

ETSI TS 155 226 V17.0.0 (2022-04)



**Digital cellular telecommunications system (Phase 2+) (GSM);
3G Security;
Specification of the A5/4 Encryption Algorithms for GSM and
ECSD, and the GEA4 Encryption Algorithm for GPRS
(3GPP TS 55.226 version 17.0.0 Release 17)**



Reference

RTS/TSGS-0355226vh00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Technical provisions.....	5
Annex F (informative): Change history	6
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

In this document are specified three ciphering algorithms: A5/4 for GSM, A5/4 for ECSD, and GEA4 for GPRS (including EGPRS). The algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key KC. Each of these algorithms is based on the KASUMI algorithm that is specified in TS 35.202 [5]. The three algorithms are all very similar. We first define a core keystream generator function KGCORE (clause 4); we then specify each of the three algorithms in turn (clauses 5, 6 and 7) in terms of this core function.

Note that:

- GSM A5/4 is the same algorithms as GSM A5/3 but with KLEN changed from 64 to 128 bits.
- and ECSD A5/4 is the same algorithms as ECSD A5/3 but with KLEN changed from 64 to 128 bits.
- and GEA 4 is the same algorithms as GEA3 but with KLEN changed from 64 to 128 bits.

1 Scope

This specification of the **A5/4** encryption algorithms for GSM and ECSD, and of the **GEA4** encryption algorithm for GPRS has been derived from TS 55.516 [1]: Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the **GEA3** Encryption Algorithm for GPRS. The only essential change is the change of external key length input from 64 bits to 128 bits.

This document should be read in conjunction with the entire specification of the **A5/3** and **GEA3** algorithms:

- Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS. Document 1: A5/3 and GEA3 Specifications.
- Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS. Document 2: Implementors' Test Data.
- Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS. Document 3: Design Conformance Test Data.

The normative part of the specification of the block cipher (**KASUMI**) on which the **A5/3**, **A5/4**, **GEA3** and **GEA4** algorithms are based can be found in TS 35.202 [5].

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] to [5] (void)

[6] 3GPP Task Force Specification: "3G Security; Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS", version 9.0.0.

Note: Reference [6] is available via <http://www.etsi.org/WebSite/OurServices/Algorithms/algorithms.aspx> and is subject to licensing conditions described at this site.

3 Technical provisions

The technical provisions of the current document are contained in the 3GPP Task Force Specification [6].

Annex F (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
02-2004	-	-	-	-	Draft presented to SA WG3 for agreement	---	0.1.0
03-2004	SA_23	SP-040170	-	-	Draft provided to TSG SA for information	0.1.0	1.0.0
09-2009	SA_45	SP-090647	-	-	Draft provided to TSG SA for approval	1.0.0	2.0.0
09-2009	SA_45	SP-090647	-	-	Approval at SA#45 and placement under CR control	2.0.0	9.0.0
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
2014-09	-	-	-	-	Update to Rel-12 version (MCC)	11.0.0	12.0.0
2016-01	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	13.0.0
2017-03	SA#75	-	-	-	Promotion to Release 14 without technical change	13.0.0	14.0.0
2018-10	-	-	-	-	Update to Rel-15 version (MCC)	14.0.0	15.0.0
2020-07	-	-	-	-	Update to Rel-16 version (MCC)	15.0.0	16.0.0
2022-03	-	-	-	-	Update to Rel-17 version (MCC)	16.0.0	17.0.0

History

Document history		
V17.0.0	April 2022	Publication