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/IEC 2025



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2025

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 **19**
5 Niveaux de sécurité des modules cryptographiques **19**
5.1 Généralités 19
5.2 Niveau de sécurité 1 20
5.3 Niveau de sécurité 2 20
5.4 Niveau de sécurité 3 20
5.5 Niveau de sécurité 4 21
6 Objectifs de sécurité fonctionnelle **22**
7 Exigences de sécurité **22**
7.1 Généralités 22
7.2 Spécification du module cryptographique 25
7.2.1 Exigences générales relatives à la spécification du module cryptographique 25
7.2.2 Types de modules cryptographiques 26
7.2.3 Frontière cryptographique 26
7.2.4 Fonctionnements du module 27
7.3 Interfaces du module cryptographique 29
7.3.1 Exigences générales relatives aux interfaces du module cryptographique 29
7.3.2 Types d'interfaces 29
7.3.3 Catégories d'interfaces 29
7.3.4 Chemin de confiance en clair 30
7.3.5 Chemins internes protégés 31
7.4 Rôles, services et authentification 31
7.4.1 Exigences générales en matière de rôles, de services et d'authentification 31
7.4.2 Rôles 32
7.4.3 Services 32
7.4.4 Authentification 34
7.5 Sécurité logicielle/micrologicielle 36
7.5.1 Exigences générales en matière de sécurité logicielle/micrologicielle 36
7.5.2 Niveau de sécurité 1 36
7.5.3 Niveau de sécurité 2 37
7.5.4 Niveaux de sécurité 3 et 4 38
7.6 Environnement opérationnel 38
7.6.1 Exigences générales relatives à l'environnement opérationnel 38
7.6.2 Applicabilité des paragraphes 39
7.6.3 Exigences relatives au système d'exploitation pour les environnements opérationnels modifiables 40
7.7 Sécurité physique 42
7.7.1 Matérialisations de la sécurité physique 42
7.7.2 Exigences générales en matière de sécurité physique 43
7.7.3 Exigences de sécurité physique pour chaque matérialisation de sécurité physique 46
7.7.4 Protection contre les défaillances environnementales/essais de défaillance environnementale 47
7.7.5 Fonctionnalités de protection contre les défaillances environnementales 47
7.7.6 Procédures d'essai de défaillance environnementale 47
7.8 Sécurité non invasive 48
7.8.1 Exigences générales en matière de sécurité non invasive 48
7.8.2 Niveaux de sécurité 1 et 2 48

© ISO/IEC 2025 – Tous droits réservés

7.8.3 Niveau de sécurité 3 ... 48
7.8.4 Niveau de sécurité 4 ... 49
7.9 Gestion des paramètres de sécurité sensibles ... 49
7.9.1 Exigences générales relatives à la gestion des paramètres de sécurité sensibles ... 49
7.9.2 Générateurs de bits aléatoires ... 49
7.9.3 Génération de paramètres de sécurité sensibles ... 49
7.9.4 Établissement automatisé de paramètres de sécurité sensibles ... 50
7.9.5 Entrée et sortie de paramètres de sécurité sensibles ... 50
7.9.6 Stockage des paramètres de sécurité sensibles ... 51
7.9.7 Abrogation des paramètres de sécurité sensibles ... 51
7.10 Auto-tests ... 52
7.10.1 Exigences générales relatives aux auto-tests ... 52
7.10.2 Niveaux de sécurité 3 et 4 ... 53
7.10.3 Auto-tests pré-opérationnels ... 53
7.10.4 Auto-tests conditionnels ... 54
7.11 Assurance du cycle de vie ... 57
7.11.1 Exigences générales relatives à l'assurance du cycle de vie ... 57
7.11.2 Gestion de la configuration ... 58
7.11.3 Conception ... 58
7.11.4 Modèle à état fini ... 58
7.11.5 Développement ... 59
7.11.6 Essais fournisseur ... 61
7.11.7 Livraison et fonctionnement ... 61
7.11.8 Guides (d'orientation) ... 62
7.12 Atténuation des autres attaques ... 63
7.12.1 Exigences générales relatives à l'atténuation des autres attaques ... 63
7.12.2 Niveaux de sécurité 1, 2 et 3 ... 63
7.12.3 Niveau de sécurité 4 ... 63

Annexe A (normative) **Exigences en matière de documentation** ... **64**

Annexe B (normative) **Politique de sécurité du module cryptographique** ... **71**

Annexe C (normative) **Fonctions de sécurité approuvées** ... **77**

Annexe D (normative) **Méthodes approuvées de génération et d'établissement de paramètres de sécurité sensibles** ... **79**

Annexe E (normative) **Mécanismes d'authentification approuvés** ... **80**

Annexe F (normative) **Mesures d'essai d'atténuation des attaques non invasives approuvées** ... **81**

Annexe G (normative) **Développement, fabrication et fonctionnement sécurisés du module** ... **82**

Bibliographie ... **83**

© ISO/IEC 2025 – 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.

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.

© ISO/IEC 2025 – Tous droits réservés

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.

© ISO/IEC 2025 – 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 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.

© ISO/IEC 2025 – Tous droits réservés

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.

© ISO/IEC 2025 – Tous droits réservés

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.

© ISO/IEC 2025 – Tous droits réservés