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

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

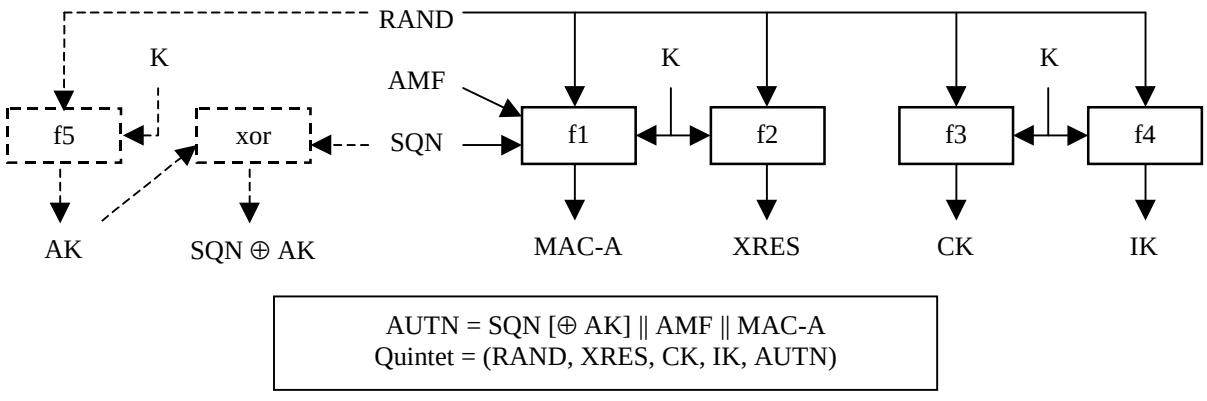
The mechanism for authentication and key agreement described in [1] requires the following cryptographic functions:

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.

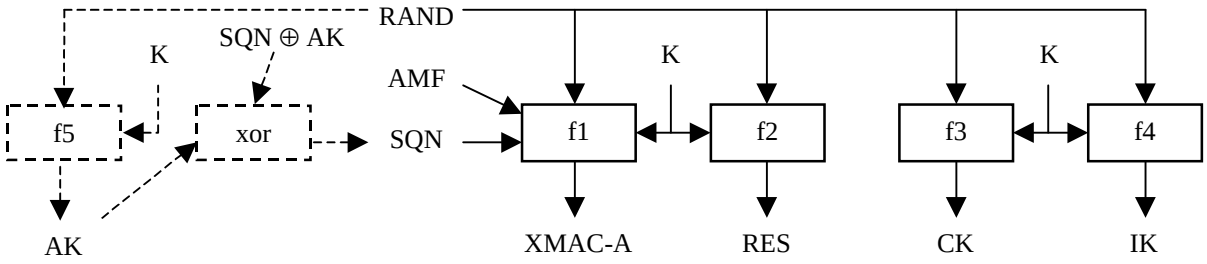
For each of the algorithms f1 to f5* there is a general requirement that it shall be computationally infeasible to derive K from knowledge of input(s) and output.

7.2 Use of the algorithms on the AuC side



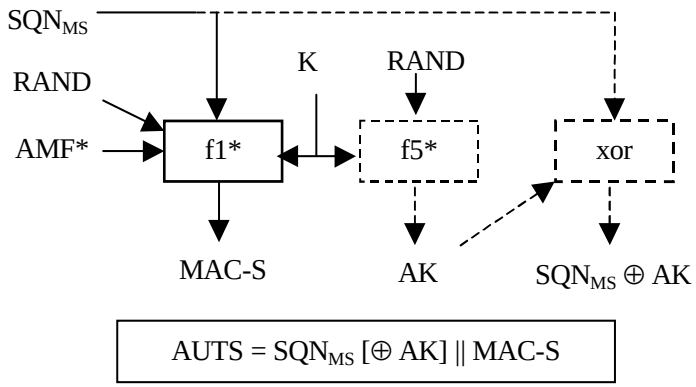
This figure describes the generation of the authentication and key generation values in the HLR/AuC

7.3 Use of the algorithms in the USIM



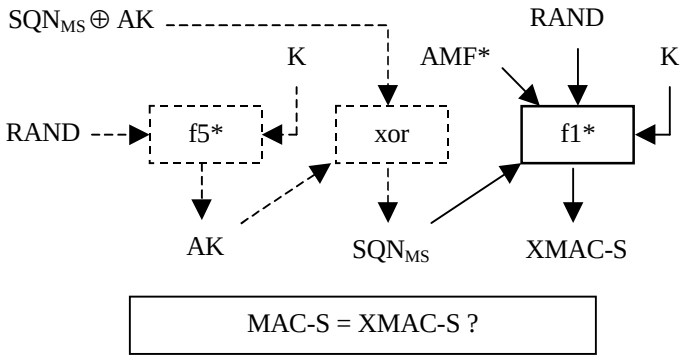
This figure describes the generation of the authentication and key generation values in the USIM

7.4 Use of the algorithms for resynchronisation in the USIM



This figure describes the generation of the re-synchronisation token, AUTS, in the USIM.

7.5 Use of the algorithms for resynchronisation in the HLR/AuC



This figure describes the control of the re-synchronisation token in the USIM

7.6 Implementation aspects

All the functions f1 to f5* shall be designed so that they can be implemented on an IC card equipped with a 8-bit microprocessor running at 3.25 MHz with 8 kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500 ms execution time.

7.7 Generic requirements for 3GPP cryptographic functions and algorithms

In section 4 of [2] generic requirements are given for all 3GPP cryptographic functions and algorithms. These are summarized below (in Italics).

Resilience

The functions should be designed with a view to its 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.

World-wide availability and use

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 which 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 which embody such algorithms should be exportable under the conditions of the Wassenaar Arrangement

7.8 Subsequent requirements on the authentication and key generation functions

In a liaison statement to SAGE the 3GPP Security Group TSG SA WG3 presented some further requirements on the authentication functions [7]:

"The basic principles of the algorithm design, as agreed by S3, are listed below:

- It is required that the algorithm fulfil the requirements specified in 3G TS 33.105.
- It is required that controlled personalisation of the algorithm is possible based on an operator variant algorithm configuration field of at least 128 bits.
- It is desirable that the algorithm is designed around a replaceable kernel function to provide an additional degree of variety.
- If an algorithm is to be designed around a kernel function, then it is required that one specific kernel function be provided.
- If an algorithm is to be designed around a kernel function, then it is desirable that a list of suitable alternative kernel functions be provided.
- If an algorithm is to be designed around a kernel function, then it is desirable that standard / publicly available algorithms may be used to implement the kernel function. However, the type or types of kernel function that could be supported is left to SAGE.

It is required that the algorithm lends itself to implementations which are resistant to Simple Power Analysis, Differential Power Analysis and other 'side-channel' attacks as appropriate when implemented on a USIM. It is acknowledged that SAGE may need to consult with smart card experts in order to be able to address this requirement."

8 Algorithms design

Based on the requirements and fixed starting points SAGE 3GPP AF TF established the following essential design criteria.

8.1 Design criteria

1. Without knowledge of secret keys, the functions ***f1, f1*, f2, f3, f4, f5 and f5**** should be practically indistinguishable from independent random functions of their inputs (RAND||SQN||AMF) and RAND.

2. It should be practically impossible to determine any part of the secret key K, or the operator variant algorithm configuration field, OP, by manipulation of the inputs and examination of the outputs to the algorithm.

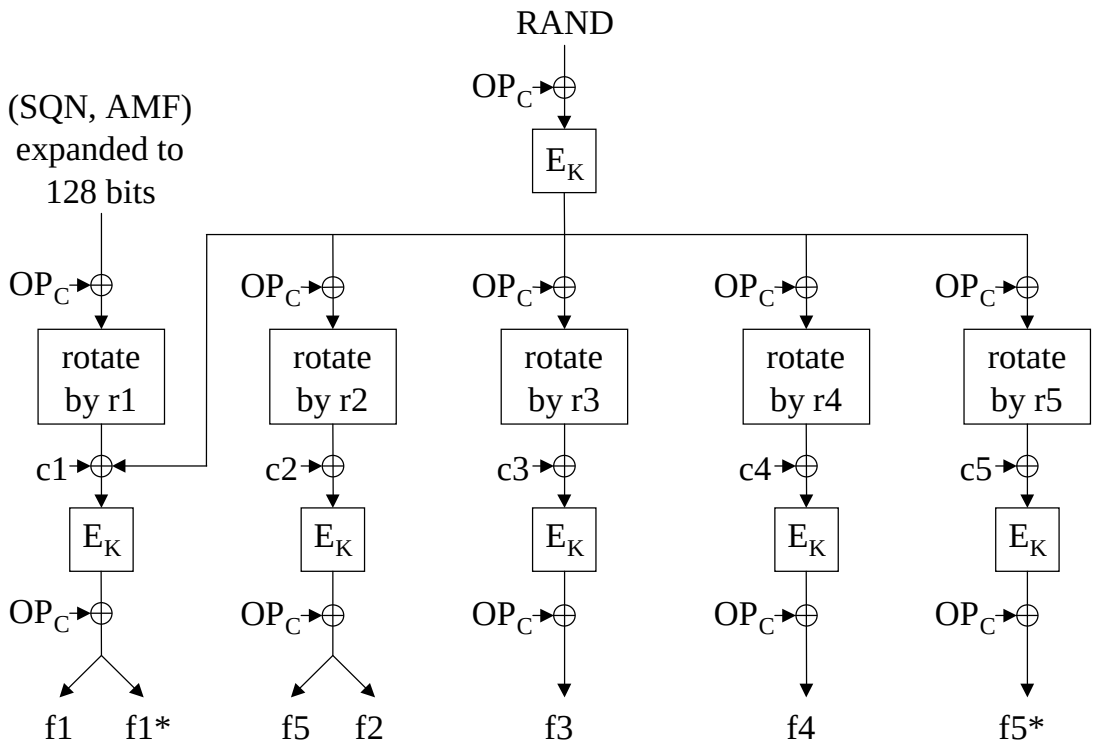
3. Events tending to violate criteria 1 and 2 should be regarded as insignificant if they occur with probability approximately 2^{-128} (or require approximately 2^{128} operations) or less.

4. Events tending to violate criteria 1 and 2 should be examined if they occur with probability approximately 2^{-64} (or require approximately 2^{64} operations) to ensure that they do not have serious consequences. Serious consequences would include recovery of a secret key or ability to emulate the algorithm on a large number of future inputs.

5. The design should build upon well-known structures and avoid unnecessary complexity. This will simplify analysis and avoid the need for a formal external evaluation.

8.2 Chosen design for the framework

The detailed specifications of the 3GPP algorithms are found in ref. [3]. The following diagram shows the framework for the functions ***f1, f1*, f2, f3, f4, f5*** and ***f5**** using the kernel function denoted E_K.



Definition of f1, f1*, f2, f3, f4, f5 and f5*

The value OP_C is derived from the subscriber key K and the operator dependent value OP by

$$OP_C = OP \oplus E(OP)_K$$

It is assumed and recommended in [3] that OPc is calculated outside the USIM cards and then stored in each card as an individual value. This will allow OP to be better protected than if OP had been stored in every card.

r1, …, r5 are five fixed rotation constants and c1, .., c5 are five fixed addition constants defined in [2].

8.3 Analysis of the role of OP and OPc

The 128-bit value OP is the Operator Variant Algorithm Configuration Field, which the Task Force was asked to include to provide separation between the functionality of the algorithms when used by different operators.

It is left to each operator to select a value for OP.

The algorithm set is designed to be secure whether or not OP is publicly known; however, operators may see some advantage in keeping their value of OP secret as a secret OP is one more hurdle in the attacker's path.

It should be difficult for someone who has discovered even a large number of (OPc, K) pairs to deduce OP. That means that the OPc associated with any other value of K will be unknown, which may make it (slightly) harder to mount some kinds of cryptanalytic and forgery attacks.

It is more likely that OP can be kept secret if OP is not stored on the USIM, as it then only takes one USIM to be reverse engineered for OP to be discovered and published. Hence the task force recommends that OPc is calculated off USIM.

8.4 Choice of kernel

Because of the short time scales it was decided to base the algorithm example set on an existing algorithm which had undergone sufficient analysis to serve as a kernel for the algorithm set so as to obviate the need for extensive cryptographic analyses and testing. A 128 bit input/output block cipher with a 128 bit key was chosen as kernel as this was considered to be a type of kernel which could easily be substituted if any operator wanted to use the framework with another algorithm.

Document [3] describes the use of the Rijndael algorithm in encryption mode for the kernel function E_K, but this choice could be replaced by any suitable 128-bit keyed function employing a 128 bit key. Rijndael was chosen as being then one of the five remaining AES candidates, was well studied, could be efficiently implemented in S/W or H/W and was available IPR-free.

Ref [6] gives general requirements on the kernel which should be considered in case of replacement.

8.5 Design methodology

The algorithms were designed using a phased iterative and interactive approach. The design process is summarised below.

- **Phase 1:** The starting points for the algorithms and design criteria were agreed. The design team then produced a first design proposal for a framework algorithm set including different options for the inclusion of OP. A block cipher was proposed as kernel with Rijndael as prime candidate

- **Phase 2:** The results of first evaluations were discussed. Choice of block cipher as kernel versus keyed hash was evaluated. Use of OP as protection against DPA was discussed. The counter mode was adopted instead of OFB. Based on these results, the design team revised the design to a second design proposal for the algorithm set. 3GPP SA3 agreed to limit RES to 64 bits in the example and to change input to the synchronization token.

- **Phase 3:** The results of the second evaluation were discussed. The use of Rijndael and the design for the algorithm set was confirmed, except for some small details. Considering the extensive analyses which have been made on Rijndael it was decided that the normal range of statistical testing need not be performed. Evaluation of complexity of implementation started.

- **Phase 4:** Details were fixed after mathematical evaluation of modes. The method for deriving OPc from OP was changed. Resistance against side channel attacks was decided to be left to implementers, with references to methods discussed in connection with Rijndael as candidate to AES. The specification documents were drafted and two parties independently carried out specification testing to check the correctness and completeness of the specification and the accompanying C-code.

- **Phase 5:** After the final review the specifications were confirmed. A summary report of the evaluation undertaken by the task force was produced and agreed [6], as well as this report.

8.6 Specification and test data

The algorithm specification and associated test data are documented in [3], [4] and [5]. An annex in [3] consists of example program listings of the algorithm set in 'C'.

Document [4] provides design conformance test data designed to help verify implementations of the algorithms. The document identifies intermediate points in the algorithms where test data is provided. Then it gives input, internal and output parameters at these points, and provides different sets of test data listings.

Document [5] is informative and provides test data designed to help verify the correct functioning of the algorithms seen as a 'black box'. The document identifies the input and output interfaces and provides a number of test sets for the different modes of operation of the algorithms.

Two parties not directly involved in the design and evaluation teams also evaluated the adequacy of the specification. To this end, these parties made independent simulations of the algorithm from the specification and confirmed these against the test data.

9 Algorithm evaluation

9.1 Evaluation criteria

The algorithm requirements as summarised in section 7 and design criteria as listed in section 8.1 leads to evaluation criteria for the mathematical evaluation and statistical evaluations. Due to the fact that the Rijndael block cipher has undergone an extensive analysis during the AES process, the task force performed no real cryptanalysis of Rijndael, but rather focused on the strength of the constructions for deriving the ***f1*** to ***f5**** modes from a strong 128-bit block cipher.

9.2 Mathematical Evaluation of the modes

The mathematical evaluation concentrated on verifying the strength of the f1-f5 construction, under the assumption that the underlying kernel is a strong block cipher.

The main criteria investigated were:

- The strength of each algorithm, considered individually (resilience of key and subsequent outputs)

- The independence between algorithms (one algorithm's strength is not harmed by knowledge of input/outputs for other algorithms)

For further details on these investigations, see [6].

9.3 Statistical Evaluation

No statistical tests were performed on the kernel, given Rijndael can be trusted to be sufficiently tested and secure through the AES process. Statistical tests on MILENAGE were considered to only yield results about the underlying kernel function. Since it was not the intention of the task force to evaluate Rijndael, statistical tests have not been performed as a consequence.

9.4 Side channel attacks evaluation

In the design process it was concluded not to be feasible to design a general algorithm framework that by itself would not be vulnerable to side channel attacks. Rijndael, as most other block ciphers, is potentially vulnerable to simple and differential power analysis (SPA and DPA) aiming to recover the secret key. It was also concluded that the use of operator constants, OPc, in the USIM cards can only play a limited role in protecting against these kinds of attacks. Hardware protection measures and masking techniques, as referenced in [6], need to be specifically implemented for protection. Also timing attacks (TA) may need implementation specific countermeasures. Rijndael as an AES candidate has been shown to readily lend itself to protection measures against side channel attacks.

9.5 Complexity evaluation

It is estimated that a non-optimized implementation of kernel and modes could be implemented with no more than 2kB ROM, 120B RAM and execute in less than 80ms. (One instance of the Rijndael cipher will execute in less than 10 ms at 3.25 MHz). Even with full protection measures against side channel attacks (SPA/DPA/TA) on Rijndael it is expected that performance will be well under the stated requirements [2].

9.6 Evaluation report

The evaluation report [6] is a summary of all results of the complete design and evaluation process. It provides the main conclusions of the evaluation work carried out by the task force..

10 Release of algorithm specification and test data by SAGE

10.1 SAGE 3GPP AF TF approval for release

Prior to release of the specification of the algorithm set the following approvals were gained.

All members of SAGE 3GPP AF TF stated that they were satisfied that the example algorithm set provides the high level of security for the authentication and key generation functions required by 3GPP.

- All members of SAGE 3GPP AF TF approved release of the algorithm set specifications and the accompanying documents to 3GPP.

10.2 Publication of the algorithm set specification

The SAGE 3GPP AF TF does not see from a security point of view any obstacles that would prevent publication of the algorithm set specifications.

10.3 Export of the algorithm set specification

The SAGE 3GPP AF TF does not see any obstacles that would prevent export of the algorithm set specifications or corresponding implementations in congruence with the requirements as given in [2].

Annex A (informative): Change history

Change history					
TSG SA #	**Version**	**CR**	**Tdoc SA**	**New Version**	**Subject/Comment**
SP-10	SAGE v 1.0	-	SP-010630	3.0.0	Approved as Release 1999
SP-11	3.0.0	-	-	4.0.0	Updated to Release 4
SP-16	4.0.0	-	-	5.0.0	Updated to Release 5
SP-26	5.0.0	-	-	6.0.0	Updated to Release 6
SP-36	6.0.0	-	-	7.0.0	Updated to Release 7
SP-42	7.0.0	-	-	8.0.0	Updated to Release 8
SP-46	8.0.0	-	-	9.0.0	Updated to Release 9

History

Document history		
V9.0.0	February 2010	Publication