An Overview of Public Key Certificate Support for Canada's Government On-Line (GOL) Initiative

Mike Just
Treasury Board of Canada, Secretariat (TBS)[1]
Just.Mike@tbs-sct.gc.ca

Abstract: The Canadian Federal Government is delivering on-line services to its citizens. A critical feature for ensuring the acceptance of these services is to ensure that security and privacy requirements are met. To this end, Canadian citizens may obtain an epass allowing them to securely obtain services through a government program web site. Technically, an epass is composed of a pseudonymous public key certificate. In this paper, we analyze the system in which this epass is managed and used, with particular emphasis as to how it supports the security and privacy of Canadian citizens.

1 Introduction

Governments have an obligation to protect the concerns of their *citizens* (hereafter referred to as *individuals*), above and beyond what might typically be provided for a more focused or specialized user base. In recent years, privacy is often cited as a primary concern. In Canada, this concern prompted the development and passing of the Personal Information Protection and Electronic Documents Act (PIPEDA) [PIPE00].[2]

As the Canadian Federal Government continues to offer online services, it is of the utmost importance that security and privacy requirements are met so as to lessen any potential concerns, and ensure user uptake. Though one of many service delivery channels (others include by phone and in-person), on-line service delivery can offer much efficiency and thus cost savings, but these can only be realized if on-line services are used. Canada has stated that government departments will have a complete online presence by 2005. With a population of greater than 31 million, and more than 1000 programs and services, the Canadian project is by no means small. This is especially true considering the collaborative potential with provincial and municipal governments.

In the remainder of this paper, we focus on the PK-based solution for the authentication of individuals using an epass. Technically, the epass is composed of a pseudonymous public key verification certificate along with its corresponding private key. The main results of this paper are twofold:

- To describe Canada's epass system, supporting secure access to online government services;
- To discuss how this system satisfies privacy and security requirements of individuals.

[1] The Treasury Board of Canada, Secretariat (TBS - http://www.tbs-sct.gc.ca/) is a central government agency whose mission is to manage the Government of Canada's human, financial and information resources. Within TBS, the Chief Information Officer Branch (CIOB - http://www.cio-dpi.gc.ca/) is responsible for coordinating Information Technology (IT) and IT Security activities.

[2] Whereas the Privacy Act [Priv85] applies to federal government institutions, PIPEDA applies to organizations that collect information for commercial purposes. Currently, PIPEDA applies to federally regulated organizations, but as of January 2004, it will also apply to provinces and territories that have not enacted similar legislation.

The epass system has undergone legal, privacy impact, and threat and risk assessments (see Lazarus [Laza02] for further information). In this paper, we focus primarily on the technical (as opposed to physical, procedural, legal, etc.) security and privacy measures. Whereas security requirements are met using familiar techniques and controls, some novel techniques are used to enhance privacy. In particular,

- Individuals are enrolled and identified only to government programs with which they already have a relationship. No identifying information is shared with the central certificate issuer.
- A Meaningless But Unique Number (MBUN) is used as the Distinguished Name (DN) in an individual's public verification certificate. On its own, this certificate contains no identifying information. Within a government program, the MBUN is tied to a Program Identifier (PID) corresponding to the individual.
- Individuals have the flexibility to use more than one epass, allowing them to fine-tune their protection based on their level of privacy concern. A sufficiently private baseline solution is offered for individuals that use a single epass.

As this system and its deployment continue to evolve, this paper captures many features that are part of the current system, though also highlights several research considerations for future applications (which are worth considering as more and more programs offer secure online services). Throughout, features that are not part of the current GOL system are explicitly noted as such.

In Section 2, we describe the management of the epass, from registration to renewal, recovery and revocation. Section 3 examines the use of epass for the Address Change Online (ACO) application provided by the Canada Customs and Revenue Agency (CCRA). We discuss the privacy and security issues regarding the management and use of the epass in Section 4. In Section 5, we provide some concluding remarks.

2 System Design

There are numerous statutory and regulatory requirements upon which a governmental service delivery system must be built. For the purposes of this paper and its security analysis, these requirements can be safely abstracted as the traditional security requirements of confidentiality, integrity, and non-repudiation, as well as ensuring that individual privacy is met. Matched against security requirements is often a requirement for ensuring system usability. Indeed, a more usable system is often used in a more secure manner.

In this section, we describe the design of the PK-based epass[3] system supporting individual authentication. Though the resultant security solution is a combination of legal, policy and technical controls, for the purpose of this paper we focus primarily on technical safeguards and in particular the use and management of public key certificates issued to individuals.

We begin with a high-level system overview, where more detail is given in the subsections below. Individuals register and obtain a single[4], pseudonymous public key certificate (an epass), issued by a central Certification Authority (CA). The identifier within this certificate is a Meaningless But Unique Number (MBUN). The property of uniqueness ensures that no two

[3] The term epass is an abstraction used to identify a generic credential used by individuals to authenticate for government services. Though generally referring to the doubly-encrypted object containing private and public keys and obtained by an individual at login, the term is sometimes used to identify only the public key certificate portion of this object.

[4] At their discretion, an individual may obtain more than one epass.

individuals possess the same MBUN, while lack of meaning ensures that given only an MBUN, no information as to the corresponding individual identity can be gleaned.

Individuals must separately enrol to each government program (one-time at first use) for which they desire electronic government services. This enrolment requires that the individual properly identify him or herself to the program (e.g. based on program-specific shared secret information), thereafter allowing the program to associate an MBUN to the individual's Program Identifier (PID) within that program.[5] The program will continue to use the PID as an index for the user, rather than the MBUN, at least since the MBUN may change. More specifically, the MBUN will be managed by the epass Management System, whereas the government program manages the PID. Hence, the MBUN may change, independently from any actions by the government program. For example, an MBUN associated with a user may change as a result of re-registration after certificate expiry or certificate revocation. Also, an individual may choose to associate a different epass with a government program at any time (and hence, associate a different MBUN with the PID).

The resulting picture is one in which pseudonymous user credentials are securely stored centrally.[6] Within a program, a translation from the MBUN to the PID is maintained in the form of a translation table. Once enrolled, a user can thereafter authenticate with their epass (using public key authentication techniques), after which a translation to the appropriate PID identifies the individual within the context of the government program.

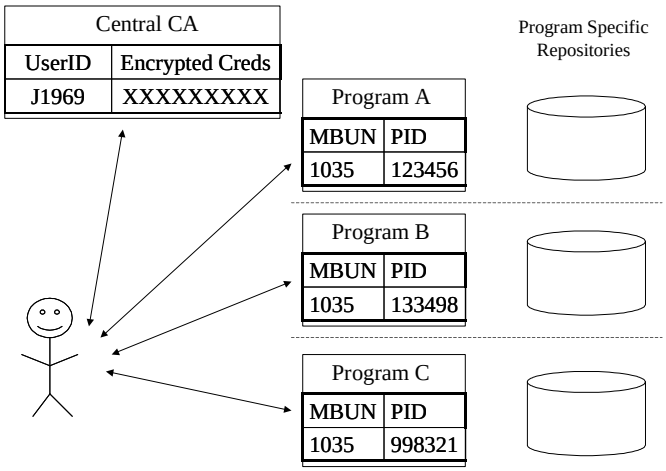

Figure 1: Distinction between MBUN and PID amongst system entities.

Recall that an individual may choose to have multiple credentials, in which case distinct Username and Encrypted Credentials would be maintained, and a separate MBUN may be used for access to each program.

The current system implementation relies on the individual having access to a web browser. A COTS product that implements a downloaded (FIPS 140-1 certified) Java applet provides the necessary additional functionality.

[5] The PID (sometimes called a legacy identifier) is chosen and managed by the government program, independent of the epass.

[6] As described below, the epass solution offers support for roaming users whereby an individual's private and public keys are stored, doubly encrypted in a central repository.

In the following subsections, the detail regarding the registration for an epass and program enrolment, in addition to the epass management, is discussed. The use of an epass for obtaining government services is discussed in Section 3.

2.1 Registration and Enrolment

Several variations are conceivable for the initial registration and enrolment of an individual for access to government services (see Section 2.1.1 for a brief description of some enrolment variations). Below, we expand on a common scenario, and in particular one that is currently offered by the Canada Customs and Revenue Agency (CCRA, formerly Revenue Canada)[7] in support of their Address Change Online (ACO) application.

Before continuing, we highlight an important terminology distinction. An individual will *register* with the central Certification Authority (CA) for an epass. The CA is not aware of any personal information regarding this user; hence the user is not required to identify for the purpose of obtaining an epass. However, when an individual *enrols* with a government program, they will identify themselves to that program. It is with a program that further services may be obtained. To facilitate use of the epass with the government program, at the time of enrolment the program will create an association between the MBUN (from the epass) to the Program ID (PID), where the latter is the index for the user within the realm or context of the program. To avoid unnecessary epass issuance, in the current system only individuals that have properly identified to a program will be redirected to the CA at the epass Management System (MS). And only once they have an epass can they complete program enrolment. Therefore, the process proceeds as three main steps:

1. Individual identification to a government program.
2. Individual registration for an epass.
3. Individual program enrolment (mapping the epass MBUN to the PID).

This process is described in more detail below.

An individual ultimately enrols in a government program by identifying him or herself to the program. This step assumes that the individual already has a relationship with the program, and in particular, has an assigned Program Identifier (PID) (see possible variations to this assumption in Section 2.1.1). As part of the identification process, the individual would typically provide information requested by the program. As a concrete example, individual enrolment within CCRA requires presentment of four pieces of information, namely

1. The individual's date-of-birth,
2. The dollar amount entered by the individual at line 150 of their 2000 or 2001 tax return,
3. A numeric identifier returned to the individual as part of their 2000 or 2001 tax assessment, and
4. The individual's social insurance number (SIN) (roughly equivalent to the US Social Security Number).

After identifying, if the individual doesn't currently have a public key certificate (or perhaps has a certificate but chooses to register for another for use with a program), the individual is transparently redirected to register for the epass. As part of registration, a random, unique MBUN is generated and placed in the certificate for the epass. The transfer to the CA for the purpose of certificate registration does not include transmission of any information that would identify the individual to the CA.

[7] http://www.ccra-adrc.gc.ca/

The steps in the process of program enrolment and certificate registration are depicted and described below.

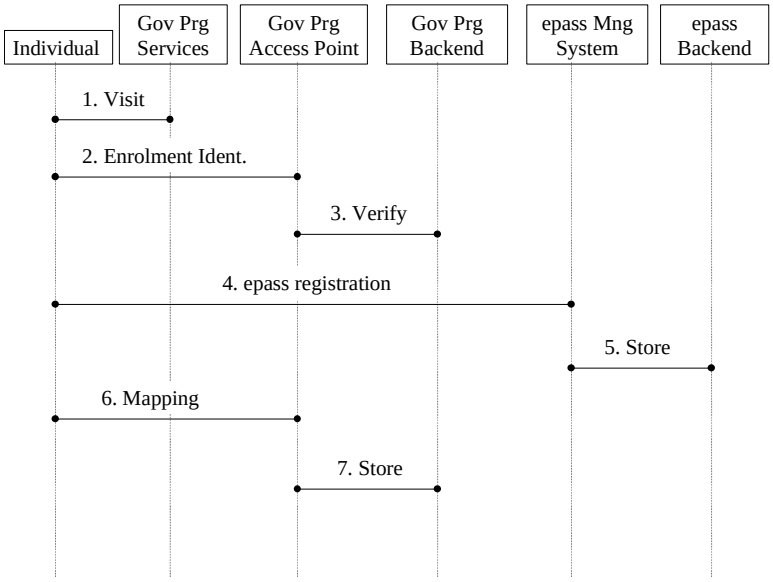

Figure 2: epass registration and government program enrolment

1. An individual visits a Federal Government program web site using their web-browsing client for the purpose of obtaining some secure services. The individual is redirected to the program Access Point (AP).
2. At the AP, there are several options, depending upon whether the user has previously registered for an epass or enrolled with the program:
    a. If the user already has an epass, they either
        i. Login (presuming the user has already enrolled with the program) and securely access program services (see Section 3), or
        ii. Enrol with the program.
    b. If the user does not have an epass, or wish to obtain a new pass for use with this program, they will proceed with enrolment.

    As part of enrolment, the registrant identifies himself or herself by answering questions posed by the program, derived from shared secret information shared between the individual and the program.
3. The registrant-provided answers are validated against the information stored in the program's legacy database.
4. If the registrant has successfully identified them self, a signed cookie is returned to their browser, and they are redirected to the epass Management System (MS) for registration (only if they wish to obtain an epass to use with this program, i.e. they don't yet have an epass, or have one but wish to use a new epass with this program). As part of this process
    a. The individual chooses a user ID and password;
    b. The individual selects recovery challenge questions and answers; and
    c. A private key is generated, with an MBUN similarly generated and assigned by the MS.
    d. The MS, given the public key and MBUN, then creates a public key certificate.
5. The individual's password-protected profile (containing their private and public keys) and recovery questions are further encrypted and stored in the MS repository. Note that no personal information is stored at this repository.

6. The information used to identify the individual as part of program enrolment is signed and encrypted. The MBUN, used as the certificate identifier for the user, is mapped by the program to the individual's Program ID (PID).
7. The program stores the signed registration information and MBUN-PID mapping.

The system supports a roaming client, as the individual's credentials may be stored in a management system repository. This so-called profile for the individual is doubly encrypted, including publicly encrypted for the management system and also encrypted using a key derived from the individual's password.

2.1.1 Variations

As suggested above, there are variations possible for the registration and enrolment process described above. In particular, the differing needs of each department will require that some flexibility exists, though from the point of view of usability, a consistent look-and-feel is maintained as much as possible for the individual. As more and more programs go online, some of these variations may be considered.

No shared secrets with program. There are situations in which direct, on-line program enrolment may not be possible, as the individual does not have a sufficient relationship with the program (e.g. may not have a PID):

1. Individuals that do not have a relationship with any program, e.g. newborn child;
2. Individuals that have a relationship with some programs, but not others, e.g. individuals that have a record of employment but no passport;
3. New citizens (e.g. landed immigrants); or
4. Programs that don't have sufficient shared information with which an individual may be identified as part of enrolment.

For these situations, there are a few options that could be considered to aid in secure enrolment (the second and third can be thought of as special cases of the first):

1. *Guarantor*. A trusted third-party (perhaps another individual, or a dedicated organization) can be used to attest as to the identity of an individual. In particular, the individual will identify to the guarantor (based possibly on some shared secret information, acceptable documentation, or based on some other form of relationship) whereby the guarantor will provide evidence attesting to some attribute for the user. A similar process is currently used for Canadian passport applications.
2. *Shared program enrolment services*. In cases where an individual is able to enrol within program A, but not program B (due to a lack of shared information with program B), the individual might choose to allow program B to request identification information from program A. Such a service would require that the individual's privacy be respected, e.g. that consent is obtained prior to the sharing of such information. The overall privacy implications for designing such a service would also have to be carefully considered.
3. *In-person registration*. Whereas an online registration relies on shared and trustworthy digital information, an in-person registration would allow a registrant to present physical identification (e.g. passport) in order to properly identify them. The cost-benefit of such a system would have to be carefully considered.

Multiple certificates. As mentioned earlier, the registration system is flexible so as to satisfy a wide spectrum of privacy requirements. In the case that an individual uses a single epass, the MBUN is not used as an index by government programs and programs cannot match data based on the MBUN (without the explicit approval of the individual) [Priv85, Priv93]. Alternatively, an

individual may obtain any number of certificates, e.g. a different epass is used for access to each program. This would not require any additional enrolment by the individual, as they must enrol one-time with each program already, though would require they register for and track each epass separately.

Business registration. In addition to individual registration and enrolment, Canada's GOL initiative will support business enrolment and registration. The first program and department to participate is expected to be the Employment Insurance (EI) program, as managed by Human Resources Development Canada (HRDC).[8] This online registration project will support the submission of Records of Employment (ROEs) by Canadian businesses. Business representatives will similarly enrol within the program, whereas a business-designated representative manages control regarding who is able to enrol.

2.2 Certificate Lifecycle Management

In the previous section, epass registration and program enrolment were discussed. In this section, we focus on the certificate lifecycle management operations of renewal, recovery and revocation.

2.2.1 epass Renewal

Presuming that an individual is able recall their password, periodic (and automated) update of an epass represents the dominant certificate management activity. This update would be attempted when a prescribed portion of their certificate lifetime has been reached, as certificate update requests would be generated (transparent to the individual) at each occasion when they login to access government services. Currently, a citizen epass is issued with a five-year lifetime, and updates are attempted once 50% of this lifetime has elapsed.

2.2.2 epass Recovery

In the case that an individual loses control of their password, additional measures must be in place. It is widely recognized that automated recovery processes are key to offering a cost-effective system; else help-desk costs can dominate (e.g. based on lost passwords). As such, as part of the epass registration process, individuals provide a list of challenge questions and corresponding answers. As a result of a successful recovery, a new verification certificate is generated, containing the same MBUN.[9]

At a later time (such as when they no longer remember their password), the user will be prompted with the question and provide the appropriate answer for each. The current question and answer model involves providing a fixed list of questions to the user, with the user selecting five and selecting from a list of fixed answers. (See [Just03] for alternative recovery question models.)

A *graduated lockout* mechanism could be used to mitigate against exhaustive attacks attempting to maliciously recover a user. In such a scheme, an individual could be temporarily locked out for several rounds, each round triggered by a number of consecutive recovery failures. Looking ahead, other options for recovery are possible, including free-form answer submission and possibly voice biometrics. In the latter case, a user could be prompted to record a short statement when registering. At recovery, the individual could be asked to repeat the statement. Of course, this would unfortunately require a change in service channel (from computer to phone).

[8] http://www.hrdc-drhc.gc.ca/

[9] Hence, this is more properly viewed as *account recovery*, rather than *epass recovery*.

If an individual is unable to recall their username, then the recovery questions cannot be retrieved and posed to the user. Since the CA does not have any other context in which they could re-register the user, this could require re-registration and further, re-enrolment in each program.[10] However, one could envision making use of the reverse PID-MBUN mapping (stored at a program) to aid recovery. Subject to the user's consent, it would be technically possible to allow the user to subsequently identify themselves to a program (that both has a record of the PIN-MBUN mapping and has a suitably secure set of shared secrets that may be used to identify the user) in which case the MBUN could then be used to proceed with the aforementioned recovery process through the CA.

2.2.3 epass Revocation

Given the distinction between registration and enrolment, we can consider two instances of "revocation." As related to public keys, an individual's epass can certainly be revoked, in which case the individual would no longer be able to use the revoked certificate to authenticate to any government program. There seem to be few reasons for which such a revocation would occur (e.g. death). Currently, the certificate owner is able to revoke their certificate by correctly responding to their recovery questions.

In addition, per-program "revocation" can occur by "de-activating" the PID-MBUN mapping so that for that program a user cannot be successfully authenticated. Depending on the reason for revocation in both cases, programs may still want to be able to verify digital signatures so that a history of the PIN-MBUN mapping is maintained.

3 System Use

The first and only application that currently makes use of the epass system is the Address Change Online (ACO) application provided by the Canadian Customs and Revenue Agency (CCRA – formerly Revenue Canada). The steps performed during the execution of this application are depicted and described below.

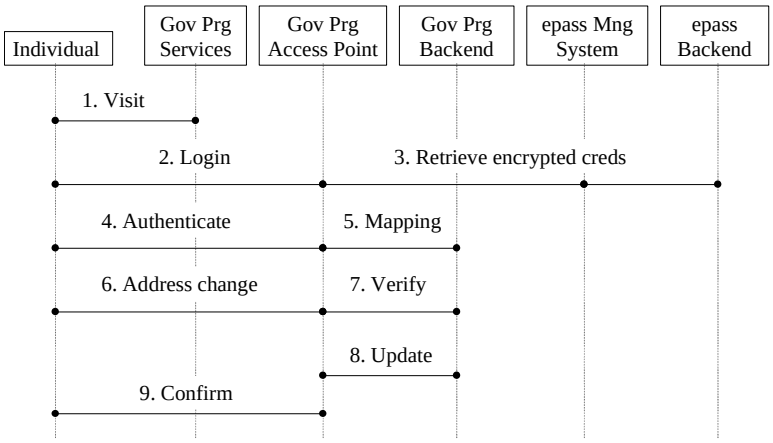

Figure 3: Program login and execution of address change application

[10] Other systems, such as Yahoo!, support the recovery of the username by matching to the user's email and sending an email, containing the username, to the user's email address-of-record. However, with the GOL solution, the CA is not privy to any personal information that might identify the user (such as an email address). Hence this solution cannot be used.

1. The individual visits a Federal Government program web site using their web-browsing client for the purpose of obtaining some secure services. The individual is redirected to the program Access Point (AP).
2. At the AP, there are several options, depending upon whether the user has previously registered for an epass or enrolled with the program:
    a. If the user already has an epass, they either
        i. Login (presuming the user has already enrolled with the program) and securely access program services (see Section 3), or
        ii. Enrol with the program.
    b. If the user does not have an epass, or wish to obtain a new pass for use with this program, they will proceed with enrolment.

    Assuming that the individual already has an epass and has enrolled with the program, at this point the individual will enter their user ID and password for retrieval of the epass.
3. Through a secure session, the individual's encrypted credentials are retrieved and returned to the individual.
4. The individual's password is used to decrypt their encrypted credentials at their browser and the individual uses their epass to authenticate to the government program. A signed cookie is returned to the browser if the authentication is successful.
5. Upon verification of the user's authentication attempt, the MBUN from the epass is used to map to the appropriate program ID (PID).
6. As part of the ACO application the user may browse their address information. When they choose to update address information, the appropriate form is returned to the user. The user completes the form then it is digitally signed and encrypted and returned to the web server.
7. The server validates the signed message, including revocation checking, and confirms that the user is authorized to make the change for the address information corresponding to the given PID.
8. The address change is made in the government program database and the signed and encrypted confirmation form is also stored.

The ACO application is particularly interesting from a privacy point of view as it represents an application whereby an individual is able to both view and correct their personal information – in this case, their address information. As with epass registration, the retrieval of the epass is achieved in an anonymous way, so that the central epass system does not know any personal information regarding the holder of the epass. Authentication and signing with the epass credentials are performed so that only the program in question is able to successfully identify the individual (through the MBUN-PID mapping).

4 Discussion

The resultant epass system is a combination of technical, legal, policy and procedural controls. As in the previous sections, in the discussion below we focus on the technical aspects, though will cite other controls as appropriate.

It is likely that a variety of other technical solutions would satisfy the security and privacy requirements for individuals, and likely more or less proficient in different areas. The primary advantage of a public key-based system is that it allows storage of persistently authenticated data with a digital signature. The management support (though not necessarily unique to PKI) is also advantageous, supporting relatively convenient automated renewal, recovery and revocation.

The advantageous properties, relating to the use of pseudonymous certificates, are discussed primarily in Section 4.1 below. The alternative of veronymous[11] certificates seems unnecessary, and would likely result in either a set of sufficiently identifying information being stored in the certificate (in order to satisfy the differing identification requirements within the context of each program) or a smaller set of information being used similar to a universal identifier. Alternative solutions, using attribute certificates for example, might also produce a sufficient solution. With the current epass solution, programs maintain their current individual identifiers.

4.1 Privacy

The familiar set of privacy principles (e.g. FIPs [FIPs00], OECD [OECD80]) cover a wide range of issues and a broader set of potential services than for the epass functionality discussed in this paper. In the discussion below, we enumerate some of these principles as relevant, as well as some additional principles that seem appropriate to analyzing an authentication system (some of which were stated in the results of the Privacy Impact Assessment performed on the epass system [Priv02]).

We focus on the attributes relevant to the epass as a pseudonymous certificate below. Note that signed messages are also encrypted so that information about an individual, as contained in a signed message, is only visible to the intended recipient.

1. *Anonymity/Pseudonymity*. Outside of a program in which an epass-holder has enrolled, the public key certificate reveals no information about an individual; to an observer, the individual is essentially anonymous. Within a program that the individual has enrolled, the MBUN acts as a pseudonym, allowing proper identification of the individual once linked to the PID.
2. *Choice*. Individuals can choose to register for a single epass, or alternatively, a separate epass for use with each program. With a single epass, a comfortable level of privacy is provided since (i) programs will continue to use the PID as their primary index (recall, the MBUN can change, outside of the control of the program), and (ii) legislation [Priv85] and policy [Priv93] restrict the sharing of information between government programs. While more than one epass might allow a more comfortable separation of program information for some, it requires registration for and tracking of more than one epass (e.g. to determine which epass is used for access the services of a particular program). More generally, further choice is offered by the maintenance of multiple channel support (e.g. telephone), in which case individuals are not obliged to obtain an epass.
3. *Inference*. Compared to an alternative solution in which the name of a particular issuer and subject are cited in a certificate (e.g. if "John Doe" were issued a certificate from the "Department of Corrections"), no similar inference may be drawn with an epass as the Government of Canada issues certificates.
4. *De-centralized information.* The only centralized entity involved in this system (the CA) does not possess, nor is ever given, personal information.
5. *Data separation*. With a single epass, programs index on a program ID (PID). Privacy legislation and policy ensure that new use of information is not performed without user consent [Priv85, Priv93]. As a technical option, users may choose to have more than one epass.

[11] A term coined by Carlisle Adams. Distinguishing from anonym ("no name") and pseudonym ("false name"), a veronym refers to a "true name." A veronymous certificate refers to a certificate that contains a veronym.

6. *Access to personal information*. As a particular example, specific to the ACO application, users may view and correct their address information within a program.

An additional concern related to privacy is that of identity theft. Such theft could allow fraudulent program enrolment. For this reason, each program ensures that a suitably high level of assurance is supported when identifying individuals. In addition, the design philosophy, whereby individuals must enrol separately to each program, mitigates the scope for potential fraudulent enrolments.

4.2 Security

Beyond system privacy, system security can be qualified. We do so by discussing the confidentiality, integrity and non-repudiation as achieved by use of an epass. In general, these properties are achieved using a combination of familiar technical security controls, in addition to other physical and procedural controls; we highlight some relevant technical controls below.

The individual interacts with programs through secure sessions. Therefore, we achieve confidentiality and integrity by reliance on this secure channel (i.e. SSL). In addition, persistent encryption and signing beyond the session may also be achieved depending the needs of a particular government program. For persistent encryption, a client is able to encrypt using the encryption certificate for a back-end server. Similarly, a client may persistently sign information, in support of authentication and non-repudiation.

Elaborating on identification, certificates are pseudonymous whereby a link is maintained at each program that matches the MBUN to the corresponding PID. In addition, at enrolment, the individual signs the evidence of enrolment. This supports proper identification (as would be necessary for further authorization requirements) and allows evidence to be contributed for non-repudiation. For an observer outside of a government program, the verification certificate attached to the signed (and encrypted) data is not readily attributable to any particular individual.

5 Concluding Remarks

In this paper, we've described and analyzed the system in which individuals may obtain an epass for accessing secure services online. Currently, this system is demonstrated through a single address change application. However, many more applications will be added as more and more departments similarly offer secure services.

This use of public keys for an epass is similar to modifications as suggested by Ellison [Elli02]. In our case, the use of some certificate identifier (other than the public key or some other value dependent upon the public key, such as its hash) allows for the same identifier to be used even as a result of epass renewal or recovery (in which case, a new public key is generated).

Looking ahead, there will be numerous opportunities for individuals to operate within multiple jurisdictions with their epass. Already, cross-certification has begun between the federal and provincial levels. And as this paper is written, the Canadian Federal Government is working towards cross-certification with the US Federal Bridge CA.

Acknowledgements

Thanks to several Treasury Board colleagues for their helpful comments, including Rick Brouzes, Michael de Rosenroll, Rhonda Lazarus, Wendy Stewart, Brenda Watkins and John Weigelt. Thanks also to the workshop referees for their comments.

6 References

[Elli02] Carl Ellison, "Improvements on Conventional PKI Wisdom," in *Proceedings of the 1st Annual PKI Research Workshop*, April 2002. http://www.cs.dartmouth.edu/~pki02/

[Laza02] Rhonda Lazarus, "Government of Canada's Legal and Policy Framework for Government On-Line," presented at *Canadian IT Law Association Conference*, October 2002. http://www.cio-dpi.gc.ca/pki-icp/issuesactiv/frame/frametb_e.asp

[FIPs00] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2000 http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

[Just03] Mike Just, "Designing Secure Yet Usable Credential Recovery Systems Using Challenge Questions", *Workshop on Human-Computer Interaction and Security Systems*, 6 April 2003. http://www.andrewpatrick.ca/CHI2003/HCISEC/index.html

[OECD80] Organization for Economic Co-operation and Development (OECD), "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 1980.

[PIPE00] Department of Justice – Canada, *Personal Information Protection and Electronic Documents Act (PIPEDA)*, 2000. http://laws.justice.gc.ca/en/p-8.6/text.html

[Priv85] Department of Justice - Canada, *Privacy Act*, 1985. http://laws.justice.gc.ca/en/P-21/index.html

[Priv93] Treasury Board of Canada, Secretariat, *Privacy and Data Protection Policy, Chapter 2-5 – Data Matching*, Dec 1, 1993. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_5_e.asp

[Priv02] Treasury Board of Canada, Secretariat, *Privacy Impact Assessment Policy and Guidelines*, May 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp