Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B

Praticien·nes

TLP:CLEAR

Canada

Avant-propos

La présente publication intitulée *Algorithmes cryptographiques pour l'information Non classifié, Protégé A et Protégé B* est un document NON CLASSIFIÉ publié par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Elle constitue une mise à jour et remplace la version publiée précédemment. Pour obtenir de plus amples renseignements, communiquez par courriel ou par téléphone avec le :

Centre d'appel

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 18 mars 2024.

Historique des révisions

Révision	Modifications	Date
1	Première version	2 août 2016
2	Version mise à jour (version 2)	17 août 2022
3	Version mise à jour (version 3)	18 mars 2024

Vue d'ensemble

La présente publication définit les algorithmes cryptographiques recommandés et les méthodes d'utilisation appropriées que les organisations peuvent mettre en œuvre pour protéger l'information sensible. Pour les organismes et ministères du gouvernement du Canada (GC), les directives contenues dans ce document s'appliquent à l'information NON CLASSIFIÉ, PROTÉGÉ A, et PROTÉGÉ B.

Votre organisation se doit d'être en mesure de protéger l'information et les données sensibles pour assurer la prestation de programmes et de services. La cryptographie fournit des mécanismes de sécurité servant à protéger la confidentialité, l'intégrité et l'authenticité de l'information.

Une cryptographie configurée adéquatement présente de nombreux avantages. Elle permet notamment d'assurer la confidentialité, l'intégrité et l'authenticité des données, l'authentification et la responsabilisation des intervenants, de même que la non-répudiation. Plusieurs algorithmes peuvent s'avérer nécessaires pour satisfaire aux exigences de sécurité, et le respect de toutes ces exigences exige parfois la mise en œuvre de chacun de ces algorithmes.

Table des matières

Liste des figures

1 Introduction

Les organisations recourent à des systèmes de technologies de l'information (TI) pour atteindre leurs objectifs opérationnels. Ces systèmes interconnectés peuvent faire l'objet de sérieuses menaces et cyberattaques pouvant mettre en péril la disponibilité, l'authenticité, la confidentialité et l'intégrité des biens d'information. Des réseaux, des systèmes ou des renseignements compromis peuvent influer négativement les activités et entraîner une atteinte à la protection des données ainsi que des pertes financières.

Le présent document aide les praticiens des technologies à choisir et à utiliser adéquatement des algorithmes cryptographiques. Lorsqu'ils sont utilisés avec des paramètres de domaine valides et des longueurs de clé spécifiques, les algorithmes cryptographiques figurant dans ce document sont des mécanismes cryptographiques recommandés pour protéger l'authenticité, la confidentialité et l'intégrité de l'information sensible de niveau NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B associée à un niveau de préjudice moyen, tel qu'il est défini dans La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [1][A] du Centre pour la cybersécurité. Pour connaître les exigences relatives à l'utilisation de la cryptographie approuvée par le Centre pour la cybersécurité aux fins de protection de l'information PROTÉGÉ C et classifiée, prière de communiquer avec le Centre pour la cybersécurité par courriel à contact@cyber.gc.ca.

Le présent document complète la Ligne directrice sur la définition des exigences en matière d'authentification [2] du Secrétariat du Conseil du Trésor du Canada (SCT). Les organisations doivent déterminer leurs objectifs et exigences en matière de sécurité dans leur cadre de gestion des risques.

1.1 Notes à l'intention du praticien

Dans le présent document, nous faisons des recommandations relatives aux algorithmes et aux paramètres cryptographiques. Nous dressons également une liste des algorithmes qui devraient être mis hors service. Ainsi, les nouvelles applications ne devraient pas utiliser ces algorithmes. Lorsque les algorithmes sont utilisés dans des applications existantes, ils devraient être remplacés par les algorithmes que nous recommandons dans cette publication. Dans le cas de certains algorithmes, nous précisons une date à laquelle ils auraient dû être remplacés. Dans d'autres cas, ces algorithmes doivent être remplacés le plus rapidement possible.

Sauf indication contraire, lorsqu'un algorithme nécessite une primitive, il doit être choisi parmi ceux qui sont recommandés dans le présent document. Par exemple, une fonction de hachage énoncée à la section 6.2 ou 6.3 doit être utilisée avec le code d'authentification de message avec hachage de clé (HMAC pour *Keyed-Hash Message Authentication Code*) énoncé à la section 8.1. Sauf indication contraire, lorsqu'un algorithme nécessite un paramètre, il doit être choisi parmi ceux qui sont recommandés dans la référence donnée pour l'algorithme.

[A] Les numéros entre crochets renvoient à des ressources figurant à la section Contenu complémentaire du présent document.

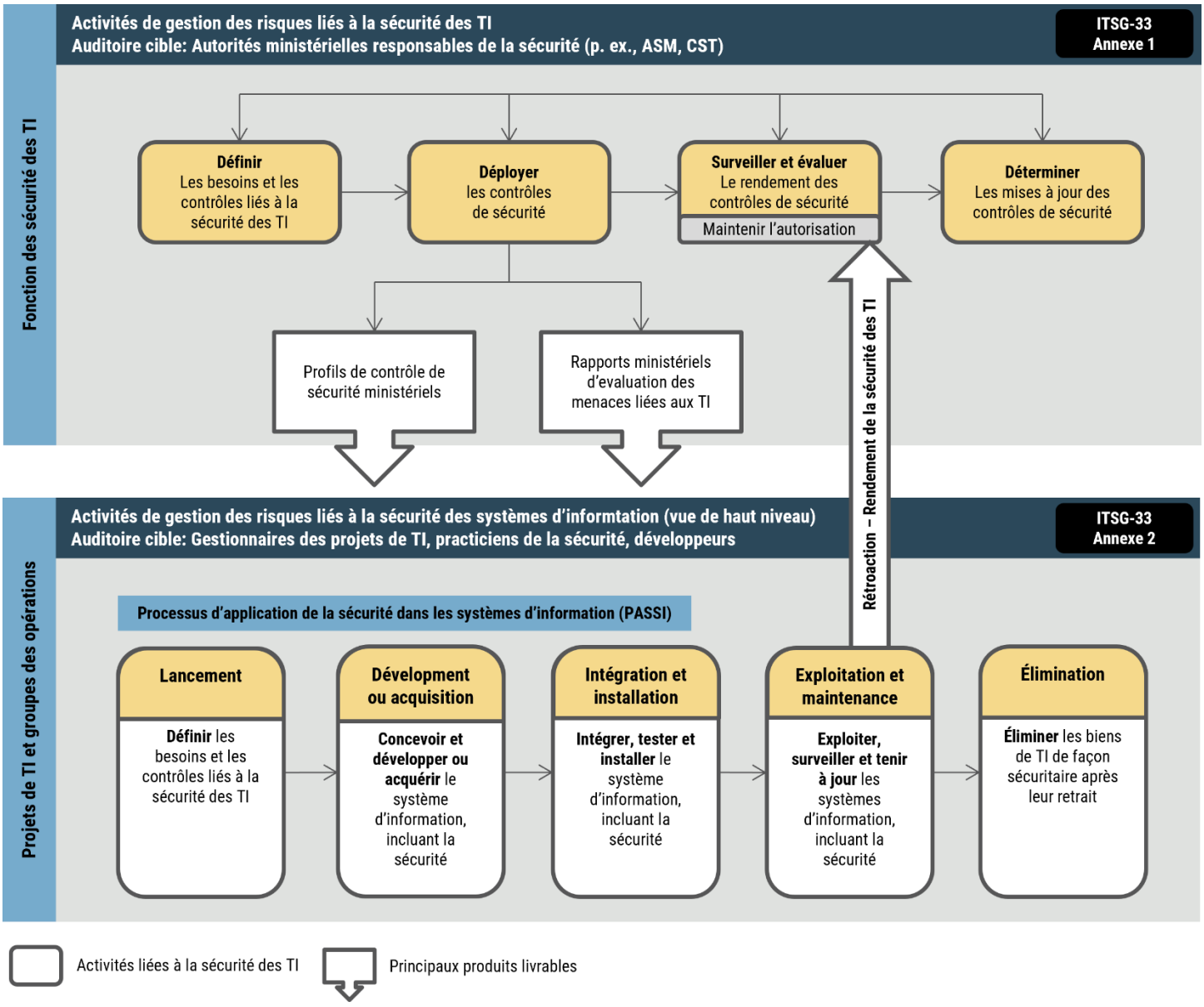
1.2 Politiques déterminantes

Afin de sécuriser les réseaux, les données et les biens, les organisations doivent analyser et contrer les cybermenaces et les vulnérabilités auxquelles elles font face. Les ministères du GC doivent veiller à ce que les politiques et procédures en matière de sécurité des TI soient mises en œuvre conformément à la Politique sur la sécurité du gouvernement [3] du SCT.

1.3 Lien avec le processus de gestion des risques liés aux TI

Les lignes directrices contenues dans La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [1] du Centre pour la cybersécurité C proposent un ensemble d'activités pour chacun des deux niveaux organisationnels suivants : niveau du ministère et niveau des systèmes d'information.

Figure 1 Processus de gestion des risques liés à la sécurité des TI



Description de la figure : Cette image décrit le processus de gestion des risques liés à la sécurité des TI de haut niveau du ministère et les activités connexes, ainsi que les activités de gestion des risques liés aux systèmes d'information. Elle souligne également le fait que les activités de gestion des risques liés à la sécurité des TI aux deux niveaux agissent de concert dans un cycle continu pour maintenir et améliorer efficacement la posture de sécurité des systèmes d'information ministériels.

Les activités du niveau ministériel sont intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques liés à la sécurité des TI. Les algorithmes cryptographiques doivent être pris en compte dans le cadre des activités de définition, de déploiement, de surveillance et d'évaluation. Ces activités sont décrites en détail à l'Annexe 1 - Activités de gestion des risques liés à la sécurité des TI (ITSG-33) [1].

Les activités du niveau des systèmes d'information sont intégrées au cycle de vie d'un système d'information pour s'assurer de ce qui suit :

- répondre aux besoins opérationnels en matière de sécurité des TI;
- mettre en œuvre des contrôles de sécurité appropriés et les exploiter comme prévu;
- le rendement des contrôles de sécurité existants est évalué en permanence, fait l'objet de rapports et des mesures appropriées sont prises pour corriger toute lacune relevée.

Les algorithmes cryptographiques doivent être pris en compte dans le cadre de toutes les activités du niveau des systèmes d'information. Ces activités sont décrites en détail à l'Annexe 2 - Activités de gestion des risques liés à la sécurité des systèmes d'information (ITSG-33) [1].

2 Algorithmes de chiffrement

La section suivante décrit les algorithmes de chiffrement que nous recommandons pour protéger la confidentialité de l'information NON CLASSIFIÉ, PROTÉGÉ A, et PROTÉGÉ B. Nous précisons également les algorithmes de chiffrement qui ont été recommandés dans une version antérieure de cette publication, mais qui auraient dû être abandonnés avant la fin de 2023.

2.1 Algorithme de chiffrement avancé

Nous recommandons l'algorithme AES (pour *Advanced Encryption Standard*), conformément aux normes FIPS (*Federal Information Processing Standards*) du National Institute of Standards and Technology (NIST) dans le document intitulé Information Processing Standards Publication 197: Advanced Encryption Standard [4] au moyen d'une longueur de clé de 128, 192 ou 256 bits.

2.2 Algorithme de chiffrement de données triple (TDEA pour *Triple Data Encryption Algorithm*)

L'utilisation de l'algorithme TDEA à trois clés aurait dû être abandonnée avant la fin de 2023.

Nous ne recommandons plus l'utilisation de l'algorithme TDEA conformément au document NIST SP 800-67 Revision 2: Recommendation for the Triple Data Encryption Algorithm Block Cipher [5]. Pour les applications héritées qui utilisent toujours l'option à trois clés de l'algorithme TDEA, une restriction importante est à noter : un trousseau de clés ne devrait pas être utilisé pour chiffrer plus de 2^{20} blocs de données de 64 bits [5].

2.3 CAST5

L'utilisation de l'algorithme CAST5 aurait dû être abandonnée avant la fin de 2023.

Nous ne recommandons plus l'utilisation de l'algorithme CAST5, conformément au document Request for Comments (RFC) 2144: The CAST-128 Encryption Algorithm [6].

3 Modes de fonctionnement des algorithmes de chiffrement

La section suivante décrit les modes de fonctionnement des algorithmes de chiffrement que nous recommandons d'utiliser avec l'algorithme AES, conformément à la section 2.1.

3.1 Protection de la confidentialité de l'information

Nous recommandons les modes de fonctionnement de chiffrement par blocs suivants pour protéger la confidentialité de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B, conformément au document NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques [7]:

- mode de chiffrement par carnet de codage électronique (ECB pour *Electronic Codebook*) – le mode ECB ne s'applique que dans des situations au cours desquelles un seul bloc de données est chiffré ou conformément à ce qui est précisé pour des algorithmes dérivés, dont l'encapsulation de clé (voir la section 10). Il ne devrait pas être utilisé pour le chiffrement de donnée en masse
- mode de chiffrement à rétroaction (CFB pour *Cipher Feedback*)
- mode de chiffrement à rétroaction de sortie (OFB pour *Output Feedback*)
- mode de chiffrement basé sur un compteur (CTR pour *Counter*)
- mode de chiffrement par chaînage de blocs (CBC pour *Cipher Block Chaining*) – lors de l'utilisation du mode CBC avec une entrée de texte clair d'une longueur de bits supérieure ou égale à la taille du bloc, une méthode de remplissage doit être utilisée tel qu'il est décrit dans l'annexe A du document SP800-38A [7]. Les protocoles précisent habituellement les méthodes particulières de remplissage pouvant être utilisées. Si aucune méthode de remplissage n'est précisée, nous recommandons les méthodes suivantes tirées de l'addenda du document du NIST Addendum to SP 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode [8]:
    - CBC-CS1
    - CBC-CS2
    - CBC-CS3

Plusieurs exigences importantes sont tirées du document SP800-38A [7] :

- les modes CBC et CFB nécessitent des motifs d'initialisation (IV pour Initialization Vector) imprévisibles;
- pour le mode OFB, l'IV doit être un nonce unique à chaque exécution de l'opération de chiffrement; il n'a pas à être imprévisible;
- le mode CTR exige un bloc compteur unique pour chacun des blocs de texte clair chiffré conformément à une clé donnée, et ce, pour tous les messages.

Pour assurer la protection des données sur des dispositifs de stockage, nous recommandons l'utilisation du mode XTS-AES, conformément au document NIST SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices [9].

3.2 Protection de la confidentialité et de l'authenticité de l'information

Nous recommandons les modes de fonctionnement suivants pour protéger la confidentialité et l'authenticité de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B :

- mode de chiffrement basé sur un compteur avec code d'authentification de message avec chiffrement par chaînage de blocs (CCM pour *Cipher Block Chaining Message Authentication Code*), conformément au document NIST SP 800–38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality [10]
- mode Galois/compteur (GCM pour Galois/Counter Mode), conformément au document SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode [11]

4 Schémas d'établissement de clés

La section suivante décrit les schémas d'établissement de clés que nous recommandons d'utiliser avec les algorithmes cryptographiques pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

4.1 Rivest-Shamir-Adleman (RSA)

Nous recommandons les schémas de négociation et de transport de clés basés sur l'algorithme Rivest-Shamir-Adleman (RSA), conformément au document NIST SP 800-56B Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography [12] avec une longueur de module RSA d'au moins 2048 bits.

La longueur du module RSA devrait être augmentée à au moins 3072 bits d'ici la fin de 2030.

4.2 Cryptographie à corps fini (FFC) de Diffie-Hellman (DH) et de Menezes-Qu-Vanstone (MQV)

Nous recommandons les schémas de négociation de clés basés sur la cryptographie à corps fini (FFC pour *Finite Field Cryptography*) de Diffie-Hellman (DH) et de Menezes-Qu-Vanstone (MQV), utilisés conjointement avec des paramètres de domaine valides pour les ensembles tailles-paramètres FB ou FC FFC, conformément au document NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [13]. La taille de corps (paramètre du module composé) devrait être d'au moins 2048 bits.

La taille du corps FFC devrait être augmentée à au moins 3072 bits d'ici la fin de 2030.

4.3 Cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur et de Menezes-Qu-Vanstone

Nous recommandons les schémas de négociation de clés basés sur la cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur (CCE CDH) et de Menezes-Qu-Vanstone (CCE MQV), conformément au document NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [13]. Nous recommandons les courbes elliptiques suivantes, conformément au document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- Courbe P-224
- Courbe P-256
- Courbe P-384
- Courbe P-521

L'utilisation de la courbe P-224 devrait être abandonnée d'ici la fin de 2030.

Nous ne recommandons plus l'utilisation des courbes binaires, conformément à l'annexe D du document NIST FIPS 186-4: Digital Signature Standard [15].

Toutes les courbes binaires devraient être abandonnées d'ici la fin de 2030. Une liste des courbes à abandonner se trouve à la section 3.3 du document NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]**.**

5 Schémas de signature numérique

La section suivante décrit les algorithmes que nous recommandons pour les applications de signature numérique offrant une intégrité des données et une authentification de l'origine des données pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Nous précisons également un schéma de signature numérique qui a été recommandé dans une version antérieure de cette publication, mais qui devrait être abandonné avant la fin de 2030.

5.1 Rivest-Shamir-Adleman

Nous recommandons l'utilisation de l'algorithme de signature numérique Rivest-Shamir-Adleman (RSA), avec RSASSA-PKCS1-v1.5 ou RSASSA-PSS, conformément au document NIST FIPS 186-5: Digital Signature Standard [16] avec une longueur de module RSA d'au moins 2048 bits.

La longueur du module RSA devrait être augmentée à au moins 3072 bits d'ici la fin de 2030.

5.2 Algorithme de signature numérique (DSA)

L'utilisation de l'algorithme DSA devrait être abandonnée d'ici la fin de 2030.

Nous ne recommandons plus l'utilisation de l'algorithme de signature numérique (DSA pour *Digital Signature Algorithm*), conformément au document NIST FIPS 186-4: Digital Signature Standard [15] avec des paramètres de domaine valides pour une taille de corps d'une longueur minimale de 2048 bits.

5.3 Algorithme de signature numérique à courbe elliptique (ECDSA)

Nous recommandons l'utilisation de l'algorithme de signature numérique à courbe elliptique (ECDSA pour *Elliptic Curve Digital Signature Algorithm*) et l'algorithme ECDSA déterministe[B], conformément au document NIST FIPS 186-5: Digital Signature Standard [16]. Nous recommandons les courbes elliptiques suivantes, conformément au document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- Courbe P-224
- Courbe P-256
- Courbe P-384
- Courbe P-521

L'utilisation de la courbe P-224 devrait être abandonnée d'ici la fin de 2030.

[B] À partir de [16], l'algorithme ECDSA déterministe « est une variante de l'algorithme ECDSA, associant à chaque message une valeur secrète, fonction de la signature finale, résultant ainsi en une relation fonctionnelle déterministe entre la signature et le message lui-même. » La vérification de la signature dans l'algorithme ECDSA déterministe se fait de la même façon que pour l'algorithme ECDSA.

Nous ne recommandons plus l'utilisation des courbes binaires, conformément à l'annexe D du document NIST FIPS 186-4: Digital Signature Standard [15].

Toutes les courbes binaires devraient être abandonnées d'ici la fin de 2030. Une liste des courbes à abandonner se trouve à la section 3.3 du document NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14].

5.4 Algorithme de signature numérique à courbe Edwards (EdDSA)

Nous recommandons l'utilisation de l'algorithme de signature numérique à courbe Edwards (EdDSA pour *Edwards-Curve Digital Signature Algorithm*), conformément au document NIST FIPS 186-5: Digital Signature Standard [16] avec les courbes elliptiques suivantes, conformément au document NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- Edwards25519
- Edwards448

Nous ne recommandons pas la version préhachage HashEdDSA.

5.5 Schémas de signature numérique à hachage dynamique

Nous recommandons d'utiliser les signatures numériques à hachage dynamique uniquement dans des situations où tous les éléments suivants s'appliquent :

1. lorsqu'un schéma de numérique post-quantique doit être mis en œuvre dans un avenir proche, avant que d'autres schémas de signature post-quantique d'usage général soient normalisés (voir la section 13);
2. lorsque la mise en œuvre aura une longue durée de vie et qu'elle n'est pas pratique pour passer à un nouveau schéma de signature numérique une fois la mise en œuvre déployée;
3. lorsque la lente génération de clés et les calculs de signature sont acceptables sur le plan opérationnel;
4. lorsque la gestion des états peut être mise en œuvre.

Dans de telles situations, nous recommandons l'utilisation des schémas de signature numérique à hachage suivants, conformément au document NIST SP 800-208: Recommendation for Stateful Hash-based Signatures Scheme [17], à l'aide d'une des fonctions de hachage SHA-256, SHA-256/192, SHAKE256/256, SHAKE256/192, conformément à la section 2.3 de [17] :

- Leighton-Micali Signature (LMS)
- Hierarchical Signature System (HSS)
- eXtended Merkle Signature Scheme (XMSS)
- Multi-tree eXtended Merkle Signature Scheme (XMSS^{MT})

6 Fonctions de hachage

La section suivante décrit les fonctions de hachage que nous recommandons d'utiliser avec les algorithmes cryptographiques précisés dans la présente publication pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

6.1 SHA-1

Nous ne recommandons plus l'utilisation de l'algorithme SHA-1 conformément au document NIST FIPS 180-4:Secure Hash Standard[18]. Son utilisation était auparavant approuvée avec les codes d'authentification de message avec hachage de clé, les fonctions de dérivation de clés et les générateurs de bits aléatoires.

L'algorithme SHA-1 ne doit pas être utilisé avec des schémas de signature numérique ou avec toutes applications nécessitant une résistance aux collisions. L'utilisation de cet algorithme doit être abandonnée avec les codes d'authentification de message avec hachage de clé, les fonctions de dérivation de clés et les générateurs de bits aléatoires.

6.2 SHA-2

Nous recommandons l'utilisation des algorithmes SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 et SHA-512/256, conformément au document NIST FIPS 180-4:Secure Hash Standard [18] pour les schémas de signature numérique, les codes d'authentification de message avec hachage de clé, les fonctions de dérivation de clés et les générateurs de bits aléatoires. La fonction de hachage tronqué SHA-256/192 précisée dans [17] n'est recommandée qu'avec les schémas de signature numérique à hachage dynamique qui figurent à la section 5.5.

L'utilisation de l'algorithme SHA-224 devrait être abandonnée d'ici la fin de 2030.

6.3 SHA-3

Nous recommandons l'utilisation des algorithmes SHA3-224, SHA3-256, SHA3-384 et SHA3-512, conformément au document NIST FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions [19] pour les schémas de signature numérique, les codes d'authentification de message avec hachage de clé, les fonctions de dérivation de clés et les générateurs de bits aléatoires.

L'utilisation de l'algorithme SHA3-224 devrait être abandonnée d'ici la fin de 2030.

7 Fonction de hachage extensible (XOF)

La section suivante décrit la fonction de hachage extensible (XOF pour *Extendable-Output Function*) que nous recommandons d'utiliser avec les algorithmes cryptographiques précisés dans la présente publication pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

7.1 SHAKE

Nous recommandons l'utilisation des algorithmes SHAKE128 et SHAKE256, conformément au document NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions [19] à utiliser dans ce qui suit :

- les schémas de signature numérique RSA (section 5.1), ECDSA (section 5.3) et EdDSA (section 5.4);
- les schémas de signature numérique à hachage dynamique à la section 5.5;
- les codes KMAC à la section 8.4.

8 Codes d'authentification de message (MAC)

Les sections suivantes décrivent les algorithmes MAC (*Message Authentication Code*) que nous recommandons pour l'intégrité des données et l'authentification de l'origine des données pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

8.1 Code d'authentification de message avec hachage de clé (HMAC)

Nous recommandons l'utilisation du code d'authentification de message avec hachage de clé (HMAC pour *Keyed-Hash Message Authentication Code*), conformément au document NIST FIPS 198-1: The Keyed-Hash Message Authentication Code [20] avec une clé d'au moins 112 bits de longueur.

La longueur de la clé devrait être augmentée à au moins 128 bits d'ici la fin de 2030.

8.2 Code d'authentification de message basé sur le chiffrement (CMAC)

Nous recommandons l'utilisation du code d'authentification de message basé sur le chiffrement (CMAC pour *Cipher-based Message Authentication Code*) conformément au document NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation:The CMAC Mode for Authentication [21] avec une clé d'au moins 112 bits de longueur.

La longueur de la clé aurait dû être augmentée à au moins 128 bits d'ici la fin de 2023.

8.3 Code d'authentification de message avec mode Galois/compteur (GMAC)

Nous recommandons l'utilisation du code d'authentification de message avec le mode Galois/compteur (GMAC pour *Galois/Counter Mode Message Authentication Code*), conformément au document NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode [11]. L'utilisation du code GMAC n'est recommandée qu'avec l'algorithme AES, conformément à la section 2.1.

8.4 Code d'authentification de message (KMAC)

Nous recommandons l'utilisation des algorithmes KMAC128 et KMAC256 (KMAC pour *KECCAK Message Authentication Code*), conformément au document NIST SP 800-185: SHA3-Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash [22] avec une clé d'au moins 112 bits de longueur.

La longueur de la clé devrait être augmentée à au moins 128 bits d'ici la fin de 2030.

9 Fonctions de dérivation de clés (KDF)

Les sections suivantes décrivent les fonctions de dérivation de clés (KDF pour *Key Derivation Function*) que nous recommandons pour la dérivation des clés cryptographiques à partir de secrets prépartagés ou d'établissement de clés. Ces fonctions sont utilisées pour la protection d'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

9.1 KDF à une étape

Nous recommandons l'utilisation de la fonction de dérivation de clés (KDF pour *Key Derivation Function*) à une étape, conformément au document NIST SP 800-56C Revision 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes [23].

9.2 KDF à deux étapes

Nous recommandons l'utilisation de la procédure de dérivation de clés par extraction puis expansion à deux étapes, conformément au document NIST SP 800-56C Revision 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes [23]. Il est à noter que la fonction HKDF utilisée dans la version 1.3 du protocole de sécurité de la couche de transport (Transport Layer Security) (TLS 1.3) utilise cette spécification.

9.3 Dérivation de clés au moyen de fonctions pseudo-aléatoires

Nous recommandons l'utilisation des KDF se servant de fonctions pseudo-aléatoires (PRF pour *Pseudorandom Function*), conformément au document NIST SP 800-108 Revision 1: Recommendation for Key Derivation Using Pseudorandom Functions [24].

9.4 KDF avec la version 2 du protocole d'échange de clés Internet (IKEv2)

Lorsqu'elle est utilisée dans le contexte de la version 2 du protocole d'échange de clés Internet (IKEv2 pour *Internet Key Exchange version 2*), nous recommandons le recours à la KDF IKEv2, conformément au document NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.5 KDF avec la version 1.2 du protocole de sécurité de la couche transport (TLS 1.2)

Lorsqu'elle est utilisée dans le contexte de la version 1.2 du protocole de sécurité de la couche de transport (TLS 1.2), nous recommandons le recours à la KDF TLS 1.2, conformément au document NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.6 KDF avec protocole Secure Shell (SSH)

Lorsqu'elle est utilisée dans le contexte du protocole SSH, nous recommandons le recours à la KDF SSH, conformément au document NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.7 KDF avec protocole de transport en temps réel sécurisé (SRTP)

Lorsqu'elle est utilisée dans le contexte du protocole de transport en temps réel sécurisé (SRTP pour *Secure Secure Real-time Transport Protocol*), nous recommandons le recours à la KDF SRTP, conformément au document NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.8 KDF avec module de plateforme fiable (TPM)

Lorsqu'elle est utilisée dans le contexte d'une session de module de plateforme fiable (TPM pour *Trusted Platform Module*), nous recommandons le recours à la KDF TPM, conformément au document NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.9 Fonction de dérivation de clés basée sur des mots de passe (PBKDF)

Pour assurer la protection des données sur des dispositifs de stockage, nous recommandons l'utilisation de la fonction de dérivation de clés basée sur des mots de passe (PBKDF pour *Password-Based Key Derivation Function*), conformément au document NIST SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications [26] à l'aide d'un mot de passe contenant au moins 12 caractères. Pour de plus amples renseignements sur les mots de passe et les phrases de passe, voir Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) [27].

10 Modes de fonctionnement des enveloppements de clé

Les sections suivantes décrivent les modes de fonctionnement des enveloppements de clé que nous recommandons pour protéger la confidentialité et l'intégrité des clés cryptographiques servant à la protection d'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Nous précisons également un mode de fonctionnement à enveloppement de clé qui a été recommandé dans une version antérieure de cette publication, mais qui aurait dû être abandonné avant la fin de 2023.

10.1 Enveloppement de clé AES (KW)

Lorsque l'entrée est toujours un multiple de 64 bits, nous recommandons l'utilisation du mode d'enveloppement de clé AES avec remplissage (KW pour K*ey Wrap*), conformément au document Key NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping [28].

10.2 Enveloppement de clé AES avec remplissage (KWP)

Lorsque l'entrée n'est pas un multiple de 64 bits, nous recommandons l'utilisation du mode d'enveloppement de clé AES avec remplissage (KWP pour *Key Wrap with Padding*), conformément au document NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping [28].

10.3 Enveloppement de clé avec chiffrement de données triple (TKW)

L'utilisation de l'algorithme TKW aurait dû être abandonnée avant la fin de 2023.

Nous ne recommandons plus l'utilisation du mode d'enveloppement de clé avec chiffrement de données triple (TKW pour *Triple Data Encryption Algorithm Key Wrap*), conformément au document NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation:Methods for Key Wrapping [28]. Ce mode était auparavant approuvé avec une clé d'une longueur de 168 bits.

11 Générateurs de bits aléatoires déterministes (DRBG)

Nous recommandons l'utilisation des générateurs de bits aléatoires déterministes (DRBG pour *Deterministic Random Bit Generators)*, conformément au document NIST SP 800-90A Revision 1:Recommendation for Random Number Generation Using Deterministic Random Bit Generators [29] pour produire des bits aléatoires aux fins d'applications cryptographiques, en vue de protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B :

- Hash_DRBG
- HMAC_DRBG
- CTR_DRBG

La valeur d'amorçage pour un DRBG devrait comporter une entropie ayant été évaluée à au moins 112 bits de longueur. Nous recommandons l'ajout périodique d'une entropie au DRBG par la fonction de reconversion (*reseed function*).

L'entropie évaluée de la diversification initiale pour un DRBG devrait être augmentée à au moins 128 bits d'ici la fin de 2030.

12 Programmes d'assurance des technologies commerciales

Outre l'utilisation recommandée dans ce document des algorithmes cryptographiques, des paramètres et des longueurs de clé pour assurer un niveau adéquat de sécurité cryptographique, nous recommandons également ce qui suit en ce qui concerne la mise en œuvre de programmes d'assurance :

1. Les mises en œuvre d'algorithmes cryptographiques devraient être testées et validées en vertu du Programme de validation des algorithmes cryptographiques (CAVP pour *Cryptographic Algorithm Validation Program* [30].
2. Les essais et la validation des modules cryptographiques devraient être réalisés en vertu du Programme de validation des modules cryptographiques (PVMC) [31] pour évaluer la conformité à la norme FIPS 140-3: Security Requirements for Cryptographic Modules [32].
3. Les produits de sécurité des technologies de l'information devraient être évalués et certifiés comme étant conformes aux Critères communs [33] par un Schéma d'autorisation de certification qui est membre de l'Arrangement relatif à la reconnaissance des certificats liés aux Critères communs (ARCC).

Les produits comportant des modules cryptographiques validés en vertu du PVMC sont mentionnés dans les listes de validation des modules du PVMC et sont accompagnés d'un document de politique de sécurité non exclusif provenant du fournisseur (voir Sélection d'un produit validé en vertu du PVMC). Ce document précise la sécurité cryptographique fournie par un module et décrit ses capacités, sa protection et ses contrôles d'accès. Nous recommandons l'utilisation du document de politique de sécurité pour sélectionner des produits de sécurité cryptographique adéquats et pour configurer les produits dans les modes de fonctionnement approuvés par les FIPS, conformément au document Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program [34] pour s'assurer que seuls des algorithmes approuvés par le Centre pour la cybersécurité sont utilisés.

13 Préparation à la cryptographie post-quantique

Les ordinateurs quantiques menacent de percer les cryptosystèmes à clé publique et d'affaiblir les cryptosystèmes symétriques que nous utilisons actuellement. Bien que les technologies quantiques ne soient pas encore suffisamment puissantes pour percer la cryptographie recommandée dans cette publication, d'importants travaux de recherche sont réalisés dans ce domaine. En 2016, le NIST a entamé un processus visant à solliciter, à évaluer et à normaliser des algorithmes cryptographiques à clé publique et post-quantiques. En juillet 2022, le NIST a annoncé les sélections initiales aux fins de normalisation [35], et nous prévoyons les inclure dans une mise à jour du présent document, lorsque les normes auront été publiées.

Le NIST devrait achever le premier ensemble de normes en 2024. D'ici là, nous recommandons les étapes de haut niveau suivantes :

- évaluer la sensibilité des renseignements de l'organisation et en déterminer la longévité afin d'identifier les renseignements pouvant être à risque (p. ex. dans le cadre de processus continus d'évaluation des risques);
- passer en revue le budget et le plan de gestion du cycle de vie des TI de l'organisation pour déterminer les mises à jour logicielles et matérielles pouvant s'avérer importantes;
- sensibiliser le personnel à la menace quantique;
- envisager l'utilisation de schémas de signature numérique à hachage dynamique si l'organisation remplit les conditions énumérées. 5.5

Pour obtenir de plus amples renseignements sur la préparation à cet égard, consultez le document Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017) [36].

Les organisations devraient attendre que les normes relatives aux schémas de signature numérique et au chiffrement à clé publique post-quantiques soient diffusées avant d'utiliser un algorithme projeté pour protéger les renseignements ou les systèmes.

14 Résumé

La cryptographie fournit des mécanismes de sécurité servant à protéger l'authenticité, la confidentialité et l'intégrité de l'information sensible. Plusieurs algorithmes peuvent s'avérer nécessaires pour satisfaire aux exigences de sécurité, et le respect de toutes ces exigences exige parfois la mise en œuvre de chacun de ces algorithmes. La présente publication offre des directives sur l'utilisation des algorithmes cryptographiques recommandés par le Centre pour la cybersécurité pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

15 Contenu complémentaire

15.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
AES	Algorithme de chiffrement avancé (Advanced Encryption Standard)
CAMC	Code d'authentification de message basé sur le chiffrement (Cipher-based Message Authentication Code)
CAVP	Programme de validation des algorithmes cryptographiques (Cryptographic Algorithm Validation Program)
CBC	Chiffrement par chaînage de blocs (Cipher Block Chaining)
CCM	Code d'authentification de message avec chiffrement par chaînage de blocs (Cipher Block Chaining Message Authentication Code)
CDH	Diffie-Hellman avec cofacteur (Cofactor Diffie-Hellman)
CFB	Chiffrement à rétroaction (Cipher Feedback)
CS	Vol de texte chiffré (Ciphertext Stealing)
CST	Centre de la sécurité des télécommunications
CTR	Compteur (Counter)
DH	Diffie-Hellman
DRBG	Générateur de bits aléatoires déterministe (Deterministic Random Bit Generator)
DSA	Algorithme de signature numérique (Digital Signature Algorithm)
ECB	Carnet de codage électronique (Electronic Codebook)
ECC	Cryptographie à courbe elliptique (Elliptic Curve Cryptography)
ECDSA	Algorithme de signature numérique à courbe elliptique (Elliptic Curve Digital Signature Algorithm)
EMR	Évaluation des menaces et des risques
FFC	Cryptographie à corps fini (Finite Field Cryptography)
FIPS	Federal Information Processing Standards
GC	Gouvernement du Canada
GCM	Mode Galois/compteur (Galois/Counter Mode)
GMAC	Code d'authentification de message avec le mode Galois/compteur (Galois/Counter Mode Message Authentication Code)
HMAC	Code d'authentification de message avec hachage de clé (Keyed-Hash Message Authentication Code)
IETF	Internet Engineering Task Force
IKE	Échange de clés Internet (Internet Key Exchange)
ITSG	Conseils en matière de sécurité des technologies de l'information (Information Technology Security Guidance)

Abréviation, acronyme ou sigle	Définition
ITSP	Conseils en matière de sécurité des technologies de l'information pour les praticiens (Information Technology Security Guidance for Practitioners)
KDF	Fonction de dérivation de clés (Key Derivation Function)
KMAC	KECCAK Code d'authentification de message (Message Authentication Code)
KW	Enveloppement de clé (Key Wrap)
KWP	Enveloppement de clé avec remplissage (Key Wrap with Padding)
MAC	Code d'authentification de message (Message Authentication Code)
MQV	Menezes-Qu-Vanstone
NIST	National Institute of Standards and Technology
OFB	Chiffrement à rétroaction de sortie (Output Feedback)
PMVC	Programme de validation des modules cryptographiques
PRF	Fonction pseudo-aléatoire (Pseudorandom Function)
RFC	Demande de commentaires (Request for Comments)
RSA	Rivest-Shamir-Adleman
SHA	Algorithme de hachage sécurisé (Secure Hash Algorithm)
SP	Publication spéciale (Special Publication)
SRTP	Protocole de transport en temps réel sécurisé (Secure Real-Time Transport Protocol)
SSH	Protocole SSH (Secure Shell)
SCT	Secrétariat du Conseil du Trésor du Canada
STI	Sécurité des technologies de l'information
TDEA	Algorithme de chiffrement de données triple (Triple Data Encryption Algorithm)
TI	Technologies de l'information
TKW	Enveloppement de clé avec chiffrement de données triple (Tripe Data Encryption Algorithm Key Wrap)
TLS	Protocole de sécurité de la couche transport (Transport Layer Security)
TPM	Module de plateforme de confiance (Trusted Platform Module)
XOF	Fonction de hachage extensible (eXtendable Output Function)

15.2 Glossaire

Terme	Définition
Authentification	Mesure de sécurité destinée à protéger un système contre les transmissions ou les imitations frauduleuses en établissant la validité d'une transmission, d'un message ou d'un expéditeur.

Terme	Définition
Authenticité	Fait d'être authentique, vérifiable et fiable; confiance dans la validité d'une transmission, d'un message ou de l'expéditeur d'un message.
Chiffrement	Transformation de données lisibles en une séquence de caractères illisibles à l'aide d'un processus de codage réversible.
Code d'authentification de message	Étiquette de longueur fixe utilisée pour vérifier l'authenticité et l'intensité d'un message.
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés.
Cryptographie	Discipline qui traite des principes, des moyens et des méthodes permettant de rendre des renseignements inintelligibles et de reconvertir des renseignements inintelligibles en renseignements cohérents.
Déchiffrement	Conversion en clair de données chiffrées par l'opération inverse du chiffrement.
Disponibilité	Fait d'être accessible et utilisable intégralement et en temps opportun.
Enveloppement de clé	Mode de fonctionnement utilisé pour chiffrer des clés cryptographiques, et approuvé pour assurer l'authenticité et l'intégrité.
Établissement de clés	Procédure qui permet à des participants multiples de créer ou d'obtenir des secrets partagés, comme des clés cryptographiques.
Fonction de hachage extensible (eXtendable Output Function	Procédure permettant de transformer un message de longueur arbitraire en une sortie pouvant atteindre n'importe quelle longueur désirée. Une extension XOF sécurisée devrait répondre à des propriétés additionnelles, comme la « résistance aux collisions », en vertu de laquelle il est impossible de trouver des messages précis ayant la même sortie.
Federal Information Processing Standards (FIPS) Publication 140-3	Une publication précisant les exigences de sécurité qui seront satisfaites par un module cryptographique utilisé dans un système de sécurité protégeant l'information protégée. Ces exigences couvrent onze classes de fonctionnalité liées à la conception et à la mise en œuvre d'un module cryptographique.
Fonction de dérivation de clés	Transformation de données secrètes (et possiblement de données non secrètes) en clés secrètes robustes sur le plan cryptographique.
Fonction de hachage	Procédure permettant de transformer un message de longueur arbitraire en un message condensé de longueur fixe. Une fonction de hachage (cryptographique) sécurisé devrait répondre à des propriétés additionnelles, comme la « résistance aux collisions », en vertu de laquelle il est impossible de trouver des messages précis ayant le même condensé.
Générateur de bits aléatoires déterministe (DRBG)	Un générateur de bits aléatoires produit une séquence de bits (0 ou 1) qui semble statistiquement indépendante et non biaisée. En se basant sur une entrée identique, un générateur de bits aléatoires déterministe produit toujours la même séquence de sortie.
Gestion des clés	Procédures et mécanismes pour la génération, la diffusion, le remplacement, le stockage, l'archivage et la destruction de clés qui contrôlent les processus de chiffrement ou d'authentification.
Information classifiée	Toute information liée à l'intérêt national et qui pourrait faire l'objet d'une exception ou d'une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, mais dont la compromission, selon toute vraisemblance, porterait atteinte à l'intérêt national.
Intégrité	Exactitude et intégralité de l'information et des biens, et authenticité des transactions.

Terme	Définition
Module cryptographique	Ensemble de matériel informatique, de logiciels et/ou de micrologiciels appliquant des fonctions de sécurité cryptographique (y compris des algorithmes cryptographiques et la génération de clés) et qui est contenu dans le périmètre cryptographique.
Mode de fonctionnement	Procédure servant à utiliser un algorithme de chiffrement, parfois à une fin particulière (comme l'enveloppement de clé).
Non-répudiation	Mesure conçue pour offrir une protection contre toute personne niant de façon mensongère avoir effectué une action.
Programme de validation des algorithmes cryptographiques (CAVP)	Programme servant à valider la pertinence fonctionnelle des algorithmes cryptographiques mis en œuvre dans un module cryptographique.
Programme de validation des modules cryptographiques (CMVP)	Programme conjoint du NIST et du Centre pour la cybersécurité servant à valider des modules cryptographiques en vertu de la norme FIPS 140-3, Security Requirements for Cryptographic Modules, et d'autres normes et recommandations cryptographiques du NIST. Le PVMC a évolué à partir de la norme FIPS 140-2.
Signature numérique	Transformation cryptographique des données qui fournit l'intégrité des données et l'authentification de l'origine des données.

15.3 Références

1. Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*, 12 novembre 2012.
2. Conseil du Trésor du Canada. *Ligne directrice sur la définition des exigences en matière d'authentification*, novembre 2012.
3. Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement*, juillet 2019.
4. National Institute of Standards and Technology. *Advanced Encryption Standard*. Federal Information Processing Standards (FIPS) Publication 197, novembre 2001. Mise à jour mai 2023.
5. National Institute of Standards and Technology. *Recommendation for the Triple Data Encryption Algorithm Block Cipher*. Special Publication 800-67 Revision 2, novembre 2017.
6. Adams, C. *The CAST-128 Encryption Algorithm*. Request for Comments (RFC) 2144. Internet Engineering Task Force (IETF), mai 1997.
7. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*. Special Publication 800-38A, décembre 2001.
8. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode.* Addendum to NIST Special Publication 800-38A, octobre 2010.

9. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*. Special Publication 800-38E, janvier 2010.
10. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*. Special Publication 800-38C, mai 2004. Mise à jour juillet 2007.
11. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode*. Special Publication 800-38D, novembre 2017.
12. National Institute of Standards and Technology. *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*. Special Publication 800-56B Revision 2, mars 2019.
13. National Institute of Standards and Technology. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. Special Publication 800-56A Revision 3, avril 2018.
14. National Institute of Standards and Technology. *Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*. Special Publication 800-186, février 2023.
15. National Institute of Standards and Technology. *Digital Signature Standard*. Federal Information Processing Standards (FIPS) Publication 186-4, juillet 2013.
16. National Institute of Standards and Technology. *Digital Signature Standard*. Federal Information Processing Standards (FIPS) Publication 186-5, février 2023.
17. National Institute of Standards and Technology. *Recommendation for Stateful Hash-based Signatures Scheme*. Special Publication 800-208, octobre 2020.
18. National Institute of Standards and Technology. *Secure Hash Standard*. Federal Information Processing Standards (FIPS) Publication 180-4, août 2015.
19. National Institute of Standards and Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Federal Information Processing Standards (FIPS) Publication 202, août 2015.
20. National Institute of Standards and Technology. *The Keyed-Hash Message Authentication Code*. Federal Information Processing Standards (FIPS) Publication 198-1, juillet 2008.
21. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. Special Publication 800-38B, mai 2005. Mise à jour juin 2016.
22. National Institute of Standards and Technology. *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*. Special Publication 800-185, décembre 2016.
23. National Institute of Standards and Technology. *Recommendation for Key Derivation Methods in Key-Establishment Schemes*. Special Publication 800-56C Revision 2, août 2020.
24. National Institute of Standards and Technology. *Recommendation for Key Derivation Using Pseudorandom Functions*. Special Publication 800-108 Revision 1, août 2022.
25. National Institute of Standards and Technology. *Recommendation for Existing Application-Specific Key Derivation Functions*. Special Publication 800-135 Revision 1, décembre 2011.

26. National Institute of Standards and Technology. *Recommendation for Password Based Key Derivation: Part 1: Storage Applications*. Special Publication 800-132, décembre 2010.

27. Centre canadien pour la cybersécurité. *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*, septembre 2019.

28. National Institute of Standards and Technology. *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*. Special Publication 800-38F, décembre 2012.

29. National Institute of Standards and Technology. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. Special Publication 800-90A Revision 1, juin 2015.

30. National Institute of Standards and Technology. *Cryptographic Algorithm Validation Program CAVP*, octobre 2016.

31. National Institute of Standards and Technology. *Cryptographic Module Validation Program CMVP*, octobre 2016.

32. National Institute of Standards and Technology. *Security Requirements for Cryptographic Modules*. Federal Information Processing Standards (FIPS) Publication 140-3, mars 2019.

33. Centre canadien pour la cybersécurité. *Critères communs*, septembre 2018.

34. National Institute of Standards and Technology. *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program*, mars 2023.

35. Centre canadien pour la cybersécurité. *Le NIST sélectionne les mécanismes cryptographiques post-quantiques*, juillet 2022.

36. Centre canadien pour la cybersécurité. *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie - ITSAP.00.017*, février 2021.