ETSI TS 135 205 V9.0.0 (2010-02)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
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 1: General
(3GPP TS 35.205 version 9.0.0 Release 9)

Reference

RTS/TSGS-0335205v900

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 (http://webapp.etsi.org/IPR/home.asp).

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.

Contents

Foreword

This Technical Specification (TS) 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.

Introduction

This document has been prepared by the 3GPP Task Force, and contains an example set of algorithms which may be used as the authentication and key generation functions ***f1***, ***f1****, ***f2***, ***f3***, ***f4***, ***f5*** and ***f5****. (It is not mandatory that the particular algorithms specified in this document are used — all seven functions are operator-specifiable rather than being fully standardised). This document is one five, which between them form the entire specification of the example algorithms, entitled:

- 3GPP TS 35.205: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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 1: General".

- 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

- 3GPP TS 35.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

- 3GPP TS 35.208: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

- 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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 5: Summary and results of design and evaluation".

1 Scope

This report is a description of the work undertaken by an ETSI SAGE Task Force on the design of the Milenage Algorithm Set: an example set of 3GPP Authentication and Key Generation Functions.

The 3GPP Authentication and Key Generation Functions are not standardized. An example set of these algorithms has been produced on request from 3GPP with the intent that it shall be offered to the UMTS operators, to utilise instead of developing their own. An ETSI SAGE Task Force has carried out this work.

The requirement specification from 3GPP SA3 stated that operator personalisation of the example set must be possible and that the basic kernel must be possible to replace.

The example set is based on the block cipher Rijndael, which at the time was one of the AES candidates and the specification describes how the 7 algorithms used in 3GPP authentication and key generation are scheduled around this basic kernel. The specification and associated test data for the example algorithm set is documented in three documents:

- A formal specification of both the modes and the example kernel [3]
- A detailed test data document, covering modes and the example kernel [4]
- A "black box" test data document [5]

A detailed summary of the evaluation is provided in a public evaluation report [6].

This report gives an overview of the overall work by the task force.

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 33.102 v3.5.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 33.105 v3.4.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements".

[3] 3GPP TS 35.206: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

[4] 3GPP TS 35.207: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

[5] 3GPP TS 35.208: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 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".

[6] ETSI SAGE 3GPP AF TF: "Report on the design and evaluation of 3GPP Authentication and Key Generation Functions".

[7] 3GPP TSG SA WG3 liaison statement to SAGE (S3-000089): "Authentication algorithm for 3GPP".

3 Abbreviations

For the purposes of the present report, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AMF	Authentication Management Field
AK	Anonymity key
AuC	Authentication Centre
AUTS	Re-synchronisation Token
CK	Cipher Key
DPA	Differential Power Analysis
$E(X)_K$	Encryption of X under key K
IK	Integrity Key
K	Subscriber key
MAC	Message Authentication Code
MAC-A	Network Authentication Code
MAC-S	Resynchronisation Authentication Code
OP	a 128-bit Operator Variant Algorithm Configuration Field that is a component of the functions ***f1, f1*, f2, f3, f4, f5 and f5****
OP_C	a 128-bit value derived from OP and K and used within the computations of the functions ***f1, f1*, f2, f3, f4, f5 and f5****
OFB	Output Feedback
RAND	Random Challenge
RES	Response to Challenge
RNC	Radio Network Controller
SAGE	Security Algorithms Group of Experts
SAGE 3GPP AF TF	SAGE Task Force for the design of the 3GPP Authentication and Key Agreement Functions
SQN	Sequence Number
SPA	Simple Power Analysis
TA	Timing Attack
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module

4 Structure of this report

The material presented in this report is organised in the subsequent clauses, as follows:

- clause 5 provides background information on the Authentication and Key Generation algorithms;
- clause 6 provides an outline of the work plan adopted by the SAGE Task Force to design and evaluate the example algorithm set and to produce the associated test data for release to 3GPP;
- clause 7 consists of a summary of the main points in the algorithm requirements specification produced by 3GPP TSG SA ;
- clause 8 describes how the SAGE Task Force designed the algorithm and produced the specification and associated test data;
- clause 9 gives an overview of the evaluation work carried out by the SAGE Task Force and the conclusions of the evaluations;
- clause 10 gives statements on the task force procedure for approval and release of the specification and the considerations for publication and export control.

5 Background to the 3GPP Authentication and Key Generation algorithms

Within the mobile communication system UMTS specified by 3GPP there is a need to provide security features. These security features are realised with the use of cryptographic functions and algorithms. In total 3GPP identified the need for 9 cryptographic algorithms and functions (ref. [1]). Two of these, f8 and f9, for cipher and integrity protection of the 3GPP radio interface have already been developed and are now part of the 3GPP standard specifications.

It was decided that the algorithms for authentication and key generation should not be standardised as they can well be proprietary to each operator and by his own choice (just like in GSM). The context for these algorithms, called f1, f1*, f2, f3, f4, f5, f5*, are described in ref. [1]. The generic requirements for these algorithms are specified in ref. [2].

It was discussed in 3GPP SA 3 if an example set of these algorithms should be produced and offered to the UMTS operators, to utilise instead of developing their own. A need for such an example set was identified with the additional requirement that operators should have a means to personalise their own algorithms. ETSI SAGE was asked to design the algorithms. To carry out this work SAGE set up a Task Force (SAGE 3GPP AF TF) based on SAGE and enlarged with cryptographers form UMTS manufacturers.

6 SAGE 3GPP AF TF work plan

The workplan for 3GPP authentication example algorithms was approved by 3GPP in July 2000. The SAGE 3GPP AF TF formally started work in August 2000 as an ETSI Task Force. This SAGE 3GPP AF TF consisted of the regular SAGE members, and three 3GPP manufacturers (Gemplus, Mitsubishi and Nokia).

The work was funded by 3GPP. The total resource budget for the SAGE 3GPP AF TF work was 16.75 man months.

The work was divided into five main tasks:

- Project Management;
- Design (approximately 14% of the budget)
- Evaluation (the major task, approximately 60% of the budget)
- Specification testing (approximately 20% of the budget)
- Liaison and publication activities

The design of the algorithm example set and a complete set of specification documents should be finalised in November 2000.

The work should be reported in 5 deliverables according to the requirements from 3GPP TSG SA.

- a short public report on the design and evaluation work (***this document)***.
- formal specification of both the modes and the example kernel [3]
- two test data reports, covering modes and the example kernel (detailed test results in [4]; black box test data in [5]
- a summary of the evaluation results in a public report [6]

The results of the evaluations was to be approved and agreed by the whole group before the final algorithms specifications were released to 3GPP.

7 Outline of algorithm requirements specification

The requirements for the authentication and key generation functions were specified by 3GPP TSG SA in: 3rd Generation Partnership Project: technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements (3G TS 33.105 version 3.4.0) [2]

7.1 The authentication and key generation functions

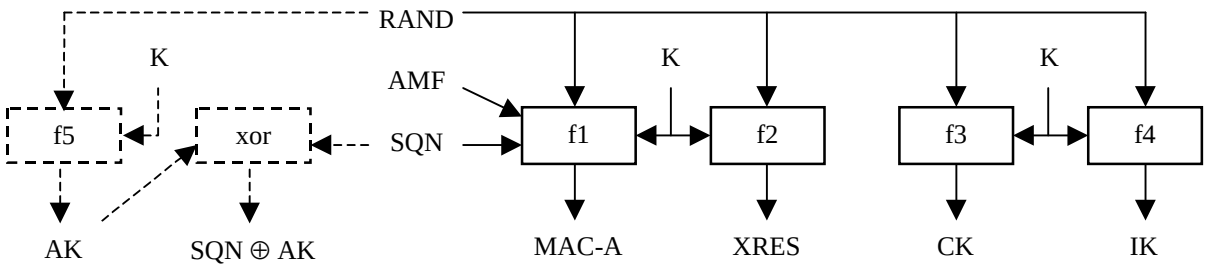
The mechanism for authentication and key agreement described in [1] requires the following cryptographic functions:

f0	the random challenge generating function;
f1	the network authentication function;
f1*	the re-synchronisation 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 the re-synchronisation message.

Regarding f0, the random generation function, it was agreed with 3GPP SA3 that an example for this function should not be proposed by the Task Force.

For each of the algorithms f1 to f5* there is a general requirement that it shall be computationally infeasible to derive K from knowledge of input(s) and output.

7.2 Use of the algorithms on the AuC side



AUTN = SQN [⊕ AK] || AMF || MAC-A
Quintet = (RAND, XRES, CK, IK, AUTN)

This figure describes the generation of the authentication and key generation values in the HLR/AuC