3GPP TR 35.936 V16.0.0(2020-07)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

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 6: Security assessment

(Release 16)

 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

GSM. UMTS, LTE, 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

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [5](#__RefHeading___Toc422407844)

1 Scope [6](#__RefHeading___Toc422407845)

2 References [6](#__RefHeading___Toc422407846)

3 Definitions, symbols and abbreviations [6](#__RefHeading___Toc422407847)

3.1 Definitions [6](#__RefHeading___Toc422407848)

4 Security assessment of the Tuak algorithm set [6](#__RefHeading___Toc422407849)

Annex A: Change history [7](#__RefHeading___Toc422407850)

# 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 provides a reference to an independent security assessment of the Tuak algorithm set carried out by the University of Waterloo, Canada.

# 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] "Security Assessment of TUAK Algorithm Set"; Guang Gong, Kalikinkar Mandal, Yin Tan, TengWu; Department of Electrical and Computer Engineering University of Waterloo, Canada (available at <http://www.3gpp.org/ftp/Specs/archive/35_series/35.935/SAGE_report/Secassesment.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 Security assessment of the Tuak algorithm set

The security assessment of the Tuak algorithm set [1] can be found here: [2].

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-140818 |  |  | Version for information and approval | 0.1.0 | 1.0.0 |
|  |  |  |  | Version after approval | 1.0.0 | 12.0.0 |
| Jun 2015 | SA#68 | SP-150302 | 001 | - | Correction of clause title and text referring to wrong subject | 12.0.0 | 12.1.0 |
| Jan 2016 | SA#70 |  |  |  | Upgrade to Rel-13 (MCC) | 12.1.0 | 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) | **15.0.0** |
| 2020-07 | - | - | - | - | - | Update to Rel-16 version (MCC) | **16.0.0** |