INTERNATIONAL STANDARD

ISO/IEC 9979

Second edition
1999-04-01

Information technology — Security techniques — Procedures for the registration of cryptographic algorithms

Technologies de l'information — Techniques de sécurité — Procédures d'enregistrement des algorithmes cryptographiques

Reference number
ISO/IEC 9979:1999(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 9979 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9979:1991), which has been technically revised.

Annex A forms an integral part of this International Standard. Annex B is for information only.

Information technology — Security techniques — Procedures for the registration of cryptographic algorithms

1 Scope

This International Standard specifies the procedures for the registering of cryptographic algorithms and the form of register entries.

This International Standard is for use by those wishing to make entries in the register and by the Registration Authority.

The ISO/IEC register of cryptographic algorithms serves as a common reference point for the identification of cryptographic algorithms by a unique name. The register is also a repository of basic parameters identified with the register entry. The principal purpose of the register is to enable entities to identify and negotiate an agreed cryptographic algorithm.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 8825:1990, *Information technology — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

ISO/IEC 9834-1:1993, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General procedures.*

3 Registration Authority[1]

The Registration Authority shall be an organization designated by ISO/IEC Councils.

4 Role of the Registration Authority

The Registration Authority shall maintain a register of cryptographic algorithms and this will be known as the "ISO/IEC Register of Cryptographic Algorithms". The Registration Authority performs a technical role in ensuring that register entries conform to the registration procedures given in this International Standard.

---

[1] For the purposes of this International Standard and according to the rules for the designation and operation of Registration Authorities in the ISO/IEC JTC 1 Procedures, ISO/IEC Councils have designated the National Computer Centre, Oxford Road, Manchester, UK, to act as the Registration Authority.

The Registration Authority does not evaluate or make any judgement of the quality of protection provided by the registered algorithm.

The Registration Authority is entrusted with the following functions:

a) to add, modify and delete register entries in accordance with the rules provided;

b) assign ISO-entry names to registered cryptographic algorithms as needed;

c) update and to have published the register when required.

5 Algorithms to be Registered

The cryptographic algorithms to be registered are those used in information protection services[2]. Annex A defines one particular use of a cryptographic algorithm (for confidentiality). Subclause 9.3 indicates other uses of cryptographic algorithms.

A registered algorithm may be one of the following types:

a) Algorithms in which a complete description of the process accompanies the registration entry;

b) Algorithms in which the complete description of the process is defined in an ISO document, or a standard maintained by a Member Body of ISO or by a liaison organization;

c) Algorithms in which the complete description is not fully defined (or not defined at all).

6 Procedures for Registration

6.1 Submission of new entries to the register may be originated or sponsored only by a Member Body, an ISO Technical Committee, or liaison organization.

It is the prime responsibility of the body or organisation submitting the new entry to provide complete, understandable and unambiguous details in respect of the information described in 7 (b to i) and optionally (j to m). Proposals shall be rejected if they fail to comply with these requirements.

Register Entry proposals shall be in the form specified in clause 9.

6.2 On acceptance of a submission for a new entry to the register, the Registration Authority will assign an entry name to the algorithm.

6.3 Submissions for modification or deletion of existing entries to the register may be originated by a Member Body or liaison organization.

6.4 When a submission concerns the modification or deletion of a registered entry, it shall be subject to approval by ISO/IEC JTC1 and the originator of the register entry.

[2] Information protection services include confidentiality, integrity, authentication and non-repudiation.

7 General Contents of the Register

For each algorithm to be registered, the Register Entry will contain the following details:

Mandatory (a to i)

a) a formal ISO-entry name for the algorithm;

b) the proprietary name (or names) given to the algorithm by its originator or owner;

c) intended range of applications for the algorithms;

d) cryptographic interface parameters;

e) a set of test words to check basic functionality;

f) the identity of the organization that requested registration of the algorithm;

g) the dates of registration and modifications;

h) whether the entry is the subject of a national standard;

i) patent licence restriction information;

Optional (j to m)

j) a list of references to any associated algorithms;

k) description of the algorithm;

l) modes of operation;

m) other information.

NOTE The date of submission is provided by the submitter, and the date of registration and modification is provided by the Registration Authority.

8 Publishing of Register Entries

8.1 The Registration Authority shall

a) publish a list of entries yearly if changes have occurred;

b) publish the complete register on request;

c) supply individual register entries on request;

d) notify changes to all sponsoring authorities within three months.

The entries shall be grouped in three parts, each part classified according to the registered algorithm types given in clause 5.

8.2 The publication of entries shall make clear that the registration authority has not evaluated or made any judgement of the quality of protection provided by the registered algorithm. Each entry shall be labelled with a statement saying that registration of the algorithm does not imply that the algorithm is an ISO standard.

9 Form for Register Entries

The headings of this clause are those that shall be used in the Register Entry. The contents of each clause and subclause are defined in the corresponding text below.

9.1 ISO Entry Name

The form of this subclause is an object identifier.

The object identifier values for ISO entry names shall be composed in accordance with the general rules for the composition of unambiguous names contained in ISO 9834-1. These object identifier values shall be in the form {iso standard 9979 algorithm-identifier (n)} where "algorithm-identifier" identifies a specific entry in the cryptographic algorithm register by means of the index value "n".

In addition to object identifiers being assigned to algorithms, such identifiers can be assigned to valid combinations of an algorithm and a mode of operation. These should be in the form {iso standard 9979 algorithm-identifier (n), mode-identifier (m)}, where n is the index of the algorithm in the register and a different value of m is used to denote each of the modes of operation identified in entry (l) of the register. See Annex B for further information.

9.2 Proprietary Entry Name

This subclause shall specify the proprietary name (or names) given to the Register Entry by its originator or owner. A typical example is Data Encryption Standard (DES). The sponsor needs to clear any issues regarding proprietary or trade names before submitting a new entry to the register.

9.3 Intended Range of Applications

This subclause shall specify the intended range of uses of the cryptographic algorithm identified in the Register Entry. This will typically be done by reference to a common set of security functions or associated mathematical transformations. Typical examples are

a) confidentiality;

b) authentication;

c) data integrity;

d) digital signatures;

e) hash functions.

9.4 Cryptographic Interface Parameters

This subclause shall specify those parameters necessary for the use of the cryptographic algorithm.

Examples of commonly known parameters are

a) input size;

b) output size;

c) key length;

d) Initializing Value size;

e) encrypt or decrypt mode.

9.5 Test Words

This subclause specifies test words and any necessary procedures to check the functionality of the implementation of the cryptographic algorithm. It is the responsibility of the originator of the entry to ensure that the tests and any necessary procedures are sufficient to validate the basic functionality.

NOTE These test words are intended only to be used to ensure that an implementation of the algorithm works. The test words are not intended to demonstrate the full functionality of the algorithm or that it conforms exactly to any mathematical description that might be available.

9.6 Name of Sponsoring Authority

This subclause shall contain the name of the sponsoring ISO Member Body or liaison organization which submitted the Register Entry, and a point of contact for questions and comments.

9.7 Dates of Registration and Modifications

This subclause shall contain the dates when the record was added and modified by the Registration Authority.

9.8 Whether the Subject of a National Standard

This subclause shall contain information as to whether the cryptographic algorithm is the subject of a National Standard(s), and if so which.

9.9 Patent Licence Restrictions

This subclause shall contain any known patent licence restrictions on the cryptographic algorithm and/or its implementation.

9.10 References

This subclause may be used to contain, in the form required by the ISO Directives, a list of all other documents referenced in this Register Entry. These would generally be ISO International Standards or ITU (International Telecommunications Union) recommendations, but may be other material covered by the ISO Directives including National Standards.

9.11 Description of Algorithm

This subclause describes the algorithm.

9.12 Modes of Operation

This subclause shall specify a set of applicable modes of operation. Examples are

a) Electronic Code Book;

b) Cipher Feedback;

c) Cipher Block Chaining;

d) Output Feedback;

e) Additive Stream Cipher;

f) Black Box.

9.13 Other Information

This subclause may contain any other relevant information not given in above. Typical examples might be:

a) design rules;

b) its cryptographic strength (or any associated analysis);

c) any judgements regarding its suitability for specific applications or systems;

d) transmission characteristics;

e) guidance on key selection.

Annex A
(normative)

Definition of a cryptographic algorithm for confidentiality

A.1 Introduction

This annex defines a cryptographic algorithm for confidentiality for the purposes of registration.

A.2 Definition

A cryptographic algorithm for confidentiality is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. This is shown in figure A.1.

This definition includes both symmetric algorithms (e.g. DES and FEAL) and asymmetric algorithms (e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter.

A.3 Figure A.1

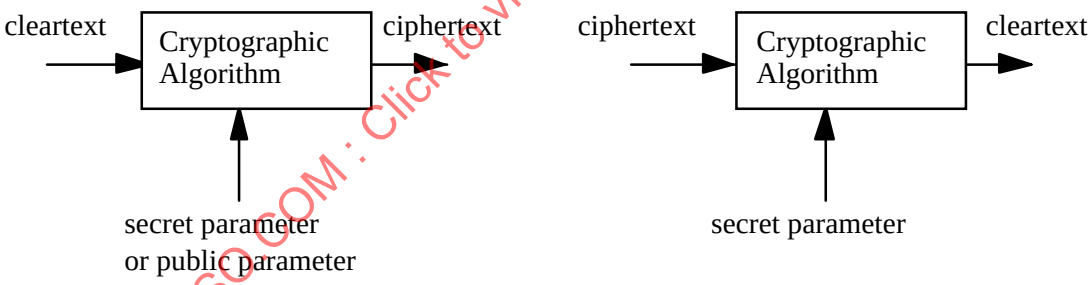

Figure A.1