

3GPP TR 55.919 V11.0.0 (2012-09)

Technical Report

**3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Specification of the A5/3 Encryption Algorithms for GSM and
ECSD, and the GEA3 Encryption Algorithm for GPRS;
Document 4: Design and evaluation report
(Release 11)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

GSM, GPRS, security, algorithm

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.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.

© 2012, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark 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
LTE™ is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword4

Introduction4

1 Scope5

2 References.....5

3 Definitions, symbols and abbreviations5

3.1 Definitions5

3.2 Symbols.....6

3.3 Abbreviations.....6

4 Technical provisions6

Annex B: Change history.....7

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 SA GE 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 Task Force Report: "Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS; Document 4: Design and evaluation report".

Note: Reference [2] is available via <http://portal.etsi.org/dvbandca/home.asp> and is subject to licensing conditions described at this site.

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 3GPP Task Force 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 3GPP Task Force 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 3GPP Task Force 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	002	-	Conversion to pointer to export controlled document	6.1.0	7.1.0
2008-12	SP-42	-	-	-	Upgrade to Release 8	7.1.0	8.0.0
2009-12	SP-46	-	-	-	Upgrade to Release 9	8.0.0	9.0.0
Note: Version 7.0.0 is a "readme" file placeholder with no technical content.							
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	11.0.0