ETSI TR 135 934 V17.0.0 (2022-04)

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 f1, f1*, f2, f3, f4, f5 and f5*;
Document 4: Report on the design and evaluation
(3GPP TR 35.934 version 17.0.0 Release 17)

Reference
RTR/TSGS-0335934vh00

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

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.

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

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).

[11] "Note on side-channel attacks and their countermeasures", G. Bertoni, J. Daemen, M. Peeters, G. van Assche (available at http://keccak.noekeon.org/NoteSideChannelAttacks.pdf).

[12] "Building power analysis resistant implementations of Keccak", G. Bertoni, J. Daemen, M. Peeters, G. van Assche (available at http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/BERTONI_KeccakAntiDPA.pdf).

[13] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org.

[14] "Announcing Draft Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Draft Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard, and Request for Comments", NIST, 28th May 2014, available at https://www.federalregister.gov/articles/2014/05/28/2014-12336/announcing-draft-federal-information-processing-standard-fips-202-sha-3-standard-permutation-based.

[15] "Early Symmetric Crypto (ESC) seminar 2013" (available at https://www.cryptolux.org/mediawiki-esc2013/index.php/ESC_2013)

[16] "The KECCAK sponge function family" (available at http://www.noekeon.org)

[17] https://www.cdt.org/blogs/joseph-lorenzo-hall/2409-nist-sha-3

[18] http://yro.slashdot.org/story/13/09/28/0219235/did-nist-cripple-sha-3

[19] https://www.schneier.com/blog/archives/2013/10/will_keccak_sha-3.html

[20] http://keccak.noekeon.org/yes_this_is_keccak.html

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Keccak: algorithm selected as the winner of the SHA-3 competition

MILENAGE: previously designed example algorithm set for the 3GPP Authentication and Key Generation Functions

TOPC: value derived from TOP and K and used within the computations of the functions *f1, f1*, f2, f3, f4, f5* and *f5**

Tuak: newly designed example algorithm set for the 3GPP Authentication and Key Generation Functions. It should be pronounced like "too-ack"

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AES	Advanced Encryption Standard block cipher
AK	Anonymity Key
AMF	Algorithm Management Field
AuC	Authentication Centre
CK	Cipher Key
CPU	Central Processing Unit
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
IC	Integrated Circuit

IK	Integrity Key
K	Long lived subscriber unique key
MAC	Message Authentication Code
MAC-A	MAC for normal authentication vectors
MAC-S	MAC for resynchronization vectors
MULTOS	Multi-application smart card operating system
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVM	Non-Volatile Memory
RAM	Random Access Memory
RAND	Random input parameter to authentication and key generation functions
RES	Response value
RNC	Radio Network Controller
ROM	Read-Only Memory
SAGE	Security Algorithms Group of Experts

NOTE: This is an ETSI Technical Committee.

SHA-2	Secure Hash Algorithm already standardized by NIST
SHA-3	Secure Hash Algorithm soon to be standardized by NIST
TOP	Tuak Operator Variant Algorithm Configuration Field
SEMA	Simple Electromagnetic Analysis
SIM	Subscriber Identity Module
SPA	Simple Power Analysis
SQN	Sequence Number
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
XMAC	Expected MAC value

4 Structure of this report

The main content of the present document is organized as follows:

- Clause 5 and 6 give the requirements and background that were considered during the design of Tuak – first recalling the functional and performance requirements that were used for MILENAGE, then noting some differences and additional points that apply for Tuak.
- Clause 7 gives a brief overview of the Tuak design.
- Clause 8 runs through choices made during the design of Tuak, and the reasons behind those choices.
- Clause 9 introduces independent assessments that have been carried out on the security and performance of Tuak. The full independent assessment reports are included as companion documents to this one.
- Clause 10 gives some further observations on software implementation and protection against side channel attacks.
- Clause 11 concludes with an overall assessment of Tuak's fitness for purpose.

Three further documents [8], [9] and [10] complete the present document, as explained in clause 9.

5 Background to the design and evaluation work

The 3rd Generation Partnership Project (3GPP) is a global initiative dedicated to the development of specifications for the next generations of cellular mobile systems. Integration of strong security services is an important feature of this system and the general security architecture is defined in ref. [2]. The implementation of these security services should be based on a variety of cryptographic functions/algorithms.

Out of the full algorithm suite, only the UMTS encryption algorithms (***f8***) and the UMTS integrity algorithms (***f9***) are fully standardized. ***f0*** represents a random number generation algorithm, and has no standardization or interoperability

requirements at all. The remaining cryptographic functions for authentication and key agreement (***f1*** – ***f5****) are allocated to the Authentication Centre (AuC) and the USIM; this means that the functions are proprietary to the home environment, and there is no need for formal standardization of these algorithms. However, there are good reasons to have a well trusted example set of functions available for this purpose, for use by operators that choose not to develop their own solutions. The MILENAGE algorithm set [4] was created to meet this need.

There are also good reasons to have a second trusted example set of (***f1*** – ***f5****) algorithms available:

- To have a fallback already in place in case MILENAGE is ever compromised.
- In particular, for the embedded UICC, where it may be sensible to have two strong algorithms installed on the platform and available for selection by subsequently loaded USIM applications. This provides choice to operators; it also provides resilience against future cryptanalysis of either algorithm, in devices that may have a long lifetime in the field.

The Tuak algorithm set [5], [6] and [7] has been created to serve as this second trusted example algorithm set.

6 Summary of algorithm requirements

6.0 Introduction

When MILENAGE was created, the requirements specification was taken from [3]. Clauses 6.1 and 6.2 below reproduce the main requirements necessary to understand the present document. Clause 6.3 describes some new requirements that came into play when designing Tuak.

6.1 General requirements for 3GPP cryptographic functions and algorithms (as stated for MILENAGE)

The functions should be designed with a view to their continued use for a period of at least 20 years. Successful attacks with a workload significantly less than exhaustive key search through the effective key space should be impossible.

The designers of above functions should design algorithms to a strength that reflects the above qualitative requirements.

Legal restrictions on the use or export of equipment containing cryptographic functions may prevent the use of such equipment in certain countries.

It is the intention that UE and USIMs that embody such algorithms should be free from restrictions on export or use, in order to allow the free circulation of 3G terminals. Network equipment, including RNC and AuC, may be expected to come under more stringent restrictions. It is the intention that RNC and AuC that embody such algorithms should be exportable under the conditions of the Wassenaar Arrangement, see reference [13].

6.2 Authentication and key agreement functions (as stated for MILENAGE)

6.2.0 Introduction

The mechanisms for authentication and key agreement described in clause 6.3 of [2] require the following cryptographic functions:

f1 The network authentication function;

f1* The re-synchronization message authentication function;

f2 The user authentication function;

f3 The cipher key derivation function;

f4 The integrity key derivation function;

f5 The anonymity key derivation function;

f5* The anonymity key derivation function for re-synchronization.

6.2.1 Implementation and operational considerations

The functions ***f1*–*f5**** should be designed so that they can be implemented on an IC card equipped with an 8-bit microprocessor running at 3,25 MHz with 8 kbyte ROM and 300 byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500 ms execution time.

6.2.2 Type of algorithm

6.2.2.1 *f1*

f1: the network authentication function

f1: (K; SQN, RAND, AMF) → MAC-A (or XMAC-A)

f1 should be a MAC function. In particular, it should be computationally infeasible to derive K from knowledge of RAND, SQN, AMF and MAC-A (or XMAC-A).

6.2.2.2 *f1**

f1*: the re-synchronization message authentication function

f1*: (K; SQN, RAND, AMF) → MAC-S (or XMAC-S)

f1* should be a MAC function. In particular, it should be computationally infeasible to derive K from knowledge of RAND, SQN, AMF and MAC-S (or XMAC-S).

6.2.2.3 *f2*

f2: the user authentication function

f2: (K; RAND) → RES (or XRES)

f2 should be a MAC function. In particular, it should be computationally infeasible to derive K from knowledge of RAND and RES (or XRES).

6.2.2.4 *f3*

f3: the cipher key derivation function

f3: (K; RAND) → CK

f3 should be a key derivation function. In particular, it should be computationally infeasible to derive K from knowledge of RAND and CK.

6.2.2.5 *f4*

f4: the integrity key derivation function

f4: (K; RAND) → IK