National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Review of the DND Public Key Infrastructure

March 2005

7050-7-19 (CRS)



Canada

NOTICE OF CAVEAT TO THE READER

This review was conducted as part of the approved Branch Work Plan. The review conclusions do not have the weight of an audit and must not be regarded as such. While sufficient to enable the development of recommendations for consideration by management, the assessments provided, and conclusions rendered, are not based on the rigorous inquiry and evidence required of an audit.

SYNOPSIS

This report presents the results of a review of the Department of National Defence (DND) Public Key Infrastructure (PKI) system. PKI is an important supporting infrastructure to the secure exchange of sensitive electronic data and communications. DND has been operating an enterprise PKI since late 2002[1] and many new PKI-enabled applications are being planned on the assumption of existing, available and reliable PKI services. As part of its 2003/04 – 04/05 Work Plan, Chief Review Services (CRS), in partnership with AEPOS Technologies Corporation (AEPOS), conducted a review to assess the capability of the DND PKI to provide secure services to departmental users and applications.

The review focused on key aspects of the governance structures, policies, processes, resources and equipment that collectively support the management and operation of the DND PKI. Future departmental PKI applications, primarily the Military Message Handling System (MMHS) that is being rolled out in the classified domain[2], were also examined to assess their impact on the existing departmental PKI infrastructure support and processes. The scope did not include an assessment of the technical aspects of the Entrust® product or its selection as the Communications Security Establishment (CSE) approved mechanism for PKI.

Approximately 60,000 PKI smartcards were issued to DND employees and Canadian Forces (CF) members as part of the rollout of the current PKI system; over half of these cards have expired. Although pockets of users such as the Military Police, Finance and Human Resources, regularly employ PKI to protect sensitive e-mail messages, overall, PKI is not widely used within the Department. Further, many departmental employees are not sufficiently aware of the necessity to protect sensitive electronic information or that the technology is readily available on most workstations. Many of the issues raised in this review are not unique to the DND PKI – for example, the requirement to better define complete business requirements and to strengthen governance and horizontal processes, are systemic issues that have been identified in previous CRS reports of other departmental systems/projects. Management attention to resolve these issues is required before current users can fully rely on the PKI and before new PKI-enabled applications can be effectively supported. PKI is more than just a technology solution and needs to be managed in the context of DND/CF business and operational requirements.

Management action plans provided by ADM(IM) demonstrate constructive attention to the majority of recommendations contained in this report. At the same time, we encourage that certain actions be set in motion earlier than currently planned, particularly regarding the development of a DND PKI Roadmap, clarification of DND PKI roles and responsibilities, and rationalization of PKI infrastructure support and processes. In this respect, interim milestones for these action plans will be requested through CRS follow-up and monitoring processes.

[1] *The currently-installed PKI operates in the designated domain (i.e. the DND Intranet), which is intended for all general-purpose electronic data traffic.*
[2] *The classified domain is a separate DND network intended for classified electronic data traffic only. Classified information is defined as being reasonably expected to cause injury to the national interest and is categorized based on the degree of potential injury (i.e. Confidential, Secret, or Top Secret).*

TABLE OF CONTENTS

RESULTS IN BRIEF

INTRODUCTION

In today's economy, there is a wide reliance on and need for online communications and transactions. Individuals and organizations now routinely transmit sensitive and confidential data (such as commercial transactions, personal data and contracts) over unsecured public networks, particularly the Internet. In addition, organizations gather and store a wealth of sensitive electronic information assets that must be protected from unauthorized access or modification. Inherent in this type of environment are many risks related to information security. The importance of validating and verifying a party's identity and credentials prior to engaging in sensitive electronic communications and transactions is critical. A public key infrastructure (PKI)[3] is designed to meet these, and other challenges, by providing security services that enable risk mitigation in today's digital environment.

The Department of National Defence and the Canadian Forces (DND/CF) has been operating an enterprise PKI since late 2002 and many new PKI-enabled applications are being planned on the assumption of existing, available and reliable PKI services. As part of its 2004 Work Plan, Chief Review Services (CRS), in partnership with AEPOS Technologies Corporation (AEPOS), conducted a review to evaluate the capability of the DND PKI in providing secure and confidential services to departmental users and applications. Planning for the review commenced in March 2004, conduct was completed by August 2004, and results were debriefed in September/October 2004.

BACKGROUND

PKI Technology

A PKI is a system of hardware, software, policies, processes and people that can support a range of information security services designed to address the risks associated with processing sensitive electronic communications and transactions. Once a PKI has been implemented in an organization, many different applications (such as an email or messaging system) can use the infrastructure and the security services supported by the PKI.

The security services supported by a PKI are as follows:

- Authentication – which corroborates the identity of an individual, entity or device. Authentication is often considered the most important basic requirement to conduct business in an electronic environment – i.e. knowing who you are dealing with.
- Data Confidentiality – which protects information (in storage and during transmission) from unauthorized disclosure;

[3] A list of acronyms and abbreviations is provided at **Annex F**.

- Data Integrity – which protects information (in storage and during transmission) against unauthorized alteration; and
- Non-Repudiation – which protects against a party falsely denying having created, signed, originated or received a given document or transaction.

PKI is based on principles associated with public key cryptography. Users are assigned a unique key pair – a public key and a private (secret) key – to encrypt data or to create digital signatures. The PKI provides assurance that individuals are properly linked to their keys and that the links are constantly maintained, by using a trusted infrastructure to manage the keys and the related technology[4].

This trusted infrastructure is achieved by the policies, processes and people required to support the operation of a PKI. PKI policies and procedures[5] define the set of rules governing the use of certificates[6] as well as the processes to be followed for issuing, managing and revoking them. There is typically a requirement for periodic, independent compliance inspections to ensure that PKI policies and procedures are being rigorously applied and strictly followed. Trusted third parties, which operate both centrally and at the local/unit level, are also established to validate the credentials of individuals[7] requesting access to the PKI system. Furthermore, a PKI relies on having adequate resources to establish and maintain requisite processes as well as to maintain and operate the PKI system (i.e. hardware and software). Public key technology is relatively straightforward. It is the implementation of the "infrastructure" (i.e. policies, processes and people) that is generally considered the biggest challenge. Similar conclusions were reached by the United States (US) General Accounting Office (GAO) in its reviews of PKI implementations in federal departments and agencies[8].

Not all electronic information and communications need to be protected by security mechanisms such as PKI. The sensitivity of the data and an organization's security policy and business model should determine the IT security measures that warrant implementation.

PKI in the Government of Canada (GoC)

In recent years, the GoC has announced a number of objectives to improve operational efficiencies and reduce costs by conducting business electronically. Major GoC initiatives supporting electronic business and communications were also introduced at the 1999 session of the Canadian Parliament. The government (at the time) expressed its intention to, "-- become a model user of information

[4] A more detailed explanation of PKI technology and public key cryptography is provided at **Annex A**.
[5] PKI policies and procedures are known as the Certificate Policy (CP) and the Certification Practices Statement (CPS).
[6] Public keys (i.e. an individual's public encryption key and digital signature verification key) are normally published in the form of electronic 'certificates'. These certificates are published in a PKI directory along with information that attests to the validity of the keys. A PKI directory is similar to a telephone book.
[7] The evidence required and the actual process to be followed for validating the identity of individuals or entities depends on an organization's PKI policy.
[8] GAO-01-277: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. February 2001. GAO-04-157: Status of Federal PKI Activities at Major Federal Departments and Agencies. December 2003.

technology and the Internet" [9]. The "Government On-Line" (GoL) initiative embodies Canada's strategy to become the most "connected" nation in the world by providing citizens access to government information and services on-line, at their time and place of choice. To help accomplish its target, the GoC selected PKI as one of the core security technologies for the underlying GoL infrastructure in order to protect the privacy of information and transactions.

In addition to the GoC's goal for service improvement, several laws, policies and directives necessitate a secure electronic infrastructure for conducting government operations:

- The Personal Information Protection and Electronic Documents Act (PIPEDA) requires the protection of personal information of Canadians from unauthorized disclosure, and legally recognizes the use of a digital signature in legal transactions;
- The Treasury Board Secretariat (TBS) PKI Policy defines how a PKI system must be set-up and operated, in addition to stating that PKI is the preferred means of electronically authenticating the identity of individuals and of documents; and
- The TBS Electronic Authorization and Authentication (EAA) Policy requires all electronic business transactions to be digitally signed by a Communications Security Establishment (CSE) approved mechanism[10].

PKI in DND

PKI was initiated in DND as a research and security project in the 1994/95 timeframe. The original PKI Entrust® purchase was made in 1995 at a cost of $3M following a recommendation made by the Directorate of IT Security (DITSec). PKI essentially operated in a DND lab environment until the Secure Common Email (SCEM)[11] project began in 2000. SCEM was deployed to all desktops connected to the Defence Wide Area Network (DWAN) or the designated domain[12], as well as to all DND employees and CF members with a DND email address. With SCEM, sensitive information, up to and including Protected B[13] (PB) information, could be sent or stored electronically on the DWAN. By late 2002, approximately 60,000 PKI smartcards[14] had been issued at a cost of approximately $16M[15]. The SCEM project handed over operations to the DND/CF life cycle management teams in early 2003.

[9] "Speech from the Throne to Open the Second Session of the Thirty-Sixth Parliament of Canada." 12 October 1999. ISBN 0-662-64508-1.
[10] The only CSE approved mechanism for PKI and digital signature is that used in the Entrust® suite of products.
[11] SCEM was rolled out as part of the umbrella Defence Message Handling System (DMHS) project.
[12] The designated domain refers to the DND/CF Intranet that can process all general-purpose traffic, up to and including Protected A information, in the clear.
[13] Protected or designated information is a security classification used to identify and protect information that could reasonably be expected to cause injury to private interests. It is classified according to the degree of potential sensitivity (i.e. Protected A (low), Protected B (particularly) or Protected C (extremely)).
[14] In the DND, an individual's secret electronic credentials (i.e. private decryption key and private signing key) are held on a PKI smartcard. This PKI smartcard is physically required to access PKI-enabled applications. Not all organizations use smartcards for storing electronic credentials – other storage media exist.
[15] The $16M SCEM rollout cost was provided by the SCEM project team.

The main DND/CF life cycle management teams responsible for supporting the DND PKI are the Directorate of IM Security (Dir IM Secur) and the Directorate of Distributed Common Engineering and Integration (DDCEI). Dir IM Secur has overall responsibility for PKI policy and PKI operations (with Dir IM Secur 3 responsible for the designated domain and Dir IM Secur 4 responsible for the classified domain[16]) while DDCEI has overall responsibility for PKI engineering and design (with DDCEI 3-5 PKI responsible for the Certification Authority[17] (CA) and DDCEI 4 responsible for Directory Services). An organizational chart is provided at **Annex B**.

Overall, SCEM and PKI are not being widely used in the DND/CF. Pockets of users, such as the Military Police, Finance and Human Resources (HR) rely quite heavily on SCEM to protect sensitive messages being sent over email on the designated domain. However, the actual extent of usage is unknown due to a lack of verifiable metrics. What can be confirmed is that out of the 60,000 PKI smartcards originally deployed as part of the SCEM rollout, 35,000 smartcards have now expired (as at August 2004). The cost of these expired PKI smartcards can be estimated at approximated $3.5M ($100 per smartcard/reader * 35,000 smartcards). However, this does not capture the cost of implementation (i.e. the project resources required to initialize and distribute the cards as well as the related training costs) or the intangible costs associated with not using the expired smartcards – for example, the potential embarrassment factor of not complying with privacy laws or the security risk of inadvertently disclosing sensitive information. Within the DND/CF, PB (and even classified) information has been sent in clear text over the designated domain. A number of incidents have been reported and are tracked by the Canadian Forces Information Operations Group (CFIOG), although these reports do not depict the true extent of the problem – only the incidents that have been reported.

Many new DND/CF PKI-enabled applications are being planned and designed on the assumption of an existing, available and reliable PKI within the designated domain. These applications include DVPNI (Defence Virtual Private Network Infrastructure – secure remote access) and the CFHIS (Canadian Forces Health Information System). In addition, a PKI is being planned for the classified domain with the MMHS (Military Message Handling System)[18] as its primary application. A list of DND PKI-enabled applications is provided at **Annex C**. This means there will be at least two separate DND PKI systems: the designated domain PKI that became operational with SCEM, and the MMHS PKI targeted to become operational in mid-2005 in the classified domain. With two separate PKIs comes the added complexity of managing both infrastructures (i.e. policies, processes and people).

It should also be noted that a distinct DND/CF pilot is being conducted on TITAN (i.e. classified) workstations to provide a similar functionality to PKI (i.e. encryption and digital signature) using a different technology. A certificate-based infrastructure (CBI)

[16] The classified domain is a separate DND/CF network intended for classified electronic data traffic only. Classified information is defined as being reasonably expected to cause injury to the national interest and comprises government information that concerns the defence and maintenance of the social, political and economic stability of Canada. Classified information is categorized based on the degree of potential injury (i.e. Confidential, Secret, or Top Secret).
[17] The CA is a key trusted element of a PKI. It is includes the hardware and software used to create, issue and manage public key certificates.
[18] The MMHS is also part of the umbrella DMHS project (that rolled out SCEM).

provides Type 1, high-grade cryptography as opposed to PKI, which provides secure but commercial-grade cryptography. A CBI faces similar challenges as a PKI with respect to implementing the requisite infrastructure (i.e. policies, processes and people)[19].

OVERALL ASSESSMENT

While some of DND's communication security requirements could be satisfied by alternative approaches or technologies, PKI offers the only scalable solution[20] at this time, to meet the security requirements of a widely distributed community in the areas of strong authentication, identification, secure remote access, confidentiality and integrity of electronic data and non-repudiation.

It is evident that the DND/CF has the following valid electronic communications security requirements, although these have not yet been formally articulated in a DND business case or defined in the overall departmental IT security framework from a business or operational perspective:

- To protect sensitive information within the department and information belonging to, and shared with, external organizations;
- To move towards automated workflow and a reduction of paper/manual processes; and
- To engage in secure e-commerce transactions with external parties (e.g. Public Works and Government Services Canada (PWGSC) and suppliers).

The currently-installed designated domain PKI, and the planned MMHS PKI, provide sound technical solutions but significant management, policy, administration and operational weaknesses need to be addressed if the DND PKI(s) are to be operationally effective. Significant issues must be resolved before current users can fully rely on the existing PKI and before new PKI-enabled applications, particularly DVPNI and MMHS, can be supported. These issues have been summarized in Table 1 below and each area has been further described in the next section of the report (Detailed Results and Recommendations). The impact to the DND/CF of *not* having a departmental PKI, and instead having to rely on an external service provider for PKI certificates, is outlined in **Annex D**.

During the course of the review, it was clear that DND/CF PKI staff members are dedicated to the success of the DND PKI(s). They are doing their best without the benefit of well-established processes, sufficient and experienced resources, proper training and adequate management involvement or direction. Individually, each one of these factors could be managed without adversely affecting operations or the level of service to users. However, all of them together present a high degree of uncertainty regarding the credibility and scalability of the overall system.

[19] The DND CBI is to be managed by a separate unit within the Dir IM Secur called the Canadian Forces Crypto Support Unit (CFCSU).
[20] Traditional secret key (or symmetric) encryption systems could be used for point-to-point communications security but do not provide the ability to accommodate a large number of distributed users or a digital signature service. See **Annex A** for more details.

The summary scorecard below, presents a simplified view of "common good practices" one would expect to see in place for any system, in particular, a PKI. The assessment was based on the review results and the professional judgment of the CRS review team[21].

Table 1 – Summary Scorecard of the DND PKI Review

Assessment Criteria		Non-Existent / Undeveloped	Early Stages / Ad Hoc	Developed / In Place	Continuous Improvement
A. Value and Relevance of PKI	Clearly defined departmental business requirements		■		
	Clearly defined departmental security requirements		■		
	Overall level of departmental awareness		■		
B. Governance and Strategic Planning	Formal PKI governance structure	■			
	Program-level PKI planning	■			
C. Policies and Procedures	Clear and accountable PKI policy owner		■		
	Formal process for PKI policy development		■		
	Clear departmental PKI policy approval authority	■			
	DND PKI-related policies approved and up-to-date		■		
	Applicable GoC PKI-related policies followed		■		
D. Roles and Responsibilities	Clearly defined and well-understood			■	
	PKI key roles are identified and filled		■		
E. Infrastructure Support and Processes	Processes are well-defined and in place		■		
	Processes are efficient and cost-effective	■			
F. Performance Measurement	A PKI cost model exists and is up-to-date	■			
	Actual PKI costs are tracked against budget	■			
	PKI usage statistics exist and are tracked		■		
	PKI usage statistics used for workload balancing	■			
	Service/Organizational level agreements in place		■		
G. Integration of PKI Technology	Good interaction btwn technical and functional groups		■		
	Good interaction btwn technical and user groups		■		

DND is not taking an enterprise management approach to PKI, and is therefore not achieving the full efficiencies and effectiveness of PKI as a supporting infrastructure to the secure exchange of data and communications. Moreover, the department's piece-meal approach to PKI leaves it vulnerable to avoidable costs and risks. PKI is more than just a technology solution and needs to be managed in the context of DND/CF business and operational requirements.

[21] The CRS review team included both CRS and AEPOS team members.

KEY RESULTS

- Although DND has valid requirements for the security services enabled by an enterprise PKI, the business and security requirements have not yet been clearly defined or articulated in a formal manner to communicate the value and relevance of PKI to senior departmental management or to the user-level.
- There is a need for a formal PKI governance structure to provide overall direction and minimize strategic-level disconnects and gaps. PKI should be managed as a common infrastructure program but is being approached as a series of independent projects.
- There is a lack of formally endorsed PKI policies and procedures. Draft policies are out-of-date and need to be revised.
- Roles and responsibilities for key positions lack clarity and definition.
- Fundamental infrastructure processes require strengthening and necessary horizontal coordination is not occurring.
- There are no cost or usage metrics for the designated domain PKI, and a PKI cost model does not exist.
- Better integration of PKI technology and business processes is needed.

POTENTIAL CAUSES / OTHER CONCERNS

Many of the issues raised during the course of this review are not unique to the DND PKI(s) but apply equally to other departmental systems. Undefined or incomplete business requirements and a lack of governance, program level planning and horizontal processes are systemic issues that have been previously identified in relation to a number of different departmental systems/projects. One of the overarching causes is related to IM governance, particularly, the lack of an enterprise approach to implementing IM projects.

In the case of the DND PKI(s), project objectives are at times in conflict with the longer-term requirements of the life cycle product management (LCPM) and operational groups. The project teams (i.e. SCEM and MMHS) were/are under constant pressure to complete deliverables while meeting cost and schedule deadlines. Some project requirements are narrowly defined due to a lack of horizontal planning processes and an enterprise approach. For example, interdependencies with other projects (i.e. between SCEM, MMHS and CBI) are often overlooked as they are considered “out of scope” of each individual project. However, this results in the LCPM or operational groups having to establish processes that are found to be lacking only after the project has been handed over to them (e.g. the case with the designated domain PKI). Other project processes, such as user training, are not robust enough (e.g. are

focused on initial one-time training as opposed to regenerative training processes) to handle user requirements over the longer-term. Unless a PKI governance structure is put in place to focus on program-level objectives and to begin managing PKI as a common departmental infrastructure program, these types of conflicts will not and cannot get resolved.

Another area of concern is that PKI has often been referred to as a "working-level" initiative (i.e. bottom-up) with insufficient visibility to ADM(IM) senior management. As a result, management does not fully appreciate the ongoing support requirements necessary to implement a sustainable and credible PKI system. This lack of visibility and management involvement was likely a factor in the incomplete definition of SCEM system requirements. In particular, it was a SCEM project decision that led to the issuance of 60,000 PKI smartcards but over half of these smartcards expired within 3 years of issuance. It should be noted that many of the issues raised in this review were also documented in an internal DND briefing note that was prepared for ADM(IM) senior management in August 2000. No observable actions were taken, likely due to the turnover in key central groups.

Lastly, while this is outside the scope of this particular review, an area of concern that should be highlighted relates to the project governance structure of the MMHS project. ADM(IM) is the Project Sponsor and also responsible for Project Implementation despite the fact that the Deputy Chief of Defence Staff (DCDS) will be the ultimate operational authority of the MMHS. In order for the MMHS to be successfully deployed, existing business processes will need to be modified to integrate the technology appropriately. In addition, new PKI-related policies may be required to recognize the new application of technology and the change to existing processes. DCDS participation during the implementation phase would increase the likelihood of user adoption of the MMHS and may also avoid some of the project transition/handover issues that were experienced with SCEM and the designated domain PKI.

KEY RECOMMENDATIONS

It is recommended that the ADM(IM):

- **Develop a PKI "roadmap"** that clearly defines and articulates DND's business and security requirements for an enterprise PKI. The "roadmap" should clearly demonstrate how and where PKI fits into the overall IT security framework in addition to defining the business requirements that PKI addresses for both existing and future applications.

- **Manage PKI as a common departmental infrastructure program** and establish requisite/appropriate governance structures and strategic planning processes to provide overall direction, formally endorse PKI policies, and ensure that strategic-level voids and disconnects are minimized.

- **Update and formally endorse necessary PKI policies**. At a minimum, this includes the CP and the CPS as well as the development of a clear departmental policy or directive on the requirement and use of PKI encryption and digital signatures. Other departmental PKI-related policies, such as the management and use of email, DND application of the Library and Archives Canada (LAC) data holdings policy, information management etc. should be developed or revised as necessary.

- **Define, clarify, assign, document and communicate key roles and responsibilities** of PKI support groups for all aspects of PKI (including policy, operation, registration (central and local/base level), external liaison, Help Desk, monitoring and evaluation/compliance).

- **Strengthen, rationalize and optimize the separate PKI infrastructure support and processes**, particularly registration, training, and Help Desk, into a combined support structure with streamlined processes for the different PKI and CBI systems.

- **Develop a PKI cost model and develop, gather, analyse, monitor and report operational performance metrics** on a regular basis to allow for performance assessment, budgeting, cost analysis and workload planning and balancing.

- **Identify / establish a new "business analyst" role to liaise with users and functional groups** to foster communication and gather requirements. The goal is to develop a solid understanding of the existing business processes and PKI requirements to determine how to best integrate PKI technology and achieve desired benefits (i.e. operational efficiencies and cost savings).

The practices and lessons learned from other organizations (provided at **Annex E**) were considered in the formulation of the above key recommendations.

MANAGEMENT ACTION PLANS

Management action plans provided by ADM(IM) demonstrate constructive attention to the majority of recommendations contained in this report. At the same time, we encourage that certain actions be set in motion earlier than currently planned, particularly, in regards to the development of a DND PKI Roadmap, clarification of DND PKI support group roles and responsibilities, and rationalization of separate PKI infrastructure support and processes (ref: serials A, D, and E of the management action plan matrix). In this respect, interim milestones for these action plans will be requested through CRS follow-up and monitoring processes. Recommendations and corresponding management action plans are presented in matrix format at **Annex G** of this report and have also been summarized in Table 1 below.

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
A.	*Develop a PKI "roadmap"* that clearly defines and articulates DND's business and security requirements for an enterprise PKI.	OPI: Dir IM Secur	Agree. Dir IM Secur should be lead for the development of a DND PKI roadmap for senior management approval. The DND roadmap will include a training and awareness program.
B.	*Manage PKI as a common departmental infrastructure program* and establish requisite/appropriate governance structures and strategic planning processes.	OPI: Dir IM Secur	Agree. It is proposed that PKI be managed as a common infrastructure program by establishing a governance framework and by integrating it into the existing key management framework.
C.	*Update and formally endorse necessary PKI policies.* This includes the CP and CPS as well as departmental PKI related-policies and procedures such as the management and use of email, DND application of the LAC data holdings policy etc.	OPI: Dir IM Secur OCI: DDCEI	Agree. Dir IM Secur will staff the existing GoC CP and DND CPS IAW the PKI governance framework. Dir IM Secur and DDCEI will also consult with the application owners for PKI enabled applications on application-specific policies and procedures.
D.	*Define, clarify, assign, document and communicate key roles and responsibilities* of PKI support groups for all aspects of PKI.	OPI: DGIMO OCI: Dir IM Secur DDCEI/CFNOC	DGIMO will establish PKI responsibilities for the PKI support groups as part of the DGIMO realignment.
E.	*Strengthen, rationalize and optimize the separate PKI infrastructure support and processes* into a combined support structure with streamlined processes for the different PKI systems.	OPI: DGIMO	DGIMO will rationalize PKI support and processes as part of the DGIMO realignment. DDCEI and Dir IM Secur will develop a resource plan for the stabilization of the PKI infrastructure.
F.	*Develop a PKI cost model and develop, gather, analyse, monitor and report* operational performance metrics on a regular basis.	OPI: Dir IM Secur OCI: DGIMO	DGIMO will ensure that system performance monitoring and capacity planning for PKI infrastructure is addressed in the Divisional realignment. DDCEI and Dir IM Secur will develop a cost model as part of the resource plan for the stabilization of the PKI infrastructure.
G.	*Identify / establish a new "business analyst" role to liaise with users and functional groups* and foster communication.	OPI: Dir IM Secur OCI: PMA PAC	Dir IM Secur will provide introductory PKI training to their analysts and PMA PKI Advisory Cell (PAC) members, in order to identify enterprise level opportunities and impacts of PKI enabled solutions.

Table 1: Summary of Management Action Plans

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

The primary objective of the review was to assess the capability of the DND PKI to provide secure and confidential services to departmental users and applications. The review also set out to assess the impact of future requirements on the development, management and operation of a sustainable, credible and scalable departmental PKI.

SCOPE

The scope included key aspects of the governance structures, policies, processes, resources and equipment that collectively support the management and operation of the DND PKI. Future departmental PKI applications and benchmarking of comparable organizations were also examined. The review did not assess the technical capabilities of the Entrust® product or its selection as the CSE approved mechanism for PKI.

METHODOLOGY

- Gathered and reviewed departmental information on the DND PKI as well as relevant GoC policies.
- Developed a PKI Framework document and a High Level Risk Assessment.
- Conducted interviews with:
  - Key departmental stakeholders and senior functional management;
  - Departmental PKI engineers and support staff;
  - Departmental users and potential users (planned applications); and
  - Other government departments as well as selected non-federal government organizations.
- Assessed the impact of new and future departmental PKI applications.
- Examined other organizations' approaches to PKI.
- Examined DND's cross-certification[22] needs and implications.

[22] Cross-certification is the process of establishing mutual trust with another PKI so that each PKI accepts the other's certificates. This permits secure inter-operation across separate PKI domains. To date, 6 government departments (not DND) and 1 provincial organization were cross-certified with the GoC PKI.

DETAILED RESULTS AND RECOMMENDATIONS

A. VALUE AND RELEVANCE OF THE DND PKI

Severed under section 20(1)(c) of the AIA – Third Party Information.

……..”[23]

The absence of clearly defined business and security requirements is contributing to the lack of awareness, understanding and use of PKI as an electronic communications security enabler within the department. PKI is often seen as a technical solution looking for a problem, rather than a response to a particular business need. Although DND has valid requirements for the security services[24] offered by an enterprise PKI, these requirements have yet to be formally articulated in a DND business case. Additionally, DND has not yet defined how or where PKI fits into the overall departmental IT security framework from a business or operational perspective. Many departmental employees are not sufficiently aware of the necessity to protect designated / sensitive electronic information and do not recognize that the technology is readily available on most workstations.

Undefined business and security requirements

- The original justification for the DND PKI purchase in 1995 was unclear and was not tied to specific business requirements.
- The departmental security requirements that PKI is intended to address have not been clearly defined as part of the overall departmental IT security framework (e.g. identifying which systems require strong authentication, based on a risk assessment).
- There is no clear departmental policy or directive requiring PKI to be used (e.g. to encrypt Protected B (PB) information or to promote / encourage the use of digital signatures for automating processes).
- Secure Common Email (SCEM), which was the driving application for PKI, is not generally regarded as a “must-have” application in the DND, and the value of secure email has not been sufficiently emphasized to protect sensitive messages during transmission.

Severed under section 20(1)(c) of the AIA – Third Party Information.

[23] ……..
……..

[24] PKI security services include: user/entity authentication, data confidentiality, data integrity, and non-repudiation.

Limited departmental awareness of PKI use and capabilities

- There is a relatively limited level of departmental awareness of the requirement to protect designated / sensitive electronic documents (i.e. PB information) and that PKI could be used to meet this requirement (as compared to the level of awareness to protect sensitive paper documents).
- The value of PKI as a security enabler and its ability to offer strong encryption are not well understood in the department.
- There is a lack of buy-in on the part of departmental personnel. Many users do not understand the requirement for PKI while the Military Police (MP), Human Resources (HR) and Finance find it of great value.
- Some DND/CF staff are reluctant to accept PKI smartcards and some units are reluctant to issue them.
- While many issued PKI smartcards have never been used, the actual extent of PKI usage in the department is uncertain due to the absence of metrics.

Examples of how PKI is being used successfully in other organizations

- Law enforcement agencies rely on PKI's strong commercial cryptography to ensure confidentiality and protection of sensitive information (e.g. communicating with undercover operators, registry of sex offenders).
- Paper processes are being eliminated or reduced by automating the issuance of cheques based on digital signatures (e.g. selected Canada Revenue Agency (CRA) rebate programs).
- Electronic versus manual transmission of sensitive documents can significantly reduce processing times and lead to cost savings and improved operational efficiencies. This is the case with drug companies that have automated key approval processes such as the Food and Drug Administration (FDA) approval processing times. Drugs can get to market quicker resulting in significant financial benefits to patent holders.

RECOMMENDATIONS

Develop a PKI "roadmap" that clearly defines and articulates DND's business and security requirements for an enterprise PKI. The "roadmap" should clearly demonstrate how and where PKI fits into the overall IT security framework in addition to defining the business requirements that PKI addresses for both existing and future applications. This should be a living document that is updated periodically and used to communicate the value of PKI to stakeholders and decision-makers. The "roadmap" should also be provided to new projects with PKI requirements to ensure they have a clear understanding of the security services offered (and not offered) by the DND PKI.

- PKI should only be deployed in response to defined business requirements and a clear financial business case (i.e. a cost/benefit analysis).

- A concerted effort must be made to increase departmental awareness and understanding of PKI use and capabilities. Departmental employees must be made aware of the requirement to protect sensitive / designated electronic information and that PKI is an approved technology for doing so.

OPI: ADM(IM)

B. GOVERNANCE AND STRATEGIC PLANNING

A formal departmental PKI governance structure is required to provide overall direction (both inter- and intra- departmental guidance) and to ensure that strategic level disconnects are minimized. Major PKI management, policy, administration and operational resolution[25] are required by a departmental-level authority for the DND PKI to fully and reliably deliver requisite security services to departmental users and applications. Although PKI should be managed as a departmental infrastructure program, it is being approached as a series of independent projects aligned with individual PKI applications. The lack of program- level planning is likely to result in operational inefficiencies and unnecessary cost expenditures from designing separate infrastructure support and processes to maintain the two main DND PKI systems[26]. Potential streamlining opportunities may also exist with a third DND system called CBI, Certificate Based Infrastructure, currently being managed by Dir IM Secur / CFCSU.

[25] Each of these areas will be discussed in detail in subsequent sections of this report.
[26] The two main DND PKI systems are the existing designated domain PKI (i.e. SCEM) and the MMHS PKI being planned for the classified domain.

Need for a formal PKI governance structure

- There is no formal DND PKI governance structure to provide strategic-level direction, program-level coordination, decision-making authority and overall accountability to operational and technical staffs and project teams.
- A departmental-level authority has not been identified to formally endorse DND PKI policies.
- The need for PKI has not been clearly articulated to DND senior management and it is not formally supported. Moreover, ADM(IM) management has only a partial understanding of the investment and ongoing support requirements necessary to implement a sustainable and credible PKI system.
- PKI roles and responsibilities are not fully appreciated by ADM(IM) senior management.

Lack of a coordinated, integrated and programmatic approach

- DND and ADM(IM) senior management are primarily engaged in PKI at the individual project level (i.e. SCEM, MMHS, DVPNI) versus the departmental or enterprise level.
- There is a need for program-level PKI strategic planning to ensure congruence with departmental versus project objectives, to provide direction on the way ahead, and to avoid operational inefficiencies and unnecessary cost expenditures.
- Specifically, DND could end up with three separate but similar systems: the designated domain PKI, the MMHS PKI in the classified domain, and the CFCSU CBI being piloted on classified TITAN workstations. While three separate systems may be necessary from a *content* perspective, possible synergies in combining the infrastructure support and processes (e.g. central registration and help desk support and processes as well as base level resources) are not being sufficiently explored, as it is considered "outside the scope" of each individual project. Potential problems may also arise from having PKI and CBI on the same classified workstation but this is also considered "out of scope" by the individual projects.
- There is no overarching departmental electronic communications security strategy to address security for new devices such as personal digital assistants (e.g. Blackberry™).
- DND's long-term strategy with respect to membership of the GoC PKI is unclear. DND's designated domain PKI is not yet interoperable (i.e. cross-certified) with the GoC PKI and there are no plans to fulfil preliminary compliance inspection requirements.

RECOMMENDATIONS

Manage PKI as a common departmental infrastructure program and establish requisite/appropriate governance structures and strategic planning processes to provide overall direction, formally endorse PKI policies, and ensure that strategic-level voids and disconnects are minimized. PKI management and oversight may be added to an existing DND governance committee provided that the committee's mandate is formally amended to include PKI responsibility and there is appropriate senior management representation from the different functional areas and commands.

- Strategic-level plans related to managing and potentially merging the infrastructure support and processes for the different PKI and CBI systems as well as direction on the way ahead (i.e. future cross-certification requirements) should be incorporated into the PKI "roadmap" recommended in Section A. Value and Relevance of the DND PKI.

OPI: ADM(IM)

C. POLICIES AND PROCEDURES

PKI policies form an integral component of a PKI system. The policies serve as the cornerstone of establishing "trust" in a public key certificate and constitute a basis for cross-certification (which permits secure interoperability) with other organizations. PKI policies are described in a set of fundamental documents known as the Certificate Policy (CP) and the Certification Practice Statement (CPS). The CP generally addresses the higher-level policy requirements (i.e. states the conditions under which PKI certificates can be issued based on an enterprise's risk assessment) whereas the CPS is a more detailed and comprehensive technical and procedural document governing the operation of the PKI (e.g. the practices employed in issuing, managing and revoking certificates, a description of service offerings etc.). The TBS mandatory requirement to perform annual inspections to verify compliance with PKI policies is intended to further augment the "trust" in a PKI system. In DND, a departmental-level authority has not yet granted formal endorsement or approval of draft PKI policies and no formal compliance inspection has been performed.

Lack of formally endorsed PKI policies and procedures

- The DND designated domain PKI has been in operation since late 2002 without any formally approved PKI policies (e.g. CP and CPS) or related procedures in place.
- PKI standard operating procedures (SOPs) – for example, SCEM and MMHS desktop SOPs – are not backed up by policy. In some cases draft PKI policies and SOPs are contradictory.
- Responsibility for departmental PKI policy sign-off is unclear given the lack of governance around PKI. This has also impeded the development of necessary PKI-related policies (e.g. PKI application in broader departmental policies such as information and electronic records management).
- The lack of approved PKI policies, strategic direction on the way ahead and program-level priority setting has left PKI operational and technical staff to set their own priorities.

Adhoc processes for PKI policy development

- Processes for development, maintenance and promulgation of PKI policy documentation are adhoc and not clearly defined. The DND PKI(s) cannot succeed without structured processes for development, implementation and maintenance of PKI and PKI-related policies and directives.
- PKI policy responsibility currently resides with Dir IM Secur 3 and 4. Based on the review, the CRS review team believes this responsibility should be re-assigned to another group to ensure adequate segregation of duties (see Section D. Roles and Responsibilities for more details).

Departmental policies have not kept pace with technological and legal changes

- Broader departmental policies and PKI-related SOPs have not kept pace with technological and legal changes.
- For example, although laws and statutes sanction the acceptance of digital signatures, this has not yet been reflected in departmental policies. In other instances, back-up paper processes and signatures are still required in SOPs despite the use of electronic processes and digital signatures.
- The Library and Archives Canada (LAC) directive of only accepting data in its original form – in the case of PKI, unencrypted and not digitally signed – was raised frequently as an impediment to developing some of the requisite PKI-related policies and SOPs. While this is a challenge, it should not prevent DND from making a decision as to how it should approach the issue.

Instances of non-compliance with policies and other risks

- TBS PKI policy requires annual compliance inspections for all departments operating their own CA/PKI. In contravention of GoC policy, the DND designated domain CA has not yet undergone an inspection to verify compliance with PKI policies (e.g. CPs and CPSs).
- There are instances where certification and accreditation (C&A) of some departmental systems have not been adequately performed. In addition, some systems have been granted Interim Authority to Process (IAP) that are not fulfilling IAP conditions but continue to operate on the DWAN[27]. This situation applies to the designated domain PKI as well as other non-PKI systems, in contravention of GoC and DND security policy.
- No explicit provision has been made for backup of private decryption keys. In the event that departmental access to PKI-encrypted files is required, a manual key recovery process must be used. Although third-party key recovery is currently possible for all current and previous DND PKI subscribers, there are no policies or procedures to assure long-term access to PKI-encrypted data.

RECOMMENDATIONS

Update PKI policies as required and present for formal endorsement to the appropriate departmental-level authority. At a minimum, the PKI policies should include the CP and the CPS (for the two main DND PKI systems) as well as the development of a clear departmental policy/directive on the requirement and use of PKI encryption and digital signatures.

- Clearly define processes for development, maintenance and implementation of PKI policies including an effective process for approval and promulgation.
- PKI SOPs (i.e. SCEM and MMHS desktop SOPs) should be revised to align with approved PKI policies.
- Perform a formal inspection to verify compliance with approved PKI policies (within a year of approval).

Review and revise departmental PKI related-policies and procedures such as the management and use of email, DND application of (or approach to) the LAC data holdings directive, information management etc.

- Identify departmental PKI related-policies and procedures requiring revision or resolution.
- The policy owner or the PKI governance committee (as deemed appropriate) should approve/endorse any updated departmental PKI related-policies.

OPI: ADM(IM)

[27] Before a new system is permitted to operate on the DWAN, it must pass through the C&A process to ensure it is designed and implemented in accordance with specified security requirements. IAP is granted as an interim measure to allow pilot systems to operate on the DWAN prior to completion of the full C&A process.

D. ROLES AND RESPONSIBILITIES

PKI-enabled security services are designed to mitigate the risks of conducting business or communications over public networks. In an electronic business environment, one of the biggest challenges is in obtaining assurance regarding the identity of the person, corporate entity or application with whom business is being transacted (i.e. user authentication). A PKI is able to provide this assurance by establishing a trusted infrastructure to bind unique electronic credentials to the individual requesting access, and by providing a mechanism to verify that the binding was initially valid and is continuously maintained. The trusted party responsible for managing and controlling the binding process is the Central Registration Authority (CRA). In a large, geographically dispersed organization, trusted agents such as Local Registration Authorities (LRAs), are used to assume many of the administrative functions from the CRA, particularly, end-user registration (i.e. face-to-face identification of the subscriber). Many issues were identified with respect to the roles and responsibilities of the trusted parties that form part of the DND PKI(s).

Inadequate separation of duties within the CRA

- Dir IM Secur 3 is the CRA for the designated domain PKI, and Dir IM Secur 4 will become the CRA for the MMHS PKI once it is fully operational in the classified domain.
- Dir IM Secur 3 (and eventually Dir IM Secur 4) has responsibility for PKI policy development, engineering, life cycle certificate management and operational activities in addition to the performance of formal compliance inspections as described in Section C. Policies and Procedures.
- There is an inadequate separation of duties within Dir IM Secur 3 (and eventually Dir IM Secur 4). Groups responsible for setting PKI policy should not be responsible for operating the system and performing the "independent" compliance function.
- Although PKI policy is documented as part of Dir IM Secur 3's responsibilities, some key personnel do not recognize their policy development role or devote any time to it. This is due in part to insufficient resources but also as a result of the governance issues and the absence of a PKI departmental-level authority to sign-off on PKI policies.

Weaknesses in CRA controls undermine "trust" relationships

- Dir IM Secur 3 control over the processes for appointing, training, retaining and replacing of LRAs and Local Registration Coordinators (LRCs) (i.e. base level PKI registration support) is not effective. For example, the CRA does not have an up-to-date list of LRAs/LRCs or a consistent process for LRAs/LRCs to communicate information about departures or replacements.
- Dir IM Secur 3 controls over certificate revocation processes are not effective. Failure to revoke LRA certificates poses a major security vulnerability and a high risk to the integrity of the designated domain PKI as LRAs have privileges associated with enrolling users and issuing PKI certificates.
- Some key Dir IM Secur 3 staff are not engaged or supportive of some registration processes within their area of responsibility.

Potential synergies in merging registration activities

- PKI and CBI central registration activities are very similar. Certificate management processes for PKI (designated domain and MMHS PKIs) and CBI (CFCSU) could be handled by a *single* CRA group provided clear and effective procedures are developed and put in place.
- Since PKI is not being managed as a common departmental infrastructure program, potential synergies and rationalization opportunities of merging processes are being overlooked and similar CRA functions will be duplicated across three separate groups (Dir IM Secur 3, 4 and CFCSU).
- There are a number of specific concerns regarding LRA/LRC roles and responsibilities including the willingness to fulfill assigned duties. Perception at the local/base level is that LRA/LRC duties are being imposed without additional resources being assigned. A risk of further resistance stemming from additional duties relating to the MMHS rollout also supports the need to merge registration functions and processes at the local/base level.

Additional cooperation and coordination required

- There is low cooperation and understanding within central PKI support groups. Differences in understanding exist between the Canadian Forces Information Operations Group (CFIOG), Dir IM Secur 3 and DDCEI 3-5 PKI groups over Help Desk processes and related roles and responsibilities.
- Some projects with PKI requirements do not appear to receive adequate design assistance from central PKI support groups such as engineering and policy. Conflicts stem from the projects' needs to complete project deliverables and the ability of central groups to provide timely assistance.

RECOMMENDATIONS

Define, clarify, assign, document and communicate key roles and responsibilities of PKI support groups for all aspects of PKI (including policy, operation, registration (local/base level and central), external liaison, Help Desk, monitoring and evaluation/compliance).

- Separate PKI policy and evaluation (compliance function) from central registration (CRA) responsibility.
- Combine central registration and certificate management activities for PKI (designated domain and MMHS PKIs) and CBI (CFCSU) within a *single* CRA organization.
- Ensure appropriate procedures are developed and in place before re-locating activities within one group.
- Strengthen controls over LRA/LRC processes and combine local registration activities for PKI and CBI at the local/base level (once processes have been streamlined and put in place).

OPI: ADM(IM)

E. INFRASTRUCTURE SUPPORT AND PROCESSES

In order to provide the security services required by users and applications, a PKI system requires structured processes in addition to ongoing operations and maintenance support of its Certification Authority[28] (CA), Directory services[29] (DS), Registration services and Help Desk services. In DND, provision for ongoing life cycle support and maintenance is inadequate in most cases and completely absent from some new PKI applications. For example, although the MMHS PKI is in pilot and expected to be fully operational by mid-2005, Dir IM Secur 4, the group responsible for PKI policy and CRA functions for the MMHS PKI, does not have any funded positions to fulfil these roles. Existing central support resources are compensating for missing processes by attempting to develop them on their own in addition to performing their regular duties. Data quality issues complicate life cycle certificate management processes, and key staff lack funding for necessary training courses.

[28] The CRA (i.e. Dir IM Secur 3) relies on the CA (equipment used to create and assign public key certificates) to manage and operate the PKI.
[29] Directory Services (DS) are required to manage the repository that holds PKI certificates. A PKI directory is similar to an email directory or a telephone book.

Adequate provision for life cycle support is essential

- CA and DS – there are insufficient CA and DS operations and engineering resources for the maintenance of documentation and for external liaison activities, such as providing consulting services to projects. Up-to-date documentation on the designated domain PKI system, such as a Concept of Operations, is not available.
- CRA – the current structure within Dir IM Secur 3 cannot support the level of registration activity required for effective operation once the MMHS PKI and other new PKI-enabled applications, such as DVPNI (secure remote access), are rolled out. At this point Dir IM Secur 3 does not have the capacity to meet significant increases in demand for registration services or support for new PKI-enabled applications without making changes to existing processes. In addition, Dir IM Secur 4 does not have any funded positions to support the MMHS PKI.
- LRA/LRC – specific concerns about LRA/LRC processes include: the appropriateness of appointments (currently approximately 1,500); the accuracy of the list of LRAs/LRCs; the provision of on-going LRA training; and the management of paper based subscriber agreements.
- Registration – the registration process could be made more efficient through the use of an automated self-service registration system and by designing and leveraging similar processes for both the designated and classified domain PKIs (central and local/base level).

Data quality issues complicate processes

- Disconnects and omissions in data repositories complicate the PKI certificate and identity management processes, weaken the authentication function for users and could, in some cases, compromise security access restrictions.
- Some HR Management System (HRMS/PeopleSoft) addressing[30] information is out of date.
- HRMS/PeopleSoft security clearances data is out-of-step with the Deputy Provost Marshal Security (DPM Secur) clearances data.
- PKI is not yet integrated with applicable records management systems (e.g. HR).

[30] Addressing information refers to information used to associate an entity with a particular location (e.g. physical and/or electronic addresses). Addressing information is required to create PKI certificates and link them to the appropriate individual or entity.

Training is critical for PKI staff and users

- It is extremely important that registration staff be properly trained on the Entrust suite of products. This does not appear to be happening either in the field (i.e. LRAs/LRCs) or at the Central Registration facility (Dir IM Secur 3) due to the perception of a shortage of funds.
- Initial user training for SCEM appears to be adequate. However, there are major questions with respect to ongoing understanding of the features and potential for PKI. Most users are not fully aware of the capabilities of the technology (e.g. they do not know how to use the digital signature feature of Entrust).

RECOMMENDATIONS

Strengthen, rationalize and optimize the separate PKI infrastructure support and processes, particularly registration, training, and Help Desk processes, into a combined support structure with streamlined processes for the different PKI and CBI systems.

- Design and implement as much automation into the registration process as possible to improve overall efficiency, minimize manual processes and reduce maintenance effort.
- Develop a resource plan to identify the number of resources required to support effective, ongoing operation of the PKI system as a common departmental infrastructure (using the new streamlined processes and clarified roles and responsibilities as a baseline). The plan should include a growth factor based on projected activity.
- Improve overall completeness, consistency and accuracy of the data required for the certificate management process by reviewing the composition and updating the processes and linkages of the various DND data repositories.
- Review the approach to PKI training and ensure that all training (for users, LRAs/LRCs and CRA staff) is appropriate, adequate and timely. A thorough review of existing PKI skill sets and current PKI training needs for CRA staff and LRAs/LRCs should be undertaken.

OPI: ADM(IM)

F. PERFORMANCE MEASUREMENT

There is an absence of PKI operational metrics to accurately report operational costs and degree of PKI usage. This makes workload planning virtually impossible, obtaining additional funding and resources challenging, and evaluating service-delivery options extremely complex (e.g. determining the cost of acquiring PKI certificates from an external PKI service provider versus providing the service internally). In order to measure PKI program performance and to allocate departmental resources and funds effectively, objective and quantifiable data is required by departmental decision-makers and stakeholders. In addition, the lack of operational level agreements (OLAs) between central PKI operational groups and the lack of service level agreements (SLAs) with new applications is resulting in differing expectations among groups and may lead to performance deficiencies.

Absence of PKI operational metrics

- No performance metrics were available for the DND PKI system. Although there is a general perception that SCEM use is fairly low, this could not be confirmed by the PKI registration system.
- Order-of-magnitude estimates can be inferred from key recovery and certificate issuance numbers. Using this data, there were approximately 25,000 *activated* certificates (as at Aug 2004). Of these, between 13,500 and 25,000 were estimated to be *active users* (active users logged onto Entrust at least once in the last year). Approximately 35,000 certificates that were issued as part of the SCEM project rollout were expired.
- No cost information is being gathered to track expenditures attributable to the PKI system. A PKI budget or cost model does not exist to track actual costs or to provide a basis for forecasting the impact of supporting new PKI applications. This is due in large part, to the governance issues and the fact that PKI is not managed as a departmental infrastructure program.

Need for OLAs and SLAs to assess current performance levels

- There are no up-to-date OLAs or SLAs in place and responsibility for either is unclear.
- The need for OLAs among central operational groups is resulting in confusion over roles and responsibilities. Required tasks are not being completed or performed.
- The lack of SLAs and undefined performance criteria prevents accurate assessment of the PKI system and may lead to differing service expectations and potential performance deficiencies (e.g. due to unexpected spikes in registration activity or insufficient workload balancing). This affects the ability of central operational groups to negotiate service levels with new PKI applications, such as the MMHS, since current performance levels are not well understood or monitored.

RECOMMENDATIONS

Develop, gather, analyse, monitor and report operational performance metrics on a regular basis to allow for performance assessment, budgeting, cost analysis and workload planning and balancing.

- Develop a complete cost model (one time + ongoing) for PKI as a common departmental infrastructure program.

Develop, negotiate and implement up-to-date OLAs between central PKI operational groups **and SLAs** with new PKI applications.

OPI: ADM(IM)

G. INTEGRATION OF PKI TECHNOLOGY

In order for the DND PKI(s) to be considered a critical part of the DND's common information technology (IT) infrastructure, PKI technology must be viewed as an enabler to improving business processes. Technology (i.e. hardware/software) is but one part of a PKI system – policies, processes and people are equally important components. In fact, it is often argued that the latter are the most critical elements in successfully deploying any new system. In the case of the DND PKI(s), it is not only important that the technology is sound, but also that the product is properly configured and tested, and business processes are re-engineered to integrate the new technology seamlessly. The DND PKI is not fulfilling its potential as a tool for digitally signing electronic documents and for automating business processes due to: conflicting policies and directives; policies that have not kept pace with technology; local workstation PKI configurations that do not provide user-friendly digital signature verification; and a lack of focus on how to smoothly integrate the technology with business processes.

Better integration of PKI technology and business processes needed

- The value of PKI could be substantially improved if certain features were configured, modified or customized to allow for better integration of technology and business processes.

  For example:

  - Current workstation configuration options of Entrust result in the removal of a digital signature once a digitally signed document has been opened. This is caused by the selected configuration options rather than a software deficiency and these may not be the most optimal or user-friendly settings for users.

Better integration required

Examples (continued)

- A user should be able to open and read a digitally signed document without having to use their individual PKI smartcard. This is currently not the case within the DND.
- In order to use digital signatures more effectively to automate and reduce approval times of existing manual processes, a "multiple" digital signature capability should be available. For example, in one organization interviewed, PKI and digital signatures are used for an overtime application. A "multiple" signature capability was required for this application to be adopted by the business owner and was achieved through customization of the Entrust software.

- These types of issues were raised to the CRS review team throughout the course of the review. Users did not know who was responsible for resolving them or who was accountable for them.
- It is important to note that the CRS review team is *not* suggesting that DND should customize its Entrust software in response to every user request. Rather, the purpose of these observations is to emphasize the need to work with the functional groups (i.e. business owners) to determine their requirements for automating business processes using PKI technology and capabilities. Once these requirements are understood, the PKI operations and technology groups must determine *how* PKI can best be integrated to provide a more efficient and cost-effective process. A business case and cost analysis should be undertaken prior to making *any* decisions to customize or modify features.

RECOMMENDATIONS

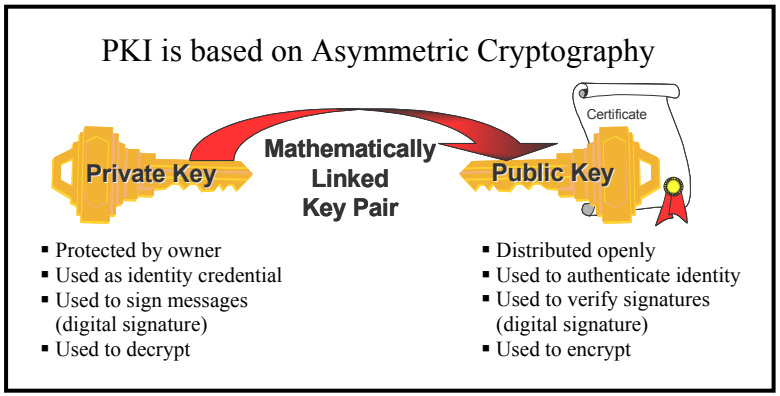
Identify / establish a new "business analyst" role to liaise with users and functional groups, foster communication and gather requirements. The goal is to develop a solid understanding of the existing business processes and PKI requirements to determine how best to integrate PKI technology to achieve the desired results (i.e. efficiencies related to a reduction in manual/paper processes).

OPI: ADM(IM)

ANNEX A – PKI TECHNOLOGY BASICS

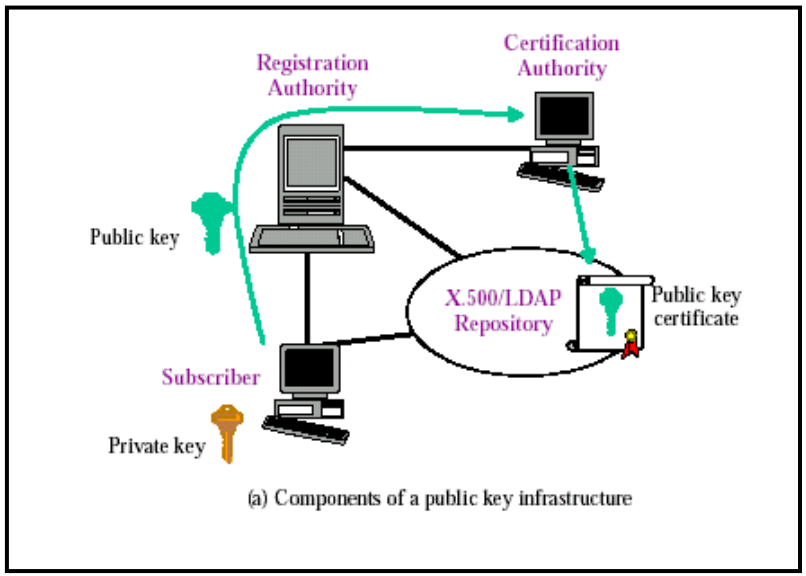
Public key cryptography encrypts information by using two mathematically related keys: one is kept private; the other is made public. The private key cannot be determined from the public key. If an individual wants to send a message, he/she uses the public key of the recipient to encrypt the message. The recipient uses his/her private key to decrypt the message. The sender therefore knows that only the intended recipient can read the message.

Public key cryptography can also be used to create ***digital signatures*** based on the same principles. A digital signature performs a similar function to a written signature and can be used to verify the origin and the contents of a message. For example, a recipient of data can verify who signed the data and that the data was not modified after being signed. This prevents the originator from falsely denying having signed the data.



Source: US Federal PKI Steering Committee Presentation – Federal Approach to Electronic Credentials – J. Spencer

PKI Technical Components



(a) Components of a public key infrastructure

A ***Certification Authority (CA)*** is a third party trusted to associate a public and private key pair with a particular individual (or entity). It identifies the individual that is to receive a key pair; issues keys; revokes keys when a private key may have been lost, stolen or otherwise made public; and provides notice as to those key pairs that have been revoked. The CA also signs the digital (PKI) certificate, which contains an individual's public key and serves as evidence that the individual identified in the certificate holds the corresponding private key.

A ***Registration Authority (RA)*** is a third party trusted to handle some of the administrative tasks off-loaded by the CA – for example, the RA confirms the identity of users on behalf of the CA and it initiates the certification process with the CA on behalf of users.

The ***PKI Directory*** (X.500/LDAP Repository) is the repository where all public key certificates are published. It is similar to an email address or telephone book.

ANNEX A

PKI is scalable

Since an individual's public key does not need to be kept secret, all public keys issued by a CA can be published in a PKI directory and made available to all PKI subscribers. This is what makes PKI a scalable solution – i.e. has the ability to accommodate a large number of distributed users. It is one of the greatest advantages over symmetric or secret key encryption, whereby two parties share a single key for encryption and decryption. Symmetric encryption[31] assumes that the parties who share a key can rely on each other not to disclose that key and to protect it against modification; therefore, the parties must trust one another completely. It should be evident that with symmetric encryption, key management can become extremely complicated when dealing with a large number of users.

On the other hand, with PKI, key management can be centrally managed so an individual only has to worry about keeping his/her own private key secret. If an individual wants to send an encrypted message to another party, they do not have to share secret keys. All that is required is for the originator to look up the recipient's public key in the PKI directory and encrypt the message for the intended party. Once the requisite PKI infrastructure is in place, it can be used to accommodate a growing number of users.

Cross-certification

Cross-certification[32] is a process undertaken by Certification Authorities to establish a trust relationship. The Certification Authorities exchange cross-certificates and enable users of certificates issued by one Certification Authority to interact electronically and securely with users of certificates issued by the other. When two Certification Authorities are cross-certified, they agree to trust and rely upon each other's Public Key Certificates and keys as if they had issued them themselves. The Canadian Federal Public Key Infrastructure Bridge, for the purposes of cross-certification or recognition of Certification Authorities, serves as the Government of Canada's Bridge Certification Authority.

Additional Information

For more information related to PKI, please refer to the website links listed below:

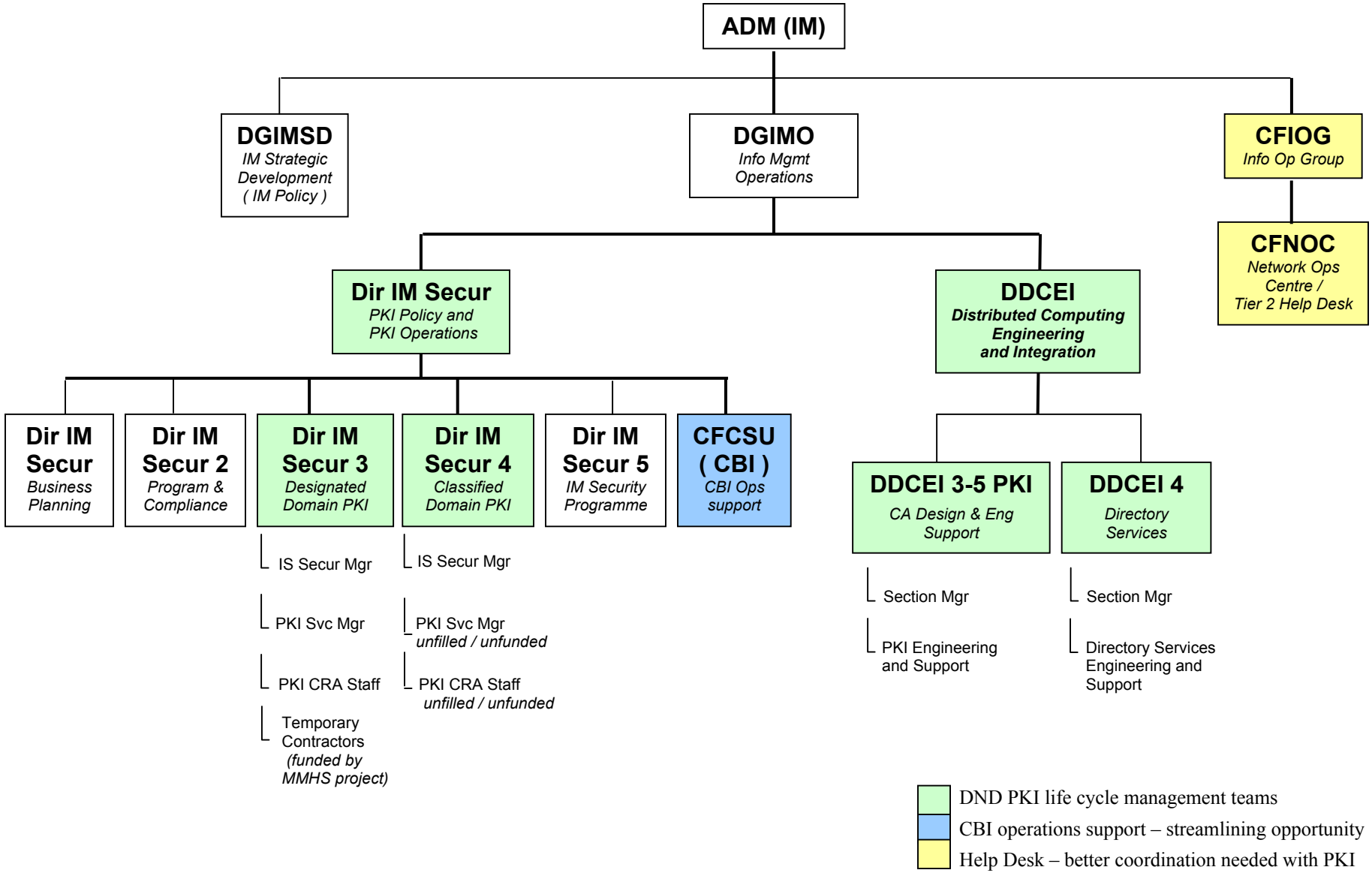
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-e.html (Chapter 19 of Handbook - Cryptography)

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/siglist_e.asp (GoC PKI Policy)

http://www.pkiforum.org/whitepapers.html (Miscellaneous PKI Whitepapers and Notes)

[31] CSE Canadian Handbook on Information Technology Security. March 1998. Section 19.1.1 – Symmetric Key Cryptography.
[32] TBS Policy for Public Key Infrastructure Management in the Government of Canada. Effective date: 26 April 2004. Section 4 – Definitions.

ANNEX B – "DND PKI" ORGANIZATIONAL CHART (SIMPLIFIED)



ANNEX C – LIST OF CURRENT AND PLANNED DND PKI-ENABLED APPLICATIONS

Current Applications	PKI Domain	Estimated number of users/certificates*	Target Service Date
SCEM *Secure Common Email*	Designated	Estimated 13,500-25,000 active certificates	Operational
MMHS *Military Message Handling System*	Classified	Estimated 5-10,000 certificates to be issued for 3,500 workstations	In pilot FSD 2005
Pending Applications	**PKI Domain**	**Expected number of users/certificates***	**Target Service Date**
CFHIS *CF Health Information System*	Designated	3,800 (800 of these will be contractors, some external)	Beginning Dec 2004
CFTS *Contracted Flying, Training and Support*	Designated	Maximum of 165 users at any time. Up to 327 trainees per year.	2005
DIHRS *Defence Integrated HR System*	Designated	Device certificates to support up to 7-8,000 users	2005
DVPNI *Secure Remote Access*	Designated	5-6,000+ active users	Beginning fall 2004
MASIS *Materiel Acquisition and Support System*	Designated	Estimated 5,000 users	Beginning late 2004
MHP *Marine Helicopter Program*	Designated	Initial use will require 50 users growing to 1,000 over a period of 4 years.	Beginning fall 2004
SAMPIS *Security and Military Police System*	Designated	1,100 users (Military Police) across Canada.	Possibly 2005

Source: *Project teams – information received during June to Aug 2004 timeframe.*

** With the exception of the MMHS, the estimated number of PKI certificates listed in the table above, do not necessarily represent the required number of PKI certificates to be issued. In most cases, if a user already has an existing PKI smartcard, it can likely be used for the pending PKI-enabled applications listed above. Since the MMHS is a classified system, a separate PKI smartcard must be issued.*

ANNEX D – WHAT IF A DEPARTMENTAL PKI WERE NO LONGER AVAILABLE?

Impact on current PKI users (i.e. SCEM):

Current users have told us that without PKI they would have to:

- Revert to paper processes and face-to-face meetings leading to inefficient use of time and resources; or
- Consider violating policy to send sensitive data in the clear risking potential embarrassment or exposure if disclosed.

Impact on pending PKI applications:

- There would be a serious impact on the rollout of pending applications such as the MMHS, DVPNI and CFHIS.
- An alternative solution would have to be found for strong Identification & Authentication.
- Communication of sensitive materials would be less efficient and IT security objectives would be harder to attain.
- PKI certificates could be obtained from an external CA service but potentially at a significant cost. There would also be a loss of control over the CA and a possible loss of sovereignty (e.g. if the CA was located outside Canada), which would be unacceptable, particularly in the case of the classified PKI.

Impact on future PKI requirements:

- Some senior DND officials have identified the need to work and exchange information securely with a number of other departments including TBS, Finance, Foreign Affairs and International Trade (DFAIT), and Justice. An externally hosted CA, such as the PWGSC/Secure Access Key Management Services (SAKMS), may be a viable alternative for obtaining PKI services, but DND would still have to maintain some registration activities and the associated costs.

- The GoC Compensation Web Application will be used by all GoC employees (~ 260,000 employees). Without a DND PKI (that has been cross-certified with the GoC PKI), employees will have to obtain a PWGSC/SAKMS or web certificate to access the Compensation Application or any new GoC PKI-enabled application including GoL services.

- In the future, DND may have cross-certification requirements with external organizations such as NATO, Department of Defence (DOD) or other allied groups. An external PKI service provider would not able to provide the security assurances required to be able to interact with these types of organizations, as the external service would not be able to support a higher level of security than medium assurance.

ANNEX E – GOOD PRACTICES AND LESSONS LEARNED FROM OTHER ORGANIZATIONS

Management and policy

- PKI must be driven by business applications – i.e. within the DND/CF, by needs for secure electronic data exchange.
- PKI is an infrastructure and must be implemented that way – i.e. as a common service to multiple systems/applications.
- PKI must be supported by senior management.
- PKI is complex and needs dedicated resources to ensure it functions as intended. There must be management understanding of the need for adequate resources to operate the system properly.
- A good Certificate Policy (CP) & Certification Practice Statement (CPS) are critical to ensure success and discipline.

Design

- PKI and security need to be integrated up-front at application design.
- Get a well-defined identity infrastructure in place first.
- Aligning the technology and approach for multiple PKIs (i.e. designated and classified systems) reduces maintenance and training requirements as well as the overall cost and effort of operating the system.

Registration

- Automation of registration is essential.
- Local Registration Authorities (LRAs) must be willing to serve. Consider having supervisors act as LRAs or add to another existing support structure as opposed to setting up a completely new one.
- Maintain regular contact with LRAs and ensure expectations are fully communicated.
- When identity credentials change (e.g. due to role change, employee movement or certificate revocation) there are many consequences and therefore, must be well managed.

Training

- Users do not read instructions – expect a high level of Help Desk calls.
  - The user interface must be clear so that the user understands what is happening.
  - Training for users can be quite informal and training is not a big issue after the initial roll-out
- Formal training is a must for PKI staff (LRAs, PKI officers etc).

Other

- Like e-mail, it is hard to measure return on investment for PKI, so business requirements must be well articulated, communicated and understood by stakeholders and senior management.

ANNEX F – LIST OF ACRONYMS AND ABBREVIATIONS

ADM(IM)	Assistant Deputy Minister (Information Management)
AEPOS	AEPOS Technologies Corporation
C&A	Certification and Accreditation
CA	Certification Authority
CBI	Certificate Based Infrastructure
CFCSU	Canadian Forces Crypto Support Unit (part of Dir IM Secur)
CFHIS	Canadian Forces Health Information System (project)
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CFTS	Contracted Flying, Training and Support (project)
COS ADM(IM)	Chief of Staff Assistant Deputy Minister (Information Management)
CP	Certificate Policy
CPS	Certification Practices Statement
CRA	Central Registration Authority
CRA	Canada Revenue Agency
CRAD	Chief Research and Development
CRS	Chief Review Services
CSE	Communications Security Establishment
DDCEI	Directorate of Distributed Computing Engineering and Integration
DFAIT	Department of Foreign Affairs and International Trade
DGIMO	Director General Information Management Operations
DGIMSD	Director General Information Management Strategic Development
DIHRS	Defence Integrated Human Resources System (project)
Dir IM Secur	Directorate of IM Security
DITSec	Directorate of Information Technology Security
DMHS	Defence Message Handling System (project)
DND	Department of National Defence
DND/CF	Department of National Defence and the Canadian Forces
DoD	Department of Defence (US)
DPM Secur	Deputy Provost Marshal Security
DS	Directory Services
DVPNI	Defence Virtual Private Network Infrastructure (project)
DWAN	Defence Wide Area Network (designated domain)
E-commerce	Electronic Commerce
FDA	Food and Drug Administration
FSD	Full-scale deployment
GAO	Government Accounting Office (US)
GoC	Government of Canada
GoL	Government On-Line
HR	Human Resources
HRMS	Human Resources Management System
IAP	Interim Authority to Process
ID	Identification
IT	Information Technology
LAC	Library and Archives Canada
LCPM	Life Cycle Product Management
LRA	Local Registration Authority
LRC	Local Registration Coordinator
MASIS	Material Acquisition and Support Information System (project)
MHP	Marine Helicopter Program (project)
MMHS	Military Message Handling System (project)
MP	Military Police
MSP	Message Security Protocol
NATO	North Atlantic Treaty Organization
NCR	National Capital Region
O&M	Operations and Maintenance
OLA(s)	Operational Level Agreement(s)
PB	Protected B
PKI	Public Key Infrastructure
PWGSC	Public Works and Government Services Canada
SAKMS	Secure Access Key Management Services (PWGSC)
SAMPIS	Security and Military Police Information System
SCEM	Secure Common Email (operational system)
SLA(s)	Service Level Agreement(s)
SOP(s)	Standard Operating Procedure(s)
TBS	Treasury Board Secretariat
TRA	Threat Risk Assessment
US	United States

ANNEX G – MANAGEMENT ACTION PLANS

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
A.	**Develop a PKI "roadmap"** that clearly defines and articulates DND's business and security requirements for an enterprise PKI. The "roadmap" should clearly demonstrate how and where PKI fits into the overall IT security framework in addition to defining the business requirements that PKI addresses for existing and future applications.	OPI: Dir IM Secur	Agree. Dir IM Secur should be lead for the development of a DND PKI roadmap for senior management approval. This is problematic, at present, due to resource limitations. To date, the US DoD PKI roadmap has been identified as a possible model for DND to follow. The DND roadmap will include a training and awareness program.
	❑ PKI should only be deployed in response to defined business requirements and a clear financial business case (or cost analysis).	OPI: Dir IM Secur OCI: IM Group Comptroller	Dir IM Secur will establish PKI requirements in consultation with departmental stakeholders. However, lack of personnel will adversely impact this activity. In addition, given the relative immaturity of large-scale PKI implementations, it is premature to develop a clear financial business case until a fuller appreciation of the benefits and costs can be determined.
	❑ A concerted effort must be made to increase departmental awareness and understanding of PKI use and capabilities.		
B.	**Manage PKI as a common departmental infrastructure program** and establish requisite/appropriate governance structures and strategic planning processes to provide overall direction, formally endorse PKI policies, and ensure that strategic-level voids and disconnects are minimized.	OPI: Dir IM Secur	Agree. It is proposed that PKI be managed as a common infrastructure program by establishing a governance framework and by integrating it into the existing key management framework. A DND PKI governance framework is proposed in a draft IMD, IMD 118 - PKI Governance, which is being prepared for ADM (IM) approval. DIMSP has already agreed to expedite the staffing of any PKI policy proposals as soon as they are received.

* **Note**: Only the Key Recommendations (alphanumeric serials) will be tracked by CRS on behalf of the Audit and Evaluation Committee (AEC). Sub-recommendations (bullet-points) are intended to provide additional guidance regarding the implementation of the Key Recommendations.

ANNEX G

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
	❑ Strategic-level plans related to merging the infrastructure support and processes for the different PKI and CBI systems as well as direction on the way ahead should be incorporated into the PKI "roadmap".	OPI: Dir IM Secur	Dir IM Secur 3 and CFCSU will study common activities and resources required by the current CBI and PKI Infrastructure (CBI/PKI study), and commonalities with existing cryptographic security and key management activities, in order to provide more streamlined processes that leverage on existing resources. The results will be documented in the DND PKI Roadmap.
C1.	**Update PKI policies and present for formal endorsement** to the appropriate departmental-level authority. At a minimum, the PKI policies should include the CP and CPS and a clear policy or directive on the requirement and use of PKI encryption and digital signatures.	OPI: Dir IM Secur OCI: DDCEI	Agree. Dir IM Secur will staff the existing GoC CP and DND CPS for ADM (IM) approval IAW the PKI governance framework.
	❑ Clearly define processes for development, maintenance, implementation, approval and promulgation of PKI policies.	OPI: Dir IM Secur OCI: DIMSP	PKI policy development, implementation and promulgation will be IAW DAOD 6000-0 and will be coordinated by DIMSP. Approval will be through the PKI Management Authority (PMA) IAW the PKI governance framework. DIMSP has already agreed to expedite any PKI policy proposals.
	❑ PKI SOPs (i.e. SCEM and MMHS desktop SOPs) should be revised to align with approved PKI policies.		It is proposed that development and maintenance of PKI SOPs will be included in the existing COMSEC document management framework.

ANNEX G

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
	❑ Perform a formal inspection to verify compliance with approved PKI policies (within a year of approval).	OPI: Dir IM Secur	Compliance inspections will be considered as part of the CBI/PKI study, and will consider including this as either part of certification and accreditation or as part of the COMSEC auditing process.
C2.	**Review and revise departmental PKI related-policies and procedures** such as the management and use of email, DND application of the LAC data holdings policy, information management etc.	OPI: Dir IM Secur OCI: DDCEI	Dir IM Secur and DDCEI will consult with the application owners for PKI enabled applications on application-specific policies and procedures.
	❑ Identify departmental PKI related-policies and procedures requiring revision.	OPI: Dir IM Secur	The PMA will be responsible for endorsing PKI management policy issues.
	❑ The policy owner or the PKI governance committee should approve any updated departmental PKI related-policies.	OPI: Dir IM Secur	IMOC will be responsible for endorsing direction on the use of PKI in departmental business processes.
D.	**Define, clarify, assign, document and communicate key roles and responsibilities** of PKI support groups for all aspects of PKI.	OPI: DGIMO OCI: Dir IM Secur DDCEI CFNOC	DGIMO will establish PKI responsibilities for the PKI support groups as part of the DGIMO realignment.
	❑ Separate PKI policy and evaluation from CRA responsibility.	OPI: Dir IM Secur	Dir IM Secur will realign internal Dir IM Secur 3 and CFCSU PKI roles once the CBI/PKI study is completed.
	❑ Combine central registration and certificate management activities for PKI and CBI (CFCSU) within a *single* CRA organization.		

ANNEX G

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
	❑ Ensure appropriate procedures are developed and in place before re-locating activities within one group.	OPI: Dir IM Secur OCI: PMA members	LRA/LRC processes will be addressed in policies and procedures to be promulgated by the PMA.
	❑ Strengthen controls over LRA/LRC processes and combine local registration activities for PKI and CBI at the local/base level (once processes have been streamlined and put in place).	OPI: Dir IM Secur	Roles and responsibilities will be documented in the DND PKI roadmap.
E.	**Strengthen, rationalize and optimize the separate PKI infrastructure support and processes,** particularly registration, training, and Help Desk, into a combined support structure with streamlined processes for the different PKI and CBI systems.	OPI: DGIMO	DGIMO will rationalize PKI support and processes as part of the DGIMO realignment.
	❑ Design and implement as much automation into the registration process as possible to improve overall efficiency.	OPI: Dir IM Secur OCI: DDCEI	DDCEI and Dir IM Secur will develop a resource plan for the stabilization of the PKI infrastructure for the Designated and Classified networks.
	❑ Develop a resource plan to identify the number of required resources to support effective, ongoing operation of the PKI system as a common departmental infrastructure.		

ANNEX G

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
	❑ Improve overall completeness, consistency and accuracy of the data required for the certificate management process by reviewing the composition and updating the processes and linkages of the various DND data repositories.	OPI: Dir IM Secur	Identity management data integrity issues will be addressed in direction to be staffed to the PMA, including OLAs with the appropriate HR and security clearance organizations. It should be noted that deficiencies in identity management processes in DND significantly impact, but are outside of the scope of, PKI.
	❑ Review the approach to PKI training and ensure that all training (for users, LRAs/LRCs and CRA staff) is appropriate, adequate and timely.	OPI: Dir IM Secur	It is proposed that the PKI support infrastructure include Training Development Officer (TDO) staff, in order to assess existing training and to determine future training requirements.
F1.	**Develop, gather, analyse, monitor and report operational performance metrics** on a regular basis to allow for performance assessment, budgeting, cost analysis and workload planning and balancing.	OPI: Dir IM Secur OCI: DGIMO	DGIMO will ensure that system performance monitoring and capacity planning for PKI infrastructure is addressed in the Divisional realignment. The organization responsible for managing the PKI infrastructure will gather and report on process (manual) statistics.
	❑ Develop a cost model for PKI as a common infrastructure program.	OPI: Dir IM Secur OCI: DDCEI	DDCEI and Dir IM Secur will develop a cost model as part of the resource plan for the stabilization of the PKI infrastructure. However, given the relative immaturity of large-scale PKI implementations, it is premature to develop an in-service cost model until a fuller appreciation of the overall costs can be determined.
F2.	**Develop, negotiate and implement up-to-date OLAs** between central PKI operational groups **and SLAs** with new PKI applications.	OPI: DGIMO OCI: PMA	The DGIMO cell responsible for OLAs and SLAs will ensure that PKI related OLAs and SLAs are drafted and staffed to the PMA.

ANNEX G

Serial	CRS Recommendation	OPI/OCI(s)	Management Action Plans
G.	**Identify / establish a new "business analyst" role to liaise with users and functional groups** and foster communication. The goal is to develop a solid understanding of the existing business processes and PKI requirements to determine how to best integrate PKI technology and achieve desired results (e.g. operational efficiencies and cost savings).	OPI: Dir IM Secur OCI: PMA PAC	Dir IM Secur will provide introductory PKI training to their analysts and PMA PKI Advisory Cell (PAC) members, in order to identify enterprise level opportunities and implications of possible, or proposed, PKI enabled solutions.

As previously stated in the **Results in Brief** section of the report, CRS encourages that certain actions be set in motion earlier than currently planned, particularly, in regards to the:

- development of a DND PKI Roadmap (serial A);
- clarification of DND PKI support group roles and responsibilities (serial D); and
- rationalization of separate PKI infrastructure support and processes (serial E).