

Rapport sur les produits et systèmes de sécurité TI

Évaluation de vulnérabilité des assistants numériques personnels (PDA)

Octobre 2002

ITSPSR-18



Page laissée intentionnellement en blanc.

Avant-propos

Le présent document, *Évaluation de vulnérabilité des assistants numériques personnels (PDA)* (ITSPSR-18), est non classifié et est publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).

Cet examen de produit a été préparé par le CST à l'intention du gouvernement fédéral. Il incorpore toute l'information connexe sur le PDA, tirée des Lignes directrices générales relatives à l'utilisation de dispositifs sans fil au sein du gouvernement fédéral. Ce document est officieux et sa portée est limitée. Il ne doit pas être considéré comme une étude, ni comme une évaluation, et ne constitue nullement une homologation du produit par le CST. Il vise à communiquer l'avis du CST à la lumière de l'information disponible au moment de sa préparation. Toute tierce partie qui choisit d'utiliser le présent document de quelque façon que ce soit, de s'y fier ou de prendre une décision en se basant sur son contenu, engage l'entière responsabilité de son choix. Le CST décline toute responsabilité en cas de dommage subi par une tierce partie et causé par toute décision ou toute utilisation ayant une quelconque relation avec ce rapport.

Les demandes de copies additionnelles, de modification de la distribution et de toute autre information doivent être transmises aux Services à la clientèle du CST, au 613-991-7600 ou à l'adresse client.svcs@cse-cst.gc.ca.

© 2002 Gouvernement du Canada, Centre de la sécurité des télécommunications (CST)

B.P. 9703, Terminus, Ottawa (Ontario) Canada, K1G 3Z4

Il est possible de reproduire cette publication textuellement et dans sa totalité sans avoir à acquitter de droit de reproduction mais seulement dans un but éducatif ou en vue d'une utilisation personnelle. L'utilisation de ce document sous forme révisée ou fragmentaire dans un quelconque but commercial nécessite cependant l'autorisation écrite du CST.

Page laissée intentionnellement en blanc.

Résumé

Le nombre de PDA utilisés à divers niveaux au sein du gouvernement du Canada (GC) est en hausse. La technologie des PDA a récemment connu un bond important en termes de puissance de traitement et de capacité de télécommunications. Sa capacité sans cesse croissante de traitement et de stockage, ses fonctionnalités conviviales de télécommunications sans fil et sa petite taille font du PDA un dispositif très attrayant pour les employés du gouvernement fédéral. Les PDA sont maintenant en mesure de gérer les fichiers et les applications que l'on trouve normalement sur les ordinateurs personnels (les PC) et les portatifs. On peut aisément transférer de l'information et des données du réseau de l'organisation aux PDA, grâce à divers supports : berceaux, liaison infrarouge, modem, émissions de radiofréquence par les réseaux locaux sans fil, Bluetooth, communications cellulaires.

Comme avec toute nouvelle technologie, les PDA présentent un certain nombre de vulnérabilités. Celles-ci sont très similaires à celles que l'on retrouve sur les portatifs. Avec le grand nombre de PDA qui, selon les prévisions, seront en utilisation au gouvernement fédéral, les occasions de compromission de l'information sensible seront encore plus grandes. La mise en œuvre des procédures et pratiques standard de sécurité des TI et l'utilisation d'un système cryptographique approuvé pour le stockage et la transmission de l'information permettront de contrer la majorité des menaces qui pèsent sur les PDA.

Le CST a effectué une analyse de vulnérabilité du système BlackBerry™, et considère que la fonction de chiffrement offerte par l'édition Enterprise est adéquate pour protéger l'information de niveau Protégé B et inférieur. Bien que le système BlackBerry™ complet ne réponde pas à toutes les exigences cryptographiques du GC, il offre néanmoins un certain niveau de protection contre la divulgation accidentelle ou l'écoute clandestine par un adversaire peu sophistiqué.

Le CST poursuit ses activités visant à évaluer la technologie des PDA et collabore avec les développeurs de l'industrie des PDA afin de renforcer les mécanismes de sécurité de leurs produits.

Page laissée intentionnellement en blanc.

Table des matières

| | |
|---|-----------|
| Avant-propos..... | i |
| Résumé..... | iii |
| Table des matières..... | v |
| Liste des figures..... | vii |
| Abréviations et sigles | ix |
| 1 Introduction | 1 |
| 1.1 Contexte..... | 1 |
| 1.2 Objet et portée | 1 |
| 1.3 Structure du document | 1 |
| 2 Lignes directrices générales sur les PDA..... | 3 |
| 2.1 Aperçu des PDA..... | 3 |
| 2.2 Sécurité matérielle et sécurité du stockage de l'information..... | 3 |
| 2.3 Sécurité des ordinateurs personnels et des serveurs | 4 |
| 2.4 Sécurité des logiciels | 4 |
| 2.5 Sécurité des communications | 4 |
| 2.5.1 Interfaces de communication | 4 |
| 2.5.2 Communications RF | 5 |
| 2.5.3 Communications dans l'infrarouge | 5 |
| 2.5.4 Interface Bluetooth..... | 6 |
| 2.5.5 Réseaux locaux sans fil (WLAN)..... | 6 |
| 2.5.6 Réseaux de téléphonie cellulaire..... | 6 |
| 2.5.7 Réseaux téléphoniques terrestres | 6 |
| 2.6 Sécurité acoustique | 6 |
| 2.7 Sécurité des émanations radioélectriques | 7 |
| 2.8 Sécurité cryptographique | 7 |
| 2.9 Sécurité des réseaux classifiés..... | 7 |
| 3 Système BlackBerry™..... | 9 |
| 3.1 Aperçu du système BlackBerry™ | 9 |
| 3.2 Relais BlackBerry™ | 9 |
| 3.3 Fonctionnalité cryptographique du système BlackBerry™ | 10 |
| 3.4 BlackBerry™ édition Internet..... | 11 |
| 3.5 BlackBerry™ à BlackBerry™ | 12 |
| 3.6 BlackBerry™ Redirector..... | 12 |
| 3.7 BlackBerry Enterprise Server™ (BES)..... | 14 |
| 3.7.1 Généralités | 14 |
| 3.7.2 Courrier électronique intraministériel à l'aide des BlackBerry™ | 16 |
| 3.7.3 Courrier électronique interministériel à l'aide des BlackBerry™ | 16 |
| 3.7.4 Port 3101 du protocole de contrôle de transmission (TCP) | 17 |
| 3.7.5 Résumé..... | 17 |
| 4 Solutions proposées pour sécuriser le système BlackBerry™ | 19 |
| 4.1 Généralités | 19 |
| 4.2 RVP entre ministères | 19 |
| 4.3 Solution BlackBerry™ avec protocole S/MIME | 21 |

| | | |
|----------|--|-----------|
| 4.4 | Version commerciale de l'agenda électronique BlackBerry™ avec protocole S/MIME | 21 |
| 5 | Conclusions..... | 23 |
| 5.1 | Résumé des pratiques recommandées | 23 |
| 5.1.1 | Pratiques recommandées générales pour l'utilisation des PDA..... | 23 |
| 5.1.2 | Pratiques recommandées pour l'utilisation du système BlackBerry™ | 23 |
| 5.2 | Recommandation | 24 |
| 5.3 | Conclusion..... | 24 |
| 6 | Bibliographie | 25 |

Liste des figures

| | |
|---|----|
| Figure 1 – Relais BlackBerry™ | 10 |
| Figure 2 – BlackBerry™ édition Internet | 11 |
| Figure 3 – Fonctionnement de l'option BlackBerry™ à BlackBerry™ | 12 |
| Figure 4 – Application BlackBerry™ Redirector | 13 |
| Figure 5 – BlackBerry Enterprise Server™ | 15 |
| Figure 6 – BlackBerry Enterprise Server™ avec des RPV déployés | 20 |

Page laissée intentionnellement en blanc.

Abréviations et sigles

| | |
|--------|--|
| ASM | Agent de sécurité du ministère |
| BES | BlackBerry Enterprise Server™ |
| CST | Centre de la sécurité des télécommunications |
| DES | Norme de chiffrement de données (<i>Data Encryption Standard</i>) |
| EMR | Évaluation des menaces et des risques |
| GC | Gouvernement du Canada |
| GPRS | Service général de radiocommunication en mode paquet (<i>General Packet Radio Service</i>) |
| ICP GC | Infrastructure à clé publique du gouvernement du Canada |
| LAN | Réseau local |
| MS | Microsoft |
| NIP | Numéro d'identification personnel |
| PC | Ordinateur personnel |
| PCMCIA | Personal Computer Memory Card International Association |
| PDA | Assistant numérique personnel |
| RF | Radiofréquence |
| RIM® | Research In Motion (Limited) |
| RPV | Réseau privé virtuel |
| SCP | Système de communications personnelles |
| S/MIME | Secure Multi-purpose Internet Mail Extensions |
| TCP | Protocole de contrôle de transmission |

Page laissée intentionnellement en blanc.

1 Introduction

1.1 Contexte

En juin 2000, le CST a entrepris d'étudier la technologie des PDA et plus spécifiquement le système BlackBerry™, en raison de son utilisation croissante au gouvernement fédéral. Plusieurs activités de recherche sur les PDA ont eu lieu depuis, notamment l'analyse du système BlackBerry™.

1.2 Objet et portée

L'objet de ce rapport est de synthétiser l'information obtenue au cours des dernières activités de recherche et de présenter des recommandations afin de sécuriser davantage l'utilisation des PDA en général, et plus spécifiquement pour le système BlackBerry™. Ce rapport porte donc initialement sur le système BlackBerry™, et les autres produits seront inclus quand les recherches effectuées sur ceux-ci seront terminées.

Ce rapport ne présente pas d'analyse détaillée, ni les vulnérabilités des protocoles de communication. Toutefois, nous faisons référence aux publications pertinentes du CST, et nous présentons un aperçu de haut niveau.

1.3 Structure du document

Le présent document est structuré comme suit :

Section 1 – Introduction : décrit le contexte et définit la portée et le but de ce rapport.

Section 2 – Lignes directrices générales pour les PDA : décrit les vulnérabilités associées à l'utilisation des PDA en général. Cette section présente également des mesures qui permettraient de contrer ces menaces.

Section 3 – Système BlackBerry™ : décrit le fonctionnement de diverses composantes du système BlackBerry™, ses différents modes de fonctionnement et les vulnérabilités associées à chaque mode.

Section 4 – Solution proposée pour sécuriser le système BlackBerry™ décrit les solutions possibles proposées par le CST pour sécuriser les communications entre l'expéditeur et le destinataire.

Section 5 – Conclusions : présente un résumé des mesures d'atténuation des menaces recommandées par le CST et l'énoncé d'approbation quant à l'utilisation restreinte du système BlackBerry™ pour la transmission d'information Protégé B.

Annexe A – Système BlackBerry™ : contient de l'information classifiée au sujet du système BlackBerry™. La diffusion de cette annexe est contrôlée. Les ministères du GC qui désirent en recevoir une copie doivent communiquer avec l'équipe des Services à la clientèle du CST, au (613) 991-7600 ou par courriel à l'adresse client.svcs@cse-cst.gc.ca.

Page laissée intentionnellement en blanc.

2 Lignes directrices générales sur les PDA

2.1 Aperçu des PDA

Les assistants numériques personnels (PDA) sont comparables aux portatifs de bas de gamme pour ce qui est de l'entrée, du traitement, du stockage, de la transmission et de la réception des données. Ils ont une capacité de traitement limitée et sont normalement utilisés conjointement avec un poste de travail ou un serveur plus puissant. Leurs capacités de traitement et de stockage continuent néanmoins de croître, pendant que leur taille et leur poids diminuent, et que la gamme des dispositifs et des applications connexes augmente. Cette plus grande commodité d'utilisation accélérera grandement la propension des utilisateurs à dépendre de ces assistants.

Les PDA, tout comme les portatifs, sont des dispositifs mobiles qui doivent faire l'objet d'une protection matérielle additionnelle, en plus des contrôles d'accès physique habituellement associés aux serveurs et aux ordinateurs personnels. Mais à la différence des ordinateurs portables, les PDA sont plus faciles à transporter et seront utilisés par un plus grand nombre d'employés du gouvernement fédéral. Le nombre accru de PDA en usage par les employés du gouvernement fédéral se traduit donc par un nombre plus grand de cibles pour des adversaires potentiels.

2.2 Sécurité matérielle et sécurité du stockage de l'information

L'accès à l'information enregistrée dans un PDA est contrôlé par les fonctionnalités de contrôle d'accès normalement intégrées dans le PDA, ou l'est par le système d'exploitation. Si la fonction de contrôle d'accès est activée sur le PDA, l'utilisateur doit entrer un mot de passe valide ou un numéro d'identification personnel (NIP) pour accéder aux applications installées et à l'information enregistrée. Les mécanismes de contrôle d'accès devraient pouvoir prendre en charge l'ensemble complet des caractères alphanumériques, afin de réduire la possibilité qu'une personne malveillante ne devine le mot de passe de l'utilisateur. Enfin, les mots de passe et les NIP devraient être choisis de manière aléatoire et modifiés régulièrement. L'agent de sécurité du ministère (ASM) peut offrir des conseils à cet égard.

On doit s'assurer d'avoir un contrôle positif d'un PDA, car c'est un facteur important pour réduire le risque que les mots de passe ne soient percés et pour contrer les attaques visant à altérer le contenu du dispositif de poche. Même un accès de courte durée à un dispositif permettrait de contourner le mécanisme de contrôle d'accès, et d'extraire de l'information sensible ou encore d'implanter une application indésirable.

La sécurité de l'information contenue dans un PDA ne devrait pas être basée uniquement sur les fonctions de contrôle d'accès du produit, mais plutôt faire appel au chiffrement. Le chiffrement de l'information, à l'aide de mécanismes qui répondent aux exigences cryptographiques du GC, devrait la protéger adéquatement, même si quelqu'un tente d'altérer ou de trafiquer le PDA. Il existe actuellement plusieurs produits commerciaux validés selon les normes FIPS 140-1 et FIPS 140-2. Un dispositif de poche dont le contenu n'est pas chiffré à l'aide de systèmes cryptographiques approuvés par le GC (c'est le cas de l'agenda électronique BlackBerry™) devrait être présumé compromis si on le perd ou s'il est volé. Le CST travaille avec l'industrie

afin d'encourager le développement de produits qui répondent aux exigences cryptographiques du GC.

2.3 Sécurité des ordinateurs personnels et des serveurs

La plupart des PDA sont utilisés conjointement avec un ordinateur personnel ou un serveur, afin de partager l'information comme les listes de personnes-ressources, les entrées dans les agendas, les courriels, les fichiers. L'ordinateur personnel ou le serveur fait fonctionner une application de communication qui permet la synchronisation automatique ou semi-automatique avec le dispositif de poche, par l'intermédiaire d'une liaison de données (p. ex., câble, modem, infrarouge, sans fil). Dans un scénario type, la liaison ordinateur personnel-dispositif de poche vise à synchroniser l'information et à sauvegarder le contenu de la mémoire du dispositif de poche dans l'ordinateur personnel. Il y a un risque potentiel que l'information puisse être téléchargée sur un dispositif de poche sans que l'utilisateur ne le sache. On doit faire preuve de prudence quand on configure le logiciel de synchronisation, afin de réduire ce risque. Ainsi, il est préférable de ne pas utiliser les dispositifs de poche avec des ordinateurs de bureau ou des serveurs qui traitent de l'information sensible.

Certains types de PDA exigent que le poste de travail de l'utilisateur demeure ouvert et connecté au réseau, tandis que d'autres interagissent directement avec les serveurs du réseau. Tout dépendant de l'environnement du poste de travail de l'utilisateur, un adversaire pourrait implanter un programme malveillant dans le poste de travail, qui serait téléchargé pendant la synchronisation avec le PDA. Par conséquent, les mesures de sécurité visant à protéger les ordinateurs de bureau ou les serveurs sans surveillance devraient être en rapport avec le niveau de sécurité de l'information traitée par le réseau.

2.4 Sécurité des logiciels

Les PDA sont capables de charger et d'exécuter des logiciels, ce qui ouvre la possibilité d'introduire du code malveillant dans ces dispositifs, les postes de travail et les réseaux avec lesquels ils se connectent. Bien que les occurrences de code malveillant dans les PDA aient été relativement rares jusqu'à présent, on prévoit que le nombre d'incidents augmentera à mesure que les PDA gagneront en popularité et que le nombre de gratuits et de partagiciels offerts pour les PDA augmentera. Une mesure raisonnable de précaution consisterait donc à utiliser et mettre à jour régulièrement les détecteurs de virus, comme ceux qui sont offerts par les sociétés Symantec, Computer Associates, Trend Micro et McAfee. À l'heure actuelle, les virus que l'on trouve dans les PDA visent davantage l'ordinateur de bureau et le réseau de l'utilisateur et se servent du PDA comme vecteur. En s'assurant que les applications antivirus fonctionnent sur l'ordinateur de bureau de l'utilisateur et sur le portatif, et que les dernières définitions de virus ont été utilisées, on obtiendra une protection optimale.

2.5 Sécurité des communications

2.5.1 Interfaces de communication

Les PDA peuvent maintenant communiquer très facilement par l'intermédiaire d'un large éventail d'interfaces de communication. À l'heure actuelle, des modules d'extension permettent

aux PDA d'accepter tous les types de cartes PCMCIA que l'on trouve normalement sur les portatifs. Par conséquent, les PDA ne sont plus désormais restreints au seul échange d'information via un berceau connecté à un poste de travail, mais peuvent communiquer grâce aux technologies infrarouges ou radiofréquences (RF).

La communication entre les dispositifs est habituellement amorcée par l'utilisateur. Toutefois, certains PDA peuvent être configurés pour accepter et transmettre automatiquement de l'information, comme les programmes de données d'application et les applets, sans aucune intervention, voire sans la connaissance de l'utilisateur. Afin de réduire le risque de recevoir et d'envoyer des logiciels non prévus ou potentiellement malveillants, les PDA offrant cette fonctionnalité devraient être configurés de sorte que la réception et la transmission de l'information soient amorcées par l'utilisateur. Si cela n'est pas possible à cause du contrôle de la configuration, on devrait à tout le moins configurer ces dispositifs pour que ce soit l'utilisateur qui lance les programmes et les applets reçus. Les paramètres de configuration des dispositifs devraient être vérifiés avec soin, car leurs valeurs par défaut rendent le dispositif vulnérable aux attaques. On commence à voir apparaître sur le marché des gardes-barrières pour PDA, et on devrait les utiliser afin d'empêcher l'accès non autorisé via ces interfaces de communication.

Le CST tente actuellement de favoriser des progrès techniques dans la technologie de la transmission sans fil, afin d'incorporer des mécanismes de sécurité qui répondent aux exigences de sécurité cryptographique du GC.

2.5.2 Communications RF

Tout dépendant du mode de transmission, les communications par radiofréquences (RF) sont plus susceptibles à l'interception et à l'exploitation, jusqu'à des distances pouvant atteindre plusieurs kilomètres. L'utilisation de produits de chiffrement comme les applications de réseau privé virtuel (RPV) ou les logiciels de chiffrement des courriels, et qui répondent aux exigences cryptographiques du GC, offrent une protection adéquate contre la divulgation accidentelle ou l'écoute clandestine par un adversaire peu sophistiqué.

Les communications RF peuvent également être visées par des attaques par inondation, qui pourraient causer un déni de service ou obliger le PDA à être resynchronisé, permettant ainsi à des utilisateurs indésirables de se joindre au réseau. La première menace est difficile à contrer avec les produits commerciaux. La deuxième peut l'être à l'aide d'un schéma d'authentification (et d'un dispositif adéquat).

2.5.3 Communications dans l'infrarouge

Les PDA utilisent l'infrarouge pour les communications à courte distance avec d'autres dispositifs de poche pareillement équipés, avec des PC ou encore avec des périphériques ou des téléphones cellulaires. Les télécommandes des téléviseurs et des magnétoscopes sont des exemples bien connus de dispositifs à infrarouge. La technologie infrarouge fonctionne seulement quand les dispositifs sont en visée directe les uns des autres, et les infrarouges ne traversent pas les murs. Ces caractéristiques font que les PDA sont moins sujets à une attaque de type déni de service. Toutefois, des PDA mal configurés sont vulnérables aux adversaires qui ont accès à l'information enregistrée ou qui peuvent intercepter la transmission en utilisant les

fonctionnalités infrarouges du PDA, bien que l'attaquant doive se trouver relativement près du PDA.

2.5.4 Interface Bluetooth

Les PDA peuvent communiquer avec des dispositifs voisins à l'aide d'une carte d'interface PCMCIA Bluetooth ou d'une fonctionnalité Bluetooth intégrée. Le protocole Bluetooth est un mécanisme de transmission qui prend en charge la voix et les données, et permet une connectivité sans fil à courte distance (jusqu'à 10 mètres) entre divers dispositifs électroniques comme les ordinateurs, les téléphones et de l'équipement de divertissement. On peut facilement se procurer et utiliser de l'équipement d'interception et d'exploitation des signaux Bluetooth. Le CST a fait des recherches sur le mode de transmission Bluetooth, et on devrait consulter le rapport intitulé *Évaluation des vulnérabilités de Bluetooth* (ITSPSR-17).

2.5.5 Réseaux locaux sans fil (WLAN)

Les PDA peuvent également communiquer sans fil sur un réseau local (LAN), en utilisant une carte de périphérique PCMCIA Ethernet sans fil. L'interface pour PDA utilise le protocole de communication IEEE 802.11, qui offre une portée d'environ 100 mètres. Le CST a effectué plusieurs recherches sur la technologie LAN sans fil, et on devrait consulter le document intitulé *Examen préliminaire de la vulnérabilité des réseaux locaux sans fil* (ITSG-14). On peut se procurer ce document à l'adresse suivante : http://www.cse-cst.gc.ca/fr/knowledge_centre/publications/manuals/ITSG-14.html.

2.5.6 Réseaux de téléphonie cellulaire

Les PDA peuvent être directement connectés aux téléphones cellulaires ou encore utiliser une interface PCMCIA pour système de communications personnelles (SCP), afin de permettre à l'utilisateur de communiquer avec le réseau de son organisation, via le réseau téléphonique cellulaire. Le CST a effectué des recherches sur les vulnérabilités du réseau SCP et on devrait consulter différents rapports à ce sujet : *Trends in Wireless Technology and Security – A Market Research Study* (ITSPSR-20), *Government of Canada Wireless Vulnerability Assessment* (ITSPSR-15) et *Personal Communication System (PCS) and Cellular System Vulnerability Assessment* (ITSPSR-16) (pas encore disponibles en français).

2.5.7 Réseaux téléphoniques terrestres

On peut également connecter les PDA à Internet et/ou au réseau de l'organisation, par l'intermédiaire d'une carte modem PCMCIA ordinaire et du réseau téléphonique terrestre. Cela présente les mêmes risques qu'un ordinateur utilisé à la maison avec un modem. La voie de communication entre le dispositif de poche et l'ordinateur de bureau ou le serveur à distance passe par une connexion Internet ou téléphonique non fiable, qui présente des possibilités de compromission ou de corruption de l'information ou encore de routage erroné.

2.6 Sécurité acoustique

Plusieurs modèles de PDA offrent maintenant une fonction intégrée d'enregistrement de la voix, qui peut facilement être activée accidentellement par la simple pression d'un bouton, même

quand le dispositif est hors tension et qu'il est protégé par un mot de passe. Ces dispositifs contiennent des microphones sensibles qui peuvent enregistrer le bruit ambiant et les conversations distantes. On ne devrait donc pas amener ces dispositifs dans des zones où des conversations sensibles se déroulent. Le cas échéant, les utilisateurs devraient au moins être avisés que leurs discussions peuvent être compromises.

2.7 Sécurité des émanations radioélectriques

Les systèmes informatiques et leurs périphériques (p. ex., les imprimantes, les systèmes de projection, etc.) produisent un rayonnement radioélectrique qui peut être intercepté et analysé, dans le but de récupérer l'information sensible qu'il peut contenir. Un PDA offrant des fonctionnalités de communication sans fil et utilisé à proximité de ce type d'équipement devient un excellent véhicule pour diffuser de l'information sensible, qui pourrait par la suite être interceptée par un adversaire sophistiqué, et l'information serait donc compromise. Les utilisateurs devraient mettre hors tension toutes les fonctions de communication sans fil sur leur PDA dans les zones où de l'information classifiée est traitée électroniquement.

2.8 Sécurité cryptographique

Le risque de compromission de l'information pendant son stockage ou sa transmission, par l'intermédiaire de réseaux de communications terrestres ou sans fil, peut être atténué grâce à des systèmes cryptographiques approuvés par le GC. Les exigences cryptographiques du GC comprennent l'utilisation :

- a. de produits cryptographiques qui sont, utilisent ou intègrent des modules cryptographiques validés selon les normes FIPS 140-1 ou FIPS 140-2;
- b. des algorithmes cryptographiques et des schémas de gestion de clés approuvés par le GC.

La validation selon les normes FIPS 140-1 ou FIPS 140-2 garantit que les fonctions cryptographiques ont été correctement implémentées dans le produit, tandis que les algorithmes cryptographiques et les schémas de gestion de clés approuvés garantissent que les données chiffrées sont résistantes aux attaques d'analyses cryptographiques. On devrait consulter les sites Web suivants du CST, où l'on trouvera une liste des algorithmes approuvés et des modules validés :

http://www.cse-cst.gc.ca/fr/services/crypto_services/crypto_algorithms.html

http://www.cse-cst.gc.ca/fr/services/industrial_services/cmv_val_products.html

2.9 Sécurité des réseaux classifiés

Une partie importante de l'information traitée sur les réseaux classifiés, comme les rendez-vous et les calendriers, n'est pas classifiée. Bien que le transfert et la transmission de cette information classifiée vers un PDA puissent sembler une pratique sûre, il subsiste néanmoins le risque que de l'information classifiée pourrait accidentellement être transférée, ou que quelqu'un obtienne un accès non autorisé au réseau classifié par l'intermédiaire d'un PDA (p. ex., à cause d'une erreur humaine ou du mauvais fonctionnement d'un logiciel). La connexion sans fil du PDA au réseau classifié requiert que la sécurité globale du réseau soit modifiée, ce qui pourrait le rendre

vulnérable aux attaques, notamment les détournements de session ou les balayages de port. Enfin, le vol ou la perte d'un dispositif de poche pourrait potentiellement compromettre l'information enregistrée sur le dispositif et offrir un accès non autorisé au réseau classifié, par l'intermédiaire de ce dispositif.

Compte tenu de tous les points soulevés dans la section 2 de ce document, on ne devrait donc pas permettre aux PDA d'accéder aux réseaux classifiés. Le CST travaille avec ses alliés afin d'élaborer des solutions qui pourraient être utilisées avec l'information et les systèmes classifiés.

3 Système BlackBerry™

3.1 Aperçu du système BlackBerry™

L'agenda électronique sans fil BlackBerry™ est un PDA de petite taille, mais puissant, qui offre diverses applications, notamment un calendrier, un carnet d'adresses, une liste de tâches, ainsi que la possibilité d'envoyer et de recevoir des courriels sans nécessiter une connexion câblée. Le système BlackBerry™ peut être configuré pour fonctionner selon quatre différents modes :

- a. édition Internet BlackBerry™;
- b. BlackBerry™ à BlackBerry™;
- c. BlackBerry™ Redirector;
- d. BlackBerry Enterprise Server™ (BES).

Chaque mode de fonctionnement est décrit brièvement ci-dessous.

À l'heure actuelle, Rogers AT&T et Bell Mobilité prennent en charge le système BlackBerry™ au Canada. Dans ce rapport, nous les désignons par l'expression « fournisseurs de services cellulaires ».

3.2 Relais BlackBerry™

Le relais BlackBerry™ est situé entre le réseau du fournisseur de services cellulaires et Internet. Son rôle est de réacheminer les communications de données en direction et en provenance des agendas BlackBerry™, d'après les NIP des dispositifs. La Figure 1 illustre son fonctionnement. Le relais BlackBerry™ est situé à l'intérieur du réseau du fournisseur de services cellulaires.

Le relais BlackBerry™ réachemine les courriels et les autres paquets de données vers l'agenda BlackBerry™ et, si le dispositif est mis hors tension, le relais conservera les courriels jusqu'à ce que l'agenda soit mis sous tension. Les données peuvent ainsi être conservées dans le relais pendant plusieurs jours, si l'agenda n'est pas mis sous tension.

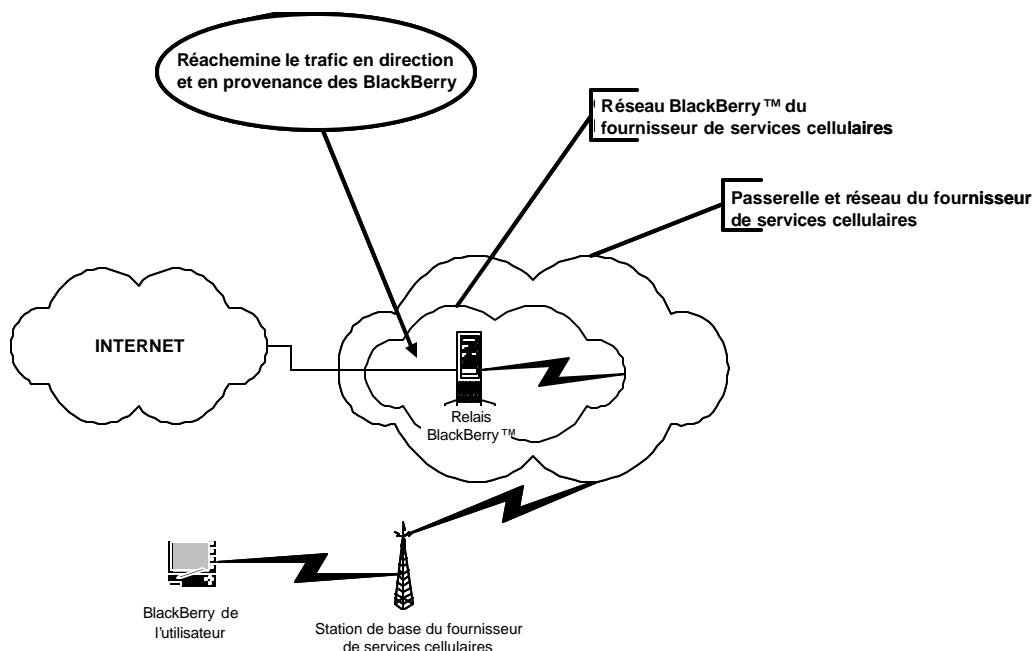


Figure 1 – Relais BlackBerry™

3.3 Fonctionnalité cryptographique du système BlackBerry™

La société Research In Motion Limited (RIM) a implémenté l'algorithme de chiffrement symétrique Triple DES (*Data Encryption Standard*), avec une clé de 112 bits. Toutefois, cette fonctionnalité de chiffrement est disponible uniquement avec les options BlackBerry™ Redirector et BES. L'algorithme Triple DES est un algorithme cryptographique approuvé par le GC pour la protection de l'information désignée. Nous recommandons que la clé de chiffrement soit changée au moins chaque semaine. Au moment de la publication, le microprogramme intégré aux produits RIM 850, RIM 857, RIM 950 et RIM 957 Wireless Handheld™ avait été validé selon les normes FIPS 140-1 ou FIPS 140-2, au niveau de sécurité 1. Toutefois, le module cryptographique contenu dans les options BES et Redirector n'avait pas été validé au niveau FIPS 140-1 et, à ce titre, le CST n'a aucun niveau d'assurance au sujet des fonctionnalités cryptographiques implémentées dans ces composants critiques du système. Pour avoir la liste actualisée des produits validés, veuillez consulter le site Web du CST à l'adresse http://www.cse-cst.gc.ca/fr/services/industrial_services/cm_val_products.html. Reportez-vous également à l'avis de sécurité pour les TI *Algorithmes cryptographiques approuvés par le CST pour la protection des renseignements désignés et pour les applications d'autorisation et d'authentification électroniques au sein du gouvernement du Canada* (ITSA-11A), pour avoir de l'information sur la gestion des clés avec l'algorithme Triple DES. Communiquez avec l'équipe des Services à la clientèle du CST au (613) 991-7600 ou à l'adresse client.svcs@cse-cst.gc.ca, pour obtenir l'annexe A, qui contient des renseignements additionnels sur les fonctions cryptographiques utilisées dans le système BlackBerry™.

3.4 BlackBerry™ édition Internet

La Figure 2 illustre l'option BlackBerry™ édition Internet. Cette option est disponible des deux fournisseurs de services cellulaires. Le fournisseur gère un serveur de courriel Microsoft (MS) Exchange et un BES, et les utilisateurs des BlackBerry™ édition Internet ont un compte sur ce serveur (p. ex., nom_utilisateur@mobile.rogers.com). Le serveur MS Exchange et le BES sont connectés au relais BlackBerry™, qui assure la connectivité avec les agendas BlackBerry™.

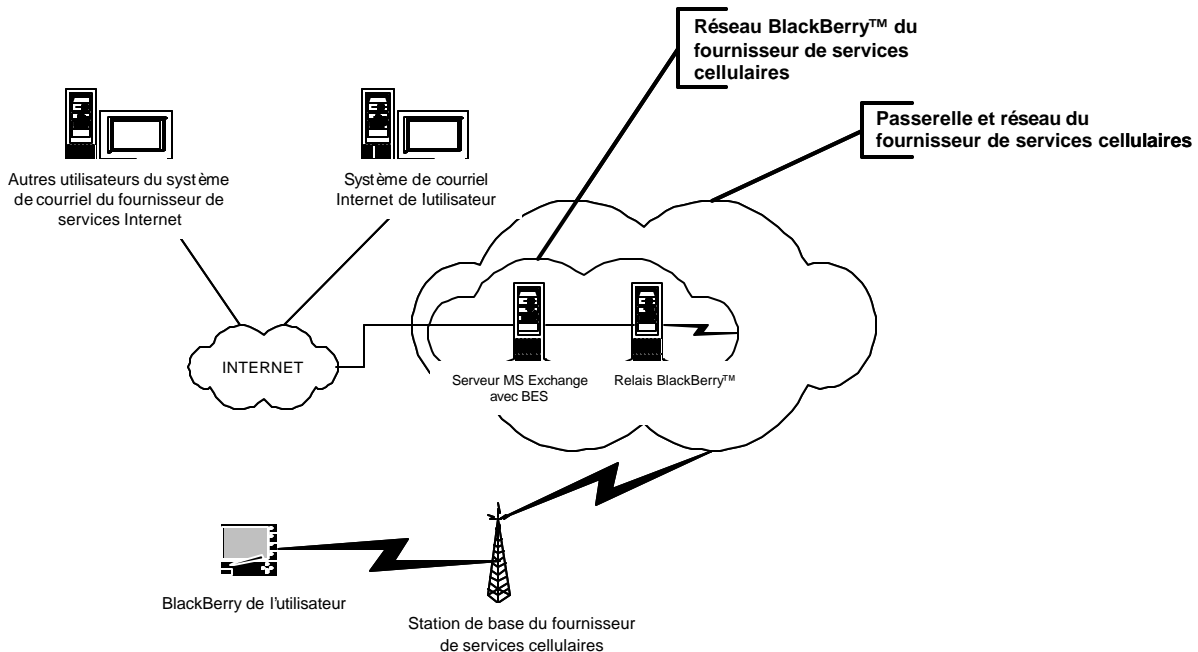


Figure 2 – BlackBerry™ édition Internet

Quand l'utilisateur envoie un courriel à un autre utilisateur, le serveur MS Exchange le reçoit et l'achemine au BES, pour qu'il soit transmis au BlackBerry™. À la différence des autres topologies utilisant le BES, la transmission vers le BlackBerry™ de l'utilisateur n'est pas chiffrée. De plus, comme avec tout autre service de courriel, les courriels sont stockés sur le serveur MS Exchange du fournisseur jusqu'à ce que l'utilisateur les télécharge vers son poste de travail. L'inverse s'applique également quand l'utilisateur envoie un courriel depuis son agenda électronique. Le message est de nouveau transmis en clair au relais BlackBerry™, par l'intermédiaire du réseau cellulaire, d'où il sera acheminé vers le serveur MS Exchange/BES, en vue de sa transmission sur Internet. Une copie du courriel est enregistrée sur le serveur MS Exchange.

L'analyse du CST a démontré que cette option présente plusieurs vulnérabilités :

- a. l'information transmise n'est pas chiffrée et peut être interceptée et exploitée;
- b. l'information réside en clair sur un serveur qui n'est contrôlé par aucun ministère du GC, et qui peut être exploitée par des pirates et du personnel malveillant chez le fournisseur de services cellulaires;

- c. il est fort probable que l'information soit sauvegardée en clair par le fournisseur de services cellulaires; elle pourrait donc être exploitée par des pirates ou du personnel malveillant chez ce fournisseur;
- d. l'information n'est pas chiffrée quand elle est téléchargée vers l'ordinateur de l'utilisateur et quand celui-ci ouvre une session sur le serveur du fournisseur de services cellulaires; elle peut donc être interceptée et exploitée;
- e. l'information pourrait potentiellement demeurer dans le relais BlackBerry™ si l'utilisateur ne met pas sous tension son BlackBerry™. Cette information pourrait donc être exploitée par des pirates ou du personnel malveillant chez le fournisseur de services cellulaires.

Le CST ne recommande pas l'utilisation de cette option par les ministères du GC pour transmettre de l'information sensible.

3.5 BlackBerry™ à BlackBerry™

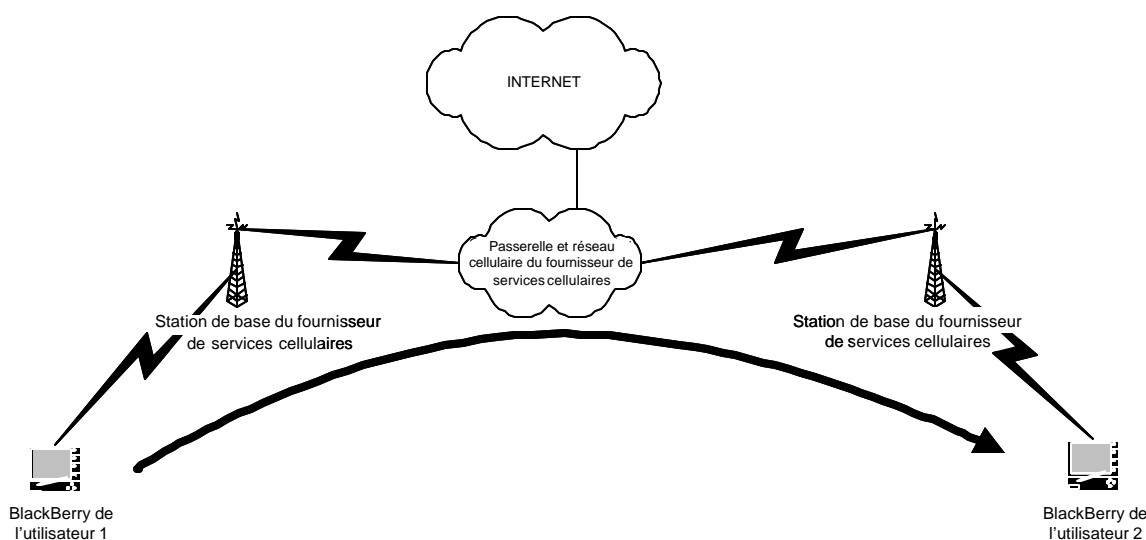


Figure 3 – Fonctionnement de l'option BlackBerry™ à BlackBerry™

La Figure 3 illustre le fonctionnement de l'option BlackBerry™ à BlackBerry™. En effet, BlackBerry™ offre l'option d'émettre de l'information directement d'un BlackBerry™ à un autre, en utilisant seulement le réseau téléphonique cellulaire, sans devoir passer par Internet. Cette option est couramment appelée option NIP-à-NIP. Le BlackBerry™ chiffre le message à l'aide de l'algorithme Triple DES, mais avec une clé cryptographique qui a été installée au préalable dans chaque BlackBerry™. Comme cette clé programmée est la même sur tous les BlackBerry™, cela crée une vulnérabilité exploitable. Le CST ne recommande pas l'utilisation de cette option par les ministères du GC pour transmettre de l'information sensible.

3.6 BlackBerry™ Redirector

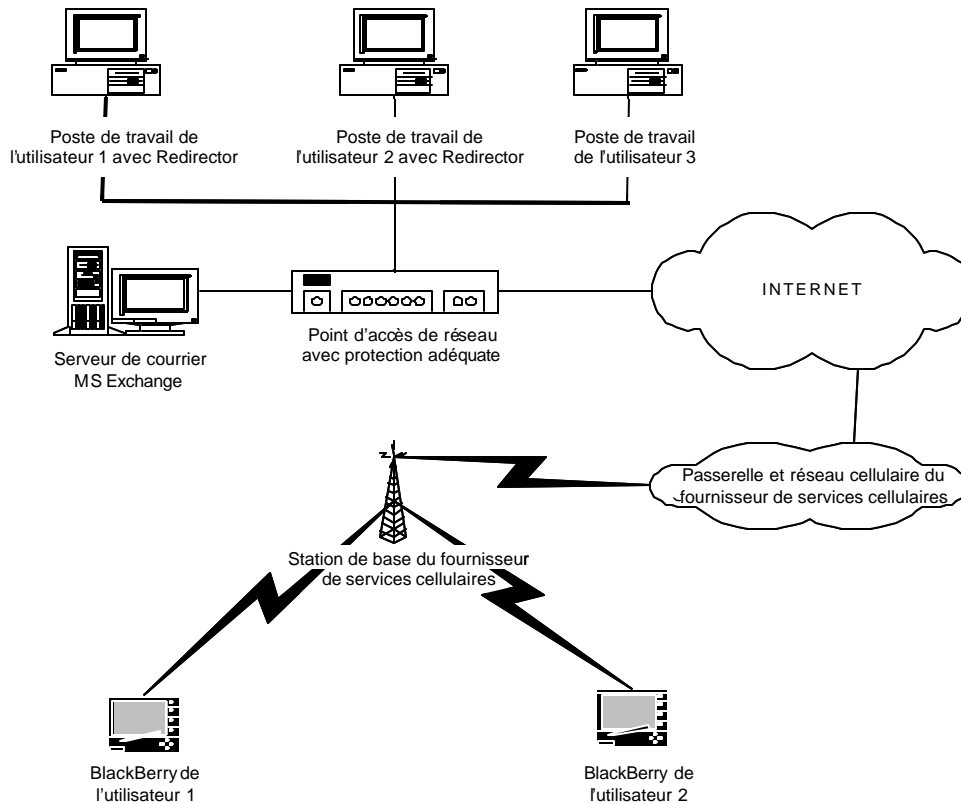


Figure 4 – Application BlackBerry™ Redirector

L'application BlackBerry™ Redirector est installée sur le poste de travail de l'utilisateur et réachemine tous les courriels entrant vers le BlackBerry™ de l'utilisateur ou, si le courriel est en provenance du BlackBerry™ de l'utilisateur, celui-ci sera redirigé vers le destinataire voulu. Cette application assure le chiffrement de tous les messages transmis sur la liaison entre le poste de travail sur lequel est installée l'application BlackBerry™ Redirector, et l'agenda électronique BlackBerry™, à l'aide de l'algorithme Triple DES. Tous les autres courriels reçus d'un autre destinataire ou envoyés à un autre destinataire ne sont pas chiffrés. Pour fonctionner, cette option requiert que le poste de travail de l'utilisateur soit mis sous tension et qu'une session sur BlackBerry™ Redirector soit ouverte. Ce scénario exige également que des mesures de sécurité adéquates soient prises afin de protéger ce poste de travail potentiellement vulnérable.

La clé Triple DES est générée sur le poste de travail de l'utilisateur et téléchargée vers le BlackBerry™, quand celui-ci est inséré dans son berceau. Bien que cette méthode de génération de clé soit jugée adéquate pour le niveau de sécurité envisagé (Protégé B), son implémentation n'a pas été testée par une tierce partie selon des critères d'essai connus (p. ex., FIPS 140-1, FIPS 140-2 ou Critères communs).

La Figure 4 décrit le fonctionnement de l'application BlackBerry™ Redirector. Si l'utilisateur 1 envoie un courriel à l'utilisateur 3 à partir de son BlackBerry™, le message sera transmis sous forme chiffrée de l'agenda électronique au poste de travail où réside l'application BlackBerry™

Redirector. Le message sera protégé pendant sa transmission sur la liaison RF, le réseau du fournisseur de services cellulaires et Internet, puis entrera dans le réseau de l'utilisateur et atteindra son poste de travail, où le message sera déchiffré. L'application de courrier électronique sur le poste de travail prendra alors en charge le message comme tout autre message, et l'enverra, sous forme non chiffrée, vers le serveur MS Exchange. Le courriel sera ensuite envoyé à l'utilisateur 3, toujours en clair. Le même processus a lieu si l'utilisateur 3 est à l'extérieur du réseau de l'utilisateur 1.

Si l'utilisateur 1 envoie un courriel à l'utilisateur 2, le courriel suivra le même chemin chiffré, jusqu'à son poste de travail, puis en clair jusqu'au serveur MS Exchange, et jusqu'au poste de travail de l'utilisateur 2. Comme l'application BlackBerry™ Redirector fonctionne sur le poste de travail de l'utilisateur 2, le message sera chiffré depuis ce poste de travail jusqu'au BlackBerry™ de l'utilisateur 2.

Cette option règle en partie les problèmes de sécurité soulevés dans le cas des options BlackBerry™ édition Internet BlackBerry™ à BlackBerry™, car l'information est enregistrée sur des réseaux et des biens contrôlés par le GC, et la génération de la Triple DES est plus sûre. Toutefois, quand on utilise cette option, on doit tenir compte des problèmes de sécurité possibles décelés par le CST pendant l'analyse :

- a. la confidentialité des courriels est garantie seulement jusqu'au poste de travail de l'utilisateur (si l'option de chiffrement est activée). Le courriel sera assujéti aux règles de sécurité automatisées qui sont imposées à tout le réseau (p. ex., tout le courriel n'est habituellement pas chiffré);
- b. les mesures de sécurité physiques appliquées au poste de travail de l'utilisateur doivent être évaluées, car ce poste de travail doit toujours être opérationnel (p. ex., les écrans de veille doivent être désactivés).

Bien que cette option offre une sécurité cryptographique adéquate, le CST n'en recommande pas l'utilisation à cause des vulnérabilités associées au poste de travail sans surveillance.

3.7 BlackBerry Enterprise Server™ (BES)

3.7.1 Généralités

La fonction de l'application BES est similaire à celle du BlackBerry™ Redirector, sauf qu'elle fonctionne conjointement avec le serveur MS Exchange. Bien que le serveur BES puisse fonctionner sur le même serveur physique que MS Exchange Server, RIM recommande d'utiliser le BES sur un serveur physique distinct. Le serveur BES centralise alors les fonctions de redirection et de chiffrement des courriels autour du serveur de courrier. Comme le BES fonctionne conjointement avec le serveur MS Exchange, l'utilisateur n'est pas tenu d'ouvrir une session sur son poste de travail, ce qui élimine les problèmes de sécurité critiques associés au fonctionnement sans surveillance du poste de travail de l'utilisateur avec le BlackBerry™ Redirector.

Le mécanisme de chiffrement utilisé avec le BES est très similaire à celui qui est employé avec le BlackBerry™ Redirector. Le chiffrement est appliqué uniquement aux messages échangés entre le BES de l'utilisateur et l'agenda électronique, et, en tant que tel, il n'offre pas une

protection inhérente de bout en bout entre le dispositif de l'expéditeur et celui du destinataire. La voie de communication entre le BES de l'utilisateur et le serveur du destinataire n'est pas protégée par le système BlackBerry™ de l'expéditeur. À l'inverse, si le destinataire est un utilisateur du BlackBerry™, la liaison de communication entre son BES et son dispositif BlackBerry™ est chiffrée, ce qui offre de nouveau un certain niveau de protection sur la liaison RF.

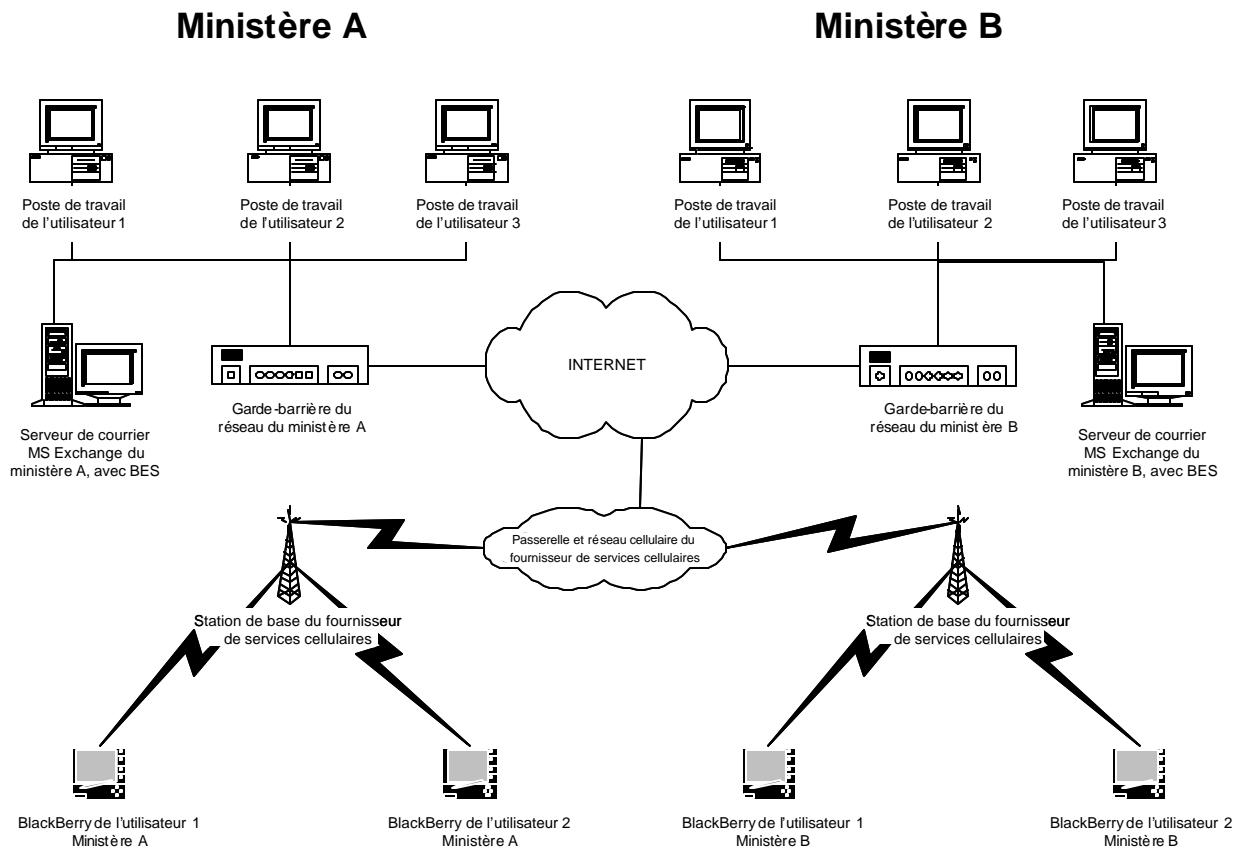


Figure 5 – BlackBerry Enterprise Server™

La Figure 5 illustre l'infrastructure proposée par RIM pour l'utilisation des agendas BlackBerry™ qui communiquent sans fil avec les réseaux locaux (LAN) des ministères. L'application BES est installée avec le serveur MS Exchange du ministère, pour réacheminer tout courriel destiné au compte de l'utilisateur mobile, depuis le serveur de courrier électronique du ministère vers le BlackBerry™ de cet utilisateur. Le BES accède aux clés Triple DES, stockées localement, afin de chiffrer tous les messages destinés à l'agenda électronique, et déchiffre tous les messages reçus de cet agenda. Tout comme dans le cas de l'application BlackBerry™ Redirector, les clés Triple DES sont générées sur le poste de travail de l'utilisateur et téléchargées vers le serveur MS Exchange, et seront utilisées par le BES. Il est important de souligner ici que la fonction de génération de clés, exécutée sur le poste de travail, ainsi que les

fonctions de chiffrement et de déchiffrement effectuées sur le BES, n'ont pas été testées et validées selon les normes FIPS 140-1 et FIPS 140-2.

On présuppose que les réseaux des ministères ont correctement été configurés et gérés, de sorte que des utilisateurs malveillants de l'extérieur ne peuvent pas accéder aux données sensibles enregistrées sur le réseau, et que les données transmises à l'extérieur de celui-ci sont adéquatement protégées.

Un courriel transmis à un utilisateur mobile arrivera d'abord à son compte de courrier au ministère où il travaille, compte qui est géré par un serveur MS Exchange. Ce serveur réacheminera le courriel vers l'application BES, qui chiffrera alors le message à l'aide de l'algorithme de chiffrement Triple DES et de la clé enregistrée localement, et enverra le courriel au réseau sans fil du fournisseur de services cellulaires, via Internet, pour la transmission sans fil du courriel vers le portatif BlackBerry™. Quand le portatif reçoit le courriel, il le déchiffre automatiquement et l'enregistre en clair dans sa mémoire interne, afin que l'utilisateur puisse le consulter ultérieurement.

À l'inverse, quand un utilisateur mobile envoie un courriel, son BlackBerry™ chiffre le message à l'aide de la clé Triple DES, et le transmet à son serveur MS Exchange par l'intermédiaire du réseau sans fil du fournisseur de services cellulaires et d'Internet. Quand l'application BES reçoit le message, elle le déchiffre et l'achemine vers le serveur MS Exchange. Ce dernier traitera le message comme tout autre message, qu'il soit destiné à un utilisateur interne ou à un utilisateur externe.

3.7.2 Courrier électronique intraministériel à l'aide des BlackBerry™¹

Dans le cas où deux utilisateurs d'un même ministère s'échangent des courriels à l'aide de leurs BlackBerry™, le trafic entre les agendas sans fil et le BES est chiffré à l'aide de l'algorithme Triple DES. Le message est jugé adéquatement protégé, car le courriel circule de l'expéditeur au destinataire sous forme chiffrée, et lorsque le message est en clair, il se trouve derrière un garde-barrière correctement configuré.

3.7.3 Courrier électronique interministériel à l'aide des BlackBerry™²

Dans ce scénario, deux utilisateurs travaillent dans des ministères différents et échangent des courriels à l'aide de leurs BlackBerry™. Un courriel transmis de l'expéditeur est chiffré sur son propre appareil sans fil, à l'aide de l'algorithme Triple DES, puis est transmis vers son application BES où il est déchiffré et acheminé au serveur MS Exchange, en vue du routage.

1 Dans cette situation, on suppose que tout le ministère se rassemble dans une seule enclave, présentant un seul point d'entrée.

2 Cette situation s'applique à tous les cas où les données sont transmises entre deux enclaves séparées, par l'intermédiaire d'Internet.

Le traitement de ce courriel par le serveur Exchange est identique à celui de tout courriel transmis depuis un poste de travail ordinaire, et sera effectué selon les politiques établies (p. ex., cryptographie à clé publique, RPV). Par conséquent, si aucun mécanisme de protection n'est mis en place entre deux utilisateurs de deux ministères différents, le message sera transmis en clair (c.-à-d. non chiffré), sur Internet.

Lorsque le courriel arrive au serveur MS Exchange du ministère du destinataire, le BES chiffre le message puis le transmet via Internet et le réseau sans fil au BlackBerry™ du destinataire. L'appareil sans fil du destinataire déchiffre le message et l'enregistre dans sa mémoire, pour que l'utilisateur puisse le lire. Une copie de ce message est également enregistrée dans le compte d'utilisateur sur le serveur MS Exchange de son ministère.

3.7.4 Port 3101 du protocole de contrôle de transmission (TCP)

Le BES requiert l'ouverture du port TCP 3101 sur le garde-barrière du ministère, pour accéder au relais BlackBerry™ situé entre Internet et le réseau du fournisseur de services sans fil. Chaque fois qu'un nouveau port est ouvert sur le réseau d'un ministère, celui-ci devrait revoir son évaluation des menaces et des risques (EMR), afin de s'assurer que cette modification n'invalidé aucune hypothèse ou décision faite pendant la préparation de l'EMR. Si les règles d'utilisation du garde-barrière sont correctement écrites, seul le BES pourra alors ouvrir une connexion sur ce port. La connexion sur le port TCP 3101 est ouverte vers l'extérieur seulement par le BES quand il établit une connexion avec le relais BlackBerry™ sur le réseau sans fil (via le port TCP 3101). Par conséquent, on devrait mettre en place des mécanismes de sécurité afin d'empêcher tout hôte autre que le BES, à l'intérieur ou à l'extérieur de l'organisation, d'établir cette connexion.

La connexion entre l'application BES et le relais BlackBerry™, situé à la lisière du réseau du fournisseur de services sans fil, par l'intermédiaire du port TCP 3101, doit être authentifiée par le BES. Si celui-ci ne peut pas vérifier l'authenticité du relais BlackBerry™, la connexion est rompue. Tout le trafic circulant par le port TCP 3101 est chiffré à l'aide de l'algorithme Triple DES.

3.7.5 Résumé

Bien que le système BlackBerry™ offre des fonctions de sécurité pour la communication sans fil entre le BES et les dispositifs de poche BlackBerry™, il n'assure pas une sécurité de bout en bout pour l'envoi d'un message entre deux utilisateurs qui sont dans le même ministère ou dans deux ministères différents. En effet, le message doit circuler entre deux serveurs MS Exchange/BES de façon non chiffrée, à moins que des mécanismes externes n'aient été mis en place (p. ex. Entrust Express, RVP) pour protéger la transmission. Cette situation peut porter les utilisateurs à croire, à tort, que « si mon BlackBerry™ chiffre le message, celui-ci est chiffré pendant toute sa transmission ».

Page laissée intentionnellement en blanc.

4 Solutions proposées pour sécuriser le système BlackBerry™

4.1 Généralités

La solution souhaitable, pour le GC, serait d'utiliser le système BlackBerry™ comme suit :

- a. assurer le chiffrement de bout en bout entre l'agenda électronique BlackBerry™ de l'expéditeur et le poste de travail du destinataire, ou utiliser des certificats numériques gérés par l'infrastructure à clé publique du gouvernement du Canada (ICP GC), directement sur le portatif;
- b. s'assurer que l'information sensible est enregistrée à l'interne sous forme chiffrée;
- c. s'assurer que toutes les applications cryptographiques répondent aux exigences cryptographiques du GC.

Des solutions provisoires sont disponibles et le CST collabore avec RIM afin d'élaborer des solutions à long terme.

4.2 RVP entre ministères

Afin d'assurer une protection de bout en bout pour la transmission des courriels par les utilisateurs mobiles, à l'aide de leurs agendas électroniques BlackBerry™ et du BES, les ministères qui prennent en charge ces utilisateurs pourraient déployer des modules de chiffrement RVP entre eux. En plus d'assurer la protection des utilisateurs mobiles, la mise en place de ces modules permettrait également de protéger tous les messages et données, sensibles ou non, transmis entre ces ministères. La Figure 6 illustre cette solution.

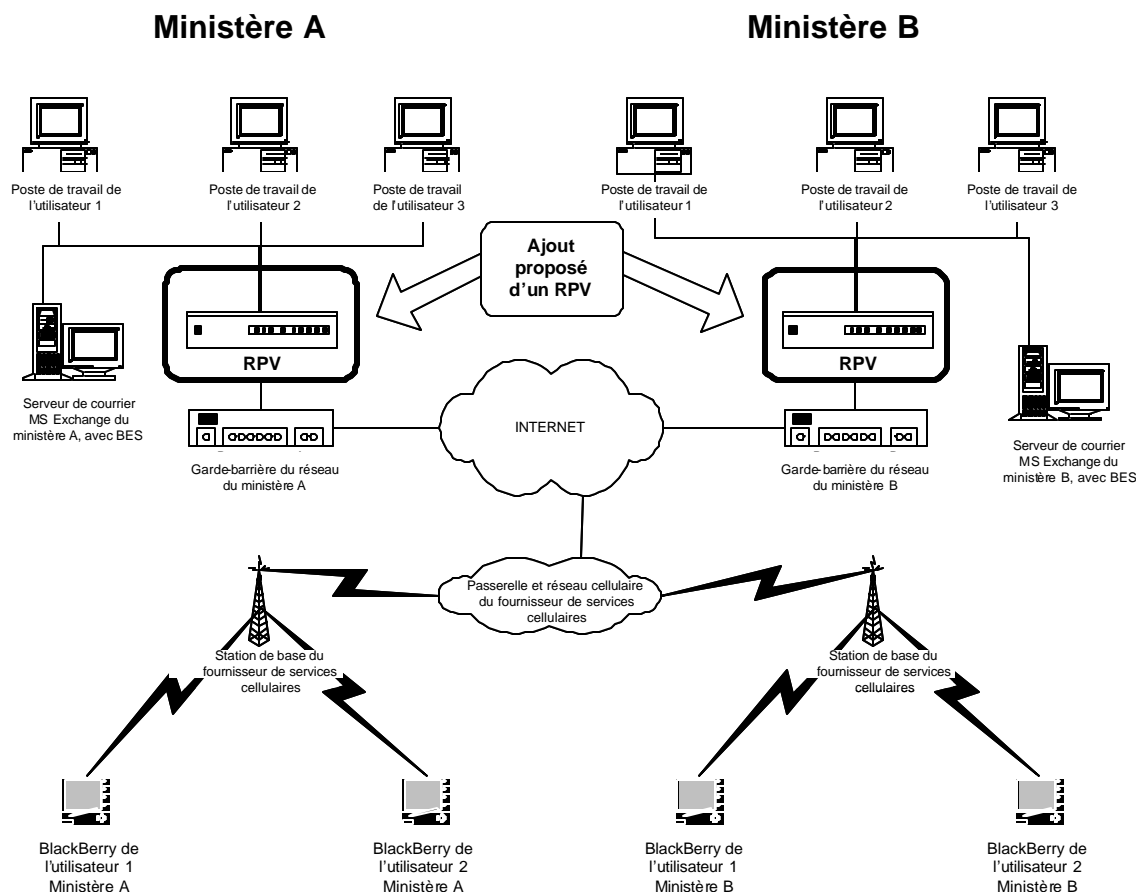


Figure 6 – BlackBerry Enterprise Server™ avec des RPV déployés

Toutefois, cette solution est limitée, en ce sens que les utilisateurs ne peuvent pas envoyer de manière sûre des courriels à des utilisateurs sur des réseaux qui n'ont pas déployé des RPV interopérables. Comme la couche de chiffrement du RPV est transparente pour les utilisateurs, ils pourraient, à tort, croire que tous les courriels transmis sont protégés de bout en bout, alors que ce n'est pas le cas. Même avec l'utilisation de modules de chiffrement RPV, les données stockées sur les agendas électroniques ne sont pas chiffrées. Les utilisateurs devraient être avisés de ces limites de leurs appareils, et savoir à quels utilisateurs/réseaux ils peuvent envoyer des courriels de manière sûre.

Cette solution serait avantageuse pour les ministères qui ont déjà déployé ou qui prévoient déployer des RPV interopérables, car le coût d'installation et de maintenance pourrait être élevé. Nous recommandons que les ministères déploient des produits qui répondent aux exigences cryptographiques du GC énumérées à la section 2 du présent document. La liste des modules cryptographiques validés, qui contient plusieurs RPV validés offerts par diverses compagnies, se trouve à l'adresse suivante :

http://www.cse-cst.gc.ca/fr/services/industrial_services/cmval_products.html

4.3 Solution BlackBerry™ avec protocole S/MIME

Le CST travaille actuellement avec RIM afin d'élaborer une solution BlackBerry™ utilisant le protocole S/MIME, solution qui est parrainée par le gouvernement et qui permettra de transmettre de manière sûre des courriels sensibles, protégés par des fonctions cryptographiques de bout en bout à l'aide du protocole S/MIME. Cette solution permettra aux utilisateurs d'envoyer des courriels à tout BlackBerry™ qui utilise une application S/MIME ou au poste de travail de tout utilisateur qui prend en charge les courriels S/MIME. Les courriels qui ont été reçus en format chiffré sont enregistrés en format chiffré sur l'agenda BlackBerry™. Les messages sont déchiffrés afin d'être lus, puis sont rechiffrés quand ils sont fermés. Cette solution utilisera l'ICP GC, déjà en place, afin de récupérer le certificat public du destinataire, lequel est crucial pour assurer la sécurité de la transmission de bout en bout. De plus, elle assurera la validité des certificats publics et utilisera des algorithmes cryptographiques approuvés par le GC. Enfin, cette solution sera ultérieurement validée selon les normes FIPS 140-1 ou FIPS 140-2.

On prévoit que la solution BlackBerry™ avec protocole S/MIME, parrainée par le gouvernement, sera implémentée à l'automne 2002.

4.4 Version commerciale de l'agenda électronique BlackBerry™ avec protocole S/MIME

La société RIM travaille actuellement sur une version commerciale de la solution BlackBerry™ avec protocole S/MIME, parrainée par le gouvernement, et qui fonctionnera dans le mode GPRS (service général de radiocommunication en mode paquet). RIM n'a pas indiqué quand cette solution sera disponible sur le marché.

Page laissée intentionnellement en blanc.

5 Conclusions

5.1 Résumé des pratiques recommandées

5.1.1 Pratiques recommandées générales pour l'utilisation des PDA

Ce rapport présente plusieurs recommandations afin de protéger l'information enregistrée sur les PDA et transmis en direction ou en provenance des réseaux d'une organisation. Voici un résumé de ces recommandations :

- a. les fonctions de contrôle d'accès doivent être activées;
- b. les utilisateurs doivent sélectionner de façon aléatoire des mots de passe et des NIP, et les modifier régulièrement;
- c. l'information enregistrée sur les PDA doit être chiffrée à l'aide de mécanismes qui répondent aux exigences cryptographiques du GC. Si le PDA n'utilise pas ces mécanismes de sécurité ou s'il est perdu ou volé, l'information enregistrée sur ce PDA est alors jugée compromise;
- d. si le poste de travail d'un utilisateur doit être connecté au réseau pour permettre le fonctionnement de son PDA, les mesures de sécurité prises pour protéger ce poste de travail doivent être à hauteur du niveau de sécurité de l'information traitée par le réseau;
- e. on doit utiliser des applications antivirus sur le PDA de l'utilisateur ou son poste de travail. Les définitions antivirales doivent être mises à jour le plus souvent possible;
- f. les communications du PDA, que ce soit par liaisons RF ou ligne terrestre, doivent être protégées à l'aide de produits qui répondent aux exigences cryptographiques du GC. Les clés cryptographiques doivent être modifiées régulièrement ou, à tout le moins, de la manière recommandée sur la page Web des algorithmes approuvés par le GC, pour l'algorithme sélectionné :
http://www.cse-cst.gc.ca/fr/services/crypto_services/crypto_algorithms.html
- g. on ne doit pas amener les PDA dans des zones où de l'information sensible est traitée ou fait l'objet de discussion;
- h. on ne doit pas permettre aux PDA d'accéder aux réseaux classifiés.

5.1.2 Pratiques recommandées pour l'utilisation du système BlackBerry™

Pour transmettre de l'information sensible, on ne devrait pas utiliser le système BlackBerry™ édition Internet, l'option BlackBerry™ à BlackBerry™ ni l'application BlackBerry™ Redirector.

Bien que le système BlackBerry Enterprise Server™ ait les meilleures fonctions de sécurité offertes par RIM, il n'assure pas une protection de bout en bout pour les courriels qui circulent à l'extérieur du réseau de l'organisation de l'utilisateur. Afin de régler ce problème, le CST recommande d'utiliser une des solutions suivantes :

- a. utiliser le BlackBerry Enterprise Server™ avec le déploiement de RPV entre les ministères;
- b. utiliser la solution BlackBerry™ avec protocole S/MIME.

5.2 Recommandation

La fonction de chiffrement offerte par le système BlackBerry™ devrait être utilisée, car elle assure un certain niveau de protection contre la divulgation accidentelle ou l'écoute clandestine par un adversaire peu sophistiqué, même si l'agenda électronique BlackBerry™ ne répond pas à toutes les exigences cryptographiques du GC. Par conséquent, on devrait utiliser ce dispositif uniquement avec l'information de niveau PROTÉGÉ B et inférieur.

5.3 Conclusion

Le CST continue de collaborer avec l'industrie afin d'élaborer des solutions sans fil pour protéger l'information sensible du GC. Le CST poursuit ses recherches sur les vulnérabilités des dispositifs sans fil en matière de sécurité, et il informera les ministères fédéraux de ses résultats et conclusions.

6 Bibliographie

- a. *Alerte de sécurité relative aux téléphones numériques mobiles SCP (Système de communications personnelles)* (ITSA-16A), février 2000, Centre de la sécurité des télécommunications.
- b. *Algorithmes cryptographiques approuvés le CST pour la protection des renseignements désignés et pour les applications d'autorisation et d'authentification électroniques au sein du gouvernement du Canada* (ITSA-11A), mars 2000, Centre de la sécurité des télécommunications.
- c. *Lignes directrices générales relatives à l'utilisation de dispositifs sans fil au sein du gouvernement fédéral* (ITSA-18), septembre 2001, Centre de la sécurité des télécommunications.
- d. *Examen préliminaire de la vulnérabilité des réseaux locaux sans fil* (ITSG-14), octobre 2001, Centre de la sécurité des télécommunications.
- e. *Government of Canada Wireless Vulnerability Assessment* (ITSPSR-15), mai 2002, Centre de la sécurité des télécommunications.
- f. *Personal Communications Systems (PCS) and Cellular System Vulnerability Assessment* (ITSPSR-16), octobre 2002, Centre de la sécurité des télécommunications.
- g. *Évaluation des vulnérabilités de Bluetooth* (ITSPSR-17), octobre 2002, Centre de la sécurité des télécommunications.
- h. *Trends in Wireless Technology and Security – A Market Research Study* (ITSPSR-20), octobre 2002, Centre de la sécurité des télécommunications.