NORME INTERNATIONALE

ISO/CEI 9979

Première édition
1991-12-15

Techniques cryptographiques — Procédures pour l'enregistrement des algorithmes cryptographiques

Data cryptographic techniques — Procedures for the registration of cryptographic algorithms

Numéro de référence
ISO/CEI 9979:1991(F)

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement des Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 9979 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information.*

L'annexe A fait partie intégrante de la présente Norme internationale. L'annexe B est donnée uniquement à titre d'information.

ISO/CEI Copyright Office • Case postale 56 • CH-1211 Genève 20 • Suisse
Version française tirée en 1992

Imprimé en Suisse

Techniques cryptographiques — Procédures pour l'enregistrement des algorithmes cryptographiques

1 Domaine d'application

La présente Norme internationale spécifie les procédures pour l'enregistrement des algorithmes cryptographiques et le format des entrées du registre.

La présente Norme internationale est destinée à ceux qui souhaitent faire des entrées dans le registre et à l'Autorité d'Enregistrement.

Le registre ISO des algorithmes cryptographiques sert de point de référence commun pour l'identification des algorithmes cryptographiques par un nom unique. Le registre est également un dépôt des paramètres de base identifiés avec l'entrée du registre. Le registre permet principalement aux entités d'identifier et de négocier un algorithme cryptographique commun.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui est en faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO/CEI 8825:1990 *Technologies de l'information — Interconnexion des systèmes ouverts — Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro 1 (ASN.1).*

ISO/CEI 9834-1 : —[1] *Technologies de l'information — Interconnexion des systèmes ouverts — Procédures pour le fonctionnement des autorités d'enregistrement OSI — Partie 1 : Procédures générales.*

3 Autorité d'Enregistrement [2]

L'Autorité d'Enregistrement doit être une organisation désignée par les conseils de l'ISO et de la CEI.

4 Rôle de l'Autorité d'Enregistrement

L'Autorité d'Enregistrement doit tenir à jour un registre des algorithmes cryptographiques connu sous le nom de «Registre ISO des Algorithmes Cryptographiques». L'Autorité d'Enregistrement assure un rôle technique en garantissant que les entrées de registre sont conformes aux procédures d'enregistrement données dans la présente Norme internationale.

L'Autorité d'Enregistrement n'évalue ni ne porte aucun jugement sur la qualité de protection offerte par l'algorithme enregistré.

L'Autorité d'Enregistrement est responsable des fonctions suivantes :

a) ajouter, modifier et supprimer des entrées du registre conformément aux règles établies ;

b) affecter des noms d'entrée ISO aux algorithmes cryptographiques enregistrés selon les besoins ;

c) mettre à jour et publier le registre lorsque cela est prescrit.

1) À publier.

2) Pour les besoins de la présente Norme internationale et conformément aux règles de désignation et d'opération des Autorités d'Enregistrement dans les procédures ISO/CEI JTC 1, les conseils de l'ISO et de la CEI ont désigné le «National Computer Centre, Oxford Road, Manchester, UK», pour servir d'Autorité d'Enregistrement.

5 Algorithmes à enregistrer

Les algorithmes cryptographiques à enregistrer sont ceux que l'on utilise dans les services de protection de l'information, comme défini dans l'annexe A.

Un algorithme enregistré peut être de l'un des types suivants :

a) Algorithmes dont la description du processus complète l'entrée de l'enregistrement ;

b) Algorithmes dont la description complète se trouve dans un document ISO, dans une norme maintenue par un comité membre de l'ISO ou par une organisation de liaison ;

c) Algorithmes dont la description est incomplète ou absente.

6 Procédures d'Enregistrement

6.1 La soumission de nouvelles entrées dans le registre ne peut venir ou être parrainée que par un comité membre, un comité technique ISO ou une organisation de liaison.

Le soumissionnaire a pour principale responsabilité de fournir des détails complets, compréhensibles et sans ambiguïté par rapport aux informations données en 7 (b à i) et éventuellement (j à m). Les propositions doivent être rejetées si elles ne se conforment pas à ces prescriptions.

Les propositions d'entrée du registre doivent se faire sous le format spécifié à l'article 9.

6.2 Lors de l'acceptation d'une soumission d'une nouvelle entrée au registre, l'Autorité d'Enregistrement affectera un nom d'entrée à l'algorithme.

6.3 Les soumissions de modification ou de suppression des entrées dans le registre existant peuvent venir d'un comité membre ou d'une organisation de liaison.

6.4 Lorsqu'une soumission concerne la modification ou la suppression d'une entrée enregistrée, elle doit être approuvée par l'ISO/CEI JTC 1 et par le soumissionnaire de l'entrée dans le registre.

7 Contenu général du registre

Pour chaque algorithme à enregistrer, l'Entrée du Registre devra contenir les détails suivants :

Obligatoires (a à i)

a) un nom formel d'entrée ISO pour l'algorithme ;

b) le (ou les) nom(s) privé(s) donné(s) à l'algorithme par son auteur ou par son propriétaire ;

c) le champ d'application prévu pour l'algorithme ;

d) les paramètres d'interface cryptographique ;

e) une série de mots tests pour vérifier la fonctionnalité de base ;

f) l'identité de l'organisation qui a demandé l'enregistrement de l'algorithme ;

g) les dates de l'enregistrement et des modifications ;

h) s'il fait l'objet d'une norme nationale ;

i) les restrictions concernant les licences de brevets ;

Optionnels (j à m)

j) une liste de références à tous algorithmes associés ;

k) la description de l'algorithme ;

l) les modes opératoires ;

m) autres informations.

8 Publication des Entrées de Registre

8.1 L'Autorité d'Enregistrement doit

a) publier une fois par an une liste des entrées si des changements sont survenus ;

b) publier le registre complet sur demande ;

c) fournir des entrées individuelles du registre sur demande ;

d) notifier les changements à toutes les autorités de parrainage tous les trois mois.

Les entrées doivent être regroupées en trois parties, chaque partie étant classée conformément aux types d'algorithme enregistré donnés dans l'article 5.

8.2 La publication des entrées doit clairement indiquer que l'Autorité d'Enregistrement n'a pas évalué la qualité de protection offerte par l'algorithme enregistré ni porté de jugement sur celle-ci. Chaque entrée doit être étiquetée avec une déclaration indiquant que l'enregistrement de l'algorithme n'implique pas que l'algorithme est une norme ISO.

9 Formats des Entrées de Registre

Les en-têtes du présent article sont ceux qui doivent être utilisés dans l'Entrée du Registre. Le contenu de chaque article et de chaque paragraphe est défini dans le texte correspondant ci-dessous.

9.1 Nom d'Entrée ISO

Le format de ce paragraphe est un identificateur d'objet.

Les valeurs d'identificateur d'objet pour les noms d'entrée ISO doivent être composées en accord avec les règles générales pour la composition de noms non ambigus tels que définis dans l'ISO 9384-1. Ces valeurs d'identificateur d'objet doivent être de la forme { ISO standard 9979 algorithm-identifier (n) } où «algorithm-identifier» désigne une entrée spécifique dans le registre d'algorithme cryptographique au moyen de la valeur d'index «n».

9.2 Nom d'entrée privé

Ce paragraphe doit prescrire le (ou les) nom(s) privé(s) donné(s) à l'entrée du registre par son auteur ou son propriétaire. Exemple type

Data Encryption Standard (DES)

L'autorité de parrainage doit clarifier tout sujet relatif aux noms privés ou commerciaux avant de soumettre une nouvelle entrée dans le registre.

9.3 Domaine d'Application prévu

Ce paragraphe doit spécifier le domaine d'utilisation prévu de l'algorithme cryptographique identifié dans l'Entrée du Registre. Cela se fera généralement par référence à un ensemble commun de fonctions de sécurité ou à des transformations mathématiques associées. Exemples types

a) confidentialité ;

b) authentification ;

c) intégrité des données ;

d) signatures numériques ;

e) fonctions de condensation.

9.4 Paramètres d'Interface cryptographique

Ce paragraphe doit spécifier les paramètres nécessaires à l'utilisation de l'algorithme cryptographique.

Exemples courants de paramètres

a) taille d'entrée ;

b) taille de sortie ;

c) longueur de clé ;

d) taille de la valeur d'initialisation ;

e) mode de chiffrement ou de déchiffrement.

9.5 Mots tests

Ce paragraphe spécifie les mots tests et toute procédure nécessaire pour vérifier la fonctionnalité de la mise en œuvre de l'algorithme cryptographique. Le soumissionnaire a la responsabilité de garantir que les essais et les procédures nécessaires suffisent pour valider la fonctionnalité de base.

NOTE — Ces mots tests sont prévus uniquement pour garantir qu'une mise en œuvre de l'algorithme fonctionne. Les mots tests ne sont pas prévus pour démontrer la fonctionnalité totale de l'algorithme ni sa conformité exacte à toute description mathématique dont on pourrait disposer.

9.6 Nom de l'Autorité de Parrainage

Ce paragraphe doit comporter le nom du comité membre ou de l'organisation de liaison ISO de parrainage qui a soumis l'entrée de registre, ainsi qu'un point de contact pour les questions et commentaires.

9.7 Dates de l'enregistrement et des modifications

Ce paragraphe doit comporter les dates auxquelles l'enregistrement a été ajouté et modifié par l'Autorité d'Enregistrement.

9.8 Algorithme faisant l'objet d'une norme nationale

Ce paragraphe doit comporter l'information indiquant si l'algorithme cryptographique fait ou non l'objet d'une (de) norme(s) nationale(s) et si oui, laquelle (lesquelles).

9.9 Restrictions sur les Licences de Brevets

Ce paragraphe doit indiquer toute restriction connue sur les licences de brevets concernant l'algorithme cryptographique et/ou sa mise en œuvre.

9.10 Références

Ce paragraphe peut être utilisé pour contenir, sous la forme requise par les Directives ISO, une liste de tous les documents référencés dans cette Entrée de Registre. Il s'agit généralement de Normes internationales ISO ou de recommandations du CCITT, mais cela peut être d'autres éléments couverts par les Directives ISO, y compris des normes nationales.

9.11 Description de l'algorithme

Ce paragraphe décrit l'algorithme.

9.12 Modes opératoires

Ce paragraphe doit prescrire un ensemble de modes opératoires applicables.

Exemples

a) Dictionnaire Électronique ;

b) Rebouclage du Cryptogramme ;

c) Chaînage de Bloc Chiffré ;

d) Rebouclage de Sortie ;

e) Chiffrement de Flux par addition ;

f) Boîte Noire.

9.13 Autres informations

Ce paragraphe peut contenir toute autre information pertinente non donnée ci-dessus. Exemples types

a) règles de conception ;

b) sa puissance cryptographique (ou toute analyse associée) ;

c) tout jugement de son aptitude aux applications ou aux systèmes spécifiques ;

d) caractéristiques de transmission ;

e) conseils sur le choix des clés.

Annexe A
(normative)

Définition d'un algorithme cryptographique

A.1 Introduction

La présente annexe définit un algorithme cryptographique pour les besoins de l'enregistrement.

A.2 Définition

Un algorithme cryptographique est défini comme un algorithme qui transforme des données pour cacher ou révéler le contenu de leurs informations et qui utilise au moins un paramètre secret. Ceci est expliqué en figure A.1.

Cette définition inclut les algorithmes symétriques (par exemple DES et FEAL) et les algorithmes asymétriques (par exemple RSA et RABIN). Dans le cas d'algorithme symétrique les données sont cachées et revélées en utilisant un paramètre secret. Dans le cas d'un algorithme asymétrique les données sont cachées en utilisant un paramètre public et revélées en utilisant un paramètre secret.

A.3 Figure A.1

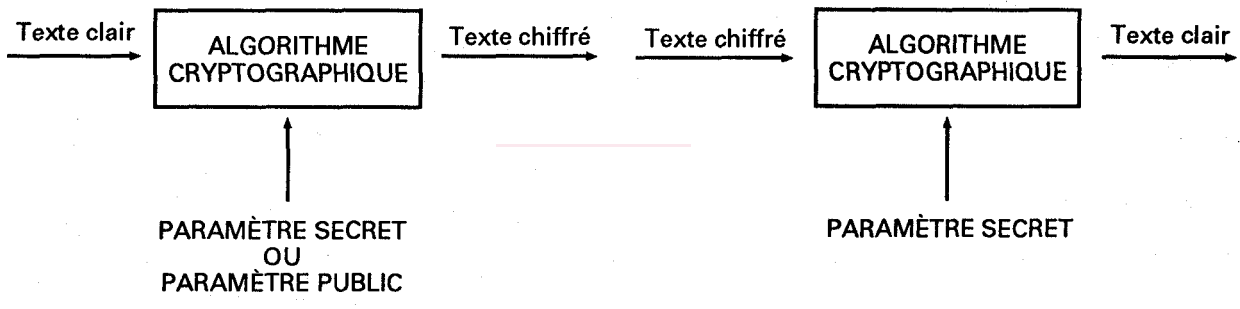

Figure A.1

Annexe B
(informative)

Modes Opératoires

B.1 Introduction

La présente annexe définit un identificateur unique, conformément à l'ISO 8825, pour les modes opératoires usuels actuellement définis.

B.2 Modes opératoires usuels

Les modes opératoires usuels sont

Dictionnaire Électronique
Rebouclage du Cryptogramme
Chaînage de Bloc Chiffrés
Rebouclage de Sortie
Chiffrement de Flux par addition

B.3 Identificateurs uniques

```
ISOModesofOperation {iso registration authority cryptographic-algorithms(7) Modules(0)
                     Modes-of-Operation(0)}

DEFINITIONS ::=
BEGIN

EXPORTS EVERYTHING

ID ::= OBJECT IDENTIFIER

id-iso-cryptographic-algorithm-entry-name ID ::= {iso standard 9979 algorithm-identifier (n)}

-- catégories

id-mod ID ::= {id-iso-cryptographic-algorithms 0} -- modules
id-MOP ID ::= {is-iso-cryptographic-algorithms 1} -- modes opératoires

-- Modules

id-mod-modes-of-operation ID ::= {id-mod 0}

-- Modes opératoires

id-MOP-electronic-code-book    ID ::= {id-MOP 0}
id-MOP-cipher-feedback         ID ::= {is-MOP 1}
id-MOP-cipher-block-chaining   ID ::= {id-MOP 2}
id-MOP-output-feedback         ID ::= {id-MOP 3}
id-MOP-additive-stream-cipher  ID ::= {id-MOP 4}

END - - of ISOModesOfOperation
```