Government of Canada Public Key Infrastructure

White Paper

February 1998

MG - 15a

FOREWORD

To facilitate electronic commerce nationally and internationally and to achieve its goal of conducting business electronically whenever possible, the federal government is embarking on the implementation of a Public Key Infrastructure (PKI). In order for electronic transactions to be seamless across Canada, it is important that similar infrastructures, policies and standards be adopted nationally.

This White Paper begins with an overview of the practice of public key cryptography, and outlines its link to electronic commerce. It then provides an introduction to the underlying concepts of a PKI, which include: third-party trust; certification authority; certificates; and cross-certification.

Once the required conceptual framework has been built, there is a discussion of the PKI that the Government of Canada (GoC) will adopt. The reader will learn about: the GoC PKI architecture and its main components; the Policy Management Authority; the role of industry in its delivery; the open commercial standards, protocols and cryptographic algorithms upon which it is based; and legal issues relating to the security of electronic information. Suggestions are provided for those who choose to proceed with the implementation of a PKI today.

This Paper presents the benefits, to organizations and to the funding federal government departments, of building a PKI that is compatible with the GoC PKI.

Note: Portions of this text have been reproduced with permission of Entrust Technologies Inc. Entrust is a registered trademark of Entrust Technologies Inc. All Entrust product names are trademarks of Entrust Technologies Inc.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. ENVIRONMENT

1.1 Introduction

The world is increasingly turning to the digital medium, and in particular to the Internet, as a tool for conducting business. However, in order to conduct business over the Internet, a secure environment must be established.

As the Government of Canada (GoC) moves toward electronic commerce, and achieving its goal of conducting business electronically whenever possible, it is embarking on the implementation of a public key infrastructure (PKI). In order for electronic transactions to be carried out seamlessly across the country, it is important that similar infrastructures, policies and standards be adopted. Public key cryptography can help provide a secure environment for the exchange of business-related and other sensitive information, between organizations as well as between individuals.

1.2 Background

Cryptography as a discipline is centuries old. Awareness of cryptography has increased, though, with the broadened use of computers and increased access to unsecure networks such as the Internet. Cryptography permits the safe exchange of private and confidential information. Plain language text is converted into unintelligible text (encryption) in order to transmit that content from one workstation to another. On the receiving end, the encrypted text is reconverted into intelligible form (decryption).

Cryptography can also be used to provide authentication, non-repudiation and integrity of information through the use of a special form of cryptography called a digital signature. A digital signature, can guarantee the origin and integrity of the information that has been exchanged, and provides a method by which the authenticity of the document can be confirmed.

Today's widespread reliance on more complex and increasingly more multitasking computer networks to conduct personal and corporate business has underscored the need for adequate security. These applications can benefit from the flexibility and robustness which public key cryptography provides.

1.3 Public Key Cryptography

Conventional cryptography uses a single mathematical "key" for both encryption and decryption of data. A secure message to an addressee is encrypted using a key known only to the sender and the recipient. Both the key and the encrypted message are passed to the recipient, so that the message can only be decrypted by the intended recipient. Conventional cryptography is known as symmetric cryptography.

Public key cryptography uses two keys. One key is kept private, and the other key is made public. The public key is used to encrypt a message, and the private key is used to decrypt the message. In

other words, to send an addressee a message, the message is encrypted with the addressee's public key, and then passed to the addressee. The addressee can use the private key to decrypt the message.

1.4 Digital Signature

Public key cryptography makes digital signatures possible. These signatures can be used to substantiate the origin of a message. To "sign" a message, a mathematical function is used to produce a unique summary of that message. This summary is then encrypted using the sender's private key. The result, referred to as a digital signature, is then appended to the message. The addressee can confirm both the origin of the message, and the integrity of the information therein, by decrypting the digital signature using the originator's public key, and comparing the result with a summary produced by passing the received message through the same mathematical function. While it sounds complicated, in practice the entire process can be as simple as selecting an icon on a computer screen.

A PKI manages the generation and distribution of public/private key pairs, as well as the certificates used to provide confidence in the validity of the keys. Although in principle public keys are available to anyone, it is important that their authenticity and ownership be verified by a PKI.

1.5 Link to Electronic Commerce

A PKI is a vital element of national electronic commerce; it ensures the security of electronic transactions, and the exchange of sensitive information between parties that do not have a prior established business relationship.

The economic and social benefits of the information highway can never be fully realized without the underpinnings of a security infrastructure. Security is a fundamental requirement for electronic business applications, such as: private e-mail; purchase orders; the transmission of credit card information; workflow automation using signature-based forms; and legally binding contracts; electronic commerce by protecting corporate and personal information, and by ensuring that electronic transactions are valid and binding.

All Canadians, including businesses, consumers and individual citizens, will benefit from the implementation of a PKI that supports seamless electronic transactions which can be trusted by everyone.

1.6 Infrastructure Requirements

To enable seamless and trustworthy electronic business transactions, an infrastructure is needed that supports a common set of security services in a standard fashion. This in turn supports wide-scale interoperability, and the realization of the full capabilities of all technologies used in business applications. For example, bank or credit card statements could be exchanged securely over open networks if the appropriate security infrastructure were in place. Secure e-mail services could be supported that would prevent interception by unwanted parties and would also allow originators

and recipients to verify each other's identity. Electronic Data Interchange (EDI) could be used to support the exchange of electronic forms in a secure manner. Financial transactions could be digitally signed and verified at the intended destination in a reliable fashion. Secure electronic commerce is possible on a global scale once a common set of security infrastructure standards are agreed upon by trading partners.

2. DEFINING PUBLIC KEY INFRASTRUCTURE

2.1 Public Key Infrastructure

A PKI enables secure electronic transactions, and the exchange of sensitive information, through the use of cryptographic keys and certificates (see Section 2.4). A PKI provides: confidentiality; access control; integrity; authentication; and non-repudiation services for electronic commerce transactions, and for their supporting information technology applications. A PKI manages the generation and distribution of public/private key pairs, and publishes the public key (along with the user's identification) as "certificates" on open bulletin boards (such as X.500 directories).

A PKI is defined as a:

- Certification Authority
- Certificate Repository
- Certificate Revocation System
- Key Backup and Recovery System
- Support for Non-Repudiation
- Automatic Key Update
- Management of Key Histories
- Cross-certification
- Timestamping
- Client-side software interacting with all of the above in a consistent, trustworthy manner.

A PKI provides a high degree of confidence that: private keys are kept secure; specific public keys are truly linked to specific private keys; and the parties holding public/private key pairs are who they say they are.

2.2 Third-party Trust

Third-party trust refers to a situation in which two entities or individuals implicitly trust each other, even though they have not previously established a business or personal relationship. In this situation, the two parties implicitly trust each other because they each share a relationship with a common third party, and that third party vouches for the trustworthiness of the first two parties.

Third-party trust is a fundamental requirement for any large-scale implementation of security services based on public key cryptography. Public key cryptography requires access to a user's public key. In a large-scale network, however, it is impractical and unrealistic to expect that each user will have previously established relationships with all other users. In addition, because a user's

public key needs to be widely available, the association between a public key and a specific individual must be guaranteed by a trusted third party, in order to prevent impersonation of legitimate users. A trusted third party, operated in a secure manner, allows users to implicitly trust any public key certified by that third party.

A third-party certification agent is referred to as a "Certification Authority" (CA).

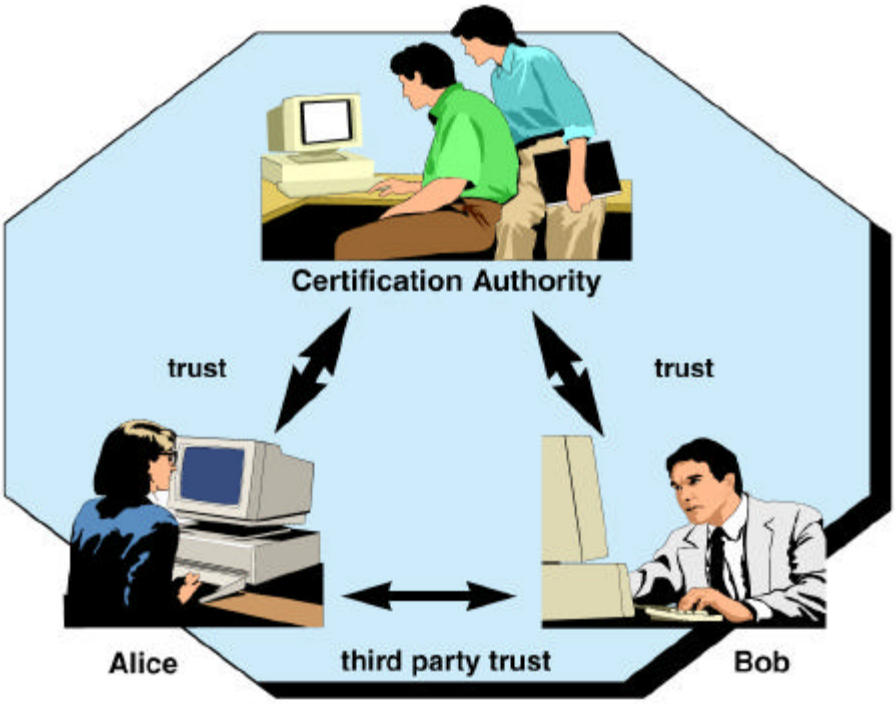

Figure 1 – Third-party Trust Through a Certification Authority

2.3 Certification Authority

A CA is a trusted entity whose central responsibility is certifying the authenticity of users. In essence, the function of a CA is analogous to that of the passport-issuing office in a government. A passport is a citizen's secure document, issued by an appropriate authority, that certifies that the citizen is who he/she claims to be. It is effectively that person's "paper identity". Any country trusting the authority of the first country's government passport office will trust the citizen's passport; this is a good example of third party trust.

Similar to a passport, a network user's "electronic identity", issued by a CA, is proof that the user is known by the CA. Therefore, through third-party trust, anyone trusting the CA can have confidence in the user's identity. The criteria to establish CAs, and the policies under which they operate, are paramount in determining the level of trust placed in them.

2.4 Certificates

A network user's certificate is the electronic equivalent of his/her passport. It contains information that can be used to verify the identity of the owner (such as the owner's name). A critical piece of information contained in a user's certificate is that owner's public key. A public key may be used to either encrypt data destined for the certificate owner, or to verify the owner's digital signature.

There are numerous "trust" issues regarding certificates. A critical one relates to how the information in a certificate is secured: how can anyone trust that the name and the public key in a certificate actually belong to the certificate's alleged owner? Indeed, without this level of trust, public key cryptography is not reliable, since there would be no assurance that information is being encrypted for the correct person, or that a digital signature can be associated with a specific individual.

To establish trust in the binding between a user's public key and other information (for example, the user's name) in a certificate, a CA digitally signs the certificate information using its private signing key. The CA's digital signature provides three important elements of security and trust to the certificate. First, by definition, a valid digital signature on a certificate is a guarantee of the certificate's integrity. Second, since the CA is the only entity with access to its private signing key, anyone verifying the CA's signature on the certificate is guaranteed that only that CA could have created and signed the users certificate. Third, since only the CA has access to its private signing key, the CA cannot deny having sign the certificate. This is a concept often referred to as non-repudiation.

2.5 Cross-certification

Cross-certification is simply an extended form of third-party trust. It is a process in which two CAs securely exchange cryptographic keying information, so that each can effectively certify the trustworthiness of the other's keys. From a technical perspective, the process involves the creation of "cross certificates" between two CAs. When a CA in one organization and a CA in a second organization cross certify, the CA in the first organization actually creates and digitally signs a certificate containing the public key of the CA in the second organization. In a similar manner, the second organization creates and signs a certificate containing the public key of the CA in the first organization. Consequently, users in either CA domain are assured that each CA trusts the other. Therefore, users in one CA domain can implicitly trust users in the other CA domain.

Since cross-certification extends third-party trust, it is important that each CA domain, in addition to exchanging cryptographic keying information, be completely comfortable with the other domain's security policies and practices which it employs in issuing certificates and in carrying out its operations.

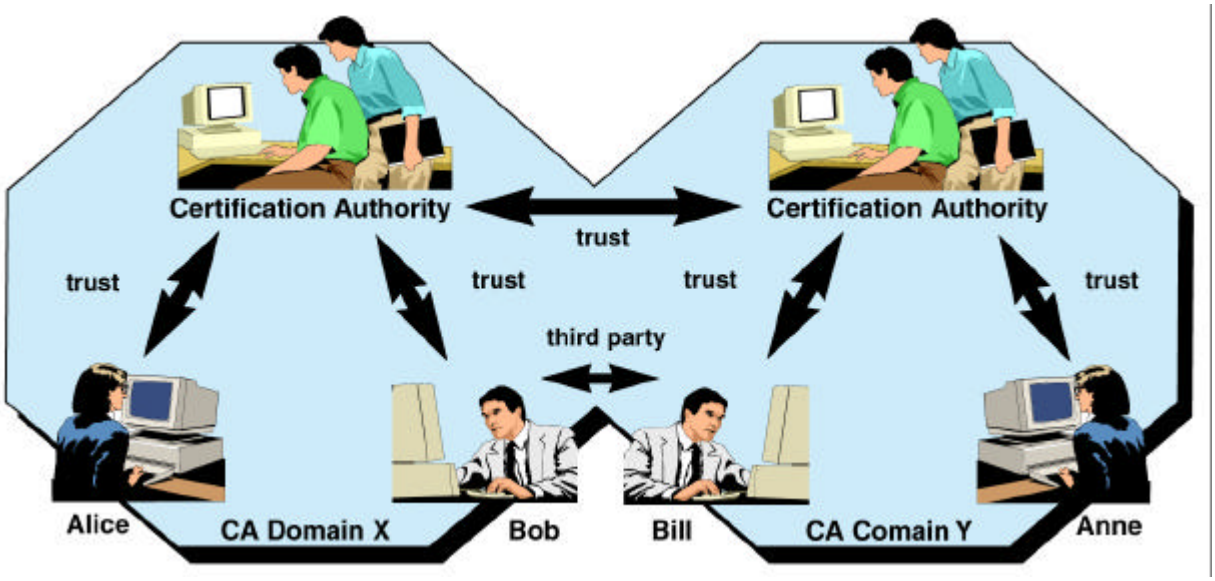

Figure 2 – Extended Third-party Trust Through Cross-certification

3. IMPLEMENTING A GOVERNMENT OF CANADA PUBLIC KEY INFRASTRUCTURE

3.1 Project Initiation

Privacy and the security of information highway transactions was one of the underlying principles of the Canadian information highway strategy. This issue was explored by the Information Highway Advisory Council (the Council), which in its September 1995 report recommended that:

- the federal, provincial and territorial governments work together to address the principal legal, trade control and security-related issues that may be impeding the use of electronic commerce in the government, the private sector and in international trade;
- the GoC work in partnership with provinces, territories, the private sector and other stakeholders to develop mutually acceptable security standards and promote the widest acceptance of these, both within Canada and with international trading partners so as to facilitate the free flow of information; and
- governments, private sector service providers, users, privacy advocates and other information highway stakeholders work together to develop and implement the policies and framework for a security infrastructure to support Canada's information highway.

The Council called on the GoC to use its proposed PKI initiative to capitalize on Canada's private sector strengths in the security field, in order to implement such an infrastructure, and to thereby catalyse private sector action. The Council also called on the Government to continue working with the private sector to develop compatible PKI policies and cross certification practices, in order to ensure interoperability with national and international entities.

In December 1995, the GoC launched a PKI project involving six departments. The resulting PKI will allow the federal government to: provide more efficient delivery of services to Canadians; facilitate secure electronic commerce; and better protect the confidentiality and privacy of information used within the federal government. Its full scale implementation is planned for 1998.

3.2 Government of Canada Public Key Infrastructure Overview

The GoC PKI will provide key management processes to support confidentiality and digital signatures in business applications across government. The GoC PKI will facilitate a seamless security solution, for the integration of the various technologies used in the Government's information management and electronic commerce applications. A uniform GoC PKI will allow cost-effective security to be provided to a full range of applications, thus avoiding the need to support different security architectures for each application.

The GoC PKI is comprised of the following components:

- Policy Management Authority (PMA);
- Canadian Central Facility (CCF),
- Certificate Authorities (CAs); and
- Local Registration Authorities (LRAs).

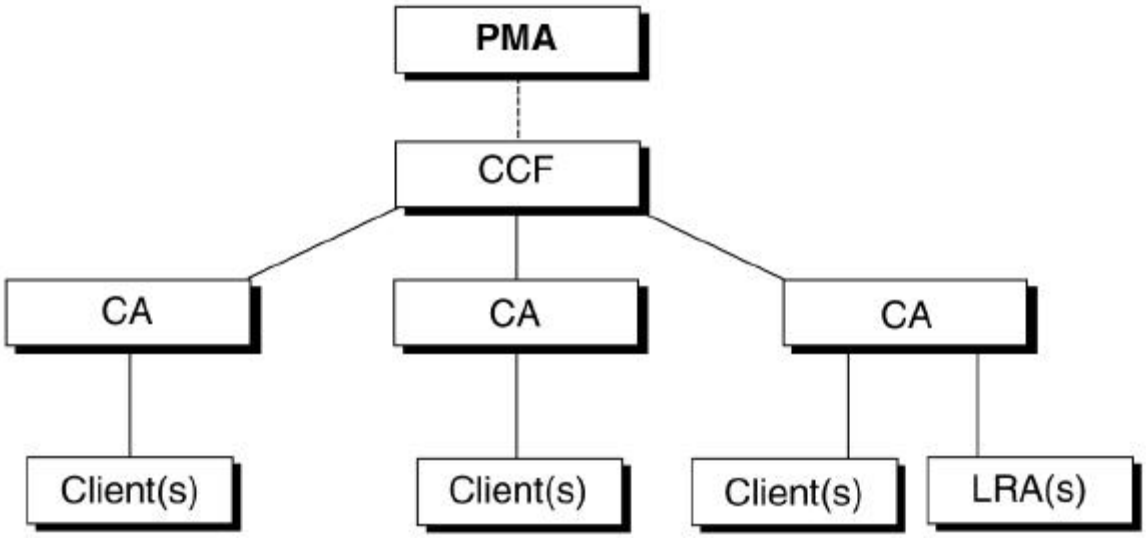

Figure 3 – Government of Canada Public Key Infrastructure

The PMA is an interdepartmental committee, chaired by the Treasury Board Secretariat. The role of the PMA (see Section 6.1) is to oversee the development of policy for the operation of the GoC PKI.

The CCF is the central certificate authority, which implements GoC PKI policies, and which provides a common point for cross-certification with external organizations (such as other national governments, other jurisdictions and private sector communities of interest). It is the only GoC PKI "level 0" certificate authority. It will be located in Ottawa. The CCF's main functions are to:

- certify all GoC PKI "level 1" Certificate Authorities;
- certify external PKIs, as requested by the PMA;
- post certificates and Certificate Revocation Lists (CRLs) to directories;

- archive all certificates and CRLs generated by itself and by GoC PKI Certificate Authorities; and
- archive CCF-level audit journals, and archive potentially sensitive audit data generated by subordinate certificate authorities (only if required by their own local security policies).

Certificate authorities are operated by departments within the government. Each certificate authority is responsible for the administration of a specific set of encryption entities, digital signature entities, LRAs and/or subordinate GoC PKI certificate authorities. Responsibility for the operation of a certificate authority will be assigned to a particular department, organization, agency, group or section. A certificate authority will issue public key certificates and lists of certificates which have been revoked. Certificate authorities at "Level 1" are immediately subordinate to the CCF. Certificate authorities at "Level 2" are directly subordinate to "level 1" certificate authorities, and may be deployed depending on the business requirements of a given department.

The primary function of an LRA is to identify and register public key certificates of their users. LRAs are operated by departments. They help to bridge the gap between the end-user and their own certificate authority when these are geographically separate from one another. They are subordinate to a designated certificate authority. Any number of LRAs may be deployed depending on the requirements of the department. They provide local access to a subset of the certificate authority functionality. They cannot directly perform certificate authority services such as issue certificates or certificate revocation lists. The LRA will:

- assist in registering, de-registering and changing attributes of subordinate end entities;
- confirm the identity of end users associated with the end entities;
- authorize requests for confidentiality key recovery or certificate recovery;
- accept and authorize requests for certificate revocations;
- physically distribute personal tokens to, and recover obsolete tokens from, individuals authorized to hold them; and
- register, de-register and assign privileges to local LRA personnel.

4. INDUSTRY PARTICIPATION

4.1 Entrust Technologies Inc.

Entrust Technologies Inc. (formerly Nortel Secure Networks) was awarded a development contract to add significant capabilities to the Entrust product line to meet the GoC PKI requirements. Entrust Technologies Inc. is one of the world's leading developers in public key cryptography, security architectures and international standards. Entrust products are used throughout financial, government and high technology sectors and have been selected as the security technology by companies such as IBM, Tandem and Hewlett-Packard.

The GoC PKI will be based on the Entrust family of software security products for fully automated key management, digital signature and encryption. These products provide a single security infrastructure that can be shared across a variety of applications. Entrust works on any size client/server network and on Windows, Macintosh or UNIX platforms. High-level application programming interfaces (APIs) also allow easy integration with applications such as e-mail, electronic funds transfers, and database transactions. Additional features include support for a range of optional hardware tokens.

4.2 Third-party Product Vendors

Applications (such as e-mail) become "Entrust-ready" through the use of one of the various Entrust Toolkit products, a family of high-level security APIs produced by Entrust Technologies Inc. These APIs provide access to the key management functions and cryptographic algorithms that provide encryption and digital signature services to applications. There is a growing number of third-party product vendors that are making their products "Entrust-ready". Two such product vendors are SAGUS Security Incorporated, and Chrysalis-ITS.

SAGUS Security Incorporated products form an integrated suite that enables organizations to deploy security on an enterprise-wide basis. Currently, organizations must buy separate products to incorporate security at each level of communication (desktop, network, server, mainframe) and manage security tools at every level. SAGUS products provide a seamless overlay to support all communications through existing applications in a transparent manner. Security functions are invoked automatically through standard TCP/IP-based networking protocols so they are invisible to users and do not affect systems applications or architecture. SAGUS Security products provide security solutions for telework and mobile computing, client server applications, database access, e-mail, and work flow. The products support portability on multiple hardware platforms (including desktop, client server and mainframe) in a completely open systems architecture. The basis for encryption and digital signature function in SAGUS Security products is the Entrust toolkit.

Chrysalis-ITS develops the Government Electronic Services Card (GESC), which is a standards-based, Type II PCMCIA token, that provides encryption, decryption and secure digital signature functions in a portable device. Designed to FIPS 140-1 Level II, GESC is compatible with Entrust, and with all Entrust-ready applications. The GESC may be used with any workstation or laptop

computer equipped with the appropriate Entrust software and a PCMCIA card reader. The GESC provides users with a higher level of security than they could obtain using software alone, since all cryptographic operations take place on the card, and not on a user's unsecured computer. The cryptographic algorithms supported by GESC are:

- Symmetric Key Encryption: CAST, DES, Triple DES, RC2 and RC4. Secret key generated on the card;
- Asymmetric Key Encryption: RSA (up to 1024 bit modulus);
- Digital Signature: RSA (up to 1024 bit modulus). The key pair is generated on the card. The private key cannot be extracted; and
- File Hashing: MD2, MD5 and SHA-1.

A list of other Entrust-ready applications is provided in Section 12.

5. OPEN STANDARDS FOR THE GOVERNMENT OF CANADA PUBLIC KEY INFRASTRUCTURE

The GoC PKI is based on open commercial standards, protocols and algorithms. The standards employed in the GoC PKI include the following.

5.1 Cryptographic Security

- FIPS 140-1: Security Requirements for Cryptographic Modules; and
- CEAP: Cryptographic Endorsement and Assessment Program.

5.2 Cryptographic Algorithms

- Symmetric Algorithms:
- DES (Data Encryption Standard), 64 bits
- Entrust Technologies CAST, 128 bits;
- Asymmetric Algorithms
- RSA/MD5 and RSA/SHA-1 for Digital Signatures, 512/1024 bit keys; and
- FIPS PUB 180-1 and 186: DSA/SHA US Digital Signature Standard;
- RC2, MD2 and 3DES.

5.3 Communications Protocol and Data Formatting

- RFC 1777 LDAP (Lightweight Directory Access Protocol);
- ISO/IEC 8824 and 8825 ASN.1 notation;
- S/MIME Message Specification: PKCS Security Services to MIME;
- PEM (Privacy Enhanced Mail);
- MSP (Message Security Protocol);
- Independent Data Unit Protection (IDUP), GSS API, Internet Draft; and
- GSS API, RFC 1508.

5.4 Network

- TCP/IP.

5.5 Infrastructure

- X.500 Directory Services, and support for other directories or repositories that have LDAP interfaces.

5.6 Public Key Infrastructure

- X.509 v3 Certificates;
- Simple Public Key GSS-API Mechanism (SPKM), RFC 2025;
- MISPC (Minimum Interoperability Specification for PKI Components);
- Secure Exchange Protocol (SEP);
- IETF PKIX:
    - Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile;
    - Internet Public Key Infrastructure Part III: Certificate Management Protocols; Certificate Policies and Certification Practice Statements Framework; and Certificate Management Services Application Programming Interface (CMS-API), Issue 2.0.

6. POLICY DEVELOPMENT

6.1 Policy Management Authority

Under the leadership of the Treasury Board Secretariat, work is in progress to determine and address the policy, management and infrastructure requirements of the Government's PKI initiative. This work is being carried out under the auspices of the PMA, an interdepartmental committee that oversees the development of policy for the operation of the GoC PKI. Included in the role of the PMA is the development of appropriate policies for GoC PKI operation within the federal government, and the approval of cross-certification agreements and policy mapping between the GoC PKI and external PKIs.

The PMA Committee has been promoting the development of a framework to assist in the writing of certificate policies and certification practice statements for the GoC PKI. An initial framework approach was presented in the report, *Certificate Policy and Certification Practice Statement Framework*, Version 1.2b, 12 November 1996.

The PMA Committee has also been promoting collaboration with the U.S. federal government, with a view to ultimately achieving a common framework and, if practical, common or optimally compatible certificate policy definitions and certification practice statements. This collaboration resulted in the preparation of the *Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework* (co-authored by Santosh Chokhani, Ph.D. and Warwick Ford, Ph.D.), which was published as an Internet draft in September 1997. This draft outlined the full range of topics that potentially need to be addressed in a certificate policy definition or in certification practice statements.

In order to test the validity and utility of such a framework, the PMA, working collaboratively with the U.S. National Security Agency and the National Institute of Standards and Technology, produced a "straw man" certificate policy definition. The goal of this document is to describe a policy which provides a "medium level" of assurance for the certificate practices described. The Chokhani and Ford document constitutes the first draft of such a straw man certificate policy definition.

The following draft documents are, or will soon be, available for review:

- CHOKHANI, and W. FORD, *Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Draft*, September 1997, available at http://www.ietf.org/html.charters/pkix-charter.html;
- Government of Canada, *Certificate Policy and Certification Practice Statement Framework*, Version 1.2b, November 1996;
- Model Certification Practice Statement (work underway); and
- Warwick FORD, *Straw man Certificate Policy Definitions: Mid-Level Policies for Digital Signature and Encryption*, December 1996, available at http://www.magnet.state.ma.us/itd/legal.

7. LEGAL ISSUES RELATING TO THE SECURITY OF ELECTRONIC INFORMATION

A Legal Issues Working Group was created by the Information Technology Security Strategy Steering Committee of the Council for Administrative Renewal. Its mandate was to identify and address legal issues (identified by the Steering Committee and associated working groups) concerning the federal government's information technology security (ITS) strategy.

Two of the objectives set forth for this working group were: to provide legal opinions with regard to existing Canadian law; and to make recommendations for legislative amendment to accommodate the federal government's ITS strategy. The working group examined the legal issues relating to the security of electronic information held by the federal government generally, and summarized the requirements of the critical statutory and policy obligations.

Legal issues relating to electronic security are important with regard to three distinct types of applications: records management; financial transactions; and electronic communications. The major security issues (arising out of the various topics surveyed by the Working Group) which should be addressed when implementing these applications include:

- obligations to create, preserve and control electronic information;
- collecting and sharing personal information;
- securing government-held commercial information;
- liability for unauthorized disclosure of confidential information;
- integrity and accuracy of published government information;
- criminal misuse of information technology;
- computer searches and privacy;
- electronic records and evidence;
- digital signature, confidentiality encryption and public key infrastructure; and
- procurement of secure technologies.

A copy of the final report of the Legal Issues Working Group is available on the federal Department of Justice Web site (http://www.canada.justice.gc.ca).

8. FUTURE DIRECTIONS

8.1 The Government of Canada Public Key Infrastructure Contract

The Entrust product line forms the developmental baseline of the GoC PKI. A development contract has been established with Entrust Technologies Inc., to add large-scale PKI capabilities to the Entrust product line.

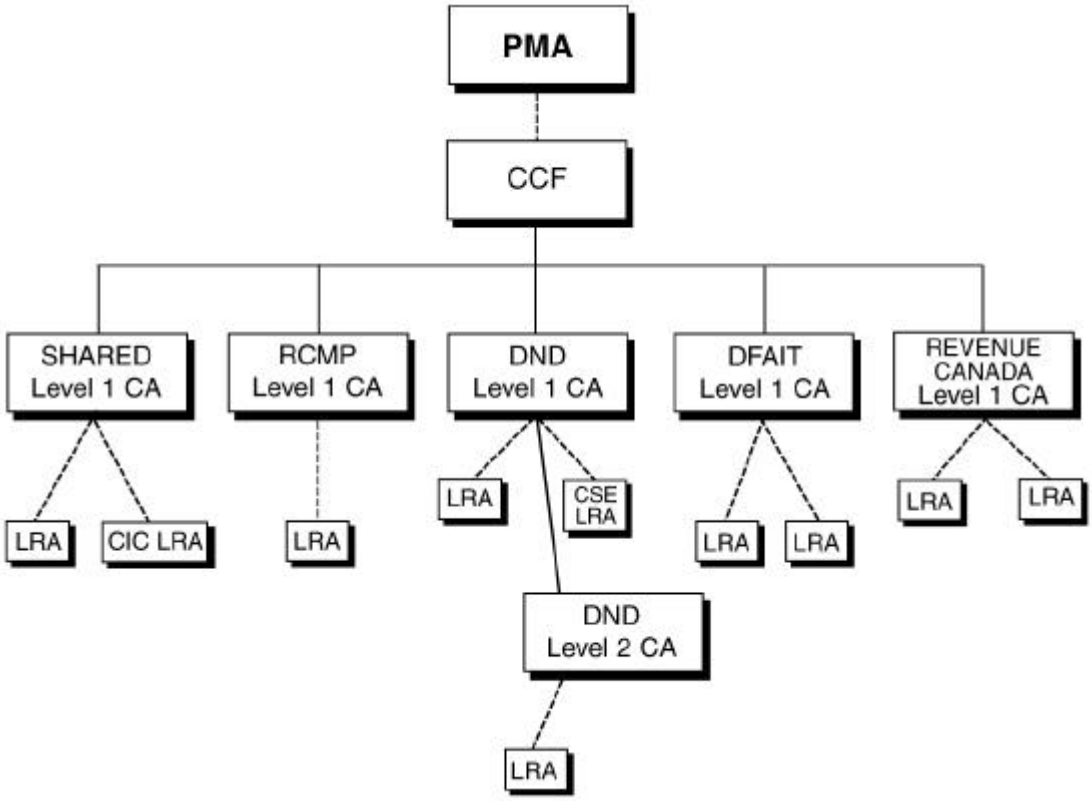

Figure 4 – Initial Government of Canada Public Key Infrastructure Architecture, for Test and System Acceptance.

The GoC PKI project will benefit from the major enhancements to the core Entrust product line;

- CA key pair update;
- a hardware cryptographic processor module;
- LRA components that facilitate the efficient extension of the PKI system across government departments;

- improvements to Entrust's support for non-repudiation to facilitate on-going administration;
- CA networking features to simplify cross-certification and management of a network of Certificate Authorities; and
- monitoring of network security status.

The project includes development, security endorsement, and certification and accreditation of these enhancements, in order to satisfy GoC business requirements.

In addition to software development, the GoC PKI project encompasses the technology evaluation, selection, testing, and delivery of numerous third party technology components, including:

- computing servers for the CCF and Certificate Authorities;
- network protection devices (such as firewalls);
- X.500 directories; and
- hardware cryptographic processors for the CCF and for Certificate Authorities.

9. IMPLEMENTING AN INTERIM PUBLIC KEY INFRASTRUCTURE TODAY

9.1 Building a Public Key Infrastructure

Organizations can employ a PKI to accelerate the introduction of electronic commerce and the sharing of electronic information, according to their business needs. Even though the GoC PKI won't be fully implemented until 1998, it is being developed using the Entrust suite of products as a baseline. This allows Government departments, other jurisdictions, and private sector firms to use the Entrust product line immediately, in order to provide users with the capability to secure local files and network communications for electronic business applications such as e-mail, forms, data interchange, database access, and Web interactivity. Since Entrust Technologies Inc. will enhance its suite of products to meet the GoC PKI requirements, technology migration will be possible from existing Entrust-based PKI implementations.

9.2 Government Telecommunications and Informatics Services

The Government Telecommunications and Informatics Services (GTIS), a branch of Public Works and Government Services Canada (PWGSC), has implemented an Entrust-based PKI in order to provide improved security for a variety of common applications. This service is available to federal organizations which do not want to operate their own PKI. The current plan is for the GTIS to integrate with to the GoC PKI, when the latter system becomes operational.

9.3 Participating in the Government of Canada Public Key Infrastructure

Federal government departments which already have PKIs (or which are planning to build PKIs in the near term) can share in the benefits of the GoC PKI (refer to Section 10.2), by joining the strategic partnership which funds the GoC PKI project.

Federal government departments with longer term requirements should ensure that new systems with potential application across the Government will be served by, and will interoperate with, the GoC PKI.

9.4 Other Governments and the Private Sector

Other governments and the private sector are encouraged to investigate implementation of the GoC PKI technology baseline, standards, policies, and practices described above. This will help achieve compatibility and security of electronic commerce transactions.

10. BENEFITS

10.1 Benefits of a GoC PKI-compatible Security Infrastructure

The benefits available to each organization involved in a GoC PKI-compatible security infrastructure include:

- a security functionality and architecture that can be scaled to cover an entire organization, and that will enable the deployment of specific services to business and trading partners, customers and citizens;
- confidentiality and digital signature services across the organization;
- open, non-proprietary APIs, which ensure that a broad range of third-party vendors will be able to develop and market security and electronic commerce products that are compatible with the GoC PKI;
- policy guidance documentation, to aid in the management of the CCF and of the departmental CAs; these documents include the Policy Management Authority (PMA) Guidance document, and the Inter-departmental Certificate Policies and Certification Practice Statement Guide; and
- Cryptographic Endorsement and Assessment Program (CEAP) security endorsement by the Communications Security Establishment (CSE), to ensure that security functions are provided in a way that satisfies government requirements and facilitates security certification by individual user departments.

10.2 Benefits to GoC PKI Funding Departments

The benefits available to GoC PKI funding departments include:

- departmental CAs that operate effectively in a multi-CA network;
- license migration to the enhanced Entrust PKI product, which fully meets government requirements;
- five LRA licenses for each GoC PKI CA;
- GoC PKI requirements that are developed into commercial, off-the-shelf versions of the Entrust product family, thus reducing in-service phase maintenance and support costs;
- cost-reduced licenses for participating departments that may not have deployed Entrust technology to date; and
- training.

11. FEDERAL INVOLVEMENT

A number of federal government departments and agencies are contributing towards the development of the GoC PKI, and introducing the Entrust baseline technology to their departments. They include: Citizenship and Immigration Canada; Communications Security Establishment; Department of Foreign Affairs and International Trade; Department of National Defence; Government Telecommunications and Informatics Services, a branch of Public Works and Government Services Canada (PWGSC); Health Canada; Revenue Canada; Royal Canadian Mounted Police; and Treasury Board Secretariat.

All federal organizations are encouraged to become funding partners, in order to help advance GoC PKI development, and to realize the early benefits of this technology, which provides the fundamental underpinnings for electronic commerce.

12. HARMONIZATION AND COOPERATION

Harmonized government decisions with respect to security policy, technical standards and infrastructure will facilitate the electronic delivery of GoC programs and business services. A uniform set of requirements and structures will provide a larger market for Canadian private sector suppliers, and will simplify the public's interaction with the Government. As other jurisdictions and private sector organizations adopt public key infrastructures based on common standards, seamless and secure electronic commerce on a national and international basis will be enabled.

Table 1 – Entrust-ready Applications

Application	Product	Vendor	Forecast	Platform
E-forms	Informed 1.4	Shana	Available now	Macintosh
E-forms	Informed 2.0	Shana	1Q97	Macintosh, Windows
E-forms	FormFlow 2.0	JetForm	Available now	Windows
E-forms	FormFlow 2.1	JetForm	Available now	Windows
E-forms	JetForm Filler	JetForm	2Q97	Windows, Windows NT
E-forms	JetForm Filler Pro	JetForm	2Q97	Windows, Windows NT
E-mail	Integrated Security Agent for BeyondMail	Zoomit	Available now	Windows
E-mail	Integrated Security Agent for SharkMail	Zoomit	Available now	Windows
E-mail	Integrated Security Agent for MailMan	Zoomit	Available now	Windows
E-mail	Integrated Security Agent for GroupWise	Zoomit	To be determined	Windows
E-mail	ArmorMail Add-On for MS Mail	LJL Enterprises	Available now	Windows
E-mail	ArmorMail Add-On for camail	LJL Enterprises	Available now	Windows

Application	Product	Vendor	Forecast	Platform
E-mail	ArmorMail Add-On for cc: Mail V6.0	LJL Enterprises	To be determined	Windows
E-mail	ArmorMail Add-On for Eudora Mail	LJL Enterprises	To be determined	Macintosh
E-mail	ArmorMail add-on for Outlook with S/MIME	LJL Enterprises	Available Now	To be determined
E-mail	ArmorMail add-on for Outlook Exrepss with S/MIME	LJL Enterprises	Available Now	To be determined
E-mail	QuickMail	CE Software	To be determined	Macintosh, Windows
E-mail	SecretAgent	Information Security Corp.	Available Now	Windows, Windows NT, UNIX
E-mail	OpenMail	Hewlett-Packard	To be determined	Windows, Macintosh, UNIX
E-mail	IsoShield	LabCal	Available Now	To be determined
NextStep Entrust	Entrust for NextStep	Computer Active	Available now	NextStep
Mainframe Entrust	Defensor/Mainframe	SAGUS Security	Available now	Multiple Virtual Storage, Others, to be determined
Firewall	Defensor Gateway	SAGUS Security	Available now	UNIX
Firewall	SecurIT	Milkyway Networks	Available now	UNIX, Windows NT
Firewall	Eagle	Raptor	Available now	To be determined
Firewall	KyberPASS	Devon Software	Available now	Windows NT
Remote Access	ExSentry RemoteWare	Exocom	Available now	Windows
Remote Access	KyberWIN	KyberPASS	Available now	To be determined
Remote Access	KyberPASS Authentication Server	KyberPASS	Available now	To be determined

Application	**Product**	**Vendor**	**Forecast**	**Platform**
Remote Access	KyberXpress	KyberPASS	Available now	To be determined
Remote Access	KyberSNA Authentication Server	KyberPASS	Available now	To be determined
Remote Access	ReachOut	Stac, Inc.	Available now	Windows
Remote Access	A2B	Simware	Available now	Windows
Remote Access	Charon	Milkyway Networks	Available now	Sun Operating System
Remote Access	Praesidium/Security Service	Hewlett-Packard	Available now	To be determined
Remote Access E-mail, FTP, WWW (http), Telnet, Client Server	Defensor Client	SAGUS Security	Available now	Windows, Windows NT
Secure Web Software Products	TradeVPI	TradeWave Corp.	Available now	Windows, UNIX
Secure Serve	Defensor Server	SAGUS Security	Available now	Windows NT, UNIX
Single Sign-On	Praesidium/Single Sign-On	Hewlett-Packard	Available now	Windows, UNIX
Smart Card	Smart Card	Hewlett-Packard	Available now	To be determined
Smart Card	SignaSURE CIP	Datakey	Available now	To be determined
PCMCIA Card	iPower PersonaCard	National Semiconductor	Available now	Windows
PCMCIA Card	GESC	Chrysalis-ITS	Available now	Windows, UNIX
Public Key Management	OnWatch Key Management & Certification Service	Bell Global Solutions	Available now	Macintosh, Windows, UNIX
Mouse	BioMouse	American Biometrics	Available now	To be determined

Application	**Product**	**Vendor**	**Forecast**	**Platform**
Network Management	Command and Control	General Network Services Inc.	Available now	To be determined
Network Management	HP Distributed Enterprise/Service Monitor	Hewlett-Packard	Available now	To be determined
Network Management Software	Nebula	Linmor	Available now	UNIX
Electronic Commerce	TrustedLink Guardian	Harbinger	1Q97	Windows, UNIX
Secure Web Software Product	FormLOCK	General Network Services Inc.	Available now	To be determined
Secure Web Software Product	PageLOCK	General Network Services Inc.	Available now	To be determined
Secure Web Software Product	ObjectLOCK	General Network Services Inc.	Available now	To be determined
Secure Web	TradeAuthority	TradeWave	Available now	Windows, Macintosh

13. POINTS OF CONTACT

For more information on the GOC PKI:

• PKI Project Office	(613) 991-7514 goc.pki@cse-cst.gc.ca
• Information Technology Security (ITS) Client Services	(613) 991-7678
• GTIS Secure Applications and Key Management Services	(819) 956-2535
• PWGSC - Entrust Products Standing Offer	(819) 956-0651
• Entrust Technologies Inc.	(613) 247-3769

World Wide Web sites of interest:

http://www.cost.se
http://www.cse-cst.gc.ca
http://www.cygnacom.com/docfiles
http://www.entrust.com
http://www.canada.justice.gc.ca
http://www.magnet.state.ma.us/itd/legal
http://www.public-key.com
http://www.sagus-security.com
http://www.tbs-sct.gc.ca
http://www.verisign.com

BIBLIOGRAPHY

1) CHOKHANI, S. and FORD, W., *Internet Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework, Internet Draft*, September 1997, available at http://www.ietf.org/html.charters/pkix-charter.html.

2) Communications Security Establishment, *Electronic Authorization and Authentication Guideline* (CID/01/15), September 1995.

3) Council for Administrative Renewal (CAR) Information Technology Security Strategy Legal Issues Working Group, *A Survey of Legal Issues Relating to the Security of Electronic Information*, June 1995, http://canada.justice.gc.ca/commerce/toc_en.html.

4) Council for Administrative Renewal (CAR) Information Technology Security Strategy EAA Working Group, *The Business Case for Electronic Authorization and Authentication in the Government of Canada*, January 1996.

5) *Final Report of the Information Technology Security Strategy Steering Committee*, Submitted to the Council for Administrative Renewal, February 1996, http://www.cse-cst.gc.ca/cse/english/car.html.

6) Policy Management Authority Committee of the Government of Canada Public Key Infrastructure, *Certificate Policy and Certification Practice Statement Framework*, Version 1.2b, November 1996, http://www.magnet.state.ma.us/itd/legal.

7) *Report of the Information Technology Security Strategy Steering Committee to the Council for Administrative Renewal*, June 1995, http://www.cse-cst.gc.ca/cse/english/car.html.

8) Treasury Board Secretariat, Treasury Board Manual, Chapter 2-2, *Policy on Electronic Authorization and Authentication of the Comptrollership*, July 1996, http://www.info.tbs-sct.gc.ca/SIGS/html/TBM_142/text/files/2-2.e.html.

9) WARWICK, Ford, *Straw Man Certificate Policy Definitions: Mid-Level Policies for Digital Signature and Encryption*, December 1996.