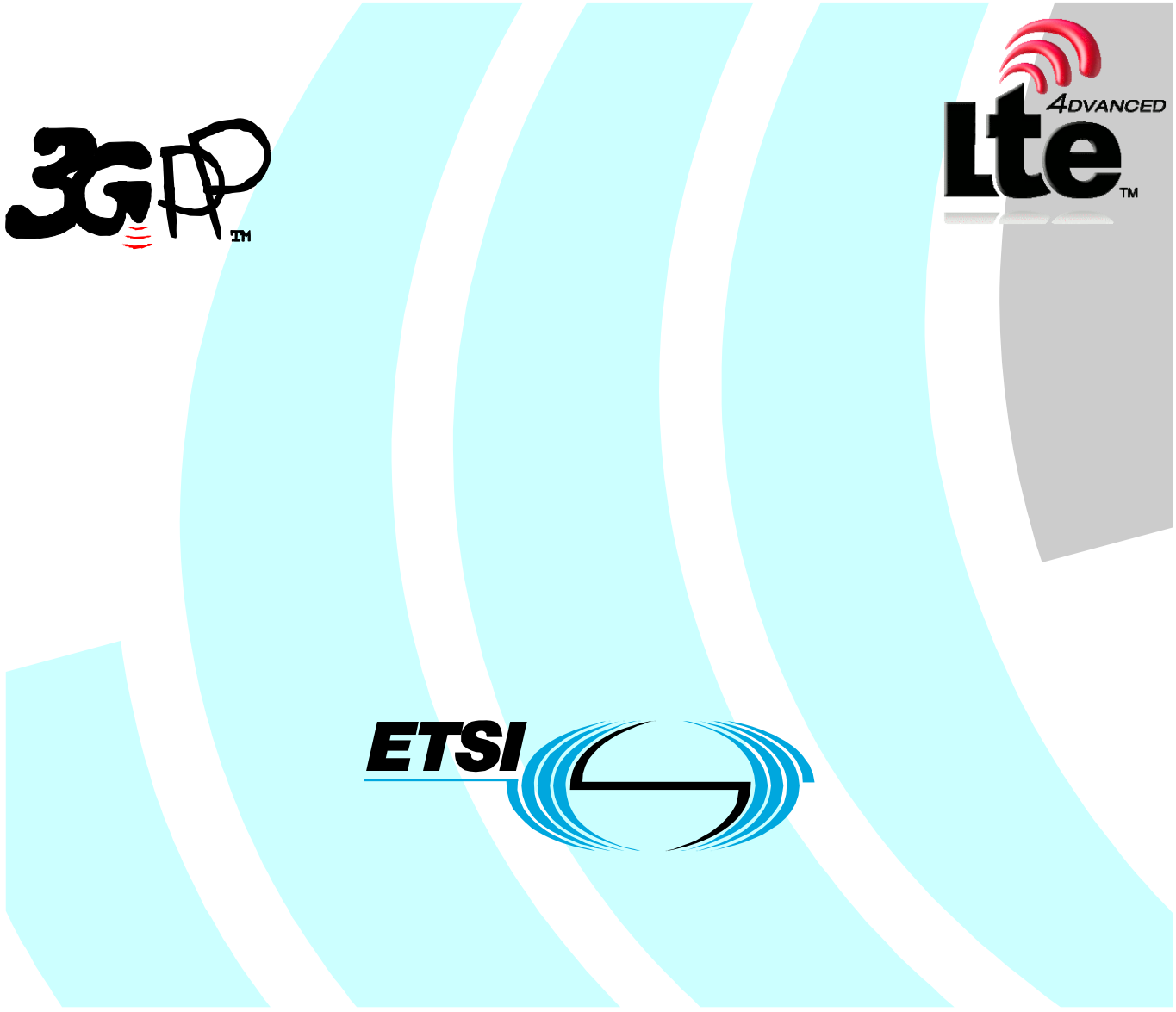
# ETSI TR 135 919 V10.0.0 (2011-04)

*Technical Report*

**Digital cellular telecommunications system (Phase 2+);**
**Universal Mobile Telecommunications System (UMTS);**
**LTE;**
**Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2;**
**Document 5: Design and evaluation report**
**(3GPP TR 35.919 version 10.0.0 Release 10)**



Reference
RTR/TSGS-0335919va00

Keywords
GSM, LTE, SECURITY, UMTS

***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

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

# 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 5: Design and evaluation report" version 1.1, 2006-09-06

NOTE: Reference [2] is available via http://www.etsi.org/WebSite/OurServices/Algorithms/3gppalgorithms.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 provisons of the current document are contained in the SAGE Specification [2].

# Annex A:
# 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. | 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 | | | | | Correction of typographical error. | 1.1.0 | 1.1.1 |
| 2006-06 | SP-32 | SP-060422 | - | - | Approved at SA #32 | 1.1.1 | 7.0.0 |
| 2008-12 | SP-42 | - | - | - | Upgrade to Release 8 | 7.0.0 | 8.0.0 |
| 2010-03 | -- | -- | -- | -- | Upgrade to Release 9 | 8.0.0 | 9.0.0 |
| 2010-12 | SP-50 | SP-100724 | 001 | 1 | Correction of reference | 9.0.0 | 9.1.0 |
| 2011-03 | - | - | - | - | Update to Rel-10 version (MCC) | 9.1.0 | 10.0.0 |

# History

| Document history | | |
|---|---|---|
| V10.0.0 | April 2011 | Publication |
| | | |
| | | |
| | | |
| | | |