ETSI TS 155 236 V14.0.0 (2017-04)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Specification of A8_V MILENAGE Algorithm:
An example algorithm for the key generation function A8_V
(3GPP TS 55.236 version 14.0.0 Release 14)**

3GPP A GLOBAL INITIATIVE
GSM® GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
RTS/TSGS-0355236ve00

Keywords
GSM,SECURITY

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

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 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**", "**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 4
1 Scope 5
2 References 5
3 Definitions, symbols and abbreviations 5
3.1 Definitions 5
3.2 Symbols 5
3.3 Abbreviations 6
4 Introductory information 6
4.1 Introduction 6
4.2 Notation 6
4.2.1 Bit/byte ordering 6
4.2.2 List of symbols 6
4.3 List of variables 6
4.4 Algorithm inputs and outputs 6
5 The A8_V MILENAGE algorithm 7
6 Test data for A8_V MILENAGE 7
6.1 Introduction 7
6.2 Format 7
6.3 Test Sets 8
Annex A (informative): Change history 12
History 13

Foreword

This Technical Specification 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 contains an example algorithm which may be used as the VSTK key generation function A8_V as described in TS 43.020 [4]. (It is not mandatory that the particular algorithm specified in this document is used - the A8_V function is operator-specifiable rather than being fully standardised.)

Clause 4 introduces the algorithm and describes the input and output parameters. Clause 5 defines the algorithm. Clause 6 provides test data.

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 35.206: "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".

[2] 3GPP TS 35.207: "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".

[3] 3GPP TS 35.208: "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".

[4] 3GPP TS 43.020: " Security related network functions".

[5] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [5], TS 35.206 [1] and TS 43.020 [4], 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 [5], TS 35.206 [1] or TS 43.020 [4].

3.2 Symbols

=	The assignment operator.
||	The concatenation of the two operands.
X[i]	The i^{th} bit of the variable **X**. (**X = X[0] || X[1] || X[2] || …..**).