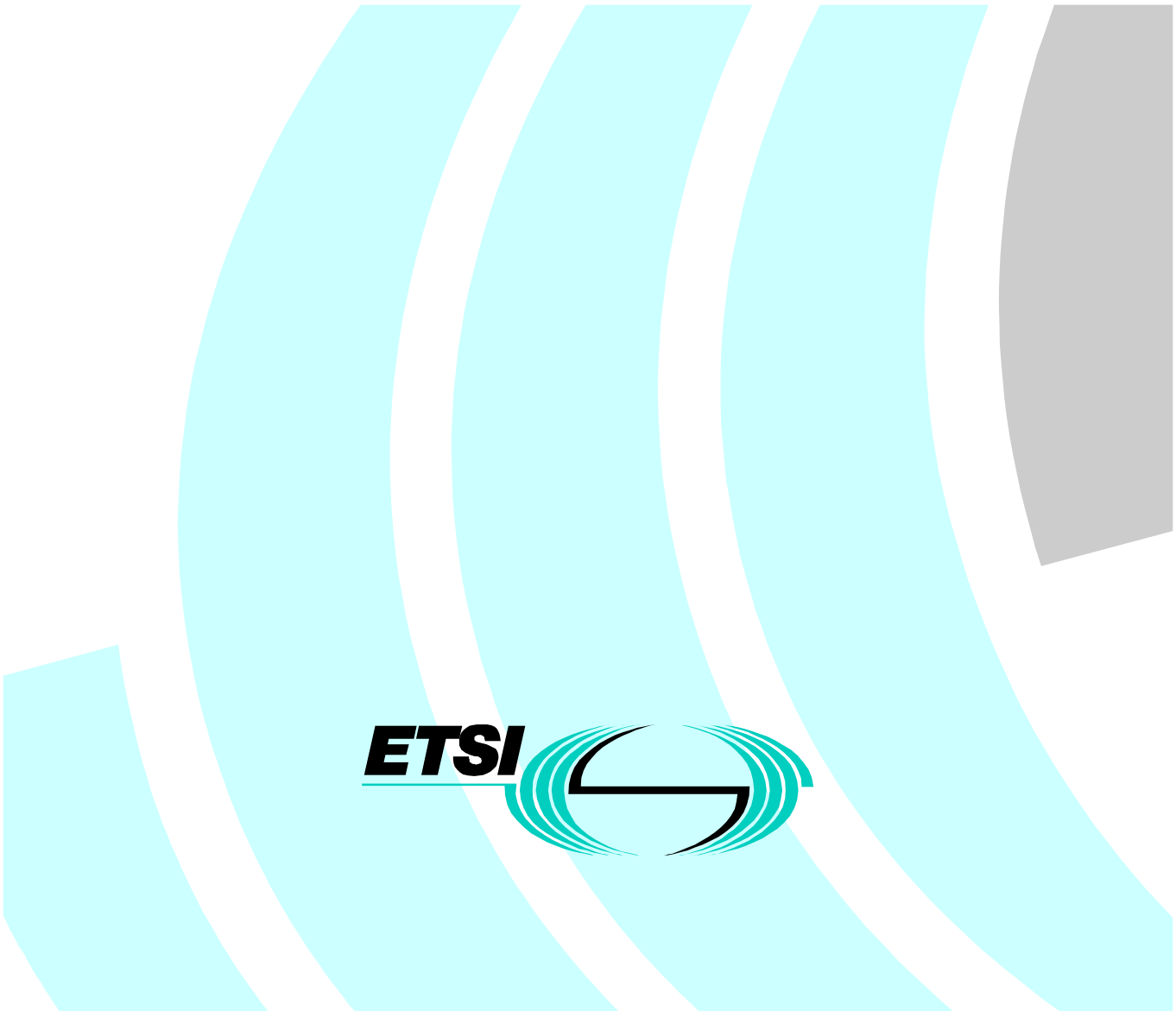
ETSI EG 200 234 V1.2.2 (2000-02)

ETSI Guide

Telecommunications Security;
A guide to specifying requirements
for cryptographic algorithms



Reference
REG/SEC-002606

Keywords
security, algorithm

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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 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://www.etsi.org/ipr).

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 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 Technical Committee Security (SEC).

The present document provides an overview on how to specify requirements for cryptographic algorithms which have to be specified as part of ETSI standards.

This information could be used as reference and/or background information when drafting new standards which incorporate security features.

1 Scope

It may be necessary to specify cryptographic algorithms as part of ETSI standards.

The present document outlines the procedure which should be followed when a cryptographic algorithm is needed for ETSI Standards (ES), European Standards (EN) or ETSI Guides (EG).

Furthermore, it provides guidelines for the formal specification of requirements when an algorithm has to be specially developed for use within an ETSI standard. A minimum set of items which should be included in the formal algorithm requirements specification 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, 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

NOTE: This one will be a living document on the SEC home page.

[2] ANSI X3.92-1981: "Data Encryption Algorithm".

3 Definitions

The definitions of security terminology in the present document conform to ETR 232 [1].

4 Abbreviations

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

ANSI	American National Standards Institute
DES	Data Encryption Standard
ECB	Electronic Code Book
IMAL	Imaginary Algorithm
IPR	Intellectual Property Right
NES	Non Existing Services (ETSI)
NISD	Needs Immediate Security Debugging
SAGE	Security Algorithms Group of Experts (ETSI)
STF	Special Task Force
TB	Tecnical Body
SEC	Technical Committee Security (ETSI)

5 Procedures for the provision of cryptographic algorithms for ETSI deliverables

The normal procedure for the provision of cryptographic algorithms for ETSI standards consists of the following phases:

5.1 Identification of needs

In this phase a TB identifies the need for a standardized cryptographic algorithm for use within an ETSI standard. SEC will provide advice if necessary.

At the end of this phase the TB should be able to provide an explicit, though not formal, description of the type and use of the algorithm. This description shall be provided for information to SEC, who could provide advice, taking into account of documented ETSI security standards and identified needs.

Responsibility for this phase is with the requiring TB.

5.2 Formal requirements specification

Having established the need for a cryptographic algorithm the responsible TB drafts a formal requirements specification according to the outline given in clause 6 of the present document.

If required, assistance may be sought from SEC. The formal requirements specification is submitted to SAGE for approval and for information to SEC, who could provide advice, taking into account of documented ETSI security standards.

Responsibility for this phase is with the requiring TB.

5.3 Decision on source of the algorithm

After approval of the requirements specification, SAGE will decide on the source for the algorithm. There are two main options:

a) an existing publicly available algorithm or an existing ETSI algorithm may be used; or

b) an application specific algorithm, possibly based on an existing algorithm, will be designed.

In the first case SAGE will check that the deliverables as described in the formal requirements specification are available and provide the TB with the adequate references for the algorithm specification. If needed SAGE will specify the rules and procedures for management and distribution of the algorithm and appoint a custodian.

In the second case the responsible TB and SAGE shall agree on a work plan, including time scales, funding arrangements and, if needed, STF assistance.

The design work will then be included as a work item in the ETSI work programme.

The responsibility for this phase is with SAGE.

5.4 Design and specification of management procedures

This phase only applies in the case where an application specific algorithm is to be designed by SAGE.

Following acceptance as an ETSI work item and agreed funding/STF arrangements, SAGE will undertake the design and/or specification work, produce the required deliverables and specify the rules and procedures for management and distribution of the algorithm. A custodian will be appointed.

The responsibility for this phase is with SAGE.

5.5 Algorithm distribution and maintenance

The custodian will distribute the algorithm according to the rules and procedures for the management and distribution. The custodian will also monitor literature for possible breaches of the security of the algorithm and take action if needed.

Responsibility for this phase is with the algorithm custodian, or with SAGE if there is no custodian appointed.

The procedures for the provision of cryptographic algorithms within ES/ENs and ETRs is illustrated in figure 1.

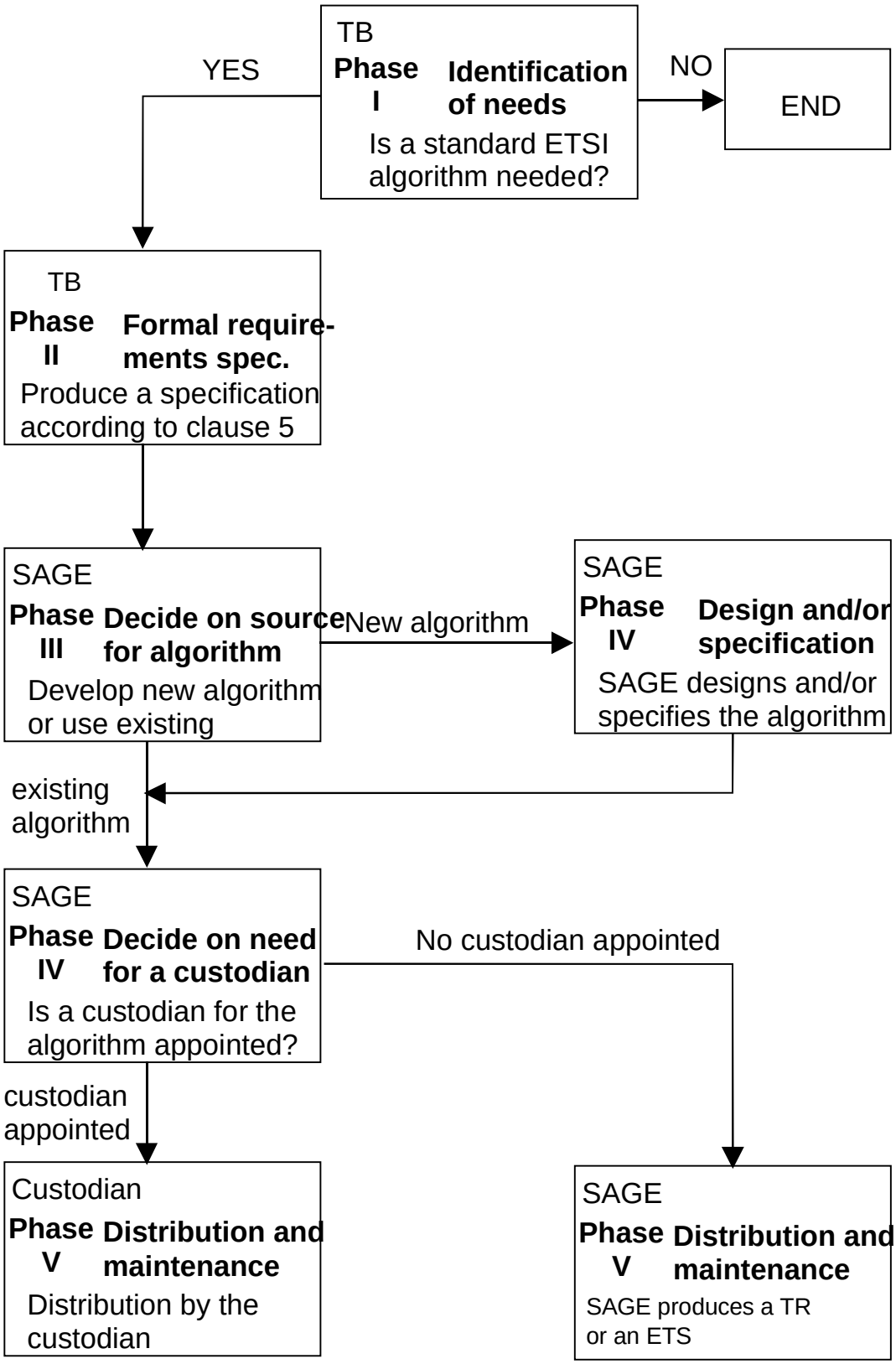

TB
Phase I
Identification of needs
Is a standard ETSI algorithm needed?
YES
NO
END
TB
Phase II
Formal require-ments spec.
Produce a specification according to clause 5
SAGE
Phase III
Decide on source for algorithm
Develop new algorithm or use existing
New algorithm
SAGE
Phase IV
Design and/or specification
SAGE designs and/or specifies the algorithm
existing algorithm
SAGE
Phase IV
Decide on need for a custodian
Is a custodian for the algorithm appointed?
No custodian appointed
custodian appointed
Custodian
Phase V
Distribution and maintenance
Distribution by the custodian
SAGE
Phase V
Distribution and maintenance
SAGE produces a TR or an ETS

Figure 1

6 Algorithm requirements specification

This clause describes an outline for a formal algorithm requirements specification which should be provided by the responsible TB to SAGE. Additional clauses may be provided on a case by case basis, if needed.

An example of an algorithm requirements specification is given in annex A.

Clause 1 - Scope

This clause shall provide an overall description of the context in which the algorithm will be used.

Clause 2 - References

All relevant references, including the ETSI standards of which the algorithm is part, should be listed in this clause. If necessary, notes may be used to indicate what the relevance of a reference is (e.g. describing the functionality, describing structure of information on which the algorithm is applied, etc.).

Clause 3 - Definitions

Where definitions do not appear in a referenced ES/EN or EG they should be defined here.

Clause 4 - Abbreviations

Any abbreviations used in the document shall be given in this clause. Care should be taken to align abbreviations with already established abbreviations used in other related documents.

Clause 5 - Background

This clause shall describe or provide references to the system in which the algorithm is to be used, the security service(s) for which the algorithm is required, the use of the algorithm in these services and the algorithm related protocol elements.

Clause 6 - Use of the algorithm

This clause should describe:

- who are the users of the algorithm;
- the purposes for which the algorithm is used;
- the places where the algorithm is used; and
- the types of implementation (hardware/software).

NOTE: The algorithm will only be specified/designed for the use described in this clause and clause 5, and not for any other use.

Clause 7 - Use of the algorithm specification

This clause should describe:

- who will own the algorithm and related test data specification;
- who will be entitled to use the algorithm specification;
- any procedures and requirements with respect to licensing and confidentiality agreements; and
- any procedures needed for distribution and management of the specification.

Clause 8 - Functional requirements

This clause should describe:

- the type of the algorithm and its relevant parameters;
- the detailed interfaces to the algorithm;
- modes of operation (if applicable);
- implementation complexity and operational constraints; and
- requirements for the strength of the algorithm.

Clause 9 - Algorithm specification and test data requirements

This clause should describe:

- what deliverables are required;
- the global contents of the deliverables;
- the format in which the deliverables should be provided (e.g. paper, magnetic disk); and
- to whom the deliverables should be submitted.

Deliverables might include the algorithm specification (including simulation code), conformance test data (for detailed testing of correctness of implementations), integration test data (for testing the correct response to interface data) and a design and evaluation report (outlining the procedures and results of the design and evaluation work, but not containing technical information on the algorithm).

Clause 10 - Quality assurance requirements

This clause should describe all requirements necessary to:

- ensure confidence that the algorithm is fit for purpose; and to
- ensure that deliverables match the desired quality standards.

Requirements may address:

- evidence that the algorithm conforms to the requirements;
- the correctness of the specification of the algorithm and test data; and
- verification of the estimates for performance and implementation complexity of the algorithm.

Clause 11 - Summary of ETSI deliverables

This clause will list the deliverables expected of SAGE.

Annex A - Bibliography

Any informative references, or further information may be included in this optional annex.

Annex A (informative): Example algorithm requirements specification

In this annex an algorithm requirement specification for an imaginary algorithm is presented. It serves as an example for a genuine algorithm specification.

Foreword

This draft ETSI Technical Report (TR) has been produced by the Non Existing Services (NES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

This TR is a requirements specification for the cryptographic algorithm Imaginary Algorithm (IMAL) for use in Needs Immediate Security Debugging (NISD) services.

This TR is intended for use by the ETSI Security Algorithms Group of Experts (SAGE), who are responsible for the design of the algorithm.

1 Scope

This draft ETSI Technical Report (TR) constitutes a requirements specification for a cryptographic algorithm which is used to protect Needs Immediate Security Debugging (NISD) services as specified by TC/NES (see TR XYZ [1]).

This TR is intended to provide the ETSI Security Algorithms Group of Experts (SAGE) with the information it requires in order to design and deliver a technical specification for such an algorithm.

The TR covers the intended use of the algorithm and use of the algorithm specification, technical requirements on the algorithm, requirements on the algorithm specification and test data, and quality assurance requirements on both the algorithm and its documentation. The report also outlines the background to the production of this TR.

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TR XYZ (1994): "Needs Immediate Security Debugging (NISD) service specification; Part 2: Security features".

NOTE: The present document provides a complete description of the information to be protected and the functional objectives of the system. For other references, see annex Ex-A.

3 Definitions

For the purposes of this TR, the definitions given in TR XYZ [1] apply.

4 Abbreviations

For the purposes of this TR, the following abbreviations apply:

ANSI	American National Standards Institute
DES	Data Encryption Standard
ECB	Electronic Code Book
IMAL	Imaginary Algorithm
IPR	Intellectual Property Right
NES	Non Existing Services (ETSI)
NISD	Needs Immediate Security Debugging
SAGE	Security Algorithms Group of Experts (ETSI)
SEC	Technical Committee Security (ETSI)

5 Background to this TR

Discussions within NES, with SEC and with other ETSI technical committees, led to the conclusion that NISD services can only be provided on a commercially solid and successful basis if appropriate security features are integrated into these services.

Consequently a report (EG NES 01234, NISD service specification, part 2, Security Features [1]) was produced, which specifies these security features. It was also concluded that, in order to support inter-operability between services providers, a standard ETSI cryptographic algorithm for use in NISD services needs to be specified.

6 Use of the algorithm

The purpose of this clause is to define those organizations for whom the algorithm is intended, describe the type of information which the algorithm is intended to protect, indicate possible geographical/geopolitical restrictions on the use of equipment which embodies the algorithm, and describe the types of implementations of the algorithm that are envisaged.

6.1 Users of the algorithm

The algorithm is intended to be used by service providers providing NISD services including the security functions as specified in EG XYZ [1].

All users of the algorithm will be required to sign a licence and confidentiality agreement with ETSI, as described in subclause 7.3.

6.2 Use of the algorithm

The algorithm may only be used for providing the NISD security features as described in EG XYZ [1].

Furthermore, within the context of EG XYZ [1], the use of the algorithm is restricted as follows:

- the algorithm may be used to provide confidentiality and integrity protection of NISD management data as defined in EG XYZ [1];

- the algorithm may be used to provide mutual authentication of an NISD service provider and the IC card of an end user of an NISD service;

- the algorithm may be used to provide mutual authentication of NISD service providers.

The algorithm may not be used to protect information on traffic channels between a user of services provided by an NISD service provider and that service provider.

6.3 Places of use

Equipment that embodies the algorithm may be located and used wherever those entitled to use the algorithm, as defined in subclause 6.1, need such equipment for the purposes defined in subclause 6.2, subject to the following:

- use of the equipment will always be under the control of an organization which is entitled to use the algorithm, and has signed a licence and confidentiality agreement with ETSI, irrespective of where the equipment may be located;
- this requirement does not apply in the case where the algorithm is located in the IC card of an end user of NISD services, where this IC card is use to provide access to NISD services;
- legal restrictions on the use or export of equipment containing cryptographic features that are enforced by various European Governments may prevent the use of equipment in certain countries.

Concerning the latter point, it is the intention that, by limiting both the organizations entitled to use the algorithm and the usage of the algorithm, and by requiring that use of any equipment that embodies the algorithm remains under the control of a party entitled to use the algorithm, any such legal restrictions should be minimal for the preferred method of implementation (see subclause 6.4).

6.4 Types of implementation

The preferred method for implementing the algorithm is either in hardware as a single chip device or on an IC card, although software implementations are also envisaged.

In the case of a software implementation of the algorithm, legal restrictions on its export and, in certain countries, on its use may be expected to be more stringent than for a hardware or IC card implementation.

Those implementing the algorithm will be required through a licence and confidentiality agreement which they shall sign with ETSI, as described in subclause 7.3, to adopt suitable measures to ensure that their implementations are commensurate with the need to maintain confidentiality of the algorithm.

7 Use of the algorithm specification

The purpose of this clause is to address ownership of the algorithm specification, to define which types of organization are entitled to obtain a copy of the algorithm specification, and to outline how and under what conditions such organizations may obtain the specification.

7.1 Ownership

The algorithm and all copyright to the algorithm and test data specifications will be owned exclusively by ETSI.

The design authority for the algorithm will be SAGE. Amendments to the algorithm specification may be made only by SAGE under instruction authorized by the ETSI Technical Assembly.

The algorithm specification will not be published as an ETSI standard or otherwise made publicly available, but will be provided to organizations that need and are entitled to receive it subject to a licence and confidentiality agreement.

The licence and confidentiality agreement will require recipient of the specification not to attempt to patent the algorithm or otherwise register an Intellectual Property Right (IPR) relating to the algorithm or its use.

7.2 Users of the specification

The algorithm specification may be made available to the following types of organizations:

- those entitled to use the algorithm as defined in subclause 6.1;
- those who need the algorithm specification in order to build equipment or components which embody the algorithm.

7.3 Licensing

Users of the algorithm, and users and recipients of the algorithm specification, will be required to sign a licence and confidentiality agreement with ETSI.

Appropriate licence and confidentiality agreements will be drawn up by ETSI.

Licences will be royalty free. However, the algorithm custodian may impose a small charge to cover administrative costs involved in issuing the licences.

It is envisaged that there will be two types of licence and confidentiality agreement: one for service provider of NISD services entitled to use the algorithm, as defined in subclause 6.1, and one for organizations who need the algorithm specification in order to build equipment or components which embody the algorithm, as defined in subclause 7.2.

The licence and confidentiality agreement signed by a service provider of NISD services will require that organization to comply with the restrictions on the use of the algorithm listed in subclause 6.2. The agreement will also require such an organization to ensure that any supplier of implementations of the algorithm to that organization signs an appropriate licence and confidentiality agreement with ETSI.

In the case of a service provider of NISD services, the licence and confidentiality agreement will also entitle it to authorize organizations, who need the algorithm specification in order to build equipment or components which embody the algorithm, to obtain the specification, by requesting ETSI to enter into a licence and confidentiality agreement to supply the specification to such organizations.

The licence and confidentiality agreement signed by an organization that needs the algorithm specification in order to build equipment or components which embody the algorithm, will require that organization to adopt measures to ensure that its implementations of the algorithm are commensurate with the need to maintain confidentiality of the algorithm. The agreement will also require such an organization only to supply implementations of the algorithm to organizations that have signed an appropriate licence and confidentiality agreement with ETSI.

7.4 Management of the specification

The distribution procedure for the algorithm specification will be specified by ETSI. The outline procedure is as follows.

- ETSI will appoint a custodian for administration of the algorithm specification.
- A service provider of NISD services may request copies of the algorithm specification (and test data) and a licence to use the algorithm from the custodian.
- If the service provider of NISD services is entitled to use the algorithm, the custodian will issue the requested algorithm specifications subject to the NISD service provider signing a licence and confidentiality agreement.
- A service provider of NISD services who is licensed to use the algorithm may request ETSI to provide copies of the algorithm specification to an organization which intends to build equipment or components that embody the algorithm. Such an organization will then be required by ETSI to sign a licence and confidentiality agreement before receiving the algorithm specifications from the custodian.

8 Functional requirements

SAGE are required to design an algorithm which satisfies the functional requirements specified in this clause.

8.1 Type and parameters of algorithm

The algorithm is to be a symmetric block cipher.

The parameters of the algorithm are to be as follows:

- block length: 64 bits;
- key length: 64 bits.

The key is unstructured data.

8.2 Interfaces to the algorithm

The following interfaces to the algorithm are defined:

- data input:

  X[0], X[1], ... , X[63]

  where X[i] is the data input bit with label i;

- data output:

  Y[0], Y[1] ... , Y[63]

  where Y[i] is the data output bit with label i;

- key input:

  K[0], K[1], ... , K[63]

  where K[i] is the key bit with label i.

8.3 Modes of operation

The algorithm shall be able to operate in all the ISO standard modes of operation for a block cipher as referenced in TR XYZ [1].

8.4 Implementation and operational considerations

The algorithm shall be designed so as to accommodate a spectrum of implementation options, ranging from implementation as a single chip device to implementations in software. At the latter extreme, it shall be possible to implement the algorithm on a 32 bit microprocessor running at 25 MHz to achieve a speed of 64 kbits/s in the ECB mode of operation for NISD services as specified in TR XYZ [1].

8.5 Resilience of the algorithm

The algorithm shall be designed with a view to its continued use for a period of at least 10 years.

When used in conjunction with appropriate security protocols and sound key management the algorithm should in practice provide impenetrable protection of the service management data it is used to secure.

SAGE are required to design the algorithm to a strength which reflects the above qualitative requirements.

9 Algorithm specification and test data requirements

SAGE are required to provide four separate deliverables:

- a specification of the algorithm;
- a set of implementors' test data;
- a set of design conformance test data; and
- a design and evaluation report.

Requirements on the specification and test data deliverables are given in this clause, those on the design and evaluation report in subclause 10.3.

9.1 Specification of the algorithm

An unambiguous specification of the algorithm shall be provided which is suitable for use by implementers of the algorithm.

The specification should include an annex which provides simulation code for the algorithm written in ANSI C. The specification may also include an annex containing illustrations of functional elements of the algorithm.

An example of a well defined specification is ANSI X3.92-1981, the American national standard for data encryption algorithms (see annex EX-A).

9.2 Design conformance test data

Design conformance test data is required to allow implementers of the algorithm to test their implementations.

The design conformance test data shall be designed to give a high degree of confidence in the correctness of implementations of the algorithm.

The design conformance test data should be designed so that significant points in the execution of the algorithm can be verified.

Separate design conformance test data for hardware and software implementations may be provided if this is judged by the designers of the algorithm to be appropriate.

9.3 Algorithm input/output test data

Algorithm input/output test data is required to allow users of the algorithm to test the algorithm as a "black box" function.

The input/output test data should allow users of the algorithm to perform tests for the modes of operation defined in subclause 8.3.

The input/output test data should consist solely of data passed across the interfaces to the algorithm.

9.4 Format and handling of deliverables

The specification of the algorithm should be produced on paper, and provided only to the ETSI appointed custodian (see subclause 7.4). The document should be marked *"Strictly ETSI confidential"* and carry the warning *"This information is subject to a licence and confidentiality agreement"*.

The design conformance test data should be produced on paper, and provided only to the ETSI appointed custodian. The document should be marked *"Strictly ETSI confidential"* and carry the warning *"This information is subject to a licence and confidentiality agreement"*.

The algorithm input/output test data should be produced on paper and on magnetic disc. The document and disc should be provided to the ETSI appointed custodian. Special markings or warnings are not required.

10 Quality assurance requirements

The purpose of this clause is to advise SAGE on measures needed to provide users of the algorithm with confidence that it is fit for purpose, and users of the algorithm specification and test data assurance that appropriate quality control has been exercised in their production.

The measures will be recorded by SAGE in a design and evaluation report which will be published by ETSI as a Technical Report.

10.1 Quality assurance for the algorithm

Prior to its release to the ETSI custodian, the algorithm shall be approved as meeting the technical requirements specified in clause 8 by all members of SAGE.

10.2 Quality assurance for the specification and test data

Prior to delivery of the algorithm specification, two independent simulations of the algorithm shall be made using the specification, and confirmed against test data designed to allow verification of significant points in the execution of the algorithm.

Design conformance and algorithm input/output test data shall be generated using a simulation of the algorithm produced from the specification and confirmed as above. The simulation used to produce this test data shall be identified in the test data deliverables and retained by SAGE.

10.3 Design and evaluation report

The design and evaluation report is intended to provide evidence to potential users of the algorithm, specification and test data that appropriate and adequate quality control has been applied to their production. The report should explain the following:

- the algorithm and test data design criteria;
- the algorithm evaluation criteria;
- the methodology used to design and evaluate the algorithm;
- the extent of the mathematical analysis and statistical testing applied to the algorithm;
- the principal conclusions of the algorithm evaluation;
- the quality control applied to the production of the algorithm specification and test data.

The report shall confirm that all members of SAGE have approved the algorithm, specification and test data.

The report shall not contain any information about the algorithm, such as design techniques used, mathematical analysis or statistical testing of components of the algorithm, which might reveal part or all of the structure or detail of the algorithm.

11 Summary of SAGE deliverables

- Specification of the algorithm - a confidential document for delivery only to the ETSI custodian.
- Design conformance test data - a confidential document for delivery only to the ETSI custodian.
- Algorithm input/output test data - in a document and on disc for delivery to the ETSI custodian.
- Design and evaluation report - to be published as an ETSI Technical Report (TR).

Annex EX-A: Bibliography

1) ANSI X3.92-1981: "Data Encryption Algorithm".

History

Document history		
Edition 1	November 1995	Publication as ETR 234
V1.2.1	October 1999	Membership Approval Procedure MV 9949: 1999-10-05 to 1999-12-03
V1.2.2	February 2000	Publication