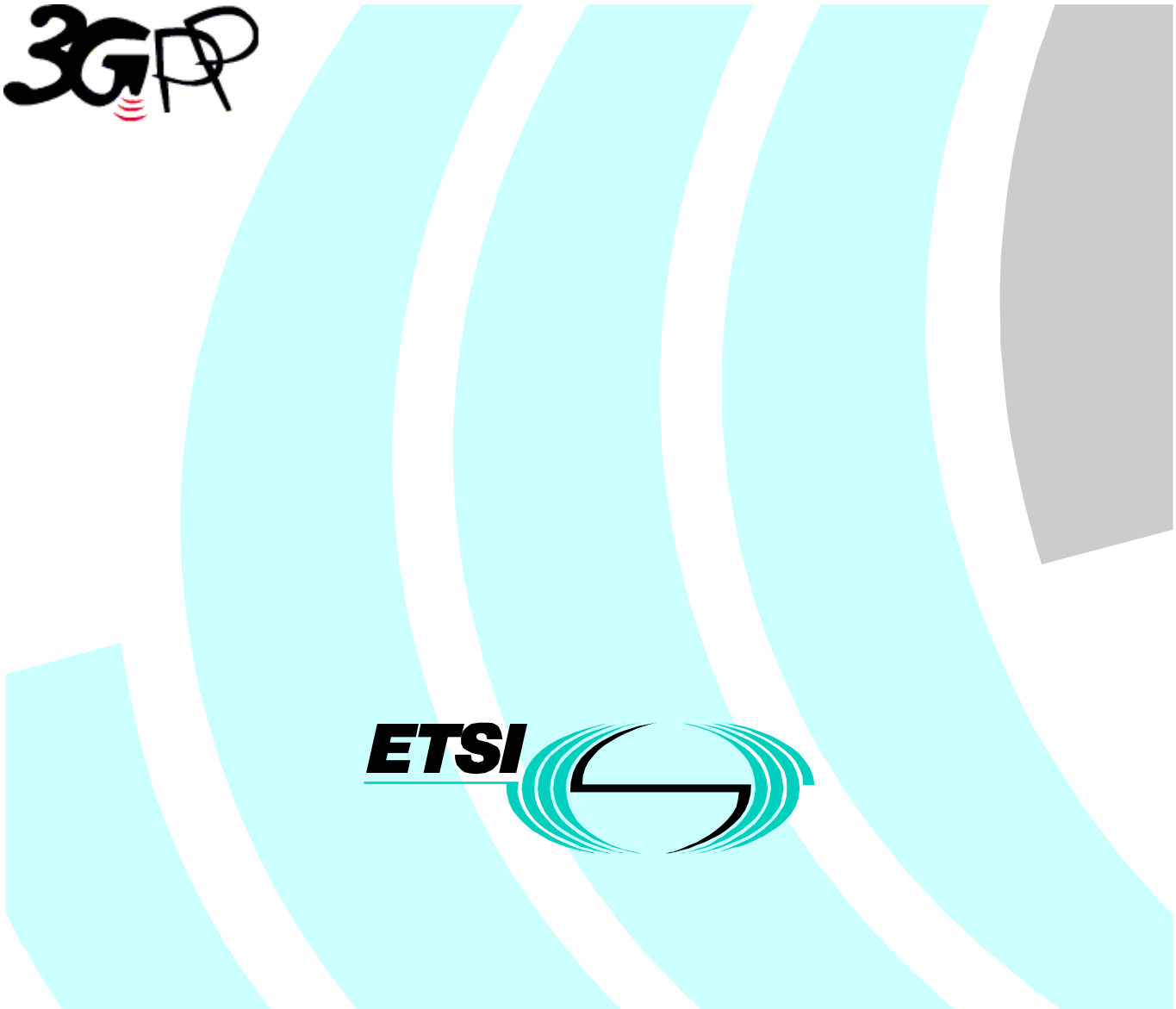
ETSI TS 133 120 V4.0.0 (2001-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
3G Security;
Security Principles and Objectives
(3GPP TS 33.120 version 4.0.0 Release 4)



Reference
RTS/TSGS-0333120Uv4

Keywords
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 (http://www.etsi.org/ipr).

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

This Technical Specification (TS) has been produced by the 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 www.etsi.org/key .

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 gives the objectives and principles of 3GPP security.

The principles state what is to be provided by 3G security as compared to the security of second generation systems. The principles will also ensure that 3G security can secure the new services and new service environments offered by 3G systems.

The objectives give general, high level requirements for 3GPP security which will be expanded upon in 3G TS 21.133 [1].

The priorities for the implementation of 3GPP security are also given.

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] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] UMTS 33.21, V3.0.0: "Universal Mobile Telecommunications System (UMTS); Security Requirements".

[3] ARIB, Volume 1: "Requirements and Objectives for 3G Mobile Services and System (Ver.0.8)", Annex 8.

[4] Tdoc S3-99014, 3GPP TSG SA, WG3 (Security), London, 2-4 February, 1999.

3 Abbreviations

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

HE	Home Environment
IMEI	International Mobile Equipment Identifier
LI	Lawful Interception
MExE	Mobile Execution Environment
SAT	SIM Application Toolkit
SN	Serving Network
SIM	Subscriber Identity Module

4 3G Security Principles

There are three key principles behind 3G security:

1) 3G security will build on the security of second generation systems. Security elements within GSM and other second generation systems that have proved to be **needed** and **robust** shall be adopted for 3G security. These elements are listed in subclause 4.1.

2) 3G security will improve on the security of second generation systems - 3G security will address and correct real and perceived weaknesses in second generation systems. The most important of these are given in subclause 4.2.

3) 3G security will offer new security features and will secure new services offered by 3G.

4.1 Second Generation Security Elements to be retained

3G security shall retain (and in some cases develop) the following security elements of second generation systems:

a) authentication of subscribers for service access.

   Problems with inadequate algorithms will be addressed. Conditions regarding the optionality of authentication and its relationship to encryption shall be clarified and tightened;

b) radio interface encryption.

   The strength of the encryption will be greater than that used in second generation systems (the strength is a combination of key length and algorithm design). This is to meet the threat posed by the increased computing power available to those attempting cryptanalysis of the radio interface encryption. Problems caused by multiple algorithms will be dealt with (note);

NOTE: The method of negotiating which algorithm to be used is open to attack.

c) subscriber identity confidentiality on the radio interface.

   However, a more secure mechanism will be provided;

d) the SIM as:

   a **removable**, **hardware** security module that is:

   - manageable by network operators;
   - independent of the terminal as regards its security functionality.

e) SIM application toolkit security features providing a secure application layer channel between the SIM and a home network server.

   Other application layer channels may also be provided;

f) the operation of security features is independent of the user, i.e. the user does not have to do anything for the security features to be in operation.

   However, greater user visibility of the operation of security features will be provided to the user;

g) HE trust in the SN for security functionality is minimised.

4.2 Weaknesses in Second Generation security

The following weaknesses in the security of GSM (and other second generation systems) will be corrected in 3G security:

1) active attacks using a “false BTS” are possible;

2) cipher keys and authentication data are transmitted in clear between and within networks;

3) encryption does not extend far enough towards the core network resulting in the cleartext transmission of user and signalling data across microwave links (in GSM, from the BTS to the BSC);

4) user authentication using a previously generated cipher key (where user authentication using RAND, SRES and A3/8 is not provided) and the provision of protection against channel hijack rely on the use of encryption, which provides implicit user authentication. However, encryption is not used in some networks, leaving opportunities for fraud;

5) data integrity is not provided. Data integrity defeats certain false BTS attacks and, in the absence of encryption, provides protection against channel hijack;

6) the IMEI is an unsecured identity and should be treated as such;

7) fraud and LI were not considered in the **design phase** of second generation systems but as afterthoughts to the main design work;

8) there is no HE knowledge or control of how an SN uses authentication parameters for HE subscribers roaming in that SN;

9) second generation systems do not have the flexibility to upgrade and improve security functionality over time.

4.3 New Security Features and the Security of New Service Features

The new service features that will be secured cannot be listed at the time of writing. However, the environment in which these features are likely to be developed can be described. 3G security will secure this environment.

The environment in which new services will be developed can be characterised by (but is not limited to) the following aspects:

- there will be new and different providers of services. For example: content providers, data service providers, HLR only service providers;

- 3G mobile systems will be positioned as the preferred means of communications for users. They will be preferable to fixed line systems;

- there will be a variety of prepaid and pay-as-you-go services which may be the rule rather than the exception. A long-term subscription between the user and a network operator may not be the paradigm. (3G security will provide satisfactory security for such systems and will not be content with insecure systems such as GSM Advice of Charge);

- there will be increased control for the user over their service profile (which they might manage over the Internet) and over the capabilities of their terminal (it will be possible to download new services and functions using systems such as MExE and SAT);

- there will be active attacks on users. (In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur);

- non-voice services will be as important as, or more important than, voice services;

- the terminal will be used as a platform for e-commerce and other applications. Multi-application smartcards where the USIM is one application among many can be used with the terminal. The smartcard and terminal will support environments such as Java to allow this. The terminal may support personal authentication of the user using biometric methods.

5 3G Security Objectives

In addition to the above principles for 3G security, there are the high level objectives given below. These will be expanded upon in 3G TS 21.133 [1]:

a) to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;

b) to ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardised are compatible with world-wide availability. (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement));

d) to ensure that the security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks;

e) to ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks (including GSM);

f) to ensure that the implementation of 3GPP security features and mechanisms can be extended and enhanced as required by new threats and services.

6 Priorities

As a priority, 3G security will provide the proven second generation security features described in subclause 4.1 and correct the weaknesses in second generation systems described in subclause 4.2.

Security for new services and service environments will then be developed as required.

Annex A (informative): Change history

Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
Jan 1999	S3_02			draft	0.0.0	Start
Mar 1999	S3_02	0.0.0			0.0.2	Submitted for approval SA#02
SP-02	33.120	2.0.0		R99	3.0.0	Approved at SA#02
SP-11	33.120	3.0.0	-	Rel-4	4.0.0	Upgrade to Release 4

History

Document history		
V4.0.0	March 2001	Publication