NORME INTERNATIONALE

ISO/IEC 19790

Deuxième édition
2012-08-15

Version corrigée
2015-11

Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques

Information technology — Security techniques — Security requirements for cryptographic modules

Numéro de référence
ISO/IEC 19790:2012(F)

© ISO/IEC 2012



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2012

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vii**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **1**

4 Abréviations **15**

5 Niveaux de sécurité des modules cryptographiques **15**
5.1 Niveau de sécurité 1 15
5.2 Niveau de sécurité 2 16
5.3 Niveau de sécurité 3 16
5.4 Niveau de sécurité 4 17

6 Objectifs de sécurité fonctionnelle **17**

7 Exigences de sécurité **18**
7.1 Généralités 18
7.2 Spécification du module cryptographique 20
7.2.1 Exigences générales relatives à la spécification du module cryptographique 20
7.2.2 Types de modules cryptographiques 20
7.2.3 Frontière cryptographique 21
7.2.4 Modes de fonctionnement 22
7.3 Interfaces du module cryptographique 23
7.3.1 Exigences générales relatives aux interfaces du module cryptographique 23
7.3.2 Types d'interfaces 24
7.3.3 Définition des interfaces 24
7.3.4 Canal de confiance 25
7.4 Rôles, services et authentification 25
7.4.1 Exigences générales en matière de rôles, de services et d'authentification 25
7.4.2 Rôles 26
7.4.3 Services 26
7.4.4 Authentification 28
7.5 Sécurité logicielle/micrologicielle 30
7.6 Environnement opérationnel 32
7.6.1 Exigences générales relatives à l'environnement opérationnel 32
7.6.2 Exigences relatives au système d'exploitation pour les environnements opérationnels limités ou non modifiables 33
7.6.3 Exigences relatives au système d'exploitation pour les environnements opérationnels modifiables 34
7.7 Sécurité physique 36
7.7.1 Matérialisations de la sécurité physique 36
7.7.2 Exigences générales en matière de sécurité physique 38
7.7.3 Exigences de sécurité physique pour chaque matérialisation de sécurité physique 40
7.7.4 Protection contre les défaillances environnementales/essais de défaillance environnementale 42
7.8 Sécurité non invasive 44
7.9 Gestion des paramètres de sécurité sensibles 44
7.9.1 Exigences générales relatives à la gestion des paramètres de sécurité sensibles 44
7.9.2 Générateurs de bits aléatoires 45
7.9.3 Génération de paramètres de sécurité sensibles 45
7.9.4 Établissement de paramètres de sécurité sensibles 45
7.9.5 Entrée et sortie de paramètres de sécurité sensibles 45
7.9.6 Stockage des paramètres de sécurité sensibles 46
7.9.7 Abrogation des paramètres de sécurité sensibles 46

© ISO/IEC 2012 – Tous droits réservés

7.10 Auto-tests 47
7.10.1 Exigences générales relatives aux auto-tests 47
7.10.2 Auto-tests pré-opérationnels 48
7.10.3 Auto-tests conditionnels 49
7.11 Assurance du cycle de vie 51
7.11.1 Exigences générales relatives à l'assurance du cycle de vie 51
7.11.2 Gestion de la configuration 51
7.11.3 Conception 52
7.11.4 Modèle à état fini 52
7.11.5 Développement 53
7.11.6 Essais fournisseur 54
7.11.7 Livraison et fonctionnement 55
7.11.8 Fin de vie 55
7.11.9 Guides (d'orientation) 55
7.12 Atténuation des autres attaques 56
Annexe A (normative) **Exigences relatives à la documentation** **57**
Annexe B (normative) **Politique de sécurité du module cryptographique** **63**
Annexe C (normative) **Fonctions de sécurité approuvées** **68**
Annexe D (normative) **Méthodes approuvées de génération et d'établissement de paramètres de sécurité sensibles** **70**
Annexe E (normative) **Mécanismes d'authentification approuvés** **71**
Annexe F (normative) **Mesures d'essai d'atténuation des attaques non invasives approuvées** **72**
Bibliographie **73**

 © ISO/IEC 2012 – Tous droits réservés

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos - Informations supplémentaires.

Le Rectificatif technique 1 de l'ISO/IEC 19790:2012 a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, Sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

La présente version corrigée du Rectificatif technique 1 de l'ISO/IEC 19790:2012 annule et remplace la première édition (ISO/IEC 19790:2012/Cor 1:2015), et intègre les mêmes révisions techniques et corrections rédactionnelles diverses présentées en texte **rouge** au lieu d'un soulignage noir:

— 3.21: le terme « frontière cryptographique » est corrigé;

— 3.80: le terme « non relatif à la sécurité » est corrigé;

— 3.108: le terme « auto-test » est corrigé;

— 7.2.2: les exigences **[02.04]**, **[02.05]** et **[02.06]** sont corrigées;

— 7.2.4.3: l'exigence **[02.31]** est corrigée;

— 7.3.3: l'exigence **[03.14]** est corrigée;

— 7.5: les exigences **[05.06]** et **[05.07]** sont ajoutées. Les exigences **[05.08]**, **[05.13]** et **[05.17]** à **[05.23]** sont corrigées;

— 7.6.3: l'exigence **[06.06]** est corrigée;

— 7.8: l'exigence **[08.04]** est corrigée;

— 7.9.1: l'exigence **[09.04]** est corrigée;

© ISO/IEC 2012 – Tous droits réservés

— 7.9.7: l'exigence **[09.37]** est corrigée;

— 7.10.2.2: l'exigence **[10.17]** est corrigée;

— 7.11.5: l'exigence **[11.26]** est corrigée;

— 7.11.7: l'exigence **[11.35]** est corrigée;

— 7.11.9: l'exigence **[11.38]** est corrigée;

— A.2.5: les exigences des 1re et 2e puces sont corrigées;

— A.2.7: l'exigence de la 3e puce est corrigée;

— A.2.10: l'exigence de la 4e puce est corrigée;

— B.2.4: l'exigence de la 9e puce est corrigée;

— B.2.5: l'exigence de la 1re puce est corrigée;

— B.2.7: l'exigence du 2e niveau de la 6e puce est corrigée;

— D.1: le texte en double a été supprimé;

— D.1.2: la référence à l'ISO/IEC 15946-3 a été supprimée;

— E.1: le texte en double a été supprimé; et

— F.1: le texte en double a été supprimé.

© ISO/IEC 2012 – Tous droits réservés

Introduction

Dans le domaine des technologies de l'information, il est de plus en plus nécessaire d'utiliser des mécanismes cryptographiques tels que la protection des données contre la manipulation ou la divulgation non autorisées, pour l'authentification d'entité et pour la non-répudiation. La sécurité et la fiabilité de ces mécanismes dépendent directement des modules cryptographiques dans lesquels ils sont mis en œuvre.

La présente Norme internationale prévoit quatre niveaux qualitatifs croissants d'exigences de sécurité destinés à couvrir un large éventail d'applications et d'environnements potentiels. Les techniques cryptographiques sont identiques dans les quatre niveaux de sécurité. Les exigences de sécurité couvrent des domaines relatifs à la conception et à la mise en œuvre d'un module cryptographique. Ces domaines incluent la spécification du module cryptographique; les interfaces du module cryptographique; les rôles, les services et l'authentification; la sécurité logicielle/micrologicielle; l'environnement opérationnel; la sécurité physique; la sécurité non invasive; la gestion des paramètres de sécurité sensibles; les auto-tests; l'assurance du cycle de vie; et l'atténuation des autres attaques.

La classification globale de sécurité d'un module cryptographique doit être choisie de façon à fournir un niveau de sécurité approprié pour les exigences de sécurité de l'application et de l'environnement dans lequel le module est appelé à être utilisé et pour les services de sécurité que le module est appelé à fournir. Il convient que l'autorité responsable de chaque organisation s'assure que ses systèmes informatiques et de télécommunications qui utilisent des modules cryptographiques offrent un niveau de sécurité acceptable pour l'application et l'environnement concernés. Étant donné qu'il incombe à chaque autorité de choisir quelles fonctions de sécurité approuvées sont appropriées pour une application donnée, la conformité à la présente Norme internationale n'implique ni une interopérabilité complète ni une acceptation mutuelle des produits conformes. Il convient de sensibiliser toutes les personnes concernées à l'importance de la sécurité et de la nécessité de faire de la sécurité de l'information une priorité en matière de gestion.

Les exigences en matière de sécurité de l'information varient en fonction des applications; il convient que les organisations identifient leurs ressources d'information et déterminent la sensibilité aux pertes et leur impact potentiel en mettant en œuvre des mesures de sécurité appropriées. Les mesures de sécurité incluent, sans s'y limiter:

— mesures de sécurité physiques et environnementales;

— contrôles d’accès;

— développement logiciel;

— plans de sauvegarde et de secours; et

— mesures de sécurité des informations et des données.

Ces mesures de sécurité ne sont efficaces que sous réserve de mise en place de procédures et de politiques de sécurité appropriées dans l'environnement opérationnel.

© ISO/IEC 2012 – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques

1 Domaine d'application

La présente Norme internationale spécifie les exigences de sécurité pour un module cryptographique utilisé dans un système de sécurité qui protège les informations sensibles contenues dans les systèmes informatiques et de télécommunications. La présente Norme internationale définit quatre niveaux de sécurité pour les modules cryptographiques afin de couvrir un large éventail de sensibilités des données (par exemple: données administratives de faible valeur, virements bancaires de plusieurs millions de dollars, données qui protègent la vie, informations d'identité personnelles et informations sensibles utilisées par le gouvernement) et une variété d'environnements d'application (par exemple: des installations gardées, un bureau, des supports amovibles, et un emplacement totalement non protégé). La présente Norme internationale spécifie quatre niveaux de sécurité pour chacun des 11 domaines d'exigences, chaque niveau de sécurité offrant une augmentation de la sécurité par rapport au niveau précédent.

La présente Norme internationale spécifie les exigences de sécurité destinées à maintenir à jour la sécurité assurée par un module cryptographique. La conformité à la présente Norme internationale n'est pas suffisante pour garantir qu'un module donné est sûr ou que la sécurité offerte par le module est suffisante et acceptable pour le propriétaire des informations qui sont protégées.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

Les documents cités dans les Annexes C, D, E et F de l'ISO/IEC 19790 *Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques*

3 Termes et définitions

Pour les besoins de la présente Norme internationale, les termes et définitions suivants s'appliquent.

3.1
liste de contrôle d'accès
ACL
liste des permissions autorisant l'accès à un objet

3.2
recommandations administrateur
contenu écrit qui est utilisé par le Responsable cryptographie et/ou d'autres rôles administratifs pour la configuration, la maintenance et l'administration correctes du module cryptographique

3.3
automatisé
sans entrée ou intervention manuelle (par exemple: via des moyens électroniques, tels qu'un réseau informatique)

© ISO/IEC 2012 – Tous droits réservés

3.4
autorité d'agrément
toute organisation/autorité nationale ou internationale habilitée à approuver et/ou évaluer des fonctions de sécurité

Note 1 à l'article: Une autorité d'agrément dans le contexte de la présente définition évalue et approuve des fonctions de sécurité sur la base de leurs mérites cryptographiques ou mathématiques, mais n'est pas l'entité d'essai qui effectuerait des essais afin d'évaluer la conformité à la présente Norme internationale.

3.5
technique d'authentification des données approuvée
méthode approuvée qui peut inclure l'utilisation d'une signature numérique, d'un code d'authentification de message ou d'un hachage par clé (par exemple: HMAC)

3.6
technique d'intégrité approuvée
hachage, code d'authentification de message ou algorithme de signature numérique approuvé

3.7
mode de fonctionnement approuvé
ensemble de services qui inclut au moins un service qui utilise un processus ou une fonction de sécurité approuvé(e) et qui peut inclure des services non relatifs à la sécurité

Note 1 à l'article: À ne pas confondre avec un mode spécifique d'une fonction de sécurité approuvée, par exemple: mode CBC (Enchaînement de blocs de chiffrement)

Note 2 à l'article: Les processus ou fonctions de sécurité non approuvés sont exclus.

3.8
fonction de sécurité approuvée
fonction de sécurité (par exemple: algorithme cryptographique) qui est référencée à l'Annexe C

3.9
technique cryptographique asymétrique
technique cryptographique qui utilise deux transformations liées; une transformation publique (définie par la clé publique) et une transformation privée (définie par la clé privée)

Note 1 à l'article: Les deux transformations ont pour propriété que, étant donnée la transformation publique, il est impossible de dériver par calcul la transformation privée dans un temps limité donné et avec des ressources de calcul données.

3.10
biométrique
caractéristique physique ou trait comportemental personnel mesurable utilisé(e) pour reconnaître l'identité, ou pour vérifier l'identité déclarée d'un opérateur

3.11
capacité de contournement
capacité d'un service à contourner, en tout ou partie, une fonction cryptographique

3.12
certificat
données d'une entité rendues infalsifiables à l'aide de la clé privée ou secrète d'une autorité de certification

Note 1 à l'article: À ne pas confondre avec un certificat de validation de module délivré par une autorité de validation

3.13
compromission
divulgation, modification, substitution ou utilisation non autorisée de paramètres de sécurité critiques ou modification ou substitution non autorisée de paramètres de sécurité publics

© ISO/IEC 2012 – Tous droits réservés

3.14
auto-test conditionnel
test effectué par un module cryptographique lorsque les conditions spécifiées pour le test sont réunies

3.15
confidentialité
propriété selon laquelle l'information n'est ni mise à disposition ni divulguée aux entités non autorisées

3.16
système de gestion de configuration
CMS
gestion des assurances et fonctionnalités de sécurité par le biais du contrôle des modifications apportées aux matériels, aux logiciels et à la documentation d'un module cryptographique

3.17
informations de contrôle
informations qui sont entrées dans un module cryptographique aux fins de pilotage du fonctionnement du module

3.18
paramètre de sécurité critique
CSP
informations relatives à la sécurité dont la divulgation ou la modification peut compromettre la sécurité d'un module cryptographique

EXEMPLE Clés cryptographiques secrètes et privées, données d'authentification telles que les mots de passe, les PIN, les certificats ou autres ancres de confiance

Note 1 à l'article: Un CSP peut être en clair ou chiffré.

3.19
responsable cryptographie
rôle endossé par une personne ou un processus (c'est-à-dire un sujet) agissant pour le compte d'une personne et qui accède à un module cryptographique afin d'exécuter les fonctions de gestion ou d'initialisation cryptographique d'un module cryptographique

3.20
algorithme cryptographique
procédure de calcul bien définie qui prend des entrées variables, qui peuvent inclure des clés cryptographiques, et qui produit une sortie

3.21
frontière cryptographique
périmètre clairement défini qui établit la frontière de tous les composants (c'est-à-dire l'ensemble de composants matériels, logiciels ou micrologiciels) du module cryptographique

3.22
fonction de hachage cryptographique
fonction efficace en termes de calcul qui relie des chaines de bits d'une longueur arbitraire à des chaines de bits de longueur fixe, de sorte qu'il est impossible de trouver, par calcul, deux valeurs distinctes qui hachent en une valeur commune

3.23
clé cryptographique
clé
suite de symboles qui commande le fonctionnement d'une transformation cryptographique

EXEMPLE Une transformation cryptographique peut inclure, sans s'y limiter, le chiffrement, le déchiffrement, le calcul de fonction de vérification cryptographique, la génération de signatures ou la vérification de signatures.

© ISO/IEC 2012 – Tous droits réservés

3.24
composant de clé cryptographique
composant de clé
paramètre utilisé conjointement avec d'autres composants de clé dans une fonction de sécurité approuvée afin de former un CSP en clair ou d'effectuer une fonction cryptographique

3.25
module cryptographique
module
ensemble des matériels, de logiciels et/ou de micrologiciels qui mettent en œuvre des fonctions de sécurité et qui sont contenus à l'intérieur de la frontière cryptographique

3.26
politique de sécurité du module cryptographique
politique de sécurité
spécification précise des règles de sécurité sur la base desquelles un module cryptographique doit fonctionner, y compris les règles dérivées des exigences de la présente Norme internationale et les règles supplémentaires imposées par le module ou l'autorité de validation

Note 1 à l'article: Voir l'Annexe B.

3.27
trajet de données
itinéraire physique ou logique emprunté par les données

Note 1 à l'article: Un trajet de données physique peut être partagé par plusieurs trajets de données logiques.

3.28
fonctionnement dégradé
fonctionnement dans lequel un sous-ensemble de l'ensemble complet d'algorithmes, de fonctions, de services ou de processus de sécurité est disponible et/ou configurable en raison d'une reconfiguration à partir d'un état d'erreur

3.29
analyse différentielle de la consommation
DPA
analyse des variations de la consommation électrique d'un module cryptographique, aux fins d'extraction d'informations liées à l'opération cryptographique

3.30
signature numérique
données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver l'origine et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)

3.31
saisie directe
saisie d'un SSP ou d'un composant de clé dans un module cryptographique, à l'aide d'un dispositif tel qu'un clavier

3.32
signature disjointe
une ou plusieurs signatures qui, ensemble, représentent un ensemble de code complet

3.33
émanations électromagnétiques
EME
signal porteur de renseignements qui, s'il est intercepté et analysé, divulgue potentiellement les informations qui sont transmises, reçues, manipulées ou autrement traitées par tout matériel de traitement de l'information

© ISO/IEC 2012 – Tous droits réservés

3.34
saisie électronique
saisie de SSP ou de composants de clé dans un module cryptographique à l'aide de méthodes électroniques

Note 1 à l'article: L'opérateur de la clé peut n'avoir aucune connaissance de la valeur de la clé saisie.

3.35
signature englobante
signature unique pour un ensemble de code complet

3.36
clé chiffrée
clé cryptographique qui a été chiffrée à l'aide d'une fonction de sécurité approuvée avec une clé de chiffrement de clé. Considérée comme protégée

3.37
entité
personne, groupe, dispositif ou processus

3.38
entropie
mesure du désordre, du caractère aléatoire ou de la variabilité d'un système fermé

Note 1 à l'article: L'entropie d'une variable aléatoire *X* est une mesure mathématique de la quantité d'informations fournies par une observation de *X*.

3.39
protection contre les défaillances environnementales
EFP
utilisation de fonctions destinées à protéger contre une compromission de la sécurité d'un module cryptographique due à des conditions environnementales situées en dehors de la plage de fonctionnement normale du module

3.40
essai de défaillance environnementale
EFT
utilisation de méthodes spécifiques dans le but de fournir une assurance raisonnable que la sécurité d'un module cryptographique ne sera pas compromise par des conditions environnementales situées en dehors de la plage de fonctionnement normale du module

3.41
code détecteur d'erreurs
EDC
valeur calculée à partir de données et composée d'informations redondantes conçue pour détecter, sans les corriger, les modifications involontaires des données

3.42
forme exécutable
forme du code dans laquelle le logiciel ou le micrologiciel est intégralement géré et contrôlé par l'environnement opérationnel du module et qui ne nécessite pas de compilation (par exemple: pas de code source, de code objet ou de code compilé à la volée)

3.43
déclenchement de fautes
technique destiné à provoquer des changements de comportement de fonctionnement du matériel par l'application de tensions transitoires, d'un rayonnement, de laser ou de techniques de décalage d'horloge

© ISO/IEC 2012 – Tous droits réservés

3.44
modèle à état fini
FSM
modèle mathématique d'une machine séquentielle composé d'un ensemble fini d'événements d'entrée, d'un ensemble fini d'événements de sortie, d'un ensemble fini d'états, d'une fonction qui relie les états et les entrées aux sorties, d'une fonction qui relie les états et les entrées aux états (une fonction de transition d'état) et d'une spécification qui décrit l'état initial

3.45
micrologiciel
code exécutable d'un module cryptographique qui est stocké dans le matériel à l'intérieur de la frontière cryptographique et qui ne peut pas être enregistré ou modifié de façon dynamique pendant l'exécution au sein d'un environnement opérationnel non modifiable ou limité

EXEMPLE Le matériel de stockage peut comprendre, sans s'y limiter, les PROM, EEPROM, FLASH, mémoire à semi-conducteurs, disques durs, etc.

3.46
module micrologiciel
module exclusivement composé de micrologiciels

3.47
spécification fonctionnelle
description de haut niveau des ports et des interfaces visibles par l'opérateur et description de haut niveau du comportement du module cryptographique

3.48
essai fonctionnel
essai de la fonctionnalité du module cryptographique telle que définie par la spécification fonctionnelle

3.49
dur/dureté
résistance relative d'un métal ou d'un autre matériau à l'enfoncement, aux rayures ou à la flexion; renforcé physiquement; robuste et résistant

Note 1 à l'article: Les résistances relatives du matériau destiné à être pénétré par un autre objet.

3.50
matériel
équipements/composants physiques situés dans la frontière cryptographique et utilisés pour traiter les programmes et les données

3.51
module matériel
module principalement composé de matériels, qui peut également contenir un micrologiciel

3.52
interface de module matériel
HMI
ensemble complet de commandes utilisées pour demander les services du module matériel, y compris les paramètres qui pénètrent dans la frontière cryptographique du module ou qui la quittent dans le cadre du service demandé

3.53
valeur de hachage
sortie d'une fonction de hachage cryptographique

3.54
module hybride
module dont la frontière cryptographique délimite la combinaison d'un composant logiciel ou micrologiciel et d'un composant matériel disjoint

 © ISO/IEC 2012 – Tous droits réservés

3.55
interface de module micrologiciel hybride
HFMI
ensemble complet de commandes utilisées pour demander les services du module micrologiciel hybride, y compris les paramètres qui pénètrent dans la frontière cryptographique du module ou qui la quittent dans le cadre du service demandé

3.56
interface de module logiciel hybride
HSMI
ensemble complet de commandes utilisées pour demander les services du module logiciel hybride, y compris les paramètres qui pénètrent dans la frontière cryptographique du module ou qui la quittent dans le cadre du service demandé

3.57
données d'entrée
informations qui sont entrées dans un module cryptographique et qui peuvent être utilisées aux fins de transformation ou de calcul à l'aide d'une fonction de sécurité approuvée

3.58
intégrité
propriété assurant que des données n'ont pas été modifiées ou supprimées de façon non autorisée ou non détectée

3.59
interface
entrée logique ou point de sortie d'un module cryptographique qui fournit un accès au module pour les flux d'informations logiques

3.60
adoptée par l'ISO/IEC
fonction de sécurité qui est:

— spécifiée dans une norme ISO/IEC; ou

— adoptée/recommandée dans une norme ISO/IEC et spécifiée soit dans une annexe de la norme ISO/IEC, soit dans un document référencé par la norme ISO/IEC

3.61
accord sur une clé
procédure d'établissement d'un SSP dans laquelle la clé obtenue est une fonction des informations fournies par deux participants ou plus, de sorte qu'aucune partie ne peut prédéterminer la valeur de la clé indépendamment de la contribution de l'autre partie en utilisant des méthodes automatisées

3.62
clé de chiffrement de clé
KEK
clé cryptographique qui est utilisée pour le chiffrement ou le déchiffrement d'autres clés

3.63
chargeur de clé
dispositif autonome capable de stocker au moins un SSP ou un composant de clé en clair ou chiffré qui peut être transféré, sur demande, dans un module cryptographique

Note 1 à l'article: L'utilisation d'un chargeur de clé nécessite une intervention humaine.

3.64
gestion de clés
administration et utilisation de la génération, de l'enregistrement, de la certification, de l'annulation d'enregistrement, de la distribution, de l'installation, du stockage, de l'archivage, de la révocation, de la dérivation et de la destruction d'éléments de mise à la clé conformément à une politique de sécurité

© ISO/IEC 2012 – Tous droits réservés

3.65
transport de clé
processus de transfert d'une clé depuis une entité vers une autre entité à l'aide de méthodes automatisées

3.66
environnement opérationnel limité
environnement opérationnel qui est conçu pour accepter uniquement des modifications de micrologiciel contrôlées qui réussissent l'essai de chargement de logiciel/micrologiciel

3.67
essai de bas niveau
essai des composants individuels ou de groupes de composants du module cryptographique et de leurs ports physiques et interfaces logiques

3.68
rôle de maintenance
rôle assumé dans le but d'effectuer une maintenance physique et/ou des services de maintenance logique

EXEMPLE Les services de maintenance peuvent inclure, sans s'y limiter, les diagnostics matériels et/ou logiciels.

3.69
manuel
nécessitant une intervention par un opérateur humain

3.70
code d'authentification de message
MAC
somme de contrôle cryptographique sur les données qui utilise une clé symétrique pour détecter les modifications tant accidentelles qu'intentionnelles des données

EXEMPLE Un code d'authentification de message fondé sur un hachage

3.71
microcode
instructions de processeur qui correspondent à une instruction de programme exécutable

EXEMPLE Code assembleur

3.72
entropie minimale
limite inférieure de l'entropie qui est utile pour la détermination d'une estimation la plus défavorable d'un échantillon d'entropie

3.73
environnement opérationnel modifiable
environnement opérationnel conçu pour accepter les modifications fonctionnelles qui peuvent contenir des logiciels non contrôlés (c'est-à-dire non fiables)

3.74
authentification multifactorielle
authentification réalisée avec au moins deux facteurs d'identification indépendants

Note 1 à l'article: Un facteur d'authentification est une information et un processus utilisés pour authentifier ou vérifier l'identité d'une entité.

Note 2 à l'article: Les catégories de facteurs d'authentification indépendants sont: quelque chose que vous connaissez, quelque chose que vous possédez et quelque chose que vous êtes.

© ISO/IEC 2012 – Tous droits réservés

3.75
module cryptographique intégré multipuce
matérialisation physique dans laquelle deux puces de circuit intégré ou plus sont reliées entre elles et sont intégrées dans un boîtier ou un produit qui peut ne pas être protégé physiquement

EXEMPLE Adaptateurs et cartes d'extension

3.76
module cryptographique autonome multipuce
matérialisation physique dans laquelle deux puces de circuit intégré ou plus sont reliées entre elles et où tout le boîtier est protégé physiquement

EXEMPLE Routeurs de chiffrement ou radios sécurisées

3.77
recommandations non destinées à l'administrateur
contenu écrit utilisé par l'utilisateur et/ou d'autres rôles non administratifs pour faire fonctionner le module cryptographique dans un mode de fonctionnement approuvé

Note 1 à l'article: Les recommandations non destinées à l'administrateur décrivent les fonctions de sécurité du module cryptographique et contiennent des informations et des procédures qui permettent l'utilisation sécurisée du module cryptographique, y compris des instructions, des lignes directrices et des avertissements.

3.78
attaque non invasive
Note 1 à l'article: attaque qui peut être effectuée sur un module cryptographique sans contact physique direct avec les composants se trouvant à l'intérieur de la frontière cryptographique du module

Note 2 à l'article: Une attaque qui n'altère ou ne modifie pas l'état du module cryptographique.

3.79
environnement opérationnel non modifiable
environnement opérationnel qui est conçu pour ne pas accepter les modifications des micrologiciels

3.80
non relatif à la sécurité
mis en œuvre de façon à ne pas gêner ou compromettre le fonctionnement sécurisé approuvé du module cryptographique

3.81
fonctionnement normal
fonctionnement dans lequel l'ensemble complet d'algorithmes, de fonctions, de services ou de processus de sécurité est disponible et/ou configurable

3.82
opaque
que la lumière ne peut traverser (c'est-à-dire la lumière située dans le spectre visible possédant une longueur d'onde comprise entre 400 nm et 750 nm); ni transparent ni translucide dans le spectre visible

3.83
environnement opérationnel
ensemble des logiciels et matériels se composant d'un système d'exploitation et d'une plateforme matérielle requis pour permettre le fonctionnement en toute sécurité du module

3.84
état opérationnel
état dans lequel les services ou les fonctions peuvent être demandés par un opérateur et où les résultats de données sortent de l'interface de sortie de données du module cryptographique

© ISO/IEC 2012 – Tous droits réservés

3.85
opérateur
personne ou processus (sujet) intervenant au nom d'une autre personne, autorisé(e) à remplir un ou plusieurs rôles

3.86
données de sortie
informations ou résultats calculés produits par un module cryptographique

3.87
passivation
effet d'un processus réactif dans les jonctions, surfaces ou composants de semi-conducteurs et les circuits intégrés, conçu pour inclure des moyens de détection et de protection

EXEMPLE Verre de dioxyde de silicium ou au phosphore

Note 1 à l'article: La passivation peut modifier le comportement du circuit. Le matériau de passivation dépend de la technologie.

3.88
mot de passe
chaine de caractères utilisée pour authentifier une identité ou pour vérifier une autorisation d'accès

EXEMPLE Lettres, nombres et autres symboles

3.89
numéro d'identification personnel
PIN
code numérique utilisé pour authentifier une identité

3.90
protection physique
protection d'un module cryptographique, de CSP et de PSP à l'aide de moyens physiques

3.91
clé en clair
clé cryptographique non chiffrée ou clé cryptographique obscurcie à l'aide de méthodes non approuvées et qui est considérée comme non protégée

3.92
port
entrée physique/logique ou point de sortie d'un module cryptographique qui fournit un accès au module

3.93
auto-test pré-opérationnel
test effectué par un module cryptographique entre le moment où un module cryptographique est mis sous tension ou instancié (après avoir été mis hors tension, réinitialisé, redémarré, après démarrage à froid, coupure d'alimentation, etc.) et les transitions vers l'état opérationnel

3.94
clé privée
clé d'une paire de clés asymétriques d'une entité, qu'il convient que seule cette entité utilise

Note 1 à l'article: Dans le cas d'un système de signature asymétrique, la clé privée définit la transformation de signature. Dans le cas d'un système de chiffrement asymétrique, la clé privée définit la transformation de déchiffrement.

3.95
de qualité de production
produit, composant ou logiciel qui a été soumis à l'essai et jugé conforme aux spécifications opérationnelles

 © ISO/IEC 2012 – Tous droits réservés

3.96
clé publique
clé d'une paire de clés asymétriques d'une entité, qui peut être rendue publique

Note 1 à l'article: Dans le cas d'un système de signature asymétrique, la clé publique définit la transformation de vérification. Dans le cas d'un système de chiffrement asymétrique, la clé publique définit la transformation de chiffrement. Une clé qui est « connue publiquement » n'est pas nécessairement disponible à l'échelle mondiale. La clé peut n'être disponible qu'aux membres d'un groupe prédéfini.

Note 2 à l'article: Pour les besoins de la présente Norme internationale, les clés publiques ne sont pas considérées comme des CSP.

3.97
certificat de clé publique
informations de clé publique d'une entité signées par une autorité de certification appropriée et par conséquent rendues infalsifiables

3.98
algorithme de cryptographie asymétrique à clé publique
algorithme cryptographique qui utilise deux clés connexes, l'une publique, l'autre privée

Note 1 à l'article: Ces deux clés ont pour propriété qu'il est impossible de dériver, par calcul, la clé privée à partir de la clé publique.

3.99
paramètre de sécurité public
PSP
informations publiques relatives à la sécurité dont la modification peut compromettre la sécurité d'un module cryptographique

EXEMPLE Clés cryptographiques publiques, certificats de clé publique, certificats autosignés, ancres de confiance, mots de passe à usage unique associés à un compteur et une date et une heure conservées en interne

Note 1 à l'article: Un PSP est considéré comme étant protégé s'il ne peut pas être modifié ou si sa modification peut être établie par le module.

3.100
générateur de bits aléatoires
RBG
dispositif ou algorithme qui produit une suite de bits qui apparaît statistiquement indépendante et non biaisée

3.101
couvercle amovible
moyen physique qui permet un accès intentionnellement conçu pour être non destructif au contenu physique d'un module cryptographique

3.102
rôle
attribut de sécurité associé à un utilisateur, qui définit les droits d'accès de l'utilisateur ou restrictions aux services d'un module cryptographique

Note 1 à l'article: Un ou plusieurs service(s) peut (peuvent) être associé(s) à un rôle. Un rôle peut être associé à un ou plusieurs utilisateurs, et un utilisateur peut assumer un ou plusieurs rôles.

3.103
contrôle d'accès basé sur les rôles
RBAC
permissions accordées à un rôle et qui accordent l'accès à un objet

© ISO/IEC 2012 – Tous droits réservés

3.104
environnement d'exécution
état de machine virtuelle qui fournit des services logiciels aux processus ou programmes quand un ordinateur est en fonctionnement

Note 1 à l'article: Cela peut se rapporter au système d'exploitation en lui-même, ou aux logiciels qui s'exécutent en son sein. La principale finalité est d'accomplir l'objectif de programmation « indépendante de la plateforme ».

3.105
clé secrète
clé cryptographique, utilisée avec un algorithme cryptographique à clé secrète, qui est associée de façon unique à une ou plusieurs entités et qu'il convient de ne pas rendre publique

3.106
fonction de sécurité
algorithmes cryptographiques, ainsi que les modes de fonctionnement, tels que les chiffrements par blocs, les chiffrements en flot, les algorithmes de clés symétriques ou asymétriques, les codes d'authentification de message, les fonctions de hachage ou autres fonctions de sécurité, les générateurs de bits aléatoires, l'authentification d'entité et la génération et l'établissement de SSP, tous approuvés par l'ISO/IEC ou par une autorité d'agrément

Note 1 à l'article: Voir l'Annexe C.

3.107
clé de diversification
valeur secrète utilisée pour initialiser un générateur de bits aléatoires

3.108
auto-test
test pré-opérationnel ou conditionnel exécuté par le module cryptographique

3.109
données sensibles
données qui, du point de vue de l'utilisateur, nécessitent une protection

3.110
paramètres de sécurité sensibles
SSP
paramètres de sécurité critiques (CSP) et paramètres de sécurité publics (PSP)

3.111
service
toute opération et/ou fonction invoquée de façon externe par un opérateur et qui peut être effectuée par un module cryptographique

3.112
entrée de service
ensemble des données ou informations de contrôle utilisées par le module cryptographique qui initient ou obtiennent des opérations ou fonctions spécifiques

3.113
sortie de service
ensemble des données et des informations d'état qui découlent des opérations ou des fonctions initiées ou obtenues par l'entrée de service

3.114
analyse simple de la consommation
SPA
analyse directe (principalement visuelle) des schémas d'exécution des instructions (ou d'exécution d'instructions individuelles), en lien avec la consommation électrique d'un module cryptographique, aux fins d'extraction d'informations corrélées à une opération cryptographique

© ISO/IEC 2012 – Tous droits réservés

3.115
module cryptographique simple puce
matérialisation physique dans laquelle une unique puce de circuit intégré (IC) peut être utilisée comme dispositif autonome ou peut être intégrée dans un boîtier ou un produit qui peut ne pas être protégé physiquement

EXEMPLE Puces de circuit intégré (IC) uniques ou cartes à puce dotées d'une unique puce IC

3.116
logiciel
code exécutable d'un module cryptographique qui est stocké sur un support effaçable et qui peut être enregistré ou modifié de façon dynamique pendant l'exécution au sein d'un environnement opérationnel modifiable

EXEMPLE Les supports effaçables peuvent inclure, sans s'y limiter, les mémoires à semi-conducteurs, les disques durs, etc.

3.117
module logiciel
module exclusivement composé d'un logiciel

3.118
essai de chargement logiciel/micrologiciel
ensemble d'essais réalisés sur des logiciels ou des micrologiciels qui doivent les réussir pour pouvoir être exécutés par un module cryptographique

Note 1 à l'article: Non applicable si le logiciel ou le micrologiciel est un remplacement d'image complet et exécuté uniquement après un cycle de mise sous tension du module

3.119
interface de module logiciel/micrologiciel
SFMI
ensemble de commandes utilisées pour demander les services du module logiciel ou micrologiciel, y compris les paramètres qui pénètrent dans la frontière cryptographique du module ou qui la quittent dans le cadre du service demandé

3.120
connaissance répartie
processus par lequel une clé cryptographique est divisée en plusieurs composants de clé, qui ne partagent entre eux aucune connaissance de la clé d'origine, qui peuvent ultérieurement être entrés par des entités distinctes dans un module cryptographique, ou en sortir, et être assemblés afin de recréer la clé cryptographique d'origine

Note 1 à l'article: L'opération de combinaison peut nécessiter la totalité ou un sous-ensemble des composants.

3.121
établissement de SSP
processus de mise à disposition d'un SSP partagé à une ou plusieurs entités

Note 1 à l'article: L'établissement de SSP inclut l'accord de SSP, le transport de SSP et l'entrée ou la sortie de SSP.

3.122
informations d'état
informations qui sont sorties par un module cryptographique dans le but d'indiquer certaines caractéristiques opérationnelles ou états du module

3.123
fort(e)
qui n'est pas facile à vaincre, qui possède une force ou une puissance supérieure à la moyenne ou à ce qui est attendu, capable de résister à une attaque ou construit de façon solide

© ISO/IEC 2012 – Tous droits réservés

3.124
technique cryptographique symétrique
technique cryptographique qui utilise la même clé secrète pour les transformations de chiffrement et de déchiffrement

3.125
détection d'effraction
détermination automatique par un module cryptographique d'une tentative de compromission de la sécurité du module

3.126
preuve d'effraction
indication observable d'une tentative de compromission de la sécurité d'un module cryptographique

3.127
réponse aux effractions
action automatique entreprise par un module cryptographique en cas de détection d'une effraction

3.128
ancre de confiance
informations fiables, qui incluent un algorithme de clé publique, une valeur de clé publique, un nom d'émetteur et, facultativement, d'autres paramètres

EXEMPLE Les autres paramètres peuvent inclure, sans s'y limiter, une période de validité

Note 1 à l'article: Une ancre de confiance peut être fournie sous la forme d'un certificat autosigné.

3.129
canal de confiance
lien de communication fiable et sûr établi entre le module cryptographique et un expéditeur ou un destinataire afin de communiquer de façon sécurisée des CSP en clair non protégés, des composants de clé et des données d'authentification

Note 1 à l'article: Un canal de confiance protège contre l'interception, ainsi que la falsification physique ou logique par des opérateurs/entités, processus ou autres dispositifs indésirables, entre les ports d'entrée et de sortie définis du module et le long du lien de communication avec le terminal souhaité.

3.130
utilisateur
rôle endossé par une personne ou un processus (c'est-à-dire un sujet) agissant pour le compte d'une personne et qui accède à un module cryptographique afin d'obtenir des services cryptographiques

3.131
validé
assurance de conformité soumise à l'essai par une autorité de validation

3.132
autorité de validation
entité qui validera les résultats des essais de conformité à la présente Norme internationale

3.133
fournisseur
entité, groupe ou association qui soumet le module cryptographique en vue de son essai et de sa validation

Note 1 à l'article: Le fournisseur a accès à l'ensemble des documents et preuves de conception pertinents, qu'il ait conçu ou développé le module cryptographique ou non.

3.134
abrogation
méthode de destruction des données stockées et SSP non protégés destinée à empêcher leur récupération et leur réutilisation

 © ISO/IEC 2012 – Tous droits réservés