

ETSI TS 133 200 V7.0.0 (2007-06)

Technical Specification

**Universal Mobile Telecommunications System (UMTS);
3G Security;
Network Domain Security (NDS);
Mobile Application Part (MAP) application layer security
(3GPP TS 33.200 version 7.0.0 Release 7)**



Reference

RTS/TSGS-0333200v700

Keywords

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

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, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

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 2007.
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
Introduction	4
1 Scope	5
2 References	5
3 Definitions, symbols and abbreviations	5
3.1 Definitions	5
3.2 Symbols.....	6
3.3 Abbreviations	6
3.4 Conventions.....	6
4 Principles of MAP application layer security.....	7
5 MAP security (MAPsec)	7
5.1 Security services provided by MAPsec	7
5.2 Properties and tasks of MAPsec enabled network elements.....	7
5.3	Policy requirements for the MAPsec Security Policy Database (SPD)
5.4 MAPsec security association attribute definition	8
5.5 MAPsec structure of protected messages	9
5.5.1 MAPsec security header	10
5.5.2 Protected payload.....	10
5.5.2.1 Protection Mode 0.....	10
5.5.2.2 Protection Mode 1	10
5.5.2.3 Protection Mode 2.....	11
5.6 MAPsec algorithms	11
5.6.1 Mapping of MAPsec-SA encryption algorithm identifiers	11
5.6.1.1 Description of MEA-1.....	11
5.6.2 Mapping of MAPsec-SA integrity algorithm identifiers.....	11
5.6.2.1 Description of MIA-1	11
5.6.3 Construction of IV	12
6 MAPsec protection profiles.....	12
6.1 Granularity of protection	12
6.2 MAPsec protection groups	12
6.2.1 MAPsec protection groups.....	12
6.2.1.1 MAP-PG(0) – No Protection.....	12
6.2.1.2 MAP-PG(1) – Protection for Reset	13
6.2.1.3 MAP-PG(2) – Protection for Authentication Information except Handover Situations.....	13
6.2.1.4 MAP-PG(3) – Protection for Authentication Information in Handover Situations.....	13
6.2.1.5 MAP-PG(4) – Protection of non location dependant HLR data.....	14
6.3 MAPsec protection profiles	14
Annex A (informative): Guidelines for manual key management	15
A.1 Inter-domain Security Association and Key Management Procedures	15
A.2 Local Security Association Distribution	15
Annex B (normative): MAPsec message flows	16
Annex C (normative): Using TCAP handshake for SMS transfer.....	19
C.1 Mobile Terminated SMS	19
C.2 Mobile Originated SMS	20
Annex D (informative): Change history	22
History	23

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.

Introduction

The absence of security in Signalling System No. 7 (SS7) networks is an identified security weakness in 2G systems. This was formerly perceived not to be a problem, since the SS7 networks were the provinces of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

For 3G systems it is a clear goal to be able to protect the core network signalling protocols, and by implication this means that security solutions must be found for both SS7 and IP based protocols.

Various protocols and interfaces are used for control plane signalling within and between core networks. The security services that have been identified as necessary are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques.