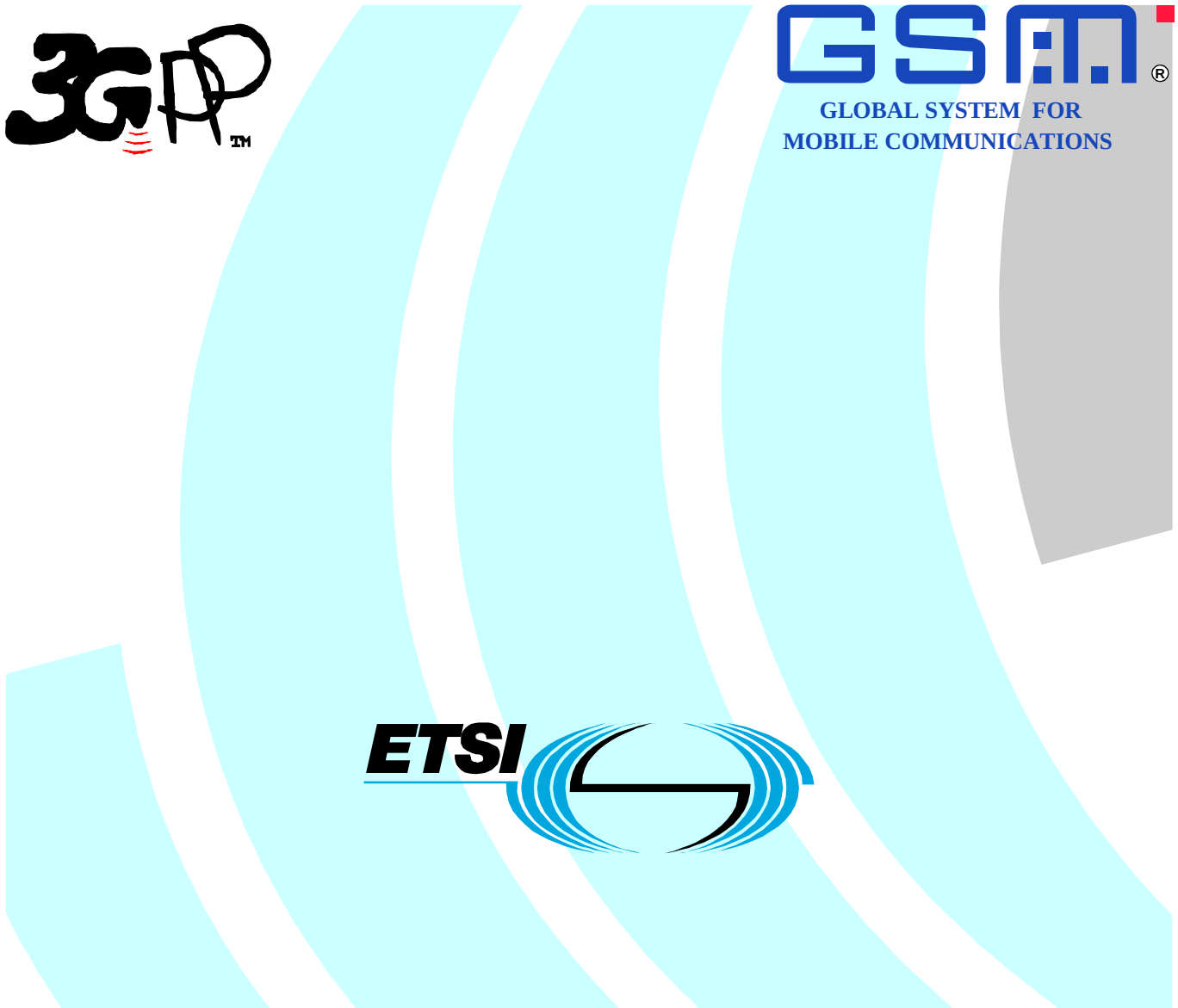
ETSI TS 123 048 V5.9.0 (2005-06)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Security mechanisms for the (U)SIM application toolkit;
Stage 2
(3GPP TS 23.048 version 5.9.0 Release 5)**



Reference
RTS/TSGC-0623048v590

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

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

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 specifies the structure of the Secured Packets in a general format and in implementations using Short Message Service Point to Point (SMS-PP) and Short Message Service Cell Broadcast (SMS-CB).

Furthermore, the coding is specified for a set of common application commands within the secured packets. This set is a subset of commands specified in 3GPP TS 51.011 [5] and allows remote management of files on the UICC in conjunction with SMS and the Data Download to UICC feature of 3GPP TS 31.111.

For UICCs based on 3GPP TS 43.019 [15], the set of commands used in the remote applet management is defined in the present document. This is based on the Open Platform card management specification [14]. For UICCs based on other technologies, other loading mechanisms may be used.

The present document is applicable to the exchange of secured packets between an entity in a 3G or GSM PLMN and an entity in the UICC.

Secured Packets contain application messages to which certain mechanisms according to 3GPP TS 22.048 have been applied. Application messages are commands or data exchanged between an application resident in or behind the 3G or GSM PLMN and on the UICC. The Sending/Receiving Entity in the 3G or GSM PLMN and the UICC are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.048: "Security mechanisms for the (Universal) Subscriber Interface Module (U)SIM Application Toolkit; Stage 1".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4: "Information technology - Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

[8] Void

[9] ISO 8731-1 (1987): "Banking - Approved algorithms for message authentication - Part 1: DEA".

[10] ISO/IEC 10116 (1997): "Information technology - Security techniques - Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".