Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

SÉRIE PRATICIENS

CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

ALGORITHMES CRYPTOGRAPHIQUES POUR L'INFORMATION NON CLASSIFIÉ, PROTÉGÉ A ET PROTÉGÉ B

ITSP.40.111

Août 2016

Canada

AVANT-PROPOS

La publication *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Les propositions de modifications doivent être envoyées aux Services à la clientèle de la Sécurité des TI, au CST, par l'entremise des coordonnateurs de la sécurité des TI du ministère.

Pour de plus amples renseignements, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CST, par courriel à ITSclientservices@cse-cst.gc.ca ou par téléphone au 613-991-7654.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le (08/02/2016).

[À signer par]
Scott Jones
Chef adjoint, Sécurité des TI

2 Août 2016
Date

APERÇU

La prestation des programmes et des services du gouvernement du Canada (GC) repose essentiellement sur la capacité du GC de protéger les données et l'information sensibles. La cryptographie fournit des mécanismes de sécurité servant à protéger la confidentialité, l'intégrité et l'authenticité de l'information du GC.

Une cryptographique 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. Différents 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 définit les algorithmes cryptographiques approuvés ainsi que les méthodes d'utilisation appropriées pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B ainsi que l'intégrité de l'information associée à un niveau de préjudice moyen, tel qui il est défini dans l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, du CST.

TABLE DES MATIÈRES

1 INTRODUCTION

Les ministères du gouvernement du Canada (GC) recourent à des systèmes de technologies de l'information (TI) pour atteindre leurs objectifs opérationnels. Ces systèmes interconnectés sont souvent l'objet de sérieuses menaces susceptibles d'influer négativement sur les activités opérationnelles du ministère. La compromission des réseaux du GC peut s'avérer coûteuse et porter atteinte à la disponibilité, à l'authenticité, à la confidentialité et à l'intégrité des ressources d'information du GC.

Le GC utilise la cryptographie pour protéger l'authenticité, la confidentialité et l'intégrité de son information. Lorsqu'ils sont employés avec des paramètres de domaine valides et des longueurs de clé précises, les algorithmes cryptographiques énoncés dans les présents Conseils en matière de sécurité des technologies de l'information pour les praticiens (ITSP pour *Information Technology Security Guidance for Practitioners*) 40.111 sont des mécanismes cryptographiques approuvés pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

Pour connaître les exigences relatives à l'utilisation de la cryptographie approuvée par le CST aux fins de protection de l'information PROTÉGÉ C et classifiée, prière de consulter l'ITSD-01A, *Directive en matière de sécurité des TI sur l'application de la sécurité des communications à l'aide de solutions approuvées par le CST* [1][1].

L'ITSP.40.111 vise à aider les praticiens des technologies dans le choix et l'utilisation appropriée des algorithmes cryptographiques pour la protection de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. L'ITSP.40.111 remplace l'ITSB-111 et vient compléter le document du Secrétariat du Conseil du Trésor du Canada (SCT) intitulé *Ligne directrice sur la définition des exigences en matière d'authentification* [2].

1.1 FACTEURS POLITIQUES

Afin de sécuriser les réseaux, les données et les actifs du GC, il est essentiel d'analyser les cybermenaces et les vulnérabilités auxquelles ils font face et de les contrer. Par conséquent, les ministères du GC doivent veiller à ce que les politiques et procédures en matière de sécurité des TI soient mises en œuvre conformément aux politiques du SCT suivantes :

- *Politique sur la gestion des technologies de l'information* [3];
- *Politique sur la sécurité du gouvernement* [4];
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* [5].

1.2 ENVIRONNEMENTS CONCERNÉS

L'ITSP.40.111 contient des conseils en matière de cryptographie pour les solutions TI dans les environnements NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Les systèmes utilisés dans les domaines PROTÉGÉ C ou classifiés peuvent faire l'objet d'autres considérations de conception qui ne font pas partie de la portée du présent document[2]. Conformément à leur cadre respectif de gestion des risques, les ministères sont tenus d'établir des objectifs de sécurité qui sont propices à la protection de l'information et des services ministériels.

[1] Les numéros entre crochets renvoient à du matériel de référence figurant à la section Contenu complémentaire du présent document.

[2] Afin d'obtenir des conseils en matière de solutions cryptographiques pour les domaines PROTÉGÉ C ou classifiés, prière de communiquer avec les Services à la clientèle en matière de COMSEC du CST.

1.3 RELATION AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS AUX TI

Les lignes directrices énoncées dans l'ITSG-33, *Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [6] proposent un ensemble d'activités pour chacun des deux niveaux organisationnels suivants : le niveau ministériel et le niveau des systèmes d'information.

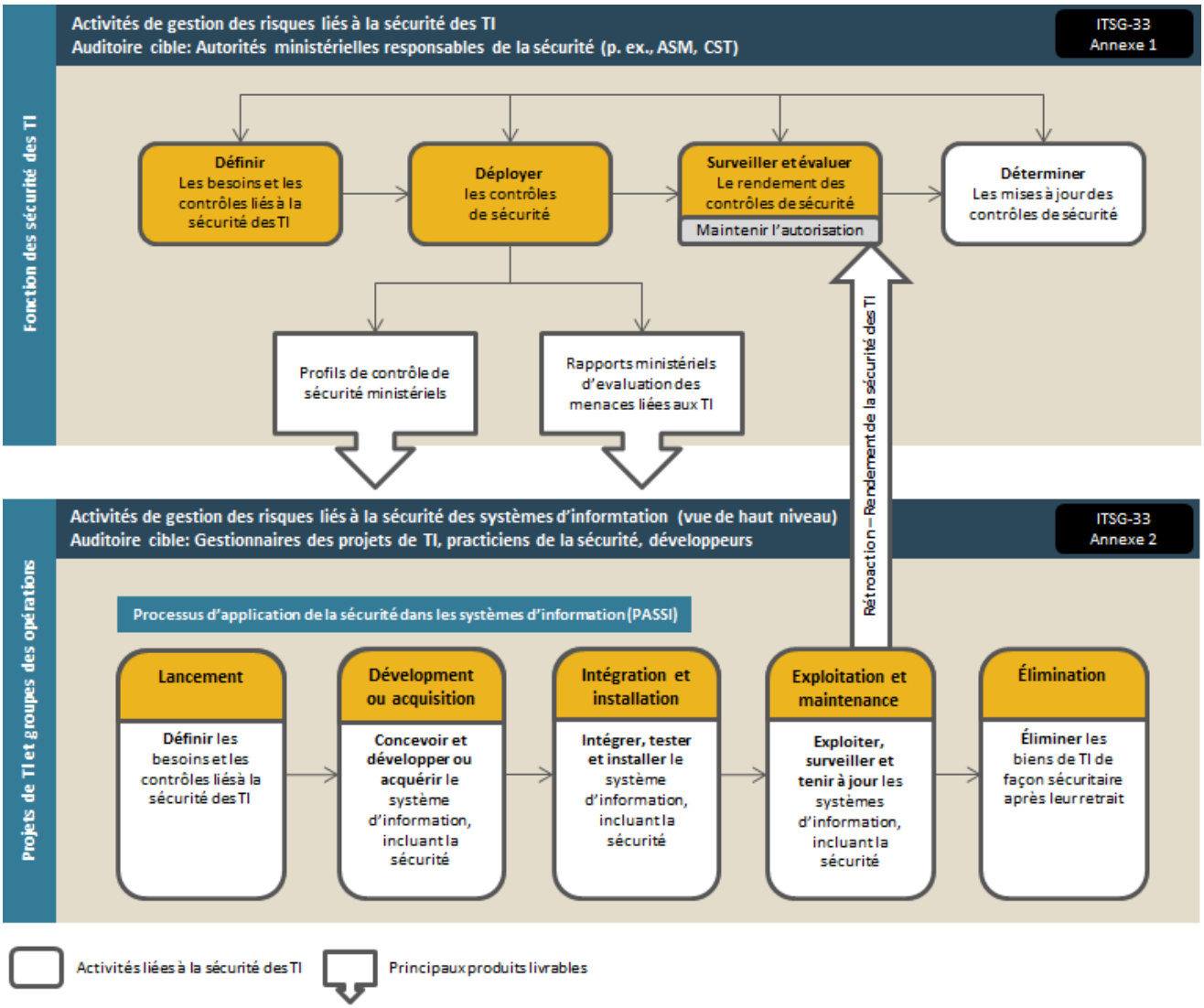

Figure 1 Processus de gestion des risques liés à la sécurité des TI

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. L'ITSP.40.111 doit être pris en compte dans le cadre des activités de définition, de déploiement ainsi que de surveillance et d'évaluation. Ces activités sont décrites en détail à l'Annexe 1 de l'ITSG-33 [6].

Quant aux activités du niveau des systèmes d'information, elles sont intégrées au cycle de vie des systèmes d'information afin de répondre aux besoins en matière de sécurité des TI des activités opérationnelles prises en charge et pour s'assurer que les contrôles de sécurité appropriés sont mis en œuvre et exploités comme prévu, que le rendement des contrôles existants est évalué en permanence et fait l'objet de rapports, et que des mesures appropriées sont prises pour corriger toute lacune relevée. L'ITSP.40.111 doit 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 de l'ITSG-33 [6].

2 ALGORITHMES DE CHIFFREMENT

La section ci-dessous énonce les algorithmes cryptographiques approuvés par le CST pour chiffrer les données, en vue de protéger la confidentialité de l'information.

2.1 ALGORITHME DE CHIFFREMENT AVANCÉ

L'algorithme de chiffrement avancé (AES pour *Advanced Encryption Standard*), utilisé conjointement avec des longueurs de clé de 128, 192 et 256 bits et conformément au document *Federal Information Processing Standards (FIPS) Publication 197: Advanced Encryption Standard* [7], du National Institute of Standards and Technology (NIST), est approuvé pour le chiffrement de l'information PROTÉGÉ A et PROTÉGÉ B.

2.2 ALGORITHME DE CHIFFREMENT DE DONNÉES TRIPLE

L'option à trois clés de l'algorithme de chiffrement de données triple (TDEA pour *Triple Data Encryption Algorithm*), utilisée conjointement avec une longueur de clé de 168 bits et conformément au document *Special Publication (SP) 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm Block Cipher* [8] du NIST, est approuvée pour le chiffrement de l'information PROTÉGÉ A et PROTÉGÉ B.

L'utilisation de l'algorithme TDEA à trois clés devrait être abandonnée d'ici la fin de 2030.

2.3 ALGORITHME DE CHIFFREMENT CAST5

L'algorithme de chiffrement CAST5, utilisé conjointement avec une longueur de clé de 128 bits et conformément au document *Request for Comments (RFC) 2144: The CAST-128 Encryption Algorithm* [9], est approuvé pour le chiffrement de l'information PROTÉGÉ A et PROTÉGÉ B.

3 MODES DE FONCTIONNEMENT DES ALGORITHMES DE CHIFFREMENT

La section ci-dessous énonce les modes de fonctionnement des algorithmes de chiffrement approuvés par le CST.

3.1 PROTECTION DE LA CONFIDENTIALITÉ DE L'INFORMATION

Lorsqu'ils sont utilisés conjointement avec un algorithme de chiffrement approuvé et conformément au document *SP 800-38A: Recommendation for Block Cipher Modes of Operation – Methods and Techniques* [10] du NIST, les modes de fonctionnement suivants sont approuvés pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B :

- mode de chiffrement par carnet de codage électronique (ECB pour *Electronic Codebook*);
- mode de chiffrement par chaînage de blocs (CBC pour *Cipher Block Chaining*);
- 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*).

Lorsqu'ils sont utilisés conjointement avec un algorithme de chiffrement approuvé et conformément au document *Addendum to NIST Special Publication SP 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC modes* [28], les modes de chiffrement par chaînage de blocs avec vol de texte chiffré (CBC-CS pour *Cipher Block Chaining with Ciphertext Stealing*) suivants sont approuvés pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B :

- CBC-CS1;
- CBC-CS2;
- CBC-CS3.

Lorsqu'il est utilisé conjointement avec l'algorithme de chiffrement avancé (AES) et conformément au document *SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices* [11] du NIST, le mode de fonctionnement XTS-AES est approuvé pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B sur des dispositifs de stockage.

3.2 PROTECTION DE LA CONFIDENTIALITÉ ET DE L'AUTHENTICITÉ DE L'INFORMATION

Lorsqu'ils sont utilisés conjointement avec un algorithme de chiffrement approuvé, les modes de fonctionnement suivants sont approuvés par le CST pour protéger la confidentialité de l'information PROTÉGÉ A et PROTÉGÉ B de même que 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 *Counter with Cipher Block Chaining Message Authentication Code*) : conformément au document *SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality* [12] du NIST;
- mode Galois/compteur (GCM pour *Galois/Counter Mode*) : conformément au document *SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode* [13] du NIST.

4 SCHÉMAS D'ÉTABLISSEMENT DE CLÉS

La section ci-dessous énonce les schémas d'établissement de clés approuvés par le CST aux fins d'utilisation avec des algorithmes cryptographiques approuvés.

4.1 RIVEST, SHAMIR, ADLEMAN

Les schémas de négociation et de transport de clés basés sur l'algorithme Rivest, Shamir, Adleman (RSA), utilisés conjointement avec un module RSA d'une longueur minimale de 2048 bits et conformément au document *SP 800-56B Revision 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography* [14] du NIST, sont approuvés pour l'établissement de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

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 DE DIFFIE-HELLMAN ET DE MENEZES-QU-VANSTONE

Les schémas de négociation de clés basés sur la cryptographie à corps fini (FFC pour *Finite Field Cryptography*) de Diffie-Hellman (DH) et sur la FCC de Menezes-Qu-Vanstone (MQV), utilisés conjointement avec des paramètres de domaine valides pour les ensembles tailles-paramètres FB ou FC FFC et avec une taille de corps d'au moins 2048 bits, et utilisés conformément au document *SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [15] du NIST, sont approuvés pour l'établissement de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

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

Les schémas de négociation de clés basés sur la cryptographie à courbe elliptique (ECC pour *Elliptic Curve Cryptography*) de Diffie-Hellman avec cofacteur (CDH pour *Cofactor Diffie-Hellman*) et sur l'ECC de MQV, utilisés conjointement avec des paramètres de domaine valides pour les ensembles tailles-paramètres EB, EC, ED ou EE et avec un ordre de sous-groupe d'au moins 224 bits, et utilisés conformément au document *SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [15] du NIST, sont approuvés pour l'établissement de clés en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B. Le CST recommande fortement d'employer les paramètres de domaine à courbe elliptique énoncés à l'Annexe D du document *FIPS 186-4: Digital Signature Standard* [16] du NIST, pour l'ECC de CDH et l'ECC de MQV.

Les ensembles tailles-paramètres EC, ED ou EE avec un ordre de sous-groupe d'au moins 256 bits devraient être utilisés d'ici la fin de 2030.

5 ALGORITHMES DE SIGNATURE NUMÉRIQUE

La section ci-dessous énonce les algorithmes de signature numérique approuvés par le CST pour l'application des signatures numériques.

5.1 ALGORITHME DE SIGNATURE RIVEST, SHAMIR, ADLEMAN

L'algorithme de signature numérique RSA, utilisé conjointement avec un module RSA d'une longueur minimale de 2048 bits et conformément aux documents *FIPS 186-4: Digital Signature Standard* [16] et *RSA PKCS #1 v2.2: RSA Cryptography Standard* [17] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

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

L'algorithme de signature numérique (DSA pour *Digital Signature Algorithm*), utilisé conjointement avec des paramètres de domaine valides et avec un module composé de nombres premiers d'une longueur minimale de 2048 bits, et utilisé conformément au document *FIPS 186-4: Digital Signature Standard* [16] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

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

5.3 ALGORITHME DE SIGNATURE NUMÉRIQUE À COURBE ELLIPTIQUE

L'algorithme de signature numérique à courbe elliptique (ECDSA pour *Elliptic Curve Digital Signature Algorithm*), utilisé conjointement avec des paramètres de domaine valides pour une taille de corps d'au moins 224 bits et conformément au document *FIPS 186-4: Digital Signature Standard* [16] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. Le CST recommande fortement l'utilisation des paramètres de domaine à courbe elliptique figurant à l'Annexe D du document *FIPS 186-4: Digital Signature Standard* [16], pour l'algorithme ECDSA.

La taille du corps devrait être augmentée à au moins 256 bits d'ici la fin de 2030.

6 ALGORITHMES DE HACHAGE SÉCURISÉ

La section ci-dessous énonce les algorithmes de hachage sécurisé (SHA pour *Secure Hash Algorithm*) approuvés par le CST aux fins d'utilisation avec des algorithmes cryptographiques approuvés précis.

6.1 SHA-1

L'utilisation de l'algorithme SHA-1, conformément au document *FIPS 180-4: Secure Hash Standard* [18] du NIST et conjointement avec des codes d'authentification de message avec hachage de clé (HMAC pour *Keyed-Hash Message Authentification Code*), des fonctions de dérivation de clés (KDF pour *Key Derivation Function*) et des générateurs de bits aléatoires, est approuvée pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

L'utilisation de SHA-1 n'est pas approuvée avec les algorithmes de signature numérique.

6.2 SHA-2

L'utilisation des algorithmes SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 et SHA-512/256, conformément au document *FIPS 180-4: Secure Hash Standard* [18] du NIST et conjointement avec des algorithmes de signature numérique, des HMAC, des KDF et des générateurs de bits aléatoires, est approuvée pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

6.3 SHA-3

L'utilisation des algorithmes SHA3-224, SHA3-256, SHA3-384 et SHA3-512, conformément au document *FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* [29] du NIST et conjointement avec des algorithmes de signature numérique, des HMAC, des KDF et des générateurs de bits aléatoires, est approuvée pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

7 CODES D'AUTHENTIFICATION DE MESSAGE

Les sections ci-dessous énoncent les algorithmes de codes d'authentification de message (MAC pour *Message Authentication Code*) approuvés par le CST pour assurer l'intégrité des données et l'authentification de l'origine des données.

7.1 CODE D'AUTHENTIFICATION DE MESSAGE AVEC HACHAGE DE CLÉ

Le code d'authentification de message avec hachage de clé (HMAC pour *Keyed-Hash Message Authentification Code*), utilisé conjointement avec une clé d'au moins 112 bits de longueur et conformément au document *FIPS 198-1: The Keyed-Hash Message Authentication Code* [19] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

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

7.2 CODE D'AUTHENTIFICATION DE MESSAGE BASÉ SUR LE CHIFFREMENT

Le code d'authentification de message basé sur le chiffrement (CMAC pour *Cipher-based Message Authentication Code*), utilisé conjointement avec une clé d'au moins 112 bits de longueur et conformément au document *SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication* [20] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

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

7.3 CODE D'AUTHENTIFICATION DE MESSAGE AVEC LE MODE GALOIS/COMPTEUR

Le code d'authentification de message avec le mode Galois/compteur (GMAC pour *Galois/Counter Mode Message Authentication Code*), utilisé conformément au document *SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode* [13] du NIST, est approuvé pour assurer l'intégrité des données et l'authentification de l'origine des données de l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

8 FONCTIONS DE DÉRIVATION DE CLÉS

La section ci-dessous énonce les fonctions de dérivation de clés approuvées par le CST pour la dérivation de clés cryptographiques à partir de secrets prépartagés ou d'établissement de clés.

8.1 FONCTION DE DÉRIVATION DE CLÉS À UNE SEULE ÉTAPE

La fonction de dérivation de clés (KDF pour *Key Derivation Function*) à une seule étape, utilisée conformément au document *SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [15] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.2 DÉRIVATION DE CLÉS AU MOYEN DE FONCTIONS PSEUDO-ALÉATOIRES

La dérivation de clés au moyen de fonctions pseudo-aléatoires (PRF pour *Pseudorandom Function*), utilisée conformément au document *SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions* [21] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.3 FONCTION DE DÉRIVATION DE CLÉS EXTRACTION PUIS EXPANSION

La KDF extraction puis expansion, utilisée conformément au document *SP 800-56C: Recommendation for Key Derivation through Extraction then Expansion* [22] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.4 FONCTION DE DÉRIVATION DE CLÉS AVEC LA VERSION 1 DU PROTOCOLE D'ÉCHANGE DE CLÉS INTERNET

La KDF avec la version 1 du protocole d'échange de clés Internet (IKEv1 pour *Internet Key Exchange version 1*), utilisée conjointement avec un HMAC et un SHA approuvés, et utilisée conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.5 FONCTION DE DÉRIVATION DE CLÉS AVEC LA VERSION 2 DU PROTOCOLE D'ÉCHANGE DE CLÉS INTERNET

La KDF avec la version 1 du protocole d'échange de clés Internet (IKEv2 pour *Internet Key Exchange version 2*), utilisée conjointement avec un HMAC et un SHA approuvés, et utilisée conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.6 FONCTION DE DÉRIVATION DE CLÉS AVEC LA VERSION 1.2 DU PROTOCOLE DE SÉCURITÉ DE LA COUCHE TRANSPORT

La KDF avec la version 1.2 du protocole de sécurité de la couche transport (TLS 1.2 pour *Transport Layer Security version 1.2*), utilisée conjointement avec un HMAC et un SHA approuvés, et utilisée conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.7 FONCTION DE DÉRIVATION DE CLÉS AVEC LE PROTOCOLE SECURE SHELL

La KDF avec le protocole Secure Shell (SSH), utilisée conjointement avec un SHA approuvé et conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.8 FONCTION DE DÉRIVATION DE CLÉS AVEC LE PROTOCOLE DE TRANSPORT EN TEMPS RÉEL SÉCURISÉ

La KDF avec le protocole de transport en temps réel sécurisé (SRTP pour *Secure Real-time Transport Protocol*), utilisée conjointement avec un algorithme de chiffrement approuvé et conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

8.9 FONCTION DE DÉRIVATION DE CLÉS AVEC UN MODULE DE PLATEFORME FIABLE

La KDF avec une session du module de plateforme fiable (TPM pour *Trusted Platform Module*), utilisée conjointement avec un HMAC et SHA approuvés, et utilisée conformément au document *SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] du NIST, est approuvée pour la dérivation de clés, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

9 MODES DE FONCTIONNEMENT DES ENVELOPPEMENTS DE CLÉS

La section ci-dessous énonce les modes de fonctionnement des enveloppements de clés (KW pour *Key Wrap*) approuvés par le CST pour envelopper des clés, en vue de protéger la confidentialité et l'intégrité des clés cryptographiques.

9.1 ENVELOPPEMENT DE CLÉ AES

Le mode d'enveloppement de clé avec l'algorithme de chiffrement avancé (AES KW pour *Advanced Encryption Standard Key Wrap*), utilisé conformément au document *SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* [23] du NIST, est approuvé pour protéger la confidentialité et l'intégrité des clés cryptographiques, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

9.2 ENVELOPPEMENT DE CLÉ AES AVEC REMPLISSAGE

Le mode d'enveloppement de clé AES avec remplissage (KWP pour *Key Wrap with Padding*), utilisé conformément au document *SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* [23] du NIST, est approuvé pour protéger la confidentialité et l'intégrité des clés cryptographiques, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

9.3 ENVELOPPEMENT DE CLÉ AVEC CHIFFREMENT DE DONNÉES TRIPLE

Le mode d'enveloppement de clé avec chiffrement de données triple (TKW pour *Triple Data Encryption Algorithm Key Wrap*), utilisé conjointement avec une longueur de clé de 168 bits et conformément au document *SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* [23] du NIST, est approuvé pour protéger la confidentialité et l'intégrité des clés cryptographiques, en vue de protéger l'information PROTÉGÉ A et PROTÉGÉ B.

L'utilisation de l'algorithme TDEA à trois clés en mode TKW devrait être abandonnée d'ici la fin de 2030.

10 GÉNÉRATEURS DE BITS ALÉATOIRES DÉTERMINISTES

Les générateurs de bits aléatoires déterministes (DRBG pour *Deterministic Random Bit Generator*) suivants, utilisés conformément au document *SP 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators* [24] du NIST, sont approuvés par le CST pour produire des bits aléatoires aux fins d'application cryptographique, en vue de protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B :

- Hash_DRBG;
- HMAC_DRBG;
- CTR_DRBG.

L'utilisation du Dual_EC_DRBG n'est plus approuvée.

11 PROGRAMMES D'ASSURANCE DES TECHNOLOGIES COMMERCIALES

En plus d'utiliser des algorithmes cryptographiques, des paramètres et des longueurs de clés approuvés par le CST pour assurer un niveau adéquat de sécurité cryptographique, il faut également tenir compte des directives suivantes liées à la mise en œuvre des exigences en matière d'assurance :

- toute application d'algorithmes cryptographiques devrait être testée et validée en vertu du programme de validation des algorithmes cryptographiques (CAVP pour *Cryptographic Algorithm Validation Program*);
- les modules cryptographiques devraient être testés et validés en vertu du Programme de validation des modules cryptographiques (PVMC) aux fins de conformité à la *FIPS 140-2* [25];
- les produits contenant des modules cryptographiques validés en vertu du PVMC font partie des listes de validation des modules du PVMC et sont accompagnés d'un document de politique de sécurité non exclusif provenant du fournisseur; ce document précise la sécurité cryptographique fournie par un module et décrit ses capacités, sa protection et ses contrôles d'accès; il devrait être utilisé pour choisir 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 140-2 and the Cryptographic Module Validation Program* [26], pour s'assurer que seuls des algorithmes approuvés par le CST sont utilisés;
- les produits de sécurité des technologies de l'information devraient être évalués et certifiés comme étant conformes aux Critères communs par un Schéma d'autorisation de certificat qui est membre de l'Arrangement relatif à la reconnaissance des certificats liés aux Critères communs (ARCC).

12 RÉSUMÉ

La cryptographie fournit des mécanismes de sécurité servant à protéger la confidentialité, l'intégrité et l'authenticité de l'information du GC. Différents 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 approuvés par le CST pour protéger l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B.

12.1 AIDE ET RENSEIGNEMENTS

Pour obtenir de plus amples renseignements sur les algorithmes cryptographiques pour l'information protégée, prière de communiquer avec les Services à la clientèle de la STI :

Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca

13 CONTENU COMPLÉMENTAIRE

13.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
AES	Algorithme de chiffrement avancé (*Advanced Encryption Standard*)
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*)
CMAC	Code d'authentification de message basé sur le chiffrement (*Cipher-Based Message Authentication Code*)
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 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 Echange*)
ITSG	Conseils en matière de sécurité des technologies de l'information (*Information Technology Security Guidance*)
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*)
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*)
PRF	Fonction pseudo-aléatoire (*Pseudorandom Function*)
PVMC	Programme de validation des modules cryptographiques
RFC	Demande de commentaires (*Request for Comments*)
RSA	Rivest, Shamir, Adleman
SCT	Secrétariat du Conseil du Trésor du Canada
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	*Secure Shell*
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 (*Triple Data Encryption Key Wrap*)
TLS	Sécurité de la couche de transport (*Transport Layer Security*)
TPM	Module de plateforme fiable (*Trusted Platform Module*)

13.2 GLOSSAIRE

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.
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 de l'expéditeur.
Chiffrement	Transformation de données lisibles en une séquence de caractères illisibles à l'aide d'un processus de codage réversible.
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 l'information (voix ou données) chiffrée par l'opération inverse du chiffrement.
Disponibilité	Fait d'être accessible et utilisable intégralement et en temps opportun.
Federal Information Processing Standards (FIPS) Publication 140-2	Normes 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.
Gestion des clés	Procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés qui commandent 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.
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.
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 (PVMC)	Programme conjoint du NIST et du CST servant à valider des modules cryptographiques en vertu de la norme FIPS 140-1, *Security Requirements for Cryptographic Modules*, et d'autres normes et recommandations cryptographiques du NIST.
Signature numérique	Transformation cryptographique des données qui fournit les services d'authentification, d'intégrité des données et de non-répudiation du signataire.

13.3 RÉFÉRENCES

Numéro	Référence
1	Centre de la sécurité des télécommunications. ITSD-01A, *Directive en matière de sécurité des TI sur l'application de la sécurité des communications à l'aide de solutions approuvées par le CST*, janvier 2014.
2	Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur la définition des exigences en matière d'authentification*, novembre 2008.
3	Secrétariat du Conseil du Trésor du Canada. *Politique sur la gestion des technologies de l'information*, 1er juillet 2007.
4	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement*, 1er juillet 2009.
5	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, sans date.
6	Centre de la sécurité des télécommunications. ITSG-33, *La gestion des risques liés à la sécurité des*

	TI : Une méthode axée sur le cycle de vie, décembre 2014.
7	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 197 Advanced Encryption Standard,* 26 novembre 2001.
8	National Institute of Standards and Technology. *Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm Block Cipher,* janvier 2012.
9	Adams, C. *The CAST-128 Encryption Algorithm* Internet RFCs, ISSN 2070-1721, RFC 2144*,* mai 1997.
10	National Institute of Standards and Technology. *Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation – Methods and Techniques,* décembre 2001.
11	National Institute of Standards and Technology. *Special Publication 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices,* janvier 2010.
12	National Institute of Standards and Technology. *Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, mai 2004.
13	National Institute of Standards and Technology. *Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode*, novembre 2007.
14	National Institute of Standards and Technology. *Special Publication 800-56B Revision 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, août 2009.
15	National Institute of Standards and Technology. *Special Publication 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, mai 2013.
16	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 186-4: Digital Signature Standard*, juillet 2013.
17	RSA Laboratories*. RSA PKCS #1 v2.2: RSA Cryptography Standard*, octobre 2012.
18	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 180-4: Secure Hash Standard*, août 2015.
19	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 198-1: The Keyed-Hash Message Authentication Code*, juillet 2008.
20	National Institute of Standards and Technology. *Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, mai 2005.
21	National Institute of Standards and Technology. *Special Publication 800-108: Recommendation for Key Derivation Using Pseudorandom Functions*, octobre 2009.
22	National Institute of Standards and Technology. *Special Publication SP 800-56C: Recommendation for Key Derivation through Extraction then Expansion*, novembre 2011.
23	National Institute of Standards and Technology. *Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, décembre 2012.
24	National Institute of Standards and Technology. *Special Publication 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, juin 2015.
25	National Institute of Standards and Technology. *Federal Information Processing Standards 140-2*, novembre 2001.

26	National Institute of Standards and Technology. *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, mai 2016.
27	National Institute of Standards and Technology. *Special Publication 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions,* décembre 2011.
28	National Institute of Standards and Technology. *Addendum to NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, octobre 2010.
29	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, août 2015.