



IT Security Alert

Alerte de sécurité TI

March 2011

ITSA-11E

Mars 2011

CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within the Government of Canada

Purpose

The aim of this ALERT is to provide Government of Canada (GC) departments with information on:

- approved algorithms for encryption, key establishment, digital signatures, key derivation functions, key transport, key wrapping, and data integrity
- approved hashing algorithms and the status of the Secure Hash Algorithm (SHA-1)
- approved padding schemes
- random number generation
- future initiatives in cryptography.

This ALERT supersedes ALERT 11(d), published in July 2008.

Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du gouvernement du Canada

Objet

L'objet de la présente ALERTE est de fournir aux ministères du gouvernement du Canada (GC) de l'information sur :

- les algorithmes approuvés pour le chiffrement, l'établissement de clés, les signatures numériques, les fonctions de dérivation de clé, le transport des clés, l'enveloppement des clés et l'intégrité des données;
- les algorithmes de hachage approuvés et la situation de l'algorithme *Secure Hash Algorithm* (SHA-1);
- les protocoles de bourrage approuvés;
- la génération de nombres aléatoires;
- les initiatives futures dans le domaine de la cryptographie.

La présente ALERTE remplace l'ITSA-11D publiée en juillet 2008.



March 2011

ITSA-11E

Mars 2011

Cryptographic Transition from 80-bits to 112-bits

The previous ALERT 11(c) and (d) announced that 80-bit cryptographic strength was to be phased out by the end of 2010 and be upgraded to a minimum of 112-bit cryptography. CSEC assesses that the threat environment with respect to Protected A and B information does not warrant a mandatory and immediate migration to 112-bit cryptography.

The permitted use of 80-bit cryptography for the protection of Protected A and B information is extended by three years to the end of 2013. However, a minimum security strength of 112-bits is strongly recommended. It is also recommended that new implementations do not use 80-bit algorithms.

GC departments using 80-bit cryptography must accept some risk that increases over time. This risk acceptance includes the use of 2-key Triple DES. The risk increases due to advancements in computing power as well as the increased probability of weaknesses uncovered by cryptanalytic research. It is the responsibility of the user or user's organization to determine the level of risk that can be tolerated for an application and its associated data.

Transition de la cryptographie à 80 bits à la cryptographie à 112 bits

Dans les alertes ITSA-11C et ITSA-11D précédentes, on annonçait que la robustesse cryptographique de 80 bits allait être graduellement abandonnée avant la fin de 2010 pour être remplacée par une cryptographie d'au moins 112 bits. Or, le CSTC estime que l'environnement de menace en ce qui concerne l'information PROTÉGÉ A et PROTÉGÉ B ne justifie pas une migration immédiate et obligatoire vers la cryptographie à 112 bits.

L'emploi autorisé de la cryptographie à 80 bits pour la protection de renseignements PROTÉGÉ A et PROTÉGÉ B est prolongé de 3 ans jusqu'à la fin de 2013. Toutefois, il est fortement recommandé de faire appel à une robustesse de sécurité minimale de 112 bits. Il est également recommandé que les nouvelles mises en œuvre n'utilisent pas d'algorithmes à 80 bits.

Les ministères du GC qui utilisent la cryptographie à 80 bits doivent accepter certains risques qui augmenteront au fil du temps. Cette acceptation des risques comprend l'utilisation de l'algorithme Triple DES à deux clés. Les risques augmentent en raison des progrès réalisés dans la puissance de calcul et d'une probabilité accrue que des faiblesses seront décelées au cours de recherches cryptanalytiques. C'est à l'utilisateur ou à son organisation que revient la responsabilité de déterminer le niveau de risque tolérable pour une application et les données connexes.



March 2011

ITSA-11E

Mars 2011

Refer to appendix B of NIST Special Publication 800-131Aⁱ for strategies to mitigate the risk of using 80-bit cryptography.

Table 1 provides the comparable strength for the algorithms in this alert.

Prière de se reporter à l'appendice B de la publication spéciale 800-131Aⁱ du NIST pour les stratégies visant à atténuer les risques présentés par la cryptographie à 80 bits.

Le tableau 1 donne une comparaison des différents niveaux de robustesse des algorithmes mentionnés dans la présente alerte.

**Table 1 : Comparable Strengths of Algorithms in ITSA-11e/
Comparaison de la robustesse des algorithmes mentionnés dans l'ITSA-11E**

Bits of Security/ Bits de sécurité	Symmetric Key Algorithm/ Algorithme à clé symétrique	Hash Algorithm/ Algorithme de hachage	Finite Field and Integer Factorization Cryptography/ Cryptographie à corps fini et à factorisation des nombres entiers	Elliptic Curve Cryptography/ Cryptographie à courbe elliptique
80	80-bit CAST5	SHA-1	1024	160
100	2-key Triple DES/ Triple DES à 2 clés ⁱⁱ			
112	3-key Triple DES/ Triple DES à 3 clés	SHA-224	2048	224
128	AES-128 128-bit CAST5	SHA-256	3072	256
192	AES-192	SHA-384	7680	384
256	AES-256	SHA-512	15360	512

Background

The cryptographic algorithms and their associated parameters described herein are

Contexte

Les algorithmes cryptographiques et les paramètres connexes décrits ci-après

March 2011

ITSA-11E

Mars 2011

applicable to confidentiality, integrity and authentication services in support of the protection of GC Protected information and for electronic authorization and authentication (EAA) applications.

In ensuring a suitable level of cryptographic security, there are factors to be considered in addition to using approved algorithms. The cryptographic algorithm implementations must be validated by the Cryptographic Algorithm Validation Program (CAVP) to ensure that they meet the specified standard. Additional assurance for the product in which the algorithm is implemented can be obtained through a FIPS 140-2 (or subsequent FIPS 140-3) validation under the Cryptographic Module Validation Program (CMVP) and Common Criteria evaluation. Aspects of security including seeding of random number generators, the application environment, and application specific threats must also be taken into account. Contact CSEC for more details.

The protection of Classified GC information is beyond the scope of this document. See CSEC ITSB-40A for information on protecting Classified information using Suite B cryptographic algorithms.

In selecting an algorithm for use, it is important to consider the period of time for which the information must be protected. An algorithm should be used only if it is acceptable for the entire period of

s'appliquent aux services de confidentialité, d'intégrité et d'authentification mis en œuvre pour protéger les renseignements désignés PROTÉGÉ du GC et aux applications d'autorisation et d'authentification électroniques (AAE).

Pour assurer un degré convenable de sécurité cryptographique, il faut tenir compte d'autres facteurs en sus de l'utilisation d'algorithmes approuvés. Les versions d'algorithmes cryptographiques doivent être validées en vertu du *Cryptographic Algorithm Validation Program* (CAVP) afin d'assurer qu'elles respectent la norme précisée. Il est possible d'obtenir un niveau d'assurance additionnel pour le produit dans lequel est mis en œuvre l'algorithme au moyen d'une évaluation selon la norme FIPS 140-2 (ou la norme FIPS 140-3 subséquente) en vertu du Programme de validation des modules cryptographiques (PVMC) et des Critères communs. Il faut également tenir compte d'autres aspects de la sécurité, notamment l'initialisation (*seeding*) de générateurs de nombres aléatoires, l'environnement d'application et les menaces particulières pesant contre les applications. Pour plus de détails, prière de communiquer avec le CSTC.

La protection de l'information classifiée du GC dépasse les limites du présent document. Prière de se reporter à l'ITSB-40A du CSTC pour plus de détails sur la protection de l'information classifiée à l'aide des algorithmes cryptographiques Suite B.

Au moment de sélectionner un algorithme, il est important de considérer la période de temps pendant laquelle l'information doit être protégée. Un algorithme ne devrait être utilisé que s'il est acceptable pour toute la durée de

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

protection. For example, if Protected B information is encrypted in 2011 and must remain secure for 5 years, 80-bit CAST5 should not be used, since it is not approved past 2013.

A cryptoperiod is defined as the time span which a specific key is authorized for use.

Encryption Algorithms

CSEC approves the use of the following algorithms for the encryption of *Protected* information with the limitations outlined below:

- AES (128, 192, 256 bits)
- Triple DES (2-key, 3-key)
- CAST5 (80, 128 bits)

Encryption algorithms may be used with a mode of operation found below. The encryption key may be established using an algorithm identified under key establishment algorithms below.

- a. **AES.** NIST standard FIPS 197 2001 (*Advanced Encryption Standard*) gives the specification for the AES algorithm.

The cryptoperiod shall not exceed 7 days.

- b. **Triple DES.** ANSI standard X9.52 1998 (*Triple Data Encryption Algorithm – Modes of Operation*) and NIST Special

la période de protection. À titre d'exemple, si des renseignements PROTÉGÉ B sont chiffrés en 2011 et qu'ils doivent demeurer sécurisés pendant 5 ans, l'algorithme CAST5 à 80 bits ne devrait pas être utilisé étant donné qu'il n'est pas approuvé au-delà de l'année 2013.

On entend par « cryptopériode » le laps de temps pendant lequel l'utilisation d'une clé particulière est autorisée.

Algorithmes de chiffrement

Le CSTC approuve l'utilisation des algorithmes de chiffrement suivants pour le chiffrement des renseignements désignés PROTÉGÉ avec les limites données plus bas :

- AES (128, 192, 256 bits)
- Triple DES (2 clés, 3 clés)
- CAST5 (80, 128 bits)

Les algorithmes de chiffrement peuvent être utilisés avec l'un ou l'autre des modes opératoires donnés plus bas. La clé de chiffrement peut être établie à l'aide d'un des algorithmes présentés dans la rubrique *Algorithmes d'établissement de clé* plus bas.

- a. **AES.** La norme FIPS-197 2001 (*Advanced Encryption Standard*) du NIST donne la spécification de l'algorithme AES.

La cryptopériode ne doit pas dépasser 7 jours.

- b. **Triple DES.** La norme ANSI X9.52-1998 (*Triple Data Encryption Algorithm – Modes of Operation*) et la publication spéciale

March 2011

ITSA-11E

Mars 2011

Publication 800-67 2004 (Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher) specify the acceptable methods of implementing Triple DES.

800-67 2004 du NIST (*Recommendation for the Triple Data Encryption Algorithm [TDEA] Block Cipher*) précisent les méthodes acceptables de mise en œuvre de l'algorithme Triple DES.

The cryptoperiod shall not exceed 7 days.

La cryptopériode ne doit pas dépasser 7 jours.

NOTE: The 3-key option provides the best security and is therefore the preferred option. The 2-key option is also currently acceptable for *Protected A* and *B*, where the key used in the final encryption is the same as in the first encryption. The single-key option, which is equivalent to DES, is not approved by CSEC for the protection of *Protected GC* information.

NOTA: L'option à trois clés offre la meilleure protection et est donc l'option de premier choix. L'option à deux clés est également acceptable à l'heure actuelle pour les renseignements PROTÉGÉ A et PROTÉGÉ B à condition que la clé utilisée pour le chiffrement final ait également servi au chiffrement initial. L'option à une seule clé, qui équivaut au DES, n'est pas approuvée par le CSTC pour protéger les renseignements désignés PROTÉGÉ du GC.

The 2-key option is not acceptable for *Protected C*. Use of the 2-key option for *Protected A* and *B* information shall be discontinued by the end of 2015. The 2-key Triple DES option has the restriction that at most 2^{20} blocks of data can be encrypted with the same key.

L'utilisation de l'option à deux clés n'est pas acceptable pour les renseignements PROTÉGÉ C. L'utilisation de l'option à deux clés pour les renseignements PROTÉGÉ A et PROTÉGÉ B sera abandonnée d'ici la fin de 2015. L'option Triple DES à deux clés restreint à 2^{20} blocs la taille des blocs de données pouvant être chiffrés au moyen de la même clé.

Use of 3-key Triple DES shall be discontinued by the end of 2025 for *Protected C*, and by the end of 2030 for all other levels of *Protected* information.

L'utilisation de Triple DES à trois clés sera abandonnée d'ici la fin de 2025 pour les renseignements PROTÉGÉ C, et d'ici la fin de 2030 pour les renseignements PROTÉGÉ de tous les niveaux.

c. **CAST5**ⁱⁱⁱ. Acceptable modes of operation are the same as those defined for AES.

c. **CAST5**ⁱⁱⁱ. Les modes opératoires acceptables pour le CAST5 sont identiques à ceux précisés pour l'AES.

March 2011

ITSA-11E

Mars 2011

The 128-bit version of CAST5 is currently valid for all levels of *Protected* information. For *Protected C* information, use of the 80-bit version should have been discontinued by the end of 2005. For *Protected A* and *B* information, use of the 80-bit version shall be discontinued by the end of 2013.

La version à 128 bits du CAST5 est actuellement valide pour les renseignements PROTÉGÉ de tous les niveaux. Pour les renseignements PROTÉGÉ C, la version à 80 bits devrait avoir été abandonnée à la fin de 2005. Elle devra l'être d'ici la fin de 2013 pour les renseignements PROTÉGÉ A et PROTÉGÉ B.

For the 80-bit version, the cryptoperiod shall not exceed 24 hours. For the 128-bit version, the cryptoperiod shall not exceed 7 days.

Pour la version à 80 bits, la cryptopériode ne doit pas dépasser 24 heures. Elle ne doit pas dépasser 7 jours pour la version à 128 bits.

Modes of Operation

Approved encryption modes of operations are defined in NIST Special Publications 800-38A, 800-38B, 800-38C, and 800-38D.

Modes of operation to provide confidentiality for AES, Triple DES, and CAST5 are the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes. The Cipher-based Message Authentication Code (CMAC) mode provides confidentiality and authentication of data for AES, Triple DES, and CAST5.

Modes opératoires

Les modes opératoires de chiffrement approuvés sont définis dans les publications spéciales 800-38A, 800-38B, 800-38C et 800-38D du NIST.

Les modes opératoires assurant la confidentialité pour les algorithmes AES, Triple DES et CAST5 sont le mode de dictionnaire (ECB pour *Electronic Codebook*), le mode d'enchaînement de blocs de chiffrement (CBC pour *Cipher Block Chaining*), le mode à rebouclage par le chiffre (CFB pour *Cipher Feedback*), le mode à rebouclage par la sortie (OFB pour *Output Feedback*) et le mode compteur (CTR pour *Counter*). Le mode de code d'authentification de message à base de fonction de chiffrement (CMAC pour *Cipher-based Message Authentication Code*) offre la confidentialité et l'authentification des données pour les algorithmes AES, Triple DES et CAST5.

The Counter with Cipher Block Chaining – Message Authentication Code (CCM), Galois/Counter Mode (GCM), and GMAC modes provide confidentiality and authentication of data for AES and 128-bit CAST5.

Key Establishment Algorithms

Key establishment algorithms establish a shared secret which is used with a key derivation function to derive one or more keys from the shared secret. CSEC approves the use of the following algorithms for the establishment of encryption keys:

- RSA (Rivest, Shamir, Adleman)
- other algorithms based on exponentiation in finite fields (e.g., Diffie-Hellman, MQV)
- Elliptic Curve algorithms

Cryptoperiods shall be approved by CSEC on a case by case basis.

- a. RSA. NIST SP 800-56b^{iv} specifies the RSA algorithm. The modulus shall be at least 1024 bits long for Protected A and B information, and 2048 bits long for Protected C information. By the end of 2013 the modulus length shall be increased to at least 2048 bits for Protected A and B information. The modulus length shall be increased to at least 3072 bits by the end of 2025 for Protected C, and by the end of 2030 for

Le mode compteur avec enchaînement de blocs de chiffrement – code d'authentification de message (CCM pour *Counter with Cipher Block Chaining – Message Authentication Code*), le mode compteur Galois (GCM pour *Galois/Counter Mode*) et le mode GMAC offrent la confidentialité et l'authentification des données pour les algorithmes AES et CAST5 à 128 bits.

Algorithmes d'établissement de clé

Les algorithmes d'établissement de clé créent un secret partagé qui est utilisé avec une fonction de dérivation de clé pour dériver une ou plusieurs clés à partir du secret partagé. Le CSTC autorise l'utilisation des algorithmes suivants pour l'établissement des clés de chiffrement :

- RSA (Rivest, Shamir, Adleman)
- autres algorithmes fondés sur l'exponentiation dans un corps fini (p. ex., Diffie-Hellman, MQV)
- algorithmes à courbe elliptique

Les cryptopériodes doivent être approuvées par le CSTC au cas par cas.

- a. RSA. La publication spéciale 800-56b^{iv} du NIST définit l'algorithme RSA. La taille du module doit être d'au moins 1024 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B et de 2048 bits pour les renseignements PROTÉGÉ C. D'ici la fin de 2013, la taille du module sera augmentée à au moins 2048 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. Elle sera augmentée à au moins 3072 bits d'ici la fin de 2025 pour les

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

all other levels of Protected information.

- b.** Other algorithms based on exponentiation in finite fields. NIST Special Publication 800-56A^V specifies the acceptable key establishment schemes that use discrete logarithm cryptography over finite fields, this includes the Diffie-Hellman and MQV algorithms. The domain parameters for the finite field shall be generated using a method specified in the NIST publication FIPS 186-3 and shall comply with the acceptable parameter sizes specified in SP 800-56A. In particular, the field size shall be prime and shall be at least 1024 bits long for Protected A and B information, and 2048 bits long for Protected C information. By the end of 2013, a field size of at least 2048 bits for Protected A and B information shall be used. By the end of 2025 a field size of at least 3072 bits shall be used for Protected C information. By the end of 2030 a field size of at least 3072 bits shall be used for Protected A and B information.

CSEC must approve the schemes in which the key establishment algorithm is embedded.

- c.** Elliptic Curve Algorithms. NIST SP 800-56A also specifies the acceptable key establishment schemes that use Elliptic

renseignements PROTÉGÉ C, et d'ici la fin de 2030 pour tous les niveaux PROTÉGÉ.

- b.** Autres algorithmes basés sur l'exponentiation dans un corps fini. La publication spéciale 800-56A^V du NIST précise les protocoles d'établissement de clé acceptables qui font appel à la cryptographie à base de logarithmes discrets dans un corps fini, notamment les algorithmes Diffie-Hellman et MQV. Les paramètres de domaine pour le corps fini doivent être générés à l'aide d'une méthode précisée dans la publication FIPS 186-3 du NIST et doivent se conformer aux tailles de paramètres acceptables précisées dans la publication spéciale 800-56A. Plus particulièrement, la cardinalité du corps doit être un nombre premier d'une taille d'au moins 1024 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B et 2048 bits pour les renseignements PROTÉGÉ C. D'ici la fin de 2013, la taille du corps devra être d'au moins 2048 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. D'ici la fin de 2025, elle devra être d'au moins 3072 bits pour les renseignements PROTÉGÉ C. D'ici la fin de 2030, la taille du corps devra être d'au moins 3072 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B.

Le CSTC doit approuver les protocoles dans lesquels l'algorithme d'établissement de clé est intégré.

- c.** Algorithmes à courbe elliptique. La publication spéciale 800-56A du NIST précise également les protocoles

Curve Cryptography (ECC). This includes the Elliptic Curve Diffie-Hellman and ECMQV algorithms. The ECC domain parameters shall be generated as specified in ANS X9.62, or selected from the recommended elliptic curve domain parameters specified in the NIST publication FIPS 186-3. The ECC shall be implemented over a finite field of order q , where q is an odd prime, or of the form 2^m where m is a prime.

Associated with the domain parameters is a key length, the length in bits of the order of the base point. The key length shall be at least 160 bits for Protected A and B information, and 224 bits in length for Protected C information. For Protected A and B information, elliptic curve key lengths of at least 224 bits shall be used by the end of 2013. CSEC strongly recommends the use of the curves found in Appendix D of FIPS 186-3 (Digital Signature Standard). NIST SP 800-56A also gives guidance on the maximum bit length of the cofactor h .

d'établissement de clé acceptables qui font appel à la cryptographie à courbe elliptique (ECC pour *Elliptic Curve Cryptography*), dont les algorithmes Elliptic Curve Diffie-Hellman et ECMQV. Les paramètres du domaine ECC doivent être générés tel qu'il est indiqué dans la norme ANS X9.62, ou sélectionnés à partir des paramètres du domaine à courbe elliptique recommandés dans la publication FIPS 186-3 du NIST. L'ECC doit être mise en œuvre dans un corps fini de l'ordre de q , où q est un nombre premier impair, ou de la forme 2^m où m est un nombre premier. Associée aux paramètres du domaine est une longueur de clé, la longueur en bits de l'ordre du point de référence. La longueur de la clé doit être d'au moins 160 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B, et 224 bits pour les renseignements PROTÉGÉ C. D'ici 2013, des longueurs de clé à courbe elliptique d'au moins 224 bits seront utilisées pour les renseignements PROTÉGÉ A et PROTÉGÉ B. Le CSTC recommande fortement l'emploi des courbes données à l'appendice D de la publication FIPS 186-3 (*Digital Signature Standard*). La publication spéciale 800-56A du NIST donne également de l'orientation sur la longueur maximale en bits du cofacteur h .

CSEC must approve the schemes in which the key exchange is embedded.

Digital Signature Algorithms

The generation of a digital signature requires a cryptographic hash function to operate on the data to be signed as well as

Le CSTC doit approuver les protocoles dans lesquels l'échange de clé est intégré.

Algorithmes de signature numérique

La génération d'une signature numérique nécessite une fonction de hachage cryptographique qui s'exécute sur les données

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

a cryptographic key and a signing algorithm to generate a signature on the output of the hash function.

CSEC approves the use of the following algorithms for digital signature applications:

- RSA (Rivest, Shamir, Adleman)
- DSA (Digital Signature Algorithm)
- other algorithms based on exponentiation in finite fields (e.g. El-Gamal)
- ECDSA (Elliptic Curve Digital Signature Algorithm)

The recommendations below do not apply to signatures made by Certification Authorities (CAs). Consult with CSEC for recommended modulus lengths or field sizes for CAs.

Cryptoperiods shall be approved by CSEC on a case by case basis.

- a. RSA.** The signature schemes are defined in ANSI X9.31 – 1998 and in RSA PKCS #1 v2.1. Guidance for implementation can be found in FIPS 186-3 (Digital Signature Standard). The modulus shall be at least 1024 bits long for Protected A and B information, and 2048 bits long for Protected C information. By the end of 2013 the modulus length shall be increased to at least 2048 bits for Protected A and B information. The modulus length shall be increased to at least 3072 bits by the end of 2025 for Protected C, and by the end of 2030 for all other levels of

à signer, de même qu'une clé cryptographique et un algorithme de signature pour générer une signature sur les résultats de la fonction de hachage.

Le CSTC approuve l'utilisation des algorithmes suivants pour les applications de signature numérique :

- RSA (Rivest, Shamir, Adleman)
- DSA (*Digital Signature Algorithm*)
- autres algorithmes fondés sur l'exponentiation dans un corps fini (p. ex., El-Gamal)
- ECDSA (*Elliptic Curve Digital Signature Algorithm*)

Les recommandations ci-dessous ne s'appliquent pas aux signatures générées par des autorités de certification (AC). Prière de consulter le CSTC pour la taille recommandée des modules ou des cardinalités pour les AC.

Les cryptopériodes doivent être approuvées par le CSTC.

- a. RSA.** Les protocoles de signature sont définis dans la norme ANSI X9.31 – 1998 et dans la RSA PKCS #1 v2.1. Les directives relatives à la mise en œuvre sont données dans la norme FIPS 186-3 (*Digital Signature Standard*). La taille du module doit être d'au moins 1024 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B et 2048 bits pour les renseignements PROTÉGÉ C. D'ici la fin de 2013, la taille du module sera augmentée à au moins 2048 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. La taille du module sera augmentée à au moins 3072 bits d'ici la fin

Protected information.

de 2025 pour les renseignements PROTÉGÉ C, et d'ici la fin de 2030 pour tous les niveaux PROTÉGÉ.

b. DSA. This signature scheme is defined in FIPS 186-3 (Digital Signature Standard). For Protected A and B information the prime modulus shall be at least 1024 bits long. For Protected C information the modulus shall be at least 2048 bits long. By the end of 2013, the modulus lengths shall be increased to at least 2048 bits for Protected A and B information. The modulus length shall be increased to at least 3072 bits by the end of 2025 for Protected C, and by the end of 2030 for all other levels of Protected information.

b. DSA. Ce protocole de signature est défini dans la norme FIPS 186-3 (*Digital Signature Standard*). Le module, dont la cardinalité est un nombre premier, doit avoir une taille d'au moins 1024 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. Pour les renseignements PROTÉGÉ C, la taille du module doit être d'au moins 2048 bits. D'ici la fin de 2013, elle sera augmentée à au moins 2048 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. La taille du module sera augmentée à au moins 3072 bits d'ici la fin de 2025 pour les renseignements PROTÉGÉ C, et d'ici la fin de 2030 pour tous les niveaux PROTÉGÉ.

c. Other algorithms based on exponentiation in finite fields (e.g. El-Gamal). The field size shall be prime and shall be at least 1024 bits in length for Protected A and B information. For Protected C information, a field size of at least 2048 bits shall be used. By the end of 2013, the field size shall be increased to at least 2048 bits for Protected A and B information. The modulus length shall be increased to at least 3072 bits by the end of 2025 for Protected C, and by the end of 2030 for all levels of Protected information.

c. Autres algorithmes fondés sur l'exponentiation dans un corps fini (p. ex., El-Gamal). La cardinalité du corps doit être un nombre premier et sa taille doit être d'au moins 1024 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. Pour les renseignements PROTÉGÉ C, un corps d'au moins 2048 bits sera utilisé. D'ici la fin de 2013, la taille du corps sera augmentée à au moins 2048 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B. La taille du module sera augmentée à au moins 3072 bits d'ici la fin de 2025 pour les renseignements PROTÉGÉ C, et d'ici la fin de 2030 pour tous les niveaux PROTÉGÉ.

March 2011

ITSA-11E

Mars 2011

CSEC must approve the schemes in which the digital signature algorithm is embedded.

d. ECDSA. This signature scheme is defined in ANSI X9.62 –2005. Guidance for implementation can be found in FIPS 186-3 (Digital Signature Standard). The elliptic curve key length shall be at least 160 bits for Protected A and B information, and 224 bits for Protected C information. For Protected A and B information, elliptic curve key lengths of at least 224 bits shall be used by the end of 2013. CSEC strongly recommends the use of the curves in Appendix D of FIPS 186-3.

Hashing Algorithms and Status of SHA-1

CSEC approves the use of SHA-224, SHA-256, SHA-384, and SHA-512 for Protected A, B, and C information. These algorithms are defined in FIPS 180-3 (Secure Hash Standard).

The use of SHA-1 for digital signature generation for Protected A and B information should be discontinued by the end of 2013. For Protected C information, the use of SHA-1 for digital signature generation should have been discontinued in 2008.

SHA-1 can be used for all other hash function applications including HMAC, key

Le CSTC doit approuver les protocoles dans lesquels l'algorithme de signature numérique est intégré.

d. ECDSA. Ce protocole de signature est défini dans la norme ANSI X9.62 –2005. Les directives relatives à sa mise en œuvre sont données dans la norme FIPS 186-3 (*Digital Signature Standard*). La taille de la courbe elliptique doit être d'au moins 160 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B et d'au moins 224 bits pour les renseignements PROTÉGÉ C. Pour les renseignements PROTÉGÉ A et PROTÉGÉ B, des clés de courbe elliptique d'une longueur minimale de 224 bits seront utilisées d'ici la fin de 2013. Le CSTC recommande fortement l'utilisation des courbes elliptiques figurant à l'appendice D de la norme FIPS 186-3.

Algorithmes de hachage et situation de l'algorithme SHA-1

Le CSTC autorise l'utilisation des algorithmes SHA-224, SHA-256, SHA-384 et SHA-512 pour les renseignements PROTÉGÉ A, PROTÉGÉ B et PROTÉGÉ C. Ces algorithmes sont définis dans la norme FIPS 180-3 (*Secure Hash Standard*).

L'utilisation de SHA-1 pour la génération de signature numérique pour les renseignements PROTÉGÉ A et PROTÉGÉ B devrait être abandonnée d'ici 2013. Pour les renseignements PROTÉGÉ C, l'utilisation de l'algorithme SHA-1 pour la génération de la signature numérique aurait dû avoir été abandonnée en 2008.

L'algorithme SHA-1 peut être utilisé pour toutes les autres applications de la fonction de



March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

derivation functions, and random number generation.

Although the use of SHA-1 is permitted, CSEC strongly recommends the use of SHA-224 or higher whenever possible.

Data Integrity Algorithms

A message authentication code (MAC) is intended to ensure data integrity and data origin authentication. CSEC approves the use of the following message authentication codes:

- HMAC (Hash-based MAC)
 - CMAC (Cipher-based MAC)
 - GMAC/Galois Counter Mode and CCM
- a. HMAC.** The Hash-based MAC is defined in FIPS 198-1 (The Keyed-Hash Message Authentication Code (HMAC)) issued in 2008. Key lengths shall be at least 80 bits. By the end of 2013, key lengths shall be increased to at least 112 bits.
- b. CMAC.** The use of Cipher-based MAC with AES or Triple DES as defined in NIST Special Publication 800-38B is approved for use with all Protected

hachage, y compris HMAC, les fonctions de dérivation de clé et la génération de nombres aléatoires.

Quoique l'utilisation de l'algorithme SHA-1 soit autorisée, le CSTC recommande fortement l'emploi de l'algorithme SHA-224 ou d'un algorithme supérieur dans la mesure du possible.

Algorithmes d'intégrité des données

Un code d'authentification de message (MAC pour *Message Authentication Code*) sert à assurer l'intégrité des données et l'authentification de l'origine des données. Le CSTC autorise l'utilisation des codes d'authentification de message suivants :

- HMAC (MAC à base de fonction de hachage)
 - CMAC (MAC à base de fonction de chiffrement)
 - GMAC/mode compteur Galois et CCM
- a. HMAC.** Le MAC à base de fonction de hachage est défini dans la norme FIPS 198-1 (*The Keyed-Hash Message Authentication Code [HMAC]*) publiée en 2008. Les clés doivent être d'une longueur d'au moins 80 bits. D'ici la fin de 2013, la longueur des clés augmentera à au moins 112 bits.
- b. CMAC.** L'utilisation du MAC à base de fonction de chiffrement avec l'algorithme AES ou Triple DES tel qu'elle est définie dans la publication spéciale 800-38B du



information. The use of 2-key Triple DES shall be discontinued by the end of 2015. Tag lengths shall be at least 90 bits for Protected A and B information and 122 bits for Protected C information. For Protected A and B information, tag lengths of at least 122 bits shall be used by the end of 2013.^{vi}

- c. GMAC/GCM and CCM.** The CCM mode is specified in NIST SP 800-38C and GMAC/GCM is specified in NIST SP 800-38D. These can be used for all levels of Protected information.

Key Derivation Functions

CSEC approves the use of the following key derivation functions (KDF) to derive secret keying material from a shared secret. The following KDF are defined in NIST SP 800-56A.

- Concatenation KDF
- ASN.1 KDF

NIST SP 800-108 specifies key derivation functions that use a cryptographic key to generate additional cryptographic keys.

- HMAC-based KDF
- CMAC-based KDF using AES

NIST est approuvée pour protéger les renseignements PROTÉGÉ de tous les niveaux. L'utilisation de Triple DES à 2 clés sera abandonnée d'ici la fin de 2015. La longueur de l'étiquette doit être d'au moins 90 bits pour les renseignements PROTÉGÉ A et PROTÉGÉ B et 122 bits pour les renseignements PROTÉGÉ C. Pour les renseignements PROTÉGÉ A et PROTÉGÉ B, des étiquettes d'une longueur d'au moins 122 bits seront utilisées d'ici la fin de 2013^{vi}.

- c. GMAC/GCM et CCM.** Le mode CCM est précisé dans la publication spéciale 800-38C du NIST, et le GMAC/GCM dans la publication spéciale 800-38D. Ces algorithmes peuvent être utilisés pour tous les niveaux PROTÉGÉ.

Fonction de dérivation de clé

Le CSTC approuve l'utilisation des fonctions de dérivation de clé (KDF pour *Key Derivation Function*) suivantes pour dériver le matériel de chiffrement secret à partir d'un secret partagé. Les KDF suivantes sont définies dans la publication spéciale 800-56A du NIST.

- Concatenation KDF
- ASN.1 KDF

La publication spéciale 800-108 du NIST précise les fonctions de dérivation de clé qui utilisent une clé cryptographique pour générer des clés cryptographiques additionnelles.

- HMAC-based KDF (KDF à base de HMAC)
- CMAC-based KDF using AES (KDF à

- CMAC-based KDF using Triple DES

The use of two-key Triple DES as the block cipher in a CMAC-based KDF shall be discontinued by the end of 2015.

Key Wrapping and Key Transport

Key wrapping is the encryption of a symmetric key by another symmetric key with integrity protection. CSEC approves the use of the following algorithms for key wrapping:

- AES
- Triple DES

While there is currently no key wrapping standard, there is an informal specification for key wrapping using AES^{vii}. If Triple DES is the chosen algorithm, the same technique shall be used.

The use of 2-key Triple DES has the restriction that at most 2^{20} blocks of data can be encrypted with the same key. The 2-key Triple DES key wrapping algorithm should be discontinued by the end of 2015. The use of 3-key Triple DES is the preferred option.

Key Transport is required when one party determines the key. CSEC approves the use of RSA for key transport as defined in NIST SP 800-56b. The modulus shall be at least

base de CMAC utilisant AES)

- CMAC-based KDF using Triple DES (KDF à base de CMAC utilisant Triple DES)

L'utilisation de Triple DES à 2 clés comme algorithme de chiffrement par blocs dans le KDF à base CMAC sera abandonnée d'ici la fin de 2015.

Enveloppement et transport des clés

On entend par « enveloppement de clé » le chiffrement d'une clé symétrique par une autre clé symétrique avec protection de l'intégrité. Le CSTC approuve l'utilisation des algorithmes suivants pour l'enveloppement des clés :

- AES
- Triple DES

Quoiqu'il n'existe aucune norme à l'heure actuelle pour l'enveloppement des clés, il existe une spécification non officielle à l'aide d'AES^{vii}. Si Triple DES est l'algorithme choisi, la même technique doit être utilisée.

L'utilisation du Triple DES à 2 clés a pour restriction qu'au plus 2^{20} blocs de données peuvent être chiffrés à l'aide de la même clé. L'algorithme d'enveloppement de clé Triple DES à 2 clés devrait être abandonné d'ici la fin de 2015. L'emploi de Triple DES à 3 clés est l'option de premier choix.

Le transport de clé est requis lorsqu'une partie détermine la clé. Le CSTC approuve l'utilisation de RSA pour le transport de clé tel qu'il est défini dans la publication spéciale

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

1024 bits long for Protected A and B information, and 2048 bits long for Protected C information. By the end of 2013 the modulus length shall be increased to at least 2048 for Protected A and B information.

Padding Schemes

Some of the key establishment and digital signature algorithms listed above require that a padding scheme be defined when the algorithm is used.

CSEC approves the use of the following RSA padding scheme for key establishment:

- a. From RSA PKCS #1 v2.1, the padding scheme defined as RSAES-OAEP

CSEC approves the use of the following RSA padding schemes for digital signatures:

- a. The padding scheme defined in ANSI X9.31
- b. From RSA PKCS #1 v2.1, the padding scheme defined as RSASSA-PSS

The use of SHA-1 in any padding scheme for digital signature generation shall be discontinued by the end of 2013.

Random Bit Generation

A CSEC approved random bit generator, (sometimes referred to as random number generator) has two components: an entropy

800-56b du NIST. La taille du module doit être d'au moins 1024 bits pour l'information PROTÉGÉ A et PROTÉGÉ B, et 2048 bits pour l'information PROTÉGÉ C. D'ici la fin de 2013, la taille du module sera augmentée à au moins 2048 bits pour l'information PROTÉGÉ A et PROTÉGÉ B.

Protocoles de bourrage

Certains des algorithmes d'établissement de clé et de signature numérique énumérés plus haut ne peuvent être utilisés si aucun protocole de bourrage n'est défini.

Le CSTC autorise l'utilisation des protocoles de bourrage RSA suivants pour l'établissement de clé :

- a. de la RSA PKCS #1 v2.1, le protocole de bourrage appelé RSAES-OAEP.

Le CSTC autorise l'utilisation des protocoles de bourrage RSA suivants pour la signature numérique :

- a. le protocole de bourrage défini dans la norme ANSI X9.31;
- b. de la RSA PKCS #1 v2.1, le protocole de bourrage appelé RSAES-PSS.

L'utilisation d'un protocole de bourrage quelconque avec l'algorithme SHA-1 sera abandonnée d'ici la fin de 2013.

Génération de bits aléatoires

Un générateur de bits aléatoires approuvé par le CSTC (parfois appelé « générateur de nombres aléatoires ») a deux composantes :

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

source and a deterministic random bit generator (DRBG). The entropy source is used to seed the DRBG, which produces pseudorandom output.

CSEC approves the following DRBGs for the production of random bits with the limitations outlined below:

- Hash_DRBG
- HMAC_DRBG
- CTR_DRBG
- Dual_EC_DRBG

It is preferable to reseed the DRBG as frequently as possible. The maximum number of outputs made by an implementation between reseeds shall be approved by CSEC.

When output from one of the above DRBGs is converted to random numbers, one of the methods given in NIST Special Publication 800-90^{viii} shall be used.

All implementations of the following algorithms must conform to NIST Special Publication 800-90.

- a. **Hash_DRBG** is approved for use with one of the hash algorithms approved above.
- b. **HMAC_DRBG** is approved for use with one of the hash algorithms approved above. The HMAC_DRBG is also

une source d'entropie et un générateur déterministe de bits aléatoires (DRBG pour *deterministic random bit generator*). La source d'entropie sert à initialiser le DRBG en lui fournissant une graine ou germe (*seed*) pour qu'il produise la sortie pseudo-aléatoire.

Le CSTC autorise l'utilisation des DRBG suivants pour la production de bits aléatoires, avec les restrictions décrites plus bas :

- Hash_DRBG
- HMAC_DRBG
- CTR_DRBG
- Dual_EC_DRBG

Il est préférable de réinitialiser le DRBG (en lui fournissant de nouvelles graines) le plus souvent possible. Le nombre maximal de sorties faites par une version entre réinitialisations doit être approuvé par le CSTC.

Lorsque la sortie d'un des DRBG ci-dessus est convertie en nombres aléatoires, l'une des méthodes décrites dans la publication spéciale 800-90 du NIST^{viii} doit être utilisée.

Toutes les versions des algorithmes suivants doivent se conformer à la publication spéciale 800-90 du NIST.

- a. L'utilisation de **Hash_DRBG** est approuvée avec l'un des algorithmes de hachage approuvés plus haut.
- b. L'utilisation de **HMAC_DRBG** est approuvée avec l'un des algorithmes de hachage approuvés plus haut. Le

March 2011	ITSA-11E	Mars 2011
------------	----------	-----------

specified in Appendix D of ANS X9.62:2005.

HMAC_DRBG est également précisé dans l'appendice D de la publication ANS X9.62:2005.

c. CTR_DRBG is approved for use with Triple DES used with 3 independent keys or with AES.

c. L'utilisation de **CTR_DRBG** est approuvée avec l'algorithme Triple DES utilisé avec 3 clés indépendantes ou avec l'algorithme AES.

d. Dual_EC_DRBG is approved for use with the NIST prime curves P-224, P-256, P-384, or P-512 and their associated parameters.

d. L'utilisation de **Dual_EC_DRBG** est approuvée avec les courbes elliptiques définies sur un corps premier P-224, P-256, P-384 ou P-512 du NIST, et les paramètres connexes.

CSEC also approves the use of the legacy DRBGs which shall be discontinued by the end of 2015. Appendix 3 of FIPS 186-2 (Digital Signature Standard) specifies the use of SHA-1 and DES to generate random bits. It is recommended to use FIPS 186-3 which updates these methods to use SHA-224 and higher.

Le CSTC approuve également l'utilisation de DRBG patrimoniaux qui seront abandonnés d'ici la fin de 2015. L'appendice 3 de la FIPS 186-2 (*Digital Signature Standard*) précise l'utilisation de SHA-1 et de DES pour générer des bits aléatoires. Il est recommandé d'utiliser la FIPS 186-3 dans laquelle ces méthodes ont été mises à jour pour utiliser SHA-224 et les versions ultérieures.

Contacts and Assistance

IT Security Client Services

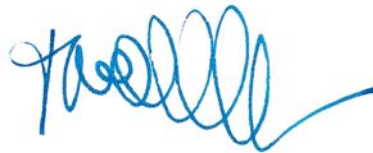
Communications Security Establishment
Canada
P.O. Box 9703, Terminal
Ottawa, Ontario K1G 3Z4
Telephone: (613) 991-7654
e-mail : ITScientservices@cse-cst.gc.ca

Aide et renseignements

Services à la clientèle de la Sécurité des TI

Centre de la sécurité des télécommunications
Canada
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4
Téléphone : (613) 991-7654
Courriel : ITScient.services@cse-cst.gc.ca

La chef adjointe de la Sécurité des TI,



Toni Moffa
Deputy Chief, IT Security

ⁱ <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>

ⁱⁱ 2-key Triple DES is considered to have 100 bits of security given the restriction that at most 2^{20} blocks of data are encrypted with the same key. It is considered to have 80 bits of security if an attacker has access to 2^{40} matched plaintext and ciphertext blocks. / Le Triple DES à 2 clés est considéré comme ayant 100 bits de sécurité étant donné la restriction qu'au plus 2^{20} blocs de données sont chiffrés à l'aide de la même clé. Il est considéré comme ayant 80 bits de sécurité si un attaquant a accès à 2^{40} blocs appariés de texte en clair et de cryptogramme.

ⁱⁱⁱ <http://www.ietf.org/rfc/rfc2144.txt>

^{iv} <http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf>

^v http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf

^{vi} Tag lengths are based on implementations that permit a maximum of 1024 invalid messages. For implementations that permit greater numbers of invalid messages, tag lengths shall be determined in consultation with CSEC.

Les longueurs d'étiquette reposent sur les versions permettant un nombre maximal de 1024 messages invalides. Pour les versions permettant un plus grand nombre de messages invalides, les longueurs d'étiquette devront être déterminées en collaboration avec le CSTC.

^{vii} http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf

^{viii} http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf