E-GOVERNMENT AND IDENTITY MANAGEMENT IN BRITISH COLUMBIA: IMPLEMENTATION OF THE BCEID

by

Vance Michael Lockton
M.Sc. (Computer Science), University of British Columbia, 2005
B.Math. (Computer Science), University of Waterloo, 2003

PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF PUBLIC POLICY

In the
Faculty
of
Arts and Social Sciences

SIMON FRASER UNIVERSITY

Spring 2009

APPROVAL

Name: **Vance Lockton**

Degree: **M.P.P.**

Title of Capstone: **e-Government and Identity Management in British Columbia: Implementation of the BCeID**

Examining Committee:

Chair: **Nancy Olewiler**
Professor, Public Policy Program, SFU

Doug McArthur
Senior Supervisor
Director, Public Policy Program, SFU

Dominique M. Gross
Supervisor
Professor, Public Policy Program, SFU

Rod Quiney
Internal Examiner
Visiting Public Service Fellow, Public Policy Program, SFU

Date Defended/Approved: April 8, 2009

Declaration of
Partial Copyright Licence

Abstract

As the Government of British Columbia looks to expand its online, public e-Government service offerings, it requires a means of controlling citizen access to these applications. An *ad hoc* system of individual service providers offering application-specific means of access is not tenable on a large scale; instead, the Province must look towards a centralized system of Identity Management and Authentication (IdMA) – the BC*e*ID. This project describes a number of the challenges associated with the development of an IdMA system, and examines some of the potential implementations of such a system by investigating the ways in which each would address these challenges. Through a multi-case analysis, it is determined that a claims-based identity system is the most appropriate for current deployment.

Keywords: e-Government; Identity Management; Privacy; BC*e*ID; Public Administration

Executive Summary

In a move towards increased efficiency and effective service provision, many governments around the world (including that of British Columbia) have been shifting towards online service provision. While such 'e-Government' programs offer significant benefit to both government and citizen, significant challenges are presented. Not least among these challenges is the determination of with whom an agency is interacting. The Internet was not designed with identification in mind, and as such there are limited means of making this determination, which is generally limited to knowledge of a shared secret (i.e. a password). Such identification is invaluable to e-Government systems, however, as an individual's rights to access services and records must be determined.

Thus, this project looks to address the question of: **How can British Columbia best address the identity management and authentication (IdMA) challenges associated with e-Government?**

Methodology

To answer the above question, a case study methodology was selected, to look at the possible impacts of various technical and social features on the variable of interest: citizen adoption and use of the IdMA system.

A survey of literature gives three primary areas likely to significantly influence adoption rates: Usability, which covers factors such as the functionality and difficulty of use of the system; Trust, which covers factors such as privacy, security, and consequences of failure; and Perception, which covers likely public opinion regarding the system. A number of investigative questions were developed in each category, and applied to the IdMA systems developed by the

respective governments of three chosen case study jurisdictions: Canada, New Zealand, and Austria.

From the resulting analysis, three primary options are proposed for British Columbia's future IdMA system, in addition to the status quo. These are:

1) Creation of a 'key' to provide access to e-Government services. This option focuses on ongoing access control, as opposed to initial identification.

2) Creation of an online identifier. This option would be similar to offline means of identification, in which the identity attributes established by an authoritative body are broadly recognized.

3) Join an Identity Federation. In this option, in addition to issuing identity credentials government services would recognize attributes issued by trusted non-governmental bodies. This is a conceptual expansion of alternative 2.

Findings and Recommendations

The above described alternatives were then tested against a number of criteria, including: acceptability (meeting of the government's IdMA principles), cost, current feasibility, advocate response, familiarity, risks upon failure, technical burden on the user, and the breadth of services offered. Three primary recommendations are derived from the analysis:

1) Select, and actively promote, a secure and intuitive claims-based online identifier. A claims-based system, which allows users to select the information about themselves being transmitted during a transaction, has significant benefits for control, privacy and security. For these benefits to be fully attained, though, the system must be promoted, highly secure, and pose a low burden to users.

2) Use an open standard for the above system. This would increase the potential for realizing the benefits of an Identity Federation should they become implementable in the future, without sacrificing the immediate availability of the proposed online identifier.

3) Look beyond current necessity. The British Columbian government has the opportunity to install itself as an innovator on this issue; doing so may not only raise its global standing, but also encourage system adoption. As such, future system development should be factored in to any analysis undertaken.

Dedication

To Wendy Foster, for finding this program, inspiring me to complete it, and improving my life in innumerable ways.

Acknowledgements

Thank you to my supervisor, Doug McArthur, for recognizing and providing the guidance I required, and to Rod Quiney, for allowing me access to the breadth of experience in his career, and bringing an 'insider' eye to this project.

Thanks also to Fred Carter at the Information and Privacy Commissioner's Office of Ontario, for our conversations on matters of privacy; you are a highly valued colleague.

Finally, endless thanks go to Wendy Foster. When I needed inspiration, one conversation with you could clarify, enhance, or even supersede days of research. And more importantly, when I needed motivation, you provided for me a beatific future upon which I can always gaze.

Table of Contents

List of Tables

1: INTRODUCTION

Devising a policy framework for the protection of digital identity and its management may be one of the most important public policy matters to shape the future of our e-society (Hardt, 2006)

In an effort to revitalize public administration, many governments worldwide are moving towards service-orientation, proactivity, efficiency and transparency (United Nations, 2008). One of the principle efforts in this transformation has been a move towards e-Government, defined by the World Bank (2008) as the use of information and communications technology (ICT) to improve the efficiency, effectiveness, transparency, and accountability of government by both providing better services to citizens and businesses and empowering through information. This use of ICT within a government can improve inter-departmental communications and coordination of authorities, the speed and efficiency of operations, research capacity, documentation and record-keeping (United Nations, 2008). Importantly for this project, though, e-Government can also re-shape a government's interactions with its citizens, and vice versa. Canada's Government Online (GOL) initiative, for instance, which was launched in 1999 and completed in 2006, has made 130 of the most common used services available online since 2005 (Underhill and Ladds, 2007). The 2006 Government On-Line report puts the number of online interactions with government in Canada at over 300 million (in 2006), comprising 30% of all citizen-government transactions (Underhill and Ladds, 2007). The same report described a 2006 survey that found 71% of Canadians sampled who were Internet users had accessed a government website in the prior 12 months.

The GOL initiative, along with its take-up by citizens, has ranked Canada among the global leaders in e-Government for the past decade. Accenture (2004), an international

management consultant and technology services company, ranked Canada as the country with the most mature e-Government offerings from 2001-2004 (the years in which that report was released); a similar study by Japan's Waseda University (Obi, 2008) has ranked Canada as one of the top 3 e-Governments globally each year from 2005 to 2008. Similarly, a 2008 United Nations survey ranked member nations on various aspects of their e-Government services; of 192 countries, Canada ranked 7th (up from 8th in 2005) in e-Government readiness, 8th (2005: same) in a measure of policy and service provision, and 11th in e-Participation utilization levels (down from 4th in 2005) (United Nations).

The government of British Columbia has also been actively moving towards the notion of e-Government. In 2006, BC's Office of the Chief Information Officer (CIO), which in that same year was mandated with governance authority for oversight, approval, and standard setting the province's information and communications technology (BC CIO, n/d), developed the Information Management / Information Technology (IM/IT) Plan. The (somewhat vague) purpose of this plan is to "support government's goals and improve information sharing to better achieve citizen outcomes" (BC CIO, n/d(a)). To achieve this, the CIO lists three desired outcomes: value for money, information sharing for better outcomes, and service transformation (BC CIO, n/d(b)). Each of these outcomes speaks to a desire, and expectation, for increases in efficiency: citizens want a streamlining of both service access and delivery, while government looks to wisely allocate their limited funds and restructure processes to remove any duplicated efforts.

1.1 Policy Problem

Access to e-Government services is highly analogous to the same access at a government office. Some interactions, such as the acquisition of government publications or the retrieval of various forms, require no identification; anyone who can gain entry to the site (physical or online) is given implicit rights to access these materials. Other interactions, though, involve personal or

otherwise sensitive information, and as such require the authentication (fully defined in Section 2.3) of an individual's identity or credentials prior to the granting of access. At an office, the authentication process will be clear, and will generally involve the presentation of an identifier to a clerk or agent. Online, however, this process is less clear; what will serve as an identifier, and how will it be presented? As an additional factor, *ad hoc* user authentication systems, tailored to individual online applications, will not be an effective pathway to the end-goal of a comprehensive and cohesive online government (Treasury Board of Canada Secretariat, 2003). Instead, to create an effective identifier while promoting e-Government adoption, a single, coherent authentication scheme (which may include a number of interconnected systems) must be developed - a fact that has been recognized by many government levels within Canada, including both the federal and British Columbian provincial governments. There are many design elements to such a scheme, however, that will have to be considered prior to any implementation; it is these elements that will shape the discussion in this work.

Coincident with the challenge of authentication there is an interesting opportunity presented. In the 'offline' world, government has effectively cornered the market on identity documentation. The vast majority of these formal identifiers (those documents or objects that will confirm an individual's identity assertions within a particular context[1]) used by an individual in his or her daily transactions are either provided directly by a government agency (driver's license, social insurance number, health card, etc.) or are issued based on the presentation of such an identifier (student or employee ids, for example, are frequently issued upon presentation of a government-provided photo id).[2] Online, this is not the case. There, when identity must be established (which, as in the offline world, is not always the case for transactions/interactions), the general means of authentication is self-assertion. The most widely used method of

[1] As opposed to informal identifiers, such as verbal declarations by a friend or colleague.

[2] Credit cards are (in some situations) a prominent exception to this rule, though applications for such cards will also frequently request a driver's license number, social insurance number, etc.

establishing identity, the username and password pair, is of that type: by entering the pair and interacting with an application using the associated credentials, an individual is effectively asserting that he/she is in fact the person with whom the credential is associated (as opposed to someone who has simply discovered – by some means – the username/password pairing). Further, there are few means (these will be discussed later) in Canada to establish a connection between an online identity and a government-issued identity, without resort to "proof-of-knowledge" of offline identity documents. The opportunity in this situation, then, is for the creation of a government-issued and/or -verified online identifier.

In its simplest form, such an identifier is one solution to the authentication problem described above: to provide e-Government services, ministries must be able to establish with whom they are interacting, and any of a range of identifiers (from username/password to a computer-stored string of encrypted data) could be created specifically for this task. An online identifier could be extended beyond this, however, should a government so desire; rather than limiting the effective realm of the of the identifier to e-Government authentication, it could be broadened to many other applications, such as online retail or e-Banking (much as the driver's license has become a general-purpose identifier offline). Of course, a government may not wish to be an exclusive online identity provider; though it is non-traditional, it may also be reasonable to consider a scheme by which a third-party-backed identity token is accepted as an authenticating document.

Thus, we are faced with an intriguing policy problem: **how can British Columbia best address the identity management and authentication challenges associated with e-Government?** The answer to this question will depend on available options and the factors motivating movement, both of which will be discussed in this paper.

1.2 Study Outline

This study is organized into seven sections, beginning with the current one which introduces the policy problem. Section two describes the current state of e-Government in Canada, British Columbia's efforts at developing an online identifier, and explicates exactly what is meant when by the term identity. Section three lays out the investigative framework that will be used to systematically review the case studies assessed in this work, which are also introduced in this section. The fourth section describes the case study analysis, and draws best practices to be followed in the development of IdMA systems. Section five introduces the alternatives available to British Columbia, which will be evaluated by the criteria introduced in section six. Section six also sets out a number of recommendations for the province's IdMA development. Finally, a conclusion and final analysis is presented in section seven.

2: BACKGROUND

In order to provide an understanding of the topic, an overview of the current state of e-Government both in Canada and the province of British Columbia, as well as a discussion of what is meant by the term 'identity' when we speak of identity management, are required, and presented in this section. This is followed by a sampling of the issues found with the current means of online identity assurance. Finally, a brief discussion of the scope of this study is undertaken, describing in particular what will *not* be covered herein.

2.1 e-Government in Canada

Canada's 'Government On-Line (GOL) / Service Improvement Initiative' was launched by the October 1999 throne speech, which made the following commitment:

> "The Government will become a model user of information technology and the Internet. By 2004 (now 2005), our goal is to be known around the world as the government most connected to its citizens, with Canadians able to access all government information and services on-line at the time and place of their choosing." (Canadian ePolicy Resource Centre, 2008)

The GOL initiative was allocated $160 million dollars over 2 years in the 2000 budget, and another $600 million (for the years 2002-2006) in the 2001 budget. This money was used to fund, among other projects, a redesign of the Canada.gc.ca website (including the grouping of services for individuals, businesses and non-Canadians) and the Secure Channel Project, which provides citizens and businesses secure access to government services. However, the keystone of this project was the development of Service Canada. Launched in 2005, Service Canada with the goal of providing citizens one-stop, client-driven, whole-of-government access to any services they might need. As of 2007, it has partnered with 14 departments to provide over 75 services, which are available at over 600 Service Canada locations, through a central phone number (1-

800-O-CANADA), or through the Service Canada website, which handled 11 million transactions during the 2006-07 fiscal year (Service Canada, 2007).

As previously stated, overall 130 of the most commonly accessed services are available online[3], and approximately 30% of all citizen-government transactions currently take place online. These numbers become of greater importance when one considers the cost-savings associated with online transactions, as compared to those occurring over the phone or in person. Public Works and Government Service Canada (PWGSC) estimates that an in person transaction costs the Government approximately $30, a transaction by mail $20, and phone transactions $10, while transactions over the Internet tend to cost less that $1 (PWGSC, 2008).[4] Thus, there are considerable savings to be had as Canadians migrate their interactions to government websites.

Though the Government On-Line initiative formally concluded in 2006, it left a legacy of online service provision that spoke to the desire of citizens for more effective, easy access to government[5]. The success of this project can serve as an example to provincial governments, which often have greater dealings with citizens that the federal government, as they look to redesign their own functionalities.

2.2 BC*e*ID

Currently, neither Canada nor British Columbia has an explicit law or policy with regards to identity management; instead, identifiers are created on an as-needed basis by various program

[3] By category, the services are informational (63), transactional (67), and complete service (45) (Canadian ePolicy Resource Centre, 2008)

[4] These savings are mitigated by other factors, however. For instance, in my interview a Revenue Canada representative revealed that though the number of phone interactions with that agency has decreased after the GOL initiative, the cost per call has increased, as the majority of calls are now about 'difficult' issues that the individual was not able to solve by him/herself online. (Quiney, personal communication, 2008)

[5] A May 2002 survey found that 92% of Canadians supported such a 'one-stop-shop' for accessing Canadian Government services (Service Canada, 2007)

requirements (Watkins, 2007). During the various developments of their e-Government portal[6], the BC government recognized such a need, and created the BC*e*ID – a single credential (username/password), issued in-person at a government Point of Service location, to be used across a range of online services[7]. This initiative was undertaken when it became clear that without an overall solution, individual government service providers would issue website-specific usernames and passwords to individuals and organizations desiring online access, a "mess that the government did not want to experience" (Watkins, 2007). By starting its investigation of this technology early on, the BC government looked to avoid the problems associated with the roll-out of a major technology, by both gaining knowledge and experience with the system prior to full deployment and not forcing a system of identity on the public before any useful, associated services could be made available (Watkins, 2007).

The next iteration of this system, the BC*e*ID Next Generation (BC*e*ID*ng*) is currently under development. Again, the BC CIO's office has taken the wise step of making a significant study of potential solutions prior to deployment, a process that has included various identity forums and task forces; as such, however, no technical details have yet been determined.

2.2.1 Pan-Canadian Identity Management Task Force

One of the projects entered into during the development of the BC*e*ID*ng* was the Inter-Jurisdictional Identity Management Task Force. This task force, made up of deputy ministers with responsibility for service delivery across provincial, territorial and federal governments and chaired by BC Chief Information Officer Dave Nikolejsin and Directeur des Politiques for Quebec Michael Rosciszewski, set out to establish a pan-Canadian strategy for Identity Management and Authentication (IdMA) that would facilitate seamless, cross jurisdictional,

[6] Among Canadian provinces, BC has been an e-Government leader. As early as 2001, the BC Connects website offered 500 services, and was ranked as the top service delivery website in Canada (Lester, 2002)

[7] As of this writing, there are just over 80 services accessible with a BC*e*ID account.

citizen-centric, multi-channel service delivery (I-J IdMA Task Force, 2007). The final report of the Task Force contains a list of principles (which are described in detail in Appendix A) to guide identity management which will guide this discussion (from I-J IdMA Task Force, 2007):

1. IdMA requirements and uses should be justifiable and proportionate to the task.
2. Clients should have choice, consent and control over their identity credentials and the uses to which they are put.
3. Use of identity information should be limited to a specific purpose and to justifiable parties.
4. IdMA processes should be client-focused and provide a consistent experience.
5. An IdMA environment should recognize a diversity of identity contexts and systems.
6. IdMA should be provided in a trusted and secure environment.
7. All IdMA activities should be transparent accountable.
8. IdMA processes and methods should provide an enduring solution, which is technologically neutral, flexible and scalable.

These principles will be taken as instrumental to the evaluation of any potential system of identity management within this work.

Also important to this work is a discussion of the role of authentication to e-Government, described as the "virtuous cycle" (OPC Canada, 2007). Specifically, it is noted that a re-enforcement takes place between a good IdMA design and e-Government, in which improved identity management leads to the more users of e-Government, which makes the online channel more important to the public service, which will increase the number of online services offered, which in turn lead to more users, and so forth (OPC Canada, 2007).

2.3 Establishing Identity

In order to discuss identity management and authentication systems for e-Government, we must understand what is meant by the term 'identity.' A person's identity is made up of a series of attributes, or claims made about that person (by him/herself or by another) (OPC Canada, 2007). This attribute information is widely varied, and includes name, appearance,

government-issued index numbers (driver's license, social insurance number, etc), personality traits, etc. These attributes are sometimes context dependent; one can easily envision personality traits varying across social situations, for instance.

Identifiers, on the other hand, are a subset of one's attributes, which uniquely identify an individual in a given context. Within a social group, for instance, it is likely that an individual's name serves as a unique identifier. Within Canada, however, this is less likely; within the world, even less so. Authentication, then, is the establishment of the full identity of the individual with whom one is transacting through the verification of his/her presented identifiers.

Authentication of one's identity comes from one or more of three factors (given in increasing level of security): something you know, something you have, or something you are. 'Something you know' refers to a piece of secret information, such as a password, or a piece of personal information that is generally unknown. Revenue Canada, for instance, will sometimes use the amount an individual entered on a particular line of their last tax return as a verification check. 'Something you have' refers to an item of which only a particular individual (or group of individuals) will be in possession. This is a commonly used check; any number of services verify individuals by the ID cards (driver's license, health card, various membership passes, etc) that they carry. Finally 'something you are' refers to an individual's personal characteristics. This can range from features as common as a picture (thus, a check of a driver's license is both a check of something you have and something you are), to fingerprints, retinal scans or other biometric traits.

Establishment of identity is not always required for service provision, however; instead, it is often sufficient to prove a particular non-identifying attribute associated with a person. Monthly (non-discounted) transit passes in Vancouver (and many other cities) do not require any personal information for use; the desired attribute (payment of fare) can be established without resort to an identifier. Similarly, a cashier selling alcohol needs to know only age – an attribute

of a person – and not, in fact, a person's identity. It is incidental, not necessary, that the generally accepted means of establishing this attribute (driver's licenses, age of majority cards, etc.) reveals many other identifiers of a person (name, picture, etc.).

Appropriate identity authentication measures are also not static within a situation, but may need to flex with individual preference. Consider, for example, the retail sector. Payments made in cash are (as close as possible to) anonymous; the payer generally requires no identifiers. Interact-based transactions are also, effectively, "zero-knowledge"[8] from the point of view of the retailer. The payer in this case is able to initiate a payment by proving knowledge of a secret (by entering a PIN) without revealing that secret to the retailer. For credit card purchases, an identifier (the payer's name & signature) is both revealed to and retained by the retailer. Each of these is a wholly valid method for authenticating payments, selection amongst which occurs at the convenience of the payer.

2.4 Issues with Identity Assurance

Finally, we must also discuss the current, and sometimes inherent, flaws associated with the current regime of online identity management. The first of these has to do with authentication. Current Internet services, government or otherwise, have a strong tendency to rely on the username-password combination to identify users. Referring back to the 3 levels of authentication security (something you know, something you have, something you are), it is immediately apparent that this schema is single-factor (something you know), with that factor having the lowest security. This is largely a technical-capacity issue; most Internet users will not have immediate access to a biometrics device (i.e. fingerprint reader) or smartcard reader, and trusted computing modules (in brief, a piece of hardware with characteristics unalterable even by

[8] Zero-knowledge systems allow individuals to prove that they know (or are in possession of) certain (generally secret) information, without revealing that information, thus maintaining the strength of their secret knowledge

the computer's owner) are under-utilized, if present. Thus, online interactions, by current necessity, are secured largely by "shared secrets."

The principle issue here is that knowledge is non-rivalrous; that is, an individual's knowledge of a password (or other security phrase) does not preclude use of the same information by another. This is in contrast to physical, and therefore rivalrous, identifiers; if an individual maintains possession of his or her driver's license, for example, he or she can be assured that it is not being used by anyone else.[9] Malicious agents have been able to take advantage of this weakness in the username-password system, extracting this key-pair from many individuals (across many different services) using phishing, keystroke logging, and other ploys. It should also be noted that this is frequently a problem with the initial assignment of usernames to individuals, in that it is very difficult to establish whether an individual in possession of a shared secret is actually the person intended; knowledge possession by itself is a weak authenticator, but is generally the factor relied on. E-Government service providers will, of course, look to avoid this possibility by, among other measures, the utilization of multi-factor authentication, wherever appropriate.

Another feature of the current online identification system that should be examined is associated with the burden of maintaining security. In the offline context, regardless of the measures employed to maintain the integrity of an identifier, the user need only carry and present the credential; he or she can be wholly ignorant of these security measures with little to no repercussions. The burden of strengthening of security measures (largely in relation to preventing production and use of false or cloned credentials) lies almost entirely with the issuing agency; the identified individual need only focus on maintaining control of the identifier (small burden in the case of a card, no burden in the case of biometrics). On the other hand, the burden of the

[9] Again, we must be cautious here. While the card itself is rivalrous, the data stored on it is not. This is one factor to, for instance, the abundance of credit and debit card fraud; all requisite data for the cloning of a card is presented at each transaction – the card itself (prior to Chip-and-Pin cards) is not a security factor. Ideally, a card would have a unique, unclonable identifier – a difficult task, to be sure.

username and password combination rests almost wholly on the user, who must recall this combination when needed. This can become significant when 'security measures' are added, which ask the user not to re-use passwords across applications, to regularly change passwords, use character combinations that include numbers and symbols, and which cannot be associated with either a dictionary word or a feature of the user (birthday, address, etc). This difficulty, be it small or great, may drive an individual away from the use of a new service, or towards poor security practices in regards to his or her credential (e.g. 'poor', re-used, or written-down passwords). Again, an e-Government service provider should, if nothing else, be aware of the burden of identification, and evaluate the costs and benefits of alleviation.

2.5 Confounding Factors in e-Government

There are two clear confounding factors when identity management is applied within an e-Government context. The first is a very small margin for error. The benchmark online identity management applications, deployed by banks and credit card companies, are generally able to correct erroneous or fraudulent transactions by financial means, such as the cancellation of charges or monetary compensation. As such, these companies are able to factor these error corrections into their business plans. E-Government services, however, tend to deal with information; should such a system be breached, there is no clear reparation available. Additionally, as e-Government is a monolithic entity, individuals cannot move to a more secure service provider (as no other provider exists); thus, no economic signal as to the value of security and correct functioning can be derived from market signals. Thus, e-Governments must, from the start, utilise very secure and very functional systems, as a cycle of post-deployment problem definition & solution will likely not be available.

The second confound of the e-Government context is that there is actually an upper limit to the level of efficiency that will be acceptable to the general public. Significant gains, for both government and the individual, in efficiency and service provision could potentially be had, for

instance, by the use of a single, universal (or national) identifier that could be correlated across services. However, the concept of such a National ID is far from generally accepted. While a survey of Canadians found that 53% of individuals favour the introduction of a National ID card (Boa et al., 2007), those that oppose such a project tend to be organized, active, and vocal. These groups[10] tend to focus on the correlation of individuals' information and the levels of surveillance and control afforded by such as the primary negative features of such a scheme. As such, the level of correlation made possible by any introduced identifier must be fully understood, and limited where possible.

2.6 Next Steps

This background section has described both the current state of e-Government, and introduced the reasons why identity management will be an important consideration. To conclude this section, two considerations about this study will be given.

First, as e-Government and Identity Management cover a rather broad spectrum, topics that will *not* be covered in this project must be specified. First, the deployment of e-Government will not be considered; the choice of what services should be made available online, or how governments should internally function, is considered out-of-scope for this project. Also out-of-scope are the technical evaluatory measures of identity management proposals; we cannot know, pre-development, how precisely these systems will function. Any identity scheme can be either more or less privacy protective and secure, depending on implementation. Instead, a list of the privacy and security considerations required of any system of identity will be presented, along with a general sense of the likely difficulties that will be encountered.

Second, the next section of this work will specify the structure of analysis. By looking at specific case studies, this work will review the response of various other jurisdictions that have

[10] Prominent examples in British Columbia include the B.C. Civil Liberties Association and the B.C. Freedom of Information and Privacy Association

faced a similar identity management issue. This will provide a framework for the potential responses of the British Columbian government, and help to identify the factors that are likely to be considered vital to the government's choice of action.

3: Methodology

The methodology used in this study is multi-case analysis, which examines the culture surrounding, and deployment of, three online identity management and authentication (IdMA) frameworks. The goal of this analysis is to identify the characteristics of both IdMA and e-Government in general that contribute to, or detract from, successful deployment of such a system in government. In this section, the rationale for the cases selected is presented, along with a description of the investigative framework that will be used.

3.1 Rationale for Case Selection

Identity management is an issue affecting governments, agencies, and private companies – not to mention individuals. Thus, there are any number of IdMA solutions available for analysis. The task here, then, is to determine cases that encompass sufficient scope as to be applicable to British Columbia, and to have come from a situation in which many of the same policy issues will arise. To this end, the online identity solutions of 3 governments have been selected: Canada, New Zealand, and Austria. Though the cases selected are all countries, as opposed to districts within a country (as British Columbia), the identity management goal remains similar; the government of British Columbia is looking to control and allow access to provincially run online services, much as the Canadian government (for example) controls access to federal services. Additionally, the notion of a provincially-issued identifier will be in no way unfamiliar in to residents of British Columbia, who already have exposure to the BC Driver's License, the BCID, the Care Card, and others.

The chart that follows describes a number of the general factors that were considered during the selection of cases. General characteristics of both the nation and its IdMA system are

presented in order to provide a sense of problem scope. E-Government rankings and Internet penetration rates are described based on a notion found in a number of studies which suggests that one of the determiners of e-Government adoption is compatibility – that is, individuals are more likely to adopt a system they believe to be compatible with their current experience and lifestyle (Carter & Belanger, 2003; Hung, Chang & Yu, 2006; Warkentin et al., 2002). For instance, individuals who make frequent use of the Internet are more likely to adopt an Internet-based identifier.

Also within this section, the identity management solutions selected in each country are further introduced and the reasons for their selection in for this work are touched on, though detailed analyses of the cases is reserved for the section 4. Following the overview of the cases, the investigative framework that will be used is explicated.

Table 3-1 Case Selection Overview

	ePass – Canada	IVS – New Zealand	Citizen Card – Austria
Population [11]	33.2 million	4.3 million	8.2 million
Internet Penetration (users / 100) (2 sources)	84.3 / 67.9	80.5 / 68.3	68.3 / 51.2
UN e-Government rankings:			
e-Government Readiness:	7th	18th	16th
Web Measurement Assessment:	8th	22nd	19th
e-Participation Index:	11th	6th	20th
Number of users of IdMA system	5-6 million expected by 2008-09	(to be launched in 2009) [12]	>10 million issued, but << 1 million activated
Department Responsible	Treasury Board Secretariat	Dept. of Internal Affairs	Central Register of Residents / Austria Secure Information Technology Center

3.1.1 ePass - Canada

In general, Canada is highly advanced when it comes to Internet usage. With regard to the citizen base, Internetworldstats.com puts Internet penetration (# of users / 100 citizens – a valuable measure when considering accessibility of e-Government) in Canada at 84.3 (IWS, 2008a), the 5th highest region in the world; a similar measure from the United Nations puts this rate at 67.9 (UN, 2008a), which ranks Canada 7th among 157 measured nations. The government

[11] As a reference point, the population of British Columbia stands at 4.4 million as of Oct. 2008, and Statistics Canada reports that Internet usage rates in British Columbia (along with Quebec and Ontario) are slightly higher than the Canadian average

[12] A 2007 survey of New Zealanders found that 8% would sign up for the service immediately, 21% would sign up after the IVS service was launched, and another 36% would "wait and see." (O'Neill, 2007)

is also advanced in it's use of information technology; as previously described, the UN ranks Canada 7th in e-Government readiness, 8th in its 'web measurement assessment' of online policy development and service provision, and 11th in e-Participation (United Nations, 2008).

In 2002, Canada began its Government Online (GOL) authentication program, issuing 'ePasses' to individuals. The ePass contains a "meaningless but unique number" (MBUN) which, when a user registers with an e-Government service (which is done separately from ePass registration), is associated with the identifier used by the service. The ePass user is then able to log-in to the Certification Authority, linked to from the desired e-Service site, to retrieve and present their ePass to the service provider. Individuals may have 1 or more ePasses, each associated with any number of e-Government services. The government does not retain information regarding the number of ePasses held by any citizen, or the services to which they have been associated. In addition to authentication, the ePass also acts as an electronic signature, certifying transactions between citizens and government. The ePass is used exclusively in the government service context.

Canada's authentication efforts are the most natural comparator case for the BC*e*ID system, as the technological base of the citizenry across BC will be nearly identical to that across Canada, and many of the same security, privacy and trust issues will be raised in both jurisdictions.

3.1.2 Identity Verification Service (IVS) - New Zealand

The second case that will here be examined is the system of identification associated with New Zealand's e-Government efforts. New Zealand is highly similar to Canada in its Internet penetration, with internetworldstats.com claiming 80.5 users / 100 citizens (to Canada's 84.3) (IWS, 2008b), and the UN stating 68.3 users / 100 (to Canada's 67.9) (UN, 2008a). The development of e-Government in New Zealand is slightly behind Canada, however, with NZ

ranking 18th in e-Government readiness and 22nd in the UN's web measurement index; however, New Zealanders have been very engaged in what e-Government is made available to them, as the country ranks 6th in e-Participation (United Nations, 2008). New Zealand is also a valuable comparator due to numerous political and social similarities to Canada and British Columbia. One factor of particular interest to this study is that many of the privacy issues found in Canada and British Columbia – for example, a strong resistance to the notion of the National ID – are also present in New Zealand culture.

The means of proving one's identity online in New Zealand was given a significant boost with the April 2008 launch of 'igovt'. The igovt service consists of two components: the Government Logon Service (GLS) and the Identity Verification Service (IVS). The GLS is, effectively, a single-sign-on mechanism, allowing users to use a single username-password combination to access a series of government services. The IVS, which is still in development but due to be released in 2009, is an online identifier that is meant to simplify the registration process for e-Government services. This is accomplished through the provision of a username-password-physical token combination that is used to access pre-verified online identity and credentials, instead of requiring other secret knowledge or paper-based documents[13]. An individual's IVS record is meant to serve as an online credential, equivalent in power to its offline, paper-based counterparts - as opposed to Canada's ePass, which does not hold any personal information about a registered individual, and acts simply as a cryptographic token. As such, the IVS proves who a person is during initial registration with an e-Government service, while the GLS authenticates during each subsequent access. Additionally, New Zealand's Department of Internal Affairs, which oversees the IVS, is exploring the possibility of allowing private organizations the ability to use the IVS for their own verification needs (such as banks/e-banking). Though the system has not yet reached full maturity, it is felt that significant insight

[13] By way of example, the Canada Revenue Agency asks registrants to provide the amount entered on line 150 of their previous tax return.

can still be gained through an examination of initial reaction to the IVS, as measured through the rather extensive public consultation process undertaken during development of the system.

3.1.3 Citizen Card – Austria

The final case that will be examined is the Austrian Citizen Card. Austria, a Federal Republic with 8.2 million citizens, also ranks within the top 20 countries in each of the UN's categories of e-Government rankings (16th in e-Government readiness, 19th in the web measurement assessment, and 20th in the e-participation index) (United Nations, 2008). Further, a 2006 Cap-Gemini survey ranked Austria first among EU members in e-Government services (Rössler, 2008). The Internet penetration rate of 68.3% (IWS, 2008) (or 51.2% by the UN's measure (UN, 2008a)) is the lowest among the three cases selected; however, by way of contexting this rate, Austria's internet penetration is 40 per cent higher than the overall European penetration rate of 48.5% (IWS, 2008c).

Access to Austrian e-Government services is granted by the use of a 'Citizen Card.' This program (the "Bürgerkarte" in native German), which started in 2003, is not a card, *per se*; instead, it is a collection of functions which combine to provide an effective online identity. Open standards and architecture are used to create a scheme by which almost any current 'chip-based' card can become a means of access for e-Government services – currently compatible cards include Maestro-based bank cards, social insurance cards, student cards from a number of Austrian universities, and others[14] - investigations are also underway into incorporating foreign eIDs into the Citizen Card system (Rössler, 2008). On activation, an 'identity link' – which consists of a cryptographically derived version of the individual's ZMR (Central Register of Residents) entry number – is stored on the card's microchip, along with other encryption certificates allowing for the creation of eSignatures. Use of the Card, regardless of form, is

[14] This concept is not limited to the 'card' form factor; the government has recognized the potential of other data devices, including cell phones, PCs and USB sticks meeting the Citizen Card requirements.

protected by a PIN. For home use, citizens require (in addition to an activated card) a card reader for their computer, which are sold throughout Austria. The software required to utilize the card for e-Government access is available, free-of-charge, from a government webpage.

Along with providing online access to e-Government services, the Card's eSignature feature (which allows users to digitally sign documents, which by Austrian law is equivalent to a physical signature) and authentication measures have been adopted by private Internet services, including eBanking. Of course, British Columbia cannot expect to reach this level of integration in the immediate future of its identity management; however, the case remains valuable for consideration as fully developed, reasonably successful system of IdMA.

3.2 Investigative Framework

Based on a review of literature, there are three primary areas of inquiry when examining the adoption of e-Government identity management systems – usability factors, trust factors, and factors of publicity. The investigative questions for each category are described below, to be answered in the next section based on publicly available data.

Though many multi-case analyses further rely upon elite interviews as a primary data source, this method was deliberately not undertaken during this project. 'Success', in an identity management project, is measured by adoption of the identity system by citizens (which is, of course, coupled with usage of the functions, such as e-Government services, facilitated by the identity system)[15]. As such, it is the opinion of the system held by members of the public that is crucial to the system's adoption, and thus success. This opinion will be influenced not by the privately-held intentions and goals of departments and actors, but by the information regarding the system that has been made publicly available; this includes published government documentation, consultations, media reports, usage experiences, and so forth. As such, it is these resources that will be examined during this analysis.

3.2.1 Usability

Usability has for some time been considered a key to technological adoption. Davis (1989)'s foundational work on a Technological Acceptance Model, which looked to explain variations in both current and future usage of computers, took up this notion, hypothesizing that perceived ease of use and perceived usefulness were the fundamental determinants of user acceptance. His study found that these were statistically significant influencing factors, though a regression analysis found that ease of use may have been a causal antecedent to usefulness, as opposed to a parallel, direct influencing factor. Davis' results have been incorporated, extended

[15] This is less true of mandatory systems of identity; however, it is clear that any British Columbian identifier will be voluntary at this time.

and re-confirmed by numerous e-Government researchers, including Werkentin et al. (2002), Hung, Chang and Yu (2006), Carter and Belanger (2003) , Moore and Benbaset (1991) among many others.

Within this study, we examine perceived usefulness as measured by the range of services associated with the identity management system in each case. Tradeoffs that the user would be forced to make for use, such as cost, are also taken into consideration, as is the mitigating factor of whether the identity management system and e-Government are inseparable – a 'package deal', so to speak. Finally, perceived ease of use is investigated through the technological requirements imposed on the user. In general, the aforementioned studies have found that as ease of use increases, so does a user's feeling of self-efficacy, and thus their willingness to adopt a new technology.

Table 3-2 Questions re: Usability Factors

Usability Factors
• What range of e-Government services is accessible through this system?
• Is the identifier targeted at, or accessible to, non- e-Government services, such as e-Banking?
• What functionality is available beyond authentication?
• Is use of the identifier mandatory for use of e-Government services?
• Is there a monetary cost to users?
• Are there any unique technological requirements for the user?

3.2.2 Trust

We take our definition of trust from Werkentin et al. (2002), who state that trust is "the belief that the other party will behave as expected in a socially responsible manner, and in doing so, it will fulfil the trusting party's expectation." We will also take trust as being instantiated in

one of two ways: institution-based and characteristic-based. Institution-based trust refers to the overall level of confidence found within a population that certification by a particular body, such as a government, implies confidence in right action. For this paper, this form of trust will be proxied by exposure – specifically, whether or not citizens are accustomed to a general-purpose identifier. If such an identifier exists within a nation or other jurisdiction (a National ID card or similar structure), the level of trust that must be created by a government introducing an online identity management system will be lower, as citizens need only be informed of the benefits of an expansion to an existing schema. If trust exists in the current institution, it should transfer reasonably easily to that institution's extension. If citizens have had no exposure to such a system, however, trust must be manufactured in a new institution – a much more difficult task.

Our other trust type, characteristic-based trust, has largely to do with trust in the system. As previously defined, trust can be seen as an individual's confidence that an actor will act in an expected manner; when dealing with non-human actors, such confidence is bred by control. Additionally, Warkentin et al. (2002) state that the Theory of Planned Behaviour would suggest that as citizens do not have full control over their interactions with government (which occur in a very prescribed manner), perceived behavioural control may be a vital factor in the adoption of e-Government. Such control is made up of two factors: self-efficacy (which is described above, as ease of use), and the facilitation of conditions that provide resources to engage in behaviour. Warkentin et al. suggest that in an e-Government context, this can take (among others) the form of control over data. Extending this to the identity management context, individuals should perceive that they have the greatest possible degree of control over access to, and use of, their identity information. Characteristics over which individuals cannot have control must also instill a sense of trust in users, though; thus, the privacy and security elements that are perceptible to citizens through either direct experience or system promotion factor into trust levels.

Table 3-3 Questions re: Trust Factor

Trust Factors
• Is there an existing identifier or database that is naturally transferable to the purpose?
• Is the service meant to provide users a 'key' (i.e. access to services) or an identifier?
• Which of the 3 authentication factors (something you know, something you have, something you are) are used?
• What privacy & security measures are perceptible to the user?

3.2.3 Perception

The final set of adoption factors that will be here examined relate to individuals' perception of the identity management system. One of the primary concerns of governments implementing identity management systems has to do citizens' initial adoption choices. Factors such as service availability are discoverable prior to use of the system; others, such as time savings, are not, except in a very general sense. It is here that publicity factors come in to play – governments and other interest groups have the capacity to influence the initial adoption choice through explanation of likely benefits (or costs) of using the system.

Rogers' (1983) work on diffusion of innovation, for instance, identifies relative advantage (i.e. benefit over a technology's precursor) as one of five attributes that affect the adoption of new technologies[16]. A number of studies of e-Government adoption have since experimentally confirmed this, such as Carter & Belanger, 2003; Hung, Chang & Yu, 2006; and Warkentin et al., 2002. These studies almost uniformly went on to suggest that governments would be well served to publicize the advantages of utilizing e-Government, such as time or cost savings, or convenience. For this study, however, this category is expanded slightly, from relative advantage to perceived advantage. Governmental promotions of IdMA do not limit

[16] The other four factors are compatibility (mentioned in section 3.1), complexity (which relates to ease of use), observability (whether users can observe the effects of technology on others), and trialability (whether the technology can be given a 'trial run').

themselves to this consideration of relativity; as such, I look to examine any purported 'advantages' to using a particular identity management system, regardless if a comparator is used or not.

Governmental organizations are likely to not be the only groups speaking out about IdMA systems, however; it is likely that privacy and security advocates will make their opinions known. Thus, when discussing perceived advantage, we must give these groups their voice, positive or negative. As such, both advocacy for and opposition to IdMA systems within each case will be considered.[17] One focal point to this discussion will be the general feeling of the populace regarding the notion of the National ID, to which comparisons are often drawn with IdMA systems. A further research area will examine the provision of means of feedback for individuals; can they express, without filtering through a representative agency or group, their opinions of the project in a way that is likely to be heard and (potentially) acted upon by government?

Table 3-4 Questions re: Perception Factors

Perception Factors
• What promotional factors are emphasized in governmental information releases about the system (i.e. convenience, security, privacy, etc.)?
• Have any interest groups, such as privacy advocates, publicly expressed concern with (or support for) the program?
• What is the general impression of the notion of a 'National ID' in the jurisdiction?
• Is there a clear mechanism for citizens to express their opinions regarding this program?

[17] It may be interesting to note, however, that Hung, Chang and Yu (2006) found that external influence is significant only in adopters of e-Government, and not non-adopters. This would seem to imply that opposition to IdMA projects does not tend to dissuade those who encounter it from utilizing the system.

In summary, this study is designed to determine factors that have led to either success or a lack thereof in various e-Government identity management systems. By this, we look to provide a framework by which British Columbia's options for identity management online can be measured, and the success of these various options can be postulated.

4: Case Study Analysis

This section summarizes the findings of the multi-case analysis. Each of the following sections begins with a matrix that briefly describes each case study in regards to the questions identified in the *Investigative Framework*; this is followed by a written summary of the findings of this research. Each section concludes with a discussion of any successful practices that can be identified from the previous subsections.

4.1 Usability

When deciding whether to try or adopt a new technology, one of the first calculations that individuals must make is between ease of use and functionality. Though the desired equilibrium point between those two factors will vary both across populations and across individuals within those populations, it is safe to believe that decreases in ease of use must be compensated for by increases in functionality, and vice versa, to maintain adoption rates. At the same time, governments understand that they will inevitably face a populous that will vary in technical competency, and as such 'ease of use' must be understood quite broadly. The questions in this section look to examine where the programs in the case studies stand in this usability / cost-benefit ratio.

Table 4-1 Usability Factor Analysis

	ePass – Canada	IVS – New Zealand	Citizen Card - Austria
Range of services?	- CRA myAccount - Passport Canada online application - Service Canada 'My Government' account - … among others	Intended to be 'all-of-government'; currently only 4 participating agencies listed[18]	Broad range of e-government services[19]
Available to non- e-Gov services?	No	Under consideration	Yes
Additional functionality beyond authentication / identification?	None.	None.	e-Signatures (Adobe .pdf documents & others)
Mandatory for e-Gov services?	Yes – non-ePass users are offered options of phone, fax, mail or in person.	No – current means of identification will remain available (identification is separate from authentication)	Yes.
Charge to user?	None.	Under consideration (none for basic authentication)	Costs vary: e.g. e-Card: free Other sources: ~25€ Card reader: ~20€
Technological requirements for user?	Some – configuration of web browser.	None.	Chip card reader; software download.

4.1.1 Analysis of Cases

There are two general factors that must be accounted for when examining the cost-side of the cost-benefit ratio of adopting a new technology: monetary cost, and ease-of-use (that is, 'psychological cost'). Financially, we find a range of charges for access to governmental Identity

[18] https://www1.logon.govt.nz/cls/static/participatingagencies.jsp
[19] Full listing of services only available in German.

Management systems. Where Canada's ePass is wholly free of charge to users, holders of the Austrian Citizen Card must acquire a card reader (if one is not integrated into their computer), as well as paying varying amounts for the card and stored certificates (and potentially a per-use charge for use of the stored certificates), depending on the identifier's source (government, cell phone provider, other secure card maker).

Ease-of-use of the identifiers is also highly varied. The token chosen for the New Zealand IVS is a prominent example of increasing security without sacrificing ease of use. The token is a Secured, as manufactured by RSA, and functions quite simply: displayed on the token is a 6-digit number, which is automatically updated every 60 seconds. When an individual is then asked for his or her username and password, he or she is also asked to enter the code found on his or her token; thus, even if a username/password combination is compromised, a malicious individual has a 1-in-1,000,000 chance of correctly guessing this code and accessing the account in question. At the same time, the burden on the legitimate account holder is limited to maintaining possession of the key-sized token.

The security measures utilized by the ePass and Citizen Card programs, on the other hand, require a measure of technical competence from users, however small. The Citizen Card program requires hardware that may or may not be incorporated into a user's computer – specifically, the card reader; an interaction environment must also be downloaded and installed on the user's computer to enable the card's functionality. Both of these factors, though not taxing to a number of individuals, will also serve to alienate some portion of the client base. Similarly, Canada's ePass program requires users to have cookies, Java, and JavaScript each enabled (with a reasonably up-to-date JVM package) within a supported web browser. It must be noted that the ePass program does provide detailed instructions regarding the proper setup of each of these features, for all supported browsers; however, there will still be users who are unwilling or unable to make the necessary changes (if required) – particularly if they are uncertain regarding the

benefits they will see from e-Government. Additionally, requiring specific browser settings for use of a web application is a notoriously 'buggy' process – as chronicled in one individual's record of his first ePass transaction ("Chris", 2006).

4.1.2 Aspects of Successful Deployment

It goes almost without saying that to the greatest extent possible, an Identity Management system should be whole-of-government, and as such offer the broadest possible range of services. However, these services should be offered in the spirit of simplification; if a service is currently available online (eg. government information and publications) without the use of an identifier, bringing the service under the umbrella of the IdMA would impose a cost on the user, without an associated benefit.

Similarly, if at all possible existing means of interaction should not be sacrificed for e-Government. Differences in technical ability and trust in government also imply that BC will not achieve 100% usage of e-Government services. The case of the Austrian Citizen Card also serves as a warning against assuming a technological determinist stance (i.e. if the system is made available, and users own access cards, then the system will be used). By all estimates, there are far more access cards and other viable access devices in Austria than citizens; however, less than 10% of the population has actually *activated* a Citizen Card – that is to say, availability does not equal use in that case. As such, British Columbia should strive to make its Identity Management system optional – certainly for access government services as a whole, and if possible for access to e-Government services as well. This has the additional benefit of creating a feedback mechanism by which the success of the IdMA system can be measured; if individuals choose to use a optional service, one can infer that a benefit is being obtained from that service.

The final practice that can be drawn from these cases is that technical requirements for the user should be minimized to the extent possible, without sacrificing security or privacy; New

Zealand's log-on token is a prime example of a highly secure interface that imposes virtually no mental cost on the user. However, where technical requirements are unavoidable, clear, step-by-step instructions must be made available (as is the case with Canada's ePass).

4.2 Trust

Another primary factor in technological adoption choices, which is frequently cited in the literature on e-Government, is trust. Repeating the definition of trust that was adopted earlier, (Warkentin et al., 2002) states that trust is "the belief that the other party will behave as expected in a socially responsible manner, and in doing so, it will fulfil the trusting party's expectation." The following set of questions has to do with the two sides of this equation: how will the IdMA selected affect the user's expectations, and how can an IdMA assure that user that his or her expectations will be met?

Table 4-2 Trust Factor Analysis

	ePass – Canada	**IVS – New Zealand**	**Citizen Card – Austria**
Transferable existing identifier?	No	No	No
Key or identifier?	Key	Identifier	Both
Authentication factors used?	Knowledge (username / password)	Knowledge (username / password) + possession of physical token	Knowledge (PIN) + possession of physical token
Perceptible security and privacy features?	- If multiple ePasses used, neither service providers nor issuing agency can correlate actions - ePass can be revoked by used in case if necessary - Issuing agency does not store personal information	- RSA securID token - Explicit query before identity information transmitted - Only 'core' identity information stored - Service providers cannot correlate users - Issuing agency knows departments accessed, but not services requested or entitlements - Ongoing privacy assessments are made public	- Different PIN for secure & standard e-Signatures - sourcePIN (i.e. identification number) cannot be stored / used by any agency (only derived numbers) - No linkages possible across service providers - Only 'core' identity information stored

4.2.1 Analysis of Cases

The level of trust that must be generated for a system to be adopted is directly related to the consequences of a failure or compromise of that system; here, our cases differ significantly. Identity management systems can provide one of two assets: a 'key' to access services, an identifier, or both. A compromised key allows the possibility of illicit service access; a compromised identifier allows the possibility of impersonation. Arguably the most dangerous case, however, is when these two factors are combined – here, compromise would allow a

malicious actor to access services while being able to 'prove' identity, as such bypassing most likely security measures. Canada's ePass does not provide a true identifier – users are provided only a digital 'key', which is associated with a service account after the confirmation of a 'shared secret', or other means of identification. New Zealand - with its Government Online and Identity Verification Services – has provided both functions but kept them separate, thus limiting vulnerabilities. With access to an Austrian citizen card (and his/her PIN number), however, both the sPIN identifier and stored certificates can be accessed, allowing for a large degree of impersonation. This service must thus provide an associated large level of trust.

Trust comes from sources that can be both clearly apparent to users, or more subtle system factors. On the 'apparent' side are factors such as immediate, user-controlled security measures and authentication factors. All of the instances studied used a password system for access and a shared-secrets method of initial authentication, demonstrating the first factor: 'something you know.' 'Something you have' was also used in two of the three cases (New Zealand and Austria). Canada's ePass program could also make an argument for using two-factor authentication; however, as the 'token' is not physically instantiated and exists only digitally, it is more appropriately in the category of 'something you know' category. None of the IdMs utilized (and generally expressed a lack of interest in) biometrics, the third part of 3-factor authentication.

Other factors leading to trust have to do with trust in the system itself. None of the cases had the possibility of migrating an existing identification scheme online; as such, trust gained through experience with a program did not exist. The primary system factor that was, however, stressed across cases had to do with the prevention of possible privacy breaches by malicious agents, even if they are internal to the agencies and conspiring, as each case describes the way by which correlation across agencies is prevented (or at least is not aided) by the identity system. Further, if the compromise of an identifier is suspected, each agency's process for revoking the credential is made clear.

A different, and interesting, means of generating non-immediate trust can be found in the Austrian privacy law. In the Citizen Card program, a national identifier is created, and assigned to every citizen in the country – which would, if left unaddressed, create a strong potential for the 'tracking' of citizens. Austrian law, however, forbids the use of a single identifier across different sectors or domains (Hollosi, n/d); thus, a cryptographically-secure derivation of the sourcePIN (Personal Identification Number), called an ssPIN (sector-specific PIN), is generated for each application used by an individual. From a single identifier (which is useful for systems designers), legal protections create a series of unlinkable numbers, theoretically raising the trust level for citizen-users of the system.

4.2.2 Aspects of Successful Deployment

The best practices with regard to trust primarily focus on security measures. As with our cases, British Columbia does not have a familiar identifier that could effectively be transformed into an e-Government access mechanism. There is also no 'best practice', *per se*, regarding the scale of an IdMA project; instead, there is instead an understanding that the development of trust in a large system requires higher levels of security protections than would be the case for a more moderate system.

There are two ways in which privacy and security measures can be provided to users: as mandatory elements of system usage, or as optional protections that can be applied by the user when he or she desires. The ramifications of the philosophy chosen should be understood: a system that functions in an unalterable, secure manner may speak to novice users, but leave others feeling disempowered. On the other hand, a system that offers a great deal of choice offers a sense of control (a precursor of trust) to the user, but this control may 1) not be universally desired, and 2) lead to privacy or security breaches due to error, manipulation, or even malicious intent. The security of transactions becomes easier to ensure as more elements of these transactions remain in the control of the service provider. As such, the best practice here

identified is to recognize the level of control being offered users and the resulting trade-offs that must be made by system designers.

4.3 Perception

The final factor that we examine with regards to the adoption of Identity Management systems is public opinion, or perception. Various parties have the opportunity to influence this factor, either positively or negatively: developers, the agency managing the IdMA system, service providers, critics, users, etc. The questions in this section seek to examine the public reactions of these parties to the various forms of Identity Management employed in our case studies, as well as examining the general perception of identifiers within the respective regions.

Table 4-3 Perception Factor Analysis

	ePass – Canada	IVS – New Zealand	Citizen Card - Austria
Government promotional factors?[20]	- Enhanced security	- Not compulsory / not national ID - Protective of privacy - Lessened risk of security breach - Convenience - Benefits to e-Government service providers	- Convenience - Faster processing times - Non-linkability - Security
Advocate response?	- Primary concern was data matching; address with allowance of multiple ePasses	- State need for caution; alternatives should remain, non-linkability should be retained	- General positive recognition for data protection
Response to national ID?	- Boa et al. (2007) finds ~53% of Canadians support national ID that must be carried - However, strong anti-National-ID sentiment amongst advocacy groups	- Plan for 'Kiwi Card' was vehemently opposed and subsequently abandoned	- No major anti-ID movements (though, no serious discussion of introduction, either) - Austrian privacy law effectively prohibit national-ID
Forum for users?	None identified.	Public consultation	Online forum[21]

4.3.1 Analysis of Cases

[20] Primary sources are, respectively, Canada: Government of Canada (2008); New Zealand: DIA NZ(2008), Government of NZ (2009); Austria: A-SIT(n/d)

[21] Available at: http://www.buergerkarte.at/forum

There were significant differences in the governmental promotion of IdMA systems. Canada's ePass is promoted principally on functionality. Privacy goes virtually unmentioned, short of statements to the effect that all data collected is protected by the *Privacy Act*. Instead, the ePass materials focus almost entirely on the security of communications afforded by the system. The IdMA systems deployed in Austria and New Zealand, on the other hand, describe a broad range of system benefits, including their privacy-protective design, the convenience and time savings available to users, and the enhanced security of the system. New Zealand also made clear that users could expect extended e-Government offerings after the introduction of the IVS system, as service providers would see benefit as well.

In each case analyzed, there was nervousness amongst privacy advocates about the possibility of the creation of a National ID within the respective regions that had to be overcome by system designers. As there was very little public outcry regarding this possibility, however, it can safely be assumed that system design combined with the public descriptions of the systems worked to overcome this problem. Each system addressed the possibility of correlation of service usage, both in design and promotion; as well, New Zealand made it explicitly clear that they were not looking to creation a system of national identification.

Finally, only the New Zealand case had a clear public forum for response to the development of an IdMA system, which was in the form of a public consultation which looked to identify likelihood for usage of the system, desired features, trust in privacy and security, and so forth. However, following the conclusion of this consultation in Dec. 2007, there was no clear forum for public opinion on the IVS.

4.3.2 Aspects of Successful Deployment

The first best practice that arises from the above analysis is that primary branding for an IdMA system should come from the agency in charge or its deployment. This can be

accomplished by a combination of factors, including the consultation of potentially adversarial groups within, or prior to, the design process, and/or with the creation of a significant promotional presence for the IdMA system. By way of example, Canada's ePass was adjusted due to concerns about the correlation of data, New Zealand's IVS was preceded by a thorough public consultation process, and Austria's Citizen Card has a significant promotional web presence.

As one of the primary means of controlling the perception, any agency responsible for an IdMA system must be aware of the general reaction to identifiers; the New Zealand case, for instance, is strongly focussed on, and directly state, the fact that the IVS and its Government Logon System do not constitute a National ID program, knowing that other similar identifiers have failed when such a connection was made.

Finally, with regards to privacy, the BC Executive Director for Cross-Government IM/IT initiatives has noted that some advocates seem to misunderstand privacy, denying the possibility of privacy-protective technological advance (Watkins, 2007). There is little that a government looking to create an IdMA system can do to please this group. There are groups, however, that are equally committed to the privacy 'cause', but who are willing to work with technologists to achieve the needs of both groups. The Ontario Information and Privacy Commissioner (IPC)'s Office[22], for instance, advocates privacy-by-design and the "positive-sum paradigm" (Kavoukian, 2008), by which system designers work with privacy advocates to identify potential privacy risks and address them in the design phase, rather than by post-production modifications (that may reduce functionality). It is the analysis of the work of these groups that will be most beneficial to this analysis, as it is based on calculation, rather than a blind ideology.

[22] The work of the Ontario office, rather than the British Columbian office, is described as the former has a policy department, which the latter office lacks entirely (being budgeted only to respond to complaints).

During a conversation between the Senior Technology Analyst at the IPC and I, four "lines in the sand" were identified – features of an IdMA system that are considered necessary (though not sufficient) to achieve support for the system within the privacy community. These factors are as follows:

1. **Risk of mis-authentication**: How can it be prevented? Who is responsible if it occurs?
2. **Over-authentication:** The presence of an IdMA system should not change the ability to interact anonymously; the strength of authentication should be commensurate with the application.
3. **Correlation:** The possibility of central monitoring or agency-side correlation of service usage should not be increased by the IdMA system.
4. **Outsourcing:** If development of the IdMA system is outsourced, risks must be understood and responsibilities assigned. (Carter, personal communication, 2008)

The first and third factors were identified as the most important to privacy protection. As such, it will be stated that the addressing of these questions is a best practice. It should be noted that the third factor is address by all of our case studies; little mention can be found, however, of any of the others. British Columbia would be wise to change this.

5: Analysis of Alternatives

5.1 Issue Definition and Policy Objectives

The case study analysis presented above has described some of the challenges associated with online authentication of individuals for the purposes of e-Government access. As British Columbia has been making a clear movement towards e-Government, the province is faced with a choice between a number of options for identity management, the merits of which must be identified and compared. Here, we present the key potential solutions for IdMA in the province, using the following as foundational elements of the analysis:

1. **To best implement e-Government structures, the BC government requires a strong system of access control.**
2. **In the course of achieving objective 1, the BC government has the opportunity to examine the notion of a non-physical identity document.**

The alternatives to achieve this are generated from the online identification and access methods currently available for, and used in, e-Government systems, taking into account the limitations of the British Columbian situation. These limitations include technical factors (the installation of various biometric scanners on home computers cannot be expected, for instance) along with cultural ones (a system cannot necessitate *all* citizens to be adopters – even e-Banking, a leader in online authentication systems, has only managed 50% penetration by 2008 (CBA, 2008)). Citizens and service providers alike will also expect a high level of security, combined with some level of familiarity and ease-of-comprehension. With this is mind, the following three identity management schemes are presented for consideration by the BC CIO:

1. Create an e-Government 'Key'
2. Create an online identifier
3. Enter into an Identity Federation

The details of these alternatives are presented below. In section 6, each alternative will be evaluated against the goals of the BC CIO's office in creating and identity management system.

5.2 Alternatives

5.2.1 Status Quo

The status quo, in the scenario, would be to not develop a comprehensive identity management scheme. Should this option be selected, each e-Government service provider would have to create its own access-control mechanism, which would in all likelihood involve a series of site-specific username and password combinations. The transaction security protections available to these providers would likely be lessened, as the mechanisms that an individual organization would consider financially feasible could not compare to those available to a whole-of-government system. The executive director of the BC IM/IT program has stated that this is a "mess that the government [does] not want to experience." (Watkins, 2007)

5.2.1.1 Key Issues

- A multitude of username/password combinations decreases security practices; individuals generally cannot internally store unique (and changing) passwords for each site they visit, so memory aides are used, including password re-use and/or the storing of passwords in either paper or digital form, each of which creates security vulnerabilities.
- Transaction security measures would be limited, and likely involve only SSL (Secure Sockets Layer), similar to most e-Commerce sites.
- Individuals are not motivated to expand their use of e-Government services; the initial process of establishing credentials is a time cost to users, and the status quo would impose this cost for each service the individual wishes to access.
- Paradoxically, it is likely that although negative experiences with a single service provider may reduce trust across e-Government systems, positive experiences will raise trust *only* with that provider.

- Multiple systems imply multiple potential points of failure, which is critical when combined with the above point.

5.2.2 Alternative 1 – Create an e-Government 'Key'

The first reasonable alternative available for governmental consideration involves a system similar to Canada's ePass, which would create a 'key' for accessing e-Government services. This option would not look to identify individuals (initial authentication) to service providers; that function would be left to the discretion of the provider itself. Instead, the focus is on ongoing authentication, as the user returns across multiple visits.

5.2.2.1 Key Points

- Minimal possible identifier.
- Fits one goal (authentication) in the most direct manner, while ignoring the second (identification); individuals must still provide proof of identity to each service for which access is desired.
- Access to the 'key' likely granted after a proof-of-identity transaction with a service provider.
- Potential for significant cost savings if this program were implemented in conjunction with Canada's ePass
- Keeping with the analogy of the key, should it be acquired by a malicious individual, all that person can do is gain access (or 'open the door') to an online space in control of a government agency, thus affording that agency opportunities for further security measures (confirmation e-mails prior to access or changes to of sensitive data, for example).
- It would be difficult (and likely ill-advised) to extend this identifier's range of uses, should that be desired in the future.

5.2.3 Alternative 2 – Create an online identifier

A second model that could be followed in the creation of an IdMA system is that of the Driver's License (DL). While maintaining the same indexing power of a SIN-type identifier (through the Driver's License number), the DL serves as many individuals' primary means of

identification, as well a one of the most widely accepted proofs of ID. Thus, the card is used not just to provide access to a record, but also to aid in the establishment of records. An online identifier could serve both of these purposes, or just the latter, as want dictates.

Current implementations of an identifier of this type, such as New Zealand's IVS and Austria's Citizen Card, contain only basic information about an individual (name, date of birth, place of birth, etc.). This could, however, be extended (or contracted) to whatever breadth of data is deemed appropriate. Similarly, presentation of this data does not have to be an all-or-nothing proposition; it is possible (again, as is the case in New Zealand) for the user to select what subset of data is transmitted to an agency, or for agencies themselves to dictate what data they will need for a transaction and accept only that. Such a 'claims-based' identity approach (a subset of the general online identifier), which is highly favoured at present by the agency in charge of the BC*e*ID*ng*, can be managed either on the user's computer or on a central server. The controlling software for such a system would likely be made highly customizable, allowing users a range of alternatives from granular control to 'trust in the government', which would permit a blanket release of whatever information is being requested by each agency without further user approval. It should also be made clear that this identifier would contain indices to individual records, not the records themselves – for example, a person's health care number, not their patient information.

The most likely means of populating such an identifier would involve an initial (likely in-person) establishment of core identity information, sufficient to uniquely identify an individual within a region in question. Optionally at this point, other e-Government service agencies that authenticate an individual based on this core information could issue supplemental attributes to be incorporated into the initial identifier. Such a multiply-populated identifier would allow for a more natural assignation of responsibility for identity attributes: for instance, health agencies

would be responsible for the certification of a health care number, should it be required by other service providers.

The creation of an identifier, as opposed to an access key, also allows for expanded usage possibilities, as a government-certified online ID would be welcomed by many e-Applications beyond e-Government – in particular, banking and commerce.

5.2.3.1 Key Points

- The IdMA system could easily be restricted only for e-Government purposes or extended for private sector use.
- Individuals identify themselves once initially, and (for as long as the integrity of the identifier is accepted) need only further prove identity in the case that attributes not yet established within the identifier are required by a service.
- The identifier must have strong protections – ideally, at least 2-factor – against identity theft. In Alternative 1, breaches can be traced; assuming the service provider keeps a log of transactions, an individual can determine exactly what actions a malicious actor has taken, etc. With an identifier, however, it will be much more difficult to determine what (if anything) needs to be done to rectify a situation; victims of identity theft often only become aware of the thief's actions after they are confronted with the consequences of those actions (i.e. an unrecognized bank loan coming due).
- If a claims-based identifier is used, further enhancements to security may be required due to the collection of multiple pieces of data in a single location.
- Broad range of user control options available, depending on implementation; can also be variable within a particular implementation.
- Potential precedent of Alternative 3.

5.2.4 Alternative 3 – Enter into an Identity Federation

A third, potentially less likely scenario would see the BC government enter into a system of Federated Identity with a group of trusted partners. In such a federation, identifiers and credentials issued by one federation member are accepted by others, allowing users to be authenticated by the member-organization with which they have established a prior trust

relationship. Thus, the role of the service provider in authentication becomes the verification of presented credentials, a much easier task than the verification of an individual's identity.

Alternative 2 is what could be termed a 'one-way' federation, in that the government would issue an identifier that was broadly recognized, but not recognize any identifiers supplied by other federation 'members'. This alternative would extend such a model to be 'two-way', in which the government would authenticate and trust a selected set of outside credentials. Austria, for example, has looked to achieve nearly such a model, in its integration of Belgian, Estonian, Finnish and Italian eIDs into the Citizen Card software (Leitold, 2006). Partners would not necessarily be limited to governments, however; theoretically, any organization (or even individual) that can demonstrate trustworthiness and authority to an acceptable degree could be accepted into the federation.

5.2.4.1 Key Points

- Pre-established relationships can be extended across Federation members, forming a 'circle-of-trust'
- To maintain trust, a Federated Privacy Impact Assessment (IPC, 2009) must be undertaken and adhered to by all participating organizations, and regular audits must be conducted.
- Extends the notion of identifiers being asserted by the appropriate agency, organization or individual, as well as the notion of claims-based identity. For instance, a foreign vital statistics agency might best know a person's date of birth; a bank is likely the entity best capable of asserting an individual's account number; an employer may (or may not) provide employment status.
- Can, or should, a government trust identifiers created by any agency other than itself and its foreign counterparts? Is the benefit of this option over, for instance, Alternative 2, worth the added security costs and potential risks?
- Could be a future extension of Alternative 2.

6: Evaluation

6.1 Criteria for Evaluating Alternative Outcomes

In order to measure the meeting of our policy objectives by each alternative, the development of a series of criteria is required which are separated into two areas: administrative and adoption (effectiveness). Table 6-1 summarizes the criteria that will be used to evaluate the potential alternatives described in the previous chapter.

Table 6-1 Criteria Definition and Measurement

Criteria	Definition	Measurement
Administrative Factors		
Acceptability	The extent to which the alternative meets the policies and principles adopted by the BC CIO's Office. That is, does the system 1) meet Pan-Canadian IdMA principles and 2) provide a user-centric experience?	Low / Moderate / High
Cost	The cost of implementing the alternative, relative to the other alternatives.	Capital costs of implementation (Low/Moderate/High, where $ figures not available)
Current Feasibility	The technical feasibility of the alternative, given current technology and identity contexts.	Low/Moderate/High
Adoption (Effectiveness) Factors		
Advocate Response	Likely response of privacy/security/civil rights advocates to the system.	Support / Neutral / Not Support

Criteria	Definition	Measurement
Familiarity	Expected user exposure to similar / equivalent systems.	Prominence of similar systems (Low / Moderate / High)
Necessarily Trusted Parties	Parties that must be trusted in order for trust in system to be fostered.	Number (and significance) of parties
Risks upon failure	The types of risk to which the system has a particular vulnerability. NOTE: These risks are worst case, and can be mitigated by various technical measures	Type of risk (service- or identity-based) / Traceability (low/high)
Technical Burden on User	The amount of technical ability that is likely needed to correctly utilize the IdMA system	Low/Moderate/High
Breadth of Services	The breadth of services likely to be made available through the given alternative, relative to the other alternatives.	Service types likely available (registered services, e-Government, and/or private services)

While these criteria may be quite general, they are meant to provide an overview of the general trade-offs associated with each alternative, from the point of view of the BC government. [Factors that are unchanging across alternatives (such as those associated with the state of British Columbian society in relation to identifiers) are not included in the analysis.] The outcomes are generated from best guesses, as it would be highly impractical to empirically test each alternative. A breakdown of the potential states for each criterion is given, in order to further explicate the predictive process in use.

The following subsection gives a detailed evaluation of the anticipated outcomes of each alternative, in relation to the criteria described above.

6.1.1 Projected Outcomes

Table 6-2 Projected Outcomes of Criteria Evaluation

Criteria	Status Quo	1) Key	2) Identifier	3) Federated Identity
Administrative Factors				
Acceptability	(-) Not client-centric (-) Violates IdMA principles[23]: 4b (Seamless consistent experience), 8a (Flexible and modular), 8c (Scalable), 8d (Reduction in administrative weight) (+) Enhances IdMA principles: None.	(-) Not client-centric (-) Violates IdMA principles: None. (+) Enhances IdMA principles: 6a (Trusted service), 6b (Secure environment)	(+) Client-centric (-) Violates IdMA principles: None. (+) Enhances IdMA principles: 2c (Client control), 3a (Least amount of identity information), 4a (Client-focused and responsive), 5a (Diversity of identity contexts),	(+) Client-centric (-) Violates IdMA principles: None. (+) Enhances IdMA principles: 2c (Client control), 3a (Least amount of identity information), 4a (Client-focused and responsive), 5a (Diversity of identity contexts), 5b (Diversity of identity systems), 6c (Accuracy and Integrity), 7b (Shared accountability)

[23] See Appendix 1.

Criteria	Status Quo	1) Key	2) Identifier	3) Federated Identity
Cost	(+/-) Low, but repeatedly borne by multiple agencies	(+/-) Potentially low if partnered with ePass; High if independently developed (ePass cost ~$476m)	(+) Potentially low (NZ's IVS was budgeted $9m) NOTE: This does not take into account the other costs associated with providing e-Government services (+) If claims-based software used, unlikely to be developed in house	(+) Low; as with 2), unlikely that system developed in house
Current Feasibility	(+) High: most common means of online identification	(+) High; ePass, for instance, has been in use since 2002	(+/-) High if centrally stored; Moderate if user-controlled claims-based software used	(-) Low: Technical requirement being introduced now, but not yet widespread; also, no clear existing Federation could be utilized
Adoption Factors				
Advocate Response	(+) No increased chance for correlation across services (-) Unnecessary data replication (-) Poor security practices (by users) likely	(+/-) No response, so long as correlation issues handled	(+) Expressions of support for claims-based identity (+/-) Caution re: possibility of correlation * Support increases correlative to level of user control of data	(+) Support for user-control of identity (+) Support for notion of federation (due to data minimization) (+/-) Caution re: commercial use of identifier

Criteria	Status Quo	1) Key	2) Identifier	3) Federated Identity
Familiarity	(+) High; standard means of online authentication	(+) Moderate/High: if well designed, indistinguishable from status quo	(+) Moderate/High: Unfamiliar online, but highly familiar offline equivalents	(-) Low; however, similar online systems are growing
Necessarily trusted parties	(-) Each agency's solution must be trusted individually	(+) Key provider	(+) Identifier provider, software developer if applicable	(+/-) Federation (as a whole ideally, as individual members otherwise), software developer
Risks upon failure	(+) Moderate, service-related, likely traceable; failure more likely due to multiple access points	(+) Moderate, service-related, likely traceable	(-) High, identity-related, likely untraceable	(-) High, identity-related, likely untraceable, likely broader than 2)
Technical Burden on User	(+/-) Low, but high knowledge burden	(+) Low, if well designed	(+) Low if centrally stored, Moderate if claims-based, client-side software	(+/-) Moderate for associated client-side software
Breadth of services	(-) e-Government services for which user has registered only	(-) e-Government services for which user has registered only	(+) full e-Government, possible private services	(+) full e-Government and private services

6.2 Summary of Criteria Evaluation

Below, a summary of the projected outcome as a result of the criteria analysis is provided. In the table, the description of the outcome relates to the measurement narrative found in table 6-1. Following this summary, an interpretation of the results for each alternative is provided.

Table 6-3 Summary of Criteria Evaluation

Criteria	Status Quo	1) Key	2) Identifier	3) Federated Identity
Administrative Factors				
Acceptability	Low	Moderate	High	Very High
Cost	Moderate	Broad range, but likely high	Low	Low
Current Feasibility	High	High	Moderate	Low
Adoption Factors				
Advocate Response	Not support	Neutral	Support	Cautious Support
Familiarity	High	High	Moderate/High	Low
Necessarily trusted parties	Many	Central	Central	Many (though potentially a single federation)
Risks upon failure	Low (but increased likelihood of failure)	Low	Moderate/High	High
Technical Burden on User	Low	Low	Moderate	Moderate
Breadth of services	Very Low	Low	Moderate-High	High

6.2.1 Status Quo

The status quo is the precise reason that the British Columbian government has expressed for pursuing an IdMA system for its e-Government offerings. Costly, prone to failure, and not client-centric, this approach is considered a "mess" by government decision-makers. It matters

little that the public fully understands this approach, having been exposed to it for much of its online experience; due to the isolated nature of the individual systems, this approach would likely preclude any possibility of the development of a holistic e-Government. Further, this approach does nothing to promote the IdMA principles adopted by the BC CIO, and in some places actually violates these principles. Given all of these factors, the status quo should be considered an untenable option moving forward.

6.2.2 Alternative #1: Key

From our analysis, it can be seen that the development of a key-style system would have numerous benefits in regards to encouraging user adoption of an e-Government system. It is accessible to users, can be branded to create a whole-of-government online experience, and needs only create trust with the central issuing party, as opposed to with each service provider, among other factors.

The system depends, however, on the availability of (and citizen need for) e-Government services, as there is effectively no other driver for adoption. Citizens will utilize the IdMA only insomuch as they utilize the services that require the 'key' for access. This factor can be seen in the adoption rates of Canada's ePass, which a CRA representative has suggested to me may have been less successful than anticipated due to the infrequency of interactions between citizens and the federal government (Quiney, personal communication, 2008). A 'key' system also does not eliminate the role of paper documents and shared secrets, as it speaks only to the re-identifying ones' self with a service provider, not with the initial identification. This identification can be quite tedious, depending on the shared secret required or the process involved; the Canada Revenue Agency, for instance, requires an individual to be mailed a security code, a process that they estimate takes five days. Similar processes will likely be required for each desired service. The key can thus be seen as not taking full advantage of the possibilities of electronic identification, effectively providing instead a security measure for traditional authentication.

6.2.3 Alternative #2: Identifier

Alternative 2, the creation of an online identifier, has many immediately identifiable benefits as well. It speaks to the IdMA principles that have been adopted by BC, is client-centric, and sees strong support from both the privacy and security communities. The costs of a system are also quite low; New Zealand, with a population base very comparable to British Columbia's, budgeted only $9M for development of their IVS.

The determining factor for user adoption of this alternative will likely be implementation. A technologically simple, familiar and highly secure centralized identifier, such as that created by New Zealand's IVS, should see high adoption rates. Individuals understand this paradigm; when proof of identity is needed, one accesses a secure container (akin to a wallet) to retrieve the necessary credential. These users might (or might not) be convinced that the most secure storage location is on a remote, centralized server, or the identifier might be allowed to reside on the user's machine. A claims-based identity system (the expressed preference of the BC CIO's office), on the other hand, may be slightly less familiar to users, who will be unaccustomed to having to navigate an 'identity agent' software program to select which claims to present (though this interface would, of course, be made as intuitive as possible). As such, education campaigns regarding safe and effective usage of the system would have to accompany its deployment. Further, depending on the system design, technical feasibility will also be affected, with the claims-based system having less current availability. Finally, due to the value of this identifier in case of compromise, users will have to be convinced of the secure nature of this system.

Ultimately, it is the benefits of client-centrism that make this alternative greatly appealing. For users, these benefits focus on consistency of experience and control of data and consistency of experience. The former factor is important in shifting an unaccustomed mode of interaction – the digital assertion of identity – into the realm of familiarity. Individuals understand the owning and presenting of an identity token, as it is a common occurrence in the

'offline' world. Online identifiers are (by design, not necessity) generally privacy enhancing as well, in two ways: first, an identity provider has no requirement know the ways in which the issued credential is being used, and second, individuals are offered a more informed choice about the proliferation of their data. Claims-based systems are particularly beneficial in this latter regard, as users are (in most designs) afforded a highly-customizable degree of control over both what information is transferred to what agency, as well as the times at which they have to make such choices. As such, users are offered an increased level of perceived control, a previously identified driver of adoption.

Thinking to future applications and expanding on benefits to government, the scalability of such a system is also significant. This feature comes from a design that does not require an identity provider to have any knowledge of a service provider for verification; instead, it is enough for both to have knowledge of the system structure. If Identity Provider A is able to authenticate an individual to Service Provider B, inherent in the system is the ability to extend to additional identity and service providers, without modification of the system's internal workings. Thus, all future development and expansion costs (excluding general capacity issues) are born by the agencies who wish to utilize the system – a significant financial advantage for the initial government operators. This system is also naturally amenable to a cross-jurisdictional design, and is scalable outside of government services (to e-Banking, for instance) or even to an Identity Federation (Alternative 3), should the desire arise.

Given current support for the creation of an online identifier from both government and advocate groups and the potential benefits to be had, it is likely that this will be the most profitable alternative.

6.2.4 Alternative #3: Federated Identity

The analysis of the Federated Identity alternative reveals a study in potential. On the one hand, such a system would be highly desirable: to the greatest extent of our alternatives, it inherently promotes the adopted IdMA principles, it is client-centric, it provides users with not just a wide range of uses but encourages Internet-wide usage, providing an adoption driver beyond the availability of e-Government services, and so forth. However, it looks to (currently) not be a feasible solution. The technical backing for the system, while in development, is not yet sufficiently tested (nor sufficiently widely distributed) to be immediately deployable on such a massive scale, and the concept is potentially not yet accessible to individuals for whom self-selection of online identity claims may feel overwhelming. If an IdMA solution is required in the near future (as seems to be the case), the notion of Federated Identity may have to be slowly introduced as an iteration of Alternative 2, the general online identifier, if at all.

6.3 Recommendations

The summaries given above describe the general outcomes that might be expected upon adoption of any of the listed alternatives. In the next section, we look at next steps, providing a number of recommendations to the Province which the analysis above would suggest should lead to a more beneficial overall experience with IdMA development.

6.3.1 Recommendation #1: Select, and Actively Promote, a Secure and Intuitive Claims-Based Identifier

The notion of a claims-based identifier, in which individuals are given the ability to select which of a series of certified attributes will be transmitted in response to an identity request, has many benefits (as described above). Primary among these are user empowerment coming from identity control, support from advocacy organizations, relatively low cost, and the cross-

jurisdictional appeal of such a system. Thus, our first recommendation to the Province is to continue work into the development of such a claims-based system, with the following cautions:

• **The system must be highly secure.** The risks associated with a compromised online identity are very high (identity theft, in particular), and must be mitigated. Claims should be encrypted in such a way as to render them for one-time use only, and to reveal no information if intercepted. Users should be aware of this security.

• **The system must be intuitive, and not burdensome.** In order to encourage usage of the system, the user interface must be very clear, and accessible to all individuals in the province to the greatest degree possible. The system should be made available freely, and if possible as a secure download from the issuing agency website. The system should also be customizable to an extent, so that frequent (or advanced) users can set preferences which free them from constant choice; however, that choice and control should always remain available if desired.

• **The system must be promoted.** Finally, any claims-based identity system should be highly publicized by the issuing agency (likely the BC CIO). The benefits to users of such a system may not be clear; thus, Internet materials describing the reasons for the card, benefits to users, instructions, etc. should be developed and promoted. The Austrian Citizen Card website <http://www.buergerkarte.at/en/> might serve as an excellent example of this crossover between promotional and explanatory materials.

• **The support of advocate agencies will be conditional.** Claims-based identifiers, while conceptually supported, are not backed without reservation. Advocate agencies will look primary at the level of user control of data enabled by such a system; thus, a clear explanation of the chosen level of control (number of attributes stored, location of storage, etc.) and the reasoning behind such choices must be provided. Ideally, advocate agencies will have been involved throughout the design process.

6.3.2 Recommendation #2: Use an Open Standard

Our analysis also reveals one of the primary barriers to the selection of Alternative 2 (as instantiated by a claims-based identity system) and Alternative 3 (an Identity Federation): the lack of current public exposure to, and development of, such systems. As these failings may both be corrected with the passing of time, it would be ideal if a claims-based identifier could be incorporated into a future Identity Federation, when the benefits of such a system could be more fully realised. So-called 'open' standards for identity allow for this possibility.

Within a decade (at most), it is likely that groups such as the Information Card Foundation (http://informationcard.net) and the Liberty Alliance (http://www.projectliberty.org) will have made significant strides towards in online identity systems, significantly increasing the likelihood of the development of and public exposure to such systems. Open, non-proprietary standards for identity systems are favoured by both of these groups, in order to both spread the use of such systems, and protect against the security hazards inherent in a single developer being in control of an entire identity system. Open standards also allow for significant flexibility in design, effectively allowing a system to grow with the technology behind it. These standards additionally speak to principle the technological neutrality cited in the government's adopted IdMA requirements.

The recommendation here made is that the BC CIO's office strongly consider the use of these 'open standards', in order to afford both the immediate implementability of an online identifier and the (future) benefits of an Identity Federation. While the additional benefits to be seen with a federated, claims-based identity system may not be sufficient to pause the development of a the British Columbian IdMA system until technical feasibility is reached, they are significant enough to warrant a system design that can take advantage of these benefits as they become available.

6.3.3 Recommendation #3: Look Beyond Current Necessity

From ENIAC to the Internet, governments have always played a significant role in the development of computing technology. Given their current position, British Columbia may be in a prime position to look to the future of e-Government and the Internet, and begin to develop the next generation of online identification and authentication. Governments generally are in a good position to roll out new technologies: they have a large, diverse and widely distributed internal user base for initial testing, a potential user base of millions from amongst which supportive external beta testers can be drawn, a coercive ability once the fully developed and tested technology is finally deployed, and the ability to endure short-term financial loss in such a deployment for long-term gain. This development cycle is precisely what is needed for the expansion of online identity.

The third recommendation for the Province, then, is to be willing to advance the state-of-the-art when it comes to online identity, and to not get trapped in a 'comfortable' technology simply due to its availability. The BC CIO's office should undertake a detailed study of the potential benefits to the Province (including to BC & Canadian banks, online retailers, and citizens) of a government-issued online identifier, and if these benefits are sufficient, should examine the ways in which BC can be a leader in the field. Carter and Belanger (2006) have suggested that perceived innovation may be a significant influencing factor on e-Government adoption; thus, in addition to the intangible benefits of being perceived as a technological leader, the province, by looking to future potential, may also solve the immediate issue of system adoption.

This is not to say, of course, that the British Columbian government should approach IdMA carelessly. Significant planning would need to be put into any potential advance; multiple iterations of pilot studies and iterations are necessary to ensure that rapid failure (even on a small scale) does not doom the project post-deployment. This would not be a new concept within the

BC government; the Enhanced Driver's License was, for instance, initially piloted with only 500 volunteers, and only then after much pre-deployment planning and negotiating. Movement to the online world is the next identity frontier, and British Columbia (along with all Canadian provinces, and Canada as a nation) have the opportunity to be among the first explorers.

7: Conclusion

Identity management for e-Government is a difficult task. Other technology providers, such as credit card companies, have the ability to recognize that sophisticated protections will not be acceptable to consumers, and incorporate certain expected levels of fraud into their business plan. This luxury is not available to government. It is in the rather singular position of facing virtually no competition, as no other group can provide government services, and these services (if essential or mandatory) can only be avoided through non-compliance or emigration. This lack of options, however, causes concerns over non-use or non-compliance; if citizens don't like a service, they will likely do their best to avoid its use. Further, once this avoidance has started, it is difficult to stop. A system, such as Identity Management or e-Government, must, to the greatest possible extent, avoid problems such as malicious use, fraudulent access, and even simple frustration, lest they be abandoned before a benefit can be seen. It is for this reason that all significant design considerations must be undertaken long before system launch.

Success of an IdMA system does not rest entirely on the factors described in this study, of course. Here, the focus was on features that could differentiate systems; there are, though, other issues that will arise regardless of system design. There are many privacy issues with authentication that must be addressed regardless of the system, for instance, including the potential for over-authentication, the assignment of risk and responsibility in case of miss-authentication, and so forth. Such general system factors cannot be forgotten when communicating to the public about a new system.

Communication, both internal and external, will be key to the success of any IdMA program that may be developed. Externally, promotion of the system will be an important factor to adoption (as previously described). However, for this promotion to be effective multiple

parties (including service providers) must be involved – and thus kept informed regarding the system's purpose and status. Depending on implementation, an IdMA system will have little appeal on its own; it will be adopted only for its use value. If the usage context is focussed on e-Government, then service providers in that realm *must* be aware of the status and value of the system, in order to join in the promotion effort.[24]

7.1 Next Steps

With regards to next steps, British Columbia has been making some efforts to subtly move towards a system of Federated Identity (even if this trend is not acknowledged – arguably misunderstanding the notion of Federation, considering it necessarily distinct from user-centric identity systems). The key aspect of Federated Identity Management is the provision of credentials that are recognized by multiple service providers within a 'circle of trust.' This notion is the foundation of the Pan-Canadian Identity Management Framework, described previously: no single jurisdiction in Canada will be able to issue a Pan-Canadian identifier, thus requiring the creation of single-jurisdiction (i.e., provincial) identifiers than are recognized by all other jurisdictions. Similarly, a pilot project between BC*e*ID and the Canada Revenue Agency looks to make a CRA-authenticated ePass transferrable to a BC*e*ID, saving individuals the hassle of registering for the latter credential in person. Once again, we see a situation in which a single identifier (the ePass) is used across multiple, independent domains. The benefits of Federation are, then, being explored; this is an encouraging factor toward the adoption of the recommendations given above.

Ultimately, British Columbia seems to be on a beneficial path towards online Identity Management. The province is undertaking significant consultation processes with regards to the state-of-the-art, and is recognizing the benefits of an inter-jurisdictional approach to this issue.

[24] By way of comparison, as of this writing the first two results of Google search for 'Canada ePass' are 'About ePass' pages from Revenue Canada and Passport Canada respectively.

Some study of public impressions of, and desires for, both Internet identity and e-Government might be warranted, but at this stage, it is felt that BC should continue its progress and look to emerge a Canadian and world-leader in the field of identity.

Appendix

Appendix 1: Identity Management and Authentication (IdMA) Principles

(Adapted from I-J IdMA Task Force, 2007)

Principle 1: Justifiable and Proportionate

a) ***Authorized Use of Identity Information****:* The use of a client's identity information by any jurisdiction, department, program or service should be authorized by legislation, policy, or program requirements. Outside these specific circumstances, any other use of identity information is justified only with the client's explicit and informed consent or where there are specific legal reasons for doing so (e.g., lawful investigative purposes).

b) ***Identify for a specific reason***: There must be a specific reason for the collection, use, retention and disclosure of a client's identity information. Similar to the "need to know" rule, even if all of the necessary authorities exist, there must be a clear need to collect, use or disclose identity information about a client.

c) ***Risk-based approach:*** The identity management and authentication process should be based on a risk-based approach, balancing all relevant considerations, including privacy and security issues. The risk assessment should consider both the external and internal threats that could pose security and privacy risks relating to identity and other sensitive information involved in a transaction.

d) ***Proportional and appropriate means:*** The identity management and authentication process should be proportionate to the assessed risk and proportional to the stated goals of the program or service. Wherever possible and appropriate, the service should use the least intrusive method for identification and authentication, avoid over-engineering and avoid using over qualified identifiers and authentication methods.

e) ***Cost-effective:*** The identity management and authentication process selected and used should clearly demonstrate the benefits over costs for clients and governmental organizations while preserving privacy, security, program integrity and other rules.

Principle 2: Client Choice, Consent and Control

a) ***Choice of channels:*** Clients should have the option of authenticating their identity and carrying out transactions through different service delivery channels (e.g., over the counter, online, by telephone) without being disadvantaged by doing so. This is particularly the case with online transactions. Not all clients are comfortable using this channel and should not be required to do so. However, if a client opts to use a specific channel, the client will be expected to consent to the applicable identity management and authentication process for that channel in order to ensure a valid and secure transaction.

b) ***Informed Consent:*** Regardless of the channel selected, the identity management and authentication process should only collect, use and disclose a client's identity information

with the client's knowledge and consent, subject to specific legislative authority in each jurisdiction. Client consent should be informed and uncoerced, and, where appropriate, the client should be able to revoke consent at a later date.

c) ***Client control:*** The identity management and authentication process should empower clients by allowing them to control, to the extent possible, their own identity credentials and the transfer of their own identity information between identity providers and service providers.

Principle 3: Limited Information for a Limited Use

a) ***Least amount of identity information***: In order to mitigate the risk of a potential breach, the identity management and authentication process should collect, use, retain and disclose the least amount of identity information possible, on a "need to know" basis.

b) ***Limit use to specified purpose:*** Once a client's identity information is collected for a specific reason (see principle 1b), any future use of that information should be confined to that purpose, unless the client consents to a new use (see principle 2b).

There are, of course, exceptions to this principle (e.g., identity information may be used or disclosed without client consent for law enforcement purposes – including to investigate identity fraud – and where required or authorized by law) but generally speaking the use of a client's identity information should be limited to the original reason for collecting it.

c) ***Limit access to justifiable parties:*** The identity management and authentication process should be designed so that access to, and disclosure of, identity information is limited to parties that have a necessary and justifiable place in the service delivery transaction.

Principle 4: Client-focused, Consistent Experience

a) ***Client-focused and Responsive to Individual Needs***: Clients should figure prominently in any identity management and authentication process and be integrated and empowered through intuitive processes that respect and address client needs and capacity. Any technology used to support the process should be intuitive and convenient with clear interfaces adaptable to the client environment, particularly for those clients with different cultural and linguistic backgrounds or motor, sensory or cognitive limitations.

b) ***Seamless, consistent experience across identity contexts, channels and jurisdictions:*** The identity management and authentication process should provide clients with a simple, consistent experience across programs and jurisdictions for services requiring a similar level of assurance while, at the same time, enabling separation of a client's different identity contexts (e.g. citizen, employee, business). As well, the methods used over different channels should be based on similar requirements, except where the unique nature of the transaction or channel used significantly changes the level of risk.

c) ***Clear Communications***: Clients need to understand the identity management and authentication process and the directions they receive in order to exercise control over their information and credentials and to maximize accessibility to services. Plain language in all communications used to interface with clients is key to this understanding. In addition, clients should be provided with sufficient information to guide their use of the service and to make informed decisions.

Principle 5: Diversity of Identity Contexts and Systems (i.e. Operators and Technologies)

a) ***Diversity of identity contexts:*** The identity management and authentication process should recognize, preserve and promote the diversity of identity contexts in which individuals simultaneously operate (e.g., citizen, employee, business) both within a jurisdiction and across jurisdictions.

b) ***Diversity of identity systems:*** The identity management and authentication process should utilize and enable the interoperation of multiple identity systems run by multiple identity providers. This provides clients with choice over the means of identification across different identity contexts and allows them to use different credentials for different services, should they choose so.

Principle 6: Trusted and Secure Environment

a) ***Trusted service:*** Just as government needs a way to authenticate the identity of clients accessing their services, clients also need a mechanism for confirming the authenticity of service providers. This is particularly the case, when clients are accessing services remotely (e.g., online or over the telephone) and need to assure themselves that they are accessing the right website or speaking to an authorized representative of the service provider.

   Clients should be made aware of the party or parties with whom they are interacting and sharing identity information and be provided with sufficient information with which to make informed decisions about whether to engage in a particular transaction. This makes the process predictable and transparent which will enhance public trust in multi-channel, multi-jurisdictional service delivery.

b) ***Secure Environment:*** Client identity information must be managed in a safe and secure manner. Sound security practices and technology should be utilized across programs and jurisdictions to support the secure delivery of multi-channel services, identity management and authentication processes and to protect both client and government information. Auditing processes should also be in place to allow for rapid determination of the impact of potential breaches of data.

c) ***Accuracy and Integrity:*** Government agencies should take every reasonable step to ensure the accuracy of the information they use, or rely upon, in a transaction (and the integrity of the process used to obtain the information), in order to prevent unwanted outcomes. In addition, trust arrangements should be established between relevant parties to provide satisfactory assurance across services and jurisdictions that communicated identity information is accurate and has been obtained through reliable processes. Such arrangements will contribute to the establishment of circles of trust within which identity information can be relied upon with confidence.

Principle 7: Transparency and Accountability

a) ***Transparency***: Activities and decisions relating to the identity management and authentication process should be open, transparent and understandable to all parties (e.g., clients, authoritative parties, relying parties). This should include a mechanism for clients to request, subject to applicable law and exceptions, access to their identity-related

information held by an organization and knowledge of which parties have had access to that information and why.

b) ***Shared Accountability and Responsibility***: All parties (e.g., clients, authoritative parties, relying parties) involved in an identity management and authentication process should be accountable and responsible for their actions, acknowledging identity management as a collective responsibility. Clients should have a clear understanding of their role and responsibilities, and have enough information to ensure that they are aware of the risks associated with using the identity management and authentication process.

   In addition, organizations involved in identity management and authentication processes should make available a dispute-handling process to respond appropriately to client concerns and to enable the efficient and effective resolution of disputes.

Principle 8: Enduring Solution

a) ***Flexible and Modular:*** The identity management and authentication process that is selected should be flexible and modular enough to accommodate technological and administrative changes, offering an extensible solution and increased return on investment.

b) ***Technologically neutral***: Identity management and authentication processes and methods should be technologically neutral (i.e., the expression of a standard must not presuppose a specific medium or technique).

c) ***Scalable***: The identity management and authentication process should be scalable. The addition of clients or any other party (jurisdictions, departments, service providers, etc.) should not affect the proper functioning of the process and the application of principles or rules.

d) ***Reduction in administrative weight and complexity***: The identity management and authentication process should not increase administrative weight and complexity over the long term. On the contrary, the process should simplify corresponding administrative processes in order to provide efficient service delivery.

Bibliography

Works Cited

Accenture. (2004). *eGovernment Leadership: High Performance, Maximum Value*. Retrieved March 12, 2009, from http://www.accenture.ca/content/en/insights/Egov%20Research%20final.pdf

A-SIT. (n/d). *The Austrian Citizen Card*. Retrieved from http://www.buergerkarte.at/en/index.html

BC CIO. (n/d). *Office of the Chief Information Officer – Mandate*. Ministry of Labour and Citizens Services. Retrieved March 12, 2009, from: http://www.cio.gov.bc.ca/governance/default.asp

BC CIO (n/d(a)). *Information Management / Information Technology (IM/IT) Plan - FAQs*. Ministry of Labour and citizens services. Retrieved March 12, 2009, from: http://www.cio.gov.bc.ca/imit/faq.asp

BC CIO (n/d(b)). *Information Management / Information Technology (IM/IT) Plan – Desired Outcomes*. Ministry of Labour and citizens services. Retrieved March 12, 2009, from: http://www.cio.gov.bc.ca/imit/outcomes.asp

BC CIO (n/d(b)). *Information Management / Information Technology (IM/IT) Plan – Desired Outcomes*. Ministry of Labour and citizens services. Retrieved March 12, 2009, from: http://www.cio.gov.bc.ca/imit/outcomes.asp

Boa, K. et al. (2007). *Can ID? Visions for Canada's Identity Policy (Working Draft)*. Information Policy Research Program, University of Toronto.

Canadian Banker's Association. (2008, Oct.). *Backgrounders on Banking Issues: Technology and Banking*. Accessed Jan. 12, 2009 from http://www.cba.ca/en/viewDocument.asp?fl=4&sl=111&tl=&docid=453&pg=1

Canadian ePolicy Resource Centre. (2008). *e-Policy Resources*. Government of Canada. Retrieved March 12, 2009, from: http://www.ceprc.ca/cgol_e.html

Carter, L. & Belanger, F. (2003). The Influence of Perceived Characteristics of Innovating on e-Government Adoption. *Electronic Journal of e-Government*, 2(1), 11-20.

"Chris". (April 6, 2006). "Government of Canada and ePass: We Paid for This?" Weblog entry. ob.blog. Retrieved March 23, 2009, from http://www.postal-code.com/mrhappy/blog/2006/04/06/government-of-canada-and-epass-we-paid-for-this/

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319-340.

Department of Internal Affairs (New Zealand). (2008, April 30). *Identity Verification Service.* Retrieved from http://www.dia.govt.nz/idconsult

Government of Canada. (2008, Dec. 1). *About e-Pass.* Retrieved from https://blrscr3.egs-seg.gc.ca/faq/aboutepass_e.html

Government of New Zealand. (2009). *IVS Overview*. Retrieved from http://www.e.govt.nz/services/authentication/ivs

Hardt, D. (Sept. 30, 2006). Keynote Speech, New York University School of Law Multidisciplinary Graduate Student Symposium, "Identity and Identification in a Networked World". New York.

Hollosi, A. (n/d). *Austria's National Identity Infrastructure.* Retrieved March 23, 2009 from http:// itm.campus02.at/fileadmin/downloads/publications/Hollosi_-_Austrian_ID_Infrastructure_-_IDM_Summit_2008_Singapur.pdf

Hung, S-Y., Chang, C-M., & Yu, T-J. (2006). Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly,* 23, 97-122.

Inter-Jurisdictional Identity Management and Authentication Task Force. (2007). *A Pan-Canadian Strategy for Identity Management and Authentication – Final Report.* Victoria, BC. Retrieved from http://www.cio.gov.bc.ca/idm/idmatf/IdMAFinalReport.pdf

Information and Privacy Commissioner of Ontario. (2009). *The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust Enabled Federation.* Retrieved from http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836

Internet World Stats. (2008) *Internet World Stats – Austria.* Retrieved March 23, 2009 from http://www.internetworldstats.com/eu/at.htm

Internet World Stats. (2008a) *Internet World Stats – Canada.* Retrieved March 23, 2009 from http://www.internetworldstats.com/am/ca.htm

Internet World Stats. (2008b) *Internet World Stats – New Zealand.* Retrieved March 23, 2009 from http://www.internetworldstats.com/sp/nz.htm

Internet World Stats. (2008c). *Internet Usage in Europe.* Retrieved March 23, 2009 from http://www.internetworldstats.com/stats4.htm

Kavoukian, A. (2008) *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum, Not Zero-Sum.* Office of the Information and Privacy Commissioner of Ontario. Retrieved from http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=758

Leitold, H. (2006, May 11). *European Electronic Identity Practices: Country Update of Austria.* Porvoo 9, Ljubljana, Slovenia, May 11-12, 2006.

Lester, R. (Sept. 2002) *e-Government in British Columbia*. BC Chief Information Officer - Presentation for Municipal Information Systems Association. Victoria, BC. Retrieved from http://www.cio.gov.bc.ca/Strategic_Initiatives/MISA_Rick_Sept_2002.pdf

Obi, T. (2008). *The Waseda University World e-Government Ranking released*. Waseda University. Retrieved March 12, 2009, from www.obi.giti.waseda.ac.jp/e_gov/2008-02_World_e-Gov_Ranking.pdf

Office of the Privacy Commissioner of Canada. (2007). *Identity, Privacy and the Need of Others to Know Who You Are: A Discussion Paper on Identity Issues.* Ottawa, ON. Retrieved from http://www.privcom.gc.ca/information/pub/ID_Paper_e.pdf

O'Neill, R. (April 10, 2007). *'Big Brother' barrier to govt ID scheme*. Retrieved March 22, 2009 from Computerworld: http://computerworld.co.nz/news.nsf/news/0ECE4016BE898E1CCC2572B4000C1D36

Public Works and Government Services Canada. (Aug. 1, 2008). *Government On-Line (GOL).* Retrieved from http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/ged-gol-eng.html

Rogers, E. (1983). *Diffusion of Innovation (Third Ed.).* New York: The Free Press.

Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. *Computer Law and Security Report*, 24, 447-453.

Service Canada. (2007). *Service Canada Annual Report 2006-2007*. Retrieved Mar. 16, 2009 from: http://www.servicecanada.gc.ca/eng/about/reports/ar_0607/index.shtml

Treasury Board of Canada Secretariat. (2003). *Challenges and Requirements of On-Line Authentication – The e-Pass Solution*. Retrieved March 12, 2009 from: http://www.tbs-sct.gc.ca/pki-icp/gocpki/challenge-defi/challenge-defi-eng.rtf

Underhill, C. and Ladds, C. (2007) *Connecting With Canadians: Assessing the Use of Government Online.* Statistics Canada. Retrieved March 12, 2009, from http://www.statcan.gc.ca/pub/56f0004m/56f0004m2007015-eng.htm

United Nations. (2008). *United Nations e-Government Survey 2008.* New York: United Nations.

United Nations, (2008a). *UNSTATS – United Nations Statistical Common Database.* Electronic Database. New York, NY.

Warkentin, M. et al. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets,* 12(3), 157-162.

Watkins, P. (Nov. 21, 2007). *Trust and Identity Management: Experience and Perspective from the Province of British Columbia, Canada.* Trust Conference: e-Government Identity Management Initiatives. The Hague, Netherlands.

World Bank. (2008). *Definition of e-Government*. Retrieved March 12, 2009, from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/EXTEGOVERNMENT/0,,contentMDK:20507153~menuPK:702592~pagePK:148956~piPK:216618~theSitePK:702586,00.html