PROJET DE NORME INTERNATIONALE

ISO/IEC DIS 19790

ISO/IEC JTC **1**/SC **27**

Secrétariat: **DIN**

Début de vote:
2023-11-27

Vote clos le:
2024-02-19

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

Information technology — Security techniques — Security requirements for cryptographic modules

ICS: 35.030

Le présent document est distribué tel qu'il est parvenu du secrétariat du comité.

Numéro de référence
ISO/IEC DIS 19790:2023(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

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. 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 : www.iso.org/iso/foreword.html.

Le comité responsable de ce document est l'ISO/IEC JTC 1, *Technologies de l'information*, SC 27.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 19790:2012, Rectificatif technique 1) dont les articles, paragraphes, tableaux, figures et annexes ont fait l'objet d'une révision technique, incluant les modifications suivantes :

— Article 3, Termes et définitions — cet article a été complété et mis à jour afin d'intégrer les changements d'exigences de l'Article 7 ;

— Article 4, Abréviations — cet article a été complété et mis à jour afin d'intégrer les changements d'exigences de l'Article 7 ;

— Article 5, Niveaux de sécurité des modules cryptographiques — cet article a été complété et mis à jour afin d'intégrer les changements d'exigences de l'Article 7 ;

— Article 6, Objectifs de sécurité fonctionnelle — la formulation de cet article a été revue et modernisée ;

— Article 7, Exigences de sécurité — bien que la structure principale de cet article ait été conservée, certaines exigences ont été reformulées et réorganisées pour des raisons de clarté. De nouvelles exigences ont été ajoutées et les exigences redondantes ou inutiles ont été supprimées ;

— Annexe A — Exigences relatives à la documentation — cette annexe a été mise à jour afin d'intégrer les changements d'exigences de l'Article 7 ;

— Annexe B — Politique de sécurité du module cryptographique — cette annexe a été mise à jour afin d'intégrer les changements d'exigences de l'Article 7 ;

— Annexe C — Fonctions de sécurité approuvées — cette annexe a été restructurée et mise à jour en fonction des normes récemment publiées ;

— Annexe D — Fonctions de sécurité approuvées — cette annexe a été restructurée et mise à jour en fonction des normes récemment publiées ;

— Annexe E — Mécanismes d'authentification approuvés — cette annexe a été mise à jour en fonction des normes récemment publiées et des exemples de méthodes de limitation du débit ont été ajoutés ;

— Annexe F — Mesures d'essai d'atténuation des attaques non invasives approuvées — cette annexe a été mise à jour en intégrant l'ISO/IEC 1785 ;

— une nouvelle Annexe G relative au développement, à la fabrication et au fonctionnement sécurisés des modules, a été ajoutée.

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.

Le présent document 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 ou le niveau de sécurité dans chaque domaine d'un module cryptographique doit être choisi 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, ainsi que 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 au présent document 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 :

— les mesures de sécurité physiques et environnementales ;

— les contrôles d'accès ;

— le maintien de la sécurité des systèmes et la gestion des correctifs ;

— les plans de sauvegarde et de secours ; et

— les mesures de sécurité des informations et des données.

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

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

1 Domaine d'application

Le présent document spécifie les exigences de sécurité pour un module cryptographique utilisé dans un système de sécurité qui protège les informations sensibles dans les Technologies de l'information et de la communication (TIC). Le présent document définit quatre niveaux de sécurité pour les modules cryptographiques afin de couvrir un large éventail de sensibilités des données (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, par exemple) et une diversité d'environnements d'application (des installations gardées, un bureau, des supports amovibles et un emplacement totalement non protégé, par exemple). Le présent document spécifie jusqu'à 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 conformité au présent document n'est pas suffisante pour garantir qu'un module est sûr ou que la sécurité offerte par le module est suffisante et acceptable pour le propriétaire des informations qui sont protégées. Il est attendu que les propriétaires d'informations sensibles évaluent les risques pour leurs informations et déploient des modules cryptographiques dans le cadre de leur plan global d'atténuation des risques, afin d'atténuer les risques spécifiques identifiés. Les recommandations contenues dans la politique de sécurité des modules donnent un bref aperçu des forces et faiblesses des modules, et il est attendu qu'elles soient appliquées pour tout déploiement donné.

2 Références normatives

Les documents ci-après sont des références normatives indispensables à 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, F et G 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 du présent document, 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 d'administrateurs 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)

3.4
autorité d'approbation
organisation ou autorité capable d'évaluer et/ou d'approuver des fonctions de sécurité

NOTE Une autorité d'approbation 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 au présent document.

3.5
technique d'authentification des données approuvée
méthode approuvée donnant l'assurance que l'expéditeur des données est bel et bien celui qui est déclaré. Les techniques d'authentification des données approuvées peuvent inclure l'utilisation d'une signature numérique approuvée, d'un code d'authentification de message approuvé ou d'un hachage par clé approuvé (HMAC, par exemple). Des techniques d'authentification des données approuvées sont spécifiées dans l'Annexe C

3.6
technique d'intégrité approuvée
méthode approuvée pour vérifier si des données ont été ou non corrompues ou modifiées. Les techniques d'intégrité approuvées peuvent utiliser des clés et inclure l'utilisation d'un hachage approuvé, d'un code d'authentification de message ou d'un algorithme de signature numérique. Des techniques d'intégrité approuvées sont spécifiées dans l'Annexe C

3.7
processus approuvé
ensemble de fonctions interdépendantes qui comprend au moins une fonction de sécurité approuvée spécifiée à l'Annexe C, qui fait référence à l'Annexe D et à l'Annexe E, et peut inclure des fonctions non cryptographiques, ou des fonctions de sécurité non approuvées qui ne sont pas relatives à la sécurité du fonctionnement des processus

EXEMPLE Une transaction bancaire, un service de compression qui inclut un chiffrement, etc.

3.8
service approuvé
service comprenant au moins une fonction ou un processus de sécurité approuvé, et pouvant inclure des fonctions ou processus non relatifs à la sécurité

NOTE Les fonctions ou processus de sécurité relatifs à la sécurité mais non approuvés sont exclus des services approuvés.

3.9
fonction de sécurité approuvée
fonctions de sécurité qui sont référencées dans l'Annexe C, qui fait référence à l'Annexe D et à l'Annexe E

3.10
algorithme ou technique asymétrique
algorithme ou technique cryptographique référencé dans l'Annexe C, qui fait référence à l'Annexe D, et qui utilise deux transformations liées ; une transformation publique (définie par la clé publique) et une transformation privée (définie par la clé privée)

NOTE Les deux transformations ont pour propriété que, compte tenu de la transformation publique, il est impossible de trouver par calcul la transformation privée en un temps limité donné et avec des ressources de calcul données.

3.11
attestation
processus utilisé pour permettre à une entité située à l'extérieur de la frontière du module cryptographique de vérifier de manière sécurisée l'identité et d'autres caractéristiques physiques ou logiques du module cryptographique en utilisant un enregistrement d'attestation, et conformément aux normes et méthodes d'attestation énumérées à l'Annexe G

3.12
enregistrement d'attestation
enregistrement accessible et généré par un module cryptographique qui prend en compte le service d'attestation. L'enregistrement d'attestation contient les détails de mesure des composants logiciels, micrologiciels ou matériels dans le module cryptographique. Les mesures peuvent inclure des valeurs de hachage ou des copies de composants logiciels, micrologiciels ou matériels dans le module cryptographique, ainsi que des réglages de configuration, des informations d'état, des registres et des valeurs de fusibles

3.13
service d'attestation
service qu'un module cryptographique peut prendre en charge et nécessitant la prise en charge d'une identité et la génération d'enregistrements d'attestation par ce module

3.14
données d'authentification
données chargées dans le module par l'opérateur, servant à authentifier l'opérateur vis-à-vis du module. Les données d'authentification sont transitoires et considérées comme un CSP temporaire. Au cours d'une tentative d'authentification, les données d'authentification sont soumises au module sous forme :

— d'entrée de données effectuée par l'opérateur (mot de passe, PIN, clé cryptographique ou équivalent, par exemple) ; ou

— de résultat d'une méthode ou d'un processus impliquant des informations liées à l'opérateur (par exemple la signature d'un challenge avec une clé privée, l'insertion d'une clé physique, le traitement de données biométriques)

3.15
autorisé
lorsqu'un opérateur a le pouvoir d'endosser un rôle spécifique et d'exécuter un ensemble de services correspondant

3.16
biométrique
caractéristique physique ou trait comportemental personnel, mesurable, utilisé pour reconnaître l'identité ou vérifier l'identité déclarée d'un opérateur

3.17
flux binaire
série d'instructions analysées par le FPGA au démarrage pour configurer sa logique interne et considérée comme une forme de code exécutable fortement personnalisée

3.18
certificat
données d'une entité rendues infalsifiables à l'aide de la clé privée ou secrète d'une autorité de certification

NOTE À ne pas confondre avec un certificat de validation de module délivré par une autorité de validation.

3.19
compromission
divulgation, modification, substitution ou utilisation non autorisée de paramètres de sécurité critiques, modification ou substitution non autorisée de paramètres de sécurité publics, ou perte d'intégrité ou de disponibilité du module cryptographique lui-même, qui peut entraîner le contournement non prévu des fonctions de sécurité prises en charge par le module

3.20
auto-test conditionnel
test effectué par un module cryptographique lorsque les conditions spécifiées pour le test sont réunies

3.21
confidentiel
souhait de ne pas mettre à disposition l'information et de ne pas la divulguer aux entités non autorisées

3.22
gestion de configuration
processus appliquant le pilotage et la surveillance techniques et administratives pour : identifier et documenter les caractéristiques fonctionnelles et physiques d'un élément de configuration, contrôler les modifications apportées à ces caractéristiques, enregistrer et rendre compte du traitement des modifications et de leur état de mise en œuvre, et vérifier la conformité à des exigences spécifiques

[SOURCE : ISO/IEC/IEEE 24765:2010, 3.770 1]

3.23
système de gestion de configuration
CMS
ensemble de procédures et d'outils (y compris leur documentation) utilisés par un fournisseur pour développer et maintenir des configurations des modules tout au long de son cycle de vie

3.24
informations de contrôle
commandes, signaux (entrée/sortie d'horloge, par exemple) et données de contrôle (y compris les appels de fonctions et les données de commandes manuelles telles que celles provenant d'interrupteurs, de boutons et de claviers) utilisés pour piloter ou contrôler le fonctionnement d'un module cryptographique ou de composants séparés d'un module hybride

3.25
entrée de contrôle
informations de contrôle qui sont entrées dans un module cryptographique ou des composants séparés d'un module hybride

3.26
interface d'entrée de contrôle
interface(s) identifiée(s) par un fournisseur, par laquelle (lesquelles) toutes les informations de contrôle sont entrées dans le module cryptographique

3.27
sortie de contrôle
informations de contrôle qui sont issues d'un module cryptographique ou d'un composant séparé d'un module hybride pour être utilisées comme une entrée de contrôle dans un autre module cryptographique ou un composant séparé d'un module hybride

3.28
interface de sortie de contrôle
interface(s) identifiée(s) par un fournisseur, par laquelle (lesquelles) toutes les informations de contrôle sont sorties du module cryptographique

3.29
paramètre de sécurité critique
CSP
informations relatives à la sécurité dont l'accès, l'utilisation, la divulgation, la modification et la substitution non autorisés peuvent compromettre la sécurité d'un module cryptographique

EXEMPLE Clés cryptographiques secrètes et privées, données d'authentification ou de vérification telles que les mots de passe ou les PIN.

NOTE Un CSP peut être en clair ou chiffré.

3.30
responsable cryptographie
opérateur qui accède à un module cryptographique afin d'exécuter les fonctions d'initialisation ou de gestion cryptographique d'un module cryptographique (initialisation du module, gestion des SSP et audit, par exemple)

3.31
algorithme cryptographique
procédure de calcul bien définie qui prend en entrée des variables, qui peuvent inclure des clés cryptographiques, et qui produit une sortie

NOTE Des normes relatives aux algorithmes cryptographiques approuvés sont spécifiées à l'Annexe C.

3.32
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

3.33
contournement cryptographique
capacité d'un service à contourner, en tout ou partie, une fonction ou un processus cryptographique

3.34
fonction de hachage cryptographique
fonction efficace en termes de calcul qui associe 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

3.35
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 valeur de contrôle cryptographique, la génération de signatures ou la vérification de signatures.

3.36
module cryptographique
module
ensemble des matériels, logiciels et/ou micrologiciels qui mettent en œuvre des fonctions de sécurité et qui sont contenus à l'intérieur de la frontière cryptographique

3.37
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 du présent document et les règles supplémentaires imposées par le module ou l'autorité de validation

NOTE Voir l'Annexe B.

3.38
opération cryptographique
mise en œuvre d'un ou plusieurs algorithmes cryptographiques dans le module

3.39
interface d'entrée de données
interface(s) identifiée(s) par un fournisseur, par laquelle (lesquelles) toutes les données d'entrée sont entrées dans le module cryptographique

3.40
interface de sortie de données
interface(s) identifiée(s) par un fournisseur, par laquelle (lesquelles) toutes les données de sortie sont sorties du module cryptographique

3.41
chemin de données
itinéraire physique ou logique emprunté par les données

NOTE Un chemin de données physique peut être partagé par plusieurs chemins de données logiques.

3.42
technique de débogage
méthode utilisée pour interrompre ou modifier l'exécution du module afin d'analyser les dysfonctionnements, en utilisant des interfaces ou des outils qui peuvent modifier des objets en mémoire, incluant par exemple du code exécutable, d'une façon susceptible de contourner les mesures de sécurité

NOTE Les fonctionnalités du code exécutable requises pour satisfaire aux exigences fonctionnelles du présent document sont considérées comme des mesures de sécurité.

