



TECHNICAL REPORT

**Universal Mobile Telecommunications System (UMTS);
LTE;**

Specification of the TUAk algorithm set:

**A second 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 4: Report on the design and evaluation
(3GPP TR 35.934 version 14.0.0 Release 14)**



Reference

RTR/TSGS-0335934ve00

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/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 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

<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/CommiteeSupportStaff.aspx>

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 2017.

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.

oneM2M logo is protected for the benefit of its Members

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 (<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.

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>.

Modal verbs terminology

In the present document "**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 |
| Foreword..... | 2 |
| Modal verbs terminology..... | 2 |
| Foreword..... | 5 |
| 1 Scope | 6 |
| 2 References | 6 |
| 3 Definitions and abbreviations..... | 7 |
| 3.1 Definitions | 7 |
| 3.2 Abbreviations | 7 |
| 4 Structure of this report..... | 8 |
| 5 Background to the design and evaluation work | 8 |
| 6 Summary of algorithm requirements..... | 9 |
| 6.0 Introduction | 9 |
| 6.1 General requirements for 3GPP cryptographic functions and algorithms (as stated for MILENAGE)..... | 9 |
| 6.2 Authentication and key agreement functions (as stated for MILENAGE)..... | 9 |
| 6.2.0 Introduction..... | 9 |
| 6.2.1 Implementation and operational considerations..... | 10 |
| 6.2.2 Type of algorithm | 10 |
| 6.2.2.1 $f1$ | 10 |
| 6.2.2.2 $f1^*$ | 10 |
| 6.2.2.3 $f2$ | 10 |
| 6.2.2.4 $f3$ | 10 |
| 6.2.2.5 $f4$ | 10 |
| 6.2.2.6 $f5$ | 11 |
| 6.2.2.7 $f5^*$ | 11 |
| 6.3 Tuak-specific requirements | 11 |
| 6.3.1 Difference from MILENAGE..... | 11 |
| 6.3.2 256-bit key support | 11 |
| 6.3.3 Operator customization..... | 11 |
| 6.3.4 Implementation and operational considerations..... | 12 |
| 7 Overview of the Tuak design | 12 |
| 8 Design rationale..... | 13 |
| 8.0 Introduction | 13 |
| 8.1 Brand new design, or design based on an existing public algorithm? | 13 |
| 8.2 Block cipher, stream cipher, MAC or hash function? | 13 |
| 8.3 Which hash function? | 13 |
| 8.4 What sort of Keccak function to use | 14 |
| 8.5 Keccak parameter selection..... | 14 |
| 8.6 Security evaluation of Keccak..... | 15 |
| 8.6.0 Introduction..... | 15 |
| 8.6.1 What about the internet stories about NIST weakening SHA-3?..... | 15 |
| 8.7 A note on IPR..... | 16 |
| 8.7.1 Keccak IPR | 16 |
| 8.7.2 Tuak IPR..... | 16 |
| 8.8 Padding bits | 16 |
| 8.9 Flexible input and output sizes | 16 |
| 8.10 Operator customization | 16 |
| 9 Independent security and performance evaluation | 17 |
| 9.0 Introduction | 17 |
| 9.1 Independent security evaluation | 17 |
| 9.2 Independent SIM card performance evaluation..... | 17 |

10 More notes on implementation and side channel attacks18

10.1 Protecting implementations against side channel attacks18

10.2 Software implementation and the NIST SHA-3 standard18

11 Conclusions18

Annex A: Change history19

History20

Foreword

This Technical Report 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 (together with three accompanying documents, [8], [9] and [10] describes the design rationale, and presents evaluation results, on the Tuak algorithm set [5] – a second example set of algorithms which may be used as the authentication and key generation functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$, e.g. as an alternative to MILENAGE.

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] 3GPP TS 33.102: "3G Security; Security Architecture", (available at <http://www.3gpp.org/ftp/specs/html-info/33102.htm>).
- [3] 3G TS 33.105 (V 3.4.0) (2000-07): "3G Security; Cryptographic Algorithm Requirements (Release 1999)".
- [4] 3GPP TS 35.206: "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", (available at <http://www.3gpp.org/ftp/Specs/html-info/35206.htm>).
- [5] 3GPP TS 35.231: "3G Security; Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$; Document 1: Algorithm specification", (available at <http://www.3gpp.org/ftp/Specs/html-info/35231.htm>).
- [6] 3GPP TS 35.232: "3G Security; Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$; Document 2: Implementers' Test Data", (available at <http://www.3gpp.org/ftp/Specs/html-info/35232.htm>).
- [7] 3GPP TS 35.233: "3G Security; Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions $f1, f1^*, f2, f3, f4, f5$ and $f5^*$; Document 3: Design Conformance Test Data", (available at <http://www.3gpp.org/ftp/Specs/html-info/35233.htm>).
- [8] "Security Assessment of Tuak Algorithm Set", Guang Gong, Kalikinkar Mandal, Yin Tan and Teng Wu, included as an accompanying document to the present report (available at http://www.3gpp.org/ftp/Specs/archive/35_series/35.935/SAGE_report/Secassesment.zip).
- [9] "Performance Evaluation of the Tuak algorithm in support of the ETSI SAGE standardisation group", Keith Mayes, included as an accompanying document to the present report (available at http://www.3gpp.org/ftp/Specs/archive/35_series/35.936/SAGE_report/Perfevaluation.zip).
- [10] "Performance Evaluation of the Tuak algorithm in support of the ETSI SAGE standardisation group – extension report", Keith Mayes, included as an accompanying document to the present report (available at http://www.3gpp.org/ftp/Specs/archive/35_series/35.936/SAGE_report/Perfevaluationext.zip).