



IT Security Bulletin

Bulletin de sécurité TI

March 2011

ITSB-40A

Mars 2011

Government of Canada Policy for the Protection of Classified Information Using Suite B Algorithms

Politique du gouvernement du Canada pour la protection de l'information classifiée à l'aide d'algorithmes Suite B

Purpose

The purpose of this Bulletin is to provide Government of Canada (GC) departments with the Communications Security Establishment Canada (CSEC) policy on:

- using Suite B algorithms for the protection of classified information at the SECRET and TOP SECRET level
- the standards and NIST Special Publications that describe the cryptographic algorithms required for Suite B

Background

Suite B is a specific set of cryptographic algorithms suitable for protecting classified information throughout the Canadian government to support interoperability with allies and coalition partners. Suite B can protect classified information at the SECRET and TOP SECRET level. Suite B uses elliptic curve cryptography to promote interoperability.

All Suite B algorithms are described in Federal Information Processing Standards (FIPS),

Objet

Le présent bulletin vise à présenter aux ministères du gouvernement du Canada (GC) la politique du Centre de la sécurité des télécommunications Canada (CSTC) sur :

- l'utilisation des algorithmes Suite B pour la protection de l'information classifiée aux niveaux SECRET et TRÈS SECRET;
- les normes et les publications spéciales du NIST dans lesquelles sont décrits les algorithmes cryptographiques nécessaires pour la Suite B.

Contexte

La Suite B est un ensemble particulier d'algorithmes cryptographiques qui convient à la protection de l'information classifiée à l'échelle du gouvernement canadien à l'appui de l'interopérabilité avec les alliés et les partenaires de la coalition. La Suite B peut protéger l'information classifiée aux niveaux SECRET et TRÈS SECRET. Elle fait appel à la cryptographie à courbe elliptique pour assurer l'interopérabilité.

Tous les algorithmes Suite B sont décrits dans les normes Federal Information Processing Standards

National Institute of Standards and Technology (NIST) Special Publications (SP), and Internet Engineering Task Force (IETF) standards.

Policy

Government of Canada departments must adhere to the following CSEC security guidelines when using Suite B for the protection of classified information at the SECRET and TOP SECRET level.

Products used to protect classified information using Suite B algorithms must be approved by CSEC on a case-by-case basis. Products that have only received a FIPS 140-2 or/and a FIPS 140-3 validation are **not** adequate or approved by CSEC for the protection of classified information.

The Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), Elliptic Curve Digital Signature Algorithm (ECDSA), and the Elliptic Curve Diffie-Hellman (ECDH) key agreement are the approved Suite B algorithms.

Table 1 lists the minimum Suite B cryptographic parameter requirements to be used for the protection of classified information at the SECRET and TOP SECRET level.

TOP SECRET requirements must be used when communicating between SECRET and TOP SECRET networks. Given that products approved up to the TOP SECRET level will only contain algorithms with the TOP SECRET cryptographic parameter requirements, TOP SECRET cryptographic parameter requirements may be used for all communications for

(FIPS), les publications spéciales (SP pour *Special Publications*) du National Institute of Standards and Technology (NIST) et les normes de l'Internet Engineering Task Force (IETF).

Politique

Les ministères du GC doivent observer les lignes directrices du CSTC en matière de sécurité lorsqu'ils utilisent la Suite B pour protéger l'information classifiée aux niveaux SECRET et TRÈS SECRET.

Les produits utilisés pour protéger l'information classifiée à l'aide d'algorithmes Suite B doivent être approuvés par le CSTC au cas par cas. Les produits qui n'ont reçu qu'une validation FIPS 140-2 ou FIPS 140-3 **ne** sont **ni** adéquats **ni** approuvés par le CSTC pour protéger l'information classifiée.

Les algorithmes Suite B approuvés sont les suivants : Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), Elliptic Curve Digital Signature Algorithm (ECDSA) et les agréments de clé Elliptic Curve Diffie-Hellman (ECDH).

Le tableau 1 énumère les exigences minimales liées aux paramètres cryptographiques Suite B qui doivent être utilisés pour la protection de l'information classifiée aux niveaux SECRET et TRÈS SECRET.

Les exigences liées au niveau TRÈS SECRET doivent être respectées dans les communications entre des réseaux SECRET et TRÈS SECRET. Étant donné que les produits approuvés jusqu'au niveau de classification TRÈS SECRET inclusivement ne contiennent que des algorithmes répondant aux exigences de paramètres cryptographiques TRÈS SECRET, ces dernières peuvent être utilisées pour toutes les communications pour une plus grande

March 2011	ITSB-40A	Mars 2011
------------	----------	-----------

increased interoperability.

interopérabilité.

**Table 1 – Suite B Cryptographic Parameter Requirements for Classified Applications/
Tableau 1 – Exigences liées aux paramètres cryptographiques Suite B pour les applications classifiées**

	Cryptographic Algorithm or Protocol/ Algorithme ou protocole cryptographique	Standard/ Norme	Minimum Requirements for classified information up to SECRET/ Exigences minimales pour l'information classifiée jusqu'au niveau SECRET	Minimum Requirements for TOP SECRET/ Exigences minimales pour l'information TRÈS SECRET
Encryption/ Chiffrement	Advanced Encryption Standard (AES)	FIPS 197	128 bit key/Clé de 128 bits	256 bit key/Clé de 256 bits
Hashing/ Hachage	Secure Hash Algorithm (SHA)	FIPS 180-3	SHA-256	SHA-384
Digital Signature/ Signature numérique	Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-3 ANSI X9.62	256 bits over prime field/256 bits sur un corps dont la cardinalité est un nombre premier	384 bits over prime field/384 bits sur un corps dont la cardinalité est un nombre premier
Key Exchange/ Échange de clés	Elliptic Curve Diffie-Hellman (ECDH)	SP 800-56A ANSI X9.63	256 bits over prime field/256 bits sur un corps dont la cardinalité est un nombre premier	384 bits over prime field/384 bits sur un corps dont la cardinalité est un nombre premier

The elliptic curves are defined in the Appendix D of FIPS 186-3.

Les courbes elliptiques sont définies dans l'appendice D de la norme FIPS 186-3.

The preferred ECDH key agreement scheme is the Ephemeral Unified Model. The second approved ECDH key agreement scheme is the One-Pass Diffie-Hellman scheme.

Le protocole d'agrément de clé ECDH de prédilection est l'Ephemeral Unified Model. Le second protocole d'agrément de clé ECDH approuvé est le protocole One-Pass Diffie-Hellman (Diffie-Hellman à une passe).

The approved Suite B cryptographic algorithms can be used with the internet protocols Transport

Les algorithmes cryptographiques Suite B peuvent être utilisés avec les protocoles Internet Sécurité de

Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Shell (SSH), and the Internet Protocol Security (IPsec) using version one or two of the Internet Key Exchange (IKE). These internet protocols must have Suite B compliant implementations and follow the guidance documents found in the References section.

References

The standards and special publications associated with Suite B algorithms are found at:

Encryption:

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Hashing:

http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Digital Signature:

http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

Key Exchange:

http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf

Implementation guidance for internet protocols can be found at:

Suite B Cipher Suites for TLS, RFC 5430

<http://tools.ietf.org/html/rfc5430>

TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

<http://tools.ietf.org/html/rfc5289>

Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME), RFC 5008

<http://tools.ietf.org/html/rfc5008>

AES Galois Counter Mode for the Secure Shell

la couche transport (TLS pour *Transport Layer Security*), Secure/Multipurpose Internet Mail Extensions (S/MIME) et Secure Shell (SSH), et la Sécurité du protocole Internet (IPSec pour *Internet Protocol Security*) utilisée avec la version 1 ou 2 de l'échange de clé Internet (IKE pour *Internet Key Exchange*). Ces protocoles Internet doivent avoir des versions compatibles Suite B et doivent se conformer aux documents d'orientation donnés dans la section Références.

Références

Les normes et publications spéciales associées aux algorithmes Suite B sont disponibles dans les sites suivants (en anglais seulement) :

Chiffrement :

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Hachage :

http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Signature numérique :

http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

Échange de clés :

http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf

Les directives liées aux versions des protocoles Internet sont données dans les sites suivants (en anglais seulement) :

Suite B Cipher Suites for TLS, RFC 5430

<http://tools.ietf.org/html/rfc5430>

TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

<http://tools.ietf.org/html/rfc5289>

Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME), RFC 5008

<http://tools.ietf.org/html/rfc5008>

AES Galois Counter Mode for the Secure Shell

Transport Layer Protocol, RFC 5647
<http://tools.ietf.org/html/rfc5647>
Suite B Cryptography for IPsec, RFC 4869
<http://tools.ietf.org/html/rfc4869>

There are implementation guides to assist the development of Suite B products:

Suite B Implementer's Guide to NIST SP 800-56A
http://www.nsa.gov/ia/files/SuiteB_Implementer_G-113808.pdf
Suite B Implementer's Guide to FIPS 186-3
<http://www.nsa.gov/ia/files/ecdsa.pdf>
Mathematical Routines for NIST Prime Elliptic Curves
<http://www.nsa.gov/ia/files/nist-routines.pdf>
Suite B Certificate and Certificate Revocation List (CRL) Profile, RFC 5759
<http://tools.ietf.org/html/rfc5759>

Contacts and Assistance

IT Security Client Services
Communications Security Establishment Canada

PO Box 9703, Terminal
Ottawa, ON K1G 3Z4
By email: itsclientservices@cse-cst.gc.ca
Telephone: 613-991-7654

Transport Layer Protocol, RFC 5647
<http://tools.ietf.org/html/rfc5647>
Suite B Cryptography for IPsec, RFC 4869
<http://tools.ietf.org/html/rfc4869>

Il existe également des guides de mise en œuvre pour aider au développement de produits Suite B (en anglais seulement) :

Suite B Implementer's Guide to NIST SP 800-56A
http://www.nsa.gov/ia/files/SuiteB_Implementer_G-113808.pdf
Suite B Implementer's Guide to FIPS 186-3
<http://www.nsa.gov/ia/files/ecdsa.pdf>
Mathematical Routines for NIST Prime Elliptic Curves
<http://www.nsa.gov/ia/files/nist-routines.pdf>
Suite B Certificate and Certificate Revocation List (CRL) Profile, RFC 5759
<http://tools.ietf.org/html/rfc5759>

Aide et renseignements

Services à la clientèle en Sécurité des TI
Centre de la sécurité des télécommunications
Canada
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4
Par courriel : itsclientservices@cse-cst.gc.ca
Téléphone : 613-991-7654

La chef adjointe de la Sécurité des TI,



Toni Moffa
Deputy Chief, IT Security