ETSI TS 155 226 V16.0.0 (2020-08)

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 16.0.0 Release 16)

3GPP™ A GLOBAL INITIATIVE
GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGS-0355226vg00

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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

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.

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

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 provisons 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**

History

Document history		
V16.0.0	August 2020	Publication