



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;

- **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.
- **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.

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

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.

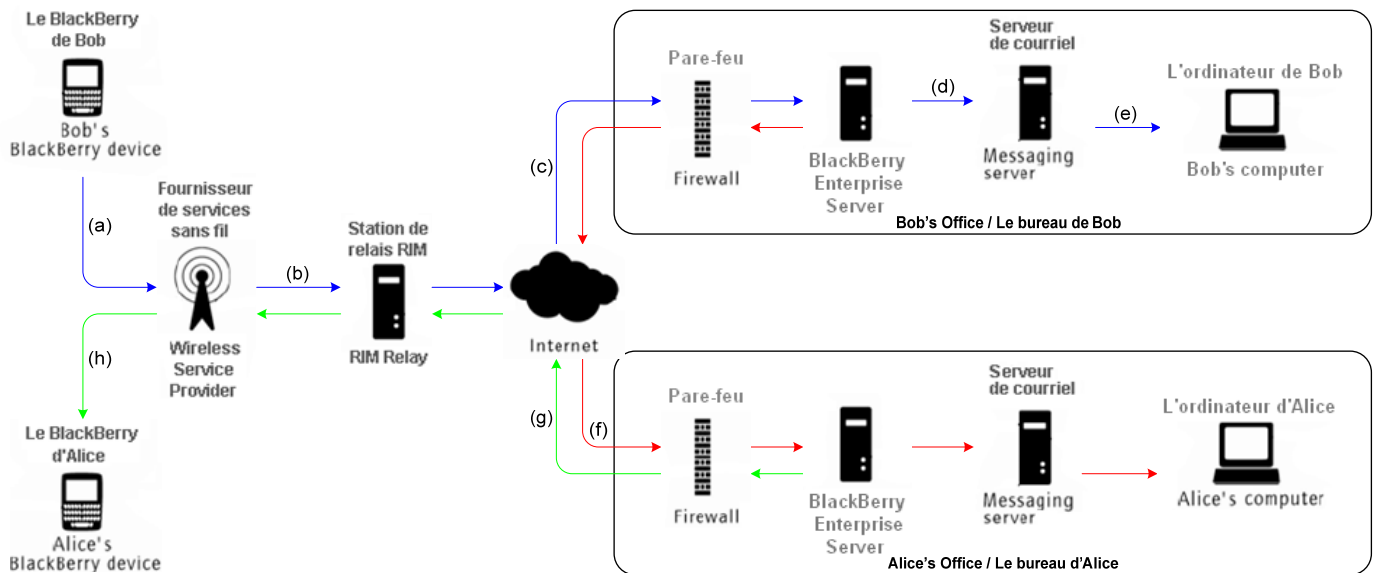


Figure 1 - Sending/Receiving E-mail on a BlackBerry device using a BES
Envoi et réception des courriels sur un dispositif BlackBerry en utilisant un BES

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

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.

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).

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:

- Only possible between BlackBerry devices
- 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.

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

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).

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 :

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

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.

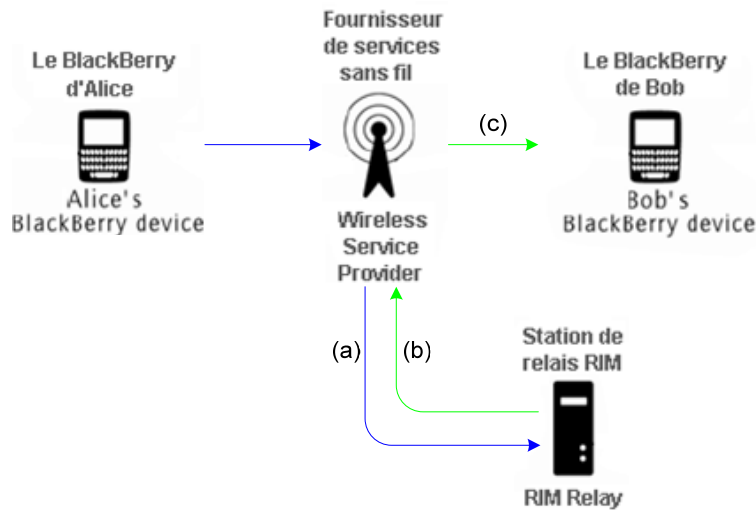


Figure 2- Sending/Receiving PIN-to-PIN Messages on a BlackBerry device
Envoi et réception de messages NIP à NIP sur un BlackBerry

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.
- 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.

Recommendations

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

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 (puisque'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.

March 2011

ITSB-57B

Mars 2011

Contacts and Assistance

IT Security Client Services
Communications Security Establishment Canada
PO Box 9703, Terminal
Ottawa, ON K1G 3Z4

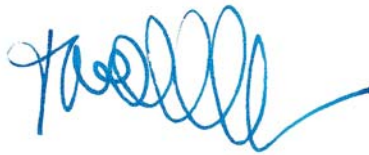
By email: itsclientservices@cse-cst.gc.ca
Telephone: 613-991-7654

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