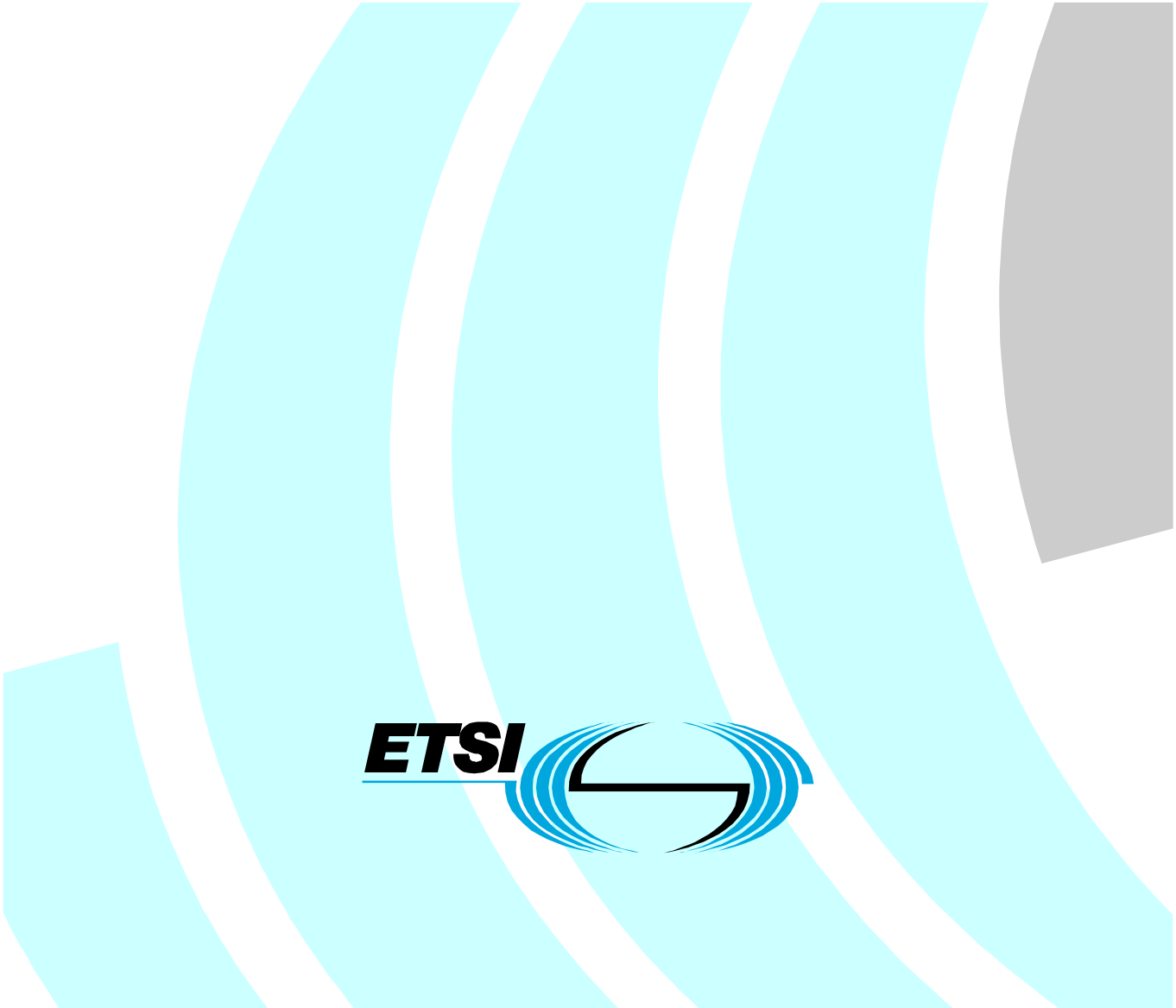
Final draft ETSI EG 202 238 V1.1.1 (2003-08)

ETSI Guide

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms



Reference
DEG/TIPHON-08007

Keywords
algorithm, security, telephony

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

Contents

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 ETSI Guide (EG) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON), and is now submitted for the ETSI standards Membership Approval Procedure.

1 Scope

The present document describes the process options for acquisition of cryptographic algorithms that are subject to standardization within ETSI Technical Bodies.

The document describes:

- design strategies;
- evaluation strategies; and
- algorithm distribution strategies.

In addition some consideration to liability and responsibility resulting from each strategy is given.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ITU-T Recommendation H.221: "Frame structure for a 64 to 1920 kbit/s channel in audiovisual teleservices".

[2] ITU-T Recommendation H.233: "Confidentiality system for audiovisual services".

[3] ITU-T Recommendation H.261: "Video codec for audiovisual services at p x 64 kbit/s".

3 Abbreviations

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

3GPP	Third Generation Partnership Project
AEG	Algorithm Expert Group
AES	Advanced Encryption System
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
BARAS	Baseline Algorithm Recommended for Audio-visual Services
BEANO	Binary Encryption Algorithm for Network Operators
B-ISDN	Broadband-Integrated Service Digital Network
DES	Data Encryption Standard
DSAA	DECT Standard Authentication Algorithm
FIPS	Federal Information Processing Standard
GEA	GPRS Encryption Algorithm
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HDTV	High Definition Television
IC	Integrated Circuit
ISDN	Integrated Service Digital Network

KAT	Known Answer Tests
MAC	Message Authentication Code
MCT	Monte-Carlo Tests
RFP	Request For Proposal
SAGE	Security Algorithm Group of Experts
TAA1	TETRA Authentication and key management Algorithms
TC	Technical Committee
TE	Terminal Equipment
UMTS	Universal Mobile Telecommunications System
UPT	User Personal Telecommunications

4 Introduction

4.1 Background

The selection of cryptographic algorithms and the evaluation of them requires a number of clearly defined steps:

- determination of purpose of the algorithm;
- determination of the outline boundary conditions for the algorithm;
- selection of design method;
- selection of evaluation method;
- selection of distribution method.

The distribution method may of itself form one of the boundary conditions to the algorithm.

4.2 Algorithm purpose

A cryptographic algorithm may be used to provide one or more of the building blocks in a security service:

- confidentiality;
- integrity; and
- authenticity.

The primary purpose shall be stated and the application environment shall be indentified (generally this will be found in the security framework specification to which the cryptographic technique shall be applied).

4.3 Export control

In recognizing that cryptographic devices may have dual-use capability (i.e. may be used for both civil and non-civil applications) the distribution and application of encryption algorithms is limited by export controls and by national or regional policy.

It can be expected that export control rules, and national/regional policy, will vary over time. The impact of this on the development of cryptographic algorithms may restrict some forms of implementation and wherever possible the full scope of application of an algorithm should be stated within the boundary conditions (including the form of device that the algorithm will be supplied to). Similarly the requirements on the strength of cryptographic mechanisms may vary with time as the capabilities of attackers develop (e.g. a 56-bit algorithm is now unlikely to offer the same degree of immunity to attack as it was 10 years ago).

4.3.1 Wassenaar Arrangement

The Wassenaar Arrangement was the first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies which includes those related to cryptology. It received final approval by the 33 co-founding countries in July 1996 and began operations in September 1996.

Cryptographic restrictions apply as limitations of key length in symmetric systems to 56 bits, and in asymmetric systems to 512 bits. However the restrictions do not apply to the use of cryptographic material for civil telecommunications systems that are not capable of end-to-end encryption. These restrictions are subject to renewal on 5th December 2003 by unanimous consent.

For systems designed for civil use the provisions of the Wassenaar Arrangement in the area of application (geographic as well as technical application) should be reviewed. For systems employing encryption for non-civil use due consideration should be taken of the impact of the Wassenaar Arrangement particularly in respect of the available strength of the algorithm if export control restrictions are to be avoided.

4.4 Acquisition methods

Each algorithm that is required can be acquired in one of 3 ways:

- selection from available off the shelf algorithms;
- invitation to submit proposals against a known set of boundary conditions; or
- commission to a dedicated design group.

NOTE: In general for ETSI technical bodies requiring the acquisition of cryptographic material the first port of call should be SAGE.

These methods are applicable both for *secret algorithms*, i.e. algorithms that are intended to be kept secret, and for **open algorithms**, i.e. algorithms that are published. The received wisdom within the security community is that **open algorithms** are to be preferred and examples that show this are to be found in the development of AES as FIPS-197 (see annex B), and in the recent work of ETSI SAGE which has built the 3GPP authentication algorithm suite on Rijndael (AES) (see annex C).

4.5 Liability and Responsibility for algorithms

In the end, someone has to take responsibility for the algorithms. It is useful to be able to predetermine which party for example is liable if an algorithm is broken and financial losses occur.

In case of a commissioned design the responsibilities are more or less clear. In principle the person/organisation which commissions the design is responsible, but some of the responsibility might, e.g. by contract, be transferred to the party which takes on the task to design the algorithm.

In case of an open call for algorithms the responsibility for the algorithm is less clear. It is probably not realistic to make responsibility part of the call (i.e. if you are submitting an algorithm and it will be used then you are liable if it is broken). So the responsibility lies with the party selecting the algorithm. But it is not clear if this selecting party is able to take on any responsibility. This will depend on the process which is applied.

An option in both cases might be to make the algorithm available (distributing, publishing) without taking any responsibility. This is certainly practical in cases where the end use of the algorithm is not fully specified.

5 Open and secret algorithms

The protection offered by an algorithm should always be evaluated under the assumptions that the attacker knows all details of the algorithm and the system it is used within. The only thing the attacker does not know is the key. Of course, keeping the algorithm secret gives an extra layer of protection, however for the purposes of evaluation it is safer in most cases to assume that the algorithm has been made public.

The trust in an algorithm is dependent in part on the trust placed on those who have evaluated it (its evaluators). An open algorithm that has undergone public review should incur more trust of the end users in the design. The competitive situation should also be considered. Where a secret algorithm is concerned, although it may be prudent to assume that the algorithm is more widely known than desired, it is unlikely that there will be any public cryptanlysis of the secret algorithm.

Possible choices.

- open algorithms;
- secret algorithms.

Assumptions:

- competitive situation is better with open algorithms;
- trust is higher in open algorithms;
- it is very difficult to keep secret algorithms secret;
- if a design flaw in a secret algorithm is detected and published, the trust is seriously hurt;
- open algorithms are always open for analysis, which may result in publication of attacks that are only of theoretical interest.

6 Design Strategy

6.1 Selection of an off the shelf algorithm

In order to select an off-the-shelf algorithm the selection shall be based on the suitability of the algorithm for its use and implementation in the system. The experts performing the selection do not necessarily need to be experts in cryptology but are required to be expert in the security and systems aspects for the end application.

Assumptions:

- the expertise needed for evaluating suitability is available;
- the selection process will not be too time-consuming (approximately 2 months);
- there exist candidates (e.g. ETSI secret algorithms, open FIPS standards and AES candidates); and
- there is no difference between selecting secret or open algorithms.

6.2 Invite submissions

Interested parties, within and outside ETSI are invited to submit proposals. The success of the approach relies on the willingness from the interested parties to submit proposals. This approach is mainly used for open algorithms but it would be possible to invite submissions for secret algorithms.

The time from issuing the Request For Proposal (RFP) until the deadline for submissions in a world-wide environment should be at least 6 months. The number of submitted proposals will be dependent on the response time. Thus there is a certain minimum response time to get any proposals at all.

If there are several proposals (but also in case of a single proposal) an evaluation/selection regarding suitability has to be performed.

Assumptions:

- interest to submit proposals is limited but present;
- the time from issuing the RFP till deadline for submissions should be at least 6 months;

- the expertise needed for evaluating suitability is available; and
- the selection process will not be too time-consuming (approximately 2 to 3 months).

NOTE: If the algorithm is open to public scrutiny the selection process will be much longer.

6.3 Commission a special group to design an algorithm

A group of crypto experts are commissioned to develop an algorithm, open or secret.

As the algorithm is a special purpose design according to a specification its suitability should be guaranteed.

The more algorithms to design the more experts are needed.

Assumptions:

- crypto experts for the design are available;
- trust will be high if the algorithm is open and the design principles published;
- a secret algorithm will have a lower trust level;
- the suitability of the algorithm is high; and
- time for design is at least 4 months.

7 Evaluation Strategy

The available methods for evaluation are either to rely on voluntary efforts or to commission a group of experts. The evaluators would be required to review any existing evaluation reports and do their own analysis.

To rely on voluntary efforts and existing available security statements is generally not sufficient. A group of experts should be assigned (commissioned) to perform the evaluation.

If the algorithm is open, the performed analysis methods and results may be published together with the evaluation report. This should give greater trust in the algorithm. If the evaluation is of a secret algorithm or if just the conclusions are published the trust in the algorithm will to a large extent depend on the trust in the experts.

The more algorithms to be evaluated the more experts are needed.

Assumptions:

- the needed expertise is scarce but available on a commissioned basis;
- the time for evaluation is at least 6 months for a new design and 2 months for an off-the-shelf algorithm that has been extensively and completely analysed in open literature. However if the algorithm should also be open to public scrutiny the selection process will be much longer;
- the trust will tend to be higher where evaluation reports are made public and themselves open to evaluation.

8 Distribution Strategy

The algorithm specifications may be distributed in the following ways.

- No distribution: refer only to existing specification including test data;
- Refer to existing specification: distribute test data; and
- Restricted distribution of specification and test data through custodian.

Methods 1 and 2 are only possible for open algorithms and 3 is the only choice for secret algorithms.

9 Relevant aspects in an algorithm acquisition process

9.1 Design methodology

The options for the algorithm design are the following options.

- Select a public of the shelf algorithm.
- Select a confidential of the shelf algorithm.
- Invite submissions for an algorithm.
- Commission a special to design an algorithm.

Option	Public trust in algorithm	Time needed	Availability (of experts/algorithms)	IPR problems or protected	Tailored for use / Suitability	Guarantee of strength
1	+	0	-/0	-/0	0	+
2	-/0 Depends on evaluation	+	-/0	0	0	0 Depends on evaluation
3	+	-	+	0	+	+
4	-/0 Depends on evaluation	+	+	+	+	0 Depends on evaluation
Key: + Good - Bad 0 No impact						

RECOMMENDATION#1: In all cases the first choice design method is to use publicly available algorithms.

RECOMMENDATION#2: In all cases to use public submission against defined boundary conditions.

NOTE: These recommendations combine design options 1 and 3.

9.2 Evaluation methodology

The options for the evaluation of a proposed selected algorithm are the following:

- expert evaluation;
- publication with request to respond;
- review of existing analysis.

Option	Public trust in algorithm	Time needed	Availability (of experts or analysis)	Guarantee of strength
1	0/+ depending on experts	0	0/+	0/+
2	+	-	+	+
3	0/+	+	-/0	0/+
Key: + Good - Bad 0 No impact				

RECOMMENDATION#3: In all cases the first choice evaluation method is to invite expert evalation.

RECOMMENDATION#4: In all cases a nominated authority to filter evalations through should be used.

RECOMMENDATION#5: In the ETSI context SAGE should be the nominated authority.

NOTE: This is a combination of options 1, 2 and 3.

Annex A (informative): Overview of ETSI Standard Algorithms

Here are listed a number of systems developed by ETSI and short descriptions of the algorithms that are used in those standards.

A.1 GSM – the Global System for Mobile communications

GSM was the first public standard digital telecommunication system with a substantial amount of cryptography integrated. The system originally used a standard encryption algorithm called A5 (later this became A5-1) which is used for the encryption of user and signalling data over the radio path. The A5-1 encryption algorithm was not developed by SAGE (SAGE did not exist at the time it was developed) but by a special group: the GSM Algorithm Expert Group (AEG).

Originally A5-1 was used in every GSM system, but when GSM started to expand outside Europe, the use of A5-1 in some cases turned out to be impossible because of controls on the export of the algorithm to certain countries. To overcome these export control problems, an alternative A5-2 encryption algorithm was developed, in this case by ETSI SAGE. However, the algorithm mostly used in GSM is A5-1.

The GSM system also uses an algorithm for authentication and encryption key generation. This algorithm is called A3/A8. It is not a standard algorithm and operators are free to choose or develop their own. For those operators who do not want to do this an example A3/A8 algorithm with the name COMP128, developed by the GSM AEG, used to be available from the GSM Association. In 1998 this algorithm was compromised and from the start of 1999 COMP128 has been replaced by another GSM Association example algorithm.

For the new GSM data service, the General Packet Radio Service (GPRS), a special encryption algorithm had to be developed (GPRS data is encrypted on a different level as regular GSM user and signalling data). This algorithm is called the GPRS Encryption Algorithm (GEA) and was developed by SAGE.

A.2 DECT – Digital Enhanced Cordless Telecommunications

DECT has security features that are similar to those in GSM. It uses an encryption algorithm, the DECT Standard Cipher (DSC), and an authentication and encryption key generation algorithm, the DECT Standard Authentication Algorithm (DSAA).

Both algorithms were developped by ETSI project teams.

A.3 ISDN based audio-visual system

ITU-T has drafted recommendations H.221 [1], H.261 [3] and H.233 [2] in the area of the use of audio-visual systems and the security for these. The ITU-T recommendations were adopted by ETSI as standards.

ITU-T Recommendation H.233 [2] specifies the use of encryption algorithms. In fact it allows different algorithms to be used. ETSI SAGE specified an encryption algorithm especially for this purpose. It is called BARAS (Baseline Algorithm Recommended for Audio-visual Services).

A.4 Multi-application telecommunications cards

Several years ago a sub committee of the ETSI TC Terminal Equipment (TE) group drafted a series of standards for a Multi-application Telecommunications IC (Smart) Card. The specifications included a number of security functions.

To support these security functions, ETSI SAGE designed and specified a cryptographic algorithm called TESA-7. The specification included four modes of use for the algorithm. These are an authentication mode, an integrity mode, a key diversification mode (i.e. calculating an individual key from an identity and a master key) and a secure (encrypted) key loading mode.

The standards for the Multi-application Telecommunication IC Card have not been very successful and the TESA-7 algorithm is therefore hardly used.

A.5 UPT - User Personal Telecommunications

UPT is a telecommunication service standardized by ETSI that enables user to register on a telephone and then be reached there under their own telephone number. This service requires authentication before it can be invoked.

ETSI SAGE designed the standard authentication algorithm, called USA-4, for this service. However, until now, the UPT standard and hence the USA-4 is not used very often.

A.6 Hiperlan - High Performance radio LAN

Hiperlan is a standard for a radio LAN over which data is transmitted at high speeds over the air interface. For this standard SAGE developed an encryption algorithm HSEA (Hiperlan Standard Encryption Algorithm). The export restrictions on the algorithm are minimal (this was an important requirement when the algorithm was designed) and it provides a basic level of security.

ETSI Project BRAN is currently standardizing a successor (called BRAN) for Hiperlan. This will support higher speeds and very probably also employ a standard encryption algorithm.

A.7 Binary Encryption Algorithm for Network Operators (BEANO)

A few years ago ETSI TC Security identified the need for an algorithm that could be used to protect the confidentiality of network management data. ETSI SAGE designed a special encryption algorithm called Binary Encryption Algorithm for Network Operators (BEANO). To overcome the conflicting requirements for a broad exportability and a very high level of security the licence and confidentiality agreement explicitly limits the use of the algorithm to the protection of network management data. The use of the algorithm for other purposes such as the protection of user data is explicitly excluded.

The algorithm is not used at the moment.

A.8 TETRA - Terrestrial Trunked Radio

TETRA is the ETSI standard for a digital private mobile radio communications system. It can be used in public networks and has been selected by many of the major Public Safety organizations in Europe as their future mobile communications system. For the latter user groups security has a high priority and therefore TETRA includes a large number of security features. These are supported by a number of standard cryptographic algorithms. There are four standard TETRA Encryption Algorithms TEA1, TEA2, TEA3 and TEA4. TEA1 is for general use in TETRA systems. The use of TEA2 is restricted to European Public Safety organizations (mainly from the "Schengen" countries), TEA3 is equivalent to TEA1 for markets where export of TEA1 is difficult, and TEA4 is similar to TEA2 for markets outside the European Public Safety organization boundary.

Furthermore SAGE has specified one set of TETRA Authentication and key management Algorithms (TAA1). The TAA1 is designed for use in all TETRA systems.

Annex B (informative): Development of AES using public RFP design strategy

The Advanced Encryption Standard (AES) was developed by means of a competitive Request For Proposals (RFP) in order to provide a replacement for the Data Encryption Standard (DES) algorithm.

General information is publicly available at: http://csrc.nist.gov/encryption/aes/

The specific timetable and selection process is summarized here and to be found in more detail at: http://csrc.nist.gov/encryption/aes/index2.html#overview

B.1 Overview of the AES selection

B.1.1 Purpose of the algorithm

The overall goal of the AES programme was to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm capable of protecting sensitive government information well into the next (21st) century. The algorithm is expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.

B.1.2 Boundary conditions

The boundary conditions have been refined from an initial proposal identified in the announcement of the competition on January 2nd 1997.

The draft minimum acceptability requirements and evaluation criteria were published as:

- AES shall be publicly defined.
- AES shall be a symmetric block cipher.
- AES shall be designed so that the key length may be increased as needed.
- AES shall be implementable in both hardware and software.
- AES shall either be a) freely available or b) available under terms consistent with the American National Standards Institute (ANSI) patent policy.
- Algorithms which meet the above requirements will be judged based on the following factors:
    - security (i.e., the effort required to cryptanalyze);
    - computational efficiency;
    - memory requirements;
    - hardware and software suitability;
    - simplicity;
    - flexibility; and
    - licensing requirements.

After refinement the public call for candidates refined this list to a simpler summary of:

- An unclassified, publicly disclosed encryption algorithm(s), available royalty-free, worldwide.
- The algorithm(s) must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits and key sizes of 128-, 192-, and 256-bits.

B.2 Overall timetable

The timetable to develop AES shows an overall process lasting some 4 years, of which a period of only some 9 months was available to the algorithm designers to prepare the algorithm submission package. This package had to contain the following:

- cover sheet;
- algorithm Specifications and Supporting Documentation;
- magnetic media;
- intellectual property statements/agreements/disclosures.

The algorithm specification and documentation is the most demanding of these contributions to produce and has to itself contain the following:

- A complete written specification of the algorithm consisting of all necessary mathematical equations, tables, diagrams, and parameters that are needed to implement the algorithm. Furthermore the design rationale (e.g., method for generating table values, rationale for number of rounds, etc.) was strongly encouraged to be submitted in order to facilitate the public evaluation process.
- A statement of the algorithm's estimated computational efficiency in hardware and software containing a statement of the efficiency estimates for the "NIST AES analysis platform" and for 8-bit processors. Each estimate had to include a: description of the platform used to generate the estimate in sufficient detail so that the estimates could be verified in the public evaluation process; and, a speed estimate for the algorithm on the NIST AES analysis platform
- A series of Known Answer Tests (KATs) and Monte Carlo Tests (MCTs).
- A statement of the expected strength (i.e., workfactor) of the algorithm along with any supporting rationale. The expected strength shall be given for ***each*** key- and block-size combination claimed to be supported by the algorithm.
- An analysis of the algorithm with respect to known attacks (e.g., known and chosen plaintext).
- Any mathematical rationale for the non-existence of "trap-doors" in the algorithm, to the greatest extent possible.
- A list of known references to any published materials describing or analyzing the security of the submitted algorithm.
- A statement that lists and describes advantages and limitations of the algorithm where these address the algorithm's ability to:
    - implement the algorithm as a stream cipher, Message Authentication Code (MAC) generator, pseudo-random number generator, hashing algorithm, etc.
    - implement the algorithm in various environments, including - but not limited to: 8-bit processors (smartcards), ATM, HDTV, B-ISDN, voice applications, satellite applications, etc.
    - use the algorithm with key- and block-sizes other than those required as a minimum

In addition if the algorithm has certain features deemed advantageous by the submitter these should be listed and described along with supporting rationale.

Table B.1: Calendar of events in development of AES

Date	Milestone
~1978	Identification in DES endorsement that a replacement will be required at next review (1998)
2nd January 1997	Initial call, identifying outline boundary conditions
12th September 1997	Formal call for candidates
15th April 1998	Closing date for receipt of candidate packages wishing NIST review for completeness
15th May 1998	Deadline for NIST to send comments back for completion (as above)
15th June 1998	Closing date for receipt of candidate packages
20th August 1998	1st Candidate conference, identification of 15 candidates
March 1999	2nd Candidate conference, public review of candidates
15th April 1999	Selection of shortlist of 5 candidates
13th-14th April 2000	3rd Candidate conference, review of shortlisted candidates
15th May 2000	Close of public comments
2nd October 2000	Selection of Rijndael as AES algorithm
28th February 2001	Announcement of FIPS proposal identifying AES (Rijndael)
6th December 2001	Announcement of approval of FIPS-197 Advanced Encryption Standard
26th May 2002	Date at which FIPS-197 came into affect being compulsory and binding on US Federal agencies for the protection of sensitive data.

B.3 Analysis of AES

The analysis of AES is continuing even post selection. Whilst the initial analysis presented in the selection process was intended to aid the selection process this cannot, by the restrictions of time placed on the initial analysis, be considered complete.

Initial analyses of all candidates can be found at: http://csrc.nist.gov/encryption/aes/.

There are a number of new analyses of AES available many of which consider the internal operation of the algorithm (i.e. open box analysis). Such anlaysis may lead to viable black-box attacks on the algorithm. The present document will not list all available analyses but two sites of general interest are:

- http://www.isg.rhul.ac.uk/~mrobshaw/rijndael/rijndael.html, this from the Royal Holloway College of the University of London.

- http://www.counterpane.com/crypto-gram.html, this from Bruce Schneier, author of Applied Cryptography.

Annex C (informative): ETSI SAGE

The Security Experts Group is responsible for creating specifications in the area of cryptographic algorithms and protocols specific to fraud prevention/unauthorized access to public/private telecommunications networks and user data privacy.

The group provides a service to all ETSI TCs and organizations with whom ETSI has a formal relationship with. The full requirements (formal external specification, target dates, commercial objectives etc.) are defined by the sponsoring TC and SAGE. The TC is responsible for getting the agreement of the General Assembly or Board as appropriate for inclusions in the ETSI Work Programme of items which are to be carried out by the Group and for allocating the budgets needed to carry out the work.

The requirements set by the Technical Committee (or outside body) and SAGE define the confidentiality of the resulting output of the Group. The output shall either be open (for public algorithms) or confidential (for secret algorithms). Open output is passed to the sponsoring Technical Committee and handled by the normal Working Procedures. Confidential output is released only to those having received a written confidentiality undertaking.

C.1 SAGE Report from 2001 (extract)

SAGE is responsible for standardization in the area of cryptographic algorithms, products specific to fraud prevention and unauthorized access to public and private telecommunications networks, and in maintaining the privacy of user data.

Early in 2000, SAGE delivered two algorithms to the Third Generation Partnership Project (3GPP) which will be used to provide confidentiality and protect the integrity of data transmitted over Universal Mobile Telecommunications System (UMTS) networks. Based on the block cipher algorithm Kasumi, they have been published by ETSI and are available, and can be downloaded, from ETSI and other 3GPP Partners. These algorithms will be mandatory standards for future UMTS systems.

The Group was also asked by the 3GPP to design a set of example algorithms for authentication and key management, which may be used by operators of UMTS systems. Christened MILENAGE, these were completed and delivered to the 3GPP in December 2000 for publication by ETSI and its 3GPP Partners in 2001. The MILENAGE algorithms set uses as kernel the well known "Rijndael" algorithm which was selected by the National Institute for Standards and Technology (NIST) in the United States as the Advanced Encryption Standard (AES).

During the course of 1999 and the early part of 2000, ETSI Project Terrestrial Trunked Radio (EP TETRA) revised its security specification. As a result, SAGE was asked to design a number of additional key management algorithms for the TETRA system, as an annex to the existing TETRA Authentication and Key Management Algorithm Set 1 (TAA1). Designed primarily as a system for public safety organizations, TETRA relies heavily on security.

SAGE has been in existence now for nearly 10 years, during which it has designed many cryptographic algorithms for ETSI standards as well as for systems created outside ETSI. The motivation for this "proprietary design" has been the lack of usable publicly available algorithms and the national export controls on equipment containing cryptographic algorithms. Over recent years, however, the scene has changed. Controls on cryptography are slowly being relaxed and national policies are being superseded by international agreements. The number of publicly available cryptographic algorithms has also increased. These developments will certainly influence SAGE's work in the future. There will be a tendency for SAGE to publish the cryptographic algorithms (as is already done in the case of the UMTS algorithms) and, wherever possible, SAGE will base its designs on publicly available algorithms. In most cases, to achieve an efficient integration of an algorithm into a standard, adaptation and tailoring of existing algorithms will be needed. It will also always be essential to evaluate the specific use of an algorithm in a standard and to produce unambiguous specifications and test data. It is in these areas that the role of SAGE will remain important.

SAGE does not have an independent work plan. It will only take action when explicitly requested by other committees inside or outside ETSI; often last minute requests are made to SAGE. It is difficult therefore to predict the group's work programme in 2001, although it is expected to include the design of a new encryption algorithm for the Global System for Mobile (GSM) communication.

History

Document history			
V1.1.1	August 2003	Membership Approval Procedure	MV 20031024: 2003-08-26 to 2003-10-24