Norme internationale

ISO/IEC 19790

Troisième édition
2025-02

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences de sécurité pour les modules cryptographiques

Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

Numéro de référence
ISO/IEC 19790:2025(fr)

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

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.

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 ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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 nature volontaire des normes, 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 www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document 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*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 19790:2012), qui a fait l'objet d'une révision technique. Elle incorpore également le Rectificatif technique ISO/IEC 19790:2012/Cor 1:2015.

Les principales modifications sont les suivantes:

— les Articles 3, 4 et 5 ont été complétés et mis à jour afin d'intégrer les changements d'exigences de l'Article 7;

— l'Article 6 a été complété et modernisé;

— les exigences de l'Article 7 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;

— les Annexes A et B ont été mises à jour afin d'intégrer les changements d'exigences de l'Article 7;

— les Annexes C, D et E ont été restructurées et mises à jour en fonction des normes publiées depuis l'édition précédente, et des exemples de méthodes de limitation du débit ont été ajoutés;

— l'Annexe F a été mis à jour en intégrant l'ISO/IEC 17825; et

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

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

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 autorisée, 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 définis dans le présent document. 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 est choisi de façon à fournir un niveau de sécurité qui est approprié pour les exigences de sécurité de l'application et de l'environnement dans lequel le module est 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 approprié 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.

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. Il est attendu que la politique de sécurité du module, qui donne un bref aperçu de ses forces et faiblesses, soit appliquée pour tout déploiement donné.

Sécurité de l'information, cybersécurité et protection de la vie privée — 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). Il définit quatre niveaux de sécurité pour les modules cryptographiques afin de couvrir un large éventail de sensibilités des données et une diversité d'environnements d'application. 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.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

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* (3.30) et/ou d'autres *rôles* (3.119) d'administrateurs pour la configuration, la maintenance et l'administration correctes du *module cryptographique* (3.35)

3.3
automatisé
sans entrée ou intervention *manuelle* (3.81) (par exemple via des moyens électroniques, tels qu'un réseau informatique)

3.4
technique d'authentification des données approuvée
méthode approuvée donnant l'assurance que l'expéditeur des données est bel et bien celui qui est déclaré

Note 1 à l'article: Les techniques d'authentification des données approuvées peuvent inclure l'utilisation d'une *signature numérique* (3.43) approuvée, d'un *code d'authentification de message* (3.82) approuvé ou d'un hachage par clé approuvé. Des techniques d'authentification des données approuvées sont spécifiées à l'Annexe C.

3.5
technique d'intégrité approuvée
méthode approuvée pour vérifier si des données ont été ou non corrompues ou modifiées

Note 1 à l'article: Les techniques d'intégrité approuvées peuvent utiliser des clés et inclure l'utilisation d'un hachage approuvé, d'un *code d'authentification de message* (3.82) ou d'un algorithme de *signature numérique* (3.43).

Note 2 à l'article: Des techniques d'intégrité approuvées sont spécifiées à l'Annexe C.

3.6
processus approuvé
ensemble de fonctions interdépendantes qui comprend au moins une *fonction de sécurité approuvée* (3.8), et peut inclure une fonction non cryptographique ou une *fonction de sécurité* (3.126) non approuvée qui ne sont pas relatives à la sécurité du fonctionnement du processus

Note 1 à l'article: Une transaction bancaire, un service de compression qui inclut un chiffrement, etc.

3.7
service approuvé
service (3.136) comprenant au moins une *fonction de sécurité approuvée* (3.8) ou un processus de sécurité approuvé, et pouvant inclure des fonctions ou processus *non relatifs à la sécurité* (3.91)

Note 1 à l'article: Les fonctions ou processus de sécurité *relatifs à la sécurité* (3.128) mais non approuvés sont exclus des services approuvés.

3.8
fonction de sécurité approuvée
fonction de sécurité (3.126) dont l'utilisation dans un *service approuvé* (3.7) est autorisée

Note 1 à l'article: Les fonctions de sécurité approuvées sont référencées dans l'Annexe C, qui fait référence à l'Annexe D et à l'Annexe E.

3.9
algorithme asymétrique
technique asymétrique
algorithme cryptographique (3.31) ou technique cryptographique qui utilise deux transformations liées: une transformation publique (définie par la *clé publique* (3.113)) et une transformation privée (définie par la *clé privée* (3.110))

Note 1 à l'article: 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.

3.10
attestation
processus utilisé pour permettre à une *entité* (3.49) située à l'extérieur de la frontière du *module cryptographique* (3.35) de vérifier de manière sécurisée l'identité et d'autres caractéristiques physiques ou logiques du module cryptographique en utilisant un *enregistrement d'attestation* (3.11)

Note 1 à l'article: Une attestation est conforme aux normes et méthodes d'attestation énumérées à l'Annexe G.

3.11
enregistrement d'attestation
enregistrement accessible et généré par un *module cryptographique* (3.35) qui prend en compte le *service d'attestation* (3.12)

Note 1 à l'article: L'enregistrement d'attestation contient les détails de mesure des composants *logiciels* (3.140), *micrologiciels* (3.58) ou *matériels* (3.64) 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* (3.145), des registres et des valeurs de fusibles.

3.12
service d'attestation
service (3.136) qu'un *module cryptographique* (3.35) peut prendre en charge et nécessitant la prise en charge d'une identité et la génération d'un *enregistrement d'attestation* (3.11) par ce module

3.13
données d'authentification
données chargées dans le *module cryptographique* (3.35) par l'*opérateur* (3.98), servant à authentifier l'opérateur vis-à-vis du module

Note 1 à l'article: Les données d'authentification à l'intérieur du module sont transitoires et considérées comme un *paramètre de sécurité critique* (3.29) temporaire.

Note 2 à l'article: Au cours d'une tentative d'authentification, les données d'authentification sont soumises au module sous forme:

a) d'entrée de données effectuée par l'opérateur (par exemple un *mot de passe* (3.102), une *valeur d'identification personnelle* (3.103), une *clé cryptographique* (3.34) ou équivalent); ou

b) 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* (3.110), l'insertion d'une clé physique, le traitement de données *biométriques* (3.15)).

3.14
autorisé
lorsqu'un *opérateur* (3.98) a le pouvoir d'endosser un *rôle* (3.119) spécifique et d'exécuter un ensemble de services correspondant

3.15
biométrique
caractéristique physique ou trait comportemental personnel, mesurable, utilisé pour reconnaître l'identité ou vérifier l'identité déclarée d'un *opérateur* (3.98)

3.16
flux binaire
série d'instructions analysées par une matrice prédiffusée programmable par l'utilisateur (FPGA) au démarrage afin de configurer sa logique interne

Note 1 à l'article: Le flux binaire est considéré comme une forme de code exécutable fortement personnalisée.

3.17
certificat
données d'une entité qui sont rendues infalsifiables à l'aide de la clé privée ou secrète d'une autorité de certification (CA)

Note 1 à l'article: Il convient de ne pas confondre ce terme avec un certificat de validation de module délivré par un *organisme de certification* (3.18).

3.18
organisme de certification
organisme tierce partie d'évaluation de la conformité mettant en œuvre un programme de certification

Note 1 à l'article: Un organisme de certification peut être gouvernemental ou non gouvernemental (avec ou sans pouvoir réglementaire).

Note 2 à l'article: Un organisme de certification qui évalue la conformité au présent document est qualifié d'autorité de validation.

Note 3 à l'article: Un programme de certification est un système associé à des produits spécifiés, auquel s'appliquent les mêmes exigences spécifiées, règles et procédures spécifiques.

[SOURCE: ISO/IEC 17065:2012, 3.12]

3.19
compromission
divulgation, modification, substitution ou utilisation non autorisée d'un *paramètre de sécurité critique* (3.29), modification ou substitution non autorisée d'un *paramètre de sécurité public* (3.115), ou perte d'*intégrité* (3.72) ou de disponibilité du *module cryptographique* (3.35) 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* (3.35) 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 24765:2017 3.779.1, modifié — Dans la définition, le terme «spécifiées» a été remplacé par «spécifiques».]

3.23
système de gestion de configuration
CMS
ensemble de procédures et d'outils (y compris leur documentation) utilisés par un *fournisseur* (3.156) pour développer et maintenir des configurations d'un *module cryptographique* (3.35) 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* (3.81) telles que celles provenant d'interrupteurs, de boutons et de claviers) utilisés pour piloter ou contrôler le fonctionnement d'un *module cryptographique* (3.35) ou de composants séparés d'un *module hybride* (3.68)

3.25
entrée de contrôle
informations de contrôle (3.24) qui sont entrées dans un *module cryptographique* (3.35) ou des composants séparés d'un *module hybride* (3.68)

3.26
interface d'entrée de contrôle
interface(s) du module, par laquelle (lesquelles) toutes les *informations de contrôle* (3.24) sont entrées dans le *module cryptographique* (3.35)

3.27
sortie de contrôle
informations de contrôle (3.24) qui sont issues d'un *module cryptographique* (3.35) ou d'un composant séparé d'un *module hybride* (3.68) pour être utilisées comme une *entrée de contrôle* (3.25) dans un autre module cryptographique ou un composant séparé d'un module hybride

3.28
interface de sortie de contrôle
interface(s) du module, par laquelle (lesquelles) toutes les *informations de contrôle* (3.24) sont sorties du *module cryptographique* (3.35)

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 entraîner une *compromission* (3.19) de la sécurité d'un *module cryptographique* (3.35)

EXEMPLE *Clés cryptographiques* (3.34) secrètes et privées, *données d'authentification* (3.13) ou *données de vérification* (3.157) telles qu'un *mot de passe* (3.102) ou une *valeur d'identification personnelle* (3.103).

Note 1 à l'article: Un CSP peut être *en clair* (3.105) ou chiffré.

3.30
responsable cryptographie
rôle (3.119) assumé par un *opérateur* (3.98) qui accède à un *module cryptographique* (3.35) afin d'exécuter les fonctions d'initialisation ou de gestion cryptographique d'un module cryptographique (initialisation du module, gestion des *paramètres de sécurité sensibles* (3.131) et audit, par exemple)

3.31
algorithme cryptographique
procédure de calcul bien définie qui prend en entrée des variables, qui peuvent inclure une *clé cryptographique* (3.34), et qui produit une sortie

Note 1 à l'article: 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 des composants *matériels* (3.64), *logiciels* (3.140) ou *micrologiciels* (3.58)) du *module cryptographique* (3.35)

3.33
contournement cryptographique
capacité d'un *service* (3.136) à contourner, en tout ou partie, une fonction ou un processus cryptographique

3.34
clé cryptographique
clé
suite de symboles qui commande le fonctionnement d'une transformation cryptographique

Note 1 à l'article: 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.

3.35
module cryptographique
module
ensemble des *matériels* (3.64) et des *logiciels* (3.140) ou *micrologiciels* (3.58) qui mettent en œuvre des fonctions de sécurité et qui sont contenus à l'intérieur de la *frontière cryptographique* (3.32)

3.36
politique de sécurité du module cryptographique
politique de sécurité
spécification précise des règles de sécurité sur la base desquelles un *module cryptographique* (3.35) fonctionnera, y compris les règles dérivées des exigences du présent document et les règles supplémentaires imposées par le module ou l'*organisme de certification* (3.18)

Note 1 à l'article: Voir l'Annexe B.

3.37
opération cryptographique
mise en œuvre d'un ou plusieurs *algorithmes cryptographiques* (3.31) dans le *module cryptographique* (3.35)

3.38
interface d'entrée de données
interface(s) du module, par laquelle (lesquelles) toutes les *données d'entrée* (3.71) sont entrées dans le *module cryptographique* (3.35)

3.39
interface de sortie de données
interface(s) du module, par laquelle (lesquelles) toutes les *données de sortie* (3.99) sont sorties du *module cryptographique* (3.35)

3.40
chemin de données
itinéraire physique ou logique emprunté par les données

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

3.41
technique de débogage
méthode utilisée pour interrompre ou modifier l'exécution du *module cryptographique* (3.35) 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 qui permet de contourner les mesures de sécurité

Note 1 à l'article: Les fonctionnalités du code exécutable requises pour satisfaire aux exigences fonctionnelles du présent document sont considérées comme des mesures de sécurité.

3.42
fonctionnement dégradé
fonctionnement dans lequel un sous-ensemble de l'ensemble complet de fonctions, services ou processus de sécurité est soit disponible soit configurable, ou les deux, en raison d'une reconfiguration à partir d'un état d'erreur

3.43
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* (3.72) de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple)

3.44
saisie directe
saisie d'un *paramètre de sécurité sensible* (3.131) ou d'un *composant de clé* (3.74) dans un *module cryptographique* (3.35), à l'aide d'un dispositif tel qu'un clavier ou un pavé numérique

3.45
signature disjointe
signature utilisée comme partie d'un groupe de signatures qui, collectivement, représentent un ensemble de code complet

3.46
saisie électronique
saisie d'un *paramètre de sécurité sensible* (3.131) ou d'un *composant de clé* (3.74) dans un *module cryptographique* (3.35) à l'aide de méthodes électroniques

Note 1 à l'article: Il est possible que l'*opérateur* (3.98) du *module cryptographique* (3.35) n'ait aucune connaissance de la valeur de la clé saisie.

3.47
signature englobante
signature unique pour un ensemble de code complet