

ETSI TS 135 206 V12.0.0 (2014-10)



**Universal Mobile Telecommunications System (UMTS);
LTE;
3G Security;
Specification of the MILENAGE algorithm set:
An example algorithm set for the 3GPP authentication
and key generation functions f_1 , f_1^* , f_2 , f_3 , f_4 , f_5 and f_5^* ;
Document 2: Algorithm specification
(3GPP TS 35.206 version 12.0.0 Release 12)**



Reference

RTS/TSGS-0335206vc00

Keywords

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

Important notice

The present document can be downloaded from:

<http://www.etsi.org>

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

<http://portal.etsi.org/tb/status/status.asp>

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

http://portal.etsi.org/chaicor/ETSI_support.asp

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.

© European Telecommunications Standards Institute 2014.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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://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.

Foreword

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, 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>.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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
Foreword.....	2
Modal verbs terminology.....	2
Foreword.....	5
Introduction	5
0 The name "MILENAGE"	6
1 Outline of the document.....	6
1.1 References	6
2 INTRODUCTORY INFORMATION	7
2.1 Introduction	7
2.2 Notation.....	7
2.2.1 Radix.....	7
2.2.2 Conventions	7
2.2.3 Bit/Byte ordering	7
2.2.4 List of Symbols.....	8
2.3 List of Variables	8
2.4 Algorithm Inputs and Outputs	8
3 The algorithm framework and the specific example algorithms	9
4 Definition of the example algorithms.....	10
4.1 Algorithm Framework.....	10
4.2 Specific Example Algorithms.....	10
5 Implementation considerations.....	11
5.1 OP_C computed on or off the USIM?	11
5.2 Customising the choice of block cipher	11
5.3 Further customisation	12
5.4 Resistance to side channel attacks	12
Annex 1: Figure of the Algorithms	13
Annex 2: Specification of the Block Cipher Algorithm Rijndael.....	14
A2.1 Introduction	14
A2.2 The State and External Interfaces of Rijndael.....	14
A2.3 Internal Structure.....	15
A2.4 The Byte Substitution Transformation	15
A2.5 The Shift Row Transformation.....	16
A2.6 The Mix Column Transformation	16
A2.7 The Round Key addition	17
A2.8 Key schedule	17
A2.9 The Rijndael S-box.....	18
Annex 3: Simulation Program Listing - Byte Oriented	19
Annex 4: Rijndael Listing - 32-Bit Word Oriented.....	26
Annex A (informative): Change history	32

History33

Foreword

This Technical Specification (TS) 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 document has been prepared by the 3GPP Task Force, and contains an example set of algorithms which may be used as the authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**. (It is not mandatory that the particular algorithms specified in this document are used — all seven functions are operator-specifiable rather than being fully standardised). This document is one five, which between them form the entire specification of the example algorithms, entitled:

- 3GPP TS 35.205: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**; Document 1: General".
- 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**; **Document 2: Algorithm Specification**".
- 3GPP TS 35.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**; Document 3: Implementors' Test Data".
- 3GPP TS 35.208: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**; Document 4: Design Conformance Test Data".
- 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions *f1*, *f1**, *f2*, *f3*, *f4*, *f5* and *f5**; Document 5: Summary and results of design and evaluation".