Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

CAN-US Security-Enhanced BlackBerry Trial

Concept Document

Mazda Salmanian and Matthew Kellet

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2004-181
September 2004

Canada

CAN-US Security-Enhanced BlackBerry Trial

Concept Document

Mazda Salmanian
Matthew Kellett
Defence R&D Canada – Ottawa

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2004-181

September 2004

Abstract

This report develops the concept for a trial of a secure wireless network for the public safety, emergency preparedness, and law enforcement communities in Canada and the US. Recent advances in the security of wireless technology have made it possible for wireless devices to be considered for inter-governmental communications. This will speed up the response time of decision makers on both sides of the border for domestic security and emergency management events. Research done during the trial is expected to help to guide future effort for a classified solution that will be suitable for military use.

This proposal is based on available commercial off-the-shelf (COTS) technology with a Communication Security Establishment (CSE)/National Security Agency (NSA)-developed security overlay. It seeks to integrate Research in Motion's (RIM) BlackBerry handheld wireless device with the joint CSE/NSA secure e-mail solution on a larger scale than previous implementations. The trial also seeks to supplement the BlackBerry's paging and cellular communications capability with the addition of satellite communications. This will add redundancy in areas with paging or cellular coverage and otherwise extend coverage throughout North America and out beyond the coasts.

This paper defines the objectives of the trial and the benefits generated by the trial for participating agencies such as Public Safety and Emergency Preparedness Canada (PSEPC) and the United States' Department of Homeland Security (DHS). The paper identifies some initial areas of research interest, and the various phases the trial is expected to go through. Some consideration is given to questions that might arise during the implementation of the trial infrastructure and a preliminary roadmap for the development of that infrastructure is presented. We attempt to present a convincing argument for the participation of other government agencies from both sides of the border in the trial.

Résumé

Ce rapport développe le concept pour une épreuve d'un réseau sans fil sécurisé pour l'agence de Sécurité Publique et Protection Civile Canadienne, ainsi que les organismes qui sont responsables des Services de Police et d'Application de la Loi au Canada et aux États-Unis. Les avances récentes dans la sécurité de la technologie sans fil ont permis pour que les dispositifs sans fil soient considères pour des communications inter-gouvernementales.

Ceci accélérera le temps de réponse des deux côtés de la frontière aux événements domestiques pour la gestion de sécurité et de secours. La recherche faite pendant l'épreuve aidera à contribuer dans le futur effort pour le développement d'une solution classifiée qui conviendra aux entités militaires. Cette proposition est basée sur la technologie des logiciels commerciaux et gouvernementaux. Elle cherche à intégrer la recherche déjà faite sur le dispositif sans fil de Research In Motion, notamment le produit Blackberry, avec le Centre de la Sécurité des Télécommunications (CST) et l'Agence de Sécurité Nationale américaine sur une plus grande échelle que les réalisations précédentes.

L'épreuve cherche également à ajouter a l’aspect pagette et cellulaire du Blackberry avec l'addition de communications par satellite. Ceci ajoutera de la redondance dans les secteurs qui sont déjà couverts par les réseaux cellulaires et pagettes dans l'ensemble de l'Amérique du Nord et au-delà des côtes maritimes. Cet article présente les objectifs de l'épreuve, les avantages aux agences qui participerons, notamment le Département Américain pour la Defence du Territoire National et l’agence de Sécurité Publique et Protection Civile Canadienne ainsi que quelques sujets de recherche a intérêts initials et les phases variées dont l’épreuve couvrira. Une certaine attention aux questions qui pourraient faire surface en ce qui est de l’infrastructure et une carte routière préliminaire pour le développement de l'infrastructure d'essai y est présentée. Cet article se tente de présenter un argument persuasif pour la participation dans l’épreuve d'autres organismes gouvernementaux des deux côtés de la frontière.

This page intentionally left blank.

Executive summary

The secure use of mobile devices for wireless messaging is a Department of National Defence (DND)/ Canadian Forces (CF) requirement. In recent years, there has been a widespread use of BlackBerry devices by DND employees, both civilian and military. This triggered DND to deploy a pilot network, secured to Protected A, so that participants could have secure, remote access to their Defence Wide Area Network (DWAN) e-mail. The BlackBerry devices have simplified access to e-mail messages, are not as intrusive as cell phones, and have effectively enabled faster decision-making. The Canadian Communications Security Establishment (CSE) and the United States (US) National Security Agency (NSA) have also piloted BlackBerry messaging networks. Their networks are approved to Protected B through end-to-end public key infrastructure (PKI) encryption.

This report develops the concept for a trial of the CSE/NSA Protected B PKI solution for the public safety, emergency preparedness, and law enforcement communities in Canada and the US. Research done during the trial is expected to help to guide future research for a classified solution that will be suitable for military applications. The deployment of the CSE/NSA BlackBerry solution will be on a larger scale than previous implementations. We will also supplement the BlackBerry's paging and cellular communications capability with the addition of satellite communications. This will add redundancy in areas with paging or cellular coverage and otherwise extend coverage throughout North America and beyond the coasts.

This paper defines the objectives of the trial and the benefits generated by the trial for participating agencies such as Public Safety and Emergency Preparedness Canada (PSEPC) and the United States' Department of Homeland Security (DHS). The paper identifies some initial areas of research interest, and the various phases the trial is expected to go through. Some consideration is given to questions that might arise during the implementation of the trial infrastructure and a preliminary roadmap for the development of that infrastructure is presented. We attempt to present a convincing argument for the participation of other government agencies from both sides of the border in the trial.

Salmanian, M. and Kellett, M. 2004. CAN-US Security-Enhanced BlackBerry Trial: Concept Document. DRDC Ottawa TM 2004-181, Defence R&D Canada - Ottawa.

Sommaire

L'utilisation sécurisée des dispositifs mobiles pour la transmission de messages sans fil est un besoin essentiel pour le Ministère de la défense nationale (MDN), ainsi que pour les Forces Canadiennes (FC). Ces dernières années, il y a eu une utilisation répandue du produit Blackberry (par Research In Motion) par les employés du MDN, civils et militaires. Ceci a déclenché le besoin pour le déploiement d'un réseau pilote au niveau "protégé A", a faire de sorte que les participants peuvent avoir un accès sécurisé à leur courriel sur le réseau étendu de la défense.

Les dispositifs Blackberry ont simplifié l'accès au courriel et ne sont pas autant disruptifs que les téléphones cellulaires, et offrent efficacement la possibilité de prendre des décisions plus rapidement. Le CST et l'ASN des États-Unis ont également piloté des réseaux de transmission de messages de Blackberry. Leurs réseaux sont fixés à "protégé B" avec infrastructure a clé publique chiffree de bout à bout. Ce rapport développe le concept pour une épreuve de la solution "protégé B" par le CST/ASN pour l'agence de Sécurité Publique et Protection Civile Canadienne, ainsi que les organismes qui sont responsables des Services de Police et d'Application de la Loi au Canada et aux États-Unis.

L'épreuve cherche également à ajouter a l'aspect pagette et cellulaire du BlackBerry avec l'addition de communications par satellite. Ceci ajoutera une redondance dans les secteurs qui sont déjà couverts par les réseaux cellulaires et pagettes dans l'ensemble de l'Amérique du Nord et au-delà des côtes maritimes. Cet article présente les objectifs de l'épreuve, les avantages aux agences qui participerons, notamment le Département Américain pour la Defence du Territoire National et l'agence de Sécurité Publique et Protection Civile Canadienne ainsi que quelques sujets de recherche a intérêts initials et les phases variées dont l'épreuve couvrera. Une certaine attention aux questions qui pourraient faire surface en ce qui est de l'infrastructure et une carte routière préliminaire pour le développement de cet infrastructure d'essai y sont présentées. Cet article tente de présenter un argument persuasif pour la participation dans l'épreuve d'autres organismes gouvernementaux des deux côtés de la frontière.

Salmanian, M. and Kellett, M. 2004. CAN-US Security-Enhanced BlackBerry Trial: Concept Document. DRDC Ottawa TM 2004-181, R & D pour la défense Canada - Ottawa.

Table of contents

List of figures

List of tables

Acknowledgements

We would like to thank the RCMP IT Infrastructure Group for their financial support during the planning of this project. We would like to especially thank Donald Montreuil for his hard work in managing our contacts with Mobile Satellite Ventures and the local commercial wireless providers, and for translating the abstract and executive summary of this document.

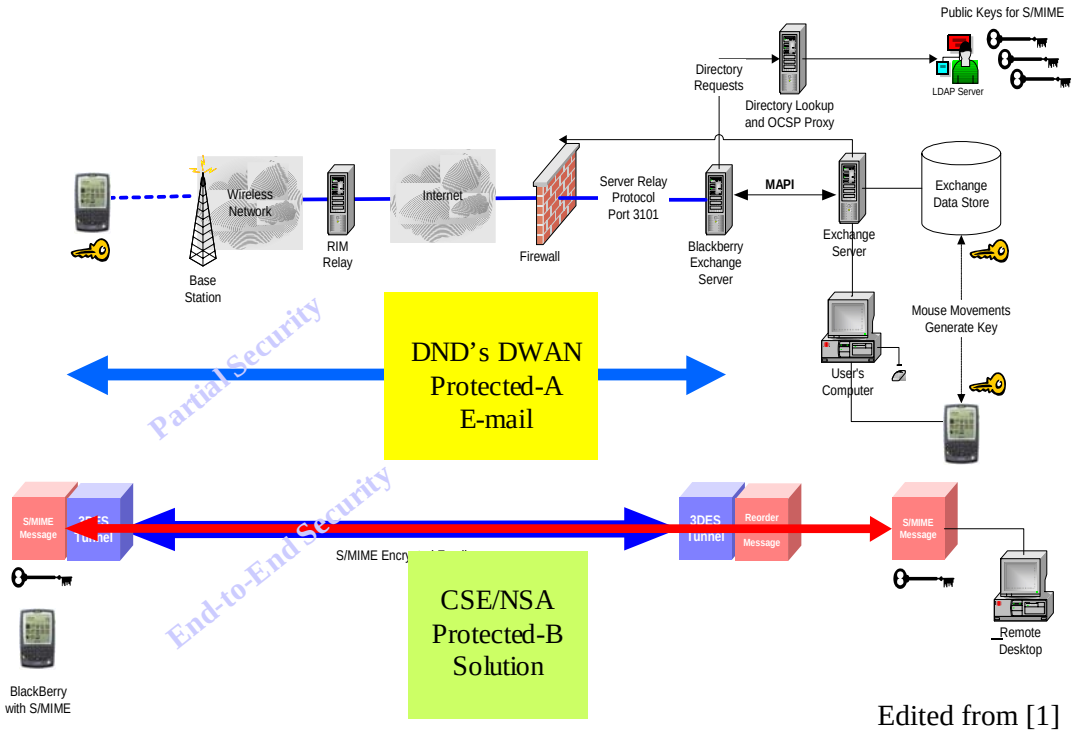
This page intentionally left blank.

1. Introduction

Recent advances in the security of wireless devices have made it possible to consider using them for public safety, emergency preparedness, and law enforcement applications. Defence R&D Canada (DRDC) proposes the design and demonstration of a pilot secure wireless network in Canada and the United States (US). This proposal was recently discussed as a potential "quick-hit" project under the joint Canada-US Public Safety Technical Program (PSTP). The proposed network will use commercial off-the-shelf (COTS) devices along with a secure e-mail solution that has been jointly developed by Canada's Communication Security Establishment (CSE) and the US's National Security Agency (NSA). The goal is to develop technical and policy solutions for a CAN-US prototype security architecture that can be overlaid on commercial communication networks, with the hope of moving this technology towards a solution at the classified level for national security and military applications.

The proposed shared network will allow decision makers on both sides of the border access to a single wireless standard and device for secure e-mail and secure text messaging. This solution demonstrates the secure use of public networks by governments to improve the transfer of critical information and speed up decision-making. DRDC proposes the use of Research in Motion's (RIM) BlackBerry, a wireless handheld e-mail client and personal digital assistant that works on both the paging and cellular networks (see Appendix A for more information on the BlackBerry's use of cellular and paging networks). The BlackBerry is currently being piloted by the Canadian military for connection to their designated network, the Defence Wide Area Network (DWAN), at the Protected A level. The implementation provides shared-key encryption between the handset and the BlackBerry Enterprise Server (BES) on the inside of the trusted network. The CSE/NSA solution adds the public key infrastructure (PKI)-enabled encryption of e-mail messages from sender to receiver on top of the already encrypted handset/BES connection. The PKI solution has been rated at the Protected B level.

The proposed network will be the first large-scale collaborative implementation of the Protected B solution. Research using the network will look at several key areas: usability, cross-border PKIs, and alternative technologies. Solutions that are difficult to use are not likely to gain user acceptance. The non-technical users involved in the trial will be able to point out problems that technical users may not notice. In order to set-up a cross-border PKI, the trial may require cross-certification of existing certificate authorities or the creation of a new authority. New and emerging alternative technologies may solve existing problems or provide enhancements to the technology being used.



Edited from [1]

Figure 1: Secure BlackBerry enterprise system

We recognize that the cellular and paging networks in both countries do not have the coverage or redundancy required to serve the full range of public safety, emergency preparedness, and law enforcement concerns. DRDC proposes the extension of coverage by integrating the BlackBerry with Mobile Satellite Venture's (MSV) network to provide full intra-continental and coastal coverage. This will enhance the network's availability and/or reliability by offering diverse means for connecting to the network.

With this paper, we attempt to present a convincing argument for the participation of other government agencies from both sides of the border in the trial.

Following this Introduction, Section 2 provides more detail on BlackBerry networks in Canada and the United States. A summary of the trial objectives, benefits, and constraints is presented in Section 3. Section 4 identifies the questions that are of initial research interest. The various phases of the trial are outlined in Section 5. Section 6 briefly examines trial security, while Section 7 deals with the various options that an installation will have and outlines DRDC Ottawa's choices. The report concludes with a brief summary in Section 8.

2. Objectives

2.1 Objectives

The main objective of this trial is *to demonstrate the use of security-enhanced wireless handheld devices on commercial wireless networks for real-world situations*.

A number of secondary objectives are integral to achieving this objective. They are to

1. Demonstrate the use of PKI over commercial wireless networks
2. Research and test emerging technologies
3. Add communication channel redundancy and extend coverage
4. Support collaboration (interdepartmental, bilateral)
5. Facilitate the transition to an operational network

In order to achieve these objectives, the project is broken into a number of overlapping phases and steps as set out in Section 4. In the following sections, we will take a closer look at the secondary objectives and how they contribute to the main objective.

2.1.1 Demonstrate the use of PKI over commercial wireless networks

PKI is a well-known, well-researched, widely used security technology. It is also the basis for the CSE/NSA S/MIME BlackBerry solution and is, therefore, a natural starting point for the trial. By looking more closely at how the S/MIME solution works in real-world situations, especially by putting the solution into the hands of non-technical users, we can focus on how to improve the application of security without compromising usability and, as a consequence, user acceptance. The newness of this technology allows us the unique opportunity to incorporate security at the earliest stages of user acceptance and make it part of the culture of the users using this technology.

PKI brings with it many technological and policy challenges that need to be overcome in order to seamlessly connect users between departments and between national governments. Possible solutions for the use of PKI in the trial include the manual exchange of certificates, the cross-certification of central authorities (a very involved process), or the creation of a new central authority. Like usability, finding solutions to these challenges will be a major focus of the trial and will be the work of Steps 1 through 3 of Phase 2. The use of PKI on commercial wireless networks is similar to work by of one of our colleagues who demonstrated its use over the Internet and has dealt with similar problems [1].

2.1.2 Research and test emerging technologies

As was noted in the previous section, PKI presents many technological and policy challenges. Technologies have emerged recently that address these problems. Other technologies can be used to enhance the security of other parts of the wireless solution. In Step 4 of Phase 2, we will investigate technologies such as identity-based encryption (IBE), which offers services similar to PKI but with less infrastructure and policy overhead. Usability in this context is not just about how easy it is for one user to send an encrypted message to another but also how much trouble it is to get both users registered with the system. IBE offers the possibility of reducing the complexity of managing users and therefore increasing the overall usability of the wireless solution. We will look closely at these and other technologies to see if they truly offer a better solution without compromising security.

2.1.3 Add communication channel redundancy and extend coverage

In general, commercial wireless networks, such as cellular and paging networks, do not provide wireless access redundancy. The base station is a single point of failure in the wireless portion of the communications path. Even where multiple networks exist, wireless handheld devices are physically limited to connecting to only one of those networks. In Phase 3 of the trial, we propose to add redundancy to the wireless portion of the communications path by adding a satellite communications capability to the wireless handheld device. This will provide redundancy in areas covered by commercial wireless networks and extend coverage to areas without such services.

2.1.4 Support collaboration (interdepartmental, bilateral)

An important part of the main objective is demonstrating this solution in “real-world situations.” We propose to do so by supporting the Public Safety Technology Program (PSTP). By supporting collaboration between essentially non-technical PSTP principals on both sides of the border, we will create these real-world situations. The PSTP program offers us the chance to use the technology in these situations without creating the expectation that the system will perform at operational levels.

2.1.5 Facilitate the transition to an operational network

Any solution that comes out of the trial requires institutional acceptance as well as user acceptance. The easiest way to achieve this is by making the transition from a research implementation of the technology to an operational implementation as seamless as possible. Given equally weighted choices, we propose to choose the one that better supports the eventual handover to corporate control. The intention is to create the system least objectionable to institutional information technology managers and, therefore, to gain earlier acceptance than a system merely designed as a prototype.

2.2 Participating agency benefits

In return for sharing the costs of the trial with DRDC Ottawa, the participating agencies will benefit from the

1. Results of the research. The results of all trial research will be shared amongst the participating agencies.

2. Creation of an interdepartmental and bilateral communications channel. The trial will encourage interdepartmental and bilateral communications amongst the public safety, emergency preparedness, and law enforcement communities.

3. Development of a secure, wireless handheld capability. The participating agencies will be developing a secure, wireless handheld capability that can be handed over to corporate control at the end of the trial.

4. Development of a platform on which to test new and emerging technologies.

2.3 Constraints

In order to keep the trial manageable and the research results relevant, we propose a number of constraints on the trial.

Duration: With the testing of new and emerging technologies, this trial runs the risk of continuing indefinitely. Limits for individual phases and steps are discussed in Section 4, however, for the trial as a whole, we suggest that it be closely scrutinized if it looks likely to continue past the end of FY2005-2006 (March 31, 2006).

Reliability: This is a research network and will be inherently unreliable. This will not be suitable for use in an operational situation.

Number of installations: The number of installations should be kept to a manageable level. This will be decided by agreement amongst the participating agencies.

Participants per installation: In order to keep local installations manageable, installations should have an average of 10 users with a maximum of 20.

Trial technical support: Overall trial technical support from DRDC Ottawa will be generally available to local installation support personnel during regular business hours.

Installation technical support: Each installation will be responsible for providing its own technical support personnel.

3. Initial research interests

The research interests of the trial will initially focus on six areas: user control, usability, usage, policy, quality of service and scalability, and application of solution. For each area, a series of questions is provided along with an estimate of which source of information will be most likely to provide the answer. The questions are marked (System) for those that can be answered by modifying the infrastructure directly, (User) for those that require user feedback, and (Analysis) for those that require further analysis of data collected during the trial.

This is intended not as an exhaustive list but as a starting point for investigation and discussion. Further questions or other areas of interest may become apparent during the trial and will be incorporated as appropriate.

3.1 User control

1. How does a participant find the public key for an external secure e-mail recipient? (System)(User)

2. How does a participant know that they can trust any given public key? (System)(User)

3. How often should revocation lists be updated and checked? (System)

4. Can the user be notified of a delay in delivery? Can the user have the option to remove the delayed e-mail from the queue? (System)

5. Can secure messages have a different time-to-live than normal messages? Is it possible for this to be under user control? (System)(User)

6. Is there any limitation (legal, technical, or diplomatic) to the use of secure e-mail outside North America, especially in Europe? (System)(User)

7. Is there a practical limitation imposed by the device, communications path, or supporting infrastructure on the number of recipients that can be included in a secure e-mail transmission (i.e., broadcast messages)? (System)(User)

3.2 Usability

1. How often do trial participants need to use secure wireless messaging immediately as opposed to returning to their offices and using their desktop systems? Are we providing a convenience or a necessity? (User)

2. Is authenticating with the device a hindrance to its use? (User)

3.3 Usage

1. What is the distribution of secure versus insecure messages? (User)(Analysis)

2. How often does a user have to authenticate with the device? (User)(Analysis)

3.4 Policy

1. How long can a BlackBerry stay unauthenticated before it should be deactivated? (Analysis)

2. Is cradling sufficient to act as a form of authentication? (Analysis)

3. Is it possible to enforce security by policy? What policies are necessary/sufficient for the security of enterprise wireless networks? (System)(Analysis)

4. Is position-based policy possible (can GPS be easily integrated)? Can it be enforced? What is a suitable policy? (System)(Analysis)

3.5 Quality of service and scalability

1. This system is based on the enterprise model, which is inherently limited in size. What and where are the constraints on system scalability in cellular or SATCOM networks? (System)

2. Can read and delivery receipts be enforced for secure messages? Can they also be secured? (System)

3. How well supported is quality of service (QoS) on the Internet? Can it be used to decrease the transit time for time-sensitive messages? Can QoS be exploited for security advantages? (System)

4. Is there an effect from the SATCOM QoS on secured versus unsecured data or voice quality? (Analysis)

5. The transfer to satellite communication (SATCOM) will be done manually by the user cradling the BlackBerry for system access. Can the cradle be miniaturized and the transfer to SATCOM automated for certain vehicular applications based on signal strength? (System)

3.6 Application of solution

1. What are the requirements for the military's use of a designated handheld solution at the tactical, operational, and strategic level? What are the requirements for a designated handheld solution in tactical-level foreign urban operations? (Analysis)

2. Can identity-based encryption (IBE) improve interdepartmental or bilateral collaborations by avoiding the need for cross-certification? Do other problems exist? Are distributed security models, as opposed to centralized, more suited for such wireless applications? (System)(User)

3. How does PGP compare to PKI or IBE in the wireless environment? (System)(User)

4. Are the current threat assessments on both the secured and unsecured BlackBerry valid? (System)(Analysis)

4. Phases

The trial will comprise three overlapping phases. The first phase involves a review of relevant literature to plan for Phase 2 and to answer questions that arise during Phase 2. The second phase involves the implementation, deployment, and testing of the trial infrastructure. The third phase, which begins towards the end of Phase 2, will extend the redundancy and range of the trial infrastructure.

A detailed work breakdown structure for the trial and each phase can be found in Appendix B. An estimated cost can be found in Appendix C. A materials list for DRDC Ottawa's installation is included in Appendix D.

4.1 Phase 1: Security analysis

Phase 1 involves a review of relevant literature to provide information needed to plan for Phase 2. Of particular interest is the difference between identity-based encryption and public key encryption. Phase 1 will continue to provide background information throughout the trial for questions that arise during the subsequent phases.

4.2 Phase 2: Installation and interconnection

Phase 2 involves the implementation, deployment, and testing of the infrastructure needed to test the secure use of wireless handheld devices over commercial wireless networks. The infrastructure will comprise a number of installations that will be brought up using the four steps outlined below.

At least three installations are currently being planned: one at DRDC Ottawa, and two at the Department of Homeland Security (DHS). DRDC Ottawa will bring up its installation first and pass its lessons learned on to the other installations.

4.2.1 Step 1: Installation and testing by technical staff

Step 1 involves local technical staff installing and configuring the local trial infrastructure. This is the initial assessment period where the local staff get comfortable with the technology and iron out any problems before the BlackBerrys are deployed to local participants.

This step is successful when local technical staff is able to send and receive secure e-mail from a test account associated with a locally connected BlackBerry.

4.2.2 Step 2: Deployment to local participants

Step 2 involves the deployment of the BlackBerrys to the local participants. BlackBerrys should be deployed incrementally to local participants, starting with the technical personnel involved in the trial. An incremental rollout will ensure that bugs are worked out of the

system before higher-level participants are affected. All participants should have access to their live mailboxes.

This step is successful when a local participant is able to send a secure e-mail to all other local participants and receive a secure reply from each.

4.2.3 Step 3: Interconnection with existing installations

Step 3 involves the interconnection of installations, which can only be done once installations have completed Step 2. The interconnection involves the exchanging of keys between participants at different installations. Initially this will be done manually, but it may eventually involve the cross-certification of CAs or the creation of a new CA solely for the purpose of the trial. This step will be the longest in the PKI testing portion of the trial. User interviews will take place at the end of this step before moving on to the investigation of alternative technologies in Step 4.

Two installations are successfully connected when a local participant at one can send a secure e-mail to a local participant at the other and receive a secure reply.

Research at this step will be complete when a number of criteria are met:

1. Research questions applicable at this step have been looked at
2. Users have had sufficient time using the technology to give useful feedback
3. Usability has been fine-tuned
4. A solution or solutions have been found the PKI interconnection problem

4.2.4 Step 4: Investigation of alternative technologies

Once the PKI portion of testing is finished, the infrastructure can be used to test alternative technologies. This will give a chance to the participating agencies to set up and run tests on technologies of interest to them. Identity-based encryption is already an area of interest for many of the participating agencies. Not all agencies need be involved in every test of alternative technology but the results of the research must be shared among all participating agencies.

Research on any new or emerging technology will follow a plan proposed by one of the participating agencies and agreed to by the other agencies interested in the technology. The plan will specify research and testing steps and the criteria for judging completion.

4.3 Phase 3: Satellite extension

As noted in the objectives, the addition of redundancy and the extension of coverage for wireless handheld devices are very important for public safety, emergency preparedness, and law enforcement applications. Phase 3 involves extending the BlackBerry's reliability and range by adding the ability to use satellite communications. Planning and implementation for this phase will take place towards the middle and end of Phase 2.

This phase is successful when it is possible to send a secure e-mail from a geographic location that does not have cellular or paging coverage and receive a secure reply. See Appendix E for a more detailed discussion of the proposed solution.

Research at this phase will be complete when the research questions regarding the satellite extension of wireless coverage have been answered and the viability of the solution has been tested.

5. Security considerations

Real-life security threats must be taken into consideration for the trial infrastructure. This section is a limited analysis of the real-world threats to the trial infrastructure and proposed responses.

5.1 Trial security level

All communications over the trial infrastructure shall be at the UNCLASSIFIED level. The trial is interested in all aspects of security at the designated or for official use only (FOUO) (US) level. The results of the research will be used to make recommendations on a possible classified solution.

5.2 Handheld

Electro-magnetic emissions: EM emissions are only a concern for the classified level and will not be taken into consideration for this trial.

Theft or loss: In order to avoid compromising the trial infrastructure due to the theft or loss of a handheld, all handhelds shall be password protected. All local participants should be instructed on whom to contact in such cases. Local technical staff should block access from handhelds reported missing and, if possible, disable them remotely. Finally, local technical staff should block access from any handheld that is acting erratically or suspiciously, while trying to contact the owner.

Insider (Malicious user): All local participants are assumed trusted for purposes of the trial, although the insider threat may be a focus of research. The existing barriers in the system should defend against accidental compromise of the trial infrastructure.

5.3 E-mail (data) in transit

All secure e-mail sent in the trial is assumed to travel between two installations or within an installation.

Traversing the Internet between installations: Due to the possible sensitive nature of some of the unclassified data being transferred, all e-mail that must traverse the Internet to reach the destination installation shall be secured. See Figure 2.

Traversing a shared network between installations: If both installations agree that the shared network is trusted and there is no possibility of the e-mail leaving the trusted network then e-mail may be sent unsecured. See Figure 2.

Traversing an installation's network: Local e-mail between local participants may be sent unsecured.

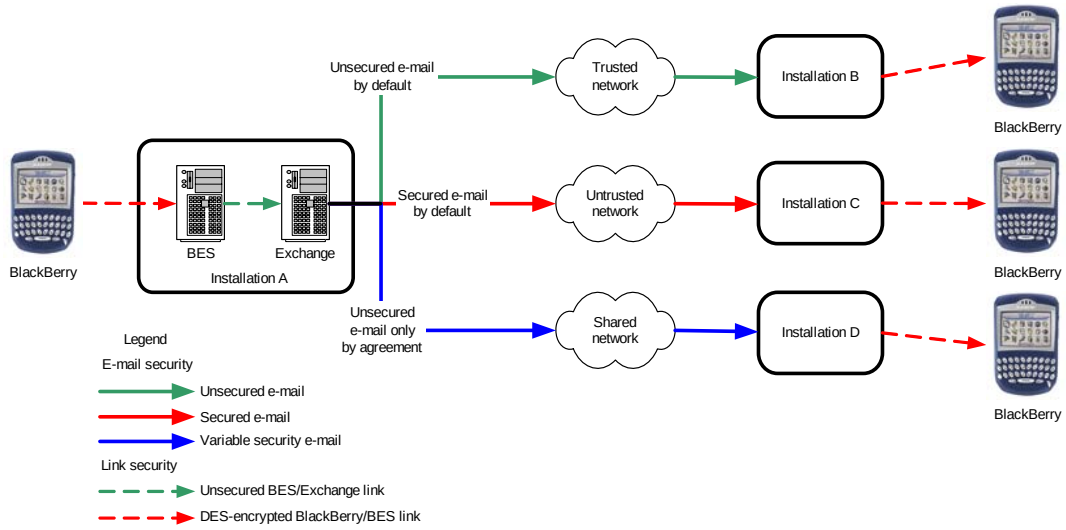


Figure 2: Security considerations for e-mail in transit (e-mail security)

Traversing from the handheld to the BES: The handheld/BES connection is 3DES-encrypted. The supporting infrastructure – handheld to base station (over the air), base station to network operations centre (over the Internet) and network operations centre to BES (over the Internet) – is assumed not to be a threat for this reason. See Figure 3.

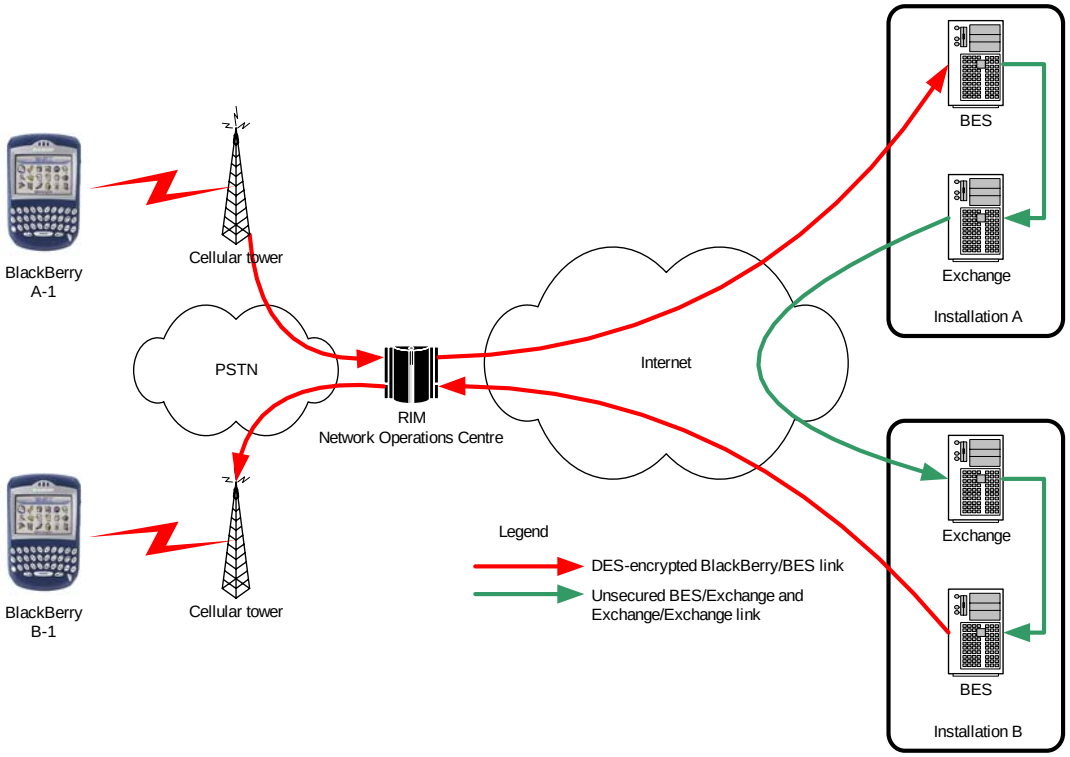


Figure 3: Security considerations for e-mail in transit (link security)

5.4 Voice in transit

Voice communications are not secured and shall not be of a sensitive nature.

5.5 Local infrastructure

Insider (Malicious technical staff): Local technical staff is assumed trusted.

Physical security: The trial infrastructure should be co-located in a limited access area with or near the corporate infrastructure to which it will be connecting (i.e. Exchange server or firewall).

6. Installation considerations

The choice of infrastructure should have little impact on the trial's research interests, which focus on secure network interactions instead of physical layer considerations. Other partners are free to choose the best network providers for their location and the best handheld options for their target audience. DRDC Ottawa's choices are discussed below.

Installations must also deal with the selection of participants. Appendix F contains DRDC Ottawa's participant selection criteria and a proposed acceptable usage policy.

6.1 Commercial network

As is discussed in Appendix A, there are three commercial wireless networks in North America: CDMA-1x, GSM/GPRS, and Mobitex. The BlackBerry started out on the Mobitex paging network but has since moved onto cellular networks, which offer higher bandwidth and the ability to add voice to the device.

DRDC Ottawa has chosen the cellular version over the paging version of the BlackBerry. The paging network has less efficient traffic management than the cellular network and, as mentioned above, does not provide a voice capability. RIM is only now updating its earlier paging network offerings, having focussed recently on advancing the cellular version of the BlackBerry. RIM's current product lines heavily favour the cellular networks.

Of the two cellular networks, DRDC Ottawa has chosen the GSM/GPRS network. This network does not have as good coverage in North America as the CDMA-1x network but does provide better overall global access. More importantly, GSM is the focus of CSE's efforts into securing voice and DRDC Ottawa intends to keep its options open if a secure voice solution becomes available during the trial.

6.2 Voice

Voice is an optional service, with a small additional fee, on cellular network versions of the BlackBerry. DRDC Ottawa has decided to enable voice for its BlackBerrys. There is likely to be a strong push towards a voice-capable version in any operational version of the secure BlackBerry. Despite voice not being secured, its use will still have an impact on the transfer of secured data, especially its timing. This may be important for the manual authentication of the exchange of public keys, where two users are able to talk to each other immediately before sending their keys via e-mail. To avoid any extraordinary expenses from voice usage, DRDC Ottawa has developed an acceptable use policy, outlined in Appendix F, that makes additional minute, long distance, and roaming charges the responsibility of the user.

6.3 Display (Colour/B&W)

There is some concern that battery life and therefore usability will be limited with the use of colour displays on the BlackBerry. However, DRDC Ottawa has chosen to go with colour displays for the following reasons:

RIM held back introducing colour displays until it had developed a battery that could provide battery life comparable to the B&W versions

Colour is likely to be a highly requested option especially among upper management

Most new models of the BlackBerry come with colour displays.

7. Conclusions

The trial is an excellent opportunity to create a culture of security around a popular new technology. We also have the chance to increase cross-border communication on public safety, emergency preparedness, and law enforcement, while at the same time tackling technological and policy barriers to the cross-border use of PKIs. The trial infrastructure will allow for the testing of new and emerging technologies that address some of the shortcomings of current technology. It will also give us the opportunity to address the shortcomings of commercial terrestrial communications by adding satellite communications to extend the range and/or provide redundancy to the wireless solution.

The CAN-US Security-Enhanced BlackBerry Trial offers the Public Safety Technology Program a way of demonstrating quick progress among authorities on both sides of the border. If successful, the trial will benefit both countries enormously. We hope that, in addition to Public Safety Emergency Preparedness Canada and the US Department of Homeland Security, other agencies will join us and contribute to making this trial a success.

8. References

1. Zeber, Dr. S., Kennedy, LCDR C., 2002. The NATO Entrust 2001 Trial. DRDC Ottawa TM 2002-036 DRDC Ottawa.

2. Richard MacLean, “GoC PKI and S/MIME V3 Enabled BlackBerry Wireless Solution”, Communication Security Establishment, September 16, 2002

3. http://www.rim.net/products/handhelds/index.shtml

4. http://www.blackberry.com

List of symbols/abbreviations/acronyms/initialisms

AP	Access Point (WLAN term)
APV	Armoured Personnel Vehicles
BER	Bit Error Rate
BES	BlackBerry Enterprise Server
BW	Bandwidth
CDMA	Code Division Multiple Access
CSE	Communication Security Establishment
CSMA	Carrier Sense Multiple Access
COTS	Commercial Off-The-Shelf
DDOS	Distributed Denial of Service
DND	Department of National Defence
DRDC	Defence R&D Canada
DWAN	Defence Wide Area Network
FDMA	Frequency Division Multiple Access
FNBDT	Future Narrow Band Digital Terminal
FOUO	For official use only (United States)
FSO	Free Space Optical
GEO	Geostationary Earth Orbit
GSM/GPRS	Global System Mobile / General Packet Radio Service
ISR	Intelligence Surveillance & Reconnaissance
ISP	Internet Service Provider

L2TP	Layer-2 Tunnelling Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
MANET	Mobile Ad hoc Networking
MSV	Mobile Satellite Ventures
MTBF	Mean Time Between Failure
NDHQ	National Defence Headquarters
NOC	Network Operations Centre
NSA	National Security Administration
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Data Assistant
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
PSTP	Public Safety Technology Program
QoS	Quality of Service
RIM	Research in Motion Limited
S-MANET	Secure Mobile Ad hoc Network
SATCOM	Satellite Communications
VHF	Very High Frequency
TDMA	Time Division Multiple Access
TNDHQ	Trans-National Defence Headquarters
TOCC	Trans-national Operational Command Centre
UAV	Unmanned Aerial Vehicle
UN	United Nations

UXV	Unmanned (aerial, marine, land, etc.) Vehicle
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

Appendix A: Cellular and Paging Background

The BlackBerry devices are widely used in Canada and the US. These devices appeal to civilian and military personnel because they offer simplified access to e-mail messaging, enabling faster decision-making. Moreover, they are, by design, not as interrupt intensive as cell phones. The devices are always connected to the e-mail server and the subscriber does not need to manually download his/her e-mails by dialling into an Internet Service Provider (ISP). The e-mails are "pushed" onto the device and the subscriber is discretely notified. Research in Motion (RIM) deploys the BlackBerry devices on paging and cellular networks.

The paging networks are the DataTAC network (800MHz) in the US and the Mobitex network (900MHz) deployed in the US and Canada. These paging networks are service providers and carriers for non-real-time data; they do not have voice switching capabilities. The BlackBerry paging network devices offer the following services: e-mail, paging, calendar, address book, task list, memo pad, calculator, and alarm [3]. The BlackBerrys operate on a C^{++}-based system and their model numbers correspond to the frequency bands in which they operate as follows:

BlackBerry 95X / Mobitex network (900MHz) - US and Canada - data only

BlackBerry 85X / DataTAC network (800MHz) - US - data only

The cellular networks are distributed on GSM/GPRS and CDMA2000 1X bands across Asia Pacific: Australia, Hong Kong, Singapore; Europe: Switzerland, United Kingdom, Austria, Germany, Italy, France, the Netherlands, Spain; and North America: Canada and the US. However, tri-band BlackBerrys operating on 850 or 900/1800/1900 MHz GSM/GPRS wireless networks allow international travellers to maintain connectivity in North America, Europe, and Asia Pacific.

In Canada, the GSM/GPRS network (850/900/1800/1900 MHz) provider is Rogers Wireless, and the CDMA2000 1X network (800/1900 MHz) providers are Bell Mobility and TELUS. In the US, AT&T Wireless, Cingular, and T-Mobile are the GSM/GPRS network providers and Verizon Wireless is the CDMA2000 1X network provider. In addition, Nextel in the US provides connectivity through the iDEN network.

Unlike the paging network, cellular networks have both voice and packet switching capabilities. Voice and data packets take separate paths from the Public Switching Telephone Network (PSTN) and the Internet to the base station and from the base station to the handheld devices. The GSM network is circuit-switched and carries voice while the GPRS feature allows for channel allocation/deallocation and routing of data packets to and from the mobile nodes in the network. Similarly, the CDMA2000 1X network also separates the circuit-switched voice path from those of packet-switched data path.

The list of services offered by cellular BlackBerrys is more impressive than those offered by their paging counterparts. The services include telephone, e-mail, Short Message Service (SMS), browser and organizer applications (calendar, address book, task list, memo pad,

calculator and alarm), colour displays supporting over 65,000 colours, available memory for additional applications, games, and data storage, and an open standards Java development platform [3].

Secure use of mobile devices for wireless messaging is a requirement for DND and the military and, as such, DND has deployed a pilot network (Protected A) based on both the paging and GSM/GPRS networks.

Appendix B: Preliminary Work Breakdown Structure

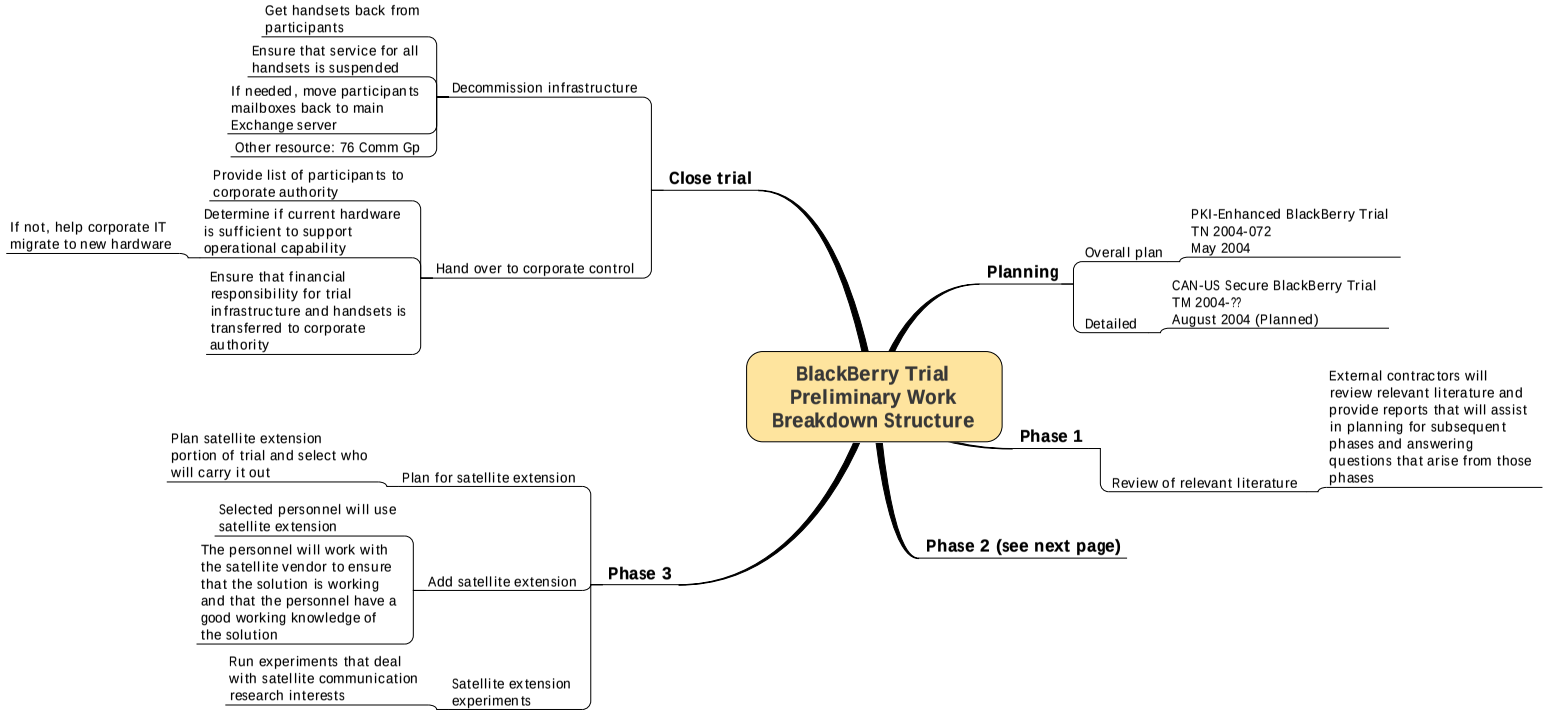


Figure 4: BlackBerry trial preliminary work breakdown structure

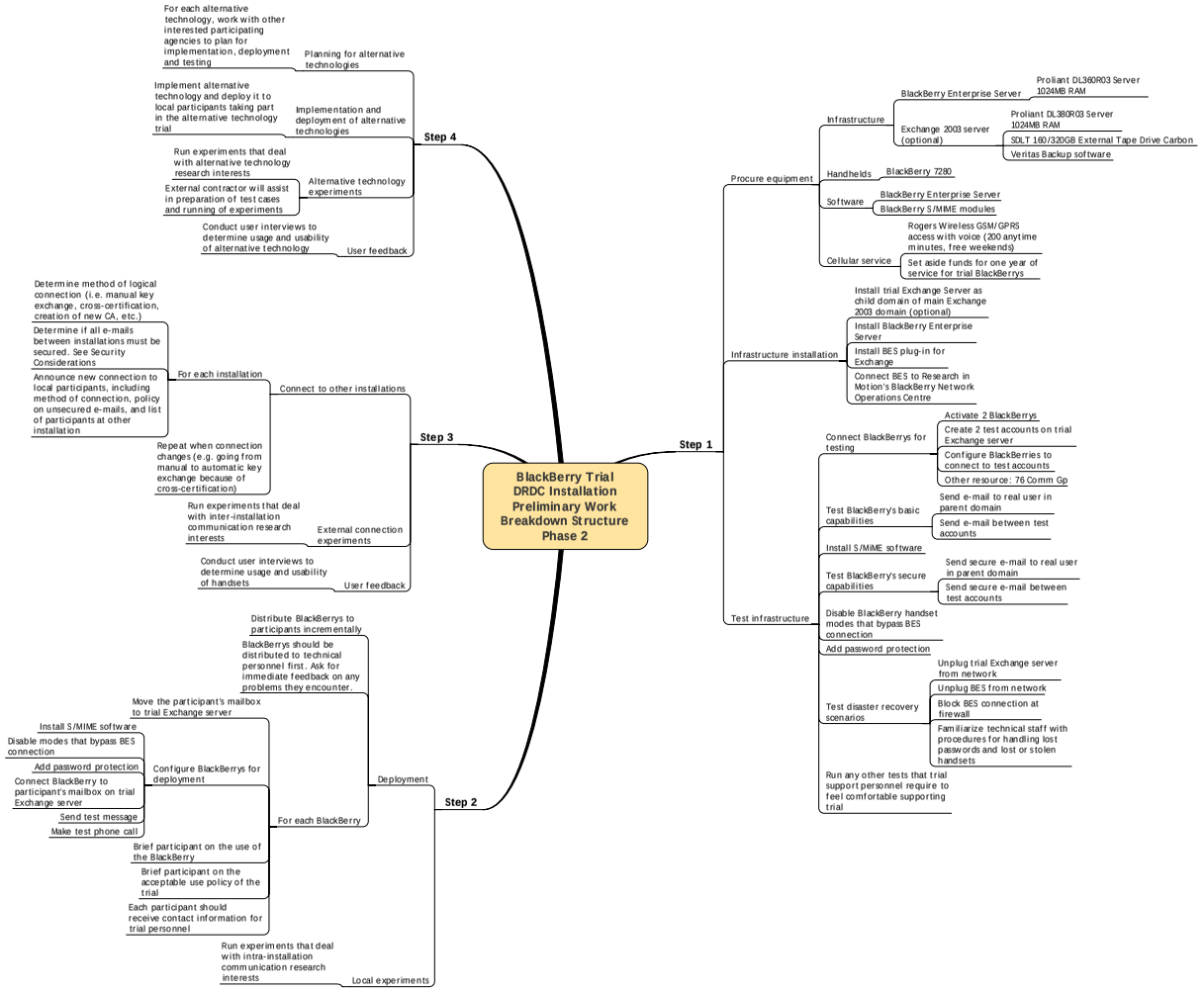


Figure 5: BlackBerry trial preliminary work breakdown structure (Phase 2)

Appendix C: Estimated Costs

A cookie cutter installation running for one year with 10 participants should cost

Project Management		
• Project definition	Fixed	$30,000
Implementation (using contractors)		
• Purchasing	Variable per participant	
• Deployment	Variable per participant	
• Connectivity	Variable per participant	
• Training	Variable per participant	$50,000
Scientific research		
• Experiments	Variable per Participant	
• Documentation	Variable per Participant	
• User Interviews	Variable per Participant	$50,000
Equipment		
• Hardware		$20,000
o BES	Variable per 20 Participants	
o Handsets	Variable per Participant	
• One year system access	Variable per Participant + Long distance and Roaming	$20,000
Total		$170,000

Table 1: Projected costs for 1-year, 10-participant cookie-cutter installation

Appendix D: Materials List

The following hardware, software, and services are being used for initial setup of DRDC Ottawa's installation.

BlackBerrys

1. BlackBerry

    1.1. (20x) Research in Motion (RIM) BlackBerry 7280

2. Software

    2.1. (20x) RIM S/MIME licenses

3. Service

    3.1. (20x) 1 year of service (GSM/GPRS)

        3.1.1. Data: Unlimited

        3.1.2. Voice: 200 anytime minutes

BlackBerry Enterprise Server

1. Server

    1.1. Proliant DL360R03 Server Xeon 2.8Ghz G3 1U Rackmount

    1.2. 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM MEMORY KIT

    1.3. (2x) 36GB 10K U320 Pluggable Hard Drive

2. Operating System

    2.1. Microsoft Windows 2003 Server

3. Software

    3.1. BlackBerry Enterprise Server Software v3.6 for Microsoft Exchange

4. Maintenance

    4.1. TX1 maintenance contract (1 year)

Exchange Server (optional)

1. Server

    1.1. Proliant DL380R03 Server 2.80Ghz-G3 (349201-001)

    1.2. Upgrade to 3 Year On-Site 24x7 4 Hour Response Enhanced Warranty (DL380/ML370)

    1.3. 1024MB of Advanced ECC PC2100 DDR SDRAM

    1.4. (4x) 36GB 10K U320 Pluggable Hard Drive

2. Operating system

    2.1. Microsoft Windows 2003 Server

3. Software

    3.1. Microsoft Exchange 2003

    3.2. Veritas Backup

        3.2.1. Veritas Backup Exec for Windows Servers (v9.1) license-1 server

        3.2.2. Veritas Backup Exec for Windows Servers Agent for MS Exchange Server (v9.1) 1 server

        3.2.3. Veritas Backup Exec for Windows Servers Intelligent Disaster Recovery Option (v9.1) license-1 server

        3.2.4. Veritas Backup Exec for Windows Servers Advanced Open File Option (v9.1) license-1 server

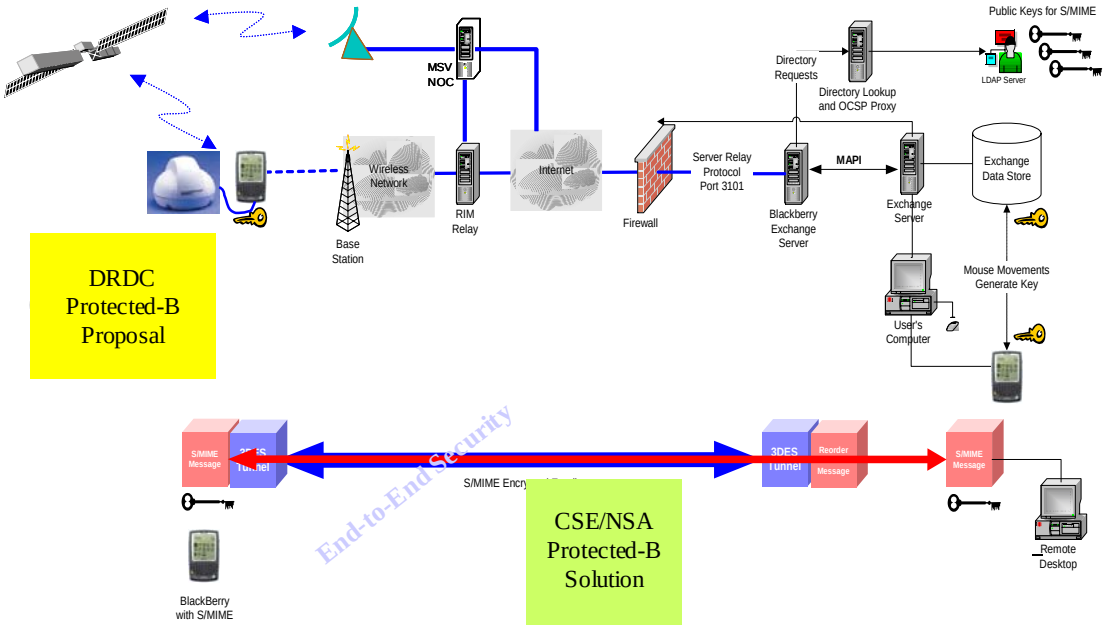
4. Tape Drive

    4.1. SDLT 160/360GB External Tape Drive Carbon

    4.2. (30x) SDLT Super DLT Tape 1 160/360GB

Appendix E: Phase 3 Network Diagram

Mobile Satellite Venture owns and operates two geostationary satellites with footprints covering North America, including 150 miles of each coast, Hawaii, Alaska, and the Caribbean. The company has demonstrated and deployed satellite network services for e-mail and text messaging for the New Mexico State Highway Patrol. MSV plans to offer terrestrial L-band spectrum by integrating its network with those of cellular providers. Their plan offers the cellular providers more spectrum and ubiquitous geographical radio coverage. The company's capabilities and radio coverage offer significant complements to those of cellular and paging networks for emergency management, communication, and coordination of local law enforcement, port authorities, border patrols, and first responders.



Edited from [1]

Figure 6: DRDC satellite extension concept

Phase 3 is to integrate MSV's network to work with BlackBerry devices, and to connect MSV's Network Operation Center (NOC) to RIM's NOC. In this phase, DRDC's pilot network will be expanded to have satellite coverage and partners on both sides of the border will have dual system access to the network. That is, in the event of a failure in the cellular network infrastructure, there will be independent satellite links for connectivity within North America.

The focus of research in this phase will be on the extent and quality of the additional coverage, the security of MSV's solution, and the exploration of other solutions.

Currently, there is only one NOC through which all North American BlackBerry messages are managed. A secure network must have sufficient redundancy in order to offer high quality of service - reliability and availability. Both MSV and RIM will be encouraged to duplicate their NOCs for load sharing and real-time (hot) stand-by transfer of network load. Their NOC duplications should be at different geographical locations. This duplication increases the reliability and availability of the network. This phase may also include testing and deployment of secure solutions that meet requirements of a Secret-level BlackBerry messaging network.

Appendix F: Local Participants

The choosing of local participants can be a politically charged process. To avoid this, DRDC Ottawa has developed selection criteria to make sure that local participants add to, rather than detract from, the trial. DRDC Ottawa has also developed an acceptable use policy to manage the expectations of the local participants and limit the potential abuse of the voice capability.

Selection criteria

Selection for participation in the trial will be based on the following (in order):

1. Technical expertise
2. Affiliation with Public Safety Technical Program (PSTP)
3. Ability to give feedback from a representative user group
4. Requirement to be available by e-mail but frequently away from their desktop computer

Acceptable use policy

Security level: The BlackBerry shall be used at the UNCLASSIFIED level only.

Personal use: Participants shall pay all charges related to their personal use of the BlackBerry assigned to them.

Long distance and other additional charges policy: The trial is responsible for all work-related data charges. The project is not responsible for additional voice charges.

Voice is included in the project for test purposes only. Participants that require the frequent use of wireless voice to fulfill their work duties should obtain a government cell phone.

Participants shall not make long distance phone calls. Participants shall not use voice roaming. Participants must not exceed the 200 anytime minutes included in the voice plan.

Network acceptable use policy: Participants are additionally bound by the acceptable use policy of the network to which they are connecting (e.g. DREnet). Where the trial acceptable use policy and the network acceptable use policy conflict, the more restrictive policy applies.

Enforcement: It is the participant's responsibility to ensure that these rules are not broken. Failure to comply with these rules will result in the participant being asked to leave the trial.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

CAN-US Security-Enhanced BlackBerry Trial: Concept Document

4. AUTHORS (Last name, first name, middle initial)

Salmanian, M., Kellett, M.

5. DATE OF PUBLICATION (month and year of publication of document)

August 2004

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

31

6b. NO. OF REFS (total cited in document)

4

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

5B36

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

N/A

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC Ottawa TM 2004-181

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

N/A

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

N/A

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This report develops the concept for a trial of a secure wireless network for the public safety, emergency preparedness, and law enforcement communities in Canada and the US. Recent advances in the security of wireless technology have made it possible for wireless devices to be considered for inter-governmental communications. This will speed up the response time of decision makers on both sides of the border for domestic security and emergency management events. Research done during the trial is expected to help to guide future effort for a classified solution that will be suitable for military use.

This proposal is based on available commercial off-the-shelf (COTS) technology with a Communication Security Establishment (CSE)/National Security Agency (NSA)-developed security overlay. It seeks to integrate Research in Motion's (RIM) BlackBerry handheld wireless device with the joint CSE/NSA secure e-mail solution on a larger scale than previous implementations. The trial also seeks to supplement the BlackBerry's paging and cellular communications capability with the addition of satellite communications. This will add redundancy in areas with paging or cellular coverage and otherwise extend coverage throughout North America and out beyond the coasts.

This paper defines the objectives of the trial and the benefits generated by the trial for participating agencies such as Public Safety and Emergency Preparedness Canada (PSEPC) and the United States' Department of Homeland Security (DHS). The paper identifies some initial areas of research interest, and the various phases the trial is expected to go through. Some consideration is given to questions that might arise during the implementation of the trial infrastructure and a preliminary roadmap for the development of that infrastructure is presented. We attempt to present a convincing argument for the participation of other government agencies from both sides of the border in the trial.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

PKI, encryption, network security, satellite communications, BlackBerry

Defence R&D Canada

Canada's leader in defence
and national security R&D

R & D pour la défense Canada

Chef de file au Canada en R & D
pour la défense et la sécurité nationale

www.drdc-rddc.gc.ca