Information
and Privacy
Commissioner/
Ontario

Concerns and Recommendations Regarding Government Public Key Infrastructures for Citizens

Ann Cavoukian, Ph.D.
Commissioner

December 2002

The Information and Privacy Commissioner/Ontario gratefully acknowledges the significant contribution of Ross Fraser in analyzing the privacy concerns regarding Public Key Infrastructure for citizens and in developing the background and recommendations contained in this report.

This publication is also available on the IPC website.

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Introduction

In an effort to provide better service to citizens, governments in many jurisdictions are considering moving some of their programs, services and information onto computer networks to allow for around-the-clock access as well as to reduce costs through the elimination of manual data processing procedures.

This approach requires some means of securing access to applications over public networks to ensure the security and privacy of two-way communications between any two interacting parties. Public Key Infrastructure (PKI) is one method of implementing security over unsecured networks. This paper examines the potential impact of PKI on the protection of personal privacy and makes several recommendations for officials establishing such systems.[1]

Background

The Office of the Information and Privacy Commissioner/Ontario

The Office of the Information and Privacy Commissioner/Ontario (IPC) was established in 1988, with a mandate to provide an independent review of government decisions and practices concerning access and privacy under the *Freedom of Information and Protection of Privacy Act*[2] and the *Municipal Freedom of Information and Privacy Act*.[3] Specifically, the IPC's mandate is to resolve appeals regarding access to information requests, investigate privacy complaints, ensure compliance with the *Acts*, research access and privacy issues and to educate the public about these laws.

According to the *Acts*, the Commissioner may:

(a) offer comment on the privacy protection implications of proposed legislative schemes or government programs;

(b) after hearing the head [*of the program or Ministry*], order an institution to:

(i) cease collection practices; and

(ii) destroy collections of personal information that contravene the *Act*.

Privacy Defined

Before outlining the IPC privacy concerns regarding PKI, it is important to distinguish between privacy and security, as the two terms are often used interchangeably. A security breach may compromise personal information and in so doing, create a privacy breach. Security is therefore seen as a prerequisite for privacy. Security does not *equal* privacy, however, as it does not represent the broader spectrum of concerns subsumed under the term "privacy."

Security centres on the following issues:

- authentication (ensuring people are who they say they are);
- data integrity (ensuring that data is accurate and up to date);
- confidentiality (ensuring that only authorized personnel have access to data under the conditions that they are authorized to use or view the data); and
- digital signature (ensuring that transactions can be verified and audited as to who conducted a transaction).

Security also tends to be organization-centric, in that it authorizes levels of access by specified persons to specific systems owned by an organization and then tracks the actions of these individuals to ensure that they do not harm or misuse the hardware, software and information assets of that organization.

Privacy can best be described as the ability to control the collection, use and disclosure of one's personal information. This includes unique names and identifiers such as those that may be used in a PKI implementation.

Privacy is also person-centric, placing control of the collection, use and disclosure of personal information in the hands of the individual. A privacy-protective PKI gives the security and information protection decisions to the individual certificate holder. It obtains the user's prior informed consent, and it operates within an appropriate legal/policy framework. It also utilises careful systems engineering. In so doing, it fosters citizen trust and encourages use of the system.

In addition, and of particular interest to government, privacy involves the state's responsibility for protecting and safeguarding personal information that the government has collected, often by force of law. The government acts as an information steward in this regard, and must therefore exercise a duty of care over the personal information under its custody and control.

Privacy and PKI

A PKI provides the technology for managing encryption certificates and digital signature certificates and their associated private keys. This provides a level of assurance regarding the authenticity and integrity of online transactions to the parties involved at either end of those transactions. The digital signature provides the communicating parties with a level of assurance that both sides are who they say they are (authentication) and that neither side is able to say that a specific communication did not take place (non-repudiation) or that the information sent has been changed in any manner after the fact (data integrity).

The organization issuing digital certificates is known as a *Certification Authority* (CA) and is an integral part of the PKI itself. The role of the CA is to issue and manage the digital certificates and the public keys they contain. Identification of the certificate holder is done prior to certificate issuance. A *Registration Authority* (RA) or *Local Registration Authority* (LRA) is usually responsible for vetting certificate holders, approving their applications for certificates, furnishing each with a *relative distinguished name* to give each a unique name that cannot be confused with any other certificate holder, and then transmitting this information to the CA so that the digital certificate can be generated.

A publicly available *directory*, much like a telephone directory in function, stores each digital encryption certificate so that other users can find a particular individual or organization and communicate securely with them. This directory does not have to be managed by either the CA or the RA/LRA but still forms a part of the PKI when used to support encryption services such as secure e-mail.

In the context of delivering government services to citizens, PKI must therefore be able to:

- maintain the confidentiality of information transmitted;
- maintain the integrity of information transmitted;
- confirm, in a reliable and trusted manner, the identification of the sender (citizen or government);
- ensure, in a reliable and trusted manner, that only the intended recipient (citizen or government) can obtain the information transmitted; and
- provide assurance, via digital signatures, that the signatory is who they appear to be and that neither the signature nor the information it was applied to has been tampered with.

PKI does this by managing one or more digital certificates for each user who needs to receive encrypted messages or who needs a digital signature. In the context of PKI, certification is the act of binding an identity to a public key.[4] Certificates are intended to be the electronic representation of a particular individual or organization. To accomplish this, digital certificates must be unique and tied only to the individual or organization they are intended to represent. Certain PKI systems do this by assigning unique identifiers and a single key pair to each certificate holder. In doing so, they may cause one or more of the following privacy concerns to be raised:

1. They may include within the digital certificate information that the certificate holder may not wish to be included for display in a publicly accessible directory (**public disclosure**);

2. They may facilitate (perhaps unintentionally) the creation of electronic records that are traceable back to the certificate holder (**data trail**);

3. They may create a unique personal identifier or digital signature shared across multiple programs or databases that can be used to profile the certificate holder through his/her activities (**data matching**); and

4. They may lay the foundation for systems to develop that allow (2) and (3) to be accomplished over time (**function creep**).

Privacy concerns such as data trail, data matching and function creep are not unique to implementations of PKI – indeed, the deployment of any authentication technology will potentially cause these concerns to be raised. The recommendations that follow are intended to address these concerns in the context of PKI for citizens, not because implementations of PKI are more likely to give rise to privacy concerns than other authentication technologies, but because PKI is a readily available technology that is actually deployed by governments in several jurisdictions around the world to provide online services to citizens. The privacy impact of PKI is therefore of more than merely theoretical interest.

In addition, there are also some technical decisions to be made during implementation that are unique to PKI technology and that can also create concerns about privacy:

- Some implementations of PKI may remove or restrict the ability of certificate holders to retain possession or control over their private keys (private key protection, recovery and escrow); and
- Some implementations of PKI may compromise digital signature functionality and encryption functionality by issuing a single key pair that must then be used to perform both functions.

Finally, policy decisions made about how certificate holders are registered to receive digital certificates can also create privacy concerns:

- Some implementations do not allow a certificate holder to adopt a pseudonym: i.e., they prohibit the citizen from remaining anonymous or pseudonymous when communicating or transacting business online.

The privacy protection of any PKI in a large-scale rollout to citizens is still untested. Whatever system is chosen and developed for Ontarians must ensure the privacy of individual certificate holders. This is the starting point for the Information and Privacy Commissioner of Ontario and the basis for the recommendations that follow.

Recommendations

Fair Information Practices

Any design for a system of secure communication and authentication in a PKI model should be based on Fair Information Practices.[5] These principles were codified in the Organisation for Economic Co-operation and Development's *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*. In Canada, the guidelines are articulated in the Canadian Standards Association's *Model Code for the Protection of Personal Privacy* and have formed the basis of the federal government's *Personal Information Protection and Electronic Documents Act*. In Ontario, the government has used the guidelines to develop their *Privacy Design Principles* as part of their *Enterprise Information and Information Management Architecture* and their *Privacy Impact Assessment Methodology*.

The Fair Information Practices can be stated as five key questions that need to be addressed by any organization collecting personal information. They are:

1. Why are you asking?

Specify the purpose for collecting personal data up-front, and then limit the collection of personal information to the stated purpose(s). In the context of PKI, this applies to the data collected for the purpose of registering certificate holders.

2. How will the information be used?

By stating the use of the information, a use limitation is introduced. That is, the information can only be used as specified, or for a consistent purpose, except with the consent of the data subject. In the context of PKI, this applies specifically to data collected during registration and certificate issuance. It also applies to any personal identifiers or other information contained in the certificates.

3. Who will be able to see the information?

This addresses the issue of restricting access to personal information within the collecting organization and spelling out what access, if any, third parties may have. In the context of PKI, this may impact the design of registration processes and the rules regarding who has access to directories containing certificates.

4. Will there be any secondary uses?

This addresses the need to provide prior notice and allow for consent, if any secondary use is contemplated for information collected. Thus, an organization may not undertake data matching of information that was collected for a different purpose. Individuals would need to be notified and would need to provide their consent before any data matching could occur. Failure to inform would constitute unauthorized use. In the context of PKI, registration information collected while issuing digital certificates to a group for some specific purpose (e.g., encrypting the electronic transmission of billing data containing provincial health insurance claims) might in theory be used for an entirely different secondary purpose (e.g., obtaining a comprehensive listing of physicians and their practice addresses). Such a secondary use would require that consent be obtained from each certificate holder.

5. Who controls the data?

In the PKI context, controlling data addresses the need for individuals to have access to, and be able to view, correct and/or update their personal information held by CAs, RAs and LRAs. This also includes program areas that hold information about an individual that can be linked (via a *relative distinguished name*) to the individual's digital certificates for the purposes of user authentication or program entitlements.

Fair Information Practices would affect the deployment of PKI in a number of ways:

1. Program areas would have to ensure that the information they hold is secured from unauthorized access, use or disclosure to protect against the misuse of data trails. Any record of transactions stored for audit or records management purposes also containing personal information or the *relative distinguished names* contained in digital certificates, would need to be secured from unauthorized access and be securely disposed of, when no longer needed.

2. All program areas must ensure that information that uniquely identifies a user is not publicly visible – to protect against data matching, data inference, profiling and function creep. This includes some digital certificate information because they uniquely identify the user and can be viewed by any person or organization that looks up the digital certificate. The user would have to be made aware of this and give informed consent before any digital certificates are issued or placed in a publicly accessible directory for viewing.

3. All program areas that deal with users must ensure that there is no way to link to either different digital certificates or role and/or attribute certificates linked to the primary digital certificate of a uniquely identifiable individual. This is a protection against data matching and function creep. The CA that issues the primary digital certificate should not do so in a way that facilitates linking a uniquely identifiable individual's certificate to certificates used by that individual in different program areas. Again, this is to protect against data matching, data inference and function creep.

4. Any citizen's interactions with PKI must not be achieved by coercion, i.e., "no consent, no service." This especially applies when a user provides personal data for enrolment into a

PKI system.[6] Certificate holders must have the right to access, review and correct personal information used by the CA, RA, LRAs, and any program areas to create a digital certificate. As well, the certificate holder must have the right to request that changes to any personal information forming part of the certificate be accurately reflected.

Recommendation #1

That a privacy impact assessment (PIA) based on the Fair Information Practices be undertaken on any Government of Ontario PKI initiative and that subsequent privacy impact assessments be undertaken for any design changes involving the collection, storage, routing and aggregation of information on individual certificate holders. The PIA should address the policy and governance issues as well as the physical infrastructure necessary to construct, deploy, govern and operate any such initiative.

Legislative Requirements for a Privacy-Protective PKI-Based Communication and Authentication System

A legislative base, whether through legislative amendment or enabling legislation, needs to oversee any CA used to issue digital certificates to citizens, and to manage their renewal or revocation. Specific assurances as to security and data handling measures to enforce compliance with privacy provisions would need to be included. The structure, roles, responsibilities and restrictions applicable to CAs, RAs and LRAs should be established in legislation rather than regulations, so as to fix overall limits to the permissible actions a CA, RA, or LRA may take and to expose future changes to public scrutiny and debate.[7]

Any provincial system for privacy-protective communication and authentication must, at a minimum, fully comply with the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), or relevant existing privacy legislation within a specific jurisdiction. It is recommended that specific legislation be introduced to define and control the use of such a system and associated infrastructure, including the data generated and stored as a result of implementing the technology. In particular, the legislation should restrict private sector use of the identifying information. It is also necessary to ensure that *function creep* does not occur, and that there are appropriate audit, enforcement and deterrent provisions in any oversight legislation. All protections should be defined in the legislation, not in associated regulations. There should be legislative assurances that the government cannot contract out of its obligations or out of the data protection provisions of the *FIPPA* or other relevant existing privacy legislation for that jurisdiction.

Restrictions should also be considered on third party use of the digital certificates and any registration information collected or used to obtain them without the express consent of the certificate holder. For example, a policy limiting the collection and use of the Distinguished Name, similar to Canada's federal Treasury Board Secretariat *Privacy and Data Protection Policy 3-04 Use of the Social Insurance Number*, would prevent unauthorized parties from requesting, collecting or using a certificate holder's Distinguished Name. This is in order to prevent the use of personal information for purposes other than the intended purpose, i.e., registration for a digital certificate to access government programs or services. Any other purpose would constitute unauthorized secondary use of information under the Fair Information Practices.

Recommendation #2

That a legislative base, whether through legislative amendment or enabling legislation, be developed prior to the implementation of an initiative to design, develop and deploy a PKI that issues digital certificates to Ontario citizens; including, in particular, the Certification Authority, Registration Authorities and Local Registration Authorities. This legislation should:

1. Define the purposes and parameters of the uses to which the system will be put;

2. Place restrictions on the private sector use of any information in digital certificates issued for government program participation, including any informational content created through the use of the digital certificate; and

3. Place restrictions on the collection and subsequent use of any documentary evidence required to obtain a digital certificate.

These protections should be defined in legislation rather than in associated regulations.

Policy Requirements for a Privacy-protective PKI

Collection, Use and Disclosure of Personal Information by RAs and LRAs

Depending upon the uses that will be made of a digital certificate, a trusted registration process[8] may be necessary to indisputably authenticate the identity of a person prior to granting them a digital certificate. This is especially the case when issuing digital signature certificates. The system of RAs and LRAs is therefore often a crucial component of a privacy-protective PKI since the LRAs can potentially handle a great deal of personal information in the course of authenticating the identity of each applicant.

Any non-government entity designated as an RA should be subject to the same restrictions and laws as government RAs. All of the Fair Information Practices should apply to the process of verifying the identity of the individual applying for a digital certificate. Careful thought should be given to the type of personal information collected for the purposes of verifying identity. Otherwise, this could lead to intrusive demands for documentation, particularly from third party document repositories like credit bureaus. This type of third party data often contains errors, which may result in the denial of registration. In this case, the applicant may have no recourse since the data is not owned by the government and is therefore unavailable for updating or correction on demand.

When the identity of an applicant must be verified prior to issuing a digital certificate,[9] a method of verification should be used similar to the model currently used for passport applications. Under this model, an individual applying for a digital certificate would furnish tombstone data (e.g., name, birth date, address) supported by original or notarized documents together with a document attesting to the accuracy of the data and, most importantly, the identity of the applicant from a professional class or character of person with the ability to provide such attestation (e.g., a notary, doctor or lawyer). The documents would be returned to the applicant once the digital certificate is approved. This measure would prevent the aggregation of personal data once the initial purpose for furnishing it was concluded.

An equally important consideration is the prevention or prosecution of identity fraud. Suppose someone prepares forged documents purporting to identify the document holder as Bob Smith of Maple Avenue, Toronto, and then uses this bogus ID to register for a digital certificate. Suppose this digital certificate is then used to sign electronic documents that defraud or defame Mr. Smith. If police and the courts have no recourse to the original identity documents used during registration, they may be unable to effectively establish that identity fraud has taken place. Worse, Mr. Smith will be hard-pressed to deny that he ever registered for the digital certificate and that he consequently never signed the electronic documents in question. This can have serious ramifications for the reliability of digital signatures. Some means must therefore be established whereby claims of identity fraud can be investigated. It has been argued above that copies of identification documents used during registration should *not* retained by the CA, RA, or LRA. An appropriate solution is to retain the unique document numbers of identity documents, so that these can be traced and investigated should a subsequent allegation of identity fraud be made. The identity documents themselves (and the personal information they contain) need not retained. Indeed, this is how some GO-PKI registrations currently function.[10]

Recommendation #3

Identity documents (or copies supported by notarized attestations of accuracy) and personal attestations by individuals authorized under law to do so should form the basis for the approvals process to procure a digital signature certificate or digital encryption certificate that will be used in such a way that the identity of the certificate holder is assured.

Identity documents, or copies thereof, should be returned to the applicant once the certificate approval has been granted. No copies of these documents should be kept by the Registration Authority or Local Registration Authority.

Unique document numbers from identity documents should be retained by the Registration Authority or Local Registration Authority for the sole purpose of preventing or investigating possible identity fraud.

Separation of Registration Processes

Only enough information should be collected about an individual to uniquely identify them for the express purpose of issuing a digital certificate. Information required by program areas for services or individual entitlements should be submitted directly to the participating program areas rather than to the CA or to the RA/LRA performing the registration for certificate issuance. This conforms to the limited collection and use principle.

Recommendation #4

Any PKI that issues digital certificates to citizens should collect digital certificate registration information in such a way that it remains separate from program registration information.

Control Over Private Decryption Keys and Private Digital Signature Keys

A privacy-protective PKI design should be person-centric. This means placing the private digital signature key(s) entirely within the control of the certificate holder. Complete control of a signature key by the certificate holder is a necessity if the digital signature is to have the property of non-repudiation.[11] This should be considered a minimum requirement for any privacy-supportive PKI design.

A distinction must be drawn between certificate holders who are issued encryption certificates by their employers in the course of their work, and certificates issued to citizens for the purpose of secure communication with government. It is reasonable that encryption certificates issued to employees be backed up by their employer (or by a CA on behalf of their employer), so that data encrypted with these certificates – data which are rightfully in the possession of the employer – remain available even after the death or dismissal of the employee who held the private decryption key. The same argument does *not* apply to encryption certificates issued to private citizens. Any party encrypting a message with an encryption certificate held by a private citizen must surely intend that message to be accessible by that citizen only (otherwise, the message would presumably not have been encrypted in this fashion). The technical issues surrounding private key generation, protection, and backup are discussed further in *Generation of Private Keys and Their Subsequent Protection*.

Recommendation #5

Any PKI that issues digital certificates to citizens must allow certificate holders to retain control over their own private digital signature keys.

Linkages and Data Matching

Government program areas using a PKI should not be able to link information about a specific certificate holder to information about that certificate holder held in other program areas. This applies whether different digital certificates are used by each program area or whether a single digital certificate and subsidiary role and/or attribute certificates are used.

Links between a digital identity certificate and program-specific role or attribute certificates are especially problematic. Steps must be taken to ensure that such linkages cannot be used to facilitate data mining or data matching of records held in the databases of unrelated programs.

Any system should be designed to prevent users, institutional or otherwise, from:

1. matching data about specific users across different program areas;

2. profiling users by tracking their data trails;

3. inferring personal information about certificate holders by linking unrelated bits of certificate or digital signature data gathered from transaction records or audit trails; and

4. linking occurrences of specific public keys together to act as unique identifiers or pointers to data about specific users in other databases (for example, by linking together records or fields of data that are signed by the same digital signature).[12]

Recommendation #6

That a Threat/Risk Assessment be performed on any PKI that issues digital certificates to citizens to ensure that it mitigates risks to the security certificate holder information posed by data matching. As such, matching could be facilitated by the use of public keys and certificates as linkages among disparate program databases.

Control Over Personal Information

In the view of the IPC, a privacy-protective PKI system would allow certificate holders control over how much personal information they disclose in a PKI environment. Just enough personal information should be collected to uniquely register for a digital certificate. As noted in *Separation of Registration Processes*, personal information required for program or service specific entitlements should be collected by the program areas directly rather than by the CA, RA, or LRA.

In addition, the system should also allow certificate holders to view, verify and, where necessary, have their personal information corrected. It should also adhere to Fair Information Practices in the handling, processing, auditing storage and disposal of certificate holders' uniquely identifiable personal information.

Recommendation #7

Any PKI that issues digital certificates to citizens should be privacy-protective in adhering to *Fair Information Practices* in the collection, use, handling, processing, auditing, disclosing, storage and disposal of uniquely identifiable personal information pertaining to certificate holders – in particular, by allowing certificate holders to view, verify and, where necessary, have their personal information corrected.

PKI Governance and Administration

The *X.509 certificate standard* defines a PKI as "the set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke public key certificates based on public key cryptography."[13] An essential part of any PKI therefore is the development and management of policies to ensure the proper deployment of the hardware, software, people and procedures that make up the PKI.

Governance refers to the framework of policy, operational and oversight directives within which all elements of a PKI would function. It is essential that any Policy Management Authority (PMA) responsible for setting PKI policy for the issuance of digital certificates to citizens be constituted and governed by legislation setting out the duties and limits of its activities. This is particularly important in view of the current local understanding of PKI governance "given that technology, policies and business rules must remain intrinsically flexible, responsive and constantly aligned with evolving technology. It must also address the broad objectives of inter-operability with other jurisdictions across Canada, and with the federal government model."[14] Policy and operational changes made without oversight and without a Privacy Impact Assessment could have deleterious consequences to personal privacy.

Within this context, IPC would be in favour of an oversight body with the ability to conduct audits, and an operational authority and PMA that are legislatively independent of the government of the day. The independent audit capability should include the capacity to conduct Privacy Impact Assessments (PIA) for any changes to policies that affect the collection, transmission, handling and use of personal information. The PIA should also be able to compel alterations in the operation of any aspect of the PKI infrastructure or operations that compromise the security and privacy of certificate holders' private keys, digital certificates, data collected during certificate registration.

Recommendation #8

That oversight be established by an independent body, with the ability to conduct audits and order changes to the operations of the PKI, where these operations affect the privacy of personal information held within the PKI. The primary focus of operations and audit should be to ensure that no changes to policies and/or operating procedures are made which could adversely affect the privacy of personal information held within the PKI.

Technical Requirements for a Privacy-protective PKI

Generation of Private Keys and Their Subsequent Protection

GO-PKI currently uses separate key pairs for encryption and for digital signature. This is a sound practice for many reasons; not least of which is that privacy issues relating to key backup and key recovery are very different for private decryption keys than they are for private signature keys. The discussion below presupposes that the key pair for encryption is distinct from the key pair for digital signature.

Recommendation #9

Separate key pairs must be generated for encryption and for digital signature.

Use of each private signature key must at all times be secured so that it can only be used by the certificate holder, otherwise a digital signature on a message can only be tied back to the signing key, not to the certificate holder (who, in the absence of strict control over the signing key, may or may not have been the one who used it to sign the message). Moreover, to ensure that the private key was never outside the possession of the certificate holder, it would need to be generated by a hardware or software process under the control of the certificate holder, rather than generated by a CA and subsequently delivered to the certificate holder.

Another problem inherent in any PKI implementation is the question of what to do if the private key(s) are lost. A distinction must be drawn between a private decryption key (that allows the recipient of an encrypted message to decode the message) and a private digital signature key (that allows the sender of a message to sign it). Loss of a private digital signature key does not necessarily pose a problem, as the certificate holder merely needs to be issued a new digital certificate. This may be costly and inconvenient, but it in no way invalidates previously applied signatures, as notices of certificate revocation always contain the date and time that the certificate was deemed to be revoked. Nor does replacing lost signature keys by issuing new certificates have significant implications for privacy protection.

Recommendation #10

The certificate holder should generate the private signature key(s) at a secure access point in the PKI infrastructure and securely retain sole control of the key(s) thereafter. Any signature key backups should be secured and accessible only by the certificate holder.

Lost signature keys should be replaced with new ones (with revocation of the certificate matching the lost key), rather than having any type of signature key recovery mechanism in place.

Use of each private decryption key must also be under the control of the certificate holder, but the issue is made complex by the necessity of backing up the decryption key.

Unlike a lost signature key, a lost decryption key cannot be replaced merely by applying for a new encryption certificate. Information encrypted with a lost encryption key becomes permanently undecipherable unless the lost key can be restored from a backup. While some users are content to manage the secure backup and recovery of their own decryption keys, others may wish this to be done on their behalf by a trusted third party and CAs sometimes fulfil this role. It is essential however, that such backup be done only upon the request of – and therefore with the informed consent of – the certificate holder.

As mentioned in *Control Over Private Decryption Keys and Private Digital Signature Keys*, a distinction must also be drawn between certificate holders who are issued encryption certificates by their employers in the course of their work, and certificates issued to citizens and others outside the Ontario Public Service. In the context of GO-PKI, it is reasonable that encryption certificates issued to civil servants be backed up by a GO-PKI CA, so that data encrypted with these certificates – data which are rightfully in the possession of the government – remain available even after the death or dismissal of the civil servant who held the private decryption key. The same argument does *not* apply to encryption certificates issued to private citizens. As indicated earlier, any party encrypting a message with an encryption certificate held by a private citizen must surely intend that message to only be accessible by that citizen (otherwise, the message would presumably not have been encrypted in this fashion).

Any form of decryption key recovery degrades the protections available from encryption. The IPC could not support a key recovery system unless the certificate holder's informed and express consent were an integral part of the key recovery process.

Recommendation #11

Certificate holders must be informed of the existence of any decryption key backup or recovery mechanisms that could be used to back up or recover their private decryption key.

Governments issuing encryption certificates to private citizens must only employ private decryption key backup or recovery mechanisms with the informed consent of the certificate holder at the time of certificate issuance; and the certificate holder must be able to withhold such consent without forfeiting the issuance of the certificate.

Key Escrow

Key escrow refers to the ability of government or other organizations to open messages encrypted with private encryption keys by requiring that a copy of every encryption key be producible on demand. Key escrow is, in effect, a form of private decryption key backup or key recovery that is imposed upon all certificate holders, whether they consent to it or not.[15] Key escrow systems are inherently less secure, more costly, and more difficult to use than similar systems without an escrow feature. The deployment of escrow-based infrastructures would require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building a transparently secure infrastructure of the scale and complexity that would be required to implement a scheme of escrow involving trusted third parties, is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs.[16] Because this compromises the very security that PKI is supposed to provide, the IPC is opposed to any form of key escrow.

Recommendation #12

There should not be any type of private key escrow built into a PKI used to issue certificates to private citizens.

Directories

To be useful for services such as secure e-mail, encryption certificates must be accessible by those who wish to send secure encrypted communications to the certificate holders. Such access is typically realized by placing the encryption certificates in a directory accessible to those who wish to encrypt communications intended for the certificate holders. These directories are widely accessible (for example, via the Internet). Great care must be taken to ensure that the design of such directories does not compromise the privacy of the certificate holders. For example, care must be taken in the design of directory attributes that record additional information about the certificate holder. Care must also be exercised in determining the rules of access to such directories. Most importantly, the technical necessity for such directories of encryption certificates must not be used as an excuse to gather information on certificate holders into a single repository, or to facilitate data mining by linking information in other directories to the encryption certificate directory.

Recommendation #13

That a Privacy Impact Assessment be made of all directories used to contain encryption certificates issued to citizens; with particular emphasis on the informational attributes contained in the directory, and the directory's rules of access.

Centralized Key Stores

From a privacy standpoint the most secure method of storing a private key is to ensure it remains in the possession of the certificate holder. This can be accomplished with a hardware token containing the private key. Other solutions include storing keys on a secure server allowing online access to certificate holders (e.g., via the Internet). This solution to the problem of private key portability raises privacy concerns since the private keys are not technically in the possession of the certificate holder. Adequate internal controls must be designed into the infrastructure itself to ensure that only certificate holders have access to their private keys. In particular, a Threat and Risk Assessment must be made to ensure that such centralized key servers cannot become the targets of attacks to steal the information for identity theft purposes. For this reason, the IPC recommends that considerable care be taken in implementing such key portability schemes.

Recommendation #14

That a thorough Threat and Risk Assessment be done on any scheme involving centralized private key storage or online accessibility to private keys to ensure that the privacy and digital identities of certificate holders are not compromised.

Conclusion

As mentioned at the outset of this review, governments in many jurisdictions are considering electronic service delivery for some of their existing programs, services and information. This would enable better service to citizens by providing around-the-clock access. It would also serve to reduce costs through the elimination of manual data processing procedures. PKI has been identified as a technology that could create the trust necessary to do this by certifying Internet-based transactions with legally binding electronic signatures and by protecting the confidentiality and integrity of information during transmission.

Some citizen interactions with government do not appear to require the unambiguous authentication that PKI can offer. For instance, transactions in which a citizen pays for a government service typically require no more than a payment of money and some cursory tombstone information in exchange for goods or a licence – hence confidentiality is required, but not necessarily authentication. Simpler security methods than PKI (such as Secure Socket Layer) may be sufficient for these types of Internet transactions. These simpler methods would avoid the privacy concerns surrounding digital certificates that have been outlined in section 3. In fact, other jurisdictions are implementing electronic service delivery models that can fulfil basic levels of interaction without the need to employ PKI.

Higher value transactions in which Ontario residents seek entitlements that cost the government money, are typically conducted through intermediaries like physicians who bill for the service, rather than being conducted directly with the citizen. In these more limited cases a PKI in which the certificate holders are service providers may provide the security necessary to ensure that no fraud has been perpetrated on the public purse.

A full-scale rollout of digital certificates to private citizens requires great care and planning, lest such a system end up looking less like a convenient security tool for electronic service delivery and more like a comprehensive monitoring system intruding upon the privacy of Ontario citizens conducting online transactions with provincial or municipal governments. By encouraging implementers to follow the recommendations above, the IPC hopes to ensure that the putative benefits of implementing a PKI for citizens are not realized at the expense of their privacy.

Notes

1. The Government of Ontario Public Key Infrastructure (GO-PKI) is currently limited to the Ontario Public Service, the broader public service, and third party contractors delivering services on behalf of the Ontario Government. This paper addresses the broader privacy issues of providing digital certificates to citizens for the purposes of conducting online transactions with governments.

2. Government of Ontario. *Freedom of Information and Protection of Privacy Act*. R.S.O. 1990, c. F.31. Queen's Printer for Ontario, 1993, at: www.ipc.on.ca/provact-e.

3. Government of Ontario. *Municipal Freedom of Information and Protection of Privacy Act*. R.S.O. 1990, c. M.56. Queen's Printer for Ontario, 1993, at: www.ipc.on.ca/munact-e.

4. Adams, C. and S. Lloyd. *Understanding Public Key Infrastructure*. Macmillan: Indianapolis, 1999, p. 88.

5. U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973). *The Code of Fair Information Practices*, at: www.epic.org/privacy/consumer/code_fair_info.html.

6. It is important to understand that citizens who do not consent to participate in a PKI may not be able to conduct some government transactions online. For example, if a citizen refuses to obtain a digital signature, some transactions requiring a signature must then be conducted with paper-based forms, rather than forms filled out online. Great care must be taken, however, to ensure that all online transactions can also be performed by offline means and that the advantages of online transactions are not leveraged to construct systems that erode privacy.

7. It is understood that technical requirements may be better placed in accompanying regulations rather than the legislation itself, as the process of amending regulations is better able to match the rapid pace of technological innovations. Overall limits need to be placed on the permissible actions of CAs, RAs, and LRAs in order to protect the rights of individuals; however, these limits should be expressed in legislation, rather than regulations.

8. A trusted registration process involves a citizen providing identifying documentation such as a birth certificate that is then verified with the issuing agency as valid and belonging to the citizen. Upon verification the citizen is registered in a program or service.

9. There are applications of PKI where no verification of identity need ever be made. For example, certain online counselling services require the initial (pseudonymous) identification of the patient to be counselled, but do not need to know the actual name and identity of the patient (billing arrangements are made separately). At each counselling session, the therapist must reliably know that: 1) they are communicating online with the same "Patient X" with whom they communicated the last time, and 2) the session is secured from third party eavesdropping. There are no further requirements for patient identification.

10. Special care must be exercised when retaining unique document numbers that are themselves valuable pieces of personal information. An example is found in the use of credit cards as identity documents: the unique document number is the credit card number, and this number may be used by itself to commit credit card fraud. Steps must be taken to prevent this: for example, by recording only certain digits of the credit card number. What is important are not the mechanics of a specific method, but rather that an appropriate analysis of threats and risks be made and that methods be chosen that mitigate those risks *without* sacrificing privacy.

11. Although the phrase "non-repudiation" is an ongoing source of controversy as a legal term (in part because Canadian courts have not yet dealt with cases involving disputes about the validity of digital signatures), it has a well-accepted meaning within the field of computer security. It is frequently used in security standards and best practices, such as those published by the International Standards Organisation (ISO) and the Internet Engineering Task Force (IETF). For a good discussion on non-repudiation, see *Draft IETF PKIX Roadmap* at: www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-09.txt.

12. A variety of cryptographic techniques are available to restrict or eliminate such unsecured linkages. For example, instead of using a common identifier to link a digital identity certificate with associated role or attribute certificates, a system could be designed so that the identity certificate is mounted in a hardware token in the possession of the certificate holder. This would enable program areas to confirm the identity of a user before allowing access to a separate role or attribute certificate created by the program area for the user, without maintaining a central directory of identity certificates. Other schemes might involve secure hashing algorithms to provide a one-way link between the role or attribute certificate containing a program specific identifier and a corresponding government issued identity certificate containing the name of the individual. This would minimize the problem of profiling a certificate holder's actions through the use of their public keys while keeping the program area identifiers unique. Such techniques can only be properly assessed when they are subjected to a rigorous Threat/Risk Assessment.

13. PKIX Working Group. *IETF PKIX Roadmap* (draft), July 2002, at www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-09.txt.

14. Government of Ontario. *Concept of Operations for the Government of Ontario Public Key Infrastructure*. Ontario: 2001. p. 6.

15. It is important to note that a certificate holder may wish to have his or her private decryption key backed up by a third party (such as the CA) as a sensible precaution against its loss or accidental destruction. Such voluntary key backup arrangements that are explicitly and consensually entered into by the certificate holder are in sharp contrast to key escrow, which by definition is mandatory, non-consensual, and uniformly imposed upon all certificate holders.

16. Abelson, H., *et al. The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*. *Ad hoc* Report, 1998, at: www.cdt.org/crypto/risks98.

References

Abelson, H. *et al. The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*. Ad hoc Report, 1998 at: www.cdt.org/crypto/risks98.

Adams, C. and S. Lloyd. *Understanding Public Key Infrastructure*. Macmillan: Indianapolis. 1999.

Brands, S.A. *Private Credentials.* Zero Knowledge Systems: Montreal, November 2000, at: www.zeroknowledge.com/media/default.asp.

Brands, S.A. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, 2000.

Buchinski, E. and S. Houlden. *Privacy Concerns with PKI Deployment*. Treasury Board Secretariat, Government of Canada: Ottawa. September 10, 1997.

Clarke, R. *Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society*, 2000 at: www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html.

Clarke, R. *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice.* Proceedings. User Identification and Privacy Protection Conference. Stockholm, June 14–15 1999, at: www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

Ellison, C. and B. Schneier. "Risks of PKI: Electronic Commerce." *Inside Risks 116*, Communications of the ACM, vol. 43, no. 2, February 2000, at: www.counterpane.com/insiderisks5.html.

Ellison, C. and B. Schneier. "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure." *Computer Security Journal*, vol. 16, no. 1, 2000, at: www.counterpane.com/pki-risks.html. pp.1–7

Government of Ontario. *Concept of Operations for the Government of Ontario Public Key Infrastructure*. Ontario, 2001.

Government of Ontario. *Freedom of Information and Protection of Privacy Act*. R.S.O. 1990, c. F.31. Queen's Printer for Ontario, 1993. at: www.ipc.on.ca/provact-e.

Government of Ontario. *Municipal Freedom of Information and Protection of Privacy Act*. R.S.O. 1990, c. M.56. Queen's Printer for Ontario, 1993, at: www.ipc.on.ca/munact-e.

Grossman, W. “Circles of Trust.” Scientific American, August 2000, at: www.sciam.com/article.cfm?articleID=000B6D6B-DFA5-1C73-9B81809EC588EF21&pageNumber=1&catID=2.

PKIX Working Group. *Draft IETF PKIX Roadmap*, July 2002, at: www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-09.txt.

U.S. Department of Health, Education and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973). *The Code of Fair Information Practices*, at: www.epic.org/privacy/consumer/code_fair_info.html.

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca