ETSI
TECHNICAL COMMITTEE
REFERENCE TECHNICAL REPORT

TCR-TR 037

November 1995

Source: ETSI TC-NA

Reference: DTR/NA-002303

ICS: 33.040

Key words: encryption, PTN, security

Security Techniques Advisory Group (STAG); Requirements specification for an encryption algorithm for operators of European public telecommunications networks

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI). This TCR-TR has been endorsed by the 21st TC Chairmens' Co-ordination (TCC 21) meeting, and approved by the 23rd Technical Assembly (TA 23).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilized by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

This TCR-TR is a requirements specification for an encryption algorithm for operators of European public telecommunications networks.

Subject to consideration and approval by ETSI Technical Committee Network Aspects (TC NA), an earlier version of this document was sent to public network operators for their comments.

This report is intended for use by ETSI SAGE who will be responsible for the design of the encryption algorithm.

Blank page

1 Scope

This Technical Committee Reference Technical Report (TCR-TR) constitutes a requirements specification for an encryption algorithm which may be used by operators of European public telecommunications networks. This TCR-TR is intended to provide 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.

This TCR-TR covers the intended use of the algorithm and 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. This TCR-TR also outlines the background to the production of this TCR-TR.

This TCR-TR includes three annexes. Annex A provides a structure for a form which public network operators were invited to use to submit comments on an earlier version of this document. Annex B is a summary of cryptographic integrity and authentication mechanisms which may be provided using the algorithm. Annex C consists of a list of references to documents used in the preparation of this TCR-TR.

2 References

This TCR-TR incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this TCR-TR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ISO/IEC 10116 (1991): "Information technology - Modes of operation for an n-bit block cipher algorithm".

For informative references, used to produce this TCR-TR, see annex C.

3 Abbreviations

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

ANSI	American National Standards Institute
DES	Data Encryption Standard
ECB	Electronic Code Book
EURESCOM	European institute for Research and Strategic studies in telecommunications
IPR	Intellectual Property Rights
ISO	International Standards Organisation
SAGE	Security Algorithms Group of Experts

4 Introduction

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

Clause 5 outlines the sequence of events which led to the production of the report.

Clauses 6 and 7 describe the context in which the algorithm and specification are intended to be used. Clause 6 outlines the intended use of the algorithm in terms of which organisations will be entitled to use it, what they will use it for, where it will be used, and how it will be implemented. Clause 7 describes the intended use of the algorithm specification in terms of who will own it, who will use it, and how and under what conditions the specification will be provided to those users.

Clause 8 specifies the functional requirements for the algorithm. This covers the type and parameters of the algorithm, the interface to the algorithm, the envisaged modes of operation of the algorithm, implementation and operational considerations which may have an impact on the design of the algorithm and requirements on the resilience of the algorithm.

Clause 9 details requirements on the algorithm specification and associated test data deliverables.

Clause 10 addresses quality assurance requirements, needed to give confidence in the design of the algorithm and the adequacy of the algorithm specification and test data.

Clause 11 is a summary of the deliverables expected from ETSI SAGE.

5 Background to the report

Discussions within ETSI NA/STAG, within other ETSI technical committees and elsewhere, concerning the potential need for an encryption algorithm which could be used by European public network operators to protect sensitive network management data, prompted the Director of ETSI to write to network operators seeking their views on the merits of a concerted and common approach to the development of a suitable algorithm. In the light of a positive response to the idea from a number of network operators, the ETSI Technical Assembly agreed that NA/STAG should make detailed recommendations for the development of an algorithm by ETSI SAGE, the recommendations to take into account work already undertaken by EURESCOM, given in the EU-P110 Task 32 Report (see annex C) on the subject.

This TCR-TR constitutes NA/STAG's recommendations on the subject. It will be submitted to ETSI SAGE for action.

6 Use of the algorithm

The purpose of this clause is to define those organisations 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 network operators who are members of ETSI licensed to operate a European public telecommunications network.

A network operator entitled to use the algorithm may authorise other parties, making use of the network management services provided by that operator, to use the algorithm to protect those services, provided the operator ensures compliance with restrictions on the use of the algorithm and equipment that embodies the algorithm given in subclauses 6.2 and 6.3 respectively.

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 to protect network management, subscription, or service related data which is held within network entities, or transferred between network entities within the same or belonging to different networks. For the purpose of this document, such data will be referred to simply as "network management data".

Although the algorithm may be used in a number of different applications, within the domain of a user entitled to use the algorithm or between the domains of such users, it is intended to be used and restricted in its use as follows:

- **inter domain uses:**

  - the algorithm may be used to provide confidentiality protection to network management data transferred between the domains of authorised users;

  - the algorithm may be used to provide integrity protection to network management data transferred between the domains of authorised users;

  - the algorithm may be used to provide authentication of entities used to transfer network management data between the domains of authorised users;

- **intra domain uses:**

  - the algorithm may be used to provide confidentiality protection to network management data transferred within the domain of an authorised user;

  - the algorithm may be used to provide integrity protection to network management data transferred within the domain of an authorised user;

  - the algorithm may be used to provide confidentiality protection to network management data stored within the domain of an authorised user;

  - the algorithm may be used to provide integrity protection to network management data stored within the domain of an authorised user;

  - the algorithm may be used to provide authentication of entities used to transfer or access network management data within the domain of an authorised user.

- **explicitly excluded uses:**

  - the algorithm may not be used to protect information on traffic channels or signalling access channels between a user of services provided by a network operator and that network operator, or between one user of such services and another;

  - the algorithm may not be used to authenticate user, or user terminal equipment, access to services provided by a network operator.

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 to protect their network management data, as defined in subclause 6.2, subject to the following:

- use of the equipment will always be under the control of an organisation 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;

- legal restrictions on the use or export of equipment containing cryptographic features that are enforced by various European Governments may prevent the use of such equipment in certain countries.

Concerning the latter point, it is the intention that, by limiting both the organisations 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 in hardware as a single chip device, 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 implementation.

Those implementing the algorithm will be required through a licence and confidentiality agreement which they shall be signed 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 organisation are entitled to obtain a copy of the algorithm specification, and to outline how and under what conditions such organisations 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 ETSI SAGE. Amendments to the algorithm specification may be made only by ETSI SAGE under instruction authorised 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 organisations that need and are entitled to receive it subject to a licence and confidentiality agreement.

- The licence and confidentiality agreement will require recipients to the specification not to attempt to patent the algorithm or otherwise register any Intellectual Property Rights (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 organisations:

- 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, ETSI 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 network operators and other parties entitled to use the algorithm, as defined in subclause 6.1, and one for organisations 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 network operator, or by an organisation authorised by a network operator to use the algorithm, will require that organisation to comply with the restrictions on the use of the algorithm listed in subclause 6.2. The agreement will also require such an organisation to ensure that any supplier of implementations of the algorithm to that organisation signs an appropriate licence and confidentiality agreement with ETSI.

In the case of network operators, the licence and confidentiality agreement will also entitle them to:

- authorise other parties, as defined in subclause 6.1, to use the algorithm, by requesting ETSI to enter into a licence and confidentiality agreement with such parties;

- authorise organisations, 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 organisations.

The licence and confidentiality agreement signed by an organisation that needs the algorithm specification in order to build equipment or components which embody the algorithm, will require that organisation 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 organisation only to supply implementations of the algorithm to organisations 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 network operator may request copies of the algorithm specification (and test data) and a licence to use the algorithm from the custodian;

- if the network operator is entitled to use the algorithm, the custodian will issue the requested algorithm specifications subject to the network operator signing a licence and confidentiality agreement;

- a network operator who is licensed to use the algorithm may request ETSI to licence the use of the algorithm and, if necessary, provide copies of the algorithm/specification to a party it authorises to use the algorithm. Such a party will then be required by ETSI to sign a licence and confidentiality agreement before using the algorithm or receiving algorithm specifications from the custodian;

- a network operator who is licensed to use the algorithm may request ETSI to provide copies of the algorithm specification to an organisation which intends to build equipment or components that embody the algorithm. Such an organisation will then be required by ETSI to sign a licence and confidentiality agreement before receiving the algorithm specifications from the custodian.

8 Functional requirements

ETSI 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 and 80 bits option

The key is unstructured data.

ETSI SAGE may design the algorithm to support longer key lengths if they consider this to be necessary (see subclause 8.5).

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 (key length = N):
  K[0], K[1], ..., K[N-1]
  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 defined in ISO/IEC 10116 [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/sec in ISO standard ECB mode of operation.

8.5 Resilience of 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 network management data it is used to secure.

ETSI SAGE are required to design the algorithm to a strength which reflects the above qualitative requirements and permits operation with a range of key lengths (see subclause 8.1).

9 Algorithm specification and test data requirements

ETSI SAGE are required to provide four separate deliverables: a specification of the algorithm, a set of design conformance test data, a set of algorithm input/output 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 implementors 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 the American national standard for DES, ANSI X3.92 (see annex C).

9.2 Design conformance test data

Design conformance test data is required to allow implementors 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, and so that all elements of any tables used in the algorithm are exercised at least once.

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 ETSI 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 ETSI 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 needs to be approved as meeting the technical requirements specified in Clause 8 by all members of ETSI 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. At least one simulation should be made by a party who has had no involvement in the design, evaluation or testing 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 ETSI 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 ETSI 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 ETSI 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.

Annex A (informative): Comment form

This annex consists of a format for a form which may be used by European operators of public telecommunications networks to help prepare and submit their comments on the requirements for the encryption algorithm which is the subject of this document.

Table A.1: Requirements specification for an encryption algorithm for operators of European public telecommunications networks

Source of Comments:			
Date:			
No.	Reference[1)]	Comment[2)]	Level[3)]
1			
2			
3			
4			

1) Give subclause and line.
2) Where the comment implies a significant change to the document, suggested replacement text should be provided on a separate sheet.
3) H = Highly significant (unless the comment is satisfactorily addressed, the originator will not use the algorithm).

Annex B (informative): Cryptographic mechanisms

It is envisaged that the algorithm may be used to provide data integrity and authentication in association with the following cryptographic mechanisms:

- Message Authentication Code (MAC) generation as specified in ISO/IEC 9797;

- entity authentication mechanisms specified in ISO/IEC CD 9798-2.

M = Moderately significant (failure to address the comment may limit some desired uses of the algorithm by the originator).

Annex C (informative): Bibliography

- ANSI X3.92-1981: "American National Standard Data Encryption Algorithm".

- EURESCOM, EU-P110 Task 32 Report, 22 April 1993: "Requirements for a cryptographic algorithm to be used in an inter-PNO environment".

- ISO/IEC 9797 (1989): "Data cryptographic techniques - data integrity mechanism using a cryptographic check function employing a block cipher algorithm".

- ISO/IEC CD 9798-2: "Information technology - Security techniques - Entity authentication mechanisms - Part 2: Entity authentication using symmetric techniques".

History

Document history			
August 1995	Draft for endorsement by	TCC 21	1995-09-25 to 1995-09-27
September 1995	Final draft for approval by	TA 23	1995-11-07 to 1995-11-09
November 1995	First Edition		