

**Digital cellular telecommunications system (Phase 2+);
Specification of the A5/3 encryption algorithms for GSM and
ECSD, and the GEA3 encryption algorithm for GPRS;
Document 4: Design and evaluation report
(3GPP TR 55.919 version 4.0.0 Release 4)**



Reference

RTR/TSGS-0355919v400

Keywords

GSM, SECURITY

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 2008.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™, TIPHON™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ 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 Report (TR) 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
4 Technical provisions.....	6
Annex B: Change history	7
History	8

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

This Report has been produced by ETSI SAGE Task Force for the design of the GSM A5/3 and GEA3 encryption algorithms.

The work described in this report was undertaken in response to a request made by Security Group GSM Association. The work was done under supervision of the ETSI Mobile Competence Centre (MCC) and the GSM Association.

1 Scope

This Technical Report has been prepared by the ETSI SAGE GSM A5/3 Task Force, and gives a detailed report on the design and evaluation of the A5/3 encryption algorithms for GSM and ECSD, and of the GEA3 encryption algorithm for GPRS (including EGPRS).

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] | Void |
| [2] | Void |
| [3] | Void |
| [4] | Void |
| [5] | Void |
| [6] | Void |
| [7] | Void |
| [8] | Void |
| [9] | Void |
| [10] | Void |
| [11] | 3GPP TR 21.905: "Vocabulary for 3GPP Specifications". |
| [12] | 3GPP TR 55.919 Release-7 (v7.x.x): "Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report". |

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [11] and in the Release 7 Report [12] apply. A term defined in the latter document takes precedence over the definition of the same term, if any, in TR 21.905 [11].

3.2 Symbols

For the purposes of the present document, the symbols defined in the Release 7 Report [12] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [11] and in the 3GPP Task Force Report [12] apply. An abbreviation defined in the latter document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [11].

4 Technical provisions

The technical provisions of the current document are contained in the Release 7 Report [2].

Annex B: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2002-05	-	-	-	-	ETSI SAGE first publication		SAGE V1.0
2002-07	-	-	-	-	Agreed at SA WG3 #24 for presentation to TSG SA #17 for approval. Converted into 3GPP TR format (TR 55.919) (Technically equivalent to SAGE V1.0)	SAGE V1.0	1.0.0
2002-09	SP-17	SP-020506	-	-	Approved for Release 6 - version 6.0.0	1.0.0	6.0.0
2002-12	SP-18	SP-020721	001	-	EGPRS algorithm	6.0.0	6.1.0
2007-12	SP-38	SP-070776	005	-	Creation of Release 4 version	6.1.0	4.0.0

History

Document history		
V4.0.0	January 2008	Publication