Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

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

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),

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

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

Canada

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

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

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IT Security Bulletin
Bulletin de sécurité TI

March 2011 | ITSB-57B | Mars 2011

Security of BlackBerry PIN-to-PIN Messaging

Purpose

The purpose of this Bulletin is to advise Government of Canada (GC) departments and agencies of the security vulnerabilities arising from the use of the BlackBerry PIN-to-PIN messaging service.

Background

The CSEC document entitled ITSPSR-18A "Smartphone Vulnerability Assessment" discusses security issues with smartphones. As explained in this document, the Research-In-Motion (RIM) BlackBerry device offers two types of communication:

- **Voice** – a built-in cellular telephone allows the user to make voice calls. Security features available for voice calls depend on the cellular technology (i.e. GSM or CDMA) used in the particular BlackBerry model and features supported by the cellular carrier; no additional security for voice calls is provided by the BlackBerry; and

Sécurité de la messagerie BlackBerry NIP à NIP

Objet

Le présent bulletin a pour objet d'informer les ministères et organismes du gouvernement du Canada (GC) des vulnérabilités en matière de sécurité résultant de l'utilisation du service de messagerie NIP à NIP du BlackBerry.

Contexte

Le document ITSPSR-18A du Centre de la sécurité des télécommunications Canada (CSTC) intitulé *Évaluation des vulnérabilités des téléphones intelligents* traite des problèmes de sécurité liés aux téléphones intelligents. Tel qu'il est expliqué dans le document, le dispositif BlackBerry de Research-In-Motion (RIM) offre deux types de communications:

- **Communications vocales** – Un téléphone cellulaire intégré permet à l'utilisateur d'établir des communications vocales. Les fonctions de sécurité disponibles pour les communications vocales dépendent de la technologie cellulaire (c.-à-d. GSM ou AMRC) utilisée dans le modèle BlackBerry particulier et des fonctions prises en charge par l'entreprise de téléphonie cellulaire; le BlackBerry n'offre aucune sécurité additionnelle pour les communications vocales;

Canada

- **Data** – the BlackBerry allows e-mail and other data transmissions (including PIN-to-PIN, Internet browsing, and other voice-data service messages) to be sent over the air. As for voice, security features for data transmissions depend on the cellular technology (e.g., Mobitex, GPRS/EDGE, 1xRTT, HSDPA, etc.) and features supported by the carrier/service provider for each particular model of BlackBerry device, but in the case of data, transmissions may also be further encrypted by the BlackBerry device for added security.

This Bulletin will focus on threats to the security of data transmissions related specifically to PIN-to-PIN communications on BlackBerry devices. GC clients interested in further details on other aspects of BlackBerry and smartphone security are advised to refer to ITSPSR-18A or to contact CSEC Client Services.

BlackBerry Internet Service (BIS) vs. BlackBerry Enterprise Server (BES)

BlackBerry devices sold through wireless service providers may be used with the consumer service (BlackBerry Internet Service (BIS), the service offered with most privately-owned devices) or with the enterprise service (BlackBerry Enterprise Server, commonly known as BES).

From a basic security perspective, the BES includes supplementary encryption and data protection for enterprise BlackBerry device users, whereas the BIS does not. From a connectivity perspective, the BES allows BlackBerry devices to be connected to

- **Communications de données** – Le BlackBerry permet la transmission par ondes hertziennes de courriels et d'autres données (y compris NIP à NIP, la navigation dans Internet, et d'autres messages de service voix-données). Comme pour les communications vocales, les fonctions de sécurité liées aux transmissions de données dépendent de la technologie cellulaire (p. ex., Mobitex, GPRS/EDGE, 1xRTT, HSDPA, etc.) utilisée et des fonctions prises en charge par l'entreprise de téléphonie cellulaire ou le fournisseur de services pour chaque modèle BlackBerry, mais les données peuvent être également chiffrées par le dispositif BlackBerry comme sécurité additionnelle.

Le présent bulletin porte principalement sur les menaces envers la sécurité des transmissions de données en ce qui a trait aux communications NIP à NIP sur les dispositifs BlackBerry. Les clients du GC intéressés à se renseigner davantage sur les autres aspects de la sécurité du BlackBerry et des téléphones intelligents sont priés de se reporter à l'ITSPSR-18A ou de communiquer avec les Services à la clientèle du CSTC.

Service Internet BlackBerry (BIS) et Serveur d'entreprise BlackBerry (BES)

Les dispositifs BlackBerry vendus par l'entremise des fournisseurs de services sans fil peuvent être utilisés en conjonction avec le service de consommation (Service Internet BlackBerry ou BIS pour *BlackBerry Internet Service*, service offert avec la majorité des dispositifs privés) ou avec le service d'entreprise (Serveur d'entreprise BlackBerry Enterprise ou BES pour *BlackBerry Enterprise Server*).

Du point de vue de la sécurité de base, le BES comprend un chiffrement et une protection des données additionnels pour les utilisateurs de dispositifs BlackBerry d'entreprise, tandis que le BIS n'en comprend pas. Du point de vue de la connectivité, le BES permet aux dispositifs BlackBerry de se connecter aux serveurs de

departmental mail servers and to access internal services.

While there are several methods that may be used, CSEC recommends using the BES to comply with the data protection requirements of the Policy on Government Security (PGS). The rest of this Bulletin assumes that the BES is being used.

E-mail and PIN-to-PIN Messaging Differences

Figure 1 illustrates the components involved in sending or receiving e-mail messages on an enterprise BlackBerry device.

courriel de l'entreprise et d'accéder aux services internes.

Bien qu'il existe plusieurs méthodes, CSTC recommande l'utilisation du BES afin de respecter les exigences en matière de protection de données de la *Politique sur la sécurité du gouvernement* (PSG). Le reste du bulletin repose sur l'hypothèse qu'on utilise le BES.

Différences entre les courriels et les messages NIP à NIP

La figure 1 illustre les composants qui entrent en jeu lorsqu'on envoie ou qu'on reçoit un courriel à l'aide d'un dispositif BlackBerry d'entreprise.

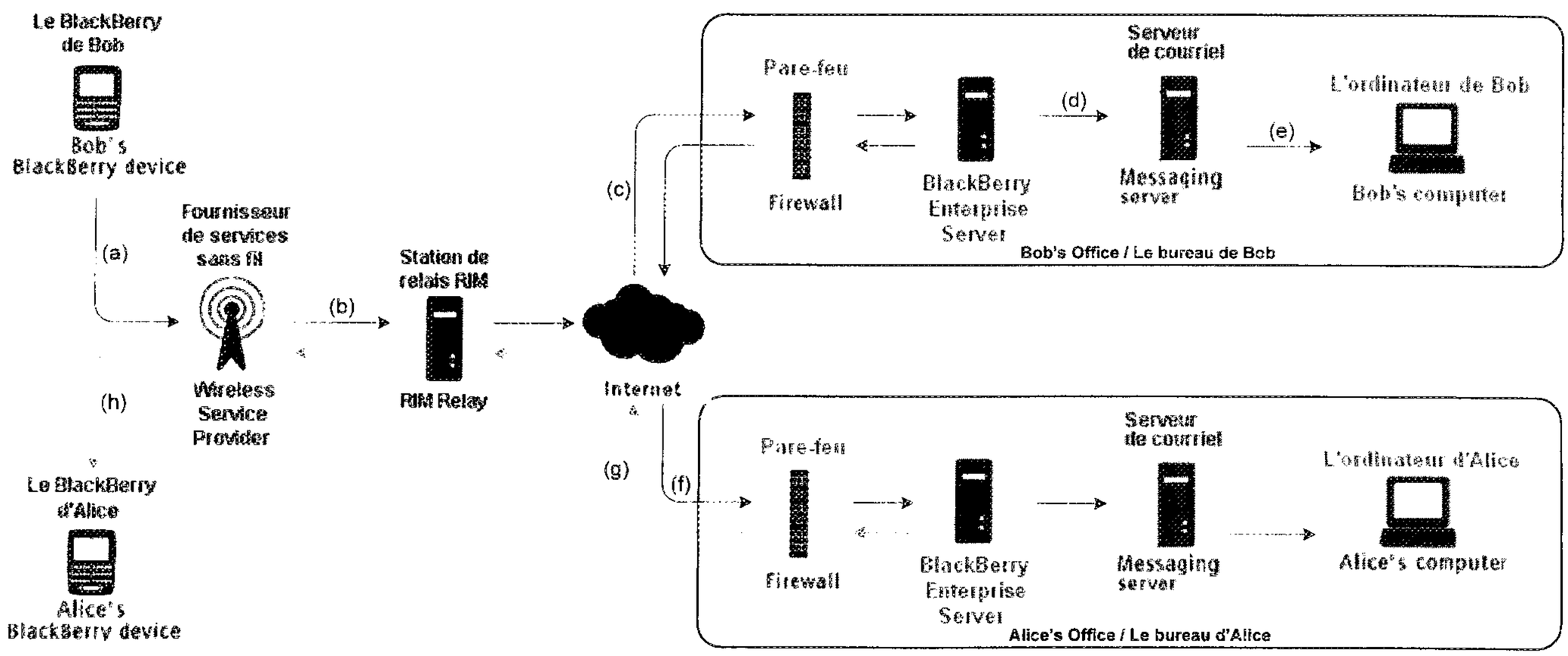


Figure 1 - Sending/Receiving E-mail on a BlackBerry device using a BES
Envoi et réception des courriels sur un dispositif BlackBerry en utilisant un BES

As shown in Figure 1, e-mail messages sent from a BlackBerry device are first AES-encrypted, and passed to the user's wireless service provider (a), which then forwards the message to one of the global relay servers operated by RIM (b). The RIM relay passes the

Comme il est illustré dans la figure 1, un courriel envoyé à partir d'un dispositif BlackBerry est tout d'abord chiffré à l'aide de AES et transmis au fournisseur de services sans fil de l'expéditeur (a), qui l'achemine ensuite à l'un des serveurs de relais globaux exploité par RIM (b). La station de relais RIM transmet

message via Internet on to the departmental BlackBerry Enterprise Server (BES) of the originating user (c), which decrypts it and forwards it to the departmental mail server (d) for delivery to the destination user (so that an e-mail from an enterprise BlackBerry device actually appears to have originated from inside the departmental network, e). If the destination user is not in the same department as the originating user, the e-mail will travel through the Internet to the destination user's network for delivery (f). Further, if the destination user is also a BlackBerry device user, the destination office will have its own BES which will forward an encrypted copy of the e-mail over the Internet (g) to the RIM relay for delivery to the destination user's BlackBerry device (h).

le message au serveur d'entreprise BlackBerry ministériel de l'expéditeur (c), qui le déchiffre et l'achemine par Internet vers le serveur de courriel ministériel (d) afin qu'il soit livré au destinataire (de sorte que le courriel d'un dispositif BlackBerry d'entreprise semble provenir de l'intérieur du réseau ministériel [e]). Si le destinataire n'est pas dans le même ministère que l'expéditeur, le courriel passera par Internet pour être livré au réseau du destinataire (f). Par ailleurs, si le destinataire est également un utilisateur de dispositif BlackBerry, le bureau du destinataire aura son propre BES qui transmettra par Internet (g) une copie chiffrée du courriel au relais RIM pour être livré au dispositif BlackBerry du destinataire (h).

BlackBerry PIN-to-PIN (sometimes referred to as Peer-to-Peer) messaging is similar to e-mail in that it allows BlackBerry device users to send messages to each other, but with important differences:

La messagerie BlackBerry NIP à NIP (parfois appelée « poste à poste ») est semblable au courriel en ce sens qu'elle permet également aux utilisateurs de dispositifs BlackBerry de s'envoyer des messages entre eux, mais elle comporte des différences importantes :

- Only possible between BlackBerry devices

- La messagerie NIP à NIP n'est possible qu'entre dispositifs BlackBerry.

- Addressed to a "PIN" instead of an e-mail address. A "PIN" is a hardware address, similar to a computer network adapter's MAC address, and is unique to every BlackBerry device. A "PIN" is **not** an authentication password **nor** is it a user identifier. It is the method by which the BlackBerry device is identified to the RIM relay for the purpose of finding the device within the global wireless service providers' networks.

- Le message doit être adressé à un NIP plutôt qu'à une adresse de courriel. Le NIP est une adresse matérielle, semblable à l'adresse MAC de la carte réseau d'un ordinateur, et elle est unique à chaque dispositif BlackBerry. Le NIP **n'**est **pas** un mot de passe d'authentification, **ni** l'identificateur d'un utilisateur. C'est la méthode par laquelle le relais RIM identifie le dispositif BlackBerry aux fins de localisation dans les réseaux globaux des fournisseurs de services sans fil.

If permitted by departmental policy, users who know the PINs of other users' BlackBerry device can use the PINs to directly exchange data messages with the other devices across the wireless network

Si la politique ministérielle l'autorise, les utilisateurs qui connaissent le NIP du dispositif BlackBerry d'autres utilisateurs peuvent l'utiliser pour échanger directement des messages de données avec ces dispositifs à l'intérieur du réseau sans fil (à

(outside the normal e-mail process), thus bypassing the internal departmental e-mail servers and security filters.

l'extérieur du processus de courriel régulier), contournant par le fait même les serveurs de courriel et les filtres de sécurité internes du ministère.

Figure 2 illustrates the process of sending or receiving PIN-to-PIN messages on a BlackBerry device.

La figure 2 illustre le processus d'envoi et de réception de messages NIP à NIP sur un dispositif BlackBerry.

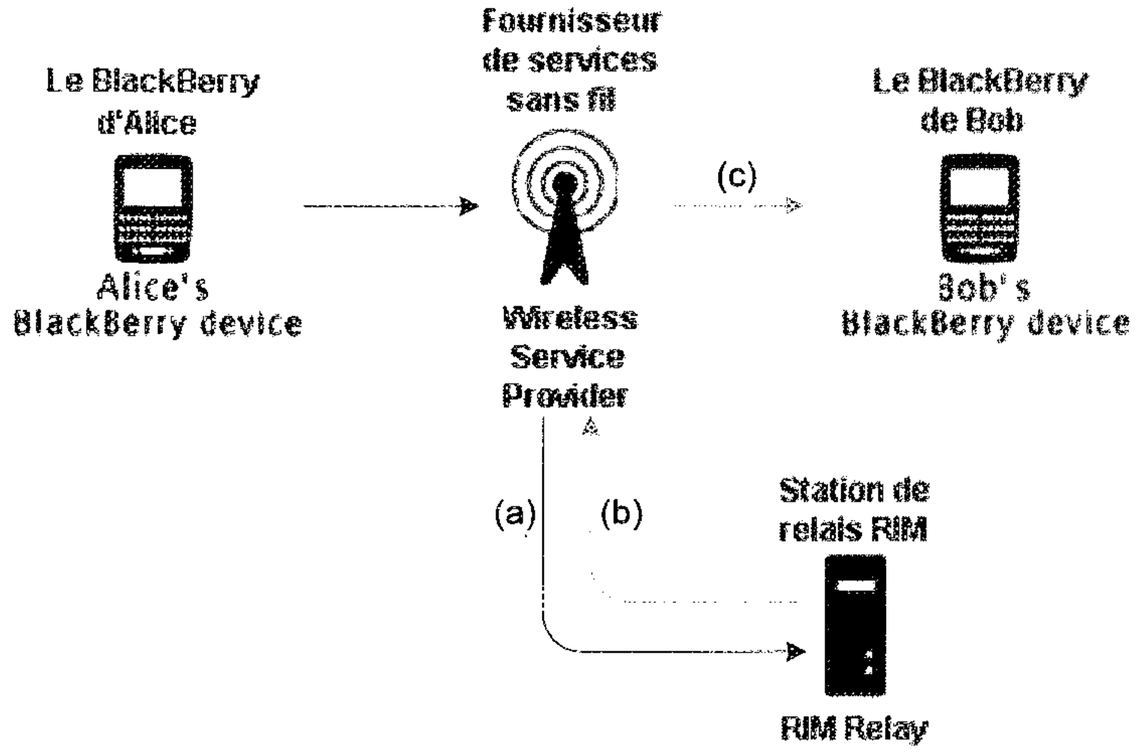


Figure 2- Sending/Receiving PIN-to-PIN Messages on a BlackBerry device
Envoi et réception de messages NIP à NIP sur un BlackBerry

In this case, a PIN-to-PIN message sent from a BlackBerry device is forwarded to the RIM relay (a) by the user's wireless service provider as in the case of e-mail. However, for a PIN-to-PIN message, instead of going back through departmental e-mail servers, the relay identifies the destination BlackBerry device by its PIN and forwards the message directly to the destination user's wireless service provider (which may or may not be the same provider as the originating user, b) for direct delivery to the destination device (c).

Dans ce cas-ci, un message NIP à NIP envoyé à partir d'un dispositif BlackBerry est acheminé au relais RIM (a) par le fournisseur de services sans fil de l'expéditeur comme dans le cas d'un courriel. Toutefois, au lieu de passer par les serveurs de courriel du ministère, le relais identifie le dispositif BlackBerry de destination par son NIP et achemine directement le message au fournisseur de services sans fil du destinataire (qui pourrait être différent de celui de l'expéditeur [b]) aux fins de livraison directe au dispositif de destination (c).

BES version 4.1 and later provides a solution whereby departments that permit the use of PIN-to-PIN messaging can configure the BES to force corporate BlackBerry devices to send copies of

Les versions 4.1 et ultérieures du BES offrent une solution permettant à un ministère qui autorise la messagerie NIP à NIP de configurer son BES de façon à forcer les dispositifs BlackBerry du ministère à

their PIN, SMS, or MMS transmissions to the BES. The departmental BES can then store those messages to help departments meet audit requirements.

PIN-to-PIN Security Issues

PIN-to-PIN messaging is typically faster than the normal e-mail process as the message passes through fewer servers and infrastructure components. For this reason, PIN-to-PIN messages are also useful for emergency communications in situations where the departmental e-mail servers are down, but the wireless service provider and RIM relay are still available. However, if the wireless carrier's cellular network (e.g., Rogers, Bell, etc.) is also down, then PIN-to-PIN messaging will also be unavailable. Unfortunately, PIN-to-PIN messaging suffers from several important security vulnerabilities that GC users should be aware of:

1. **PIN-to-PIN transmission security:** PIN-to-PIN is not suitable for exchanging sensitive messages. Although PIN-to-PIN messages are encrypted using Triple-DES, the key used is a global cryptographic "key" that is common to every BlackBerry device all over the world. This means **any** BlackBerry device can potentially decrypt **all** PIN-to-PIN messages sent by any other BlackBerry device, if the messages can be intercepted and the destination PIN spoofed. Further, unfriendly third parties who know the key could potentially use it to decrypt messages captured over the air. Note that the "BlackBerry Solution Security Technical Overview" [1] document published by RIM specifically advises users to "consider PIN messages as scrambled, **not** encrypted".

envoyer au BES une copie de leurs transmissions NIP, SMS ou MMS. Le BES ministériel peut ensuite stocker ces messages pour aider le ministère à satisfaire aux exigences en matière de vérification.

Problèmes liés à la sécurité de la messagerie NIP à NIP

La messagerie NIP à NIP est généralement plus rapide que le processus normal d'acheminement de courriels car elle fait appel à un plus petit nombre de serveurs et de composants d'infrastructure. Pour cette raison, les messages NIP à NIP sont également utiles pour les communications d'urgence dans des situations où les serveurs ministériels sont en panne, mais où le fournisseur de services sans fil et le relais RIM sont toujours disponibles. Toutefois, si le réseau cellulaire de l'entreprise sans fil (p. ex., Rogers, Bell, etc.) est également en panne, la messagerie NIP à NIP ne sera pas disponible non plus. Malheureusement, la messagerie NIP à NIP présente de nombreuses vulnérabilités importantes en matière de sécurité que les utilisateurs du GC devraient connaître :

1. **Sécurité de transmission NIP à NIP :** La messagerie NIP à NIP ne convient pas à l'échange de messages sensibles. Quoique les messages NIP à NIP soient chiffrés à l'aide de Triple-DES, la clé utilisée est une clé cryptographique générale commune à tous les dispositifs BlackBerry à travers le monde. En d'autres mots, **tout** dispositif BlackBerry est capable de déchiffrer **tous** les messages NIP à NIP envoyés par un autre dispositif BlackBerry, si ces messages peuvent être interceptés et le NIP de destination usurpé. Par ailleurs, des parties hostiles qui connaissent la clé pourraient s'en servir pour déchiffrer des messages captés en direct. À noter que le document *BlackBerry Solution Security Technical Overview* [1] publié par RIM conseille aux utilisateurs de considérer les messages NIP comme étant brouillés, **et non** chiffrés.

2. **PIN Address Vulnerability:** A BlackBerry device that has been used for PIN messaging should **not** be recycled for re-use. The reason is that the hard-coded PIN cannot be erased or modified, and therefore the PIN does **not** follow a user to a new device. Even after memory wiping and reloading, the BlackBerry device still has the same PIN identity and will continue to receive PIN messages addressed to that PIN. This can expose unsuspecting users of BlackBerry devices to potential information compromise in the following ways:

   - A new owner of the recycled BlackBerry device could view PIN messages sent from a colleague of the previous owner who is unaware that the message is now going to the wrong recipient (recall that the PIN is a device ID, and **not** a user ID).

   - A message sent by the BlackBerry device's new owner contains a known PIN credential which might be mistakenly accepted as being from the previous owner (impersonation).

3. **Bypass of Virus/Malware Scanning and Spam Filtering mechanisms:** As described previously, PIN-to-PIN messaging bypasses all corporate e-mail security filters, and thus users may become vulnerable to viruses and malware code as well as spam messages if their PIN becomes known to unauthorized third parties.

Recommendations

GC departments are advised to consider all the aforementioned security issues before allowing

2. **Vulnérabilité liée à l'adresse NIP :** Un dispositif BlackBerry qui a été utilisé pour la messagerie NIP **ne** devrait **pas** être recyclé aux fins de réutilisation. La raison est que le NIP fait partie intégrante du programme et qu'il ne peut donc être ni effacé ni modifié et, par conséquent, il **ne** peut être transféré dans un autre dispositif. Même après que sa mémoire a été effacée et rechargée, le dispositif BlackBerry conserve son NIP et continuera de recevoir des messages adressés à ce NIP. Cela pourrait avoir pour effet d'exposer les utilisateurs peu méfiants à la compromission possible de l'information comme suit :

   - Le nouveau propriétaire d'un dispositif BlackBerry recyclé pourrait visualiser les messages NIP envoyés par un collègue du propriétaire précédent, qui ne sait pas que ses messages sont maintenant envoyés au mauvais destinataire (rappel : le NIP est l'ID du dispositif et **non pas** celui de l'utilisateur).

   - Un message envoyé par le nouveau propriétaire du dispositif BlackBerry recyclé contient les justificatifs d'identité d'un NIP connu, lesquels pourraient être acceptés par mégarde comme étant ceux de l'ancien propriétaire (usurpation d'identité).

3. **Contournement des mécanismes de détection des virus/maliciels et de filtrage des pourriels :** Comme il a été décrit précédemment, la messagerie NIP à NIP contourne tous les filtres de sécurité de courriel internes et, par conséquent, expose les utilisateurs aux virus et aux programmes malveillants, ainsi qu'aux pourriels, si leur NIP est révélé à des tierces parties non autorisées.

Recommandations

On recommande aux ministères du GC de tenir compte de tous les problèmes de sécurité

PIN-to-PIN messaging. Departments can disable PIN-to-PIN messaging with the appropriate BES IT Policy settings. For departments with specific requirements for PIN-to-PIN messaging (e.g. emergency communications), it is recommended that a clear policy on the use of PIN-to-PIN messaging be put in place, and that the following supplementary measures be considered to protect the privacy and confidentiality of PIN-to-PIN Messages:

1. Using the S/MIME option which leverages GC PKI infrastructure and strong encryption to provide true end-to-end (user-to-user) encryption of messages (e-mail and PIN messages only). BlackBerry S/MIME encryption is approved by CSEC for the protection of up to Protected B information, and can mitigate some of the risk by ensuring that only authorized parties can read transmitted information. Note that using the BlackBerry S/MIME module requires that departments use the GC PKI infrastructure and train users in the use of digital PKI certificates.

2. Setting an organization-specific PIN-to-PIN encryption key in the BES. This overrides the default global encryption key and limits the ability to decrypt PIN-to-PIN messages to departmental BlackBerry devices which are connected to the BES. However, this also prevents PIN-to-PIN communication with BlackBerry devices outside of the department, and may prevent emergency communications with outside organizations (e.g. first-responders) as the same global key is no longer shared. Consequently, use of this feature should be carefully considered.

susmentionnés avant d'autoriser la messagerie NIP à NIP. Les ministères peuvent désactiver la messagerie NIP à NIP à l'aide des paramètres appropriés de la politique TI du BES. Pour les ministères qui ont un besoin précis d'utiliser la messagerie NIP à NIP (p. ex., pour les communications d'urgence), il est recommandé de mettre en place une politique claire sur l'utilisation de la messagerie NIP à NIP et de tenir compte des mesures supplémentaires suivantes pour protéger les renseignements personnels et la confidentialité des messages NIP à NIP:

1. Utilisation de l'option S/MIME qui tire profit de l'infrastructure à clé publique (ICP) du GC et d'un chiffrement robuste afin de fournir un chiffrement réel de bout en bout (utilisateur à utilisateur) des messages (courriels et messages NIP seulement). Le chiffrement BlackBerry S/MIME est approuvé par le CSTC pour la protection de l'information allant jusqu'au niveau PROTÉGÉ B inclusivement et peut atténuer certains des risques en faisant en sorte que seules les parties autorisées puissent lire l'information transmise. À noter que l'utilisation du module BlackBerry S/MIME nécessite que les ministères utilisent l'ICP du GC et forment les utilisateurs sur l'utilisation de certificats ICP numériques.

2. Établissement d'une clé de chiffrement NIP à NIP propre à l'organisation dans le BES. Cela a pour effet de remplacer la clé de chiffrement générale par défaut et limite la capacité de déchiffrer des messages NIP à NIP aux dispositifs BlackBerry du ministère qui sont connectés au BES. Toutefois, cela contribue également à empêcher les communications NIP à NIP avec les dispositifs BlackBerry se trouvant à l'extérieur du ministère, et pourrait empêcher les communications d'urgence avec les organisations externes (c.-à-d. les premiers intervenants) étant donné que la clé générale n'est plus partagée. L'utilisation de cette fonction devrait donc être soigneusement pensée.

Note that in both cases above, although the body of the message may be secure, the PIN itself is still transmitted in the clear (as it is used as an address and is needed to identify the originator and recipient of the message), and if the identity of an individual and assigned PIN are known, an adversary may be able to use this information for targeting purposes.

PIN number lists should be kept separate from phone/e-mail lists and never be disclosed or released to unauthorized individuals.

Because PINs are associated with the physical device and not a specific user, BlackBerry devices which have been used for PIN messaging, particularly those which have been used by senior GC personnel, should **not** be recycled, but destroyed instead.

The minimum destruction standard for BlackBerry devices must ensure that the printed circuit board inside the device has been broken into at least two parts. Note that only breaking the screen, keyboard and / or plastic housing is **not** sufficient to ensure that the BlackBerry devices cannot be recycled, as these components can be replaced.

References

[1] *BlackBerry Enterprise Solution: Security Technical Overview, for BlackBerry Enterprise Server Version 4.1 Service Pack 5 and BlackBerry Device Software Version 4.5*, Document Part #17930884 Version 2, Research-In-Motion, 2008.

À noter que, dans les deux cas mentionnés plus haut, le corps du message est sécurisé mais que le NIP lui-même est toujours transmis en clair (puisqu'il sert d'adresse et qu'il est nécessaire pour identifier l'expéditeur et le destinataire du message). À noter également que si l'identité d'une personne et le NIP qui lui est associé sont connus, un adversaire est en mesure d'utiliser cette information à des fins de ciblage.

Les NIP sont considérés comme des renseignements personnels et devraient être conservés séparément des listes de numéros de téléphone et d'adresses de courriel. Par ailleurs, ils ne devraient jamais être divulgués ou révélés à des personnes non autorisées.

Parce que les NIP sont associés à un dispositif physique et non à un utilisateur particulier, les dispositifs BlackBerry qui ont été utilisés pour la messagerie NIP à NIP, et plus particulièrement ceux qui ont été utilisés par des cadres supérieurs du GC, **ne** devraient **pas** être recyclés, mais devraient plutôt être détruits.

La norme de destruction standard minimale des dispositifs BlackBerry doit être telle que la carte de circuits imprimés du dispositif est brisée en au moins deux parties. Briser l'écran, le clavier ou le boîtier du dispositif **ne** suffit **pas** pour assurer qu'il ne peut pas être recyclé, étant donné que ces éléments peuvent être remplacés.

Références

[1] *BlackBerry Enterprise Solution: Security Technical Overview, for BlackBerry Enterprise Server Version 4.1 Service Pack 5 and BlackBerry Device Software Version 4.5*, Document n° 17930884, version 2, Research-In-Motion, 2008.

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

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

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

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

IT Security Bulletin
Bulletin de sécurité TI

July 2011 ITSB-79 Juillet 2011

Guidance for the Communications Security of SECRET Information

Purpose

The purpose of this bulletin is to inform the Government of Canada (GC) of the Communications Security Establishment Canada's (CSEC) guidance regarding the use of commercial technologies to safeguard the communications of classified information at the level of SECRET within a departmental local enclave.

CSEC has determined that specific Commercial-Off-The-Self (COTS) Virtual Private Network (VPN) devices can provide adequate protection for the communications security of SECRET information being transmitted within the confines of a departmental local enclave.

This technical safeguard should facilitate the implementation of a departmental SECRET network that is based on users operating a thin-client desktop configuration within a departmental unclassified operations zone and connecting to a back-end security zone where the processing and storing of the SECRET information occurs.

Lignes directrices pour la sécurité des communications liées à l'information SECRET

Objet

Le présent bulletin vise à informer les ministères du gouvernement du Canada (GC) sur les lignes directrices du Centre de la sécurité des télécommunications Canada (CSTC) concernant l'utilisation de technologies commerciales pour protéger la communication de l'information classifiée au niveau SECRET à l'intérieur d'une enclave locale ministérielle.

Le CSTC a déterminé que des dispositifs de réseau privé virtuel (RPV) commerciaux peuvent sécuriser adéquatement la communication de l'information SECRET dans les limites d'une enclave locale ministérielle.

Cette mesure de protection technique devrait faciliter la mise en œuvre d'un réseau ministériel SECRET où les utilisateurs se servent d'ordinateurs de bureau client léger dans une zone de travail non classifiée ministérielle et se connectent à une zone de sécurité dorsale pour le traitement et le stockage de l'information SECRET.

Background

CSEC, as the GC lead security agency for developing and promulgating COMSEC related policy for classified information, has recently concluded an analysis regarding the usage of commercial cryptosystems when safeguarding classified information at the SECRET level. Specifically, the use of COTS products were examined in regards to safeguarding the communication of SECRET information within a departmental local enclave.

A departmental local enclave is defined as a site with a single physical perimeter that maintains a common set of security policies (physical, personnel and Information Technology (IT)) under a single authority. External to the enclave represents where communications occur that extend past the perimeter, for example the Secure Channel Network (SC Net).

Secure Platform for Application Delivery

CSEC is partnering with Public Works and Government Services Canada (PWGSC) to deliver cost effective solutions for departmental SECRET networks. PWGSC offers a solution that can be tailored to departmental needs. This offering by PWGSC is titled Secure Platform for Application Delivery (SPAD).

Contexte

À titre de responsable de la sécurité du GC chargé d'élaborer et de promulguer des instruments de politique liés à la COMSEC à l'égard des renseignements classifiés, le CSTC a terminé récemment une analyse de l'utilisation de systèmes cryptographiques commerciaux pour protéger l'information classifiée au niveau SECRET. L'analyse portait plus particulièrement sur l'utilisation de produits commerciaux en ce qui a trait à la protection de la communication de renseignements SECRET à l'intérieur d'une enclave ministérielle locale.

Une enclave ministérielle locale est un site circonscrit par un périmètre physique unique et qui applique un ensemble commun de politiques de sécurité (matérielle, du personnel et des technologies de l'information [TI]) sous une seule et même autorité. L'extérieur de l'enclave représente l'endroit où sont établies les communications qui s'étendent au-delà du périmètre comme, par exemple, le Réseau de la Voie de communication protégée (VCP).

Livraison d'applications par plateforme protégée

Le CSTC travaille en partenariat avec Travaux publics et Services gouvernementaux Canada (TPSGC) pour fournir des solutions rentables pour les réseaux SECRET des ministères. TPSGC offre une solution qui peut être adaptée aux besoins d'un ministère, soit la Livraison d'applications par plateforme protégée (LAPP).

Recommendations

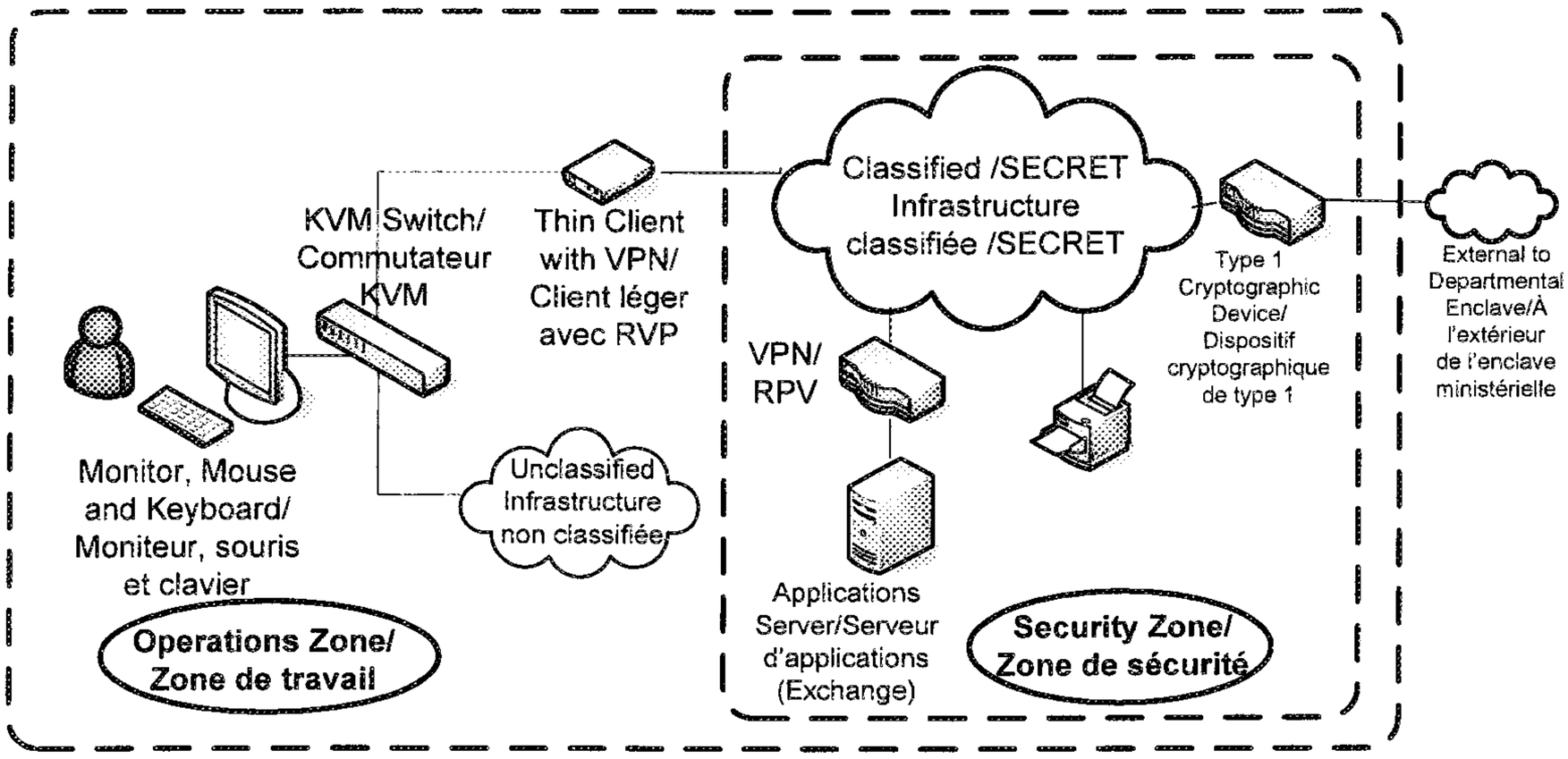
The analysis concluded:

- Communications security external to a local departmental enclave - that departments continue to use the current CSEC approved technical solution, which is a Type 1 cryptographic device.
- Communications security within a local departmental enclave – with the maturity and capability of available commercial technologies, specific commercially available VPN solutions can be used to adequately secure the communications of SECRET information.

Recommandations

Conclusions de l'analyse :

- Sécurité des communications à l'extérieur d'une enclave ministérielle locale – Les ministères continuent d'utiliser la solution technique approuvée par le CSTC à l'heure actuelle, soit un dispositif cryptographique de type 1.
- Sécurité des communications à l'intérieur d'une enclave ministérielle locale – Les technologies disponibles sur le marché ont atteint un niveau de maturité et de capacité tel, qu'il est possible d'utiliser certaines solutions RPV commerciales pour sécuriser adéquatement la communication de l'information SECRET.



Description of Alternative Technical Solution for Departmental Enclaves

Departments who plan to deploy a SECRET network are advised to begin their Threat and Risk Assessments (TRA) early in the

Description de solutions techniques de rechange pour les enclaves ministérielles

On recommande aux ministères qui prévoient déployer un réseau SECRET d'entreprendre leur évaluation des menaces et des risques (EMR) tôt au

Requirements stage. The appropriate steps to conduct for the TRA are described in the *Harmonized TRA Methodology*, available on the CSEC website. Subject to the findings of the TRA, CSEC specified COTS VPN devices may be used.

Departments are advised to use CSEC recommended COTS VPN solutions available from CSEC upon request. COTS VPN solutions are also available through PWGSC's SPAD offering for departmental Secret networks. Any COTS VPN solutions will need to be configured, operated, and maintained according to CSEC guidance.

moment de la définition des besoins. La marche à suivre appropriée est donnée dans la *Méthodologie harmonisée d'EMR* disponible sur le site du CSTC. Les résultats de l'EMR détermineront s'il est possible d'utiliser des dispositifs RPV commerciaux approuvés par le CSTC.

Il est conseillé aux ministères d'utiliser les solutions RPV commerciales qui sont recommandées par le CSTC. On peut se procurer une liste des produits disponibles auprès de celui-ci. Des solutions RPV commerciales sont également disponibles par l'intermédiaire du programme LAPP de TPSGC pour les réseaux SECRET ministériels. Il faudra configurer, exploiter et maintenir la solution RPV commerciale sélectionnée conformément aux lignes directrices du CSTC.

Contacts and Assistance

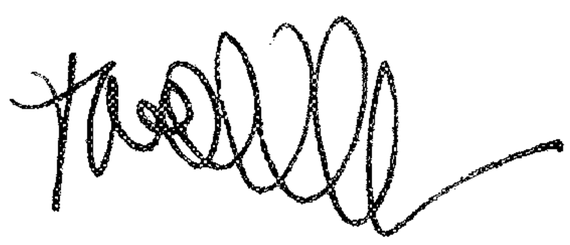
IT Security Client Services
Communications Security Establishment Canada

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

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

La chef adjointe de la Sécurité des TI,



Toni Moffa

Deputy Chief, IT Security

2011-07-07
Date

s.15(1)
s.16(2)(c)
s.21(1)(a)

==========
- Information Note 11-08-001
Date: 05 August 2011
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

Title
=====
McAfee Report references Government of Canada victims

Details
=======
McAfee (www.mcafee.com), a commercial internet security entity, recently released a Whitepaper report detailing a multi-year hacking campaign titled "Operation Shady RAT".
Within the report, McAfee cites that two Canadian Government Agencies were found to be victims of the hacking campaign. The report does not name the impacted agencies.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

s.15(1)
s.16(2)(c)

Note to readers

==========

The
provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact
at @cse-cst.gc.ca

==========
- GC Cyber Flash GCCF11-001
Date: 12 August 2011
==========
AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within the federal government.
Title
=====
Malicious activity observed
Details
=======
has received several reports of recently identified malicious activity The reported activities include but are not limited to
etc.

Mitigation
==========

Page 23

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

Critical Note:

Reporting
=========
Any government department suspecting they have incidents related to this activity are requested to provide a written report to http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which cannot verify the accuracy and integrity. does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to readers
===============
The
provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. helps ensure that critical GC

infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

s.15(1)
s.16(2)(c)

To report incidents affecting GC infrastructures, please contact
at @cse-cst.gc.ca

s.15(1)
s.16(2)(c)

==========
- Information Note 11-002
Date: 26 August 2011
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

Title
=====
Leveraging secure communications for timely cyber threat information

Details
=======
Maintaining IT services and protecting departmental IT assets are central to supporting your departmental operations. Receiving timely cyber threat information is key.

Given the persistent nature of cyber threats, it is key to provide timely and relevant information to GC departments. Many departments within the Government of Canada have access to secure communications technologies, for example, secure phones (STEs) and secure fax machines.

When threat information is classified in nature, appropriate dissemination methods must be used to deliver information to Government of Canada departments. With this in mind, we encourage you to proactively engage your Security Department to inquire about your secure communications options and to take time to familiarize yourself with the usage of the technology.

The following departmental representatives will be able to provide you with more information and guidance:

- COMSEC Custodian
- Departmental COMSEC authority (DCA)
- IT Security Coordinator (ITSC)
- Departmental Security Officer (DSO)

Below are questions to address in your conversation:

- What are my options for secure communications with CSEC?
    - Classified information (i.e. SECRET): secure phone, secure fax?
    - Protected information: PKI encrypted email

- Where is the equipment located?
- What are the step-by-step instructions for using the equipment?

Leveraging secure communication technologies will result in your department receiving threat information more quickly and more efficiently.

@cse-cst.gc.ca

Note to readers
==========
The
provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact
at @cse-cst.gc.ca

==========

- Note d'information n° 11-002

Date : 26 août 2011

==========

s.15(1)

s.16(2)(c)

PUBLIC

========

Cette note d'information est destinée aux professionnels des TI et aux gestionnaires au sein du gouvernement fédéral.

Titre

=====

Miser sur les communications sécurisées pour une information opportune sur les cybermenaces

Détails

=======

Le maintien des services de TI et la protection des biens de TI sont au coeur même du soutien des opérations de votre ministère. Or, il est essentiel que l'information sur les cybermenaces soit fournie en temps opportun.

Compte tenu de la nature persistante des cybermenaces, il est essentiel de pouvoir fournir aux ministères du GC l'information pertinente en temps opportun. Or, de nombreux ministères fédéraux ont accès à des technologies de communications sécurisées, tels les postes cryptophoniques (STE) et les télécopieurs sécurisés.

Lorsque l'information sur les menaces est classifiée, les méthodes appropriées de diffusion doivent être utilisées pour la transmettre aux ministères du GC. Dans cette optique, nous vous encourageons à vous renseigner auprès de votre service de sécurité sur les options qui s'offrent à vous en ce qui a trait aux communications sécurisées et à prendre le temps de mieux les connaître.

Les représentants ministériels suivants seront en mesure de vous renseigner et de vous conseiller davantage :

- le gardien COMSEC
- l'autorité COMSEC du ministère (ACM)
- le coordonnateur de la sécurité des TI (CSTI)
- l'agent de sécurité du ministère (ASM)

Voici quelques-unes des questions que vous pourriez leur poser :

- Quelles sont mes options pour établir des communications sécurisées avec le CSTC?

- information classifiée (c.-à-d. SECRET) : poste cryptophonique, télécopieur sécurisé?
- information Protégé : courriels chiffrés au moyen de l'ICP?

s.15(1)

- Où se trouve l'équipement?
- Quelle est la marche à suivre pour l'utiliser?

s.16(2)(c)

En misant sur les technologies de communications sécurisées, votre ministère sera en mesure de recevoir l'information sur les cybermenaces plus rapidement et plus efficacement.

cse-cst.gc.ca

Note aux lecteurs
==========
Le est le centre de coordination des alertes liées aux cybervulnérabilités et aux cybermenaces, des analyses et des interventions. Le aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale face aux incidents de cybersécurité d'intérêt national. L'équipe du qui évolue au sein du Centre de la sécurité des télécommunications Canada, cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la

situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

s.15(1)
s.16(2)(c)

Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le à l'adresse suivante : @cse-cst.gc.ca

==========
- Information Note IN11-003
Date: 2 September 2011
==========

==========
Emergency Management Notification Systems - Security Best Practices
==========

AUDIENCE
========
This Information Note is intended for IT professionals and managers within the federal government.

ASSESSMENT
==========
EMN systems are used by both government and critical infrastructure organizations to ensure critical emergency management information is correlated and disseminated rapidly to personnel involved in emergency management operations.

s.15(1)
s.16(2)(c)
s.21(1)(a)

SUGGESTED ACTION
==========

strongly recommends that EMN system clients, owners and operators implement security best practices such as those mentioned above to ensure the security and integrity of EMN systems and information.

==========

is not responsible for the information found through these links, nor does it endorse the sites and their content.

s.15(1)
s.16(2)(c)
s.21(1)(a)

Note to readers
==========
The
provides a focal point for the GC's cyber threat and vulnerability warning, analysis and response. helps ensure that critical GC infrastructures are secure through: monitoring threats; providing leading-edge guidance and strategic advice; and coordinating a federal response to cyber security incidents of national interest. The team, within the Communications Security Establishment Canada (CSEC), aims to strengthen the security of federal information and information systems.

We would like to take this opportunity to remind IT Stakeholders of the importance of GC IT IMP reporting from a situational awareness perspective and we encourage departments to contact us regarding IT Security concerns.

To report incidents affecting GC infrastructures, please contact
at @cse-cst.gc.ca

==========
- Note d'information n° 11-003
Date : 2 Septembre 2011
==========

==========

Systèmes de notification de gestion des urgences - Pratiques exemplaires en matière de sécurité

==========

PUBLIC
========
Cette note d'information est destinée aux professionnels des TI et aux gestionnaires au sein du gouvernement fédéral.

ÉVALUATION

==========

Le gouvernement et les organismes responsables des infrastructures essentielles se servent des systèmes de notification de gestion des urgences pour veiller à ce que l'information critique sur la gestion des urgences soit mise en corrélation et divulguée rapidement au personnel qui participe aux activités de gestion des urgences.

Page 34

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

s.15(1)

s.15(1)
s.16(2)(c)
s.21(1)(a)

MESURE RECOMMANDÉE

==========

Le recommande fortement que les propriétaires et les opérateurs de systèmes de notification de gestion des urgences appliquent les pratiques exemplaires en matière de sécurité énoncées ci-haut afin de veiller à la sécurité et à l'intégrité des systèmes de notification de gestion des urgences et de l'information.

Les liens vers les sites Web sur lesquels le gouvernement du Canada (GC) n'exerce aucun contrôle sont fournis aux utilisateurs seulement pour des raisons de commodité. Le GC n'est pas responsable de l'exactitude, de l'actualité ni de la fiabilité du contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites ou leur contenu.

s.15(1)

s.16(2)(c)

Note aux lecteurs
==========
Le
est le centre de coordination des alertes liées aux cybervulnérabilités et aux cybermenaces, des analyses et des interventions. Le aide à assurer la sécurité des infrastructures essentielles du GC en surveillant les menaces, en fournissant une orientation d'avant-garde et des conseils stratégiques, et en coordonnant l'intervention fédérale face aux incidents de cybersécurité d'intérêt national. L'équipe du qui évolue au sein du Centre de la sécurité des télécommunications Canada, cherche à renforcer la sécurité de l'information et des systèmes d'information du gouvernement fédéral.

Nous aimerions profiter de l'occasion pour rappeler aux intervenants en TI qu'il est important, du point de vue de la connaissance de la situation, de déclarer les incidents en vertu du PGI TI GC, et nous encourageons les ministères à nous faire part de leurs préoccupations en matière de sécurité des TI.

Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le à l'adresse suivante : @cse-cst.gc.ca