



**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 5: Performance evaluation  
(3GPP TR 35.935 version 16.0.0 Release 16)**



---

**Reference**

RTR/TSGS-0335935vg00

---

**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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

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.

© ETSI 2020.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

**3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

**GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

## 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 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. 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 "**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
Legal Notice .....	2
Modal verbs terminology.....	2
Foreword.....	4
1 Scope .....	5
2 References .....	5
3 Definitions, symbols and abbreviations .....	5
3.1 Definitions .....	5
4 Performance evaluation of the Tuak algorithm set.....	5
<b>Annex A: Change history .....</b>	<b>6</b>
History .....	7

---

# Foreword

This Technical Report has been produced by the 3<sup>rd</sup> 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 provides a reference to an independent performance evaluation report of the Tuak algorithm set carried out by the ISG Smart Card Centre of the Royal Holloway University of London.

---

# 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 TS 35.231: "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".
- [2] "Performance Evaluation of the TUAK algorithm in support of the ETSI Sage standardisation group"; Keith Mayes; ISG Smart Card Centre, Royal Holloway University of London; (available at [http://www.3gpp.org/ftp/Specs/archive/35\\_series/35.936/SAGE\\_report/Perfevaluation.zip](http://www.3gpp.org/ftp/Specs/archive/35_series/35.936/SAGE_report/Perfevaluation.zip))
- [3] "Performance Evaluation of the TUAK algorithm in support of the GSMA and ETSI SAGE standardisation group"; Keith Mayes; ISG Smart Card Centre, Royal Holloway University of London; Crisp Telecom Limited; (available at [http://www.3gpp.org/ftp/Specs/archive/35\\_series/35.936/SAGE\\_report/Perfevaluationext.zip](http://www.3gpp.org/ftp/Specs/archive/35_series/35.936/SAGE_report/Perfevaluationext.zip))

---

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 35.231 apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TS 35.231 [1].

---

# 4 Performance evaluation of the Tuak algorithm set

The performance evaluation report of the Tuak algorithm set [1] can be found here: [2].

An extension to the performance evaluation report can be found here: [3].

## Annex A: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
Nov 2014					First TR version		0.1.0
Dec 2014	SA#66	SP-140817			Version for information and approval	0.1.0	1.0.0
					Version after approval	1.0.0	12.0.0
Jan 2016	SA#70				Upgrade to Rel-13 (MCC)	12.0.0	13.0.0

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-03	SA#75					Promotion to Release 14 without technical change	14.0.0
2018-06	-	-	-	-	-	Update to Rel-15 version (MCC)	<b>15.0.0</b>
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	<b>16.0.0</b>

---

# History

<b>Document history</b>		
V16.0.0	August 2020	Publication