THE GOVERNMENT OF ICELAND'S COMMITTEE ON PKI

PRELIMINARY PKI STUDY ON REQUIREMENTS AND COMPARABLE INITIATIVES IN OTHER COUNTRIES.

MAY 2001

THIS REPORT CONTAINS 70 PAGES

REPORT PREPARED BY KPMG ON THE REQUEST OF THE COMMITTEE ON PKI

kpmg

Contents

1 Management Summary

The Icelandic government is promoting the use of Internet-technology to enhance the government's service delivery as well as its internal operations. However, the potential for improvements in service delivery and internal operations come with many of the security risks faced by existing systems as well as with new risks. In some cases, the sensitive information and communications that may be involved in these activities will require greater security assurances than can be provided by security measures as are implemented today (e.g. requiring passwords to gain access to a system).One of the ways to offer these higher security assurances is through deploying a so-called Public Key Infrastructure (PKI). A PKI is made up of organizational and technical components that allow for the use of digital signatures, digital IDs and encryption which together provide a range of security services[1].

Recognising the aforementioned, the Icelandic Treasury Department established a committee to make suggestions for a government wide PKI and set the course on the use of digital signatures in the government system. As a first step the committee performed a study with the following two main objectives:

1 To identify the specific security requirements of the government of Iceland relating to the electronic communications both within the government and with external parties (business and citizens) with respect to using a PKI to fulfil these.

2 To provide an overview of governmental PKI approaches in Canada, the Netherlands and Sweden.

To fulfil the first objective, interviews where conducted with over 15 organisations (most of them governmental) including Statistics Iceland, the Tax Office, Directorate of Customs, the Data Protection Agency, the Office for Vehicle Registration and a number of Health related organisations. It is important to note that the study did not cover an inventoryation of all initiatives or potential PKI usage, but aimed at providing a basis for decisions by the government regarding the use of PKI-technology.

The results of these interviews show that:

- Almost all governmental organisations have identified ways to use the Internet-technology and the majority of the organisations interviewed have initiated projects to that end. The main goals are to increase efficiency (amongst others by replacing paper-based communication by digital communication) and improved quality of service.
- In each of the domains (Government internal, Government-Business, Government-Citizen) all applications require varying levels of confidentiality, integrity, authentication and non-repudiation. However, all applications have such a mix of requirements that there is always at least one of these trust aspects that scores high and at least one that scores medium level.

[1] The appendix of this report includes an introduction to PKI.

- Digital certificates are considered to be the preferred solution by almost all interviewed organisations to fulfil their security requirements, and these organisations expect to initiate such a solution in the (near) future**.**

Discussions with some of the Icelandic banks learned that they are preparing PKI deployments as well as being willing to co-operate with the government on this subject.

Desk research and interviews with the project leaders of the Dutch and Swedish governmental PKI projects have been performed for the second objective of this study. As a first step the e-government approaches of Canada, the Netherlands and Sweden where studied. This showed that all three countries have this subject 'high on the agenda'. When looking at the PKI initiatives in these countries it became clear that Canada is at least a few years ahead in using PKI technology for e-government applications. The type of applications identified are to a large extent similar to those anticipated in Iceland, supporting the conclusion that Iceland may benefit from using PKI technology as well. Though the Netherlands and Sweden are not nearly as far as Canada, they also have a clear view that PKI technology is required to be able to fulfil the security needs of e-government applications. In both Canada and the Netherlands a co-ordinating infrastructure (made of both organizational and legal standards and technology) is put in place to facilitate departments that want to use PKI technology. By using a common approach and standards, the result is an interoperable infrastructure. In Sweden a simpler model is used, defining a government certificate for citizens that can be issued by multiple private organizations.

Based on the findings above it is concluded that there exists a need for PKI technology for deploying Iceland's e-government applications. Establishing a PKI requires substantial effort and time and therefore further governmental action on this matter should commence shortly to be able to service the governmental departments and agencies when required. It is important that the government starts building internal expertise on the subject of PKI to allow for a effective deployment and operations.

The steps taken as part of this study can be seen as the initial steps in the process of developing the PKI approach for the government of Iceland. We recommend that the following step is a strategic study into the different alternative scenarios for the PKI approach. This study should take legal and financial consequences into account aimed at choosing the most favourable and feasible scenario. It is further recommended to use a phased approach for the PKI deployment and to start with a limited number of pilot projects in areas where a successful implementation is most likely. The results of these projects will provide valuable insights and expertise for sub sequential government-led PKI deployments.

2 Introduction

2.1 Background

In October 1996 the government of Iceland published its "Vision for the Information Society", presenting the government's strategy in this area. The chief objective of the government is to ensure that Iceland shall be in the forefront of the world's nations in the utilization of information technology for enhancing the quality of life and greater prosperity. Following the publication of the strategy, the government decided in May 1997 to establish a long-term development project for the information society in Iceland. To set and control the project's direction a steering group (Information Society Taskforce), operating under the auspices of the Office of the Prime Minister, was established. The main task of the Information Society Taskforce is to promote the implementation of the government's strategy.

In light of rapid developments in information and telecommunications technology, the government added in March 2000 the subjects of e-commerce and e-government to the original objectives of the information society project. E-government can be defined as the usage of Internet-technology to enhance the government's service delivery. There are three primary reasons why e-government is important. It encourages the take-up of digital technologies that are crucial to economic competitiveness, it allows government to redefine its role and become more citizen-focused, and it can reduce the cost while not compromising the quality of public services. In general three application areas for electronic service delivery can be distinguished:

- within government (between governmental institutions / departments);
- between government and citizens;
- between government and business.

One of the most important prerequisites for electronic service delivery is to be able to offer an equal level of trustworthiness of information streams as in the paper world. To realize this the following security services are required[2]:

- confidentiality: to ensure that no unauthorized party can access the content of a message;
- integrity: to ensure that no unauthorized changes can be made to a message during transmission or storage;
- authentication: to ensure the identity of the sender and / or receiver of a message;

[2] For simplicity's sake the example of sending a message is used. However, the same services apply to other forms of electronic communication.

✍✍ non-repudiation: to ensure that someone can not deny having send/received a message.

One of the ways to offer these security services is through deploying a so-called Public Key Infrastructure (PKI). A PKI is made up of organizational and technical components that allow for the use of digital signatures, digital IDs and encryption which together can fill in all aforementioned security services[3].

Given the aforementioned developments, the Icelandic Treasury Department took the initiative to form a committee that is to make suggestions for a government wide PKI and set the course on the use of digital signatures in the government system. As a first step the committee performed a study into the requirement and comparable initiatives in other countries.

2.2 Objective of the study

The study has two main objectives:

3 To identify the specific security requirements of the government of Iceland relating to the electronic communications both within the government and with external parties (business and citizens) with respect to using a PKI to fulfil these.

4 To provide an overview of governmental PKI approaches in Canada, the Netherlands and Sweden.

2.3 Approach

To identify the security requirements of the government of Iceland a large number of interviews where conducted with governmental departments and private sector companies. Within these organisations interviewees were selected based on their involvement in e-business initiatives or their expertise of areas that form likely candidates for such initiatives. The overview of other government's PKI approaches is based on desk research as well as interviews with representatives of these initiatives.

2.4 Structure of this report

Chapter three describes the security requirements of the government of Iceland.

Chapter four provides an overview of the e-government activities in Canada, the Netherlands and Sweden.

[3] The appendix of this report includes an introduction to PKI.

Chapter five describes the PKI approaches of Canada, the Netherlands and Sweden.

Chapter six details the conclusions and recommended next steps.

The appendices contain an overview of the conducted interviews, additional information relating to the PKI organisation structure of the government of Canada, a PKI glossary, a list of references and a short introduction to PKI technology.

3 Requirements

3.1 Introduction

This chapter describes the anticipated e-government services as where identified during the conducted interviews (see appendix). A distinction is made between application for government internal usage, for government to business usage and for government to citizens usage. For each e-government application the security requirements are described as well. At the end of the chapter an overview of these is provided. The chapter concludes with a discussion of how PKI technology can be used to address the identified security requirements.

3.2 Anticipated e-government services and security requirements

3.2.1 Government internal

Statistics Iceland: receiving of statistical data

Statistics Iceland provides a PC software program which allows its users (government departments as well as companies) to enter their statistical data. Currently a project is underway to replace this PC software with a web application. The main security requirement for this application will be confidentiality and integrity. User authentication is needed but not expected to be so critical as to need digital certificates (username and password will suffice).

Statistics Iceland's Person register: receiving information from hospitals and agencies

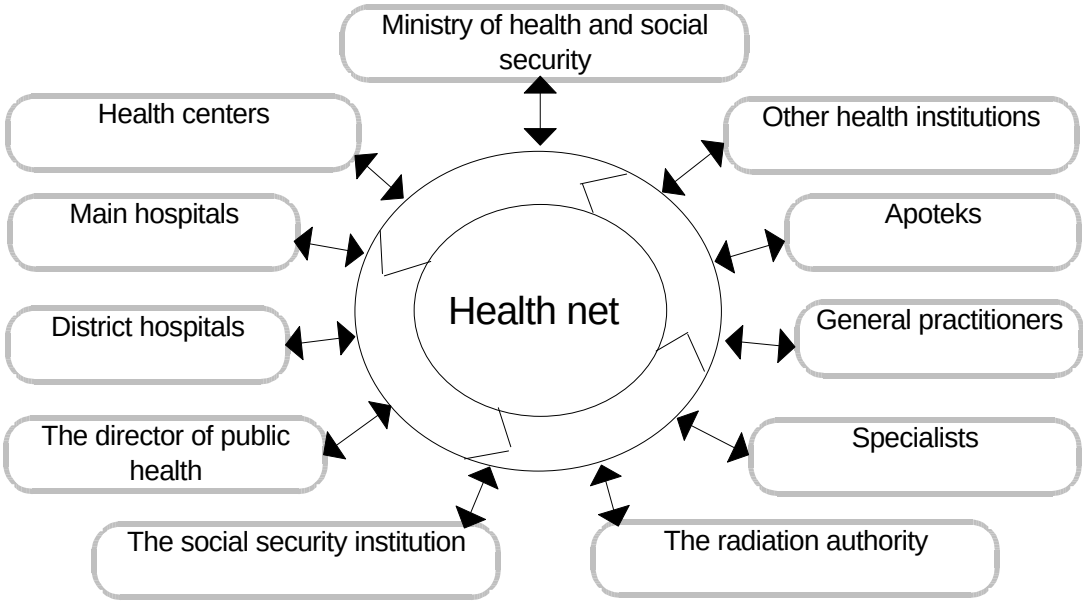
Updates and new entries to the Person register are received from hospitals, agencies and sometimes the individual citizen itself. Currently most to all of this information is received through paper forms (though sometimes these are faxed). Statistics Iceland views these as good candidates for web applications. Such applications require the data to remain confidential, assure integrity and provide user authentication. For certain information a digital signature is needed as well.

Secure e-mail

A number of government agencies / departments have stated that they would very much welcome the ability to send and receive e-mails in a secure manner. Since e-mail is often the most convenient way of communicating, people sometimes use it for sensitive information. This should only be done if confidentiality is guaranteed, which is not the case with regular (present) e-mail systems. Integrity is of relevance if e-mails are used for more or less formal communications. In some instances it is required to be able to verify who has sent a specific e-mail; this could be done by applying a digital signature.

The Icelandic Healthcare Network

The concept of the Icelandic Healthcare Network has been developed following the 1997 strategy statement of the Ministry of Health and Social Security. The Health Network's objective is to connect all parties involved in the health services in Iceland. Information that is currently transported by paper, such as doctor's letters, medical prescriptions and investigative test results will be transported on the net. Parties that shall use the Health Network include: hospitals, senior citizens institutions, health centres, private service offices, Ministry of Health and Social Security, the director of public health, pharmacies, the radiation authority and the social security institution. The picture below illustrates this.



The development of the Health Network will be incremental and through the execution of various projects that provide one component / phase at a time. A starting point is to use open standards as much as possible; Internet-technology is definitely among these. Given the nature of the information transmitted it is evident that the security needs of the Health Network are high. It is therefore emphasised that security is an integral part of the development of the Health Network and not some necessity that has to be done 'at the end of the project'.

Following are a few projects that can be considered part of the Health Network.

Division of Health Statistics: collecting health data (e.g. on accidents, complaints, HRM database)

This division collects all kinds of information from different parties within the health services. Examples are accidents, abortions, medical-complaints, and information on the individuals working in the health industry. Currently most of this information is collected on paper on an annual basis. This division aims at using the Internet where possible to make data collection easier and more frequent (e.g. have the institutions enter the data in a web form). For the database with medical staff the division believes that it may be useful to have people update this data themselves. Other users could be the pharmacists that need to know who are licensed doctors (that can issue subscriptions). Another future application is the registration for small institutions: currently these have their own systems, but a central system accessible over the Internet would be much more efficient. Given the nature of this information it is clear that the security requirements are high. Besides confidentiality and integrity, there is a need for user authentication and possibly also for digital signatures.

National Hospital: electronic discharge letter and admission letter

The hospital has a project underway that is developing an electronic discharge letter which is send from the hospital to the general practitioner (house-doctor) after a patient leaves the hospital. In conjunction with this an electronic admission letter is developed that is send from the doctor to the hospital. Since details about the patients condition are the main content of these letters, there is a clear need for security. There is a high requirement for confidentiality and integrity; a digital signature would probably be necessary as well.

National Hospital: single sign-on for intranet

The hospital has a large intranet which provides access to numerous applications. At present each application maintains its own user registration meaning that often users need to remember a multitude of usernames and passwords. This way of working is both inefficient and user-unfriendly. Therefore the hospital has started a project called ‘unified access’ that is looking into the possibility for single sign-on. A single system for user authentication is required to provide for this.

State Social Security Institute: in/out information from hospitals

The institute has started a project to develop a system that allows for the electronic receiving of in/out information from hospitals. This information contains the names of the patients that are entering or leaving the hospitals and is considered sensitive. Security needs are confidentiality, integrity and user authentication.

State Social Security Institute: invoices from physiotherapist and specialists

At present the institute receives invoices from physiotherapists and specialists in paper form, which are entered into the institute's systems by data entry staff. As it is expected that a large cost and time saving is possible when this information is received electronically, a project has started to look into the possibilities. Because each invoice contains details of the patient and the treatment, the security requirements are high. Next to confidentiality and integrity, user authentication is required.

3.2.2 Government to business

Customs import/export declarations

To allow smaller companies (without EDI capabilities) to submit electronic declarations, a new system was developed. Customs is required by law to provide adequate security since some of the information is very sensitive. In anticipation of the EU directive (on digital signatures) being implemented in Iceland, Customs choose to use digital signatures. Currently there are around 100 users, who after registration receive a one-time PIN that is used to obtain a certificate at Verisign (Skyrr). However, the certificate is issued in the name of Customs (private CA). Through username and password, one gains access to the application that provides a declaration form to fill. When submitting the form, the information is digitally signed. Both the information and the signature are stored by Customs. The certificate is issued in the name of an individual, not the company. There is a contract with the company making them responsible for informing if this person leaves the company or that specific function. It that case the person's record is deleted and a new certificate can be issued to his successor. The user's keys and certificate are stored in the browser, a smart card was deemed neither practical nor necessary. A smart card could be introduced in the future if available or required by the government. As only short-term contracts have been entered into, it is also possible to change to a different certificate provider. Security requirements of this application are confidentiality, user authentication, integrity and non-repudiation.

Tax: profit tax, VAT, withholding tax

The Tax Office is already an extensive user of Internet applications. Below the applications that relate to businesses are described.

Profit Tax: there is a PC application that organisations can use to fill in their data. When completed, the data is send to the tax office by e-mail. For this the security system Pretty Good Privacy (PGP) is used to sign and encrypt the data. The user has to come to the tax office beforehand to provide his public key (paper and disk), and sign the 'key' to show that indeed it is his public key. The Tax Office uses this key when verifying the data that is received. This system is also used for sending in the annual statement. Often accountants that perform the tax declaration for their clients use this system.

VAT: currently a pilot is starting with 100 companies that will use a web application to provide VAT declaration information to the Tax Office. Before they can do this, they have to request a PIN (on-line) in the process of which they have to print out a paper, sign it and send it to the Tax authority. Only after this has been received, will the system be opened for the specific user. This system uses 128-bit SSL (Verisign) encryption for confidentiality and server authentication. Once the VAT details are received, the system automatically provides the payment information to the user's Internet Banking application in which the authorised employee can perform the payment.

Withholding TAX: an application similar to the aforementioned VAT application will be developed.

The Tax Office has stated that the aforementioned systems work satisfactory but that using PKI technology may even enhance them. Basically the security requirements are confidentiality, integrity, user authentication and non-repudiation.

Government purchasing ageny: Procurement system

The government of Iceland is planning to set up a procurement system to enhance the efficiency and effectiveness of the procurement processes by using the Internet. As part of the system designated civil servants can access an Internet portal that maintains the catalogs of participating suppliers and place orders for goods. The system needs to be able to authenticate its users, assure integrity and confidentiality of the orders (to other suppliers) and for enhancement of the legal status of the orders a digital signature (non-repudiation) may be required.

Statistics Iceland's Organisations Register: receiving applications and changes

When someone wants to establish a new business they have to register it with Statistics Iceland. Usually this is done through an agency. It can take some iteration before the documentation is accepted. Changes (e.g. new director) to the existing information in this registry are coming from different sources (accountants, companies, agencies) and are mostly in paper form. An application making this communication possible over the Internet is expected in the future. The security requirements are confidentiality, integrity, user authentication and non-repudiation.

Land Registry of Iceland: receiving information related to properties

The Land Registry of Iceland is in the process of enhancing its central database and other systems. It is expected that in the (near) future more and more of the information flows that are still paper-based today will become electronically. Due to the legal status of the information in the registry the related security requirements are high. There is especially a need for non-repudiation, user authentication and integrity. Some of the information needs to remain confidential.

Health Network

The Health Network has some private organisations as its participants (e.g. the pharmacists) see section 3.2.1 above for more details.

Secure e-mail

A number of government agencies / departments have stated that they would very much welcome the ability to send and receive e-mails in a secure manner. As e-mail is often the most convenient way of communicating, people sometimes use it for sensitive information. This should only be done if confidentiality and integrity is guaranteed, which is not the case with regular (present) e-mail systems. In some instances it is required to be able to verify who has sent a specific e-mail; this is possible by applying a digital signature.

3.2.3 Government to citizens

Form.IS

Though not a governmental institution itself (but a private company) Form.IS is in fact operating as an e-government portal for Iceland. Through the website of Form.IS citizens can access a range of forms which can be used to submit applications to different governmental institutions. Form.IS converts existing paper forms to an electronic versions and makes them available on the web. Users have to register beforehand to receive a password. Following this, they can log into their own area of the system, fill in the relevant forms and submit these to the respective institution. Form.IS will forward this information to the institution which (after processing the information) can provide an electronic response to the user. The user receives the response and can keep on the system for future reference. The security requirements are confidentiality, integrity, user authentication and depending on the nature of the application non-repudiation as well. Form.IS has, as of now, two government agencies as customers: The Icelandic Student's Loan Fund and the Government Building Fund

At present the most prominent user is the Student's Loan Fund whose application will be discussed below.

Student's Loan Fund: basic and subsequent applications

The Loan Fund started to use Form.IS for subsequent loan applications which existing students have to submit to receive their money for the new year. The basic application was considered too critical (due to legal reasons) to allow for electronic submittal. However, due to the success of the system (around 50% of the subsequent applications came in through Form.IS resulting in a large financial saving) the organisation decided to start using Form.IS for this basic application as well. It was decided that the risk relating to not having a valid signature on the application is outweighed by the advantages (savings) of electronic communication. It is clear that a digital signature would greatly enhance the security of this

application. In addition, there are requirements for user authentication, integrity and confidentiality.

Other Form.IS applications

Other customers of Form.IS are municipalities such as Reykjavík, Hafnarfjörður and Akureyri in addition to a few companies. For many of the applications of the municipalities there is a definite need for authentication, integrity and confidentiality and in some instances non-repudiation.

Some cooperation between the municipalities and the government can be seen and should be researched.

State Social Security Institute: receiving applications through the web

At present the Institute uses a whole range of paper forms to receive applications from citizens. It is expected that most of these could be offered in electronic form relatively easily. However, some applications need to be accompanied by a signed statement from the doctor. Security requirements are confidentiality, integrity, non-repudiation and possibly user authentication.

Tax Office: personal income tax

Citizens can fill in their tax declaration using an Internet-application and a PIN code that was send to them by regular post. The system uses 64-bit session encryption (SSL with Verisign certificate). The Tax office is satisfied with the current system (over 50% of declarations are received electronically) but definitely sees potential for PKI to further enhance their processes. If citizens where to possess a private key and certificate there would for example be no more need to send out PIN numbers resulting in large financial savings.

Statistics Iceland's Person register: receiving information from persons on marriage and location moves

See description above (Government to Government section).

Icelandic Registration Office for Vehicles: change of car ownership form

When a second-hand vehicle is sold, both the seller and the buyer, as well as a third person (witness) have to sign the special form and send it to the Registration Office. The Registration Office is interested in offering a web based application for this process, but requires a solution for signing the form digitally.

Health Network

The Health Network will eventually include communication with patients as well, see previous description (government to government section).

Secure e-mail

Different government agencies / departments have stated that they would very much welcome the ability to send and receive e-mails in a secure manner. As e-mail is often the most convenient way of communicating, people sometimes use it for sensitive information. This should only be done if confidentiality and integrity is guaranteed, which is not the case with regular (present) e-mail systems. In some instances it is required to be able to verify who has sent a specific e-mail; this is possible by applying a digital signature.

3.3 Summary of security requirements

3.3.1 Government internal

Application	Confidentiality	Integrity	User authentication	Non-repudiation
Receiving of Statistical data	H	H	H	-
Person register: receiving information from hospitals and agencies	H	H	H	L
Secure e-mail	H	M	M	L
The Icelandic Healthcare Network	H	H	H	H
Collecting health data	H	H	H	L
Electronic discharge letter and admission letter	H	H	-	H
Single sign-on for intranet	H	-	H	-
In/out information from hospitals	H	H	L	L
Invoices from physiotherapist and specialists	H	H	H	L

3.3.2 Government to business

Application	Confidentiality	Integrity	User authentication	Non-repudiation
Customs import/export declarations	H	H	H	H
Tax: profit tax, VAT, withholding tax	H	H	-	H
Procurement system	L	H	H	M
Organisations Register: receiving applications and changes	H	H	L	H
Receiving information related to properties	L	H	H	H

3.3.3 Government to citizens

Application	Confidentiality	Integrity	User authentication	Non-repudiation
Form.IS	H	H	H	L
Student Loan Fund: basic and subsequent applications	L	M	L	H
State Social Security Institute: receiving applications through the web	H	H	L	H
Tax office: personal income tax	H	H	H	H
Change of car ownership form	L	M	-	H

3.4 How PKI can address the security requirements

As stated in the introduction, PKI technologies can be used to realise different security services. This paragraph discusses how PKI technology can be used to provide for the security requirements as identified in the previous sections of this chapter.

3.4.1 Confidentiality

As discussed in the security requirements summery, confidentiality is a critical requirement for almost all applications. PKI technology is capable of providing confidentiality by encryption of data to be transferred. PKI uses asymmetric encryption, which has major advantages over the alternative symmetric encryption by its substantially simpler key management. This simplicity results from the fact that the key that is used to encrypt the data does not need to be kept secret between the communicating parties. By using asymmetric encryption, the receiver's public key is used; this key is available in the certificate, which is usually publicly available. By validating the certificate the sender can make sure that he is using the correct public key. The receiver can use his corresponding private key (that only he possesses) to decrypt the data that was sent to him.

From an implementation perspective it is relevant how the communication model of the application is designed. Most of the identified applications have a many-to-one communication model, which means that there are numerous parties that all communicate with a single counter party. For example, all citizens have to communicate with a single Tax office to fill in there tax return. In such a scenario (communication model), it is usually relatively easy to realise the required confidentiality by using SSL and a single certificate for the one counter party (a so-called (web) server certificate). Such a certificate can simply be obtained from an external Certificate Service Provider and hence does not justify implementation of a PKI. In a many-to-many communications model (e.g. secure e-mail), every entity may communicate with every other entity and hence everyone needs to be issued a certificate with a public key.

Of all applications identified in this study and mentioned in the previous paragraphs, only the secure e-mail and the Healthcare Network have a many-to-many communications model. This means that for the other applications the confidentiality requirement can be relatively easily met without implementing a full-scale PKI.

3.4.2 Integrity

Integrity is in almost all applications a requirement because without this function the essence of communication itself is lost. The consequences of this may vary (e.g. an informal e-mail between colleagues versus a added zero in a procurement system resulting in an order of 10.000 instead of 1000 pair of shoes). Technically it is relatively easy to realise integrity (use of hash or similar mathematical functions) and often it is included in measures for confidentiality.

3.4.3 User authentication

From the analysis of the security requirements a clear need for the user authentication service arises. In general one can distinguish three different classes of user authentication:

- Systems based on something the user 'knows': the ordinary user-ID and password is the most widely used example;

- Systems based on something the user 'holds' (in his possession): examples are a private key (with certificate) and / or a token (smart card, calculator, etc.);

- Systems based on something the user 'is': a fingerprint or retinal scan are examples.

It is widely recognised that password-based systems provide only a limited level of security as they are often easily guessable or broken by hacking tool and some users tend to be careless in using them. Another drawback is the high cost associated with managing the passwords and with assisting users that have forgotten their password. A big advantage is that it is usually easy and inexpensive to implement a password-based system.

PKI technology is based on something the user holds in his possession (e.g. the private key). Often there is a password required to gain access to this private key, meaning that in practice PKI is based on both something the user knows and something the user holds. The security level can be further increased by using a smart card to store the digital certificate, rather than storing it on the user's PC. With or without smart card solution, PKI provides a considerably higher level of security then a password-based system. In addition, PKI is often used to realise single sign-on solutions (e.g. in an Intranet) enhancing both manageability and user-friendliness of authentication in a network environment.

Whereas systems based on something the user is (a fingerprint or voice recognition) offer features that provide an even higher level of security; however, these solutions are still in an early phase of development and few (large-scale) implementation exist today. Moreover, some implementations have had to cope with false positive (unauthorised access) and false negative validations (unnecessary access denial), as well as cultural barriers as users did not accept their fingerprint or retina data to be obtained and stored by organisations.

We conclude that PKI offers strong capabilities to satisfy the user authentication requirements of the identified applications. However, some of the applications can probably use password-based systems due to lower security requirements with respect to user authentication.

3.4.4 Digital signatures

Based on the analysis of security requirements, it is evident that quite a number of applications require digital signature as one of the key security services. Much like the hand-written signature, using a digital signature provides for legally binding an individual to a document and / or transaction.. Examples are submitting forms, sending or receiving specific data (e.g. an e-mail message) and "ordering/buying" public services. PKI is at present the only proven and accepted technology that allows for the creation of these digital signatures. It can therefore be concluded that PKI technology is required for some of the identified applications.

4 Other countries e-government approach

4.1 Introduction

In this chapter the e-government approaches of Canada, the Netherlands and Sweden are described. Each countries' vision and strategy relating to this subject is included, followed by an overview of realised or planned e-government services / applications.

4.2 Canada

E-government vision and strategy

Under the key government initiative *Connecting Canadians*, Canada is aiming to become the most connected nation in the world with all key government services fully on-line by 2004. Currently, a number of key strategies and initiatives are in place which support the Connecting Canadians *(www.connect.gc.ca/)* agenda. They include:

- The Government Online (GOL) initiative whose aim is to provide Canadians with electronic access to key government information and services by December 31, 2004. In the February 2000 federal budget, $160 million over two years was allocated to design and launch the GOL initiative.

- Strategic Directions for Information Management and Information Technology: enabling 21st Century service to Canadians *(www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_OIMP/sdimit_e.html)*. This strategy outlines broad-based visions and plans for a more citizen-centred government, which delivers quality services that meet the needs of users. It also outlines a series of priorities that will lever government's significant investments in Information Management and Technology towards a more integrated, collaborative model of government.

E-government projects and applications

Canada's SchoolNet *(www.schoolnet.ca)* was established in 1993 and is designed to promote the effective use of information technology amongst Canadians by helping Canadian schools and public libraries connect to the Internet. SchoolNet, with the assistance of its partners, successfully connected all Canadian schools and public libraries to the Internet on March 30, 1999. It is now planned that SchoolNet will continue to work with provinces, territories and the private sector to extend connectivity from schools to the classroom by March 31, 2001.

Human Resources Development Canada (HRDC) maintains an Internet-based job matching service, the Electronic Labour Exchange (ELE). Employers create a profile of the vacant position and job seekers create similar profiles describing their own skills and experience. ELE then matches the two together. The ELE website can be found at *http://ele-spe.hrdc-drhc.gc.ca/index.html*.

Another electronic services provided by HRDC is Job Bank on the Internet – an electronic listing of jobs, work or business opportunities provided by employers across Canada.

Health Canada *(www.hc-sc.gc.ca)* has the overall responsibility for the provision of health services in Canada. However, the Office of Health and the Information Highway (OHIH) was created in 1997 in recognition of the growing importance of ICTs in the delivery of future health services. It was set up to assist the Minister of Health and Health Canada address new and evolving issues and develop a longer term strategy regarding Canada's Health Info-structure. Through establishing OHIH, Health Canada gave itself a focal point for co-ordinating, facilitating and managing health information structure-related activities both within the department and with external stakeholders.

Health Canada provides a considerable amount of health information through its website as well as simple interactivity through mini applications such as a height/weight machine and active living quizzes that help Canadians better understand current health issues.

Health Canada is a pioneering partner in Secure Electronic Service Delivery. Within a year this project will allow key initiatives such as the First Nations Health Information System (FNHIS) – targeted at health care for example remote Inuit communities - to communicate with the highest degree of security currently available, thereby ensuring privacy. Together with the legal framework of Bill C-6, Health Canada will also be able to communicate using electronic signatures, making signed e-mails legally binding and paving the way for e-commerce. As a funding partner in the Government of Canada Public Key Infrastructure project, Health Canada is working alongside other government departments to lay the necessary groundwork for secure electronic transactions with other departments, provincial and territorial governments, and the private sector.

Public Works and Government Services Canada *(www.pwgsc.gc.ca).* is responsible for the development of electronic government procurement in Canada. A wide range of well-developed e-procurement services are accessible through their website. The Automated Buyer Environment (ABE) is an end-to-end procurement system that handles all aspects from receipt of requisition to bid evaluation. This system links seamlessly to a number of other databases and procurement systems, including the key service, MERX *(http://contractscanada.gc.ca/en/tender-e.htm)*, which is Canada's official tendering service.

MERX is an on-line service that advertises government contracting opportunities to potential bidders. It is owned and operated by Cebra Inc, which provides the service to the federal government under contract.

Departments must use MERX for requirements subject to any of the trade agreements. Some departments are also using it for other purchases. PWGSC also uses MERX to advertise requirements for printing services estimated at $10,000 or above, most goods and services estimated at $25,000 or above, and communications services worth $50,000 or more. It advertises requirements estimated at $60,000 or above for real estate, leasing and maintenance services. It also advertises requirements estimated at $72,600 or above for

architectural and engineering consulting. More and more of the government of Canada's requirements are advertised on MERX and this amounts to $5 billion annually.

MERX is accessible from any location in Canada on a 24 x 7 basis. Customers have free access to view the notices of opportunities on the Internet and pay a subscription fee for additional services. It also provides information on:

- how to order bid documents;
- what the federal government has purchased in the past, the names of the contractors and the value of each contract;
- other federal and provincial opportunities as well as U.S. and other international opportunities.

MERX also allows users to identify other suppliers ordering bid documents to help organisations to determine who competitors are or to identify a bid partner and also provides an on-line support facility.

The Buying Power 2000 application (BP2K) provides authorized federal employees with the capability to make on-line, low value purchases from electronic catalogues over the Federal government Intranet, including confirmation of receipt and electronic settlement with the client department at the back end. (Stage 3) This project was funded from the annual departmental appropriation and won a gold medal at the 1999 Technology in government Conference. Sales during 1999-2000 were $1.5 million with an average transaction value of $209. Users are enthusiastic about the system, and when surveyed, over 80% said they were satisfied with the service. Part of the success of BP2K is attributable to promoting awareness of the service to potential customers as well as the provision of a Help Desk that answers customer queries.

On average, BP2K saves the government $29 a transaction or 25% of the total administrative costs. The cost per transaction before the introduction of BP2K was nearly $120.

Industry Canada has a mandate to help make Canadians more productive and competitive in the global, knowledge-based economy and is one of the federal departments responsible for the provision of services to businesses in Canada. It delivers information and services through its primary web site, Strategis *(www.strategis.gc.ca)*, which was launched in 1996. Strategis is a comprehensive site for Canadian businesses and consumers to help identify new markets, find business partners and locate emerging technologies.

A number of databases are on-line for direct queries and forms can be completed and transmitted on-line on the Strategis web site, including federal incorporations, patent and trademark protection, Investment Canada filings, lobbyist registration, and the Canadian company capability directory entries and updates.

Industry Canada has made progress in providing clients with on-line interaction and official on-line responses (other than receipt acknowledgement) for four services. These services are federal corporations, Investment Canada filings, on-line spectrum license auction, and the automated name search service.

The Canada Customs and Revenue Agency (CCRA) is involved in a partnership with the province of Nova Scotia that has resulted in the creation of an electronic single-window registration service to business (*http://www.ccra-adrc.gc.ca/eservices/bro/menu-e.html*). Businesses can now obtain a Business number to register for CCRA programs, register a business name, or apply for certain provincial licences. Later this year, new partnerships with Ontario and Manitoba are planned with a view to providing business registration services.

In addition to these application specific areas, Canada is committed to developing web sites or portals which link or integrate information and services according to citizen and business requirements. A number of these are operating today:

- Government of Canada portal *(www.canada.gc.ca);*
- Canada Business Service Centers portal *(www.cbsc.org)* which is the premier gateway to government information for business;
- Canadian Consumer Information Gateway at (*www.consumerinformation.ca*), a new portal for consumer information and services;
- ExportSource at *(www.ExportSource.gc.ca)* is the on-line source for export information;
- Youth Resource Network of Canada at *(www.youth.gc.ca)* designed and managed by Youth offers a multitude of information on the employment world.

4.3 The Netherlands

E-government vision and strategy

The Netherland's key target is to achieve a level where at least 25% of public services can be delivered electronically by 2002. It is expected that deploying ICT will ultimately lead to cost savings. An annual budget of 30 million Dutch guilders has been made available for the Electronic Government Action Programme, although the operational costs of projects will be funded by mainstream budgets.

The two key policy documents are *The Electronic Government Action Plan* and the *Digital Delta*. *The Electronic Government Action Plan* was submitted to Parliament in December 1998. The principles of the Action Plan include electronic accessibility of government information and services, improved public services and better internal processes.

The White Paper 'The Dutch Digital Delta, The Netherlands oN-Line' is a joint publication by a group of Dutch Ministries. Published in June 1999, it is a follow-up to the National Action Programme on Electronic Highways and offers a framework for a range of specific measures regarding government policy on ICT for the next 3 to 5 years.

The Ministry of the Interior and Kingdom Relations is responsible for information policy in the public sector. A new directorate has been formed - Information Policy for the Public Sector which is responsible for strategic policy, research, international contacts and benchmarking. A strategic vision has subsequently been developed on the role of government in an information society entitled *Contract with the future* and submitted to parliament by minister Van Boxtel in May 2000.

E-government projects and applications

A system of authentic registers is being developed in order to improve data collection and data flows. The aim is to ensure that citizens and business are required to submit the same information to the government only once. An example of an authentic register is the Municipal Records Database which automatically enters every 18-year-old into the electoral register. If a citizen has a change of address that is reflected in this register, the change can be transmitted to approximately 300 other public sector organisations as long as that citizen is registered with them.

In order to connect up all ministries, an Intranet is being installed which will provide secure e-mail for all civil servants. It is expected that this will enable disparate parts of government to work together more easily.

The government portal website *(www.overheid.nl)* was launched in September 1999, enabling all government information to be accessed via a single access point. A helpdesk has been set up with the aim of encouraging government authorities to put their information on the Internet. A monthly award is given to the best government website in order to improve and raise awareness on quality levels.

The Public Counters 2000 programme aims to launch a network of 'desks' which citizens and business can consult for information and services without being referred elsewhere. These 'desks' are customer-friendly and accessible 24 hours a day. Four special counters will be launched nationally. These counters will deal with

1 Care and Welfare

2 Building and Living

3 Work and Income, and

4 Business.

The latter will be an integrated counter for business with a basic Register for Firms, which is expected to be implemented by 2002.

The Electronic Delivery of Mandatory information (EHD) aims to improve the electronic communication between small and medium-sized enterprises and government by introducing one common interface for all institutions.

There are numerous examples of innovative electronic services. In the healthcare sector, a Care-Passport is being piloted. This project aims to standardise electronic communication amongst patients, care institutions and insurance companies by using a health care smart card. Another pilot project based on a new European identity card containing biometric data will commence shortly.

Since 1996 it has been possible to electronically transmit tax forms; 1.2 million Dutch citizens now use this services on an annual basis. A pilot project is currently underway that allows businesses to pay VAT and income tax via the Internet in a secure manner.

The main focus is on the improvement of government services and the Dutch government has been very proactive in using ICT for this end. For example:

- citizens who receive national assistance benefits can be advised of their potential rights to individual housing, exemption from local authority taxes and local authority refund schemes;

- In the past, when a car is sold, excess vehicle licence duty had to be claimed by filling in a form. Today, this refund can be obtained from the tax authorities automatically;

- The database of the Social Insurance Bank (the organisation responsible for pensions) is now linked with other databases to identify people who are entitled to pensions for which they have not applied;

- Birth records can now include all 'inoculation records' of the local health authorities, marking the beginning of the medical supervision of the child, including standard vaccinations and supervision via the health centre;

- When a child is born, the Social Insurance Bank automatically sends out an application form for child benefit to the parents. After the application has been recorded, child benefit payments are automatically paid into the parents' bank account each quarter. In the past, a new application had to be submitted every quarter. The Social Insurance Bank is therefore able to work much more efficiently as processing of application forms has been reduced significantly.

4.4 Sweden

E-government vision and strategy

Swedish administration is an early adopter of ICT and provider of on-line government services. The government's overall information technology (IT) policy objective is for Sweden to become the first country to create an information society for all.

Swedish agencies normally finance their own contributions to ESD initiatives from existing budgets, although for major investments loans are available from the Swedish National Debt Office and some seed corn funds are centrally allocated. Some large programmes are separately financed.

A new national strategy for the information society *An Information Society for All* was presented to Parliament on 28 March 2000, supplanting the earlier 1996 IT Bill. The government proposes that state investment be focussed primarily in the areas of regulatory systems, education & training and infrastructure. The overall aim of this is to boost confidence in IT, competence in the use of IT applications and accessibility to the services of the information society.

In 1998 the government presented a Bill to Parliament on the future of the government administration *Public Administration in the Service of the People*. This is the principal document for the development of the civil service and emphasises the importance of IT in the public sector to improve service and dialogue with the citizens.

In recent years the government has appointed committees and assigned agencies to take a leading role in fields such as secure communication between authorities, legal basis for the provision of data, better use of information resources, and electronic signatures.

Statskontoret, the Swedish Agency for Administrative Development (SAFAD) has proposed criteria for central e-government developments based on the notion of the *24x7 Agency* (*http://www.statskontoret.se/24-timmarsmyndighet/summary.html*).

E-government projects and applications

The National Agency for Education operates the Schoolnet service which aims to integrate ICTs in the education sector. Schoolnet is an Internet-based gateway that provides teachers and pupils with access to a wide range of information and learning materials. Services currently available through Schoolnet include:

- the *School Data Network* which runs several services for students and teachers in Swedish secondary schools, for example, Lexin - electronic dictionaries in Swedish/English and Swedish/Finnish.

- the *Link Larder* which provides several links on various educational topics which are quality-controlled and continually reviewed by teachers and librarians.

- an electronic newspaper, *Klassrum Direkt* for reporting on latest Internet developments which users can subscribe to.

- the Multimedia Bureau which serves as a source of material, ideas, courses and knowledge. The Bureau is intended for use as a tool for distance publishing and to facilitate exchange of experience. Its overall aim is to induce teachers and pupils to use new media at school. A tool has been developed which enables content providers to populate the Bureau remotely. The Bureau also offers this tool to Swedish schools to enable collaborative projects. For example, to jointly produce Internet-based teaching aids without having to master the underlying technology.

The Swedish Public Employment Service provides a range of Internet based job searching services Job seekers can access the Job Bank and can consult lists of vacancies by region or profession. A description of each vacancy outlining the nature of the job and full contact details is given. In October 1999, the Job Bank received 1,400,000 visits and the numbers are increasing. The Job Seekers Bank offers job seekers an opportunity to enter personal data onto a database so that prospective employers accessing the service are able to identify and contact suitable candidates for interviews. This service receives around 5000 visits per day, 10% of which are employers. By the end of 1999, 20,000 Swedish companies were registered users of the Job Seekers Bank and it contained 50,000 CVs.

A collaborative initiative between the Swedish Patent and Registration Office (PRV) and The Swedish National Tax Board is to develop an Internet-based service where individuals can register a new business. This is going to be a one-stop service where data is shared between the two departments and is distributed automatically to other relevant authorities. In connection with this initiative, the Swedish National Tax Board is planing to make it possible to submit VAT returns in the near future.

As elsewhere, there is a thrust to provide joined-up services between different agencies, and the private sector. One collaborative project between agencies in tax, employment, student services, and social services, involves the provision of services via a network of over 600 kiosks. A collaborative venture between the Post Office and Tax Board provides a one-stop change of address service at *www.adressandring.se*.

In developing electronic vehicle registration services, the Swedish Vehicle Registry has been able to reduce its number of offices from 24 to 1 and also the number of customer service staff has decreased significantly despite demand for services increasing by 20%.

5 Other countries PKI approach

5.1 Introduction

The PKI approaches of Canada, the Netherlands and Sweden are described in this chapter. Each country's section starts out with a short overview of the legal situation. Next, the approach that was (is being) used in developing the PKI is discussed. Following, the country's PKI organisation and architecture is described. Each section concludes with an overview of the PKI projects and applications that are present or anticipated in the respective countries.

5.2 Canada

5.2.1 Legal situation

Canada has put in place a policy framework to encourage trust in electronic transactions. This includes legislation to protect personal information in private sector transactions, and to provide legal certainty for the use of electronic signatures and records, as well as a policy encouraging the use of cryptography for electronic commerce.

On 13 April 2000, the Personal Information Protection and Electronic Documents Act passed into law. The act supports and promotes electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending amongst others the Canada Evidence Act. The act grants authority to the appropriate authorities to make regulations about how form requirements may be satisfied using electronic means and describes the characteristics of secure electronic signatures and grants authority to make regulations prescribing technologies or processes for the purpose of the definition secure electronic signature.

On 30 September 1999, the Uniform Law Conference of Canada (ULCC) together with the Justice Department has adopted the Uniform Electronic Commerce Act (UECA), which allows the use of electronic signatures in communications with the government. The law contains general provisions for equivalence between traditional and electronic signatures and is modelled after the UNCITRAL Model Law on E-Commerce

In Canada, there are no rules governing the establishment of companies offering certification services and an industry-led accreditation scheme is in operation. However, companies who intend to provide services to, or interact with, the federal government must meet certain cross-certification requirements laid down by the Government of Canada's PKI management policy.

5.2.2 Governmental approach to PKI

In 1993, under the leadership of the Communications Security Establishment (CSE) and with the participation of departmental partners, the government contracted with a group in Bell Northern Research (now Entrust Technologies Limited) to develop a PKI. The product was to have a Commercial Off-The-Shelf (COTS) potential, to employ open standards that met government needs, and to be delivered in stages by December 1998.

In 1995, the Information Technology Security Strategy Committee of the Council for Administrative Renewal looked at several aspects of security with respect to government services and information technology. One of these working groups, mandated to look at PKI issues, developed a business case for a government PKI of encryption and digital signature services. This business plan culminated in the approval of the initial phase of development and implementation of the GOC PKI.

In November 1995, the Prime Minister decided on core responsibilities for the implementation and management of the GOC PKI initiative:

i. the CSE would be the location for the Canadian Central Facility (CCF) – the primary certification authority for the GOC PKI; and

ii. the Treasury Board of Canada Secretariat (TBS) would chair an interdepartmental management committee to oversee the implementation and management of the PKI initiative. The committee would report to the President of the Treasury Board for overall policy issues.

In April 1998, an Interdepartmental PKI Task Force (TF) was established, based in TBS/Chief Information Officer Branch (CIOB), to support and co-ordinate GOC PKI implementation activities. The TF was responsible for developing and implementing the PKI operational framework that will provide a sustainable and interoperable infrastructure to support electronic service delivery to Canadians and internal government operations.

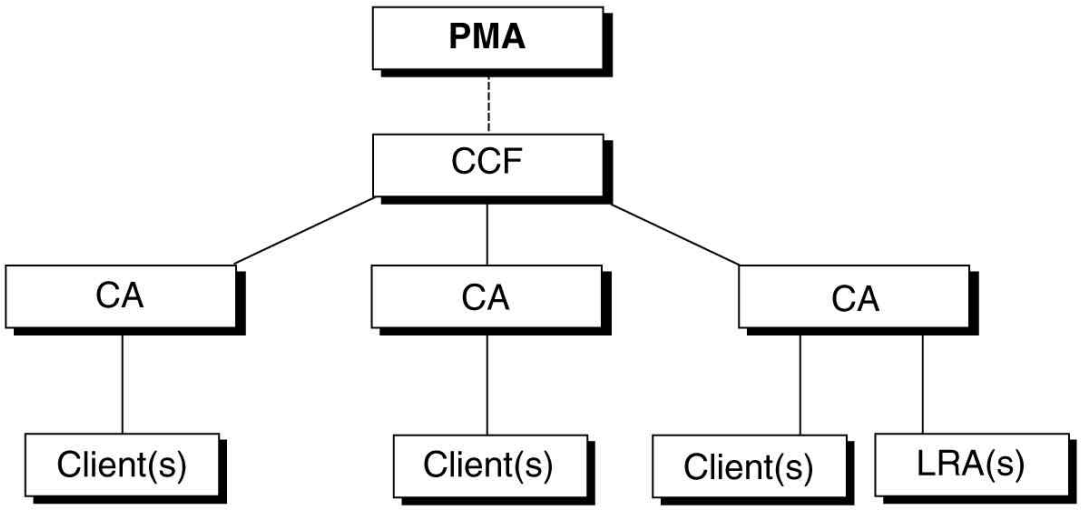
In December 1998, the GOC PKI certificate policies document was published. This document provided eight model certificate policies (four assurance levels for digital signatures and for confidentiality) for use by departmental Certification Authorities.

In May 1999, The GOC PKI became operational and the Treasury Board Ministers approved the Policy for PKI Management in the GOC, which outlines requirements for departments that issue, or have issued on their behalf, digital certificates. The GOC PKI Task Force became the GOC PKI Secretariat.

5.2.3 Organisation and architecture

The GOC PKI became operational in May 1999 and is being managed and further developed by what is called the GOC PKI Team. This is a comprehensive interdepartmental network of federal departments and agencies, committees, sub-committees, and working groups.

Appendix C provides an overview of the organisational structure and responsibilities of the different actors within it. The basic model of the GOC PKI itself is depicted below.



Following is a description of the different entities.

PMA

The Policy Management Authority (PMA) is an interdepartmental committee, chaired by the Treasury Board Secretariat. The PMA comprises representatives of each federal department operating at least one CA that is part of the Government of Canada PKI. Its membership also includes a representative of the Canadian Central Facility (CCF). The PMA is responsible for the oversight and management of the Government of Canada PKI. It is the authority for establishing procedures and standards both for the CCF and for lower level CAs that are part of the Government of Canada PKI. The Policy Management Authority is also responsible for recommending, to the Secretary of the Treasury Board, the approval or rejection of requests for cross-certification.

CCF

The CCF is the central Certificate Authority (Root CA), 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. The CCF's main functions are to:

✍✍ certify all GoC PKI "level 1" CAs;

✍✍ 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.

CA

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.

Departments may buy CA services from external service providers but the responsibility for the service remains with the Department. They have to set up a “virtual CA” with CPS. They may also take services from another Departments’ CA and adopt those CA’s practices. All back-up key material must remain within Canada. But a CA supplier may well be a foreign company. All certificates must be issued in the name of Her Majesty. Each CA must operate a repository. Repositories of all CA’s must be interoperable and be registered. There is no requirement to use GoC generated keying material only in case of non-GoC employees. Self-generated private keys are not stored for key recovery. All CA’s are subject to their Departments’ internal audit.

LRA

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.

Policies

The following documents describe the policies adopted for the GOC PKI:

- The policy for Public Key Infrastructure Management in the Government of Canada;

- Digital signature and confidentiality policies for the GOC PKI;

- GOC PKI Cross Certification Methodology and criteria.

The policy for Public Key Infrastructure Management in the Government of Canada stipulates that if a departmental Certification Authority intends to issue, or have issued on its behalf, certificates outside the department, it must cross-certify with the Canadian Central Facility (that is part of the GOC PKI). For cross-certifications internal to the federal community, the Government of Canada Public Key Infrastructure Management policy requires departments to sign a cross-certification arrangement formally describing the terms and conditions of the cross-certification. Cross-certifications with the private sector or with certification authorities not part of the Government of Canada Public Key Infrastructure require the implementation of formal cross-certification arrangements between the government of Canada and the external entity.

To facilitate cross-certification, departmental CAs are encouraged to adopt one or more of the eight GoC Certificate Policies which have been defined. These CPs classify digital certificates according to four certificate assurance levels Rudimentary, Basic, Medium or High. Each department must decide the types of information and services for which each assurance level of certificate may be used, and must set the financial liability limits for each level.

Each CP has a different liability paragraph. The amounts mentioned must be seen as recommended minimal amounts. Departments may accept higher levels of liability but do so at their own risk. Claims are paid from a central fund in which each department contributes according to a certain key factor. Liability is restricted to the CA operation and services. Applications are explicitly excluded from liability. CA operations are self-insured by the GoC. Applications are expected to be CP aware so they can act according to the certificate policy encountered in a certificate. If they are not, this must be dealt with in policies and procedures. It is expected that the defined CP level 3 will be the GoC general level for certificates. There is no clear view on the issue of exchanging information between different CP levels. It is assumed that a department that receives a certain level certificate will deal with it according to the associated CP.

External personnel have to sign an agreement in which the Terms and Conditions are explicitly accepted. This is essential for limiting the liability. GoC personnel have to be informed of the Terms and Conditions.

5.2.4 PKI projects and applications

Several PKI-related pilot projects are underway in the Federal agencies, a number of which have been selected as special projects under the GoC PKI Pathfinder program. Pathfinder projects represent major innovative work initiatives undertaken within the federal government involving the practical development, application and use of PKI technology.

There are already 17 PKI Pathfinder projects and over 100 PKI pilot projects which are using the Internet and PKI to deliver services on-line. The following is a brief description of the 17 Pathfinder projects.

1 Secure Applications and Key Management Services (SAKMS)

The Secure Application and Key Management Service (SAKMS) was initiated in December of 1995 as the Government Telecommunications and Informatics Services (GTIS) PKI. Conceived as a comprehensive portfolio of services, SAKMS offers departments an ideal opportunity to experience secure GTIS solutions or to utilise the GTIS Certification Authority (CA) as an infrastructure component in building their own electronic commerce solutions

2 Investment Review -Electronic Filing Pilot

The Investment Review Division (IRD) of Industry Canada administers the Investment Canada Act, which involves the processing of up to 1,000 applications each year from up to 200 legal firms across Canada. These filings are currently in paper form via either regular mail or fax. To improve the quality of service and reduce overall costs, IRD is undertaking a pilot project for the secure electronic filing of information using PKI technology. This project also supports Industry Canada’s declared leadership role in electronic service delivery to clients, and electronic commerce.

3 Spectrum Radio Licensing Pilot

Spectrum Information Technologies and Telecommunications (SITT) in Industry Canada are mandated to license the radio spectrum on behalf of the government of Canada. This involves the paper based processing of up to 850,000 applications each year ranging from individuals, small and large firms and other organizations. Users pay for their licenses on an annual basis: revenues total over $150 million a year. The Spectrum Electronic Commerce Pilot involves establishing a trial for the secure filing of radio System licensing applications

in which clients are provided with the opportunity to file their license applications electronically using PKI technology for confidentiality and digital signatures.

4 Electronic Regulatory Filing Project

The National Energy Board (the NEB) is an independent federal regulatory agency that was established in 1959. The Board regulates specific aspects of the energy industry relating to the construction and operation of inter-provincial and international pipelines, power lines; the export and import of natural gas; the export of oil and electricity; and, frontier oil and gas activities. The NEB receives about 750 applications yearly, ranging from 20 to 3,000 pages in length. Applicants sometimes file 20-35 copies of their application and related documents for a regulatory proceeding. In late 1992, the NEB investigated the feasibility of moving away from a paper-based regulatory process to an electronic one. The Electronic Regulatory Filing (ERF) project was conceived as a way of facilitating that change. The ERF initiative involves three main aspects. It deals with electronic document exchange; with developing a repository of those documents for public access; and, ultimately, with changes to the Board's information systems and processes.

5 Network Security Strategy

The Mission of Indian and Northern Affairs Canada (INAC) is "Working together to make Canada a better place for First Nations and Northern peoples". Sensitivity Statements completed by INAC users and Threat and Risk Assessments (TRAs) performed by the Information Technology Security Co-ordinator in the last few years have indicated that network security is a requirement. The INAC network does possess certain security safeguards for the processing of non-sensitive information. However, various factors have increased the security requirements of the network, including: an increasing need to process sensitive information; the need to share information between government and non-government bodies; and the increasing use of the Internet for communicating and accessing corporate information. The Network Security Strategy is intended to secure corporate information of a *Non-Designated* and *Designated* level with outside agencies, and *Classified* (up to secret) with its employees, regions and other government departments. Parts of the Strategy have been implemented by utilizing the security features built into existing systems. Other components of the Strategy involve PKI for encryption and digital signatures. The project is scheduled for implementation over four years.

6 Labour Market Development Agreement (LMDA) Connectivity Project

The Ministry of Human Resources and Development Canada (HRDC) communicates with provinces and territories for instance relating to the employment area involving training and jobs. In support of this connectivity to certain HRDC systems and applications and databases is needed. Security and authenticity of access from provincial sites is, therefore, one of the key connectivity requirements. The Connectivity Project provides a unique challenge in that the authorized external users of HRDC systems are many and widely dispersed. The

Ministry of Human Resources and Development Canada (HRDC) network is protected from outside access by a secured perimeter comprising Eagle Raptor firewalls and KyberPass authentication servers. Data encryption between the HRDC network and partner work stations is provided by the KyberPass product. Strong authentication of provincial partners has been achieved by implementing a KyberWin client accompanied with Entrust public key cryptography software on remote workstations. Entrust–based Public Key Infrastructure (PKI) is the basis of HRDC's strong authentication and encryption services. In the summer of 1997, HRDC established a departmental Certification Authority (CA) and a supporting service delivery infrastructure to issue and manage key pairs and public key certificates to facilitate the use of PKI. To date, over 2,200 certificates have been issued in support of LMDAs. It is expected that once implementation is completed for all LMDAs, a total of 5,000 provincial and territorial employees will have the capability of accessing HRDC systems from their desktops.

7 Canada Educational Savings Grant (CESG) System

In its February 1998 Budget the federal government announced a significant new education support initiative: the Canada Education Savings Grant (CESG) Program. Under this program, parents can potentially add as much as $7,200 plus compound interest earnings to a child's future post secondary education fund. The CESG System is critical to the delivery of this new program. It is a cost-effective and a secure solution designed to provide secure, two-way data transmissions of sensitive information and financial deposits over the Internet between Human Resources Development Canada (HRDC) and the financial institutions serving as trustees administering the RESP funds. It is expected that over 30 million secure electronic transactions will be exchanged with the CESG Program in the first year of operation, involving initially up to 100 partner financial institutions (and eventually up to 200 in a mature system).

8 Travel Management System

Travel management within Statistics Canada is a non-automated, manual process currently making extensive use of paper forms (generic, standard government of Canada forms). The forms are used to request cash advances and process expense claims. The forms are completed and signed by prospective travellers, and then forwarded for signed approval by managers at the appropriate level of authority. Administration of the process is carried out by administrative staff who verify the contents of the forms and by financial officers who audit the contents of the forms prior to the disbursement of funds. The Financial Policies and Systems Division of the Finance Branch is undertaking a pilot project to automate the Travel Management Process in order to reduce the overall costs involved and time required in the process. This pilot involves the use of Web-enabled electronic forms, workflow technology and Public Key Infrastructure (PKI) technology, which will provide digital signatures and the necessary level of authentication and security.

9 Business Registration On-line Internet Pilot

The Business Returns and Payments Processing Directorate (BRPP) in Revenue Canada is responsible for registering businesses for Business Numbers (BN) and four Revenue Canada program accounts. These accounts are Goods and Services Tax, Payroll Deductions, Import/Export, and Corporate Income Tax. In order to improve service delivery and reduce paper and compliance requirements, particularly for small businesses, BRPP is undertaking the Business Registration On-line Internet Pilot. This Pilot will move the registration process to the Internet. Users will be able to complete and submit the necessary information on-line. A BN and program account numbers will be returned on-line to complete the transaction. PKI technology will be tested as the means of securing these transactions since protected information of a sensitive nature is involved.

10 Secure Messaging Pilot

The Secure Messaging Pilot is a priority initiative of the GOC PKI implementation. The purpose of the pilot is to conduct a systematic, practical testing of the interoperability of using public keys in various e-mail systems across departments on a government-wide basis. The experience and results will provide a needed, valuable assessment of the actual use of public keys in the most common, widely used application in government.

11 Secure Electronic Service Delivery (SESD)

The Secure Electronic Service Delivery (SESD) Project is a comprehensive, three-year, corporate initiative in Health Canada to provide essential security services across the department. The main focus is to provide a standard, coordinated and integrated Internet based security solution to fulfill the mandatory security requirements of the department's electronic services and applications. An SESD technical infrastructure involving both a production and a test/development area has been created and is being made operational. This environment is based on the GOC PKI model and uses Entrust software and tools. Delivery of this technical infrastructure was taken in March of 1998 as the Health Canada GOC PKI management node. Health Canada has adopted the GOC PKI Certificate Policies at the medium assurance level; is finalizing its Certificate Practices Statement; and has provided a transition plan to become a full member of the GOC PKI by the summer of 1999.

12 Spectrum Internet Auction

Industry Canada is responsible for managing the radio frequency spectrum and ensuring that this variety of uses co-exists compatibly. Demand for access to this scarce resource often exceeds supply. A spectrum auction is a market-based tool that the department has recently introduced to award licences when mutually exclusive demand for spectrum exists. Industry Canada's spectrum auction was conducted securely over the Internet and employed the latest in Canadian Public Key Infrastructure (PKI) encryption and digital signature technologies to ensure the confidentiality and authenticity of the bids. This spectrum auction represents one

of the largest business to government electronic commerce transactions ever to have taken place over the Internet, with bids exceeding $170 million. The software for the Auction Management System was purchased from expert auction consultants and the encryption and digital signature technology was incorporated in the software by a local Ottawa firm, General Network Services (GNS). GNS' FormLock product is essentially a customized Internet browser plugin and uses Entrust Technologies Inc.'s PKI engine. To increase the speed of bid transactions, the Auction Management System also incorporates a new protocol called *On-line Certificate Status Protocol* (OCSP).

13 New Canada Payroll Savings - Secure Web Site Pilot

The Bank of Canada (BoC) undertook to develop a secure web-based application, to facilitate small companies with little IT expertise to submit a purchase file to the BoC's direct sales system. The application's security should ensure that only those who should have access to the site do and that they are able to see only their own employee data. The solution decided upon was the use of PKI technology for the required encryption and authentication. A Certificate Authority was being built and established in the BoC as an administrative framework, and being used in support of the Bank's Telework initiative. Given the nature of the data, the level of authentication sufficient to build trust required a Medium Assurance certificate. The Pilot is scheduled to commence its first transmissions in December of 1999 and initially involve over 50 companies with an average of 120 employees each. It is expected that some 5,000 employers will be included next year.

14 Large Value Transfer System (LVTS)

The LVTS is a new, state-of-the-art electronic credit transfer system designed to manage large-value or time-sensitive Canadian dollar payments in Canada. It enables individuals, businesses and governments to make final payments in a rapid, secure and efficient manner. It incorporates real-time risk controls to ensure certainty of settlement of all transactions and to ensure immediate finality of payment for all users. Although the LVTS uses the SWIFT network (Society for Worldwide Interbank Financial Telecommunications) to communicate payments, the bulk of its work is performed using the private LVTS Direct network. The LVTS Direct network uses PKI in order to deliver the services outlined for end to end encryption, digital signatures and token and password access requirements.

15 Record of Employment on Web Pilot

Every termination of employment means that an employer must complete a ROE form. Each year over 1 million employers create and complete 8 million multiple-part ROE forms totalling to some 36,000 forms per day. HRDC is currently undertaking a pilot to accept secure, Web-based transmission of ROE data from employers over the Internet. HRDC will deploy two versions of Web ROE: one aimed at low-volume users where individual browser forms will be completed and submitted in an interactive, real-time process; and the another for higher volume users where bulk FTP transfers will submit several ROEs for validation

and acceptance. Since both processes involve the transmission of sensitive personal data, there is a requirement for security services and mechanisms to protect the confidentiality, integrity and authenticity of the exchanged information. In addition to the risk of divulging sensitive information about employees, fraudulent use of ROE forms can cost taxpayers an estimated $5,000 per misdirected or fraudulently obtained form. Entrust-based PKI is the basis of HRDC's strong authentication, encryption and digital signature services.

16 Customs Internet Gateway Project

The Customs Automated Data Exchange (CADEX) system was implemented in 1988 as a system to permit the transmission of data from importers/brokers to Revenue Canada. The Customs Internet Gateway Project will develop a facility to send and receive CADEX, CUSDEC, ACROSS and RNS data over the Internet. Security is to be provided by PKI. The CCRA will manage a Certification Authority for the purpose of issuing PKI certificates to its business partners. The CCRA PKI is based on the Entrust product suite. Participants will be registered and issued a CCRA PKI certificate, the software package required to access the certificate (i.e. Entrust Entelligence), and a user installation guide. The license of the software and certificate belongs to the CCRA and is to be used for CCRA business only.

17 GENet Secure Remote Access (SRA)

Secure Remote Access (SRA) is a Virtual Private Network service from the Government Telecommunications and Informatics Services (GTIS) on the Government Enterprise Network (GENet). It provides departments with remote dial-in or department-to-department dedicated access to their LAN/WAN Intranet services in a highly secure manner up to the Protected B level. This enables government users, whether teleworkers at home, business travellers on the road or from a mobile office, to securely access their departmental Intranet for e-mail, applications, files, databases and more. SRA is based upon a proven encryption and authentication suite of products and the Government of Canada Public Key Infrastructure (GOC PKI).

5.3 The Netherlands

5.3.1 Legal situation

The Ministry of Justice and the Ministry of Transport, Public Works and Water Management, which also supervises the telecommunications and Internet sectors, have prepared a proposal for an electronic signature act. This act will implement the EU Directive on electronic signatures and will provide changes to the Dutch Civil Code as well as the Dutch Telecommunications Act. Apart from the provisions of the EU Directive, which will probably be almost integrally derived from the Directive, the proposal is also expected to include a broadly-scoped and open provision concerning the legal recognition of electronic signatures following the example of the UNICTRAL Model Law on Electronic Commerce.

In March 1998, a special working group of the Ministry of Justice published a report which favoured the approach introduced by the UNCITRAL in its Model Law on Electronic Commerce: the functional-equivalence approach. The electronic document and electronic signature must be functionally equivalent or, in other words, fulfil the same relevant functions as a paper document with a manual signature. Amongst these functions are: the evidential function, the information and communication function and the protection of third parties. The proposal is expected to pass through parliament mid-2001.

5.3.2 Governmental approach to PKI

In the summer of 1999, a special group within the Dutch government on Information Security (ACIB) performed a study into the use of PKI technology for the Dutch government. The study concluded the following:

- that for further development of electronic government a system that allowed the proof of electronic identities (authentication) was needed;
- that PKI technology was best suited for this goal and that there was a general support both within the government and in the market for using PKI technology;
- that a future governmental PKI should be partly set up by government and partly be outsourced to commercial parties;
- that a co-ordinated approach to setting up a governmental PKI was needed to allow for sufficient flexibility to accommodate differences between departments while ensuring interoperability.

As an outcome of the study the Council of Ministers established the PKI Taskforce that started early 2000.The objective of the PKI Taskforce is to realise a workable and reliable infrastructure for PKI services covering a single security level for the communication needs of the government. The chosen security level should be sufficient to cover 80% of the communication and security needs. The PKI Taskforce published its project plan for the year 2000. This plan defines the short-term objectives: to analyse requirements and participate in experiments in order to gain knowledge to be leveraged for the long-term objective.

The project plan states the following:

- The Taskforce scope includes not only intra-governmental communications, but also communication with citizens and businesses. Solutions should be generic and portable from one domain to another;
- PKI is merely an enabler and the Taskforce is studying the most effective methods to achieve this supporting role. However, deploying this technology in applications and changing back-office processes remains the responsibility of the individual departments;

- The PKI to be developed should be able to support 80% of the governmental communications needs. For state secrets and other 'top secret' information different solutions may be needed. However, these solutions should still be able to interoperate with the regular systems based on the 'basic' PKI solution;

- The users of the PKI services should be able to do so easily (user-friendliness requirement);

- The following specific tasks have been defined for the Taskforce:

  - To realise a common governance and management structure for governmental PKI services;
  - To prepare decision-making on this subject in the council of ministers;
  - To solve legal, policy, technical and organisational issues relating to PKI services;
  - To participate in standards-making activities of industry and other standardisation bodies;
  - To develop migration strategies;
  - To ensure that the solution is interoperable on an international scale;
  - To promote the possibilities of PKI and to educate governmental departments (especially higher management);
  - To identify and support PKI pilot projects within the government relating to implementing, testing and safeguarding interoperability.

In April and May 2001, the PKI Taskforce has published a series of draft documents stating the requirements for the governmental PKI relating to security, technical interoperability, governance policies and user-friendliness. These include a generic Certificate Policy and certificate profiles for use by the Dutch government. The objective of publishing these documents – while still in draft stage – is to be able to solicit feedback from all stakeholders of the governmental PKI (including non-governmental entities like potential suppliers). In this manner, the Taskforce expects to gain a wide acceptance as well as a high quality of implementation. The implementation is planned for 2003.

The PKI Taskforce has used the European standards, of which some are still under development, as a starting point and has supplemented where necessary. This includes:

- A further detailed statement of requirements; for example where the European standards state that the revocation of a certificate should be published 'timely', the Taskforce has specified 'within 4 hours'. In addition, the Taskforce will require that the current status of every certificate will be validated;

- Formulating additional requirements relating to confidentiality services: the European standards focus on digital signature services, whereas the Dutch government will also need certificates to be used for encryption of data that needs to remain confidential;

- Formulating additional requirements relating to certificate usage for non-human entities. The government will need certificates for legal entities as well as for automatic processes (computer systems). These are not addressed in the European standards.

5.3.3 Organisation and architecture

The Dutch governmental PKI will have three different hierarchical levels of which the first two form the governance / policy setting levels while the third one is the operational level. At this level the direct interaction with the users takes place. The three levels are:

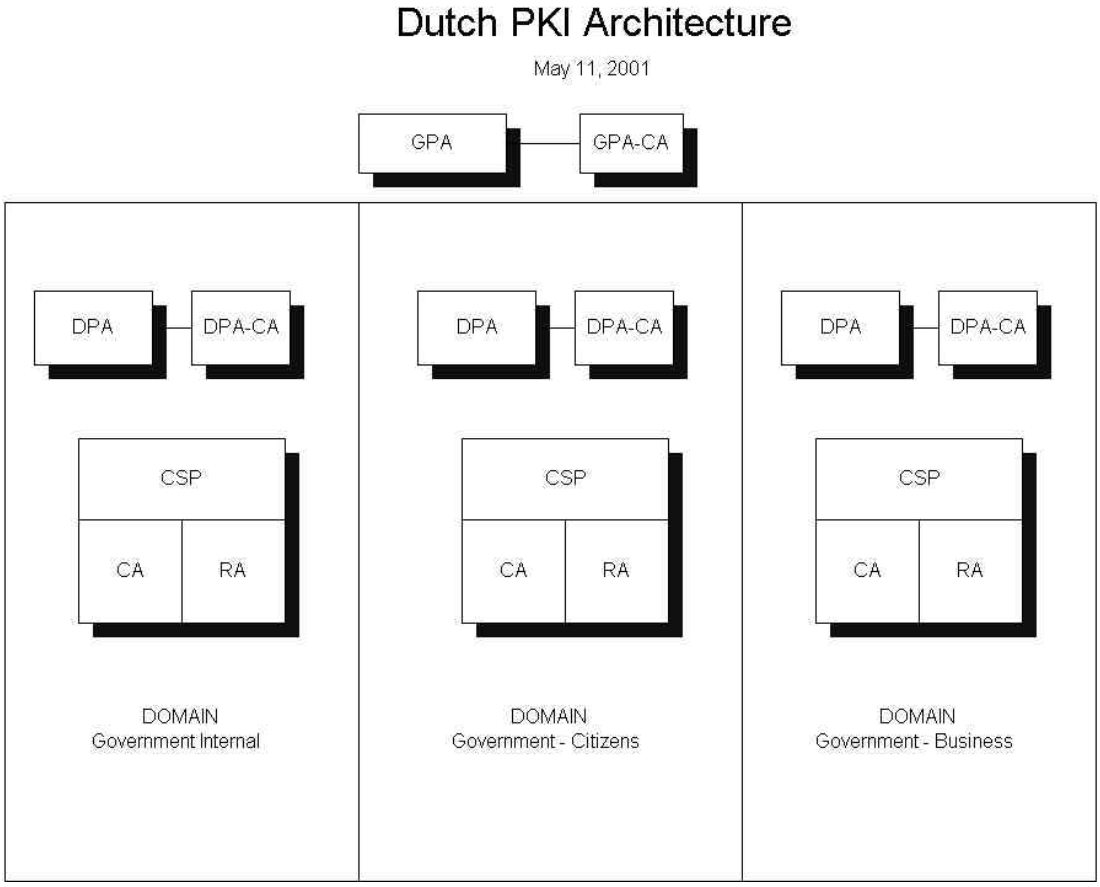
Government level: at this level the overall standards for PKI usage in the government are set by the Government Policy Authority (GPA). Its main objective is to realise interoperability.

Domain level: three different domains (government, citizens and businesses) exist, each with its own Domain Policy Authority (DPA). The DPA is established to define domain-specific policies (based on the standards defined by the GPA) to take into account the specific requirements of these domains. For example, the process of issuing a certificate to citizens is expected to deviate considerably from that of issuing a certificate to a civil servant.

CSP level: at this level the Certification Service Providers (CSP) operate. The term CSP is used in accordance with the definition of the European Directive on electronic signatures. A CSP holds the final responsibility for the provision of the certification services and hence for the issuing of certificates to end-entities. Within the CSP the Certificate Authority (CA), that is responsible for creation of certificates, and the Registration Authority (RA), who is being responsible for verifying the subscribers' identity, are distinguished. The CA and RA functions may be performed by different parties or departments.

There can be multiple CAs and RAs under a single CSP. According to the Taskforce, a CA will issue only one type of certificate. An RA can have relationships with more then one CA.

The governmental PKI has a hierarchical structure, which means that there are CAs at the two top levels as well. The GPA-CA issues certificates to the DPA-CAs. Each DPA-CA will issue certificates to the CSPs below it. The self-signed certificate of the GPA-CA forms the ultimate central point of trust within the governmental PKI. The following figure visualises this hierarchy.



The DPA will only issue a certificate to a CSP after it has verified that the CSP operates according to the required standards. The PKI Taskforce has defined these standards in the draft document 'General Certificate Policy' which is based on the ETSI document 'Policy Requirements for CAs issuing Qualified Certificates' (ETSI TS 101456). The GPA may cross-certify with CSPs that are outside the governmental PKI.

Other relevant aspects:

- The Taskforce aims at limiting the number of different types of certificates / digital signatures. In particular it is desirable to have only one signature per citizen that is used in all his or her communications with the government;

- As a consequence, the Taskforce aims at providing only a single level of trust;

- The certificates / digital signatures are role-based: at present the Taskforce has identified the need for a citizen's certificate as well as for a 'civil servant in function' certificate. The latter can sign for his or her employer. Other types are expected;

- The certificate for citizens will only contain a limited set of data. For example, only name and number (a durable personal identifiable number to realise a persistent connection to the respective person's data in the back-office systems). This will reduce any privacy issues in conjunction with using certificates. For civil servant certificates the respective organization will have the opportunity to include additional data;

- The Taskforce expects to use smart cards as the standard token of private keys and digital certificates. However, depending on the specific implementation or usage, deviations will be possible and allowed if needed;

- There will be separate certificates for digital signatures on the one hand and encryption / confidentiality on the other hand;

- The supervision of certified CSPs is the responsibility of the OPTA (Onafhankelijke Post and Telecommunicatie Autoriteit), CSPs may elect whether they would like to self-certify or let an independent, accredited organisation certify them. It is expected that market forces will lead to most CSPs being certified by independent assessors

5.3.4 Initiatives

The communication processes that the government is involved in define the domains the PKI Taskforce distinguishes. The Dutch government includes bodies at state, provincial, and city level, as well as semi state-controlled (associated) institutions and the social security (insurance) organisations. It is considered necessary to have multiple domains as each domain has a different target group with communication processes that lead to different PKI requirements. Three domains are distinguished:

?? government-citizen;

?? government-business;

?? intra-government.

Government – Citizen

In the domain government – citizen, the PKI Taskforce anticipates the following application areas that will need a PKI:

- Electronic voting;

- The digital government desk;

- Numerous applications for the Tax office;

- Student loans administration;

- Social benefits administration;
- Central Collection Bureau for Justice department (tickets payment etc.);
- Land register;
- Lodging of objections (appeals);
- Requests for subsidies and licenses.

Within this domain the following (pilot-) projects are underway:

- EasyTax: a project at the Tax office relating to the different forms of electronic tax returns for citizens;
- A pilot project of the social service of Delft which encompasses:
  - Remote completion of working forms;
  - Electronic delivery of income statements;
  - Entering / removal of unemployed;
  - Entering of available jobs and candidates;
- Digital ID card: the Dutch Organisation of Cities is working on a digital ID card that allows citizens to interact with their local authority via the Internet.

Government - Business

In the domain Government – Business the following application areas are anticipated:

- Tax applications;
- Electronic public tendering;
- Lodging of objections (appeals);
- Requesting subsidies and licenses.

Pilot projects in this area are a number of projects at the Tax office (EDI-tax, Wages-tax & VAT, Transit (electronic processing of international transports) and electronic request for the Euro-vignette) and projects at the Chamber of Commerce (for querying and updating the register of companies via the Internet).

Government -Government

In the domain Government – Government the following application areas have been identified:

- The State Government Intranet
- Secure e-mail within the government;
- Remote access for people working at home (telecommuting).

Specific projects in this area:

- Secure mobile communication for customs and the police;
- Secure e-mail for the Justice department.

5.4 Sweden

5.4.1 Legal situation

On 18 May 2000, the government introduced a proposal in Parliament for legislating electronic signatures. In November 2000, the Swedish Parliament has approved the Act on Qualified Electronic Signatures, which implements the EU Directive on Electronic Signatures. This Act has entered into force on 1 January 2001.

The Post and Telecom board is appointed to supervise the issuers of qualified certificates.

5.4.2 Governments approach to PKI

During the late 1990s, the Swedish national, regional and local government has co-operated in the Top Managers' forum concerning strategies for the use of smart cards for identification purposes. The Swedish government liaises closely with industry and the financial institutions through the Secure Electronic Information in Society (SEIS) orgnaisation, a non-profit entity whose work is targeted on introducing smart card solutions for utilisation in several parts of Swedish society. Specifications in the area of certificate format, Certification Authority policy, and on-board smart card file structures have been defined. Norway has adopted the SEIS standards in its own specifications as well.

The ICT Commission, an advisory body to the Swedish government in the field of information technology, has recommended establishing a committee to stimulate and co-ordinate the usage of PKI within and by the government. Next, the cabinet of ministers has appointed a commission with representatives of the Swedish Tax board, Social Insurance

board, the Patent and Registration office and Statskontoret. The commission has started a project to co-ordinate and stimulate the use of PKI for government electronic services.

5.4.3 Organisation and architecture

The PKI commission in Sweden distinguishes two areas:

- Certificates for usage within government agencies and departments;
- Certificates for usage by citizens in their communication with the government (both central and local).

Sweden does not intend to establish a governmental PKI; certificates for both areas are to be provided by commercial parties in the market. To this end, two different procurement frameworks have been defined.

For issuing certificates for the governmental internal area a contract is being established with Swedish Post and Telia (and possibly some other vendors). Under this contract a governmental agency or department can procure certificates for its specific application.

For issuing certificates to be used by citizens in their communications with the government, the commission is in negotiation with different parties – including most of the banks. It is expected that with a number of these parties contracts will be established under which they are able to issue government certificates to their customers. For example, when a new Internet banking customer is being 'connected' by the bank, at that stage the customer can receive a government certificate issued by that bank. This is independent whether or not the customer needs a certificate for the Internet banking application.

The commission has not formulated any specific Certificate Policy (CP) as such. Since these are often comprehensive documents, they do not expect that it will hold up in court. In other words: the judge will not hold citizens responsible for complying with the rules in a CP if that document is too difficult to understand for the average citizen. Instead, the commission has formulated different sub-sets (limited policies) relating to specific areas that are normally dealt with in a CP. These policies are based on the ETSI standard and will be part of the contract between the government and the CA, as well as part of the user agreements.

The certificate will probably contain the national ID number that each citizen holds. These numbers are widely used by the back-office systems of the government, making it more convenient for all parties involved to use certificates with these systems. However, as using a national ID number has certain implications, no decision has been made as of the time of this study.

The government agency that uses a certificate issued by a bank will in most likely have to pay the CA when validating a certificate (on a transaction basis). The banks are probably

going to use a collective ICT infrastructure for providing these validation services (though each will issue its own certificates).

None of the above is going to be mandatory, so governmental departments and agencies may procure certificates under their own terms, or even set up an internal, closed PKI.

Smart cards are viewed as the preferred or standard storage device for keys and certificates in the near future. At present the technology is considered too complex for large deployments.

5.4.4 Initiatives

The Tax office is currently performing a pilot with a group of companies for their monthly tax declarations. For this pilot standard certificates from Swedish Post are used.

A number of Swedish agencies anticipate the use of digital certificates as the basis for providing electronic services to the public. These services include student loan applications, start-up of companies and applications for health insurance.

The government has started a portal called “24 hours government” that at present provides forms and information as well as a job-matching application. For an increasing number of anticipated applications, that the application of a digital signature is required.

6 Conclusions

6.1 Introduction

In this final chapter the major findings of the study are presented. Next, some considerations are discussed and possible next steps are recommended.

6.2 Findings

6.2.1 Situation in Iceland

The findings of this study clearly show that within the government of Iceland numerous applications are anticipated that will need or at least benefit from applying and using PKI technology. Most of the departments and agencies interviewed expect that they will use digital signatures and encryption based on digital certificates.

No significant differences were identified in requirements for PKI between the three domains (government internal, government – citizens and government - business). However, it must be noted that very few applications have actually reached a project development or implementation phase yet (hence the word *anticipated* above), which lead to the result that detailed requirements could only be identified to a limited extent. Exceptions which are further along include the identified applications at the Tax Office, Customs and the Student Loan Fund. The latter outsourced its application to Form.IS which has more governmental customers in need for digital signatures.

Based on our discussions with some of the Icelandic banks, it has become clear that they are planning to issue smart cards to all of their customers starting later this year. This fact may be of relevance due to the possibility that private keys and digital certificates may be stored on such a card. In addition, the banks have stressed that they are more then willing to participate with the government on these PKI and smart card matters. We can also conclude that most governmental departments have in principle no objection to using a certificate that was issued by a private company. We note that the present banking card is used as a de-facto ID by many – public and private – organisations in Iceland, even though officially it is not.

6.2.2 Other studied countries

When looking at the PKI initiatives in Canada, the Netherlands and Sweden, the following tentative conclusions can be drawn:

- It is clear that Canada is at least a few years ahead in using PKI technology for e-government applications. The type of applications that this study identified are to a large extent similar to those anticipated in Iceland. This fact supports the conclusion that Iceland may benefit from using PKI technology and be aligned to the Canadian

approach where possible. Though the Netherlands and Sweden are not nearly as far as Canada, they also have a clear view that PKI technology is required to be able to fulfil the security needs of e-government applications.

- Canada and the Netherlands have a similar approach to deploying the governmental PKI. In both countries a co-ordinating infrastructure (made of both organizational and legal standards and technology) is put in place to facilitate departments that want to use PKI technology. By using a common approach and standards, the result is an interoperable infrastructure. In Sweden a simpler model is used, defining a government certificate for citizens that can be issued by multiple private organizations (e.g. the banks). However, these CSPs are not operating under a common root (public) CA.

- Both the Netherlands and Sweden use the European standards (ETSI) as a basis for their own policies. They both expect smart cards to emerge as the standard storage device for keys and certificates in the (near) future.

6.3 Considerations

This report has identified the need for PKI technology for deploying Iceland's e-government applications. It also looked into the approaches that some other countries took in meeting their e-government trust and security objectives. Emerging from this is the overall conclusion that further action from the Icelandic government is required. Related to this are the following considerations:

Timing

The study showed no pressing need for PKI functions at this point in time but given the anticipated governmental applications this need will manifest itself within the near future. Establishing a structure capable of fulfilling this need requires substantial effort and time. Therefore, further action on this matter should commence shortly to be able to service the governmental departments and agencies when required. In this way the risk of the arising of non-interoperable PKI-islands (e.g. different certificates for each governmental application) can be avoided.

Building expertise within the government

As stated before PKI technology is a complex matter and little knowledge regarding its development and usage is available either within the private or public sector. The process of the government of Iceland becoming a large user of this technology will be most effective if at least a certain level of expertise if

available from internal governmental employees. This expertise should cover organisational, legal as well as technical aspects of PKI.

International Governmental Forum

Iceland is not the only country to adopt PKI technology for e-government applications. Numerous other nations have done so of which some quite early. Participating in the international platforms (forums) that exist on (governmental) PKI, provides the opportunity to learn from the experiences of others.[4]

6.4 Recommended next steps

As mentioned in the introduction, the requirement analysis is an important yet initial step in the process of developing the PKI approach for the government of Iceland. Next steps in this process should include the following:

Develop alternative scenarios for fulfilling the digital certificates needs (requirements)

Insight in the different options and their respective advantages and disadvantages can be derived from developing a number of likely scenarios in which the digital certificate needs can be fulfilled. These scenarios should distinguish between – amongst others – the level of in/outsourcing or corporation with other parties; the scope of certificate usage, the usage domains distinguished. The consequences on or interdependencies with the government's PKI originating from the Icelandic legislation should be reckoned with in building the scenarios. Financial consequences should also be analysed. Another critical subject to be addressed in this step is the reciprocal impact in the event a national ID card will be used in Iceland.

Determinethe PKI approach

In this step the most favourable and feasible (combination) of scenario(s) is chosen.

Develop initial PKI Trust and Governance Model

A PKI Trust Model describes the position and roles of the different PKI components and should be based

[4] One particular useful forum (which is only open to governmental employees) is organised by the Chair of the Federal PKI Steering Committee (of the U.S.A.) Judy Spencer (judith.spencer@gsa.gov or 202-208-6576202-208-6576).

on the government of Iceland organisational structure and ICT infrastructure. The Governance model describes how the PKI is controlled and kept trustworthy. A Policy Management Authority or similar committee may be established that defines standards and sets policies as a main component of a Governance model.

Set up initial government PKI organisation and start with implementing a few pilot projects

It is recommendable to use a phased approach for the PKI deployment and to start with a limited number of pilot projects in areas where a successful implementation is most likely. In these projects, the embedding of PKI within the overall security architecture needs to be addressed. The results of these projects will provide valuable insights and expertise for determining the preferred approach for all government-led PKI deployments.

A Overview of interviews

Organisation name	Organisation name	Interviewed persons
Federation of Icelandic Industries ICEPRO	Samtök atvinnulífsins	Guðmundur Ásmundsson Stefán Jón Friðriksson
Statistics Iceland	Hagstofa Íslands	Eiríkur Hilmarsson Skrifstofustjóri, Davíð
The National Archives of Iceland	Þjóðskjalasafnið	Bjarni Þórðarson, Eiríkur G. Guðmundsson Ólafur Ásgeirsson
The Icelandic Tax Authority	Ríkisskattstjóri	Ómar Ingólfsson
Icelandic Registration Office	Skráningarstofan hf	Þorvardur Kári Ólafsson Birgir Hákonarson Sandra Baldvinsdóttir
Data Protection Agency	Persónuvernd	Hörður H. Helgason Sigurður Guðmundsson
Bank of Iceland Iceland Agricultural Bank Audkenni	Íslandsbanki-FBA Búnaðarbanki Íslands Auðkenni	Haukur Oddsson, Ingi Örn Geirsson Guðlaugur Sigurgeirsson
Skýrr	Skýrr	Jóhann Kristjánsson Atli Arason
Icelandic Banks Data Centre		Bjarni G. Olafsson
Directorate of Customs	Ríkistollstjóri	Karl F. Garðarsson Ragnar Gunnar Þórhallsson
Ministry of health	Heilbrigðisráðuneytið	Þorgeir Pálsson Ingimar Einarsson Daði Einarsson
Division of Health Statistics	Landlæknir	Sigridur Haraldsdóttir Guðrún Kr. Guðfinnsdóttir
State Social Security Institute	Tryggingastofnun	Hermann Ólason
National Hospital	Landspítali Háskólasjúkrahús	Björn Gunnarsson Þorgeir Pálsson
National Audit Office	Ríkisendurskoðandi	Albert Ólafsson
Form.IS	Form.is	Guðmundur Óskarsson
The Land Registry of Iceland	Fasteignamat ríkisins	Haukur Ingibergsson Sigurjón Friðjónsson
Swedish PKI governmental commission		Dag Osterman (project leader)
Dutch PKI Task Force		Michel Bouten (project leader)
Smarttrust (ID2)		Simon Corell

B References

- 'Advances and Remaining Challenges to Adoption of PKI Technology', US General Accounting Office, February 2001
- 'A coordinated Policy for the development of Electronic Commerce', The Ministry of Industry, Employment and Communication, Sweden
- 'Digital signature and confidentiality policies for the GOC PKI', version 3.02 April 1999
- 'Digital Signatures, a technological and legal overview', Swedish interministerial working group on digital signatures, February, 1998
- 'e-Europe 2002 Impact and Priorities', Spring European Council, Stockholm, March, 2001
- 'Electronic Government for New Zealand: Managing the transition', Brendan Boyle, June, 2000
- 'Government of Canada Public Key Infrastructure – White Paper', Government of Canada, Communications Security Establishment (CSE), 1998
- 'Government of Canada PKI Cross Certification Methodology and Criteria V1.0', April, 2000
- 'Information Age Government, Benchmarking Electronic Service Delivery', UK Central IT Unit of the Cabinet Office, July 2000
- 'PKI in Practice: Government of Canada Pathfinders Leading the Way', (http://www.cio-dpi.gc.ca/pki-icp/pathfinders/project_e.asp)
- 'PKI Overheid: Eisen en Wensen (deel 1 t/m 4) versie concept', Taskforce PKI Overheid, april 2001
- 'Plan van aanpak 2000 PKI Overheid', Taskforce PKI Overheid, maart 2000
- 'Policy for Public Key Infrastructure Management in the Government of Canada V1.0', May, 1999
- 'Policy requirements for certification authorities issuing qualified certificates' European Telecommunications Standards Institute (ETSI), 2000
- 'The Government 's Proposal in Government Bill 1999/2000:86 "An information society for all ", Ministry of Industry,Employment and Communications, Sweden March 2000

✍✍ 'Trusted Services and PKI, an ICA Study Group Report', International Council for Information Technology in Government Administration.

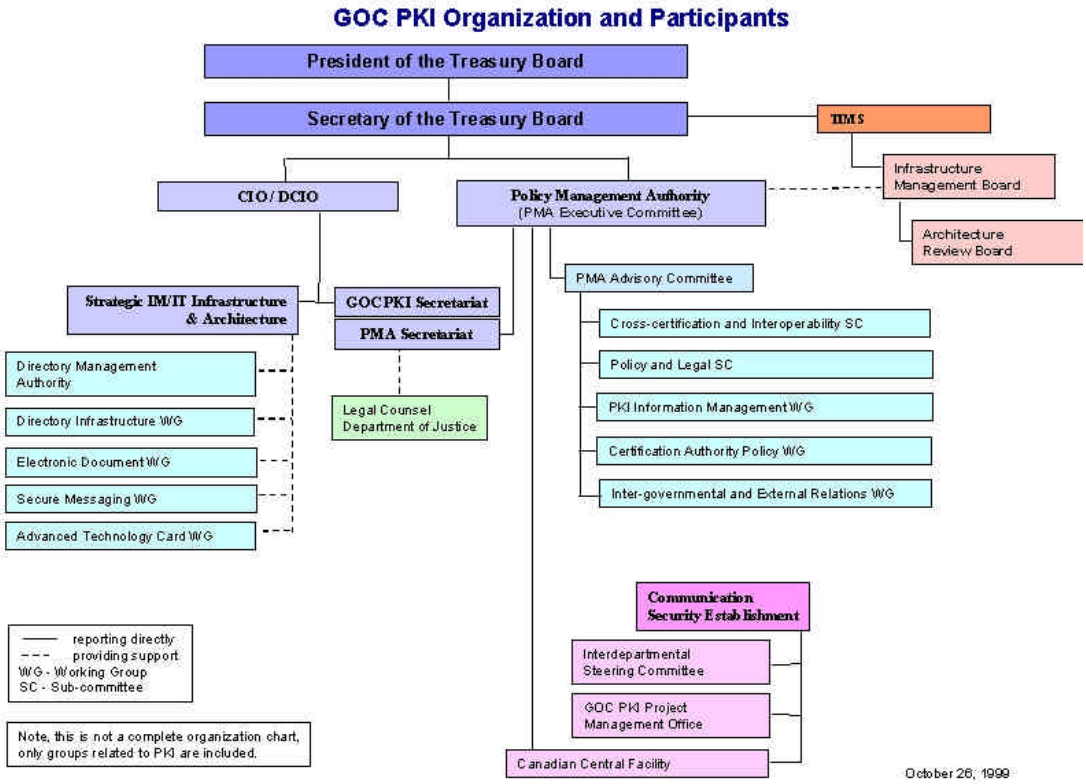
✍✍ 'Trusted Third Party diensten voor de Rijksoverheid', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag 1999

✍✍ 'Using Electronic ID-cards, a guide for users and application developers', SEIS, Sweden

✍✍ 'Webtrust Program for Certification Authorities v1.0', AICPA/CICA, August 2000

C The Government Of Canada PKI Team

The GOC PKI Team is an interdepartmental network of federal departments and agencies, committees, sub-committees, and working groups. The picture below provides an overview of this.



Below is a description of the different responsibilities.

The President of the Treasury Board, on the advice and recommendation of Secretary of the Treasury Board, is responsible for entering into and terminating written arrangements for cross-certification on behalf of the government.

The Secretary of the Treasury Board is responsible for co-ordinating and setting overall direction for PKI management within the government.

The Policy Management Authority (PMA) is a senior executive committee responsible to the Secretary of the Treasury Board for the direction and management of the GOC PKI and for providing overall strategic directions for GOC PKI. It makes recommendations to the Secretary with respect to membership in the GOC PKI and cross-certification. The PMA also provides a link to the of the Information Management Sub-Committee (TIMS) of the

Treasury Board Secretariat Advisory Committee (TBSAC), the Advisory Committee on Information Management (ACIM) and the Information Management Board (IMB).

The Policy Management Authority Executive Committee (PMA EC) is a committee of the PMA that acts on behalf of the PMA between meetings of the PMA. The PMA EC deals with routine matters or decisions that must be made promptly. It comprises the Chair and Deputy Chair of the PMA and at least four other members of the PMA appointed by the Chair. Other members of the PMA may choose attend the PMA EC. The Terms of Reference of the PMA EC are set by the PMA and the decisions of the PMA EC are as binding as if the PMA made them; however, PMA EC decisions may be appealed to the PMA.

The Policy Management Authority Secretariat supports the PMA and the Secretary concerning their respective responsibilities for the direction and management of GOC PKI.

The Policy Management Authority Advisory Committee (PAC) is an interdepartmental committee of PKI executives, managers and experts mandated by the Policy Management Authority (PMA) to oversee the establishment and operation of the GOC PKI management structure and policy framework. The PAC provides support to the PMA by:

- reviewing and commenting on documents, proposals, etc. - referred to it for consideration, including submissions to PMA;
- reviewing questions or studying issues sent to it by the PMA and providing advise to the PMA on them;
- assisting the GOC PKI Secretariat, as appropriate, in the development of policies and other documents, intended for submission to the PMA;
- discussing issues concerning GOC PKI tabled by PAC members or others in areas related to GOC PKI and, where appropriate, advising the PMA on these issues and their resolution;
- obtaining their departments' positions on all items tabled for discussion at subsequent PAC meetings; and
- reporting to appropriate officials in their departments on all GOC PKI decisions, initiatives and plans that are discussed at PAC meetings.

The **Communications Security Establishment** manages and operates the Canadian Central Facility, which, under Policy Management Authority (PMA) direction, serves as the Government of Canada's central Certification Authority and provides a source for:

- technical assistance, technical support and support to the PMA on PKIs;
- information technology security advice to the PMA;

- technical advice related to cross-certification; and

- training related to technologies employing public key cryptography.

The Canadian Central Facility: signs and manages the cross-certificates of top-level (Level-1) departmental Certification Authorities and non-departmental Certification Authorities.

The GOC PKI Secretariat has been created within the CIO Branch of TBS and is responsible for:

- the provision of staff and operational support to the Policy Management Authority (PMA) and the PMA Advisory Committee (PAC) in the discharge their responsibilities;

- chairing, and/or acting as secretary to, the PMA, the PMA Advisory Committee and all committees and working groups reporting to the PMA Advisory Committee;

- the corporate management structure and policy framework for GOC PKI;

- resolving legal, policy, technical and operational issues related to GOC PKI;

- encouraging and supporting PKI projects undertaken by departments, as well as selected Pathfinder Projects;

- developing and revising cross-certification arrangements for interoperability of public key infrastructures within the government and with external public key infrastructures operated by other governments and the private sector;

- increasing awareness, understanding and acceptance of PKI among government departments including the production of position papers to promote discussion and resolution of PKI issues; and

- liaising with provincial, territorial, other national or state governments, corporations, and businesses, and speaking at conferences and trade shows to promote PKI and common interoperability standards for PKI.

GOC PKI Committees and Working Groups

A number of additional interdepartmental committees and working groups have been established with assignments related to PKI implementation, standards development and electronic commerce.

Committees and Working groups reporting to the Policy Management Authority Advisory Committee:

- Certification Authority Policy Working group (CAP)
- Cross-Certification and Interoperability Sub-committee (X-CIS)
- Intergovernmental and External Relations Working Group (IER WG)
- PKI Information Management Working Group (PIM WG)
- Policy and Legal Sub-Committee (PALS)

Committees and Working groups reporting to the TBS/CIOB Strategic IM/IT Infrastructure and Architecture initiative:

- Advanced Card Technology Working Group (ACT WG)
- Directory Management Authority (DMA)
- Directory Infrastructure Working Group (DI WG)
- Electronic Document Working Group (ED WG)
- Secure Messaging Working Group (SM WG)

D Introduction to PKI

The text below provides an introduction to PKI.

(source: 'Webtrust Program for Certification Authorities v1.0', AICPA/CICA, August 2000)

What is a Public Key Infrastructure?

With the expansion of e-commerce, PKI is growing in importance and will probably be the most critical enterprise security investment a company will make in the next several years. PKI enables parties to an e-commerce transaction to identify one another by providing authentication with digital certificates, and allows reliable business communications by providing confidentiality through the use of encryption, and authentication, data integrity, and a reasonable basis for nonrepudiation through the use of digital signatures.

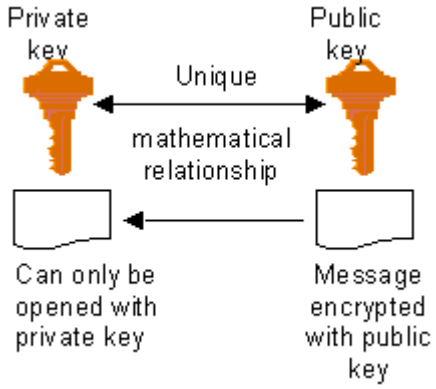
PKI uses public/private-key pairs–two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust in e-commerce transactions, namely: confidentiality, authentication, integrity, and nonrepudiation.

Using PKI, a subscriber (meaning, an end entity (or individual) whose public key is cryptographically bound to his or her identity in a digital certificate) has an asymmetric cryptographic key pair (meaning, a public key and a private key). The subscriber's private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a digital certificate to ensure that relying parties know with confidence the identity to which the public key belongs. Using public key cryptography, the subscriber could send a message signed with his or her private key. The signature can be validated by the message recipient using the subscriber's public key. The subscriber could also encrypt a message using the recipient's public key. The message can be decrypted only with the recipient's private key.

A subscriber first obtains a public/private key pair (generated by the subscriber or for the subscriber as a service). The subscriber then goes through a registration process by submitting their public key to a Certification Authority or a Registration Authority (RA), which acts as an agent for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (that may be contained in a Certification Practice Statement), and then issues a digital certificate. The certificate includes the subscriber's public key and identity information, and is digitally signed by the CA, which binds the subscriber's identity to that public key. The CA also manages the subscriber's digital certificate through the certificate life cycle (meaning, from registration through revocation or expiration). In some circumstances, it remains important to manage

digital certificates even after expiry or revocation so that digital signatures on stored documents held past the revocation or expiry period can be validated at a later date.

The following diagram illustrates the relationship between a subscriber's public and private keys, and how they are used to secure messages sent to a relying party.



A transaction submitted by a customer to an online merchant via the Internet can be encrypted with the merchant's public key and therefore can only be decrypted by that merchant using the merchant's private key—ensuring a level of confidentiality. Confidentiality can also be achieved through the use of Secure Socket Layer (SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), and other protocols, such as Secure Electronic Transaction (SET).

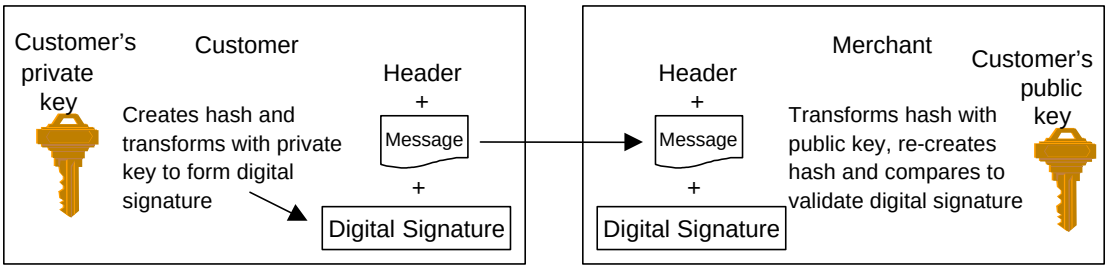
What is a Digital Signature?

Digital signatures can be used to provide authentication, integrity, and nonrepudiation. Generally speaking, if a customer sends a digitally signed message to a merchant, the customer's private key is used to generate the digital signature and the customer's public key can be used by the merchant to verify the signature. The mathematical processes employed are somewhat different depending on the kind of asymmetric cryptographic algorithm employed. For example, the processes are slightly different for reversible algorithms (i.e., those which can be readily used to support digital signatures as well as encryption) such as Rivest Shamir Adleman (RSA) and irreversible algorithms such the Digital Signature Algorithm (DSA).

The following example illustrates the digital signature generation and verification process for a reversible asymmetric cryptographic algorithm (such as RSA). Suppose a customer wants to send a digitally signed message to a merchant. The customer runs the message through a hash function (meaning, a mathematical function that converts a message into a fixed length block of data, the hash, in a fashion such that the hash uniquely reflects the message – in effect, it is the message's "fingerprint"). The customer then transforms the hash using the

algorithm and the customer's private key to create the digital signature which is appended to the message. A header is also appended to the message, indicating the merchant's email address, the sender's email address, and other information such as the time the message is sent. The message header, the message itself, and the digital signature are then sent to the merchant. The customer can optionally send his/her public key certificate to the merchant in the message itself. All of this is usually done by the e-mail software in such a way that the process is transparent to the user.

The following diagram illustrates the process of using a subscriber's key pair to ensure the integrity and authenticity of a message sent by the customer (subscriber) to a merchant.



To determine whether the message came from the customer (meaning, authentication) and to determine whether the message has not been modified (meaning, integrity), the merchant validates the digital signature. To do so, the merchant must obtain the customer's public key certificate. If the customer did not send his or her public key certificate as part of the message, the merchant would typically obtain the customer's public key certificate from an online repository (maintained by the CA or another party acting as the agent of the CA, or any other source even if unrelated to the CA). The merchant then validates that the customer's digital certificate (containing the customer's public key) was signed by a recognized Certification Authority to ensure that the binding between the public key and the customer represented in the certificate has not been altered. Next, the merchant extracts the public key from the certificate and uses that public key to transform the digital signature to reveal the original hash. The merchant then runs the message as received through the same hash function to create a hash of the received message. To verify the digital signature, the merchant compares these two hashes. If they match, then the digital signature validates and the merchant knows that the message came from the customer and it was not modified from the time the signature was made. If the hashes do not match, then the merchant knows that the message was either modified in transit or the message was not signed with the customer's private key. As a result, the merchant cannot rely on the digital signature.

Digital signatures can also be used to provide a basis for nonrepudiation (meaning that the signer cannot readily deny having signed the message). For example, an online brokerage customer who purchases one thousand shares of stock using a digitally signed order via the Internet should have a difficult task if he or she later tries to deny (meaning, repudiate) having authorized the purchase.

What are the Differences Between Encryption Key Pairs and Signing Key Pairs?

As stated earlier, establishing a reasonable basis for nonrepudiation requires that the private key used to create a digital signature (meaning, the signing private key) be generated and stored securely under the sole control of the user. In the event a user forgets his or her password or loses, breaks, or destroys his/her signing private key, it is acceptable to generate a new signing key pair for use from that point forward with minimal impact to the subscriber. Previously signed documents can still be verified with the user's old signature verification public key. Documents subsequently signed with the user's new signing private key must be verified with the user's new signature verification public key.

Extra care is required to secure the Certification Authority's signing private key, which is used for signing user certificates. The trustworthiness of all certificates issued by a CA depends upon the CA's protecting its private signing key. CAs often securely back up their private signing key(s) for business continuity purposes to allow the CA to continue to operate in the event that the CA's private signing key is accidentally destroyed (but not compromised) as a result of hardware failure, for example. Except for CA business continuity purposes, there are generally no technical or business reasons to back up a signing private key.

On the other hand, and as cited earlier, it is often desirable that a key pair used for encryption and decryption be securely backed up to ensure that encrypted data can be recovered when a user forgets his or her password or otherwise loses access to his or her decryption key. This is analogous to requiring that the combination to a safe be backed up in case the user forgets it, or becomes incapacitated. As a result, a PKI typically requires two key pairs for each user: one key pair for encryption and decryption and a second key pair for signing and signature verification.

What is a Certification Authority?

In order for these technologies to enable parties to securely conduct e-commerce, one important question must be answered. How will we know in the digital world that an individual's public key actually belongs to that individual? A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the answer. This document is digitally signed by a trusted organization referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate. The public keys of many common Root CAs (as later defined) are pre-loaded into standard Web browser software (for example, Netscape Navigator or Microsoft Internet Explorer). This allows the relying party

to verify the issuing CA's signature using the CA's public key to determine whether the certificate was issued by a trusted CA.

The purpose of a CA is to manage the certificate life cycle, which includes generation and issuance, distribution, renewal and rekey, revocation, and suspension of certificates. The CA frequently delegates the initial registration of subscribers to Registration Authorities (RAs) which act as agents for the CA. In some cases, the CA may perform registration functions directly. The CA is also responsible for providing certificate status information though the issuance of Certificate Revocation Lists (CRLs) and/or the maintenance of an online status checking mechanism. Typically, the CA posts the certificates and CRLs that it has issued to a repository (such as an online directory) which is accessible to relying parties.

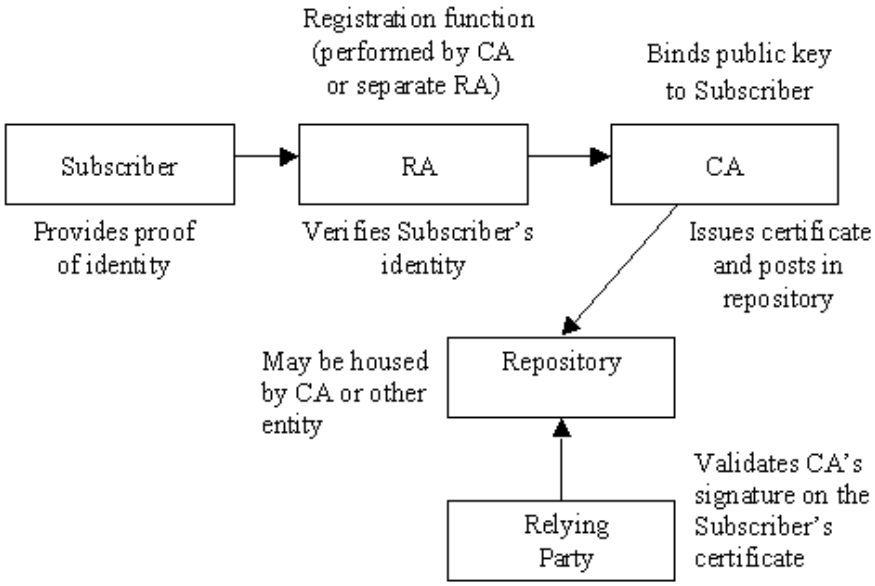
What is a Registration Authority?

A Registration Authority (RA) is an entity that is responsible for the identification and authentication of subscribers, but does not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally. In other cases, the CA might delegate the RA function to external registration authorities (sometimes referred to as Local Registration Authorities or LRAs) that may or may not be part of the same legal entity as the CA. In still other cases, a customer of a CA (for example, a company) may arrange with that CA to perform the RA function itself or using its agent. These external registration authorities are required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a Certification Practice Statement and applicable Certificate Policy(s). In performing a WebTrust for Certification Authorities engagement, the practitioner must consider how the CA handles the RA function and whether the RA function is within the scope of the examination. For example, a CA that provides CA services to several banks, might delegate the subscriber registration function to RAs that are specifically designated functional groups within each bank. The functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities examination performed for the CA. In this case management's assertion should specify those aspects of the registration process that are not handled by the CA.

The initial registration process for a subscriber is as follows, though the steps may vary from CA to CA and will also depend upon the Certificate Policy under which the certificate is to be issued. The subscriber first generates his or her own public/private key pair. (In some implementations, a CA may generate the subscriber's key pair and securely deliver it to the subscriber, but this is normally done only for encryption key pairs, not signature key pairs.) Then the subscriber produces proof of identity in accordance with the applicable Certificate Policy requirements and demonstrates that he or she holds the private key corresponding to the public key without disclosing the private key (typically by digitally signing a piece of data with the private key, with the subscriber's digital signature then verified by the CA). Once the association between a person and a public key is verified, the CA issues a certificate. The CA digitally signs each certificate that it issues with its private key to provide the means for establishing authenticity and integrity of the certificate.

The CA then notifies the subscriber of certificate issuance and gives the subscriber an opportunity to review the contents of the certificate before it is made public. Assuming the subscriber approves the accuracy of the certificate, the subscriber will publish the certificate and/or have the CA publish it and make it available to other users. A repository is an electronic certificate database that is available on-line. The repository may be maintained by the CA or a third party contracted for that purpose, or by the subscriber, or by any other party. Subscribers may obtain certificates of other subscribers and certificate status information from the repository. For example, if a subscriber's certificate was revoked, the repository would indicate that the subscriber's certificate has been revoked and should not be relied upon. The ability to update the repository is typically retained by the CA. Subscribers and other relying parties would have read only access to the repository. Because the certificates stored in the repository are digitally signed by the CA, they cannot be maliciously changed without detection, even if someone were to hack into the repository.

The following diagram illustrates the relationship between the subscriber and the RA and CA functions.



What are a Certification Practice Statement and a Certificate Policy?

A Certification Practice Statement (CPS) is a statement of the practices which a Certification Authority employs in issuing and managing certificates. A Certificate Policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular Certificate Policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

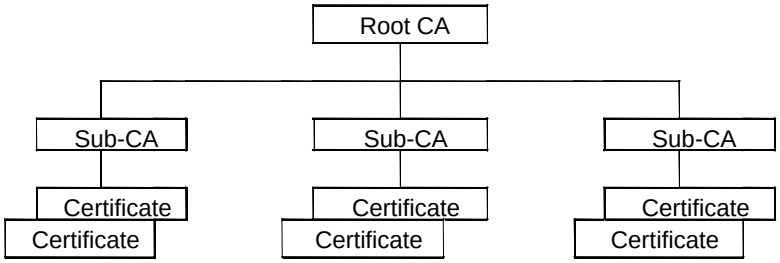
What is the Difference Between Licensed and Nonlicensed CAs?

Many countries, states, and other governmental jurisdictions have enacted or are developing digital signature laws. In those jurisdictions that have digital signature laws and provide for CA licensing, certificates issued by licensed Certification Authorities typically have a higher level of legal recognition than those issued by nonlicensed CAs. For a number of jurisdictions, the use of certificates issued by licensed CAs are provided specific recognition in those jurisdictions' digital signature laws. In the United States, for example, several state digital signature laws require that audits of Certification Authorities be performed as a requirement for licensing. One of the purposes of this document is to provide standards that would meet the requirements of various governmental jurisdictions and the marketplace.

What Are the Hierarchical and Cross-Certified CA Models?

CAs may be linked using two basic architectures or a hybrid of the two: (1) hierarchical and (2) cross-certified (shared trust). In a hierarchical model, a highest level (or "Root") CA is deployed and subordinate CAs may be set up for various business units, domains or communities of interest. The *Root CA* validates the subordinate CAs, which in turn issue certificates to lower tier CAs or directly to subscribers. Such a Root CA typically has more stringent security requirements than a subordinate CA. Although it is difficult for an attacker to access the Root CA (which in some implementations is only on-line in the rare event that it must issue, renew, or revoke subordinate CA certificates), one drawback to this model is that the Root CA represents a single point of failure. In the hierarchical model, the Root CA maintains the established "community of trust" by ensuring that each entity in the hierarchy conforms to a minimum set of practices. Adherence to the established policies may be tested through audits of the subordinate CAs and, in a number of cases, the Registration Authorities.

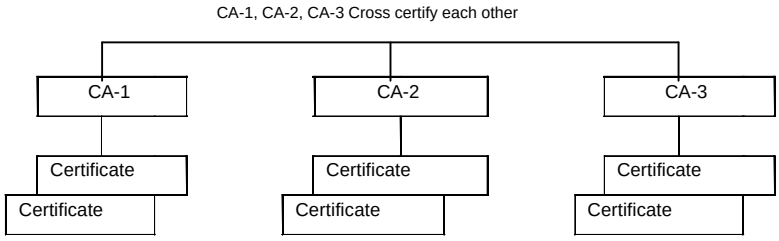
The following diagram illustrates the structure and relationships between certification authorities and subscribers operating in a hierarchical model.



In an alternative model, cross-certified CAs are built on a "peer-to-peer" model. Rather than deploying a common Root CA, the cross-certification model shares trust among CAs known to one another. Cross-certification is a process in which two CAs certify the trustworthiness of the other's certificates. If two CAs, CA1 and CA2, cross-certify, CA1 creates and digitally signs a certificate containing the public key of CA2 (and vice versa). Consequently, users in

either CA domain are assured that each CA trusts the other and therefore subscribers in each domain can trust each other. Cross-certified CAs are not subject to the single point of failure in the hierarchical model. However, the network is only as strong as the weakest CA, and requires continual policing. In the cross-certified model, to establish and maintain a community of trust, audits may be performed to ensure that each cross-certified CA conforms to a minimum set of practices as agreed upon by the members of the community of trust.

The following diagram illustrates the structure and relationships between certification authorities and subscribers operating in a cross-certified (shared trust) model.



In a hybrid model, both a hierarchical structure and cross-certification are employed. For example, two existing hierarchical communities of trust may want to cross-certify each other, such that members of each community can rely upon the certificates issued by the other to conduct e-commerce.

E Glossary

(source: 'Advances and Remaining Challenges to Adoption of PKI Technology', US General Accounting Office, February 2001)

Authentication Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or means of verifying an individual's authorization to receive specific categories of information.

Certificate A certificate is a digital representation of information that at least (1) identifies the certification authority issuing it, (2) names or identifies the person, process, or equipment that is the user of the certificate, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A certificate is the means by which a user is linked—"bound"—to a public key.

Certification Authority (CA) A CA is an authority trusted by one or more users to issue and manage X.509 public key certificates and certificate revocation lists.

Certification Path Certification path is a method used by PKIs for recognizing and trusting digital certificates issued by other PKIs in order to create larger, connected networks of trust. Three conceptual models for creating certification paths include (1) trust lists, (2) hierarchical model, and (3) mesh architecture.

Certificate Policy Certificate policy is a specialized form of administrative policy that addresses all aspects of the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. By controlling critical elements of a certificate's data structure, a certificate policy and its associated enforcement technology can support provision of the security assurances required by particular applications.

Certification Practice Statement A certification practice statement is a statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in the certificate policy or requirements specified in a contract for services).

Certificate Revocation List A certificate revocation list is a list maintained by a CA of the certificates it has issued that have been revoked prior to their stated expiration date.

Compromise Compromise is the disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality Confidentiality is the assurance that information is not disclosed to unauthorized entities or processes.

Cross-Certificate A cross-certificate is a certificate used to establish a trust relationship between two certification authorities.

Data Integrity Data integrity is the assurance that data are unchanged from creation to reception.

Digital Signature Digital signature is the result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate and (2) whether the message has been altered since the transformation was made.

Encryption Certificate An encryption certificate is a certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

Public Key Infrastructure Policy Authority This authority is a body responsible for administering and enforcing policies regarding how agency PKIs will interoperate.

Hierarchical Certification Path Model The hierarchical model is a conceptual model for creating a certification path that is based on the designation of a single “root” certification authority trusted by all users. The root certification authority issues certificates to subordinate certification authorities that may in turn issue certificates to lower-level certification authorities.

Integrity Integrity is the assurance that data are protected against unauthorized modification or destruction of information.

Interoperability Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Key Pair A key pair includes two mathematically related keys that have the following properties: (1) one key can be used to encrypt a message that can only be decrypted using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.

Mesh Certification Path Model The mesh model is a conceptual model for creating a certification path that establishes links among peer certification authorities.

Nonrepudiation Nonrepudiation is the assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical nonrepudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that

signature had to have been made by the corresponding private signature key. Legal nonrepudiation refers to how well possession or control of the private signature key can be established.

Peer CA Peer CA is a CA in a mesh certification path that has a self-signed certificate that is distributed to its certificate-holders and that is used by them to start certification paths. Peer CAs are not subordinated to other certification authorities; instead, they cross-certify one another.

Privacy Privacy defines restricting access to subscriber or relying party information in accordance with the relevant law.

Private Key The private key is (1) the key of a signature key pair used to create a digital signature, or (2) the key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key The public key is (1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.

Public Key Infrastructure (PKI) PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

Registration Authority Registration Authority belongs to an entity responsible for identification and authentication of certificate subjects, but not for signing or issuing certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).

Relying Party The relying party is a person or agency receiving information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and in a position to rely on them.

Revoke a Certificate To revoke a certificate means to prematurely end the operational period of a certificate effective at a specific date and time.

Risk Risk is the expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Root CA In a hierarchical PKI, the root CA is the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Server A server is a system entity that provides a service in response to requests from clients.

Signature Certificate A signature certificate contains a public key intended for verifying digital signatures rather than for encrypting data or performing any other cryptographic functions.

Subordinate CA In a hierarchical PKI, the subordinate CA is a CA whose certificate signature key is certified by another CA and whose activities are constrained by that other CA.

Threat A threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Trust List A trust list is a conceptual model for creating a certification path that is based on a standardized collection of trusted certificates used by relying parties to authenticate other certificates.

X.509 X.509 is the most widely used standard for defining the format for digital certificates.