Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

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 de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- Courriel : contact@cyber.gc.ca
- Téléphone : 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

La présente publication entre en vigueur le 29 mai 2026.

Historique des révisions

Révision	Modifications	Date
1	Première version	2 août 2016
2	Version 2	17 août 2022
3	Version 3	19 mars 2024
4	Version 4	5 mars 2025
5	Version 5	29 mai 2026

D97-3/40-111-2026F-PDF
ISBN: 978-0-660-99821-3

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. Dans le cas des ministères et des organismes du gouvernement du Canada (GC), les conseils offerts s’appliquent aux documents NON CLASSIFIÉ, PROTÉGÉ A, et PROTÉGÉ B.

Votre organisation doit être en mesure de protéger l’information et les données sensibles pour assurer la prestation de programmes et de services. Une cryptographie adéquatement configurée fournit des mécanismes de sécurité servant à protéger la confidentialité, l’intégrité et l’authenticité de l’information. Plusieurs algorithmes peuvent s’avérer nécessaires pour satisfaire aux exigences de sécurité de votre organisation, et chaque algorithme devrait être choisi et mis en œuvre de manière à respecter ces exigences.

Table des matières

1 Introduction 6

1.1 Remarques à l'intention de la praticienne ou du praticien 6

1.2 Politiques déterminantes 7

1.3 Lien avec le processus de gestion des risques liés aux TI 7

2 Cryptographie post-quantique 10

3 Algorithmes de chiffrement 11

3.1 Algorithme de chiffrement avancé 11

4 Modes de fonctionnement des algorithmes de chiffrement 12

4.1 Protection de la confidentialité de l'information 12

4.2 Protection de la confidentialité et de l'authenticité de l'information 13

5 Mécanisme d'établissement de clé 14

5.1 Rivest Shamir-Adleman 14

5.2 Cryptographie à corps fini de Diffie-Hellman et de Menezes-Qu-Vanstone 14

5.3 Cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur et de Menezes-Qu-Vanstone 14

5.4 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens 15

6 Algorithmes de signature numérique 16

6.1 Rivest-Shamir-Adelman 16

6.2 Algorithme de signature numérique 16

6.3 Algorithme de signature numérique à courbes elliptiques 16

6.4 Algorithme de signature numérique à courbe Edwards 17

6.5 Algorithme de signature numérique basé sur des réseaux euclidiens 17

6.6 Algorithme de signature numérique basé sur un hachage sans état 17

6.7 Algorithmes de signature numérique basés sur un hachage avec état 18

7 Fonctions de hachage 19

7.1 Algorithme de hachage sécurisé 1 (Secure Hash Algorithm-1) 19

7.2 Algorithme de hachage sécurisé 2 (Secure Hash Algorithm-2) 19

7.3 Algorithme de hachage sécurisé 3 (Secure Hash Algorithm-3) 19

8 Fonctions de hachage extensibles 20

8.1 SHAKE 20
9 Codes d'authentification de message 21
9.1 Code d'authentification de message avec hachage de clé 21
9.2 Code d'authentification de message basé sur le chiffrement 21
9.3 Code d'authentification de message avec le mode Galois/compteur 21
9.4 Code d'authentification de message KECCAK 21
10 Fonctions de dérivation de clés 22
10.1 Fonction de dérivation de clés à une étape 22
10.2 Fonction de dérivation de clés à deux étapes 22
10.3 Dérivation de clés au moyen de fonctions pseudo-aléatoires 22
10.4 Fonction de dérivation de clés avec le protocole d'échange de clés Internet version 2 22
10.5 Fonction de dérivation de clés avec le protocole de sécurité de la couche de transport version 1.2 22
10.6 Fonction de dérivation de clés Secure Shell 23
10.7 Fonction de dérivation de clés du protocole de transport sécurisé en temps réel 23
10.8 Fonction de dérivation de clés du module de plateforme sécurisée 23
10.9 Fonction de dérivation de clés basée sur des mots de passe 23
11 Modes de fonctionnement des enveloppements de clé 24
11.1 Enveloppement de clé à norme de chiffrement avancée 24
11.2 Enveloppement de clé à norme de chiffrement avancée avec remplissage 24
12 Générateurs de bits aléatoires 25
13 Programmes d'assurance des technologies commerciales 26
14 Résumé 27

Liste des figures

Figure 1 : Processus de gestion des risques liés à la cybersécurité 7

Liste des annexes

Aucune entrée de table des matières n'a été trouvée.

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 susceptibles de 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 sur les activités opérationnelles et donner lieu à une atteinte à la protection des données ainsi qu'à des pertes financières.

La présente publication aide les praticiennes et praticiens des TI à choisir et à utiliser adéquatement des algorithmes cryptographiques. Lorsqu'ils sont utilisés avec des paramètres de domaine valides et des longueurs de clé particulières, les algorithmes cryptographiques figurant dans cette publication sont des mécanismes cryptographiques recommandés pour protéger l'authenticité, la confidentialité et l'intégrité de l'information sensible NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B associée à un niveau de préjudice moyen, tel qu'il est défini dans le document Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie (ITSP.10.033) 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.

La présente publication complète la Ligne directrice sur la définition des exigences en matière d'authentification du Secrétariat du Conseil du Trésor du Canada (SCT). Chaque organisation est responsable de déterminer ses objectifs et exigences en matière de sécurité dans son cadre de gestion des risques.

1.1 Remarques à l'intention de la praticienne ou du praticien

Dans la présente publication, le Centre pour la cybersécurité fait des recommandations relatives aux algorithmes et aux paramètres cryptographiques. Le Centre pour la cybersécurité dresse également une liste des algorithmes qui devraient être mis hors service. Ainsi, les nouvelles applications ne devraient pas utiliser ces algorithmes. Lorsque ces algorithmes sont utilisés dans des applications existantes, ils devraient être remplacés par des algorithmes recommandés dans la présente publication. Dans le cas de certains algorithmes, le Centre pour la cybersécurité précise une date à laquelle les organisations devraient les remplacer. Dans d'autres cas, les organisations devraient remplacer ces algorithmes le plus rapidement possible.

Si un algorithme nécessite une primitive, les organisations devraient choisir l'un des algorithmes recommandés dans la présente publication, sauf indication contraire. Par exemple, une fonction de hachage énoncée à la section 7.2 Algorithme de hachage sécurisé-2 devrait être utilisée avec le code d'authentification de message avec hachage de clé (HMAC pour *Hash-Based Message Authentication Code*) mentionné à la section 9.1 Code d'authentification de message avec hachage de clé. Lorsqu'un algorithme nécessite un paramètre, les organisations devraient choisir parmi ceux qui sont recommandés dans la référence donnée pour l'algorithme, sauf indication contraire.

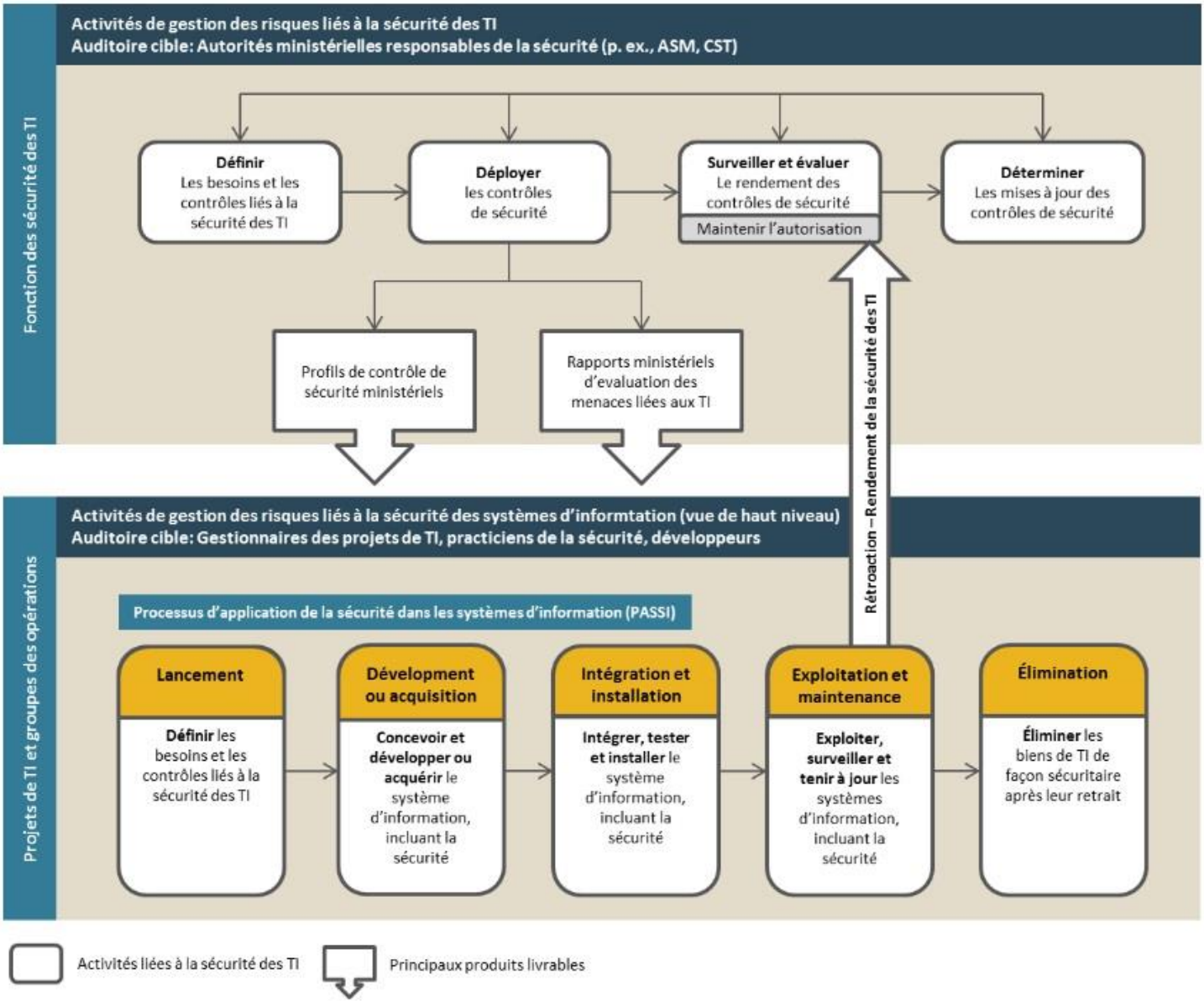
1.2 Politiques déterminantes

Résoudre et contrer les cybermenaces et les vulnérabilités auxquelles font face les réseaux sont des étapes cruciales pour sécuriser les réseaux, les données et les biens. Les ministères du GC doivent veiller à mettre en œuvre les politiques et procédures en matière de sécurité des TI conformément à la *Politique sur la sécurité du gouvernement*.

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

Les lignes directrices contenues dans le document Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie (ITSP.10.033) du Centre pour la cybersécurité recommandent que les organisations entreprennent des activités à deux niveaux organisationnels : au niveau du ministère et au niveau du système d'information.

Figure 1 : Processus de gestion des risques liés à la cybersécurité



Description longue – Figure 1 : Processus de gestion des risques liés à la sécurité des TI

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.

Au niveau du ministère, voici quelques activités de gestion des risques liés à la sécurité des TI menées par les autorités ministérielles responsables de la sécurité (par exemple, l'ASM, le CSTI) :

- Définir les besoins et les contrôles liés à la sécurité des TI.
- Déployer les contrôles de sécurité.
- Surveiller et évaluer le rendement des contrôles de sécurité, puis maintenir l'autorisation.
- Déterminer les mises à jour des contrôles de sécurité.

Les principaux produits livrables associés au déploiement des contrôles de sécurité sont les profils de contrôle de sécurité ministériels et les rapports ministériels d'évaluation des menaces liées aux TI. Ces livrables constituent des éléments clés des activités de gestion des risques liés à la sécurité au niveau des systèmes d'information.

Au niveau des systèmes d'information, voici quelques activités de gestion des risques liés à la sécurité des TI menées par les gestionnaires de projets de TI, les praticiens de la sécurité et les développeurs :

- Définir les besoins et les contrôles liés à la sécurité des TI.
- Concevoir et développer ou acquérir le système d'information, incluant la sécurité.
- Intégrer, tester et installer le système d'information, incluant la sécurité.
- Exploiter, surveiller et tenir à jour les systèmes d'information, incluant la sécurité.
- Éliminer les biens de TI de façon sécuritaire après leur retrait.

L'information découlant des activités opérationnelles et des activités liées à la maintenance contribue à la réalisation des activités de surveillance et d'évaluation au niveau organisationnel. La rétroaction sur le rendement de la sécurité des TI soutient l'activité liée au maintien de l'autorisation dans le cadre de la surveillance et de l'évaluation.

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 devraient être pris en compte dans le cadre des activités de définition, de déploiement, de surveillance et d'évaluation du processus de gestion des risques. Ces activités sont décrites en détail à l'Annexe 1 – Activités de gestion des risques liés à la sécurité des IT (ITSG-33).

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 les contrôles de sécurité appropriés et les exploiter comme prévu;
- évaluer en permanence le rendement des contrôles de sécurité existants, faire rapport du rendement et prendre les mesures appropriées pour corriger toute lacune relevée.

Les algorithmes cryptographiques devraient 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).

2 Cryptographie post-quantique

En août 2024, le National Institute of Standards and Technology (NIST) des États-Unis a publié des normes pour trois algorithmes post-quantiques qui sont sûrs contre les attaques connues menées au moyen d'un ordinateur quantique :

- le mécanisme d'encapsulation de clés basé sur des réseaux euclidiens (ML-KEM pour *Module-Lattice-Based Key-Encapsulation Mechanism*) (voir la section 5.4 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens);
- l'algorithme de signature numérique basé sur des réseaux euclidiens (ML-DSA pour *Module-Lattice-Based Digital Signature Algorithm*) (voir la section 6.5 Algorithme de signature numérique basé sur des réseaux euclidiens;
- l'algorithme de signature numérique basé sur un hachage sans état (SLH-DSA pour *Stateless Hash-Based Digital Signature Algorithm*) (voir la section 6.6 Algorithme de signature numérique basé sur un hachage sans état).

Le ML-KEM établit le matériel de clé partagée entre deux parties sur un canal public. Il remplacera les mécanismes d'établissement de clés dans les sections 5.1 Rivest Shamir-Adleman, 5.2 Cryptographie à corps fini de Diffie-Hellman et de Menezes-Qu-Vanstone et 5.3 Cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur et de Menezes-Qu-Vanstone pour la plupart des cas d'utilisation.

ML-DSA et SLH-DSA sont des algorithmes de signature numérique. Le ML-DSA est un algorithme de signature numérique basé sur des réseaux d'usage général. Il remplacera les algorithmes de signature numérique dans les sections 6.1 Rivest-Shamir-Adelman à 6.4 Algorithme de signature numérique à courbe Edwards pour la plupart des cas d'utilisation. Les signatures basées sur le hachage, y compris les algorithmes de signature numérique post-quantique basés sur un hachage avec état et SLH-DSA, reposent sur un problème mathématique différent de ML-DSA. Les algorithmes de signature numérique basés sur un hachage avec état comportent un niveau supplémentaire de complexité dans la mesure où les mises en œuvre de la génération de signature doivent gérer avec soin un état interne. Une mauvaise gestion peut entraîner une perte complète de sécurité. L'algorithme SLH-DSA ne nécessite pas de gestion des états, mais il offre un rendement inférieur et des signatures encore plus volumineuses que les algorithmes ML-DSA et que les algorithmes de signature numérique basés sur un hachage avec état.

Les organisations internationales de normalisation intègrent ces nouveaux algorithmes post-quantiques dans les protocoles réseau. À mesure que de nouvelles normes de protocole sont disponibles, la publication Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) du Centre pour la cybersécurité sera mise à jour pour inclure les configurations post-quantiques. Pour obtenir de plus amples renseignements sur la préparation à cet égard, prière de consulter le document Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017).

Cette version de l'ITSP.40.111 comprend de nouvelles dates de retrait définitif pour les mécanismes d'établissement de clés et les algorithmes de signature numérique vulnérables à l'informatique quantique.

Les organisations ne devraient utiliser que des algorithmes de signature numérique et de chiffrement à clé publique post-quantiques qui sont conformes aux normes finales publiées (comme il est indiqué dans la présente publication) pour protéger l'information ou les systèmes.

3 Algorithmes de chiffrement

La section suivante décrit les algorithmes de chiffrement recommandés pour protéger la confidentialité de l'information NON CLASSIFIÉ, PROTÉGÉ A, et PROTÉGÉ B.

3.1 Algorithme de chiffrement avancé

Le Centre pour la cybersécurité recommande l'algorithme AES (Advanced Encryption Standard), conformément aux normes FIPS (Federal Information Processing Standards) du NIST énoncées dans le document Information Processing Standards Publication 197: Advanced Encryption Standard (en anglais seulement) avec une longueur de clé de 128, 192 ou 256 bits.

4 Modes de fonctionnement des algorithmes de chiffrement

La section suivante décrit les modes de fonctionnement des algorithmes de chiffrement que le Centre pour la cybersécurité recommande d'utiliser avec l'algorithme AES, conformément à la section 3.1 Algorithme de chiffrement avancé.

4.1 Protection de la confidentialité de l'information

Le Centre pour la cybersécurité recommande 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 Special Publication (SP) 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques (en anglais seulement) :

- le mode de chiffrement par carnet de codage électronique (ECB pour *Electronic Codebook*) 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 11 Modes de fonctionnement des enveloppements de clé). Il ne devrait pas être utilisé pour le chiffrement de données en masse;
- le mode de chiffrement à rétroaction (CFB pour *Cipher Feedback*);
- le mode de chiffrement à rétroaction de sortie (OFB pour *Output Feedback*);
- le mode de chiffrement basé sur un compteur (CTR pour *Counter*);
- le 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 comme il est décrit dans l'annexe A du document NIST 800-38A (en anglais seulement). Les protocoles précisent habituellement les méthodes particulières de remplissage pouvant être utilisées;
    - si aucune méthode de remplissage n'est précisée, le Centre pour la cybersécurité recommande les méthodes suivantes tirées du document *NIST Special Publication (SP) 800-38A Addendum* (en anglais seulement) :
        - CBC-CS1;
        - CBC-CS2;
        - CBC-CS3.

Le document NIST SP 800-38A fait mention de plusieurs exigences importantes :

- les modes CBC et CFB nécessitent des motifs d'initialisation (IV pour *Initialization Vectors*) 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, le Centre pour la cybersécurité recommande 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 (en anglais seulement).

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

Le Centre pour la cybersécurité recommande 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 (en anglais seulement);
- mode Galois/compteur (GCM pour *Galois/Counter Mode*), conformément au document NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (en anglais seulement).

5 Mécanisme d'établissement de clé

Un mécanisme d'établissement de clé est une procédure qui permet à des participantes et participants multiples de créer ou d'obtenir des secrets partagés, comme des clés cryptographiques. La section suivante décrit les mécanismes d'établissement de clés que le Centre pour la cybersécurité recommande d'utiliser avec les algorithmes cryptographiques pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

5.1 Rivest Shamir-Adleman

Le Centre pour la cybersécurité recommande les schémas de négociation et de transport de clés basés sur l'algorithme Rivest-Shamir-Adleman (RSA), conformément au document NIST SP 800-56B Rev 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography (en anglais seulement) avec un module de chiffrement RSA (en anglais *RSA modulus*) de taille d'au moins 2048 bits.

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

L'utilisation de l'algorithme RSA sans mécanisme d'établissement de clés post-quantique devrait être abandonnée d'ici la fin de 2035.

5.2 Cryptographie à corps fini de Diffie-Hellman et de Menezes-Qu-Vanstone

Le Centre pour la cybersécurité recommande 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 taille-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 (en anglais seulement). La cardinalité du corps (paramètre du module premier, en anglais *field size* ou *prime modulus parameter*) devrait être au moins 2048 bits.

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

L'utilisation de l'algorithme FFC DH et FFC MQV sans mécanisme d'établissement de clés post-quantique devrait être abandonnée d'ici la fin de 2035.

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

Le Centre pour la cybersécurité recommande les schémas de négociation de clés basés sur la cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur (ECC CDH pour *Elliptic Curve Cryptography Cofactor Diffie-Hellman*) et ECC MQV, conformément au document NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (en anglais seulement). Le Centre pour la cybersécurité recommande les courbes elliptiques suivantes, conformément au document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography:Elliptic Curve Domain Parameters (en anglais seulement) :

- 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. Le Centre pour la cybersécurité ne recommande plus l'utilisation des courbes binaires, conformément à l'annexe D du document NIST FIPS 186-4:Digital Signature Standard (en anglais seulement).

L'utilisation de toutes les courbes binaires devrait être abandonnée d'ici la fin de 2030. Une liste des courbes dont l'utilisation sera abandonnée se trouve à la section 3.3 du document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters (en anglais seulement).

L'utilisation de l'algorithme ECC CDH et ECC MQV sans mécanisme d'établissement de clés post-quantique devrait être abandonnée d'ici la fin de 2035.

5.4 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens

Le Centre pour la cybersécurité recommande le mécanisme d'encapsulation de clés basé sur des réseaux euclidiens (ML-KEM pour *Module-Lattice-Based Key-Encapsulation Mechanism*) comme mécanisme d'établissement de clé post-quantique d'usage général, tel qu'il est précisé dans le document NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (en anglais seulement) avec les paramètres suivants :

- ML-KEM-512
- ML-KEM-768
- ML-KEM-1024

6 Algorithmes de signature numérique

La section suivante décrit les algorithmes que le Centre pour la cybersécurité recommande 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. Le Centre pour la cybersécurité précise également un algorithme de signature numérique qui a été recommandé dans une version antérieure de cette publication, mais qui devrait être abandonné avant la fin de 2030.

6.1 Rivest-Shamir-Adelman

Le Centre pour la cybersécurité recommande 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 (en anglais seulement) avec module de chiffrement RSA de taille d'au moins 2048 bits.

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

L'utilisation de l'algorithme RSA sans algorithme de signature numérique post-quantique devrait être abandonnée d'ici la fin de 2035.

6.2 Algorithme de signature numérique

L'utilisation de l'algorithme de signature numérique (DSA pour *Digital Signature Algorithm*) devrait être abandonnée d'ici la fin de 2030.

Le Centre pour la cybersécurité ne recommande plus l'utilisation de l'algorithme DSA conformément au document NIST FIPS 186-4: Digital Signature Standard (en anglais seulement) pour les nouvelles applications. Les applications existantes doivent utiliser des paramètres de domaine valides pour un corps avec cardinalité (paramètre du module premier, en anglais *field size* ou *prime modulus parameter*) d'au moins 2048 bits.

6.3 Algorithme de signature numérique à courbes elliptiques

Le Centre pour la cybersécurité recommande l'utilisation de l'algorithme de signature numérique à courbe elliptique (ECDSA pour *Elliptic Curve Digital Signature Algorithm*) et de l'algorithme ECDSA déterministe[1], conformément au document NIST FIPS 186-5:Digital Signature Standard (en anglais seulement). Le Centre pour la cybersécurité recommande les courbes elliptiques suivantes, conformément au document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography:Elliptic Curve Domain Parameters (en anglais seulement) :

- Courbe P-224
- Courbe P-256

[1] Selon ce qu'indique le document NIST SP 800-186 (en anglais seulement), l'algorithme ECDSA déterministe est une variante de l'algorithme ECDSA, dans laquelle un numéro secret par message est généré pour faire partie du message signé, ce qui se traduit par un mappage déterministe pour fournir des signatures de mappage. La vérification de la signature dans l'algorithme ECDSA déterministe se fait de la même façon que pour l'algorithme ECDSA.

- Courbe P-384
- Courbe P-521

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

Le Centre pour la cybersécurité ne recommande plus l'utilisation des courbes binaires, conformément à l'annexe D du document NIST FIPS 186-4:Digital Signature Standard (en anglais seulement).

L'utilisation de toutes les courbes binaires devrait être abandonnée d'ici la fin de 2030. Une liste des courbes dont l'utilisation sera abandonnée se trouve à la section 3.3 du document NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters (en anglais seulement).

L'utilisation de l'algorithme ECDSA sans algorithme de signature numérique post-quantique devrait être abandonnée d'ici la fin de 2035.

6.4 Algorithme de signature numérique à courbe Edwards

Le Centre pour la cybersécurité recommande 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 (en anglais seulement) avec les courbes elliptiques suivantes précisées dans le document NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography:Elliptic Curve Domain Parameters (en anglais seulement) :

- Edwards25519
- Edwards448

Le Centre pour la cybersécurité ne recommande pas la version préhachage HashEdDSA.

L'utilisation de l'algorithme EdDSA sans algorithme de signature numérique post-quantique devrait être abandonnée d'ici la fin de 2035.

6.5 Algorithme de signature numérique basé sur des réseaux euclidiens

Le Centre pour la cybersécurité recommande l'algorithme de signature numérique basé sur des réseaux euclidiens (ML-DSA pour *Module-Lattice-Based Digital Signature Algorithm*) comme algorithme de signature numérique post-quantique d'usage général, tel qu'il est précisé dans le document NIST FIPS 204: Module-Lattice-Based Digital Signature Standard (en anglais seulement) avec les paramètres suivants :

- ML-DSA-44
- ML-DSA-65
- ML-DSA-87

6.6 Algorithme de signature numérique basé sur un hachage sans état

Le Centre pour la cybersécurité recommande l'algorithme de signature numérique basé sur un hachage sans état (SLH-DSA pour *Stateless Hash-Based Digital Signature Algorithm*) comme algorithme de signature numérique post-quantique, tel qu'il est précisé dans le document NIST FIPS 205: Stateless Hash-Based Digital Signature Standard (en anglais seulement) avec les paramètres suivants :

- SLH-DSA-SHA2-128s
- SLH-DSA-SHAKE-128s
- SLH-DSA-SHA2-128f
- SLH-DSA-SHAKE-128f
- SLH-DSA-SHA2-192s
- SLH-DSA-SHAKE-192s
- SLH-DSA-SHA2-192f
- SLH-DSA-SHAKE-192f
- SLH-DSA-SHA2-256s
- SLH-DSA-SHAKE-256s
- SLH-DSA-SHA2-256f
- SLH-DSA-SHAKE-256f

6.7 Algorithmes de signature numérique basés sur un hachage avec état

Les algorithmes de signature basés sur un hachage avec état sont une autre famille d'algorithmes de signature numérique post-quantiques. La mise en œuvre de la génération de signature pour des algorithmes de signature numérique basés sur un hachage avec état doit gérer judicieusement un état interne. Il s'agit d'une complexité supplémentaire en comparaison à d'autres types d'algorithmes de signature numérique. Une mauvaise gestion de l'état interne peut entraîner une perte complète de sécurité. Le Centre pour la cybersécurité recommandait auparavant d'utiliser les signatures numériques basées sur un hachage avec état lorsque certaines conditions s'appliquaient, notamment lorsqu'un algorithme de chiffrement post-quantique devait être mis en œuvre avant que des algorithmes de signature post-quantiques d'usage général soient normalisés. Même si les algorithmes de signature numérique basés sur un hachage avec état peuvent quand même être utilisés, les algorithmes de signature numérique post-quantique nouvellement normalisés ML-DSA et SLH-DSA ne nécessitent pas de gestion des états (sections 6.5 Algorithme de signature numérique basé sur des réseaux euclidiens et 6.6 Algorithme de signature numérique basé sur un hachage sans état) et ils peuvent être utilisés dans la plupart des cas où un algorithme de signature numérique est nécessaire. Les signatures numériques basées sur un hachage avec état ne devraient être utilisées que lorsque la ou le signataire n'a pas à produire rapidement des signatures et est en mesure de protéger et de gérer un état de clé privée.

Si vous utilisez des signatures numériques basées sur un hachage avec état, le Centre pour la cybersécurité recommande les algorithmes de signature numérique post-quantiques suivants, comme il est précisé dans le document NIST SP 800-208: Recommendation for Stateful Hash-based Signatures Scheme (en anglais seulement), à l'aide d'une des fonctions de hachage SHA-256, SHA-256/192, SHAKE256/256 ou SHAKE256/192, conformément à la section 2.3 du document NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes (en anglais seulement).

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

7 Fonctions de hachage

Une fonction de hachage est une procédure permettant de transformer un message de longueur arbitraire en une sortie, appelée « signature », 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. La section suivante décrit les fonctions de hachage recommandées pour une utilisation avec les algorithmes cryptographiques précisés dans la présente publication pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

7.1 Algorithme de hachage sécurisé 1 (Secure Hash Algorithm-1)

Le Centre pour la cybersécurité ne recommande plus l'utilisation de l'algorithme de hachage sécurisé-1 (SHA-1) conformément au document NIST FIPS 180-4:Secure Hash Standard (en anglais seulement). Son utilisation était auparavant approuvée avec les codes d'authentification de message avec hachage de clé, les fonctions de dérivation de clés (KDF pour *Key Derivation Functions*) et les générateurs de bits aléatoires (RBG pour *Random Bit Generator*).

L'algorithme SHA-1 ne doit pas être utilisé avec des algorithmes de signature numérique ou avec toute application nécessitant une résistance aux collisions. L'utilisation de cet algorithme devrait être abandonnée avec les codes d'authentification de message avec hachage de clé, les KDF et les RBG.

7.2 Algorithme de hachage sécurisé 2 (Secure Hash Algorithm-2)

Le Centre pour la cybersécurité recommande 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 (en anglais seulement) pour les algorithmes de signature numérique, les codes d'authentification de message avec hachage de clé, les fonctions KDF et les RBG. La fonction de hachage tronqué SHA-256/192 précisée dans le document NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes (en anglais seulement) n'est recommandée que pour un usage avec les algorithmes de signature numérique basés sur un hachage avec état indiqués dans la section 6.7 Algorithmes de signature numérique basés sur un hachage avec état.

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

7.3 Algorithme de hachage sécurisé 3 (Secure Hash Algorithm-3)

Le Centre pour la cybersécurité recommande 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 (en anglais seulement), pour les algorithmes de signature numérique, les codes d'authentification de message avec hachage de clé, les fonctions KDF et les RBG.

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

8 Fonctions de hachage extensibles

Une fonction de hachage extensible est une procédure permettant de transformer un message de longueur arbitraire en une sortie pouvant atteindre n'importe quelle longueur désirée. Une fonction de hachage extensible 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. La section suivante décrit deux fonctions de hachage extensibles que le Centre pour la cybersécurité recommande d'utiliser avec les algorithmes cryptographiques sélectionnés qui ont été précisés dans la présente publication pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

8.1 SHAKE

Le Centre pour la cybersécurité recommande l'utilisation de l'algorithme SHAKE128, conformément au document NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions (en anglais seulement) dans ce qui suit :

- ML-KEM (section 5.4 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens)
- Les algorithmes de signature numérique
  - RSA (section 6.1 Rivest-Shamir-Adelman)
  - ECDSA (section 6.3 Algorithme de signature numérique à courbes elliptiques)
  - ML-DSA (section 6.5 Algorithme de signature numérique basé sur des réseaux euclidiens)
- Code d'authentification de message (KECCAK pour *Message Authentication Code* ou KMAC) (section 9.4 KECCAK Code d'authentification de message)

Le Centre pour la cybersécurité recommande l'utilisation de l'algorithme SHAKE256, conformément au document NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions (en anglais seulement) dans ce qui suit :

- ML-KEM (section 5.4 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens)
- Les algorithmes de signature numérique
  - RSA (section 6.1 Rivest-Shamir-Adelman)
  - ECDSA (section 6.3 Algorithme de signature numérique à courbes elliptiques)
  - EdDSA (section 6.4 Algorithme de signature numérique à courbe Edwards) avec courbe Edwards448
  - ML-DSA (section 6.5 Algorithme de signature numérique basé sur des réseaux euclidiens)
  - SLH-DSA (section 6.6 Algorithme de signature numérique basé sur un hachage sans état)
  - Algorithmes de signature numérique basés sur un hachage avec état (section 6.7 Algorithmes de signature numérique basés sur un hachage avec état)
- KMAC (section 9.4 KECCAK Code d'authentification de message)

9 Codes d'authentification de message

Un code d'authentification de message (MAC pour *Message Authentication Code*) est une étiquette de longueur fixe utilisée pour vérifier l'authenticité et l'intégrité d'un message. Les sections suivantes décrivent les algorithmes MAC que le Centre pour la cybersécurité recommande pour l'intégrité des données et l'authentification de l'origine des données pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

9.1 Code d'authentification de message avec hachage de clé

Le Centre pour la cybersécurité recommande 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 (en anglais seulement) avec une clé d'une longueur d'au moins 112 bits.

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

9.2 Code d'authentification de message basé sur le chiffrement

Le Centre pour la cybersécurité recommande 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 (en anglais seulement). L'utilisation du code CMAC n'est recommandée qu'avec l'algorithme AES, conformément à la section 3.1 Algorithme de chiffrement avancé.

9.3 Code d'authentification de message avec le mode Galois/compteur

Le Centre pour la cybersécurité recommande 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 (GCM) and GMAC (en anglais seulement). L'utilisation du code GMAC n'est recommandée qu'avec l'algorithme AES, conformément à la section 3.1 Algorithme de chiffrement avancé.

9.4 Code d'authentification de message KECCAK

Le Centre pour la cybersécurité recommande l'utilisation du code d'authentification de message KECCAK (KMAC 128 et KMAC 256), conformément au document NIST SP 800-185: SHA3-Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash (en anglais seulement) avec une clé d'une longueur d'au moins 112 bits.

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

10 Fonctions de dérivation de clés

Une fonction de dérivation de clés (KDF pour *Key Derivation Function*) est une transformation de données secrètes (et possiblement de données non secrètes) en clé secrète robuste sur le plan cryptographique. Les sections suivantes décrivent les KDF que le Centre pour la cybersécurité recommande 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.

10.1 Fonction de dérivation de clés à une étape

Le Centre pour la cybersécurité recommande l'utilisation de la fonction de dérivation de clés à une étape, conformément au document NIST SP 800-56C Rev. 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes (en anglais seulement).

10.2 Fonction de dérivation de clés à deux étapes

Le Centre pour la cybersécurité recommande l'utilisation de la procédure de dérivation de clés par extraction puis expansion à deux étapes, conformément au document NIST SP 800-56C Rev. 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes (en anglais seulement). Il est à noter que la fonction de dérivation de clés faisant appel au HMAC (HKFD pour *HMAC-based Extract-and-Expand Key Derivation Function*) utilisée dans la version 1.3 du protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*) suit cette spécification.

10.3 Dérivation de clés au moyen de fonctions pseudo-aléatoires

Le Centre pour la cybersécurité recommande l'utilisation des KDF se servant de fonctions pseudo-aléatoires, conformément au document NIST SP 800-108 Rev. 1: Recommendation for Key Derivation Using Pseudorandom Functions (en anglais seulement).

10.4 Fonction de dérivation de clés avec le protocole d'échange de clés Internet version 2

Lorsque cette fonction est utilisée dans le contexte de la version 2 du protocole d'échange de clés Internet (IKEv2 pour *Internet Key Exchange version 2*), le Centre pour la cybersécurité recommande le recours à la KDF IKEv2, conformément au document NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions (en anglais seulement).

10.5 Fonction de dérivation de clés avec le protocole de sécurité de la couche de transport version 1.2

Lorsque cette fonction est utilisée dans le contexte du protocole TLS version 1.2, le Centre pour la cybersécurité recommande le recours à la KDF TLS 1.2, conformément au document NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions (en anglais seulement).

10.6 Fonction de dérivation de clés Secure Shell

Lorsque cette fonction est utilisée dans le contexte du protocole SSH (Secure Shell), le Centre pour la cybersécurité recommande le recours à la KDF SSH, conformément au document NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions (en anglais seulement).

10.7 Fonction de dérivation de clés du protocole de transport sécurisé en temps réel

Lorsque cette fonction est utilisée dans le contexte du protocole de transport sécurisé en temps réel (SRTP pour *Secure Real-time Transport Protocol*), le Centre pour la cybersécurité recommande le recours à la KDF SRTP, conformément au document NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions (en anglais seulement).

10.8 Fonction de dérivation de clés du module de plateforme sécurisée

Lorsque cette fonction est utilisée dans le contexte d'une session de module de plateforme fiable (TPM pour *Trusted Platform Module*), le Centre pour la cybersécurité recommande le recours à la KDF TPM, conformément au document NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions (en anglais seulement).

10.9 Fonction de dérivation de clés basée sur des mots de passe

Pour assurer la protection des données sur des dispositifs de stockage, le Centre pour la cybersécurité recommande l'utilisation de la KDF basée sur des mots de passe, conformément au document NIST SP 800-132: Recommendation for Password-Based Key Derivation: Part 1: Storage Applications (en anglais seulement) à l'aide d'un mot de passe contenant au moins 12 caractères. Pour de plus amples renseignements sur les mots et phrases de passe, prière de consulter le document *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032) du Centre pour la cybersécurité.

11 Modes de fonctionnement des enveloppements de clé

Les sections suivantes décrivent les modes de fonctionnement des enveloppements de clé que le Centre pour la cybersécurité recommande pour protéger la confidentialité et l'intégrité des clés cryptographiques servant à la protection d'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

11.1 Enveloppement de clé à norme de chiffrement avancée

Lorsque l'entrée est toujours un multiple de 64 bits, le Centre pour la cybersécurité recommande l'utilisation du mode d'enveloppement de clé AES, conformément au document Key NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping (en anglais seulement).

11.2 Enveloppement de clé à norme de chiffrement avancée avec remplissage

Lorsque l'entrée n'est pas un multiple de 64 bits, le Centre pour la cybersécurité recommande l'utilisation du mode d'enveloppement de clé AES avec remplissage, conformément au document NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping (en anglais seulement).

12 Générateurs de bits aléatoires

Un RBG produit une séquence de bits (0 ou 1) qui semble statistiquement indépendante et non biaisée. Le Centre pour la cybersécurité recommande l'utilisation de RBG conformément au document NIST SP 800-90C: Recommendation for Random Bit Generator (RBG) Constructions (en anglais seulement). Ces constructions ont recours à une source d'entropie et à un générateur de bits aléatoires déterministes (DRBG pour *Deterministic Random Bit Generator)*.

Un DRBG produit toujours la même séquence de sortie lorsqu'il reçoit la même valeur de départ initiale. Le Centre pour la cybersécurité recommande l'utilisation des DRBG suivants, conformément au document NIST SP 800-90A Rev. 1:Recommendation for Random Number Generation Using Deterministic Random Bit Generators (en anglais seulement) 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 source d'entropie des constructions de RBG et la valeur de départ initiale d'un DRBG devraient être conformes aux recommandations formulées dans le document NIST SP 800-90B Recommendations for Entropy Sources Used for Random Bit Generation (en anglais seulement) et devraient être évaluées de manière à correspondre à au moins 112 bits.

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

13 Programmes d'assurance des technologies commerciales

Outre l'utilisation recommandée dans cette publication des algorithmes cryptographiques, des paramètres et des longueurs de clé, le Centre pour la cybersécurité recommande également ce qui suit pour assurer un niveau adéquat de sécurité cryptographique :

- les mises en œuvre d'algorithmes cryptographiques devraient être testées et validées en vertu du Programme de validation des algorithmes cryptographiques NIST Cryptographic Algorithm Validation Program (CAVP) (en anglais seulement);
- les essais et la validation des modules cryptographiques devraient être réalisés en vertu du Programme de validation des modules cryptographiques (PVMC) pour évaluer la conformité à la norme NIST FIPS 140-3: Security Requirements for Cryptographic Modules (en anglais seulement);
- les produits de sécurité des TI devraient être certifiés comme étant conformes aux Critères communs par une ou un membre de l'autorisation de certification relevant 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 modules validés du NIST (en anglais seulement) et sont accompagnés d'un document de stratégie de sécurité non exclusif provenant du fournisseur (lire 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. Le Centre pour la cybersécurité recommande l'utilisation du document de stratégie 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 (en anglais seulement) pour s'assurer que seuls des algorithmes recommandés par le Centre pour la cybersécurité sont utilisés.

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 demande 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.

A.1 Révisions

La version originale de ce document a été publiée en août 2016. Le sommaire ci-dessous dresse la liste des changements notables dans la plus récente version (version 5), ainsi que dans les versions précédentes.

A.1.1 Version 5

- Mise à jour la section 2 pour préciser que ce document comprend maintenant les dates de retrait définitif des mécanismes d'établissement de clés et des algorithmes de signature numérique vulnérables à l'informatique quantique.
- Ajout des dates de retrait définitif pour l'utilisation de tous les mécanismes d'établissement de clés et les algorithmes de signature numérique vulnérables à l'informatique quantique. Les dates de retrait définitif sont indiquées dans chaque sous-section touchée :
    - pour les mécanismes d'établissement de clés :
        - section 5.1, Rivest-Shamir-Adelman
        - section 5.2, Cryptographie à corps fini de Diffie-Hellman et de Menezes-Qu-Vanstone
        - section 5.3, Cryptographie à courbe elliptique de Diffie-Hellman avec cofacteur et de Menezes-Qu-Vanstone
    - pour les algorithmes de signature numérique :
        - section 6.1, Rivest-Shamir-Adelman
        - section 6.3, Algorithme de signature numérique à courbes elliptiques (ECDSA)
        - section 6.4, Algorithme de signature numérique à courbes elliptiques (EdDSA)
- Dans la section 5.2, nous avons supprimé les recommandations spécifiques concernant la taille des paramètres afin de nous aligner sur les nouvelles exigences regardant la cardinalité du corps (en anglais *field size*)~~Correction d'une coquille à la section 5.2 qui créait de la confusion quant aux jeux de paramètres recommandés~~.
- Changement du nom de la section 12 de « Générateurs de bits aléatoires déterministes » à « Générateurs de bits aléatoires » et ajouté de nouveaux conseils sur l'utilisation des RBG et les sources d'entropie des RBG.
- Modification de la troisième puce à la section 13 pour plus de clarté.

A.1.2 Version 4 (mars 2025)

- Inclusion des nouvelles normes post-quantiques établies par le NIST :
    - NIST FIPS 203 Mécanisme d'encapsulation de clés basé sur des réseaux euclidiens (section 5.4)
    - NIST FIPS 204 Norme pour la signature numérique basée sur des réseaux euclidiens (section 6.5)
    - NIST FIPS 205 Norme pour la signature numérique basée sur un hachage sans état (section 6.6)
- Mise à jour de la section sur la cryptographie post-quantique et déplacement à la section 2.

- À la section 3 : Algorithmes de chiffrement, retrait des sous-sections sur les algorithmes TDEA et CAST5, étant donné que tout usage des TDEA et CAST5 aurait dû être abandonné à la fin de 2023.
- À la section 6.7 : Algorithmes de signature numérique basés sur un hachage avec état, clarification des conseils sur l'utilisation des signatures numériques basées sur un hachage avec état en ce qui a trait aux autres algorithmes de signature numérique post-quantique.
- À la section 8.7 : Fonctions de hachage, extension XOF, ajout des algorithmes ML-KEM, ML-DSA et SLH-DSA à la liste des algorithmes qui peuvent utiliser SHAKE. Ajout d'une précision indiquant que les algorithmes SLH-DSA et EdDSA ne permettent que la fonction SHAKE256, (et pour EdDSA, c'est uniquement avec la courbe Ed448).
- À la section 9.2 : Code d'authentification de message basé sur le chiffrement, retrait de l'énoncé exigeant que la longueur de la clé soit augmentée à au moins 128 bits à la fin de 2023. Le Centre pour la cybersécurité recommande plutôt l'utilisation du code CMAC uniquement avec l'algorithme AES, car les algorithmes TDEA et CAST5 ont été retirés.
- À la section 11 : Modes de fonctionnement des enveloppements de clé, retrait des sous-sections sur l'enveloppement de clé TDEA, étant donné que tout usage de TDEA aurait dû être abandonné à la fin de 2023.
- Le Centre pour la cybersécurité a retiré la section Contenu complémentaire. Des références sont liées tout au long du document, des éléments du glossaire sont définis dans le texte ou dans le glossaire du Centre pour la cybersécurité, et l'expression abrégée des acronymes est présentée au long à la première occurrence dans le document.

A.1.3 Version 3 (mars 2024)

- Plusieurs changements viennent refléter le document FIPS 186-5 :
  - À la section 4.3 : CCE DH et MQV et à la section 5.3 : ECDSA, l'utilisation de quatre courbes elliptiques (courbe P-224, courbe P-256, courbe P-384 et courbe P-521) est préconisée. Le Centre pour la cybersécurité a ajouté une note demandant que la courbe P-224 et toutes les courbes binaires soient abandonnées avant la fin de 2030. Dans la section 5.3, le Centre pour la cybersécurité recommande de façon explicite l'algorithme ECDSA déterministe.
  - À la section 5 : Algorithmes de signature numérique, le Centre pour la cybersécurité recommande l'abandon de l'algorithme DSA d'ici la fin de 2030, et a ajouté la nouvelle sous-section 5.4 Algorithme de signature numérique à courbe Edwards.
- Le Centre pour la cybersécurité a ajouté une nouvelle section sur les extensions XOF (section 7).
- À la section 8 : Codes d'authentification de message, le Centre pour la cybersécurité a ajouté la nouvelle sous-section sur le KMAC (section 8.4).
- À la section 11 : Générateurs de bits aléatoires déterministes, le Centre pour la cybersécurité a ajouté les exigences suivantes concernant l'entropie évaluée de la diversification initiale pour un DRBG.
  - La diversification initiale pour un DRBG devrait comporter une entropie ayant été évaluée à au moins 112 bits de longueur. Le Centre pour la cybersécurité recommande 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.

A.1.4 Version 2 (août 2022)

- Le Centre pour la cybersécurité a mis à jour la terminologie pour passer de « approuvé/supprimé » à « recommandé/abandonné ».
- Les références au CST ont été remplacées par l'utilisation de Centre pour la cybersécurité.
- À la section 2 : Algorithmes de chiffrement, le Centre pour la cybersécurité recommande l'abandon des algorithmes CAST5 et TDEA d'ici 2023. La version de 2016 ne comportait pas de date de fin pour l'algorithme CAST5, et la version 2 recommandait de cesser l'utilisation de TDEA d'ici 2030. Le Centre pour la cybersécurité a également ajouté une restriction indiquant qu'un trousseau de clés ne devrait pas être utilisé pour chiffrer plus de 2^{20} blocs de données de 64 bits dans l'algorithme TDEA.
- À la section 3 : Modes de fonctionnement des algorithmes de chiffrement, le Centre pour la cybersécurité a formulé des conseils supplémentaires sur l'utilisation du mode ECB, ainsi que des recommandations pour la génération de motifs d'initialisation.
- À la section 5 : Algorithmes de signature numérique, le Centre pour la cybersécurité a ajouté une nouvelle sous-section sur les algorithmes de signature numérique basés sur un hachage avec état.
- À la section 6 : Algorithme de hachage sécurisé, le Centre pour la cybersécurité ne recommande plus l'utilisation de l'algorithme SHA-1, qui était auparavant approuvé avec les HMAC, KDF et RBG. Il a employé des formulations plus fortes (en caractère gras) pour mettre en garde contre son utilisation pour toute application nécessitant une résistance aux collisions. Il a également ajouté des dates de retrait définitif pour les algorithmes SHA-224 et SHA3-224.
- À la section 7 : Codes d'authentification de message, le Centre pour la cybersécurité a mis à jour la recommandation pour que la longueur de la clé CMAC soit augmentée à au moins 128 bits d'ici la fin de 2023 (il avait recommandé précédemment 2030). Il a également ajouté l'énoncé « L'utilisation du code GMAC n'est recommandée qu'avec l'algorithme de norme de chiffrement avancée (AES), conformément à la section 2.1 », qui n'avait pas été explicitement formulé dans la version précédente.
- À la section 8 : Fonctions de dérivation de clés, le Centre pour la cybersécurité a mis à jour la formulation de certains énoncés. Par exemple, KDF à étape unique et KDF par extraction puis expansion sont maintenant respectivement KDF en une étape et KDF en deux étapes (cela est en conformité avec les normes NIST mentionnées). Le Centre pour la cybersécurité a supprimé la fonction KDF IKEv1 et ajouté une section pour la fonction de dérivation de clés basée sur des mots de passe.
- À la section 9 : Modes de fonctionnement des enveloppements de clé, le Centre pour la cybersécurité ne recommande plus l'utilisation du mode d'enveloppement de clé avec chiffrement de données triple (TKW pour *Triple Data Encryption Algorithm Key Wrap*). Il a également recommandé une date de retrait définitif de 2023 (précédemment 2030).
- À la section 11 : Programmes d'assurance des technologies commerciales, le Centre pour la cybersécurité a ajouté une référence au PVAC et au programme de critères communs. Le site Web du Centre pour la cybersécurité a également été ajouté comme référence.
- Le Centre pour la cybersécurité a ajouté une nouvelle section appelée « Préparation à la cryptographie post-quantique » (Section 12).