

ETSI TS 122 048 V5.0.0 (2003-06)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Security Mechanisms for the (U)SIM application toolkit;
Stage 1
(3GPP TS 22.048 version 5.0.0 Release 5)**



Reference

RTS/TSGT-0322048v500

Keywords

GSM, 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

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, send your comment to:

editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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://webapp.etsi.org/IPR/home.asp>).

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 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> .

Contents

Intellectual Property Rights	2
Foreword.....	2
Foreword.....	4
1 Scope	5
2 References	5
3 Definitions and abbreviations.....	5
3.1 Definitions	5
3.2 Abbreviations	6
4 Introduction	6
5 Security requirements.....	7
5.1 Authentication	8
5.1.1 Definition.....	8
5.1.2 Purpose	8
5.1.3 Functional requirements	8
5.2 Message integrity	9
5.2.1 Definition.....	9
5.2.2 Purpose	9
5.2.3 Functional requirements	9
5.3 Replay detection and sequence integrity	9
5.3.1 Definition.....	9
5.3.2 Purpose	9
5.3.3 Functional requirements	9
5.4 Proof of receipt and proof of execution.....	9
5.4.1 Definition.....	9
5.4.2 Purpose	10
5.4.3 Functional requirements	10
5.5 Message confidentiality.....	10
5.5.1 Definition.....	10
5.5.2 Purpose	10
5.5.3 Functional requirements	10
5.6 Security management	10
6 Normal procedures	11
6.1 Security mechanisms.....	11
6.1.1 Authentication mechanisms	11
6.1.2 Message integrity mechanisms	11
6.1.3 Replay detection and sequence integrity mechanisms	11
6.1.4 Proof of receipt mechanisms.....	11
6.1.5 Message confidentiality mechanisms	12
6.2 Security mechanisms and recommended combinations	12
6.2.1 Non-cryptographic mechanisms	12
6.2.2 Cryptographic mechanisms.....	12
6.2.3 Recommended combinations of cryptographic mechanisms	13
7 Exceptional procedures	13
7.1 Authentication or integrity failure.....	13
7.2 Sequence and replay detection failure	13
7.3 Proof of receipt failure	13
Annex A (informative): Change History	14
History	15