3GPP TS 35.215 V9.0.0 (2009-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications (Release 9)

Keywords
UMTS, 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

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 3GPP confidentiality and integrity algorithms known as UEA2 and UIA2.

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] ETSI TC SAGE Specification: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications" v2.1.

Note: Reference [2] is available via http://www.etsi.org/WebSite/OurServices/Algorithms/algorithms.aspx 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 [1] and in the SAGE Specification [2] apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Symbols

For the purposes of the present document, the symbols defined in the SAGE Specification [2] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [2] and in the SAGE Specification [2] apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

4 Technical provisions

The technical provisions of the current document are contained in the SAGE Specification [2].

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2006-10					Draft document from ETSI SAGE		0.1.0
2006-03	SP-31				For information to TSG SA. Document not provided due to limitations arising from export controls.	0.1.0	1.0.0
2006-03					3GPP Support Team recast of document to refer to SAGE Specification	1.0.0	1.1.0
2006-06	SP-32	SP-060422	-	-	Approved at SA #32	1.1.0	7.0.0
2008-12	SP-42	-	-	-	Upgrade to Release 8	7.0.0	8.0.0
2009-03	SP-43	SP-090140	0001		Improvement to sample C code, and removal of apparent keystream length limit	8.0.0	8.1.0
2009-12	-	-	-	-	Update to Rel-9 version (MCC)	8.1.0	9.0.0