

Inter-jurisdictional
Identity Management
and Authentication
Task Force

Final Report

July 2007

A Pan-Canadian Strategy for Identity Management and Authentication



July 31, 2007

Deputy Ministers Responsible for Service Delivery

Dear Deputy Ministers,

On behalf of the Inter-jurisdictional Identity Management and Authentication Task Force, we are pleased to submit the attached Final Report. This report provides a strategy, recommendations and action plan for implementing a pan-Canadian Identity Management and Authentication (IdM&A) Framework that will facilitate client centred, cross-jurisdictional, multi-channel service delivery for citizens and businesses.

The Task Force has made significant progress since it delivered its Interim Report to you in April of this year. It has fine-tuned the vision and value proposition presented to you in April; conducted a detailed review of the current challenges in IdM&A and cross-jurisdictional initiatives, generally; and proposed solutions to these challenges through the development of a strategy and action plan that includes a comprehensive IdM&A framework, pilot projects, and an interim governance structure to oversee continued work in this area.

With this work, the Task Force has significantly advanced the thinking of what it would take to achieve a pan-Canadian solution to IdM&A and has set a strong foundation for future collaboration in this area. This initiative is, in a word, “transformational”. Achieving the vision of a pan-Canadian solution to IdM&A where “governments in Canada are trusted and collaborative partners” in providing citizens and businesses with “simple, convenient and protected access to multi-jurisdictional services through “no wrong door” multi-channel access” is a considerable undertaking. As such, it will require the investment of significant and sustained effort, resources and time as well as commitment and leadership from the highest levels.

It is also the opinion of this Task Force that success will require the extension of responsibility for this initiative beyond the Deputy Ministers responsible for service delivery. While service delivery is an important component, there are many other sectors that have significant interest and solutions to offer in the area of IdM&A. Vital Statistics, Citizenship and Immigration, Border Security, Passport Canada, Driver Licensing, Health and Criminal Justice all play a role in the identification and authentication of citizens and their active participation in a pan-Canadian solution will be key. Engagement of the broader public sector, industry experts, academia and the general public will also be important.

The effort to date has, for the most part, been led by a “coalition of the willing”. While notable progress has been made, success will ultimately be dependent on the active and effective participation of key stakeholders in all jurisdictions. This effort will require the commitment, participation and financial support of leaders in all jurisdictions. Either we collectively see the benefits to taking a pan-Canadian approach and commit fully to this road, or we go back to doing what we were doing before – implementing separate, and perhaps divergent, IdM&A services in our own jurisdictions. In saying this, the Task Force

does not underestimate the challenge of bringing these stakeholders together or engaging leaders in all jurisdictions. It will be difficult but, in the long run we believe, worth doing.

In the meantime, the Task Force recommends an interim governance structure and concrete steps that can be taken now to set the foundation for greater collaboration and move this initiative toward the longer goal. Those initial steps and priorities are set out in the report's action plan.

In concluding our remarks, we wish to thank our fellow Steering Committee members for their unflinching commitment to this cause and for making this initiative a priority despite many conflicting demands. We also wish to thank the dedicated members of the Task Force Working Group for the long hours and hard work they committed to this project. And finally, we wish to thank the many, many staff, stakeholders and experts in each jurisdiction who assisted in this endeavour and made themselves available, often at short notice, for consultation and advice.

Sincerely,

Dave Nikolejsin
Task Force Co-Chair
Chief Information Officer
British Columbia

Michel Rosciszewski
Task Force Co-Chair
Directeur, Direction des politiques
Quebec

Task Force Membership

The Co-Chairs wish to thank the following members of the Task Force Steering Committee and Working Group for their commitment and support over the last six months:

Co-Chairs:

Dave Nikolejsin, Chief Information Officer, Province of British Columbia
Michel Rosciszewski, Directeur des Politiques, Province of Quebec

Steering Committee:

Donna Achimov/ Lois Fraser, Public Sector Service Delivery Council (PSSDC)
Ken Cochrane, Government of Canada
Rob Dowler, Province of Ontario
Siegfried Fuchsbichler, Public Sector Chief Information Officers Council (PSCIOC)
Gerry Matte, Municipal Information Systems Association (MISA)
Tom Thackeray, Province of Alberta

Working Committee:

Mitch Fuhr, Province of Alberta (Lead)
Barry Cameron, Government of Canada
Andre Michel Couture, Government of Canada
Martin Franche, Province of Quebec
Charmaine Lowe, Province of British Columbia
Wendy Paquette, Province of Ontario
Murray Rosenthal, Municipal Information Systems Association (MISA)

Secretariat:

Nadine Goman, Institute of Citizen Centred Service
Kathy Rampersad, Institute of Citizen Centred Service

Table of Contents

1. INTRODUCTION.....	6
2. TASK FORCE MANDATE AND ACCOMPLISHMENTS.....	9
2.1 Formation of Task Force	9
2.2 Task Force Mandate.....	10
2.3 Task Force Accomplishments	10
3. VISION AND VALUE PROPOSITION.....	12
3.1 Task Force Vision.....	12
3.2 The IdM&A Value Proposition	13
4. PAN-CANADIAN IdM&A CHALLENGES: PROBLEM AND SOLUTION ANALYSIS.....	15
4.1 Capacity Challenges.....	17
4.2 Identification and Authentication Challenges	19
4.3 Inter-jurisdictional Relationship and Trust Challenges	34
5. STRATEGY AND HIGH LEVEL RECOMMENDATIONS	41
5.1 Pan-Canadian IdM&A Framework.....	41
5.2 Pilot Projects.....	44
5.3 High Level Recommendations	44
6. GOVERNANCE RECOMMENDATIONS.....	48
6.1 Analysis of Governance Models.....	48
6.2 Governance Strategy – Direction from Steering Committee	49
6.3 Recommendations.....	50
6.4 Proposed Structure and Mandate	52
7. ACTION PLAN	59
7.1 Action Lines	59
7.2 Roadmap	67
ANNEX: PAN-CANADIAN IdM&A FRAMEWORK.....	68
A1 IdM&A Principles	70
A2 Lexicon	77
A3 Legal Component	81
A4 Privacy Component	84
A5 Security Component.....	92
A6 Assurance Component.....	99
A7 Identity Component	113
A8 Trust Component.....	119
A9 Service Management Component.....	128
APPENDICES	133
A. Task Force Meetings and Consultations	134
B. Task Force Financial Report	136

C.	Environmental Scan of IdM&A Initiatives	137
D.	Identity Fraud: Causes and Factors	142
E.	Recommended Pilot Projects	147
F.	Governance Workshop.....	161
G.	IdM&A Models	170
REFERENCES		178

1.0 Introduction

All Canadian governments -- federal, provincial, territorial and municipal -- share a common need to provide services to citizens and businesses across multiple channels (i.e., online, over the telephone, by mail and in person) in a client-centric way. The potential benefits of doing this are significant: improved service delivery and client engagement through increased accessibility and choice and significant cost reductions.

Many informational services are already provided through these delivery channels. However, there is a growing need to offer transactional services through these channels (particularly over the Internet) and to provide a seamless service delivery experience in a cross-jurisdictional context. Before this can happen, however, it is imperative that governments be able to properly identify both citizens and the beneficiaries of services. This is particularly important where personal information is involved. In the health and social services sectors, for example, the proper identification of clients is necessary to ensure that those who are eligible for services do in fact, receive the appropriate benefits and services. Incidents of fraud and abuse cause financial loss to taxpayers, while preventing those in need from receiving necessary services.

The need for effective and efficient co-ordination of client identification and authentication is growing. Increasingly there are stories about identity fraud resulting in the wrong person accessing costly government services and benefits, or recently, about a person being denied rightful access to a Citizenship Certificate because of inconsistent naming requirements between provincial and federal agencies¹. And as more transactional services move on-line, new identification and authentication policies and practices are being created (and recreated) in ad hoc ways, which will make future service transformation increasingly more difficult and costly.

In the service delivery world, more and more services are being organized by life events, where a common understanding and trust of authentication processes will be critical.

Better Outcomes for Citizens, Clients and Governments:

1. A university aged student could have contact with a wide range of public sector programs in a short period of time, where each program will want to assure themselves of the student's identity to a greater or lesser degree. The student may want to apply for a student loan or scholarship, apply as a foreign student, find off campus housing and change their address. As a teenager, he may want to vote for the first time, work part time, get a drivers license, buy a car, apply for street parking, sign up for sports at the community center, borrow a book from the library, etc. In an ideal world, the student would have no wrong door access to these services (primarily on-line) with streamlined identification and authentication processes designed to share limited personal information with other programs with the student's consent.

¹ See the Task Force's Interim Report for details (<http://www.iccs-isac.org/eng/ITF2007.html>)

2. When a family member dies, there are a myriad of federal, provincial and municipal programs to be notified and each have their own authentication process. There are benefits to cancel (e.g. CPP, Old Age Security, Veteran's Affairs, provincial social benefit, tax benefits, etc). The SIN must be deactivated, death and survivor benefits must be initiated, and a number of credentials cancelled (e.g. Passport, driver's license, health card, etc). In an ideal world, the client's next of kin or representative would register the death once and the appropriate programs would be automatically notified. From the government's perspective, this has huge opportunities in limiting fraudulent access to these services and from the citizen's perspective it provides much needed convenience during an emotionally trying time.
3. From a small and medium business perspective, traditional licensing and permit services have tended to be informational (where no authentication is needed), but there is a growing need to offer more transactional services on line. This will require new authentication and delegation models as well as collaborative arrangements between those government agencies that can provide assurance of a business' identity claims and those agencies that need to rely on such assurances.

A continuing challenge has been to keep pace with the rising expectations of citizens and businesses for high quality, cost-effective public services. Clients benchmark their expectations against previous service experiences in both the private and public sector. They are now used to multi-channel access for information and forms and services like online banking and therefore increasingly expect to interact with government about an array of specific services through a channel they choose, and at their convenience.

Looking ahead, larger and more complex vertical and horizontal service initiatives can be anticipated as programs increasingly collaborate across department and jurisdictional boundaries. Citizens are also expecting greater engagement with government, more control, and greater choice. Thus, Internet-related technologies are having and will continue to have a profound effect on service delivery. However, there are as yet no broad authentication solutions to support this deeper client engagement with the public sector. At present, jurisdictions are creating authentication solutions and frameworks independently, using non-standard terminology and architecture. The longer this situation continues, the more costly and difficult it will be for jurisdictions to collaborate and streamline service delivery in the future. A scan of work in this area revealed at least 14 different IdM&A initiatives that have been completed or are underway across the country.

Maintaining the status quo will clearly not produce the inter-operable environment that is necessary to enable the vision of seamless multi-channel cross-jurisdictional service delivery. Adding to the complexity is the fact that cross-jurisdictional service delivery encompasses many federal departments, 13 provinces and territories, 7000 municipalities and numerous agencies, boards and commissions and may include cross-border initiatives. As a result, service delivery initiatives, their content and processes will become increasingly complex and more vulnerable to security and privacy breaches and fraud.

One of the building blocks for making these kinds of service delivery transformations secure and sustainable is a flexible Pan-Canadian Identity Management and Authentication framework for:

- trusted public sector collaboration;
- increased flexibility to quickly meet the ever growing expectations of citizens and businesses; and,
- the provision of secure and privacy enhancing services that uphold Canadian rights and values and ensure the fair and equitable treatment of clients by operating in a non-discriminatory manner.

A Pan-Canadian Framework could enable the kind of service transformation needed to reassure the public that they can trust governments to deliver the services they need in a secure and private manner. The framework would act as a reference for relying programs to help them understand what important program related elements must be thought through when collaborating and designing a service improvement with identification and authentication needs.

The development of a Pan-Canadian strategy and framework on identity management and authentication (IdM&A) would be a significant step forward to enable governments to offer client-centric service delivery that is both seamless and secure across jurisdictions.

2.0 Task Force Mandate and Accomplishments

This section sets out the Task Force's mandate and accomplishments. Further information about the structure of the Task Force, its terms of reference and its approach to developing a Pan-Canadian Identity Management and Authentication (IdM&A) Strategy can be found in its Interim Report which is available at <http://www.iccs-isac.org/eng/ITF2007.html>

As well, the Appendices to this report set out the following information:

- Appendix A: Task Force Meetings and Consultations
- Appendix B: Task Force Financial Report
- Appendix C: Environmental Scan of IdM&A Initiatives

2.1. Formation of Task Force

A Joint Declaration of the Quebec meeting of Provincial and Territorial Ministers responsible for e-government (Fall 2005) recommended the development of a "Pan-Canadian e-government strategy" and the creation of common standards and solutions to support interoperability notably in terms of infrastructure, security identification and authentication.

In June 2006, at the first inter-jurisdictional meeting of Deputy Ministers on Service Delivery Collaboration held in Victoria, twelve priorities for collaboration were identified. The highest priority was to standardize citizen and business identity management and authentication (IdM&A) across jurisdictions.

The Deputies asked the Joint Councils of the Public Sector Service Delivery Council (PSSDC) and the Public Sector Chief Information Officers Council (PSCIOC) to rank the priorities and offer their advice on how best to move forward in each area and to identify time lines, resource requirements and key deliverables for IdM&A to the Deputy Ministers at their next meeting.

On November 17, 2006, the Joint Councils reported back to the Deputy Ministers that standardizing IdM&A should indeed be a top priority. The Joint Councils recommended a course of action, which incorporated a proposal, tabled by Quebec (in Montebello), for the creation of a taskforce to develop a "pan-Canadian strategy, with a plan of action, on identification and authentication in a service delivery context".

Decisions were made regarding the formation of a short term Identity Management and Authentication Task Force, along with a budget. It was determined that the Task Force would report to the Deputies in July 2007, with an interim report in April 2007.

2.2. Task Force Mandate

The Task Force was given a six-month timeframe in which to achieve three key deliverables:

1. A Pan-Canadian Strategy for IdM&A, including:

- A framework for IdM&A that will facilitate cross-jurisdictional, multi-channel service delivery for citizens and businesses. This will leverage the work done to date in each jurisdiction and represent the optimal solution for Pan-Canadian use.
- Recommendations for how to align with privacy policies and ensure consistency between IdM&A and privacy efforts.
- Recommended tools and management models.

2. An Action Plan outlining how the strategy will be implemented and how existing work will be aligned with it. This will include recommendations on:

- Pilot projects with corresponding deliverables.
- The timelines, resources, and costs involved.
- Monitoring and reporting (e.g., indicators, evaluation, and verification methods).

3. A Governance Structure and funding model.

2.3 Task Force Accomplishments

The Task Force has completed the deliverables assigned to it within the 6 month time period and on budget (see the Task Force's Financial Report in **Appendix B**).

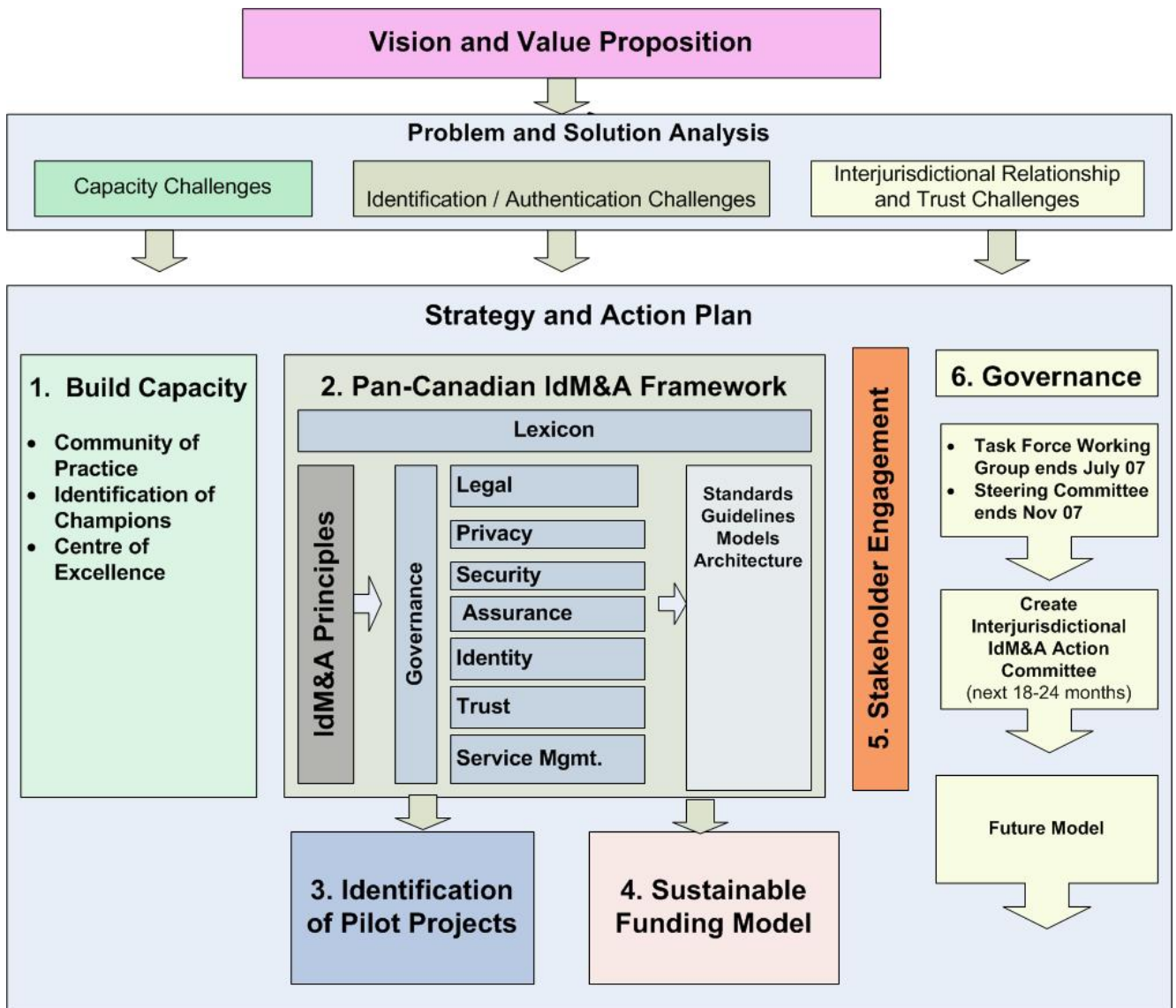
The following chapters set out the steps the Task Force took in developing the Pan Canadian IdM&A Strategy, Governance Structure, and Action Plan:

- **Chapter 3** sets out the Vision and Value Proposition the Task Force created for a Pan-Canadian IdM&A Strategy and Framework.
- **Chapter 4** summarizes the high level analysis the Task Force conducted of the current challenges or problems most jurisdictions face in moving towards the Vision.
- **Chapter 5** presents the Strategy and High Level Recommendations the Task Force developed based on its analysis of possible solutions to the challenges it identified.
- **Chapter 6** contains governance recommendations.

- **Chapter 7** sets out a proposed Action Plan to implement the strategy and recommendations.
- The **Annex** to this report contains the proposed Pan-Canadian IdM&A Framework, the endorsement of which is recommended in the Strategy and Recommendations chapter.

Figure 1, below, illustrates the key deliverables of the Task Force and their relationship to the preliminary work of the Task Force (i.e., vision and value proposition, problem and solution analysis). This figure also serves as a visual guide for the next chapters.

Figure 1. Work of the Task Force



3.0 Vision and Value Proposition

As governments increasingly improve the electronic delivery of services and move to the seamless delivery of services across programs, channels, and jurisdictions, they must trust that they can identify and authenticate the citizens and businesses requesting their services. The information age has dramatically changed the ways and the situations in which individuals are identified and authenticated, and as such, electronic service delivery, in particular, requires some rethinking of traditional approaches to IdM&A.

To meet current client demands (from both citizens and businesses) for more seamless, coherent, services from all levels of government, it is imperative to find ways to recognize and accept electronic credentials across service delivery programs and, eventually, across jurisdictions. It is also important to leverage the various existing identification and authentication infrastructures in many jurisdictions. Collaborating on identity and authentication standards will also facilitate a shift toward client-centred service delivery, help focus attention on improving government services, and create a more efficient means to deliver services.

There are several reasons why governments would want to collaborate and cooperate on a cross-jurisdictional basis to deliver services:

- A client typically interacts with multiple jurisdictions to receive related services;
- A client is a taxpayer in those same jurisdictions and is therefore interested in reducing duplication of effort and investment; and,
- All governments need to increase security and reduce identity fraud.

3.1 Task Force Vision

The overarching vision of the Task Force has been a Pan-Canadian IdM&A Framework that supports access by citizens and businesses to a seamless, cross-jurisdictional, user-centric, multi-channel service delivery experience when interacting with government. Achieving such a vision requires the development of trusted, collaborative relationships across jurisdictions based on common goals and standards. The details of this strategic vision and the value this vision brings to both clients and governments is set out below.

Task Force Vision

- **Citizens and businesses enjoy simple, convenient and protected access to multi-jurisdictional services in a manner they choose and control.**
- **Governments in Canada are trusted, collaborative leaders in citizen-centred service delivery.**

The Task Force has concentrated on what is needed to properly identify and authenticate clients for transactional purposes. While all service delivery channels have been considered, the Task Force focused primarily on facilitating delivery of online services as this channel presents the greatest IdM&A challenges and is likely to yield the greatest service delivery benefits.

In working towards its Vision, the Task Force has been guided by the following service delivery design principles:

Service Delivery Design Principles

- Simplified access to public services, particularly transactional services, for citizens and businesses, according to their needs.
- The vertical regrouping of services to citizens and businesses (federal–provincial–territorial –municipal) while recognizing regional differences.
- The ability to leverage existing infrastructure and the increased interoperability of systems.
- Support for the development of e-government initiatives.
- The efficient and effective use of government services.
- A risk-based approach.
- Privacy and security of personal information and confidential business information.
- Strong public administration, trust and accountability.
- An enduring solution.

3.2 The IdM&A Value Proposition

From its inception, the Task Force has recognized that for a Pan-Canadian IdM&A solution to be broadly adopted by governments, citizens and businesses, there must be widespread recognition of the value it would deliver. In its Interim Report, leaders were asked to imagine....

the value that would be created by all governments if agencies would agree among themselves upon common identification elements, accept the same authentication credentials, and assist each other with identity proofing.

Since then, the Task Force has worked to articulate a clear value proposition for all stakeholders.

A. For Citizens and Businesses, a Pan-Canadian IdM&A solution will:

- Improve their experience with service delivery by enabling them to seamlessly access services as needed, regardless of the jurisdiction.
- Provide them with access to a greater range of transactional services.
- Be easy to use and consistent.
- Require less duplication and effort.
- Promote business efficiency and compliance, minimizing cost.

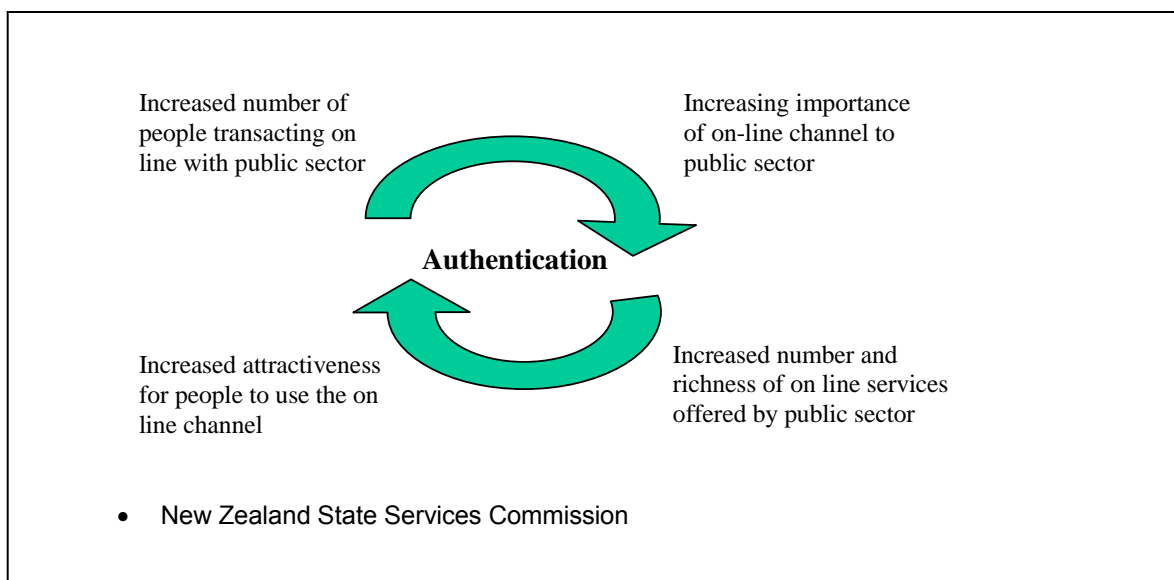
- Increase their trust that both personal and confidential business information are managed in a private and secure way.
- Increase their willingness to transact with government (particularly on-line).

B. For all levels of government, a Pan-Canadian IdM&A solution will:

- Enable cost effective service delivery by leveraging consistent processes, reducing errors, streamlining front and back end processing and maximizing infrastructure investments.
- Provide sustainable, practical authentication practices.
- Leverage existing work done by jurisdictions.
- Establish a foundation for transparent IdM&A principles and standards, leading to seamless service delivery and public confidence in identity proofing.
- Enhance trust and confidence in the public sector through improved client satisfaction and access to more on-line services requiring authentication.
- Enable the public sector to respond faster to cross-jurisdictional needs.
- Reduce risk and liability and the likelihood of fraud.
- Increase the likelihood of clients transacting on-line as concerns about privacy and identity theft decline.

Finally, improved IdM&A processes can actually stimulate the development of seamless, cross jurisdictional services. As the Government of New Zealand noted recently, “authentication can prime a virtuous cycle” (New Zealand, 2007). This cycle is illustrated in Figure 2, below.

Figure 2. The "Virtuous Cycle" of Improved IdM&A



4.0 IdM&A Challenges: Problem and Solution Analysis

The Task Force was asked to investigate, analyze, and propose solutions to the current barriers or challenges we face in establishing a Pan-Canadian Identity Management and Authentication (IdM&A) framework for the purpose of facilitating seamless, cross-jurisdictional, multi-channel service delivery.

METHODOLOGY:

This analysis identifies the key challenges, problems and constraints jurisdictions face in implementing effective IdM&A processes which, in turn, are hindering the implementation of seamless, cross-jurisdictional, multi-channel service delivery. The analysis also searches for opportunities and possible solutions to the identified problems.

It is important to note that this analysis represents, for the most part, the views of participating jurisdictions on the Task Force. The Task Force has done its best to solicit views and concerns from non-represented jurisdictions, primarily through the Joint Councils (PSSDC and PSCIOC), but clearly that process is not as effective as actually having a seat on, and contributing directly to the work of, the Task Force. Consequently, non-represented jurisdictions may have different views of the challenges and the best way to solve them that are not articulated here. This analysis is essentially a preliminary analysis that represents, to the best of our knowledge, based on the consultations we have conducted and the input received to date, a common vision of the IdM&A challenge.

Furthermore, the challenges set out below are not an exhaustive list; rather they represent an amalgamation of the key and common challenges identified by participating jurisdictions to establishing a Pan-Canadian IdM&A framework. The objective was to identify the real bottlenecks that all jurisdictions have identified as a high priority and that all jurisdictions wish to overcome. The challenges are also represented in a general way; and should not be considered a detailed analysis of each problem and its corresponding relationships (i.e., causes and effects).

Finally, it is important to note that this analysis is only concerned with those challenges posed by establishing a Pan-Canadian IdM&A framework. While there may be other challenges to facilitating cross-jurisdictional, multi-channel, seamless service delivery (e.g., channel convergence, bridging the digital divide), those challenges are outside the scope of this Task Force.

SOURCES:

The information that forms the basis of this analysis was gleaned from a number of sources. In addition to the reference material listed in the bibliography, information and feedback on IdM&A challenges and barriers was provided through stakeholder consultations that occurred within each jurisdiction and through workshops the Task Force held in Victoria, Montreal and Niagara-on-the-Lake.

The following documents were of particular value in informing this analysis:

- Professor Kenneth Kernaghan's May 2003 report, entitled *Integrated Service Delivery: Beyond the Barriers*, prepared for the Chief Information Officer, Government of Canada;
- *Modinis*, "Modinis Study on Identity Management in eGovernment", prepared for the eGovernment Unit (DG Information Society and Media, EC), 6 June 2006, deliverable D.3.9.
- BTEP Identity Management: Mapping the Continuum, prepared by Team BCE, Secure Channel Project, Government of Canada
- "Canadians' Views on Privacy, Security, Information Sharing and Identity Management", Cathy Ladds, Research and Analysis Division, CIOB, Treasury Board of Canada Secretariat, Prepared for the Federal and Provincial and Territorial Deputy Ministers, December, 2006
- A summary of participants comments from the Montreal Identity Management workshop.

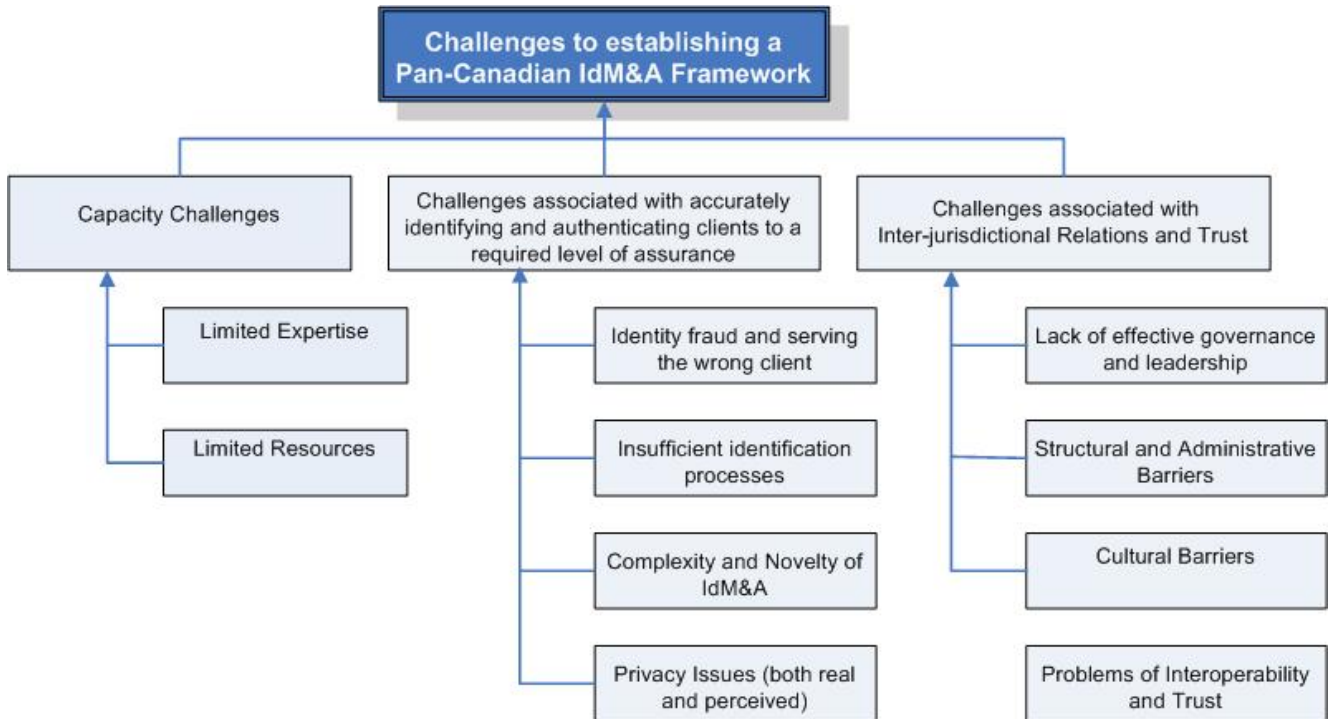
THE CHALLENGES:

Based on the aforementioned information, the Task Force concluded that there are three main sets of challenges that must be addressed or overcome in order to establish a Pan-Canadian IdM&A framework:

- 1) Capacity challenges;**
- 2) Challenges associated with accurately identifying and authenticating clients to a required level of assurance; and,**
- 3) Challenges associated with establishing effective inter-departmental and inter-jurisdictional working relationships.**

As illustrated in Figure 3, each of these high-level challenge statements can be broken down into a set of key problems.

Figure 3: Challenges to Establishing a Pan-Canadian IdM&A Framework



4.1 Capacity Challenges

Capacity challenges relate both to the ability of each jurisdiction to participate and engage in a Pan-Canadian IdM&A framework, and to the ability of some jurisdictions to engage in any IdM&A activities at all, even within their own jurisdiction. It is important to note that capacity is much more than training and formation: it also includes material and financial aspects.

The Task Force identified two main categories of capacity challenges:

1. Limited expertise; and,
2. Limited Resources.

4.1.1 Limited expertise

It has been widely recognized by participating jurisdictions on the Task Force that there is limited in-house expertise and practical experience that can equip individuals with the understanding, skills, knowledge and training that enables them to perform effectively in managing issues relating to IdM&A within their own jurisdictions or at a pan-Canadian level. Furthermore, the number of experts and the quality of the expertise is different in each jurisdiction.

This is a crucial issue in terms of policy-making, advising policy-makers and making effective decisions in system design and technology selection. Also, unlike related disciplines such as privacy or security, few jurisdictions have dedicated staff to this area, let alone established a specific department or program to work on this evolving and critical topic. The Government of Canada is the only known jurisdiction to have a specific division responsible for IdM&A.

These challenges are exacerbated when government agencies acquire technology and services from the private sector where expertise is focused primarily on business IdM&A needs, as opposed to government or public sector IdM&A specific needs and requirements. To date, most innovation in IdM&A has occurred in the private sector within a business perspective. This perspective does not necessarily meet governmental requirements or specifications, particularly with respect to privacy.

Furthermore, the few in house experts that do exist are usually assigned to one program area to focus on program IdM&A needs. Experts who are assigned to departments with a horizontal or corporate perspective, usually operate within a context or discipline (such as security or privacy) which includes IdM&A issues but does not encapsulate the entire IdM&A discipline. This is exacerbated by the fact that no one department in any jurisdiction has clear legislative responsibility over IdM&A in terms of policy. Consequently, experts will engage in IdM&A within their own context and with only a partial reflection of the whole picture.

The limited pool of experts is also caused by the fact that IdM&A is a relatively new discipline and as such there is limited practical expertise and experience in this area, particularly in an interdepartmental or inter-jurisdictional context.

4.1.2. Limited resources

Material and financial resource allocation is a challenge that is common to all jurisdictions engaging in horizontal initiatives even within their own jurisdiction; and it is even more the case when it comes to cross-jurisdictional and pan-Canadian initiatives. Obtaining resources for horizontal initiatives is a pervasive challenge with political and structural implications as well as managerial, operational and cultural ones. Yet, the success of any pan-Canadian initiative depends highly on the availability and nature of resources that jurisdictions allocate.

Horizontal funding depends, to a high degree, on government priorities, institutional settings and governance rules that still favour departmentalism. The challenge is to overcome the reluctance or inability of governments to fund projects on a horizontal basis.

Cross-jurisdictional initiatives are often multi-year initiatives that require substantial up-front investment and take considerable time to harvest savings. Moreover, the savings may accrue to the government as a whole rather than to the department making the savings. In other words, economies of scale are possible at the horizontal level but lacking at the vertical level as capital investment is relatively high. In this regard, available methods do a

poor job of demonstrating benefits as most horizontal projects are relatively new and return on investment needs a longer term.

Changing a department's or a government's budgetary system to permit dedicated funding of horizontal projects can be extremely difficult. Moreover, even when such funds are made available, decisions on their allocation are shared among the partners and accountability is often diffused.

Furthermore, resource allocation for horizontal projects that leverage existing solutions or infrastructures to improve them or produce economies of scale is often frustrated by the fact that jurisdictions and their departments are inclined to defend local choices in existing infrastructures and solutions. This, in turn, increases the reticence to deploy, or make available, resources to engage in any changes.

4.2 Challenges associated with accurately identifying and authenticating clients to a required level of assurance

Why is it so difficult to accurately identify and authenticate clients to a required level of assurance, particularly when providing services to them remotely (e.g., over the telephone or the Internet)?

In examining this issue, the Task Force identified four key challenges in this area:

1. Concerns about identity fraud and serving the wrong client (e.g., improper payments);
2. Insufficient identification processes;
3. Complexity and novelty of IdM&A; and
4. Privacy issues.

4.2.1 Identity Fraud and serving the wrong client

“Identify fraud” (or “identity theft as it is sometimes called) is an extremely controversial term to which there is currently no universally accepted definition. However, identity fraud usually refers to a process where someone obtains another person’s personal information or identification and uses it without that person’s knowledge or consent to commit fraud (e.g., creating false accounts in another’s name) for financial gain or for another criminal purpose.

The consequences of identity fraud are considerable. For example, “Nine per cent of Canadians – or 2.7 million people – have fallen victim to identity theft at some point in their lives, according to the findings of a 2003 Ipsos Reid survey.”²

² From Privacy Commissioner web site on “Identity Theft – A Primer” http://www.privcom.gc.ca/id/primer_e.asp

How identity thieves get your personal information

- Stealing mail from your mailbox or recycling bin, or fraudulently redirecting your mail by forging your signature on a "change of address" form.
- Stealing personal and private information from lost or stolen wallets or purses, from your home, your vehicle, or your computer.
- Stealing personal information from lost or stolen personal electronic devices such as, personal digital assistants (PDAs), digital audio players, cellphones and laptops.
- Posing as a trusted official of a company or of law enforcement, in person or online, and requesting your personal information such as your credit reports or bank account password.
- Tampering with automated banking machines (ABMs) and point of sale terminals, so that your debit or credit card number and personal identification number (PIN) can be recorded.
- Taking information from within organizations, such as employees who accept bribes or who steal your personal information on behalf of others. Organizations may also unwittingly release your personal information to criminals who pose as legitimate businesses.
- Searching public sources, such as newspapers (obituaries), phone books, and records open to the public (professional certifications).
- Using "spoof" emails and fraudulent websites ("brand spoofing") to fool customers into divulging their personal and financial information in a practice known as "phishing".
- Using "spyware" to steal information from your computer.

Source: Consumer Measures Committee <http://www.cmcweb.ca/epic/site/cmc-cmc.nsf/en/fe00084e.html>

Concerns about identity fraud and providing a service or a payment to the wrong person are serious and growing problems for government, particularly as it moves towards providing services and conducting transactions over telephone and Internet channels. Identity fraud is growing because more personal information is collected and retained than ever before, and the risks of fraud multiply every time information is transmitted, retained or disposed of in an unsafe manner. In addition, a criminal often doesn't need that much information to commit fraud and seriously disrupt someone's life: often a name, address, and date of birth are enough to get started.

Much has been written about identity fraud, its causes and effects, and every year thousands of citizens become new victims of some kind of identity fraud. As a result, citizens are becoming more and more cautious about providing their identity information to anybody, particularly over what they regard as insecure channels.

A fuller analysis of the causes and factors that increase or make possible identity fraud can be found in **Appendix D**.

4.2.2 Insufficient identification processes

The issue here is that most identification and authentication services currently used or available to the service delivery community are not sufficient to identify and authenticate clients to a high level of assurance, particularly over remote channels such as the telephone or the Internet. This problem is only exacerbated when one considers a pan-Canadian

solution. There are a number of factors that contribute to this issue but the key reasons communicated to the Task Force through its consultation with stakeholders were:

- a. It is unclear what organizations are authoritative on “identity” or identity attributes in Canada;
- b. There is currently no consistent and uniform way to uniquely identify citizens and businesses across services and jurisdictions;
- c. It is difficult to assess the risks involved;
- d. Data integrity or quality is currently insufficient; and,
- e. There is currently no consistent and uniform way to uniquely identify dependants, designates and delegates.

4.2.2.1 It is unclear what organizations are authoritative on “identity” or identity attributes in Canada

Because most organizations will not accept as evidence the word of the individual or business seeking a service or entitlement where a high level of assurance is required, trusted third parties are often relied upon to vouch for or verify identity claims. But who are these trusted third parties? Are they parties who actually have authority over “identity” or the identity attributes being claimed by the client?

Currently, there is no clear authority on “identity” in Canada. It is also the case that many government organizations and jurisdictions rely upon identity assurances outside of their direct control. As a result, IdM&A in Canada has evolved into a complex web of assurances not backed by any specific authority. In many instances, an assurance is based upon documentary evidence (a credential) presented by the individual and accepted at face value. Also, in many cases, related but different assurances are inferred from documents not intended to provide these assurances. For example, when an individual applies for a provincial health card, the *assurance of identity* and *assurance of residency* are often inferred from documents not intended for that purpose (e.g. a valid driver’s license and a recent utility bill). While these practices may be currently acceptable, there are many hidden risks to the overall ‘system’. The result is the presence of many vulnerabilities which can be easily exploited.

4.2.2.2 No consistent and uniform way to uniquely identify individuals and businesses across services and jurisdictions

There is no consistent and uniform system of identification in Canada. While identification and verification processes may be more consistent within a jurisdiction or within a sector across jurisdictions (e.g., health, vital statistics, driver licensing), they are not consistent across all sectors and all jurisdictions.

Identification Information

There is also no uniform agreement on what identification information should be collected from a client to distinguish them from others. Generally, an individual is identified by her name and birth date but programs vary on whether they require an individual's legal name or not and on the format in which they record the name and birth date.

Businesses in Canada can be identified by a unique Business Number or by their legal name but it is just as common for programs to identify them by their operating name, operating address, and other contact information such as the names of principals or representatives.

Other information may also be collected for identification purposes depending on the authority and needs of the agency requesting the identification. (For example, some program areas have the authority to collect the Social Insurance Number, others do not)

In some cases, identity information may be accepted as valid without verification (i.e., accepted at face-value) or with limited verification; and it can be accepted in incomplete and varied forms (e.g., Kathy Smith instead of Katherine Jane Smith or A & B Electric rather than Abbot and Brown's Electrical Supplies, Inc.).

This inconsistency creates a lack of trust in identification elements from other departments and jurisdictions. There can be concerns about the source of key information and the thoroughness of the identity verification process.

Use of Different Documents as Evidence of Identity

The lack of a clear authority on "identity" in Canada has led to a multitude of documents being accepted as assurance of identity. Documents, such as the driver's licence and passport, have become, through general practice and acceptance, "de-facto" identity cards in Canada. These documents are generally accepted as proof of identity because they contain biometric factors such as photographs and signatures and because they are issued through a relatively reliable process that most people are familiar with.

On the other hand, some government agencies do not consider these documents to be acceptable as proof of identity because they are not "foundation" documents. Some argue that only "foundation" documents such as birth certificates, citizenship certificates and permanent residency cards should be accepted as identity because they are the foundation of identity in Canada - other documents are merely permits to drive or travel. While there is some merit in this argument, one of the obvious weaknesses with relying only on "foundation" documents to prove identity is that most of them do not include photographs. The lack of a photograph and other key identity information (such as current address) make it difficult to validate that the client presenting a birth certificate is really the owner of the document. So while foundation documents are clearly crucial documents in terms of establishing a chain of identity – from birth to death – they may not be sufficient on their own to prove identity, and likely should be accompanied by a verification at the point of issue process.

Solution Analysis:

The Legal and/or Identity Component of the IdM&A Framework could set out what agencies are, or should be, authoritative on what specific identity claims.

Since there is no one authority on identity or identity attributes in Canada, particularly one that is authoritative on all the different identity attributes a person may use in different contexts (i.e., in a business transaction or as a patient or employee), organizations may have to rely on a number of different authorities to verify an identity claim, depending on the service being sought and the identity claim being made.

The organization may need to link assurance of identity back to a foundation document (e.g., birth certificate) but it may also need to verify that the person presenting the foundation document is indeed who they say they are by requesting government issued photo identification or other acceptable evidence. The Assurance Component of the Framework should clarify what level of identity proofing is required for different identity assurance levels.

As well, the Identity Component of the IdM&A Framework should set semantic and syntactic (i.e., format of information) standards for identity information that is collected to facilitate inter-operability.

4.2.2.3 Difficulty assessing the risks involved

Assessing the risk of accepting a particular identifier or relying on a particular identification or authentication process is difficult to begin with, but it is particularly difficult when the risks are continually evolving and changing. Indeed, the nature of a transaction or the sensitivity of the information that is being accessed can change in accordance with an evolving client situation. For example, should the address of a particular client become highly sensitive information, the risks associated with transactions involving that address increase, which, in turn, increases the strength of the required authentication process.

As well, there is much debate on how the system or the identification and authentication models used will distribute the risks among the different parties involved. As an example, the use of a single identifier or centralized IdM&A model may centralize some of the risk as opposed to the use of multiple identifiers and a decentralized model where the risks are more distributed.

Conventional risk analytic tools are not well suited to risk assessment in the context of identity management and authentication, particularly, when considering cross-jurisdictional initiatives. As a result, government organizations may deploy identification and authentication processes that are insufficient for the risks involved, which pose risks to security and privacy. On the other hand, government organizations also need to be concerned about deploying identification and authentication processes that are over engineered or overly intrusive in comparison to the risks involved, as such processes may also negatively impact privacy and the user experience while increasing costs unnecessarily.

Solution Analysis:

The Security Component of the IdM&A Framework should address the development of analytical tools to assess risks relating to identity management and authentication, including guidelines on how to map assurance levels to different classifications of information and to different types of transactions.

The Trust Component of the IdM&A Framework should address liability issues and the distribution of risk among the parties involved in an IdM&A process.

4.2.2.4 Insufficient Data Integrity or Quality

Identification and authentication of clients to a high level of assurance is dependent, to a high degree, on the quality and integrity of the data being relied upon to make identification decisions. The Task Force was repeatedly told by multiple stakeholders that insufficient data integrity or quality was a major issue and one which was primarily due to the lack of effective linkages within and across jurisdictions for the sharing of identity and vital events information.

In fact, any database can quickly become outdated as the real world situations they record change. “The progressive, slow degradation of the accuracy of data items in databases is very common and one that often proves extremely difficult to control. It creates difficulties in databases even when users and operators have strong interests in maintaining good integrity. Database pollution is a serious problem because small amounts of data pollution can lead to a disproportionate drop in confidence in the integrity of the database as a whole and thus undermine its effectiveness.”(LSE Identity Project Report, 2005, p. 198).

The sharing or verification of identity information is important to the realization of seamless cross-jurisdictional service delivery both from a horizontal perspective because clients are mobile and from a vertical perspective because citizens are simultaneously clients of different levels of government. Clients may reside, work and attend university in different provinces than the one in which they were born. The lack of effective linkages between governments for information sharing both hinders the ability of government to provide seamless, coherent services and negatively affects the accuracy and quality of the information each jurisdiction holds. This increases the possibility of identity fraud and unauthorized access to government services.

On a positive note, there are currently a number of cross-jurisdictional initiatives underway aimed at improving data integrity and quality. For example, agreements between Vital Statistics agencies across Canada enable the sharing of vital events data where relevant (For example, if an individual dies in a province other than the one in which he was born, that information will be shared with the province where he was born). Driver Licensing agencies across Canada have similar information sharing agreements which enable them to verify licences from other provinces, check on driving restrictions and ensure that citizens only have one licence in Canada. These initiatives are an example of what can be achieved in the interests of improving data quality but these types of linkages are often restricted to a specific sector, (sometimes for legislative or policy reasons). Establishing additional linkages across sectors, where warranted and where permitted by legislation and policy,

may assist program areas and different levels of government that are involving in identifying and authenticating clients to verify documents presented for identification and to maintain accurate and up-to-date identification information – both of which are key to enabling multi-channel, seamless service delivery.

Solution analysis:

The Legal Component of the IdM&A Framework should address the need for a legislative scan to determine what legislative barriers, if any, exist to sharing identity information.

The expansion of cross-jurisdictional initiatives aimed at improving data integrity and quality (such as the Vital Events National Routing System and Integrated Birth Registration) should be encouraged.

As well, where no legislative barriers exist, pilots aimed at establishing linkages between authoritative parties and relying parties for the purpose of verifying and updating identification information could be considered.

4.2.2.5 No consistent way to uniquely identify dependants, designates and delegates

When it comes to uniquely identifying dependants, designates and delegates, all of the same challenges that exist for identifying clients apply, but with the added complexity of verifying a relationship between the client and the dependant, designate or delegate. There is currently no consistent method for establishing the myriad of relationships and different authorities that could exist between a client and his children and other dependants, employees, agents, attorneys and others that are empowered to act for the client (e.g., committee, guardian, power of attorney, etc.). The type of evidence required, how it should be verified and who is authoritative on such relationships are all issues that need to be addressed.

There are also difficulties creating and maintaining systems that can adequately store and update authorization information (such as roles and permissions) which would enable a designate or delegate to access information and/or conduct a transaction on behalf of a client. As noted in the Modinis Report (2006, p. 8), “in an e-Government context it is particularly important to accurately define who may give and accept mandates, which authorizations these mandates entail, and how they can be managed and revoked”. For businesses, identifying and managing employees who have authority to act on behalf of the business for all, or specific, transactions is complex and difficult to manage. This situation is even more problematic in a cross-jurisdictional context because legal requirements may vary.

Solution analysis:

The Identity Component of the IdM&A Framework could set standards or guidelines for identifying dependants, designates and delegates, including what evidence is required to verify a relationship between the client and the dependent, designate or delegate.

4.2.3 Complexity and Novelty of IdM&A

IdM&A is an extremely complex and relatively novel subject, particularly when considered from the horizontal or cross-jurisdictional perspective. The environmental scan conducted by the Task Force of existing IdM&A initiatives reinforced this notion by revealing different perspectives, different lexicons, different levels of maturity and different approaches to IdM&A. In fact, it was extremely difficult to make any meaningful comparison or establish commonalities because the perspectives and understanding of the subject and terms used were so different.

This section examines the key reasons why IdM&A is so complex and explores the novelty and corresponding challenges of IdM&A in the context of multi-channel service delivery and e-government.

Specifically this section examines the following issues:

1. Multiple identity contexts or roles;
2. Identity attributes that change over time; and,
3. The novelty of IdM&A in the context of multi-channel service delivery.

4.2.3.1 Multiple Identity Contexts or Roles

As an example of the complexity of IdM&A, consider the concept of “identity”. Does a person have only one identity or can a person be viewed as having different identities in different contexts (i.e., as an employee, business representative, student, parent, patient, etc.)

There is no universal agreement in the Identity Management and Authentication field as to whether we should refer to a person as having one identity and multiple roles, or multiple and different identities depending on the context. This is especially an issue when we refer to “digital identities” where one person can have multiple digital identities. Most jurisdictions recognize the need to separate a person’s identity contexts or roles. Different information and different processes may be necessary to identify and authenticate a person in different contexts (i.e., information necessary to identify or authenticate an employee, may not be sufficient or suitable to identify or authenticate a patient or business representative).

Adding to the complexity of “identity” is the issue of pseudonymous identities. It is not uncommon for citizens, and even businesses, to use pseudonymous identities, particularly over the Internet. A common example of a pseudonymous identity or identifier is a hotmail ID.

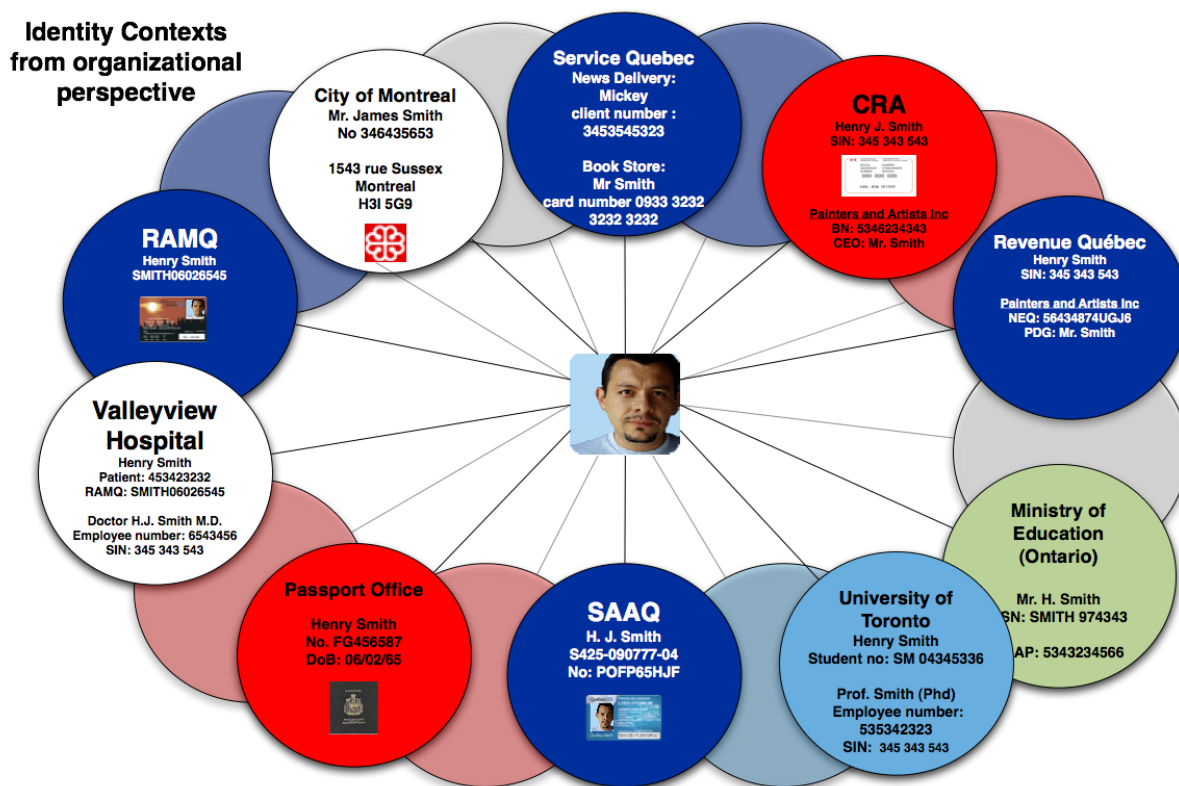
Figure 4, below, illustrates the different identities one person may legitimately have. In this example, Dr. Smith is identified one way by government institutions (e.g., his legal name, date of birth, and Social Insurance Number) and another way in his professional life by the hospital he works for and by his patients. In his personal life, Dr. Smith is not known to his friends and family by his legal first name, Henry; but is instead known by variations of his

middle name (James, Jim, Jimmy) or by a nickname. Dr. Smith also uses a number of pseudonymous identities on the Internet to conduct non-identified transactions. Meanwhile Figure 5 illustrates identity context from an organizational perspective in terms of the different ways one person may be known across contexts.

Figure 4. One person: Different Identity Contexts



Figure 5. Identity Context from an Organizational Perspective



The Identity Component of the IdM&A Framework should address the issue of “identity context” and provide guidance for how to identify individuals and businesses in different contexts.

4.2.3.2 Identity attributes change over time

Another complexity is that many identity attributes (e.g., name, address, profession, physical characteristics) change over time. Certain identity attributes such as address are less permanent than others such as birth date, with names falling somewhere in between. The permanency of names is of particular concern given its primacy as an identifier. Names can change due to marriage, divorce, adoption, or personal choice. In addition, names are problematic as identifiers because they have many variants. As in the example set out in Figure 4, above, individuals may use a shortened or cultural variation of their name or be generally known by their middle name.

Identity attributes such as biometric identifiers (e.g., fingerprint and iris scans) are less subject to change but are more costly to use and may impose privacy risks depending on the manner in which they are implemented.

4.2.3.3 Novelty of IdM&A in the context of multi-channel service delivery

Identifying and authenticating people to a high level of assurance is not, in and of itself, a novel concept. Certain sectors (such as Criminal Justice, Border Security, Vital Statistics, Citizenship and Immigration, Passport Canada and Driver Licensing) have a long history in IdM&A and their mature thinking and advanced processes reflect that experience. However, this is not the case in many other service delivery communities, and it is particularly not the case when it comes to multi-channel service delivery.

Identifying and authenticating people to a high level of assurance has traditionally been done using, or leveraging, in-person processes. Obtaining an equivalently high level of identity assurance using remote channels (particularly over the Internet) for the purpose of providing cross-jurisdictional, seamless service delivery is a relatively novel concept, and one that poses unique challenges.

Remote channels (e.g., telephone, internet) create uncertainty and providing services over these channels depends on the cooperation and willingness of clients to engage these service delivery channels. As well, seamless cross-jurisdictional service delivery will depend, to a not insignificant extent, on the client agreeing to provide information for this purpose to multiple agencies. This is quite different from other sectors that have the authority to require clients to submit to certain processes and, in some cases, to collect and share information without the client’s knowledge or consent.

4.2.4 Privacy issues (both real and perceived)

IdM&A has deep implications for privacy. It is important, therefore, to understand how privacy can be impacted by various IdM&A processes. Whether or not an IdM&A system is privacy invasive or privacy enhancing will depend to a great extent on how the system is designed, implemented and managed and on the technology used.

Unfortunately, privacy is a very misunderstood concept. Its impact is both underestimated and overestimated by program areas struggling to understand its requirements. Partly this is because privacy is subjective (i.e., it means different things to different people) and context specific. For example, the same information – a person's name – may be innocuous in one context (e.g., in a telephone book) but highly sensitive in another (e.g., on an AIDS list).

In addition, privacy issues are sometime difficult to reconcile, as they are often balanced against competing interests like law enforcement, the public interest and – in the service delivery context – convenience and efficient program delivery.

This section examines the key privacy challenges to establishing a Pan-Canadian IdM&A framework. These challenges include:

1. The need to balance the convenience of cross-jurisdictional seamless service delivery and IdM&A requirements with privacy requirements (i.e., data sharing limitations);
2. The fact that privacy means different things to different people and the value one attaches to privacy changes over time;
3. Citizen concerns about profiling and tracking (i.e., big brother);
4. Emotional issues about identification and assigned identifiers; and,
5. The lack of available and commonly used Privacy Enhancing Technologies

4.2.4.1 Difficulty balancing cross-jurisdictional seamless service delivery and IdM&A requirements with privacy requirements (i.e., data sharing limitations)

Surveys and studies conducted on sharing client information for the purpose of providing better, quicker and more seamless service experience indicate that while clients want convenience, they also want assurance that their privacy is protected.

Achieving both seamless service delivery – which is generally understood to involve more information sharing – and privacy protection – which is generally understood to involve less information sharing – requires a delicate balance and creative solutions. For example, it is likely that identity information can be shared in many cases across departments and jurisdictions for the purpose of providing a seamless, multi-channel service delivery experience, but it must be done in a controlled way and with the knowledge and consent of the client, where appropriate.

There is also a balancing exercise that must occur between authentication requirements and privacy. As the National Research Council in the USA noted “[t]here is an inherent tension between authentication and privacy, because the act of authentication involves some disclosure and confirmation of personal information. Establishing an identifier or attribute for use within an authentication system, creating transactional records, and revealing information used in authentication to others with unrelated interests all have implications for privacy. The many possible impacts of authentication may not be considered by system designers [...] and they may not be appreciated by the public.”³

The Citizens First 4 study indicates that the more knowledge and control citizens have over their information, the more comfortable they are using government Internet sites. In particular, the study indicated that the following conditions contributed to lessening and even overcoming citizens’ privacy and security concerns:

- Client information is protected from unauthorized use;
- Legislation protects the privacy and security of personal information;
- Clients know how their personal information is being used;
- Clients are asked for consent to share information for specific purposes;
- Clients are able to view personal information online; and,
- Clients can contact a government official on line if they have security concerns.

It is likely that some of these same conditions can be employed in the service delivery and IdM&A context to make citizens more comfortable with their personal information being shared for the purpose of receiving more convenient, coherent and seamless services.

Solution analysis:

A legislative and policy scan could be conducted to determine what legislative or policy barriers, if any, exist to sharing personal information for the purpose of IdM&A and providing cross program and cross-jurisdictional seamless service delivery .

The Privacy Component of the IdM&A Framework should set out what privacy requirements (e.g., consent, notification, limits on use) apply to IdM&A processes.

4.2.4.2 Privacy means different things to different people and the value one attaches to privacy changes over time

Because privacy is a very subjective concept, it is difficult to predict how individual clients will react to specific identification and authentication processes and to their personal

³ Stephen T. Kent and Lynette I. Millet (edi.), “Who goes there?: Authentication through the lens of privacy”, National Research Council, 2003, p. 7.

information being shared to facilitate cross-jurisdictional seamless service delivery. Adding to this difficulty is the fact that the value an individual person attaches to his own privacy may change over time or in a different context. The value one attaches to privacy may change for a variety of personal reasons but dramatic changes are commonly caused by a change in circumstance (e.g., celebrity or wealth) or by a traumatic event (i.e., victim of identity fraud, abuse or stalking).

Because one size will not fit all, when it comes to privacy, the best solution to meeting all clients' privacy needs is to provide them with the maximum amount of control over their identity information in terms of how it is used and to whom it is shared; and the maximum amount of choice over their use of service channels. In this way, each client, with full knowledge of the potential benefits and drawbacks, can draw their own line between privacy and convenience.

4.2.4.3 Citizens are afraid of profiling and tracking (big brother) – they want more control over their information

If citizens and businesses don't trust an online service, they won't use it. Therefore, communication with them will be key to the success of any IdM&A initiative. They must be assured that their information is protected and that the goal of the service is to provide a more coherent, seamless service experience - not to profile or track them.

Solution analysis:

Providing citizens with maximum knowledge of, and control over, the uses of their identity information is key to assuaging clients' concerns about profiling and tracking.

Transparency in terms of why information is being collected and how it is to be used will be important as will be the availability of a knowledgeable person who can answer questions about the need for, and the process used to obtain and verify, information.

Government agencies that collect identity information from clients should be prepared to justify their collection and use of that information, both in terms of their legal authority to do so and the specific reason certain information is required.

In addition, policies that clearly limit the use of identity information that is collected for service delivery purposes from being used for other purposes, including profiling and tracking of citizens, would go a long way in mitigating client concerns. Such a policy would of course include law enforcement exceptions, where warranted, but generally speaking clients should be assured that their movements are not being tracked through the use of a global identifier. Wherever possible, only those parties that have a justifiable role in the transaction should be aware of it.

All of these requirements should be addressed by the Privacy Component of the IdM&A Framework.

4.2.4.4 Emotional issues connected to identification and assigned identifiers.

Many citizens experience an emotional reaction to the idea of being required to identify themselves, particularly when they are required to identify themselves in a way that is not their choice or does not hold any meaning to them (i.e., being required to use a number as opposed to their name).

Being identified by a number continues to be a dehumanizing emotional issue for many individuals, just as the idea of being digitally captured, filed, stamped, indexed, fingerprinted, numbered and profiled by de-personalized identification systems is.

In addition, many people fear identification systems because of the threat they pose to civil liberties. There are unfortunately too many historical examples of universal identification systems being used, primarily by totalitarian regimes, to curtail freedoms and create “dossiers” on law-abiding citizens. Phrases such as “your papers, please” continue to conjure negative emotional responses because they remind people of past injustices and raise concerns that, without proper controls and limitations, identification systems could once again be used as surveillance tools.

Solution Analysis:

1. Identification only where justified and necessary.
2. Strict limitations on how identification information used.
3. Personalized communications to clients: While the use of identifying numbers may be necessary to uniquely identify clients and to ensure that the right service is being provided to the right client, wherever possible communications with clients should be personalized (i.e., they should not be addressed by a number, unless it is a self-generated number that the client has asked be used).
4. Sensitivity to this issue and recognition that many clients have no choice but to provide identity information to government in order to prove eligibility for a service. Because they have no choice, they may feel even more negative about the identification process.

The Privacy and Service Management Components of the IdM&A Framework should address the aforementioned issues.

4.2.4.5 Lack of available and well-developed Privacy Enhancing Technologies (PETs)

There are a range of technologies that could ensure the protection of privacy in identification and authentication systems. Unfortunately, these are still poorly known and not yet widely available. There are many reasons for the underdevelopment of (PETs)⁴. First,

⁴ From: *Government of Quebec, “Report on e-government : Connecting Quebec to its Citizens”, Quebec, 2004*

governments' legal frameworks do not require or promote the implementation of privacy-enhancing technologies, so demand is not felt. Second, the development of these technologies is being held back by various market forces in the software industry. The cost of developing and marketing new products specifically for the purpose of privacy protection seems too high for many in this industry. However, the industry will essentially build whatever is demanded so if PETs become a requirement of government, industry will respond.

Solution Analysis:

The Task Force spoke to a number of industry experts at the Workshop it hosted in Montreal and at the Privacy and Security Conference in Victoria about the relative unavailability of Privacy Enhancing Technologies (PETs). All were unanimous in responding that the industry will essentially build whatever the client demands. In other words, the message was that if privacy enhancing technologies are a requirement, government should say so and the industry will respond.

On a related note, the Task Force heard a lot about "User-Centric" Identity Management models and technology which while not specifically PETs, are inherently more privacy enhancing than other IdM&A models due to the ability of users to control the transfer of their identity credentials from one agency to another. While this technology is currently not available, it is under development (e.g., Card Space by Microsoft) and is being considered in some jurisdictions (e.g., British Columbia).

Governments may wish to consider the use of, and pay attention to the development of, "privacy enhancing" or "user-centric" technologies as a way to address privacy and other issues.

4.3 Challenges Associated with Inter-jurisdictional Relations and Trust

Most of the challenges identified in this section were drawn from Dr. Ken Kernaghan's 2003 report or compiled from the Governance Workshop held in Niagara on the Lake. Although the focus of Dr. Kernaghan's report was governance barriers to Integrated Service Delivery, many of the barriers he identified are equally applicable to the establishment of a Pan-Canadian IdM&A framework.

The barriers or challenges identified by Dr. Kernaghan, as adapted by Task Force, can be divided into the following categories:

1. Lack of effective governance and leadership (for both inter-departmental & cross-jurisdictional initiatives);
2. Structural and Administrative Barriers;
3. Cultural Barriers; and,
4. Interoperability and Trust Challenges.

4.3.1 Lack of effective governance and leadership (inter-departmental & cross-jurisdictional)

Lack of effective governance and leadership for both inter-departmental and cross-jurisdictional initiatives can be a non-starter. There are four key issues that contribute to this problem:

- Not all political or senior leaders understand the challenges;
- Individual ministerial accountability conflicts with cross-jurisdictional responsibility and initiatives;
- Reliance on influence rather than authority; and,
- Political visibility issues.

4.3.1.1 Not all political or senior leaders understand the challenges

As stated previously in this analysis, IdM&A is extremely complex and novel. For this reason, not all political or senior leaders understand the challenges to establishing a Pan-Canadian IdM&A framework or fully appreciate what it would take to achieve consistency across jurisdictions. Strong leadership and commitment from the highest level will be necessary to fully realize a Pan-Canadian framework. A pan-Canadian approach to IdM&A needs strong and influential champions.

4.3.1.2 Individual ministerial accountability conflicts with cross-jurisdictional responsibility and initiatives

The individual responsibility (or accountability) of ministers for the conduct of their departments encourages them to focus on the vertical dimension of government. The political motivation of ministers to avoid risk and blame underpins the traditional "silo" design of departments which stand as barriers to the horizontal linkages required for establishing a Pan-Canadian IdM&A framework. Moreover, ministers become increasingly wary as collaborative arrangements cross from the inter-departmental sphere to the inter-jurisdictional and inter-sectoral ones. However, to the extent that ministers prosper politically from effective service delivery by their departments, their individual responsibility encourages them to promote IdM&A *within* their departments.

4.3.1.3 Reliance on influence rather than authority

Barriers to initiatives within a department or even within a jurisdiction can be easier to overcome, especially if there is strong support from senior officials who have *authority* to make things happen. Cross-jurisdictional initiatives, however, generally involve or require the exercise of *influence*. Reliance on influence, persuasion and negotiation is characteristic of horizontal government in general. In the absence of command and compliance, some senior officials will still strive to overcome all obstacles to a Pan-Canadian IdM&A framework and cross-jurisdictional seamless service delivery whereas others will - and can - simply refuse to collaborate.

While Canada has a successful history of implementing cross jurisdictional initiatives built on trust, influence, persuasion and negotiation – rather than authority – that success is dependent on a number of factors. Complex horizontal initiatives are generally dependent on: influential champions; committed leadership; shared purpose and culture; clearly articulated governance and accountability; integrated planning; and ongoing relationship management. Of all of these factors, the most important for the successful implementation of a Pan-Canadian IdM&A Framework, particularly in the start-up phase, is influential champions.

4.3.1.4 Political visibility issues

Both individual ministers and the government as a whole strive to ensure visibility or "profile" in the sense of credit for their financial and other contributions to improved service delivery. Collaboration with other departments and especially with other jurisdictions can blur the relative contributions of the different departments and governments involved. An example of public servants' sensitivity to this important political consideration can be seen in HRDC's commitment to develop a partnership strategy for multi-channel service delivery that will "get the most value and federal presence from our partnerships."⁵ Governments sometimes receive little public recognition for their substantial investment in cross-jurisdictional initiatives. The sharing of resources that accompanies efforts to blend organizational operations and cultures and to project an image of cross-jurisdictional seamless service

⁵ Human Resources Development Canada, *Service Delivery in the New Millennium: HRDC's Service Delivery Policy* (Ottawa: HRDC, 1999), p.12.

delivery sometimes means that one government will contribute most of the resources and receive only half - or even less - of the public credit.

4.3.2 Structural and administrative barriers

Another challenge to implementing cross-jurisdictional initiatives is the continued presence of structural and administrative barriers. These include:

- Departmentalism (Silos);
- Different laws, regulations & policies across jurisdictions;
- The tension between innovation and accountability which may create a risk-averse environment; and,
- Resistance to change.

4.3.2.1 Departmentalism (silos)

The main structural barrier is the departmental model of organization. This constraint is closely related to the ministerial concern about accountability (discussed above) that perpetuates the departmental approach to organizational design. This silo system runs strongly counter to the current movement towards horizontal government and, in particular, to the collaborative arrangements required for cross jurisdictional seamless service delivery and the establishment of a Pan-Canadian IdM&A framework.

The decisions of public servants, like those of their ministers, are greatly constrained by accountability considerations. The challenge for public servants is to maintain an appropriate measure of vertical accountability while supporting horizontal initiatives for which the lines of accountability are much less clear. In general, the difficulty and the risk increase as collaborative efforts go beyond inter-departmental arrangements to inter-jurisdictional ones.

4.3.2.2 Different laws, regulations policies and levels of understanding across jurisdictions

A Pan-Canadian IdM&A strategy must comply with a variety of legislation, policy and best practices across jurisdictions. While privacy legislation and related policy is similar across Canadian jurisdictions, there are, nevertheless, some key differences. In addition, some jurisdictions have sector or program specific legislation that may limit the use or sharing of certain information. To the extent that such limitations may impose legal impediments to the sharing of information for the purpose of identification or authentication, they must be identified.

Solution Analysis:

The Legal Component should set out where laws, regulations and policies that impact IdM&A differ across jurisdictions and what that may mean in terms of implementing cross-jurisdictional IdM&A and service delivery. As well, legal and policy barriers common or unique to jurisdictions should be identified.

4.3.2.3 The tension between innovation and accountability may create a risk-averse environment

Another challenge is that there is tension within individual departments between the need to hold public servants accountable and the need to promote innovative approaches to IdM&A and cross-jurisdictional seamless service delivery. Before HRDC's grants and contributions crisis in 2000, local offices of the department enjoyed enough discretionary authority to undertake innovative Integrated service delivery initiatives, including, for example, the celebrated Livingston Centre in Tillsonburg, Ontario. The fallout from the crisis has been a risk-averse milieu requiring stricter adherence to rules and thereby discouraging innovation. A different aspect of the accountability issue can be illustrated by the case of Department A using information provided by Department B to answer a client's question incorrectly. Is this the fault of Department B for not providing clear information or of Department A for not understanding the information?

4.3.2.4 Resistance to change (Tunnel vision and turf tension)

A strong organizational culture can be conducive to intra-departmental initiatives but it can also be a major barrier to the blending of organizational cultures required by many service delivery arrangements that extend across departments and jurisdictions. Long experience working in silos under strict accountability requirements creates a culture of tunnel vision rather than the peripheral vision needed for horizontal government. This tunnel vision is often accompanied by turf tension as individuals and organizations strive to protect established mandates and processes, in part by restricting the sharing of information. These barriers can be exacerbated by the absence of incentives and a culture of innovation supporting creative efforts to pursue cross-jurisdictional seamless service delivery.

Since values are the essence of organizational culture, it is essential to cultivate shared commitment to those values, such as citizen-centred service, trust, teamwork, leadership and accountability that are most likely to support cross-jurisdictional initiatives. It is widely acknowledged, however, that culture change takes a long time and, therefore, while it should be continuously pursued, it should not be viewed as the shorter-term solution that structural change usually is.

The Modinis report states that “the fact that (working) [IdM&A] solutions cannot be expected to undergo significant changes in the short run stems from the fact that any relatively large scale [IdM&A] infrastructures typically requires a significant investment, both financial and in effort, of its organizers. As a consequence, there is a certain reticence to make any changes that would effectively nullify part of this investment, even if the final result could be an improvement over the original. For this reason, smaller updates (that have no significant impact on the general workings of the system) are possible in the short run, whereas larger shifts in technology or strategy are not” (p. 7).

4.3.3 Cultural barriers

There are also cultural barriers to establishing a Pan-Canadian IdM&A. These may include:

- Different values and mentality across jurisdictions; and,
- Addressing First Nations and immigrant communities' identity concerns.

4.3.3.1 Different values and mentality

Jurisdictions often have distinct perceptions of what is acceptable and what is not acceptable for their respective population. These different perceptions and cultural sensitivities are likely to play a key role in designing a Pan-Canadian solution to IdM&A. Different jurisdictions will have different opinions and expectations about how e-government should impact their lives, including the perceived benefits of specific technical solutions such as biometrics and radio-frequency identification (RFID).

Solution Analysis:

There is currently little information about how cultural sensitivities and different values and mentality affect a person's perception of IdM&A. A public stakeholder engagement process could be used to determine these views.

4.3.3.2 Addressing First Nations and immigrant communities identity concerns

Issues of concern to First Nations and immigrant community groups have not been specifically addressed in this report. However, it is acknowledged that they require consideration in future stages of the Pan-Canadian IdM&A strategy.

It is important to note that the Task Force did meet with representatives from Indian and Northern Affairs Canada and learned that they have developed a strong cooperative working relationship with First Nations people on IdM&A activity (e.g., enhancements to the Indian Status Card program). Their knowledge, experience, and processes could be leveraged in future stages of the Pan-Canadian IdM&A strategy, particularly with respect to stakeholder engagement.

Solution Analysis:

Consultation process with First Nations and immigrant communities, leveraging existing processes established by organizations such as Indian and Northern Affairs Canada.

4.3.4 Problems of interoperability and trust

The Modinis Report notes that "any solution that requires [IdM&A] systems to interconnect and exchange data [...], is strongly dependant on the reliability and trustworthiness of every single data provider [...]. This is an important issue, as a service provider needs to be able to assess the procedures used for the issuance and management of credentials, in order to

determine whether the outcome of an entity authentication procedure is sufficiently reliable to allow a user access to its service.” (p. 14.)

This statement is certainly applicable to the establishment of a Pan-Canadian IdM&A framework and is validated both by the results of the environmental scan and our discussions with stakeholders. The following three issues contribute to the interoperability and trust challenges:

- No common language and lexicon and no common principles;
- No common policies, models, processes and standards; and,
- Apprehension by municipalities that IdM&A costs will be unilaterally downloaded.

4.3.4.1 Lack of common principles, understanding and language (lexicon)

The environmental scan conducted by the Task Force clearly revealed a lack of common principles, understanding and language across jurisdictions in the IdM&A space. There is a lack of common understanding even with the most basic terms such as identity, identification and authentication. And, we are far from a consensus on what attributes (i.e., name, address, age, profession, etc.) define or constitutes identity in Canada. The environmental scan clearly demonstrates this challenge.

Without common understanding of terms and principles, it is very difficult for jurisdictions to move forward with, and engage in, the development of a pan-Canadian IdM&A framework. Without this common ground, jurisdictions are constantly diverted from the task at hand to debate the meaning of terms and the relative importance of fundamental principles.

Solution Analysis:

The development of a Pan-Canadian IdM&A Framework should be guided and defined by common principles and a common lexicon.

4.3.4.2 Lack of common policies, models, processes, standards and architecture

Inter-operability is usually discussed in the context of technological barriers to electronic service delivery, resulting from the incompatibility of technologies across departments and particularly across governments. However, inter-operability is a broader issue that presents several problems for cross-jurisdictional service delivery that do not lend themselves easily to technological solutions. Formidable managerial and operational difficulties can arise from differences between partners in respect of laws, policies, rules, regulations and standards.

The environmental scan conducted by the Task Force revealed that while jurisdictions have some policies, models, processes and standards in common, they were not universally common or common in all respects. As an example, there are currently:

- no universally accepted standards in Canada for issuing documents to prove identity (although a great deal of work has been done towards standardization in some sectors, such as Vital Statistics and Driver Licensing)
- No universally accepted identity proofing standards or processes;

- No common policies or standards on what attributes should be used to identify an individual or a business;
- No common semantic and syntactic models, and,
- No common trust and assurance models.

Solution Analysis:

The development of a Pan-Canadian IdM&A Framework will guide the development of common standards, policies and models.

4.3.4.3 Apprehension by municipalities that IdM&A costs will be unilaterally downloaded

There is an apprehension or perception of risk by municipalities that jurisdictions may decide to unilaterally download IdM&A-related costs to municipalities such that municipalities would then be in the untenable position of having to foot capital/operating costs that were not considered as part of the municipalities' annual budgeting processes.

Solution Analysis:

The establishment of trust/cooperation and agreed-to protocols regarding inter-jurisdictional cost-sharing arrangements to be enforced through: Memoranda of Understanding (MOUs), Service Levels Agreements (SLAs), Operating Level Agreements (OLAs), contracts, written agreements and protocols that govern cost-sharing across jurisdictions.

5.0 Strategy and High-Level Recommendations

The Task Force conducted a detailed solution analysis of the key challenges hindering the establishment of a Pan-Canadian IdM&A Framework. This analysis was then rolled up into six high level recommendations that form the foundation of the overall Strategy.

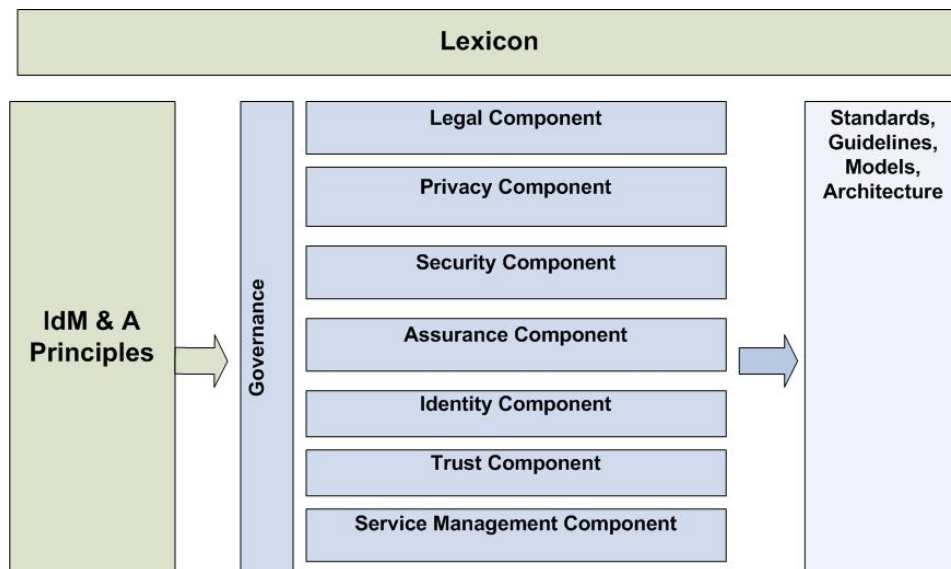
5.1 Pan-Canadian IdM&A Framework

The Task Force recommends the endorsement of the Pan-Canadian IdM&A Framework it developed to address key issues identified in its problem analysis such as the need for:

1. Common language and principles;
2. Clarity on legal authorities and restrictions that impact IdM&A;
3. Clarity on privacy issues and requirements;
4. Clarity on security requirements and the need for common standards;
5. Common or equivalent standards on identity assurance levels, registration, identity-proofing and authentication processes;
6. Common or equivalent identification standards for clients and their delegates that take into consideration the different contexts that clients operate in (i.e., citizen, business)
7. Processes and models for establishing trust between the different parties and jurisdictions involved in an identification or service delivery process; and,
8. Interoperable service management processes and models.

Figure 6, below, is a reference model for the entire IdM&A Framework which illustrates the various components of the framework (i.e., Legal, Privacy, Security, etc.) and the importance of the IdM&A Principles in guiding the framework and the Lexicon in defining the framework. The reference model also depicts how the various components of the framework will guide the eventual development of common standards, models, guidelines and architecture.

Figure 6. Pan-Canadian IdM&A Framework



The complete Pan-Canadian IdM&A Framework, with recommendations on what should be addressed in each component, is included in the Annex to this report. The following descriptions provide a brief overview of the purpose and scope of each component in the IdM&A Framework:

A. Lexicon – A list of common IdM&A terms and definitions.

B. IdM&A Principles – A cohesive set of identity management norms and rules that guide and constrain the formulation of frameworks, models, policies, standards and solutions. The Task Force seeks endorsement of the following principles:

Principle 1:	Justifiable and Proportionate
Principle 2:	Client Choice, Consent and Control
Principle 3:	Limited Information for a Limited Use
Principle 4:	Client-focused, Consistent Experience
Principle 5:	Diversity of Identity Contexts and Systems
Principle 6:	Trusted and Secure Environment
Principle 7:	Transparency and Accountability
Principle 8:	Enduring solution

C. Governance – The body and rules that will govern the continued development of the IdM&A Framework and associated activities such as capacity building and development of pilot projects.

D. Framework Components:

- 1. Legal Component:** The set of laws, legislation, regulations and authorities that govern identity management and authentication within Canada.
- 2. Privacy Component:** The context within which privacy requirements are applied to identity management. This component includes issues such as Privacy Impact Assessments, notification and consent, limiting collection, use and disclosure of identity information, client control of identity information, and accuracy, access and accountability. This component also contains recommendations on next steps that would lead to the development of standards and guidelines for ensuring privacy of identity management services.
- 3. Security Component:** The context within which security requirements are applied to identity management. The security component includes issues such as setting up an environment that engenders trust, the adoption of common security standards (e.g., ISO/IEC 27002:2005), security threat and risk assessments, the

predetermination of Transaction Trust Levels based on the security classification of information, processes for auditing and monitoring compliance and detecting and responding to incidents, and a robust and effective security awareness training program. Standards for ensuring the security of identity management services would flow from this component.

4. **Assurance Component:** Sets out the notion of the Identity Management, Authentication, and Authorization “chain of trust” and establishes that there are general gradients of assurance for each component of the chain. This component proposes a Pan-Canadian Assurance Model that establishes different levels of assurance through a combination of different levels of registration and identity-proofing processes and different levels of credential strength, all supported by a securely managed underlying infrastructure. Standards on acceptable registration channels, verification processes, evidence of identity and authentication factors would flow from this component.
5. **Identity Component:** Sets out different identity contexts or user groups (i.e., citizen, business, employee), and the identifiers or identity attributes that could apply to each. The identity component also addresses the different types and requirements for agency, dependants and designates/delegates. The identity component sets the basis for a generic, semantic model of information associated with identity management services – essentially a conceptual data model. Semantic and syntactic standards would flow from this (i.e., interoperability of identity management services will hinge strongly on common information standards) as well as other policy and standards.
6. **Trust Component:** Sets out the essential requirements for the establishment of trust relationships between parties involved in IdM&A services. It essentially deals with how one party can trust another party’s identity assertions. This component also sets out the different trust roles involved in assuring identity claims and in issuing and accepting credentials (e.g., relying party, authoritative party, etc.) Standard templates and language for trust agreements could flow from this component as could the development of transparent processes on defining liability, decision-making, and audit and compliance.
7. **Service Management Component:** The context within which service requirements like consistent user experience, intuitive, predictable processes, and clear understandable language are applied to identity management. This component could lead to the development of common service and functional models and standards for clear interfaces and controls and options that enhance the client’s experience.

5.2. Pilot Projects

The Task Force recommends the use of pilot projects to begin addressing significant IdM&A barriers and to verify the applicability of the aforementioned IdM&A Principles and Framework.

Given the early stage of the Pan-Canadian IdM&A Framework and the complexities involved in setting up inter-jurisdictional IdM&A processes and trust relationships, the Task Force recommends that pilot initiatives be used in an incremental manner:

- to test and refine the Framework;
- to ensure that the Framework is, and continues to be, of practical value to collaborating partners; and
- to demonstrate the value of the Framework in real service situations.

The Task Force has, therefore, identified a number of smaller targeted pilot projects whose main objective is to provide practical short-term results by testing one or more elements of the Framework, identifying gaps, building understanding, and informing governance. A description of these pilot opportunities and their expected outcomes can be found in **Appendix E**.

Early pilots will involve inter-jurisdictional initiatives that lay the foundation for bundled transactions requiring authentication; and implement, and report on, a range of new business processes involving data sharing, and shared or leveraged identity-proofing and authentication processes. These early pilots will be self-funded and governed bilaterally, with partner jurisdictions committing to using the Framework to the extent possible, to build capacity, transparency and trust. While some of these initiatives would likely have gone forward without the involvement of the Task Force, the key difference is that jurisdictions involved in pilot projects will commit to the sharing of their experiences and lessons learned with other jurisdictions and with the governing structure overseeing the continued development of the Pan-Canadian IdM&A Framework.

As the Framework improves and becomes more robust, with the addition of standards, guidelines and tools, future pilots will test these new standards and guidelines. As well, several proposed pilots are conceptual in nature. Their purpose is to think through new ideas on how to achieve the longer term vision. Ultimately, one all-encompassing pilot may test the complete IdM&A Framework across all jurisdictions, much like Canada Health Infoway did for electronic health records.

5.3 High-Level Recommendations

In addition to endorsing the above framework and utilizing pilot projects to test and inform the framework, the Task Force also recommends building knowledge, innovation and capacity in IdM&A; developing a sustainable funding model; stakeholder engagement; and the adoption of the Task Force's Vision and Value Proposition, Action Plan and proposed Governance Model.

The Task Force recommends that the Deputy Ministers Responsible for Service Delivery across Canada approve the following six high level recommendations and associated Action Plan (set out in Chapter 7):

Recommendation 1: Increase Knowledge, Innovation and Capacity

To increase knowledge, stimulate innovation, and build capacity for IdM&A within governments who are seeking to enhance service delivery the Task Force **recommends**:

- a. The recognition of IdM&A as its own discipline, related to, but broader than and distinct from, Privacy, Security and Service Delivery. As such, it requires broad engagement of the public sector (Deputy Ministers responsible for Service Delivery need to join forces with their colleagues that have responsibility for IdM&A in other sectors). Together these Deputies should lead and encourage the development of a strong knowledge base to address emerging and existing identity management and authentication issues through the engagement of the broader government sector, the private sector and academia.
- b. The increased exchange and sharing of information, ideas, new technologies and solutions, use cases and best practices across departments and between jurisdictions to improve and leverage the level of IdM&A expertise within governments across Canada.
- c. The integration of IdM&A curricula in education and training programs for government employees, in cooperation with key stakeholders such as government human resource development agencies and higher education institutions.

Recommendation 2: Pan-Canadian IdM&A Framework

To address the unique challenges associated with identifying and authenticating clients, and to increase consistency, interoperability and trust across and between jurisdictions in processes relating to IdM&A, the Task Force **recommends**:

- a. The endorsement of the Task Force's IdM&A Principles, Lexicon, and Framework (illustrated and defined in the Annex) by all jurisdictions as a starting point for the implementation of a Pan-Canadian IdM&A Framework.
- b. The completion of the Pan-Canadian IdM&A Framework components, including the development of common or interoperable policies, models, standards, processes, and architecture flowing from each of the framework components.
- c. The testing and implementation of the Pan-Canadian IdM&A Framework across jurisdictions.

Recommendation 3: Pilot Projects

To concretely address the further development and completion of the Pan-Canadian IdM&A Framework, the Task Force **recommends**:

- a. An incremental approach to the implementation of pilot projects where early pilot projects (set out in **Appendix E**) are smaller in scope and self-funded and governed. Jurisdictions involved in these early pilot projects commit to applying the IdM&A Framework, reporting back on its usefulness, and making recommendations for improvement in a timely manner to the appropriate governance body. The main objective of these early pilots is to provide practical short-term results by testing one or more elements of the Framework, identifying gaps, building understanding, and informing governance.
- b. The capturing and dissimulation of experiences and lessons learned from the early pilot projects to help inform the further development and refinement of the IdM&A Framework, governance, standards, guidelines, models, and future pilot projects.
- c. The conceptualization and development of a broader pilot project whose prime objective is to test the complete Pan-Canadian IdM&A Framework, a sustainable funding model (see Recommendation 4) and next generation IdM&A processes and technology (e.g., user-centric) with the participation of at least one federal department, one provincial department and one municipality.

Recommendation 4: Sustainable Funding

To increase financial and material resources necessary for inter-jurisdictional initiatives that aim to enhance seamless, cross-jurisdictional, multi-channel service delivery, the Task Force **recommends**:

- a. The development of a sustainable funding model, that provides clear economies of scale for all participating jurisdictions in the implementation of the Pan-Canadian IdM&A Framework.

Recommendation 5: Stakeholder Engagement

In recognition of the highly sensitive nature of IdM&A in a service delivery context and the importance of validating, promoting and increasing awareness of IdM&A in order to build trust amongst governments, stakeholders and clients, the Task Force **recommends**:

- a. A constructive engagement process with key government stakeholders (e.g. Privacy Commissioners, Vital Statistics Agencies, key government service providers, etc.) to validate the Pan-Canadian IdM&A Principles and Framework and to increase awareness of IdM&A issues and solutions, generally.

- b. A public stakeholder engagement process with private sector experts, academia and the general public, to validate, and build acceptance for, the Pan-Canadian IdM&A Principles and Framework.
- c. A general public awareness process to build client knowledge, trust and comfort with IdM&A processes and increase the demand for multi-channel cross-jurisdictional service delivery initiatives, utilizing consistent and protected IdM&A processes.

Recommendation 6: Proposed Governance and Next Steps

To oversee the continued work on IdM&A between jurisdictions, the implementation of the previous five recommendations – in particular the continued development and completion of a Pan-Canadian IdM&A Framework – and to improve the governance and leadership for inter-jurisdictional and horizontal initiatives, the Task Force **recommends**:

- a. The adoption of the Task Force’s Vision and Value Proposition (set out in Chapter 3) establishing common ground for further work on IdM&A between jurisdictions in Canada.
- b. The adoption of the proposed governance strategy, structure and recommendations set out in Chapter 6.
- c. The adoption of the Action Plan set out in Chapter 7 to operationalize the recommendations and take concrete steps towards achieving the overall vision and strategy.

6.0 GOVERNANCE RECOMMENDATIONS

Governance is a challenge when pursuing work between jurisdictions for a number of reasons that have been well-documented in Section 4.3 – Challenges Associated with Inter-jurisdictional Relations and Trust. These challenges are even greater when jurisdictions have different levels of maturity and capacity, as is the case with IdM&A.

Jurisdictions operate under different mandates, structures, contexts, and capacities when engaging in any inter-jurisdictional initiative. However, without the capacity to make collective decisions through a fair and transparent process, none of the benefits of taking a collective approach to a shared problem, such as IdM&A, can be achieved. A Pan-Canadian governance structure is necessary to provide this shared problem-solving capacity.

There is also a need for the proposed governance structure to acknowledge and align with existing collaborative structures, such as the PSSDC and the PSCIOC (and their associated sub-committees). The Joint Councils, as they are collectively known, are the key collaborative bodies in service delivery and information management/information technology for governments across Canada. The Joint Councils informed the Deputy Ministers in the fall of 2006 about the creation of its new committee, the National Committee on Information Management and Authentication (NCIMA). The PSCIOC also has two sub-committees, the Privacy Subcommittee and the National CIO Subcommittee on Information Protection (NCSIP), whose expertise and established contacts in Privacy and Security should be leveraged.

Finally, any proposed governance model requires active and effective participation from all stakeholders that have a critical role in IdM&A in each jurisdiction.

6.1 Analysis of Governance Models

As a first step to determining the best governance model to move ahead on the implementation and use of the Pan-Canadian IdM&A Framework, the Task Force organized a workshop on governance to explore challenges and possible models. Representatives from Canada Health Infoway, Interac, and the Canadian Council of Motor Transport Administrators were invited to present an overview of their governance structure and to share critical success factors, challenges and lessons learned. A summary of the workshop results and of the governance models that were evaluated can be found in **Appendix F**).

Coming out of the workshop, the Task Force, with the assistance of workshop participants, identified six critical success factors upon which an IdM&A governance model should be built:

- **Leadership** throughout each of the partnering jurisdictions and political buy-in.
- **Flexibility and evolution:** A structure that starts small and evolves will allow its members to influence its direction.
- **Clear vision** that is inspirational and which markets the need for IdM&A.

- **Core principles** for the governance framework.
- **Stakeholder engagement** to develop trust and encourage buy in.
- **Sustainable funding and support** for the governance organization.

6.2 Governance Strategy - Direction from Steering Committee

As the strategy and action plan were developed, the Steering Committee members were canvassed on their views about outstanding issues relating to governance. The following summary reflects the consensus opinions from the Steering Committee on the direction the Task Force should take in developing a governance strategy and proposing a governance structure.

The Task Force should only recommend as much governance as is required, focusing on the work that needs to be governed (e.g., the development of standards and the implementation of the framework, etc.). This direction is consistent with the aforementioned critical success factor about flexibility and evolution. The governance structure should start out small and evolve over time as the organization's mandate and strategic objectives change or evolve. This ensures that the governance structure is designed for effectiveness and also permits members and stakeholders to influence its evolution.

The strategy should take a “soft governance approach”. For example, the governance body should be empowered to make decisions on the development of standards, tools and guidelines but not to impose them on jurisdictions just because those jurisdictions participate in, and support, the governance process. Jurisdictions should have the latitude to decide timing and scope for implementation of standards and tools for themselves. The alignment process will take some time and many jurisdictions will need support.

Participation in the governance structure will require active commitment and financial support. There will be a need to invest in one or two full time positions to support the governance structure and to keep processes moving (by, among other things, tapping into the broader network of stakeholders with an interest and/or expertise). This direction is consistent with another critical success factor raised at the governance workshop – sustainable funding and support. The governance structure must be properly funded and properly supported in order to be successful.

With respect to membership in the governance structure, each jurisdiction should be able to decide on how they can best participate. However, the governance structure will require senior representatives at the table, but not so senior that they are always forced to delegate. It will be key to have mandated representatives at the governance table – people well plugged in to their home jurisdiction and able to speak on behalf of that jurisdiction.

Leadership from a “coalition of the willing” is key (this is essentially what the Task Force has been) but some element of representation from other jurisdictions would be helpful even if they are not among the group most anxious to move ahead. The governance structure will need someone looking at, or providing advice on, issues of extensibility.

The model of two lead provinces (i.e., as Co-chairs) has worked well on the current Task Force. This is a model that could be carried forward to the new governance structure but it will be important to maintain regional representation. A combination of permanent and rotating membership might help to address representational issues – permanent members at the table could “pay to play” while others rotate in and out.

The mandate of the governance structure should be specific, defining critical year one priorities that will give necessary traction and put a timeline on delivery that will be relevant. As well, it is important for building momentum to engage Ministers with the first round of key deliverables. This will also illustrate leadership support, another critical success factor.

It will be important to validate proposed standards with a number of different stakeholders (e.g., MISA, industry experts, PSCIOC, PSSDC). Regular updates to the Joint Councils are also important. This direction is consistent with the critical success factor of stakeholder engagement. To be successful, the governance structure should engage key stakeholders early and engage them often.

While the initial set of proposed pilot projects do not require pan-Canadian governance, it is critical that the bilateral governance they do have is committed to sharing information and lessons learned with the Pan-Canadian governance structure. Those experiences and lessons learned will be critical to developing and refining standards that work and address key problems.

Finally, the engagement of a standards setting body like the Canadian Standards Association and/or procurement opportunities for the development of IdM&A standards should be considered.

6.3 Governance Recommendations

This section contains recommendations for the establishment of an Inter-jurisdictional IdM&A Action Committee to implement the strategy and action plan proposed by the Task Force. As the Task Force’s work ends in July of 2007, and the Deputy Ministers will not meet until November 2007, this section also contains interim recommendations to ensure that core work and general momentum continues until November.

6.3.1 *Create an Inter-jurisdictional IdM&A Action Committee*

To implement the above governance strategy and as an incremental step towards a long-term governance structure, the Task Force recommends:

- The creation of an **Inter-jurisdictional IdM&A Action Committee (IJAC)**.

The Inter-jurisdictional IdM&A Action Committee (IJAC) will ensure the continuation of the Task Force’s work, with a mandate to achieve concrete progress on key deliverables within a defined time period (e.g., 18-24 months), providing only as much governance as is required to achieve its strategic objectives.

Key deliverables (including the validation of the IdM&A Framework and the development of standards) and related timeframes are set out in the Action Plan.

At the end of its term, IJAC will propose a long-term governance structure for the continuing governance of the Pan-Canadian IdM&A Framework and related activities.

To support IJAC, participating jurisdictions must commit:

- To sharing costs;
- To mandating their representative on IJAC with the authority to make decisions from a Pan-Canadian perspective; and,
- To bringing forward deliverables for review and consideration by political leadership.

6.3.2 Continue Momentum – Interim Governance (August to November 2007):

Success of the Pan-Canadian IdM&A Strategy will be contingent on the ability of the Inter-jurisdictional IdM&A Action Committee (IJAC) to hit the ground running following approval of the Task Force's recommendations at the Deputy Minister's November 2007 meeting in Halifax. Therefore, the Task Force recommends for the interim:

- That the Task Force Steering Committee immediately re-constitute itself as an interim governance committee, from August to November 2007. (The full-time dedicated Task Force Working Group will still disband at the end of July 2007).
- That work continue on formulating a detailed budget and proposal for the set up of IJAC; discussing business requirements for proposed pilot projects; and validating the IdM&A Framework with internal stakeholders. A detailed governance proposal and updates on pilot discussions will be presented to the Deputy Ministers at the November 2007 meeting in Halifax, where they will be asked to approve the Task Force's recommendations and action plan.
- That expert resources in each jurisdiction continue to be available to the Steering Committee during this interim period for consultation and engagement in the aforementioned priorities.

6.3.3 Interim Funding Needs (September – November 2007)

To support the work that the Steering Committee, as the Interim Governance body, must do between September and the Deputy Minister's meeting in November, the Task Force recommends:

- That the Deputy Ministers commit, on the September teleconference call, to jointly contribute \$50K to support the production of a detailed proposal for the set up of the IJAC, including terms of reference, strategic planning with clear priorities, and an operating budget. The funding amount of \$50K is for business analyst support, meeting expenses, translation services and other miscellaneous expenses as may arise.

- That the interim budget of 50K be recovered from jurisdictions using a formula similar to that employed to fund the Task Force. The formula and the contribution amounts by jurisdiction is set out below:

Interim Budget: \$50K

- A. Federal Government contributes 33%: \$16,500.
- B. Provinces and Territories contribute a percentage of the balance (\$33,500) to be determined based on a base amount of \$1000 and a percentage of the distribution of the population figures (StatsCanada – October 1, 2006)
<http://www.statcan.ca/Daily/English/061221/d061221d.htm>
- C. Municipalities, through the Municipal Information Systems Association (MISA), would contribute the base amount of \$1000.

Jurisdiction	% of Population	Base Fee	% Share	Total
Newfoundland and Labrador	1.56%	\$1,000.00	\$303.23	\$1,303.23
Prince Edward Island	0.42%	\$1,000.00	\$82.57	\$1,082.57
Nova Scotia	2.85%	\$1,000.00	\$556.56	\$1,556.56
New Brunswick	2.29%	\$1,000.00	\$445.90	\$1,445.90
Quebec	23.43%	\$1,000.00	\$4,569.09	\$5,569.09
Ontario	38.87%	\$1,000.00	\$7,579.38	\$8,579.38
Manitoba	3.60%	\$1,000.00	\$702.12	\$1,702.12
Saskatchewan	3.01%	\$1,000.00	\$587.35	\$1,587.35
Alberta	10.43%	\$1,000.00	\$2,033.67	\$3,033.67
British Columbia	13.22%	\$1,000.00	\$2,578.20	\$3,578.20
Yukon	0.10%	\$1,000.00	\$18.56	\$1,018.56
Northwest Territories	0.13%	\$1,000.00	\$24.98	\$1,024.98
Nunavut	0.09%	\$1,000.00	\$18.38	\$1,018.38
Canada (33%)		\$16,500.00		\$16,500.00
MISA Canada		\$1,000.00		\$1,000.00
Total	100.00%	\$30,500.00	\$19,500.00	\$50,000.00

6.4 Proposed Governance Structure and Mandate

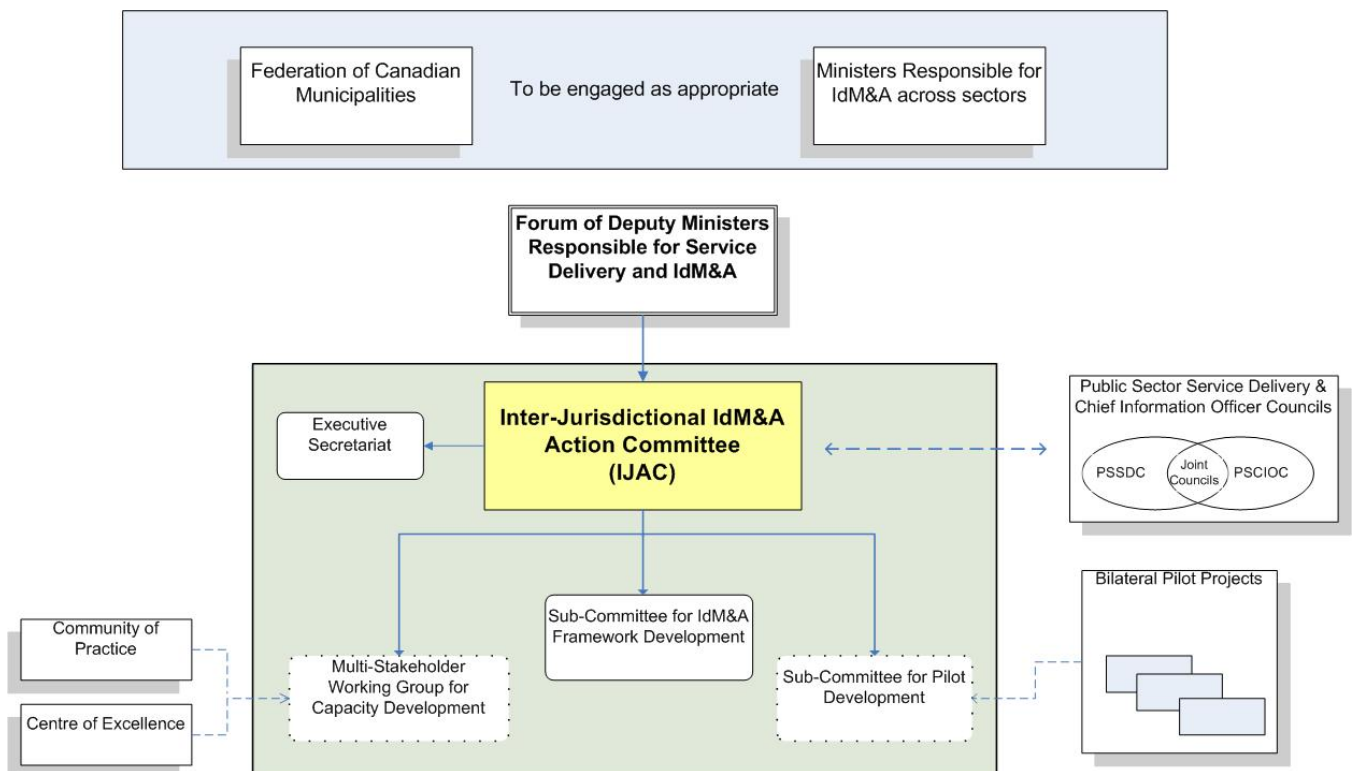
This section sets out the proposed governance structure, mandate and accountabilities of the Inter-jurisdictional IdM&A Action Committee (IJAC) and its subcommittees and working group.

As set out in the above strategy, governance will focus only on those actions that need to be governed, specifically framework and standards development, with a “light touch” on elements that can be primarily self-governing but may need some initial set-up help and mechanisms to report results of interest (e.g., the Community of Practice and the bilateral pilot projects)

The Task Force proposes one main governance body, the “Inter-Jurisdictional IdM&A Action Committee (IJAC)” with having overall responsibility for implementing the approved recommendations and actions lines. The IJAC will have the authority to develop standards but not to impose them on jurisdictions. Jurisdictions will have the latitude to adopt standards according to a schedule that suits them.

Neither the IJAC nor the proposed Sub-committee for Pilot Development will have authority over the initial set of pilots proposed by the Task Force. Pilot activity will be controlled and managed exclusively by the jurisdictions participating in the pilot through the use of bilateral agreements. However, the IJAC may mandate the Sub-committee for Pilot Development to develop a mechanism for capturing and reporting on successes, lessons learned and recommendations from each pilot in order to inform the further development of the IdM&A Framework and future pilot projects.

Figure 7. Inter-jurisdictional IdM&A Action Committee: Proposed Governance Structure



As illustrated in Figure 7, above, IJAC will report to a Forum of Deputy Ministers responsible for Service Delivery and IdM&A.

It is recommended that the current Forum of Deputy Ministers responsible for Service Delivery be expanded to include other Deputy Ministers responsible for IdM&A activities such as Vital Statistics, Citizenship and Immigration, Border Security, Criminal Justice, Health and Driver Licensing. This broader set of responsibilities will be necessary to align efforts (e.g., standard development) across sectors and make real progress towards a true Pan-Canadian IdM&A framework.

To ensure political support and leadership for this effort, the Deputy Ministers should engage Ministers responsible for IdM&A and the Federation of Canadian Municipalities as, and when, appropriate. For example, when appropriate material is available, the Forum of Deputy Ministers responsible for Service Delivery and IdM&A should recommend a venue for a Pan-Canadian conference of Ministers responsible for IdM&A in order to get political approval.

The mandate and accountabilities of IJAC and its sub-committees and working group are outlined below.

6.4.1 *Inter-Jurisdictional IdM&A Action Committee (IJAC)*

The IJAC is accountable to the Deputy Ministers responsible for Service Delivery and IdM&A across Canada and is responsible for the realization of the high level recommendations in the Strategy and for the implementation of the Action Plan set out in Chapter 7.

The IJAC will replace the current Task Force Steering Committee as the governance body responsible for the development of the Pan-Canadian IdM&A strategy and framework, and will be supported by a Secretariat to co-ordinate activities and manage relationships and progress. IJAC may also be supported, at its discretion, by three sub-committees or working groups:

1. Multi-Stakeholder Working Group for Capacity Development
2. Sub-Committee for IdM&A Framework Development
3. Sub-committee for Pilot Development

Mandate and Accountabilities

The IJAC will have the authority to:

- Complete and develop the Pan-Canadian IdM&A Framework and standards but not impose them;
- Make decisions on behalf of the jurisdictions they represent;
- Create working groups and subcommittees as needed.

Responsibilities

The IJAC will be responsible for:

- Implementing the Strategy and Action Plan.

- Overseeing the set up of the Community of Practice and Centre of Excellence.
- Overseeing the set up of constructive dialogue processes across jurisdictions with key stakeholders to validate and move committee work forward.
- Overseeing the continued development and completion of the IdM&A Framework, including standards development.
- Setting priorities for standard development.
- Preparing strategic and operational plans for the approval of the Deputy Ministers responsible for Service Delivery and IdM&A.
- Reporting progress, decisions and next steps to Deputy Ministers on a biannual basis.
- Proposing, monitoring, allocating and reporting on its Operating Budget.
- Hiring secretariat staff and consultants as necessary.
- Proposing, at the end of its term, a long-term governance model for the Pan-Canadian IdM&A Framework and pilot projects.

6.4.2 Multi-Stakeholder Working Group for Capacity Development

This working group is responsible for coordinating activities associated with building capacity, increasing knowledge, and stimulating innovation in IdM&A across government sectors to better address the growing needs of both government organizations and citizens. This multi-stakeholder working group should contain members from multiple government sectors that have an interest in IdM&A (e.g., service delivery, vital statistics, criminal justice, citizenship and immigration, driver licensing, etc) to ensure a broad range of views and to align the work happening across sectors in IdM&A.

This working group is also responsible for liaising with the Community of Practice and Centre of Excellence but not for their governance.

Responsibilities

- Building the necessary bridges across government sectors (i.e., between service delivery departments and other government agencies with a key interest in standardizing and improving IdM&A processes) to share knowledge, align activities and realize opportunities for collaboration.
- Coordinating the set up of the Community of Practice and, eventually, the Centre of Excellence.

- Liaising with the Community of Practice and the Centre for Excellence to gather, and assist in the dissemination of, information, ideas, new technologies and solutions, use cases and best practices with respect to IdM&A.
- Liaising with human resources departments and higher educational institutions to develop an IdM&A curriculum and tool kit that can be integrated into education and training programs for government employees.
- Developing an educational and formative tool kit for the general population to build citizen knowledge, trust and comfort with IdM&A processes and to increase the demand for multi-channel cross-jurisdictional service delivery initiatives, utilizing consistent and protected IdM&A processes.

6.4.3 Sub-Committee for IdM&A Framework Development

This sub-committee is responsible for coordinating activities related to validating and advancing the framework and to developing standards and interoperable processes necessary to enhance trust among jurisdictions, stakeholders and clients engaging in IdM&A processes.

Jurisdictions would continue to have the responsibility to decide timing and scope for implementation of standards and processes for themselves.

Responsibilities

- Engaging key government stakeholders in a dialogue to validate the IdM&A Principles, Lexicon and Framework and determining priorities for next steps.
- Liaising with the Joint Councils' National Committee on Identity Management and Authentication (NCIMA)
- Utilizing the validated IdM&A Principles, Lexicon, and Framework as a starting point for the development of Pan-Canadian IdM&A standards, guidelines, and processes that address, among other matters, the following issues:
 - Information sharing for the purpose of identifying and authenticating clients across departments and jurisdictions, including the identification of any legislative or policy barriers to information-sharing.
 - The identification of organizations in Canada that are authoritative on specific identity attributes.
 - Standards and tools for establishing trust between jurisdictions, defining liability, assessing risk, and monitoring compliance.
 - Standard templates or language for agreements used to manage trust relationships between jurisdictions.
 - Standards or processes for improving data accuracy and integrity of information that will be used to make identification or authentication decisions.
 - Setting up dispute-handling processes for IdM&A systems and processes.

- Completing and testing the Pan-Canadian Assurance Model as a framework for establishing common processes and enabling inter-jurisdictional identification and authentication processes. The complete model could include:
 - Standards for establishing different Levels of Assurance.
 - Identity proofing standards including acceptable methods of verification, acceptable “shared secrets”, acceptable evidence of identity, and acceptable authoritative parties.
 - Registration standards including acceptable registration channels for different levels of assurance.
 - Credential issuing standards including acceptable credential issuing channels for different levels of assurance.
 - Standards on the relative strength and number of factors required for different levels of assurance (including factors that are unacceptable either because they are too weak or too intrusive).
 - Standards for identifying and authenticating dependants, designates and delegates.
- Liaising with the Joint Councils’ National CIO Subcommittee on Information Protection and Privacy Sub-committee to develop standards, guidelines and risk assessment tools that address the following IdM&A privacy and security issues:
 - Guidelines for assessing the risk of typical transactions and services (based on the sensitivity of the information involved and other risk factors) and mapping those specific transaction types to the appropriate Transaction Trust Level.
 - Guidelines for incorporating notice, consent and access to information requirements into IdM&A systems and processes.
 - Guidelines for incorporating fair information practices, such as limiting the collection, use and disclosure of personally identifying information, into IdM&A systems and processes.
 - Standards for audit and compliance, fraud detection, security breach management, system interrogation facilities and the periodic testing and evaluation of the effectiveness of IdM&A security policies, procedures and practices.
 - The development of a Privacy Impact Assessment and Security Threat and Risk Assessment template for IdM&A initiatives.

6.4.4 Sub-Committee for Pilot Development

This sub-committee is responsible for coordinating activities related to conceptualizing, developing and reporting on pilot projects whose main objective is to test and inform the Pan-Canadian IdM&A Framework.

As stated above, this sub-committee has no authority over the initial set of pilots proposed by the Task Force (**see Appendix E**). However, the sub-committee may be responsible for developing and maintaining a mechanism for capturing and addressing recommendations

and lessons learned from each pilot in order to inform the further development of the IdM&A Framework and future pilot projects.

Responsibilities

- Developing and maintaining a mechanism for capturing and addressing recommendations and lessons learned from each of the early bilateral pilots for the purpose of informing and improving the IdM&A Framework and informing the development of future pilot projects.
- Conceptualizing and developing a broader pilot project whose prime objective is to test the complete Pan-Canadian IdM&A Framework, a sustainable funding model and next generation IdM&A processes and technologies with the participation of at least one federal department, one province and one municipality.
- Identifying and recommending the institutional means (long-term governance structure and other regulatory requirements) necessary for the efficient implementation of the broader pilot project.

7.0 Action Plan

The Task Force's Vision and Strategy are brought to life through this Action Plan. The Action Plan outlines concrete steps towards the long term objective of implementing a Pan-Canadian IdM&A Framework for the purpose of facilitating seamless, cross-jurisdictional multi-channel service delivery for all jurisdictions.

The implementation of the Action Plan will be overseen, in its initial stage, by the Interim Governance Committee (i.e., the Task Force Steering Committee); and, after November 2007, by the Inter-jurisdictional Action Committee (IJAC). The IJAC is also responsible for measuring and reporting on the outcomes of the Action Plan and making adjustments and course corrections where necessary.

The focus of the Action Plan is on the next 18-24 months which is the expected duration of the IJAC. While the realization of some actions lines will extend beyond this period and may take up to four years to complete, the goal of the Action Plan is to establish immediate priorities that can begin right away and provide necessary traction for the longer term activities.

As these action lines are implemented, the differences in maturity and capacity between jurisdictions with respect to IdM&A (particularly for smaller jurisdictions) will need to be addressed.

7.1 Action lines

1. Increase Knowledge, Innovation and Capacity Building

1.A The establishment of a Pan-Canadian IdM&A Community of Practice to facilitate the sharing of ideas, new technologies and solutions, use cases and best practices between jurisdictions and governmental stakeholders.

The Community of Practice would be self-sustaining and self-governed but a relationship for the sharing of information should be established between it and the IJAC.

Responsibility: IJAC

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

- 1.B** The identification of champions across government sectors in each jurisdiction to participate in the proposed Community of Practice above, to promote the value of, and vision for, a Pan-Canadian approach to IdM&A and to encourage engagement in inter-jurisdictional IdM&A initiatives.

The champions will be the key contacts for the sector they represent in their jurisdiction, responsible for providing other jurisdictions and stakeholders with relevant information that relates to the practice of IdM&A in their home jurisdiction.

Responsibility: Deputy Ministers responsible for Service Delivery and IdM&A

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

- 1.C** The establishment of a mechanism for the gathering and dissemination of information, ideas, solutions, use cases and best practices arising out of the Community of Practice.

Responsibility: IJAC

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

- 1.D** The creation of a **Multi-Stakeholder Working Group for Capacity Development** (or similar working structure) to coordinate activities associated with building capacity, increasing knowledge and stimulating knowledge in IdM&A across government sectors. This group would also liaise with the Community of Practice and assist in the set up of a Centre of Excellence for IdM&A.

Responsibility: IJAC

Timeline: Start Up  and Implementation 





2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

1.E The creation of a Centre of Excellence for Identity Management, Authentication and Authorization in partnership with universities and industry leaders.

The creation of the Centre of Excellence would occur much later than the Community of Practice (and may even replace it), allowing time for sufficient expertise to build across Canada.

Responsibility: IJAC







Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q					1Q	2Q	3Q	4Q	Forward

1.F The development of an educational and formative curriculum and tool kit for capacity development in IdM&A with an emphasis on creating a critical mass of qualified and skilled professionals and experts.

Responsibility: Multi-Stakeholder Working Group for Capacity Development

Timeline: Start Up  and Implementation 



2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q							Forward

2. Development and completion of the Pan-Canadian IdM&A Framework and its corresponding components

2.A The creation of a **Sub-committee for Framework Development** (or similar working structure) to complete the Framework and develop common or interoperable policies, models, standards, processes, and architecture. The sub-committee could be comprised of existing committees or it could be a new committee with consultation links to relevant committees and agencies (i.e., sub-committees reporting to the Joint Councils).

Responsibility: IJAC













Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q			3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

2.B The continued development of the IdM&A Framework, based on feedback from the government stakeholder dialogue (see action line 5C), and the development of common or interoperable standards, policies, models, processes and architecture.

Responsibility: Sub-committee for Framework Development

Timeline: Start Up  and Implementation  Deadline for completion of the Framework 





2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q													Forward

3. Pilot Projects to Test and Inform the Pan-Canadian IdM&A Framework

3.A ServiceOntario and Service Canada implement Integrated Birth Registration Pilot Project, commit to assessing the IdM&A Framework, and report back on its usefulness, making recommendations for improvement.

Responsibility: ServiceOntario and Service Canada






Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q					3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

3.B Service Canada and a provincial partner implement a SIN Validation pilot whereby a province is able to validate the SINs of certain individual clients directly against the Social Insurance Registrar (SIR).

Responsibility: Service Canada and provincial partner

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q						1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

3.C Partners involved in other proposed pilot projects discuss business requirements and interoperability issues and provide status update to Deputy Ministers in November. Proposed pilot projects include:

- BCeID leveraging CRA's identity-proofing to offer online registration to clients.
- Reciprocal trust agreements between CRA and Quebec and between Service Canada and provincial partners.

See **Appendix E** for a complete list of the proposed pilot projects and participating partners.

Responsibility: Relevant Partners (see Appendix E)

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

3.D The creation of a **Sub-committee for Pilot Development** (or similar working structure) as a mechanism for capturing, disseminating and reporting on pilot successes, lessons learned and recommendations for improvement. This information will be used to inform the further development and refinement of the IdM&A Framework, governance, standards, guidelines, models and future pilot projects.

Responsibility: IJAC

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

3.E Components of the current and evolving framework, standards and guidelines are tested through implementation of self-funded and self-governed pilot projects, including those pilots mentioned in 3C and:

- Integrated Multi-jurisdictional death notification service.
- Single identity proofing bodies/enhanced BizPal.

See **Appendix E** for a description of each of these pilots. In these early pilots, partners commit to applying IdM&A Framework and reporting back on its usefulness, making recommendations for improvement.

Responsibility: Partners Involved in Pilot Projects

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

- 3.F** The development and conceptualization, with the active participation of key stakeholders, of a pilot project whose prime objective is to test the complete Pan-Canadian IdM&A Framework, the sustainable funding model and next generation IdM&A processes and technology (i.e., user-centric).

Responsibility: Sub-committee for Pilot Development

Timeline: Start Up ☐ and Implementation ☐

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

4. Sustainable Funding Model

- 4.A** Development of a budget and funding model to set up and support the activities of the Inter-jurisdictional IdM&A Action Committee (IJAC).

Responsibility: Task Force Steering Committee (as Interim Governance Committee)

Timeline: Start Up ☐ and Implementation ☐

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

- 4.B** Development of a sustainable funding model for the implementation and use of the Pan-Canadian IdM&A Framework

Responsibility: IJAC

Timeline: Start Up ☐ and Implementation ☐

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

5. Stakeholder engagement

- 5.A** Steering Committee members begin validation of IdM&A framework within home jurisdictions and with the Joint Councils (PSSDC and PSCIOC).

Responsibility: Task Force Steering Committee (As Interim Governance Committee)






Timeline: Start Up ☐ and Implementation ☐

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

5.B The development of a communication and stakeholder engagement plan.

Responsibility: Task Force Steering Committee (as Interim Governance Committee)





Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q						1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

5.C The set up of a constructive dialogue process across jurisdictions, involving key government stakeholders, to validate (and modify as necessary) the Pan-Canadian IdM&A framework, set priorities for standard development, and assess the interest, willingness and capacity of jurisdictions to actively participate in its further development.

Responsibility: Sub-committee for Framework Development

Timeline: Start Up  and Implementation 





2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q					1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

5.D The development and coordination of a public stakeholder engagement strategy with industry experts, academia and the general public to validate and build acceptance of the Pan-Canadian IdM&A Principles and Framework.

The strategy should be flexible enough to accommodate jurisdictional interests and implementation at a local, regional, and national level.

Responsibility: Sub-committee for Framework Development

Timeline: Start Up  and Implementation 

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q					1Q	2Q	3Q	4Q	Forward

5.E The development of an educational and formative tool kit for the general population to build client knowledge, trust and comfort with IdM&A processes and to increase the demand for multi-channel cross-jurisdictional service delivery initiatives, utilizing consistent and protected IdM&A processes.

Responsibility: Multi-Stakeholder Working Group for Capacity Development

Timeline: Start Up □ and Implementation □

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

6. Governance

6.A Task Force Steering Committee reconstitutes itself as Interim Governance Committee (from August to November 2007).

Responsibility: Task Force Steering Committee

Timeline: Start Up □ and Implementation □

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

6.B Creation of Inter-jurisdictional IdM&A Action Committee (IJAC).

Responsibility: Deputy Ministers responsible for Service Delivery and IdM&A

Timeline: Start Up □ and Implementation □

2007				2008				2009				2010				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

6.C The development of a proposal for the institutional means (i.e., long-term governance structure and other regulatory requirements) for the effective oversight of the implementation of the Pan-Canadian IdM&A Framework and the pilot project that will test the complete Framework, sustainable funding model and next generation IdM&A processes and technology (i.e., user-centric).

Responsibility: IJAC

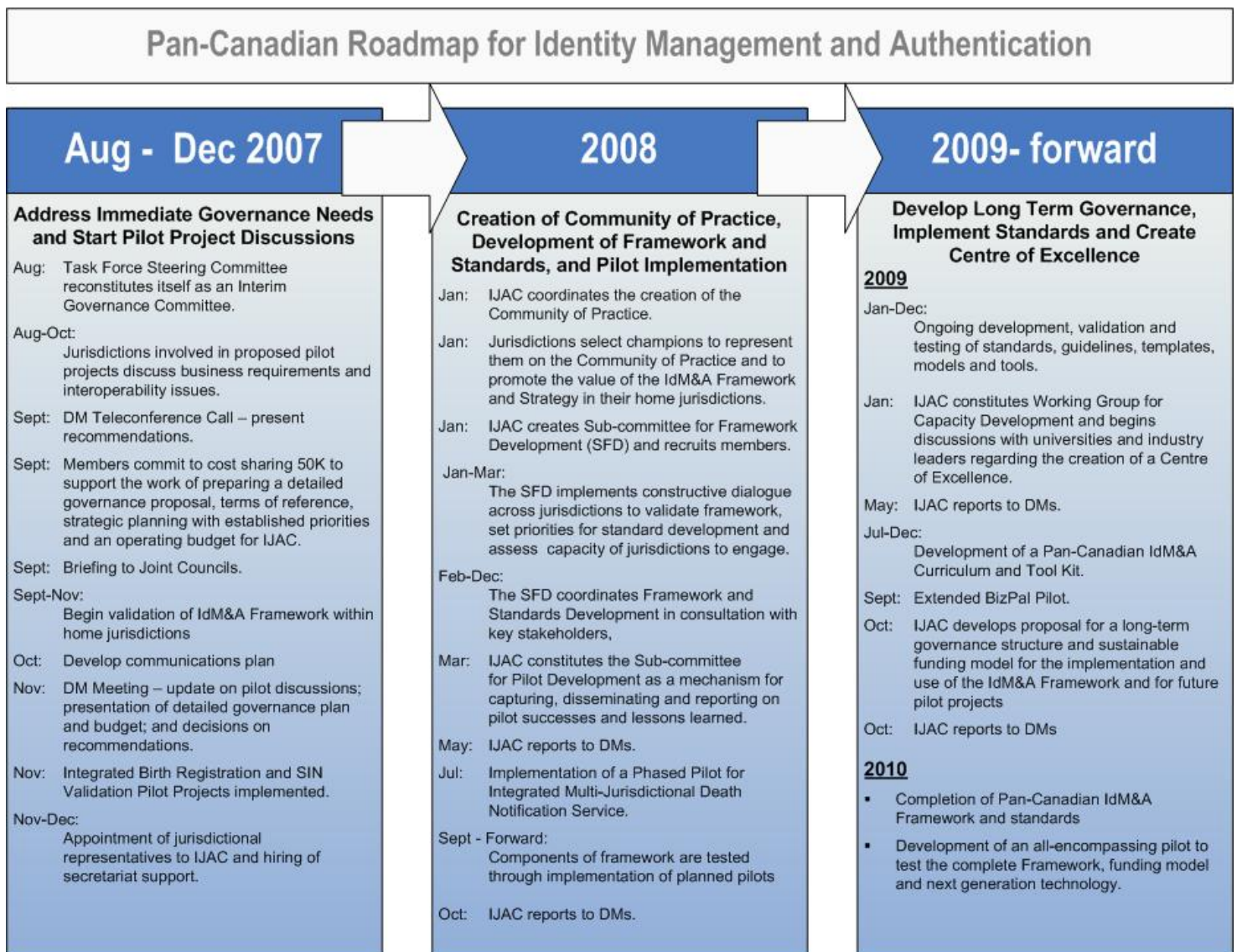
Timeline: Start Up □ and Implementation □

Year 1				Year 2				Year 3				Year 4				Forward
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	Forward

7.2 Roadmap for the Implementation of a Pan-Canadian IdM&A Framework

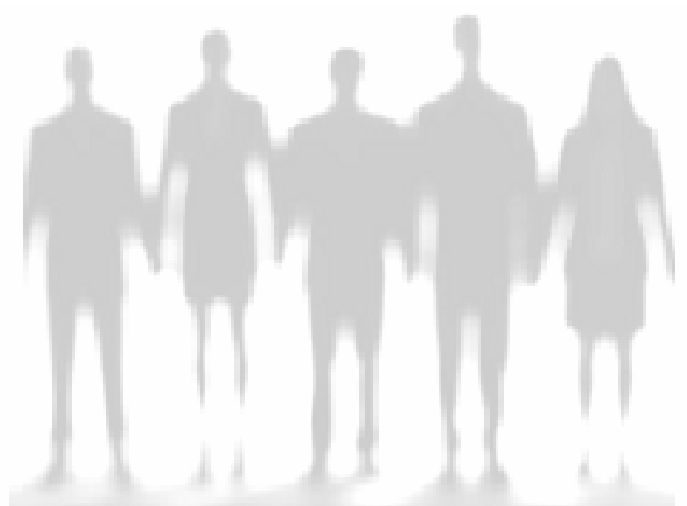
Figure 8, below, sets out a roadmap, with proposed dates for the implementation of key action items.

Figure 8. Roadmap for Implementation of Key Action Items



Annex

Pan-Canadian IdM&A Framework



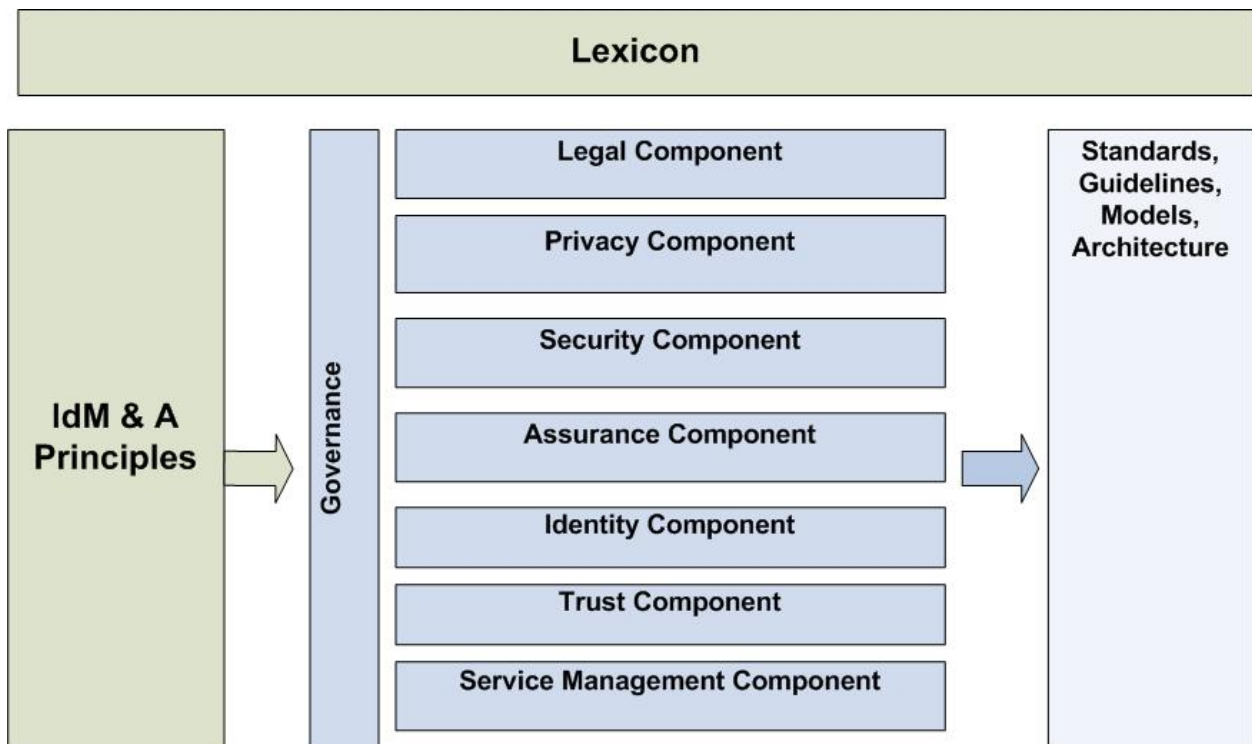
Pan-Canadian IdM&A Framework

One of the primary recommendations coming out of the IdM&A Challenges and Strategy chapters was the need for a Pan-Canadian Framework on IdM&A that would deal with issues such as:

1. Legal authorities and restrictions;
2. Privacy issues;
3. Security requirements (including Threat and Risk assessments);
4. Assurance levels and models;
5. Identity standards for clients and their delegates that takes into consideration the different contexts that clients operate in;
6. Processes and models for establishing trust between the different parties and jurisdictions involved in an identification or service delivery process; and,
7. Service management processes and models.

Figure 9, below, is a reference model for the entire IdM&A Framework which illustrates the various components of the framework (i.e., Legal, Privacy, Security, etc.) and the importance of the IdM&A Principles in guiding the framework and the Lexicon in defining the framework. The reference model also depicts how the various components of the framework will guide the eventually development of common standards, models, guidelines and architecture.

Figure 9. The Pan-Canadian IdM&A Framework



The framework was developed after an analysis of the challenges and opportunities associated with identifying and authenticating clients which provides the rationale for each component of the framework. The analysis also informed the development of the framework's principles.

This chapter sets out the principles and the lexicon the Task Force developed to guide and define the development of the Framework. The next seven sub-sections then set out the key issues and concepts that should be included in each of the IdM&A Framework components. Further work is necessary to complete each component, as well as the overall framework, and this chapter offers guidance and recommendations on this future work.

A.1 Identity Management and Authentication Principles

The purpose of these principles is to set out, at a high level, a cohesive set of fundamental rules or norms that will guide and constrain the development of the Pan-Canadian Identity Management and Authentication framework.

These particular principles were selected based on:

- a. their ability to address key challenges identified in the Problem and Solution Analysis;
- b. a comparative study of IdM&A principles developed by other jurisdictions, not-for-profit organizations, over-sight bodies and the private sector (see below); and,
- c. their applicability in a service delivery context.

A.1.1 Comparative Study

In developing these principles the Task Force considered:

- the “7 Laws of Identity” formulated on an open blog by a global community of experts through the leadership of Kim Cameron, Chief Identity Architect at Microsoft.
- Ontario Privacy Commissioner, Ann Cavoukian’s privacy-embedded Laws of Identity (which mapped fair information practices over the 7 Laws of Identity);
- the Government of Canada’s Identity Principles;
- the not-for-profit Center for Democracy and Technology’s 10-point set of authentication and identity management guidelines;
- the New Zealand Government’s *Best Practice Framework for Authentication*;
- the Australian Government E-Authentication Framework principles, and,
- the London School of Economics and Political Science’s (LSE) principles.

The Task Force found many similarities in the aforementioned principles, the differences mainly being in emphasis, degree of detail, and perspective (i.e., technical, privacy, business). Since the Task Force was asked to focus on IdM&A in a service delivery context, the principles it developed reflect that perspective.

The following principles represent an amalgamation of the key and common concepts reviewed by the Task Force, with a focus on the service delivery perspective.

A.1.2 Identity Management and Authentication Principles for Multi-Channel, Cross Jurisdictional Service Delivery

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

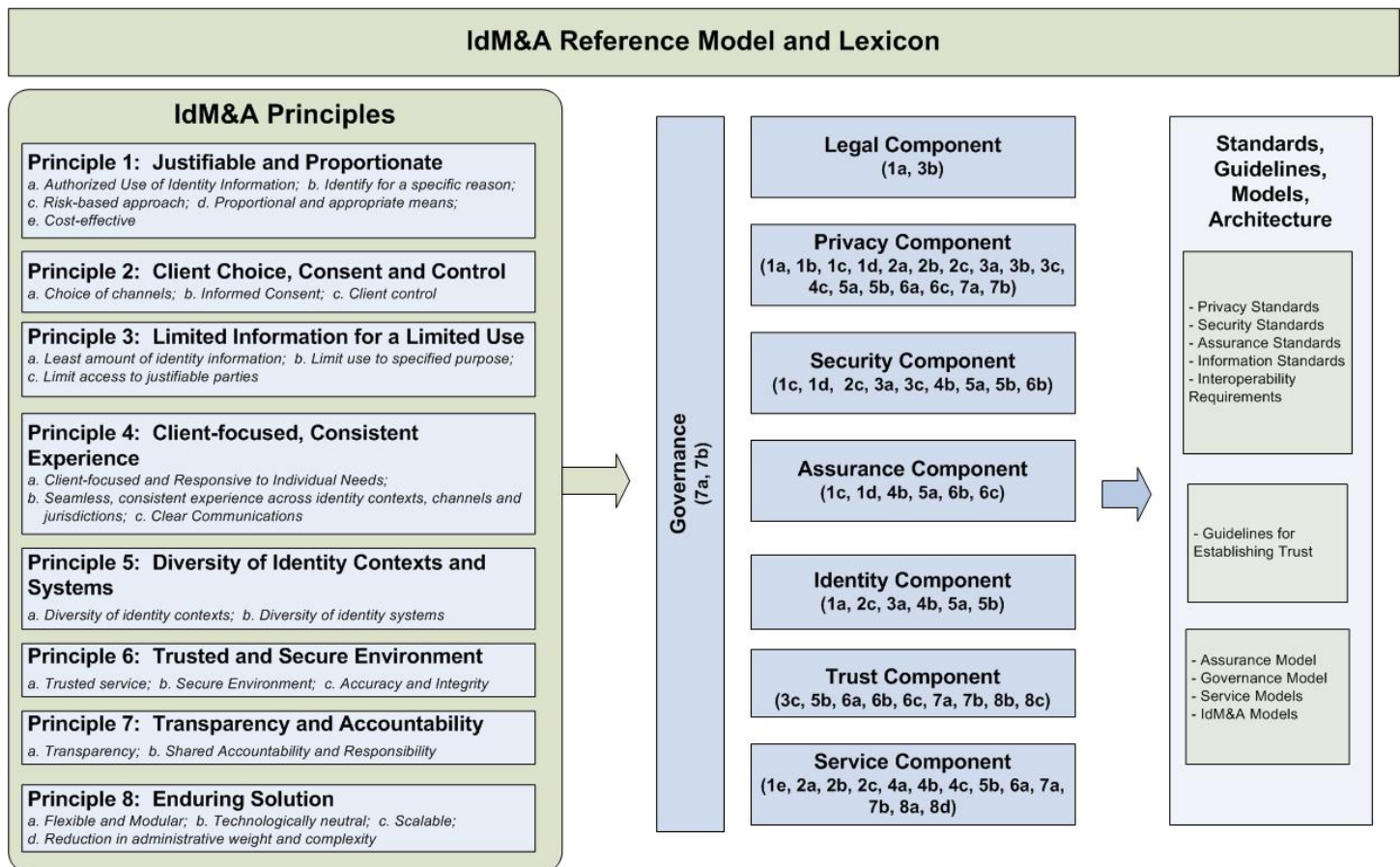
The identity management and authentication process should be scalable. The addition of clients or any other party (jurisdictions, departments, service providers, etc.) should not affect the proper functioning of the process and the application of principles or rules.

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.

Figure 10 maps each of these principles to the most relevant framework component(s).

Figure 10. A Mapping of IdM&A Principles to Applicable Framework Components



A.2 Pan-Canadian IdM&A Lexicon

The development of a common lexicon to define the IdM&A Framework and to facilitate discussions between jurisdictions on key IdM&A issues is key to common understanding. The Task Force, itself, was hampered by ongoing challenges with inconsistent use of terminology and for some terms could not come to an agreement. The list of common IdM&A terms and definitions found here should, therefore, be viewed as the starting point for a more complete lexicon. As the Pan-Canadian IdM&A Framework is further developed, new terms will arise that should be added to the lexicon.

Table 1. Pan-Canadian IdM&A Lexicon

Accountability	<ul style="list-style-type: none"> ▪ The state of accepting consequences when a commitment goes unrealized. Accountability cannot be delegated.
Assurance	<ul style="list-style-type: none"> ▪ A measure of certainty that a statement or fact is true.
Assurance Level	<ul style="list-style-type: none"> ▪ A relative measure (i.e., low, medium, high) of the strength of assurance that can be placed in an identity claim. A lower level of assurance means less certainty in an identity claim, while a higher level of assurance indicates a higher degree of certainty. <p>Unlike trust levels, assurance levels cannot be pre-established. They are created through authentication events and are dependent on a number of factors including: the rigorousness of the original registration and identity proofing process; the strength of the presented credential; the authentication event itself (i.e., successful log-on, in person verification); and, the underlying infrastructure/environment within which the authentication event occurs.</p>
(Identity) Attribute	<ul style="list-style-type: none"> ▪ A quality or characteristic ascribed to a person (e.g. name, date of birth, occupation, address) that may or may not be unique.
Authentication	<ul style="list-style-type: none"> ▪ The act of establishing or confirming something (or someone) as authentic, that is, that claims made by, or about, the thing are true. Authenticating a person often consists of verifying their identity. <p>In the digital world, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in.</p>
Authoritative Party	<ul style="list-style-type: none"> ▪ A party whose authority to make claims is recognized by one or more relying parties. Claims made by recognized authoritative parties are used by relying parties to make access control decisions.
Authorization	<ul style="list-style-type: none"> ▪ Validating that a person has a right to use a protected resource.

Biometric	<ul style="list-style-type: none"> ▪ The automated recognition of individuals based on their behavioural and biological characteristics (e.g., retinal or fingerprint scan, gait or voice recognition).
Client	<ul style="list-style-type: none"> ▪ A person (citizen or business representative) seeking or receiving a service.
Client Agent/Delegate	<ul style="list-style-type: none"> ▪ A person acting on behalf of a client who may or may not assume responsibility or liability for the client (depending on the nature of the agency or delegation).
Consent	<ul style="list-style-type: none"> ▪ Informed and voluntary agreement with what is being done or proposed. Consent is unequivocal and does not require any inference on the part of the organization seeking consent.
Credential	<ul style="list-style-type: none"> ▪ A qualification, competence, status, clearance or token etc. that is granted to a person. In the context of IdM&A, identity credentials can be cards like driver's licences or smart cards; documents like passports; or, in the context of digital identities, UserIDs and passwords or digital certificates.
Credential Issuer	<ul style="list-style-type: none"> ▪ A party that manufactures and issues a credential, asserting identity attributes or privileges associated with a person.
Identification	<ul style="list-style-type: none"> ▪ The act of distinguishing (identifying) an individual, organization or device.
Identifier	<ul style="list-style-type: none"> ▪ Qualities or attributes that name, describe or reference an individual, business or device.
Identity⁶	<ul style="list-style-type: none"> ▪ A reference or designation used to distinguish a unique and particular individual, organization or device.
Identity Assurance	<ul style="list-style-type: none"> ▪ A measure of assurance that an identity claim or assertion is true.
Identity Claim	<ul style="list-style-type: none"> ▪ An assertion of the truth of something which pertains to a person's "identity". An identity claim could convey a single attribute such as an identifier (e.g., a student number) or it could convey that a person is part of a certain group or has certain entitlements (e.g., "I am over 18", "I am a company employee"). A set of identity claims could provide sufficient identity attributes (e.g., name, date of birth, address) to permit the identification of a unique "identity" or person.
Identity Context	<ul style="list-style-type: none"> ▪ The situation or context in which an identity (or person) operates (i.e., as a parent, patient, business representative, etc.).

⁶ Further discussion is required to come to an agreement on this term and to address concerns that the definition is too narrow.

Identity Fraud	<ul style="list-style-type: none"> Assuming the identity of another individual (dead or alive) for financial gain or for another criminal purpose.
Identity Management	<ul style="list-style-type: none"> The set of principles, practices, policies, processes and procedures used to realize the desired outcomes (or goals and objectives) concerning identity.
IdM&A	<ul style="list-style-type: none"> Identity Management and Authentication.
Integrity	<ul style="list-style-type: none"> An undiminished state derived from a strict adherence to code or soundness of process.
Interoperability	<ul style="list-style-type: none"> People, processes and systems working in a collaborative fashion to share information.
Jurisdiction	<ul style="list-style-type: none"> Designation of the level or type of area in Canada within which authority and control are exercised (e.g., Canada, province, territory, municipality).
Personal Information	<ul style="list-style-type: none"> Recorded information about an identifiable individual.
Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> A tool that identifies and assess the impact to privacy of any proposed initiative or change to an existing service.
Registrar	<ul style="list-style-type: none"> A party that collects and verifies identity claims a client makes during a registration process.
Registration	<ul style="list-style-type: none"> A process by which a name, fact, etc. becomes formally recorded in a particular register. Registration, in the IdM&A context, is the process by which a person obtains an identity credential, such as a username or digital certificate, for subsequent authentication. Depending on the level of assurance required, registration and credential issuing can be done in-person or remotely through various channels such as browsers, telephones, mail or on-line.
Relying Party	<ul style="list-style-type: none"> A party that accepts a credential and its assertions to conduct a transaction with a client.
Responsibility	<ul style="list-style-type: none"> The state of accepting ownership for a commitment. Responsibility may be delegated.
Security Threat and Risk Assessment (STRA)	<ul style="list-style-type: none"> A tool that identifies general business and security risks for the purpose of determining the adequacy of security controls with the service and mitigating those risks.
Service	<ul style="list-style-type: none"> A means, administered by a program, of producing a final valued output.

Transaction Trust Level (or Trust Level)	<ul style="list-style-type: none"> ▪ A pre-established statement of the level of certainty in an identity claim that is needed to access information or conduct a transaction. The pre-determination of Trust Levels, based on information security classifications and other risk factors, is a necessary first step in the establishment of an overall IdM&A Assurance Model.
Trust	<ul style="list-style-type: none"> ▪ A firm belief in the reliability or truth or strength etc. of a person or thing (v) to place trust in, believe in, rely on the character or behaviour of.
Trust Level	<ul style="list-style-type: none"> ▪ See “Transaction Trust Level”.
Verification	<ul style="list-style-type: none"> ▪ The process or an instance of establishing the truth or validity of something.

A.3 Legal Component

The legal component of the Pan-Canadian IdM&A Framework sets out the laws, legislation and regulations that govern IdM&A across jurisdictions in Canada.

As a starting point, it is important to note that there is currently no overarching Identity Management and Authentication legislation in Canada that:

- (a) defines “identity”;
- (b) sets up an “identity” authority or authorities; or,
- (c) governs the “identity” lifecycle (i.e., the verification, provision, use, and disposition of “identity”).

This raises three key issues or questions that should be addressed in this component:

A.3.1 What is the authority for “identity” or identity management in Canada?

As identified in the problem and solution analysis, there is no clear authority on “identity” in Canada. This means that government organizations and jurisdictions may rely on a number of different authorities to obtain assurance of identity, often without a real understanding of what that authority is authoritative on. For example, many organizations rely on driver’s licences for assurance of identity, without questioning whether or not the issuers of driver’s licences in Canada are authoritative on identity. Some would argue that issuers of driver’s licences are only authoritative on an individual’s driving privileges.

Further discussion may be warranted on whether or not the current ad hoc identity assurance ‘system’ is acceptable. It may also be time to consider whether or not there should be a clear authority on “identity” or identity management in Canada or within each province or territory. Such an issue is likely beyond the current scope of this Task Force.

However, until these issues are resolved, the Legal Component of the IdM&A Framework should attempt to address the issue through guidelines that:

- Identify the organizations in Canada that are currently relied upon to provide assurance of identity claims;
- Characterize the specific authority of each organization (i.e., legislation or mandate); and,
- Indicate the specific identity attributes on which the organization is authoritative (e.g., name, birth date, address, business number, professional standing).

A.3.2 What laws govern or impact IdM&A in Canada?

The Legal Component should consider all applicable federal, provincial and municipal laws that impact IdM&A, including those that protect the rights of individuals such as human rights legislation, the Quebec Civil Code and the Charter of Rights and Freedoms. It is imperative that the IdM&A Framework, and related policies and procedures, comply with all applicable laws and safeguard the rights of the individual.

However, in general there are two categories of legislation that are applicable to IdM&A:

- a. legislation that authorizes or enables IdM&A; and,
- b. legislation that limits, constrains, or otherwise impacts IdM&A.

Because there is no overarching IdM&A legislation in Canada, the authority service providers have to identify clients is usually specific to their program or jurisdiction. Constraining legislation, on the other hand, usually applies more broadly to multiple programs or entire jurisdictions. It is, therefore, not unusual for government organizations to be authorized to deliver services to clients (and to collect necessary identity and other information in support of providing those services) by one piece of legislation, while at the same time being constrained in their activities by another piece of legislation.

Authorizing legislation sometimes contains its own restrictions and requirements which must be considered; but where it is silent on identification requirements for clients, privacy and other legislation will guide and constrain the identification process and requirements. Overarching legislation that constrains or impacts the identification of clients and the “identity” lifecycle includes:

- Privacy legislation (dealt with more fully in the Privacy Component);
- Records Management legislation;
- Electronic Transaction legislation;
- Name or Change of Name legislation; and,
- Business number legislation.

In addition, certain legislation like the federal *Income Tax Act* or the *Health Act* in British Columbia restrict the sharing of identity and other information to specific purposes. Certain policies like the Treasury Board of Canada Secretariat’s Privacy and Data Protection Policy restrict the use of identifiers like the Social Insurance Number. Additional restrictions may exist in other legislation and policy and more research and analysis is needed in this area to form a complete picture of all the legislative and policy barriers to IdM&A.

A.3.3 Whose law applies or takes precedence (i.e., federal, provincial, municipal) when an IdM&A process or transaction spans jurisdictions?

Finally, the Legal Component of the IdM&A framework needs to address the issue of whose law applies or takes precedence in situations where identity information which is originally collected by one jurisdiction is disclosed to, and stored in, another jurisdiction for the purpose of facilitating cross-jurisdictional seamless service delivery.

Further research and analysis is likely needed to determine to what extent and, in which ways, the notion of legislative precedence is an issue. Following this research and analysis, future working groups or committees could consider mechanisms for clarifying or ensuring legislative precedence such as Memorandums of Understanding and Information Sharing Agreements.

Next Steps:

The Task Force has set out the issues that it believes should be addressed in the Legal Component of the Pan-Canadian IdM&A Framework, based on:

- those issues identified by stakeholders as key challenges or potential barriers; and,
- their ability to address applicable IdM&A Principles such as “Authorized use of identity Information” and “Limiting use of identity Information to a specified and authorized purpose”.

However, it must be noted that the Task Force is not an expert on legal matters nor has it sought legal advice in developing this component. For this reason, the Task Force recommends:

1. that the Legal Component be reviewed by legal counsel.

Secondly, the Task Force has commissioned a scan of federal, provincial, and municipal statutes governing individual identification information and the exchange of personal information. Once this scan is complete, the Task Force recommends:

2. that the results of the scan be incorporated into the legal component, as appropriate, and that the final component be reviewed by legal counsel; and,
3. that, subject to the advice of legal counsel, further scans or analysis be conducted, as necessary, until there is a complete picture of the laws and legal issues governing or binding IdM&A in Canada.

A.4 Privacy Component

The Privacy Component sets out the context within which privacy requirements are applied to IdM&A.

First, in terms of how privacy does and does not apply to IdM&A, it is important to note that privacy law only applies to personal information. For this reason, privacy requirements will always apply to the identification and authentication of citizens and employees but its application to the identification and authentication of businesses and other organizations is less clear. Certainly, privacy requirements will not apply to the identification and authentication of corporations but they may apply to the identification and authentication of the corporation's principals and to the identification and authentication of sole proprietorships and partnerships. Whether or not privacy requirements apply in these situations will depend on what information is being used to identify principals, partners and sole proprietors, and on how "personal information" is defined (and/or interpreted) in each jurisdiction (i.e., whether or not it applies to the names and contact information of individuals operating in a business capacity).

As a result of the problem and solution analysis and in accordance with the applicable IdM&A Principles, the Task Force has identified six key privacy areas that should form the basis of the Privacy Component for the IdM&A Framework:

1. Compliance with privacy law (e.g., fair information practices);
2. Privacy Impact Assessments (PIAs);
3. Notification and consent;
4. Limiting collection, use and disclosure of identity (and other client) information;
5. The notion of control or "informational self-determination"; and,
6. Accuracy, Access and Accountability.

A.4.1 Compliance with Privacy Law

Privacy law, in this context, refers to privacy legislation and regulations but also more broadly to the Canadian Standards Association's Model Code on Privacy and to relevant jurisprudence in this area such as decisions by Privacy Commissioners and by the Courts. This section is closely related to the Legal Component of the Framework.

The key point here is that IdM&A policies, standards and processes must be compliant with all applicable privacy laws. All privacy laws in Canada are based, for the most part, on the same "fair information practices" (such as notification of purpose, limited collection use and disclosure of personal information, etc.) but they do differ in some details. For example, privacy legislation in British Columbia clearly distinguishes and excludes information that would identify a person at a place of business (e.g. business contact information) from

personal information. Other jurisdictions do not make this distinction and may consider this information to be personal information. In addition, privacy legislation in British Columbia and Nova Scotia contains provisions that limit the storage and disclosure of personal information outside of Canada. Other jurisdictions do not have such restrictions.

The privacy component of the framework needs to set the backdrop for privacy as it applies to IdM&A by pulling relevant privacy requirements from all applicable authorities or laws. Applicable laws would include federal, provincial and municipal privacy legislation and regulations but also sector specific legislation or regulations that contain privacy requirements such as Health and Social Services legislation. As well, to the extent that it is applicable, private sector privacy legislation and regulations should be considered. As stated above, there will be a core set of privacy requirements that apply to IdM&A, but there also may be some unique requirements that need to be highlighted and factored in to the overall framework.

A.4.2 Privacy Impact Assessments (PIAs)

The purpose of a Privacy Impact Assessment (PIA) is to identify and assess the impact to privacy of any proposed initiative or change to an existing service. A PIA, when completed at the appropriate time (early in the design phase), can serve as an early warning signal to developers and program managers of privacy issues that need to be resolved or mitigated prior to implementation. It will also help identify intrusive processes and the use of over-qualified identifiers, permitting the early consideration of alternatives or privacy enhancing technologies or solutions.

“Privacy is better built-in than bolted on. Privacy enhancing technologies are most effective when integrated in the design stage”.⁷

Protecting privacy can involve technical solutions, but it also can include changes to policy and processes, changes to physical security, and changes to responsibilities and accountabilities.

A PIA should be conducted of any new IdM&A system; or of any significant changes or upgrades to existing IdM&A systems. A PIA should also be conducted by any program area that is significantly changing the method by which it delivers services to clients (including delivering the service over new channels such as over the telephone or Internet) to determine whether or not those changes create any new risks to privacy.

Some jurisdictions require the completion of a PIA by law or by policy, but there is currently no standard PIA format or template that is used by all jurisdictions across Canada, nor is there a PIA template that is specifically geared towards IdM&A initiatives.

⁷ GUIDE, 2005: D2.1.1.A: *Institutional, political, and policy frameworks affecting IMS for eGovernment v.1*, page 57 (<http://istrg.surrey.ac.uk/projects/guide/files/documents/D2.1.1.A.pdf>)

A Pan-Canadian standard PIA template could bring consistency across jurisdictions and produce a more focused assessment. As completion of a Security Threat and Risk Assessment is noted as a key security requirement in the Security Component of the Framework, consideration could be given to developing a tool or template that combines both assessments as they relate to IdM&A initiatives.

A.4.3 Notification and consent

An IdM&A Framework must incorporate notification and consent requirements. Consent is not always required where a program area has the authority to collect identity information without consent; but notification is generally always required.

Both private sector and public sector privacy laws require organizations to inform clients why it is necessary to collect personal information and to explain to them how the information will be used, before or at the time of collection. As well, where the organization does not have the legal authority to collect or use the identity or other personal information without consent, it must also obtain the client's consent.

While obtaining consent is not currently a requirement for many public organizations that collect identity information from clients, it is likely to become more of an issue as organizations move towards providing cross-jurisdictional seamless services. This is because many government organizations that have the authority to collect identity information from clients without consent for the purpose of providing mandated services will not necessarily have the authority to share that identity information with other organizations, particularly in other jurisdictions, without the consent of the client. It is also important to note that most private sector organizations in Canada are required to obtain client consent to collect and use client information; so to the extent the an IdM&A service or process involves a private sector partner, obtaining consent may be necessary for part of the transaction. As well, Canada Health Infoway has adopted the Canadian Standard Association's Model Privacy Code as their standard (which includes the requirement for consent) so where an IdM&A service or process involves a health provider, obtaining consent may be necessary. For these reasons, organizations that haven't had to worry about obtaining consent in the past, may need to turn their minds to it, if they wish to participate in cross-jurisdictional and cross-sector seamless service delivery.

It should also be pointed out, that even where an organization isn't legally obligated to obtain consent, it may wish to do so anyway as a privacy best practice and as a way of providing more empowerment to the client.

With respect to notification and consent, the Privacy Component of the IdM&A Framework should set standards or guidelines for:

- “Informed consent” -- what is it and how to obtain it.
- Forms of acceptable consent (e.g. written, oral, implied).
- When consent is and isn’t required.
- How to obtain consent over different channels.
- What notification should include (e.g., legal authority, purpose for collection, who to contact with questions).
- Providing notice over different channels.
- Notifying clients of:
 - the current party they are interacting with when they are providing identity information (this is particularly important over remote channels where a client can seamlessly move from one organization’s website or call centre to another without necessarily knowing it); and,
 - all the parties that will be involved in a particular IdM&A process or service delivery transaction (i.e., if another organization will be contacted to verify an identity claim).
- Exceptions to notification requirements.

A.4.4 Limiting collection, use and disclosure of identity and other client information

A key principle, common to all privacy laws, is limiting the collection, use and disclosure of personal information. Collection of personal information should be limited to: firstly, what you are authorized to collect; and secondly, to what you need to collect. In the same vein, use and disclosure of personal information should be limited to the purpose for which the information was originally collected (or for a use consistent with that purpose) and to only that information that needs to be used or disclosed.

When applied to IdM&A, this means that any identity information that is collected must be authorized by legislation, policy or program requirements and must be justified in terms of there being a clear need for that identity information. Organizations should not collect identity information that they don’t need or that they don’t need now but might find a use for later.

In addition, identity information that is collected for one purpose (e.g., to provide, or determine eligibility for, a specific service) should not be used for any other purpose, without first obtaining the consent of the client. There are, of course, exceptions to this requirement (e.g., where authorized or required by law, or for law enforcement purposes, including the investigation of identity fraud) but generally speaking, other uses of identity information without consent are not permitted, regardless of the perceived benefit they might impart.

This is a difficult concept for some service delivery communities to implement as it often flies in the face of delivering what they perceive as client-centric seamless service. Using client information to advise clients about new services, build profiles on services they already

receive, and cluster related services are often done to improve the service delivery experience for the client. The difficulty is that such actions, while well-intentioned, could contradict privacy laws and could offend some clients who resent or fear the notion of government tracking their activities, 'in their best interests'. In order to meet the needs of all clients, including the many clients who might welcome the 'enhanced' service, programs should inform clients ahead of time that their information may be used for such purposes. This would provide more control to the client and could set up a situation where a client, with full knowledge of the benefits he would be foregoing, could choose to opt out of such a service.

Lastly, access to and disclosure of, identity information should be strictly controlled, preferably through technological measures. Only those individuals or organizations that have a necessary and justifiable place in the IdM&A process or in the service delivery transaction should have access to a client's identity information. Controlling access to a client's identity information is also addressed in the Security Component (as this is an area where security and privacy requirements overlap).

A.4.5 The notion of control or “informational self-determination”.

The notion of control or “informational-self-determination” is at the very heart of the right to privacy and is one of the key ways in which privacy is distinguished from related terms like confidentiality and security. Whereas confidentiality and security are focused on the safe-keeping of information and preventing unauthorized access, “informational self-determination” is broader and reflects Dr. Alan Westin's description of privacy:

“The right of the individual to decide what information about himself should be communicated to others and under what circumstances.”⁸

Client control is a term that raises concerns for many organizations. It raises concerns because they think it means that clients will be given absolute control over the process. But that is not what control means in the privacy or IdM&A context. Clearly, the organizations responsible for an IdM&A process will manage that process (and related technology) and set the requirements for the IdM&A service, including the level of assurance in an identity claim necessary to conduct a particular transaction. Client control in this context really means “informational self-determination. It is the ability of the client to control – to the greatest extent possible and within the boundaries of the IdM&A process – the collection, use and sharing of his identity information.

Depending on the situation and available technology, different levels of control may be possible. For example, there is technology currently under development – user centric technology – that would permit the client to actually control the transfer of his identity credentials from one party to another (Microsoft's Card Space, is one example). Currently, the technology to enable this type of client control over their electronic identities is not yet widely available. But this does not mean that clients currently have no control. Rather, the

⁸ Westin, A., Privacy and Freedom, New York: Atheneum, 1970.

key to the Client Control principle is to provide clients with the greatest amount of control possible, utilizing existing measures. Where clients cannot physically control their credentials and identity information, other measures such as informed consent can be employed. By informing clients of the purpose for which identification is required, seeking their consent where necessary and allowing them choice over the use of credentials, clients exert control. The more choices a client has and the more often his consent is sought, the more control he generally has. Control can also be provided to clients by permitting them to see what personally identifiable information an organization holds about them and letting them know who has accessed it and why.

At the end of the day, client control or “informational self-determination” is about respect. A respectful IdM&A system that uses fair information practices and transparent processes fosters trust and acceptance amongst clients. Failure to promote client control and trust may lead to the clients objecting to or refusing to use remote channels to conduct government transactions. One might assume that the notion of client control and trust is automatically foreseen in the client-centered design and development of new services, but in practice, many systems are still built today that do not comply with best practice of user-centric development (in terms of allowing the client to control his own identity credentials and to consent to the transfer of his identity information to specifically identified organizations)⁹.

The Privacy Component should address the following issues related to client control:

- Defining what client control does and does not mean in an IdM&A context.
- Different measures for providing greater control to clients.
- Limitations on control, where necessary and appropriate.
- The importance of usage transparency.
- Encouraging the use of user-centric and privacy enhancing technologies.

A.4.6 Accuracy, Access, and Accountability

Clients should have confidence that organizations are taking reasonable efforts to ensure the accuracy and integrity of the information they use to make identity and authorization-related decisions. In addition, they should have the right to oversee or check on the management of their personal information through access to information requests. Finally they should be assured that someone is accountable to them for protecting their identity information, monitoring the organization’s compliance with privacy and security requirements, and addressing the client’s questions, concerns and complaints.

⁹ *Roadmap for Identity Assurance in the UK*, Information Assurance Advisory Council

To provide clients with accountability, access and transparency, the Privacy Component should provide guidelines on:

- “Reasonable” steps to ensure the accuracy and integrity of information used to make identity-related or authorization decisions (including any limitations on steps an organization should take).
- What to do when information used to make a decision about a client is found to be inaccurate or out-of-date.
- Processes for providing a client access to her identity-related information, including what laws and exceptions apply.
- Processes for informing a client, upon request, what parties have had access to his identity-related information and for what reason, including any exceptions that might apply to such a request (i.e., access by law enforcement agencies).
- How to establish transparent dispute-handling processes, so that a client understands the process and knows to whom she should address a question, concern or complaint. This is particularly important where more than one organization is involved in a particular transaction or identity verification process and raises the question of whether there should be a central oversight authority to whom clients can either directly address, or escalate, IdM&A concerns and complaints.

Next Steps:

The Task Force has set out the main issues that it believes should be addressed in the Privacy Component of the Pan-Canadian IdM&A Framework, based on:

- the key challenges or problems it identified in the problem and solution analysis; and,
- the guiding IdM&A Principles it developed.

It is important to note, however, that the Task Force does not consider itself to be an expert on Privacy law or Privacy principles and best practices. For this reason, the Task Force recommends:

1. That the Privacy Component be reviewed by more expert bodies such as the Joint Council’s (Public Sector Chief Information Officers Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC)) Privacy Sub-committee and Privacy Commissioners before further work is undertaken.
2. Once this review is complete, the Task Force recommends that the Privacy Component be completed as the starting point for Pan-Canadian standards and policies on ensuring privacy of identity information, notification, consent, client control, etc. This work could be overseen by a new committee or by the existing PSCIOC Privacy Sub-Committee, possibly utilizing qualified consultants.

3. Subject to the review of the Joint Council's Privacy Subcommittee, the Task Force recommends:
 - a. the development of a Privacy Impact Assessment template and guidelines specifically geared to IdM&A privacy issues that can be used and/or adapted by all jurisdictions; and,
 - b. in consultation with the National Chief Information Officer Subcommittee for Information Protection (NCSIP), that consideration be given to combining the Privacy Impact Assessment and the Security Threat and Risk Assessment into one tool or template for the purpose of assessing the risks related to IdM&A.

A.5 Security Component

The Security Component sets out the context within which security requirements are applied to identity management.

The Task Force has identified six key security areas or issues that apply to, or would support, a Pan-Canadian IdM&A framework:

1. Setting up an environment that engenders trust;
2. The adoption of common security standards (e.g., ISO/IEC 27002:2005) upon which each jurisdiction's IdM&A security policies would be based;
3. The requirement to conduct a security threat and risk assessment (and perhaps the adoption of a common approach or template for IdM&A initiatives);
4. The need to predetermine Transaction Trust Levels based on a risk assessment that includes the Canadian Public Sector Security Classification Guideline developed by the National CIO Subcommittee for Information Protection (NCSIP);
5. Setting up processes for auditing and monitoring compliance, detecting and responding to incidents; and,
6. A robust and effective security awareness training program.

A.5.1 Setting up an environment that engenders trust

One of the key issues identified in the problem and solution analysis was the requirement to set up an IdM&A environment that engenders trust. A trusted service is important not just to clients whose identity information it must protect; but also to users and partners of the system. This section is, therefore, closely related to the Privacy Component in that privacy is dependant on processes that properly secure personal information. It is also closely related to the Trust Component in that confidence and trust in using an IdM&A system will be dependent, in part, on the security underpinnings.

Public services can be offered only within an environment where trust and confidence flourish. Such environments should always guarantee secure interaction and access for citizens and business.

European Commission on e-Government (2003)¹⁰

¹⁰ Commission of the European Communities (2003) *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: The role of eGovernment for Europe's future*

The protection of privacy and the confidentiality, integrity and availability of data in the context of IdM&A initiatives is one of the most contentious issues surrounding IdM&A. Debates surrounding plans to implement an IdM&A system are often fraught with disagreement regarding the extent to which it would jeopardize the security of personal information. While not discussed or debated as much, protecting confidential business information and protected or sensitive government information is also crucial. Very strong measures are necessary to ensure that privacy is safeguarded, that confidential business and government information is protected, and that the following IdM&A principles are realized:

- Principle 2a – Enabling, where permitted, client control over their credentials and the transfer of their identity information;
- Principle 3a – Ensuring that only necessary and limited identity information is accessed or disclosed for a specific purpose;
- Principle 3c – Ensuring that identity information is only accessed by, or disclosed to, those parties that have a justifiable role in the IdM&A process or service delivery transaction;
- Principle 4b – Enabling a simple, consistent experience for clients across programs and jurisdictions in a manner that does not compromise security;
- Principle 5a – Enabling the separation of an individual's identity contexts (i.e., as a citizen, business or employee);
- Principle 5b – Enabling the secure interoperation of multiple identity systems run by multiple identity providers; and,
- Principle 6b – Providing a secure environment for both client identity information and for the secure delivery of multi-channel, cross-jurisdictional services.

A.5.2 The adoption of common security standards

As a first step to establishing a secure and trusted Pan-Canadian IdM&A environment (as well as enabling the aforementioned principles), the Security Component should be based on internationally recognized standards (such as ISO/IEC 27002:2005). The adoption of these standards would then guide the creation and adoption of common, equivalent or minimum security policies for IdM&A services (e.g., security policies on strong authentication, personnel screening, secure areas, incident response, etc.). Common or equivalent IdM&A security policies will greatly assist in the establishment of trust across jurisdictions and will provide greater consistency for clients engaging in cross-jurisdictional IdM&A processes.

A.5.3 Security Threat and Risk Assessments

Security Threat and Risk Assessments (STRA) of the IdM&A service must be regularly conducted to identify general business and security risks, to determine the adequacy of security controls with the service, and to mitigate those risks.

As is the case with a PIA, a STRA, when completed at the appropriate time (early in the design phase), can serve as an early warning signal to developers and program managers of security issues that need to be resolved or mitigated prior to implementation. However, more than is the case with a PIA, a STRA may need to be continually revisited and adapted as new threats and risks emerge and evolve.

A STRA should be conducted of any new IdM&A system; or of any significant changes or upgrades to existing IdM&A systems. A STRA should also be conducted by any program area that is significantly changing the method by which it delivers services to clients (including delivering the service over new channels such as over the telephone or Internet) to determine whether or not those changes create any new risks to security.

As with privacy, protecting security can involve technical solutions, but it also can include changes to policy and processes, changes to physical security, and changes to responsibilities and accountabilities.

Finally, while most jurisdictions require the completion of a STRA, there is currently no standard STRA format or template that is used by all jurisdictions across Canada, nor is there a STRA template that is specifically geared towards IdM&A initiatives. Such a template could bring consistency across jurisdictions and produce a more focused assessment.

Combining the PIA and STRA processes:

Because there are so many similarities between the purpose and process for completing PIAs and STRAs (including the timing of when they should be completed), the Task Force has recommended in the Privacy Component above that consideration be given to developing a Pan-Canadian tool or template that combines both assessments as they relate to IdM&A initiatives. In addition to creating a more efficient process, the combining of the two assessments could also help ensure a more balanced overall assessment and avoid the possibility of contradictory recommendations (i.e., where a recommendation for a stronger security measure in one assessment is determined to be an unwarranted intrusion on individual privacy in another).

A.5.4 Establishing Transaction Trust Levels based on the Security Classification of the Information involved and additional risk factors

A Transaction Trust Level (or trust level) is a pre-established statement of the level of certainty in an identity claim that is needed to access information or conduct a transaction.

The pre-determination of trust levels is the first step in the establishment of an overall IdM&A Assurance Model which recognizes that different levels of identity assurance are required for different types of transactions. As such, this section is closely related to the Assurance Component.

The level of assurance needed in an identity claim to access a particular service should be based on two factors:

- the *risk of providing the service* through a given medium; and,
- the *security classification of the information* involved.

The risk of providing the service through a given medium should be assessed as part of the aforementioned Security Threat and Risk Assessment. With respect to the security classification of the information, the Task Force endorses the recommendation made by the former IAAWG¹¹ that this assessment be based on the Canadian Public Sector Security Classification Guideline developed by the National CIO Subcommittee for Information Protection (NCSIP). This Guideline, which is available at http://www.iccs-isac.org/eng/pubsec_security_class.htm⁶ was developed to facilitate the sharing of electronic information between provincial, territorial, municipal, and Government of Canada jurisdictions by establishing a common way to classify and rate the sensitivity of information.

The Security Classification Guideline sets out classification ratings based on the risks associated with providing access to increasingly sensitive information, based on the loss, damage or harm that may result from an error in identification, authentication, or authorization. The Guideline classifies the sensitivity of information and services into four categories:

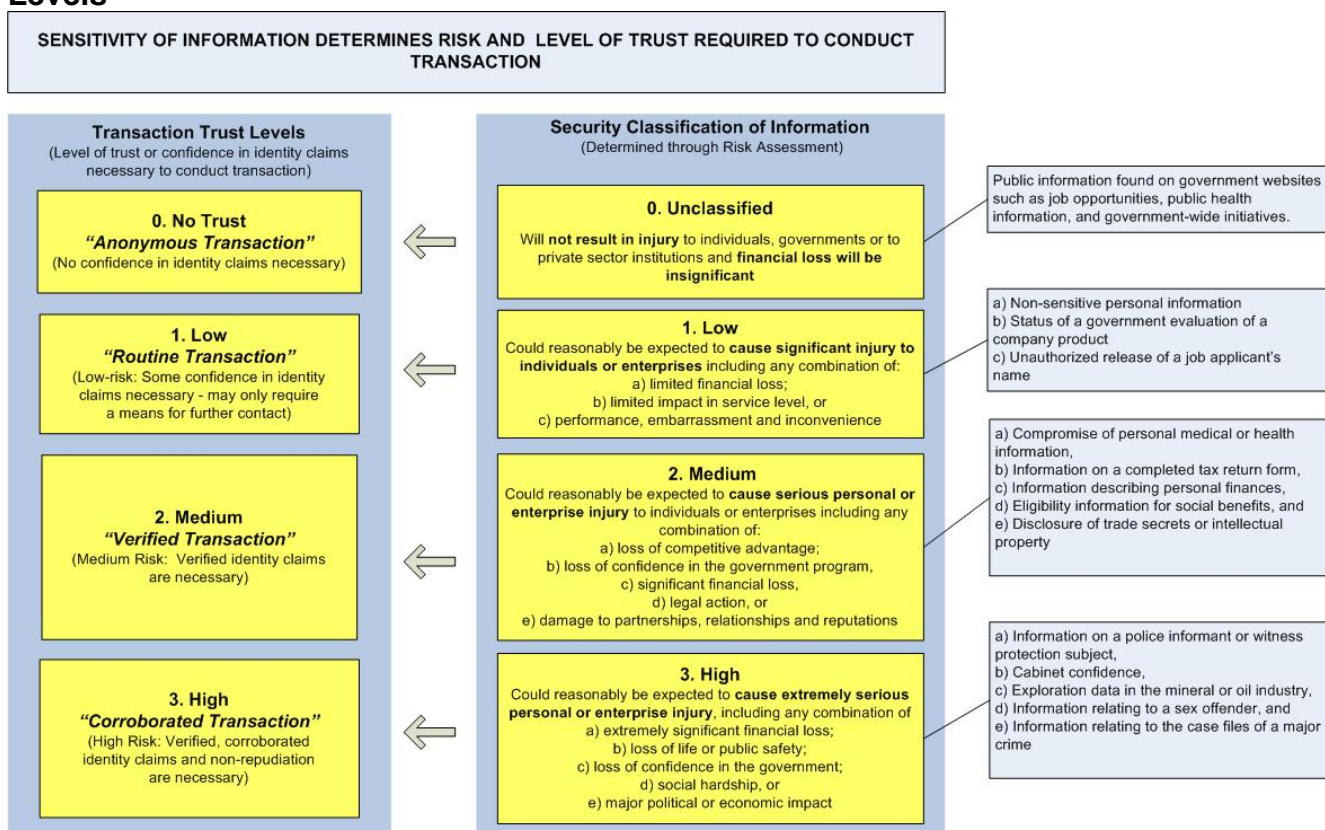
- a) Unclassified;
- b) Low;
- c) Medium; and,
- d) High.

Since there is a direct relationship between the sensitivity level of information and services and the level of assurance in an identity claim that is required to permit access to that information or service, it makes sense to establish four Trust Levels that correspondingly increase the level of trust required.

¹¹ Identification, Authentication and Authorization Working Group

Figure 11, below, illustrates the direct relationship between Information Classification and Trust Levels:

Figure 11. Relationship between Information Classification and Transaction Trust Levels



In this way, the Information Classification Schema becomes the foundation for the entire Assurance Model (further developed in the Assurance Component). If information is unclassified, or classified at a low level of sensitivity, then little or no assurance is needed in an identity claim. On the other hand, if information is classified at a high level of sensitivity, then an accordingly high level of assurance is needed in an identity claim. In summary, the more sensitive the information or service, the higher the level of assurance in an identity claim that will be needed to conduct the transaction.

It is important to note that the Security Classification Guideline classifies information, not transactions. The Guideline provides examples of the type of information that might be included in each sensitivity level, based on confidentiality, availability and integrity requirements. Examples of information that could be included in each level based on confidentiality requirements are set out in Figure 11, above. However, the Guideline does not translate these information classifications into typical transactions or services that might be offered to clients through multiple channels and that would require identification and authentication processes. While the information classification is a good starting point, more work is required to classify the sensitivity of typical transactions and services and map these to Trust Levels.

The development of guidelines to assist organization in assessing the risk of typical transactions and services (based on the sensitivity of the information involved) and mapping those specific transaction types to the appropriate Trust Transaction Level, should be considered.

A.5.5 Processes for Auditing and Monitoring Compliance and Detecting and Responding to Incidents

The Security Component of the IdM&A framework should address the key importance of auditing and monitoring compliance of security policies, procedures and practices as well as procedures for detecting, reporting and responding to security incidents.

Audit processes are closely related to accountability and trust. Audit trails monitor access and use of identity information but they also protect identity and other sensitive information from abuse by revealing inappropriate use, and providing evidence for examination in the event of security incidents. Auditing is also important for the protection of privacy.

The Security Component should set standards or guidelines for audit processes. Making organizations accountable to its clients through the deployment of audit trails and other security mechanisms engenders trust by providing transparency and accountability. The Security Component should also set standards or guidelines for fraud detection, security breach management, system interrogation facilities, and the periodic testing and evaluation of the effectiveness of IdM&A security policies, procedures and practices. This system of checks and balances will have the dual purpose of increasing system functionality while at the same time promoting public trust in the system.

These processes are key to ensuring a secure and trusted IdM&A environment, enabling the applicable IdM&A principles, and setting the foundation for the establishment of Trust Models which are set out in the Trust Component of the IdM&A framework.

A.5.6 A robust and effective security awareness training program

As identified in the problem and solution analysis, education and awareness training is one of the most cost-effective ways to mitigate security risks and threats.

The security component of the IdM&A framework should set guidelines for ongoing, robust, and effective security awareness training for all government employees, contractors and other individuals that are involved in the IdM&A process.

Next Steps:

The Task Force has set out the main issues that it believes should be addressed in the Security Component of the Pan-Canadian IdM&A Framework, based on:

- the key challenges or problems it identified in the problem and solution analysis;
- its knowledge of security best practices; and,
- the guiding IdM&A Principles it developed.

However, the Task Force believes that the work done to date on the Security Component would benefit from a review by individuals with more experience in security best practices. For this reason, the Task Force recommends:

1. That the Security Component be reviewed by a more expert body such as the aforementioned National CIO Subcommittee for Information Protection (NCSIP).
2. Once this review is complete, the Task Force recommends that the Security Component be completed as the starting point for the creation and evolution of Pan-Canadian IdM&A security standards and policies (e.g., security policies on strong authentication, personnel screening, secure areas, incident response, etc.) This work could be overseen by a new committee or by the NCSIP, possibly utilizing qualified consultants.
3. Subject to the review of the NCSIP, the Task Force also recommends:
 - a. the development of a Security Threat and Risk Assessment template and guidelines specifically geared to the risks and threats posed by IdM&A issues that can be used and/or adapted by all jurisdictions; and,
 - b. the development of guidelines to assist organizations in determining what Trust Level should apply to their specific transaction or service. These guidelines would build on the Security Classification Guideline by:
 - i. assessing the sensitivity of typical transactions and services (based on the sensitivity of the information involved); and ,
 - ii. providing guidance on how to map transaction types or services to appropriate Trust Levels.

A.6 Assurance Component

The Assurance Component expands on identity assurance concepts introduced in the Task Force's Interim Report (such as an IdM&A "chain of trust", authentication factors, gradients of identity assurance, etc.) and sets the framework for the development of a Pan-Canadian Assurance Model.

The development of a Pan-Canadian Assurance model is necessary to converge the independent work that is currently taking place in many jurisdictions across Canada in terms of developing and defining requirements for identity assurance levels. Agreement in this area will:

- a) facilitate interoperability between jurisdictions;
- b) ensure the consistent implementation of applicable IdM&A Principles;
- c) enable the joint development of supporting tools and guidelines; and,
- d) provide a seamless, consistent experience across jurisdictions for clients.

The Pan-Canadian Assurance Model sets out the relationship and interdependencies between Security Classification Levels and Transactions Trust Levels (as set out in the Security Component) and the various factors necessary to establish Assurance Levels. As is the case with security classifications and trust levels, each component of the Assurance Model is separated into discrete levels: None, Low, Medium and High.

The Assurance Component should address the following key issues associated with developing a Pan-Canadian Assurance Model:

- 1. Identity Assurance;
- 2. The "Chain of Trust";
- 3. The Role of Information Security Classifications and Trust Levels;
- 4. Establishing Assurance Levels;
- 5. Identification Levels and Registration Processes; and,
- 6. Identity Credentials and Authentication Factors.

A.6.1 Identity assurance

Identity assurance is a measure of assurance that an identity claim or assertion is true. The reference to an "identity claim" rather than an "identity" is an important distinction. It makes the point that there are different types of claims, many of which will not permit the identification of a unique individual. For example, an identity claim might be "I am over 18 years of age", "I am a student", or "I am a Canadian citizen". For some transactions, this may be all the identity information that is needed. Of course, where necessary, an identity claim may also assert a unique identity (e.g., full legal name, date of birth, SIN, residential address, etc.).

Most IdM&A frameworks recognize the need to distinguish between different levels of identity assurance, based on the needs of the organization and the nature of the transaction. For example, there are many transactions that do not require any assurance of identity (e.g.,

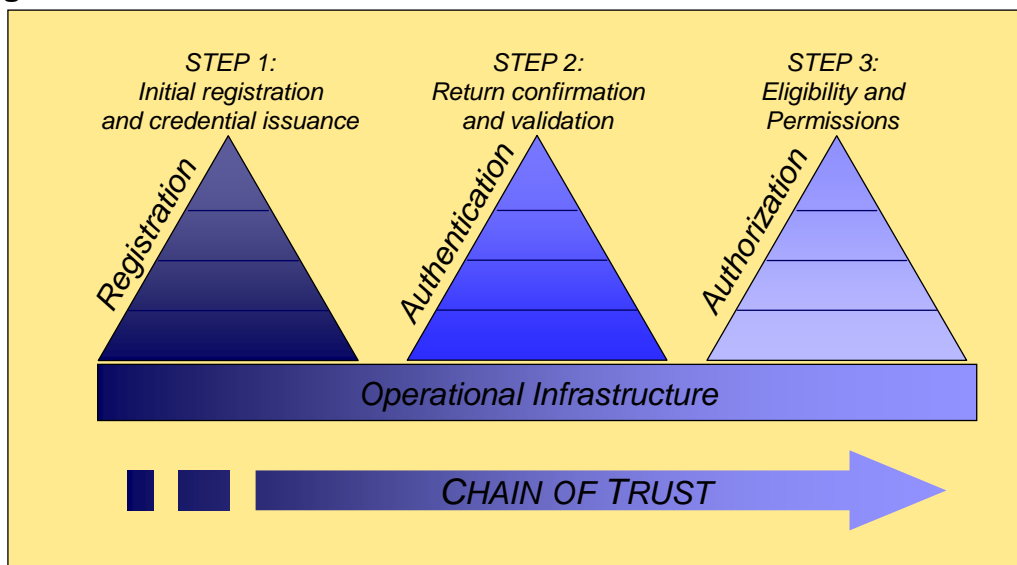
access to public information on a government website) while other situations, such as access to a secure area, require a high degree of certainty in an asserted identity. These different levels of assurance, which generally range from “none” to “high”, reflect the degree of confidence required in an identity claim before permitting access to a specific transaction or service.

Different levels of identity assurance are arrived at through a series of steps or business processes, linked together in what is commonly referred to as a “Chain of Trust”, but which might more appropriately be renamed a “Chain of Assurance.”

A.6.2 Chain of Trust /Assurance

The Chain of Trust (or Chain of Assurance), set out in Figure 12, below, is a reference model that illustrates how the main components of an IdM&A assurance framework are linked together and dependent on one another to establish a “chain of trust” or “chain of assurance” in a specific identity claim.

Figure 12 – The “Chain of Trust”



The key components of an IdM&A “Chain of Trust” are:

1. **Registration or Identification.** These processes, which could include identity proofing and document verification, answer the question: “*Who are you?*” Once an identity is established to required level of assurance, a credential may be issued.
2. **Authentication¹².** These processes, such as credential verification, answer the question: “*How do I know it’s you?*”

¹² Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. Authenticating a person often consists of verifying their identity. In computer security, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in.

3. **Authorization.**¹³ These processes, which may include determination of eligibility and role assignment, answer the question: “*What are you allowed to do or see?*”

The “Chain of Trust” is built and maintained by an operational infrastructure of people, processes and technology that securely manages identification, authentication and authorization, so that trust (or assurance) is not compromised at any stage of the chain.

A Chain of Trust Illustration

To illustrate how the “Chain of Trust” works, consider the case of a citizen wishing to view records related to a service he is receiving from government, online from home:

Registration. The government organization first needs to know whether the person is who he says he is. Therefore, the citizen must *prove his identity* with documents, such as a birth certificate or citizenship certificate, and possibly government-issued photo id. Once the government agency is sufficiently confident of the person’s identity, it will *issue credentials*, that is, give him a digital identity (e.g., user ID) and credentials (e.g., a password) that are associated with his proven identity.

Authentication. Then, when the citizen signs in, online, with his user ID, the government organization needs to assure itself that *this* is the person who owns the ID. This can be done through a variety of methods, such as, passwords, shared secrets, smart cards, biometrics.

Authorization. Once the citizen has successfully logged on, the government organization needs to associate the person’s digital identity with his digital records. This could be done, for example, by linking the file number with his digital identity at the time of registration.

Operational infrastructure. Both the citizen’s and the government organization’s trust are enhanced through the design of the underlying systems and processes supporting the chain (e.g., firewalls, secure networks, registration processes, and accountabilities) which ensure that information has not been compromised.

Adapted from: the Ministry of Health (B.C.) Identity Management and Authentication Business Requirements

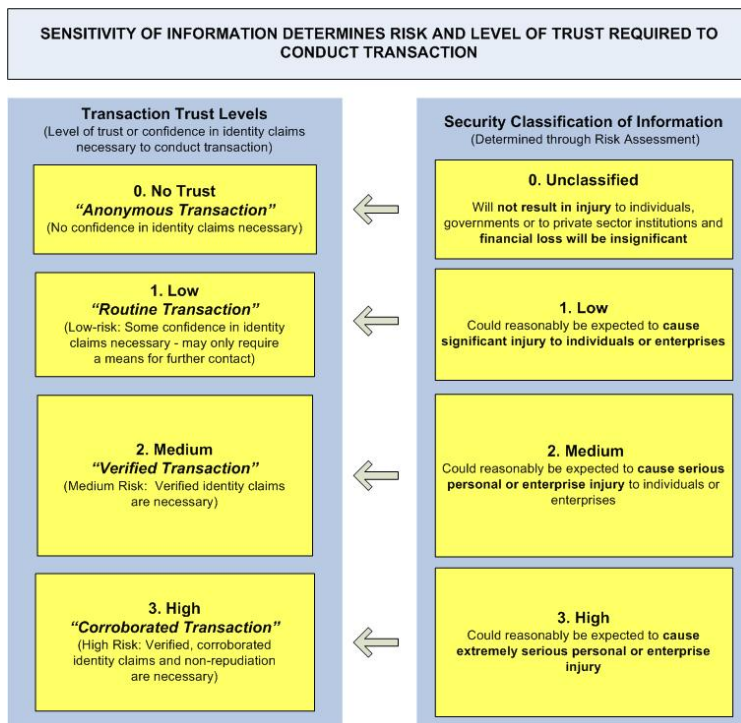
It is generally accepted that the level of assurance attached to an identity claim is dependent on the strength of each component (registration, authentication, authorization) in the Chain of Trust. Thus, assurance can be compromised if any component in the chain of trust is insufficient. For example, an authenticated identity claim that is based on a rigorous identity proofing process, (e.g., a combination of in person registration, verification of presented

¹³ While Authorization is part of the Identity Management “Chain of Trust”, it is not within the scope of the Task Force’s work.

government ID at point of issue and corroboration of identity by a trusted third party), but on a weak authentication credential (such as a password), may not result in a high level of assurance. Similarly, strong authentication credentials (e.g., hardware tokens or smart cards) do not make up for weak identity proofing processes. As a result, a desired level of assurance can only be achieved where agreed upon levels of identification, credential issuance, authentication, and due diligence occur.

A.6.3 The Role of Information Security Classifications and Trust Levels

As set out in the Security Component and summarized here, the level of assurance needed to access a particular service should be based on two factors: the *risk of providing the service* through a given medium; and the *security classification of the information* involved. The Canadian Public Sector Security Classification Guideline developed by the National CIO Subcommittee for Information Protection (NCSIP) will be used as a guideline for determining the security classification of the information and the risk of providing the related service or transaction.

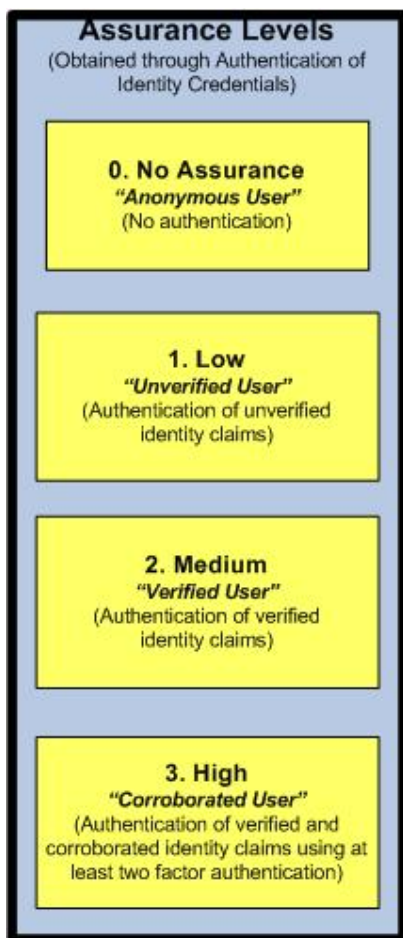


There is a direct relationship between the security classification of information and the level of assurance in an identity claim that is required to permit access to that information or related service. In simple terms, the more sensitive the information or service, the higher the level of assurance that is required to conduct a related transaction.

A Transaction Trust Level (or Trust Level) is a pre-established statement of the level of certainty in an identity claim that is needed to access information or conduct a transaction. The pre-determination of Trust Levels, based on information security classifications and other risk factors, is a necessary first step in the establishment of an overall IdM&A Assurance Model.

A.6.4 Establishing Assurance Levels

An Assurance Level is a relative measure of the strength of assurance that can be placed in an identity claim. A lower level of assurance means less certainty in an identity claim, while a higher level indicates a higher degree of certainty.



The following identity assurance levels map to the aforementioned Trust Levels:

0. No Assurance ("Anonymous User")

- No authentication is performed and no identity claims are made or assured.
- Appropriate for access to public information or for transactions where anonymity is required or preferred (e.g., AIDS/HIV survey).

1. Low Assurance ("Pseudonymous or Unverified User")

- Authentication of a pseudonymous or unverified identity claim. Identity assertions made by a claimant are not verified.
- Results in an account that is similar to an internet mail account (e.g., "hotmail").
- Appropriate for participating in an on-line learning course, signing up for e-mail newsletter or for paying a bill, parking ticket, etc. where no identity is required, only an authorized payment.

*Unverified to Low Verified: If combined with a shared secret match, may provide some additional assurance in an identity claim that could be used to conduct routine personal or business transactions.

2. Medium Assurance ("Verified User")

- Authentication of a verified identity claim. Identity assertions made by a claimant are verified using authoritative parties.
- Appropriate to conduct transactions where a medium level of assurance in an identity claim is required (e.g., online access to tax records, registering a business).

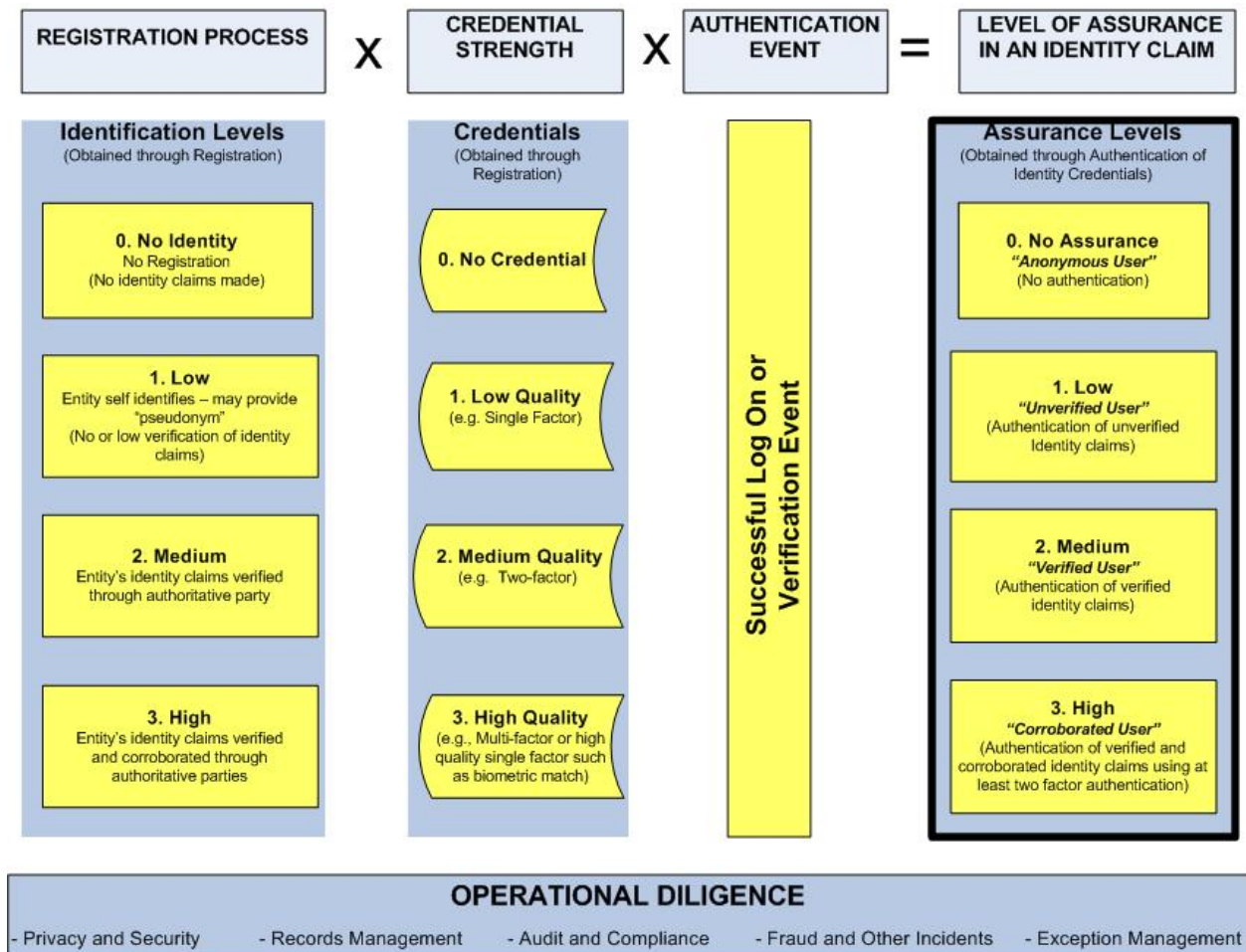
3. High Assurance ("Corroborated User")

- Authentication of a verified and corroborated identity claim. Corroboration of an identity claim by a trusted third party (e.g., lawyer, doctor, minister) is similar to the Canadian passport model.
- Requires at least two-factor authentication
- Appropriate to conduct transactions where a high level of assurance in an identity claim is required (e.g., access to witness protection lists, on line drug prescribing, or access to high security areas).

Figure 13, below, illustrates the fundamental interrelationships between identification and registration processes, credential strength and assurance levels. All of these concepts are

developed further in this section, but at the highest level, identity assurance involves verification of an identity claim through the presentation of credentials associated with that identity claim.

Figure 13. The Assurance Equation



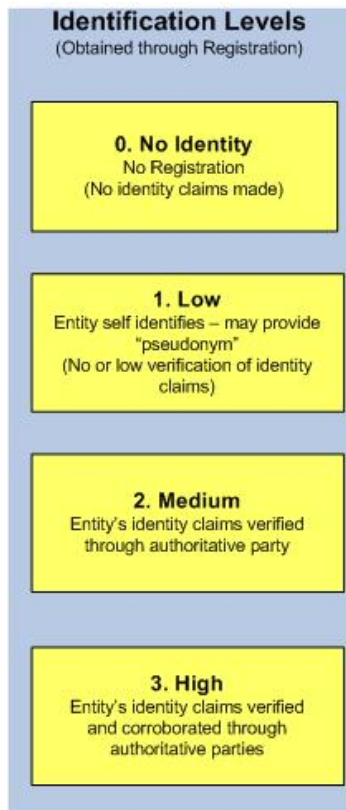
Unlike trust levels, assurance levels cannot be pre-established. Rather, they are created through authentication events (e.g., successful login, in-person verification) and are dependent on a number of factors. The best way to understand an assurance level is to consider it as an equation. It is the compound result of:

- the rigorousness of the original registration and identity proofing process;
- the manner in which an identity credential is issued (in-person, by mail, online);
- the strength of the credential (i.e., number of authentication factors used plus the strength of each factor);
- the authentication event, itself, (i.e., successful log-on, in person verification); and,

- the underlying infrastructure/environment within which the authentication event occurs.

A.6.5 Registration Process

The first step in establishing an Assurance Level that can be mapped to a pre-determined Trust Level is the identification level achieved through a given registration process. The identity of a given entity (i.e., a citizen, an organization, or a government employee) can be substantiated to varying degrees of certainty through different registration processes. Possible levels of identification are:



0. No Identification (“Anonymous Identity”)

- Entity is not identified and no identity claim is associated with the entity.

1. Low Identification (“Pseudonymous, Unverified or Low Verification”)

- Entity self identifies (may provide a pseudonym) and an identity claim is either not verified or it is verified to a low degree (i.e., through a shared secret match or knowledge of file history).

2. Medium Identification (“Verified Identity”)

- Entity is uniquely identified through a managed registration process and an identity claim is verified with documentary evidence or through authoritative source(s).

3. High Identification (“Corroborated Identity”)

- Entity is uniquely identified through a managed registration process and identity claim is both verified against authoritative source(s) and corroborated by a trusted third party (i.e., similar to the Canadian passport model).

Registration, in the IdM&A context, is the process by which a person obtains an identity credential, such as a username or digital certificate, for subsequent authentication. Depending on the level of assurance required, registration and credential issuing can be done in-person or remotely through various channels such as browsers, telephones, mail or on-line.

The registration process may require the person to present proof of real-world identity (such as a birth certificate and passport or driver’s licence) and/or proof of other identity attributes depending on the intended use of the credential (e.g., proof that an individual works for a particular organization). However, as noted above, not all registration processes require proof of a real-world identity. Where only a low level of identification is required, the registration process may not require any proof of identity or it may require the verification of

only a single identity attribute (e.g., age, residency, etc.) And, for unclassified transactions, where no identity claims are made, there may be no registration process at all.

Proof of Identity

Where verification of a real world identity is required by the registration process (i.e., for Medium level identification or higher), proof of identity (or assurance of an identity claim) is commonly established by relying on authoritative parties. There are two primary ways that organizations rely on authoritative parties when verifying identity claims (and sometimes both methods are used):

1. **Evidence Based Identity Proofing** – An identity claim is assured through the presentation and verification of documentary evidence that has been issued by an authoritative party (e.g., a citizen or business representative presents government-issued photographic documentation at a counter).

In this case, standards need to be set for what constitutes acceptable evidence and what documents are authoritative on which identity claims.

2. **Authoritative Party Based Identity Proofing** – An identity claim is assured through direct verification by an authoritative party (e.g., Vital Statistics Agency, Revenue Canada) and/or corroborated by a trusted third party professional (e.g., lawyer, doctor, minister). The verification process may involve the exchange or confirmation of shared secrets.

In this case, standards need to be set regarding what and/or who constitutes an authoritative party.

Standards may also be necessary on the conditions that should apply to the relationship between the trusted third party professional and the person being identified (e.g., the lawyer might need to be in good standing with the Law Society and to have known the person for at least two years).

And finally, standards may be required on what constitutes an appropriate “shared secret”.

The authoritative party used in a given circumstance will depend to a large part on the identity context or role (e.g. citizen, business, doctor, lawyer, government employee) and on the desired identification level. For example, an authoritative party for:

- a. a government employee, could be the employer;
- b. a corporation, could be a Corporate Registry;
- c. a doctor, could be the College of Physicians and Surgeons;
- d. a lawyer, could be the Law Society; and,
- e. a citizen, could be the Vital Statistics Agency, Citizenship and Immigration, Revenue Canada or Revenue Quebec.

The rigor of the identity proofing process directly impacts the Identification Level achieved (i.e., the more rigorous, the higher the Identification Level). The rigorousness of the identity proofing is assessed on two grounds:

- the method of verification (i.e., whether evidence is accepted at face-value or verified at point of issue; whether verification is done in person or remotely; whether evidence is corroborated by a trusted third party professional; etc.); and,
- the strength of the evidence used (e.g., type of document used as evidence, strength of shared secret, etc.).

While not an exhaustive list, Table 2, adapted from the IAAWG's Guidelines¹⁴, provides examples of various identity proofing methods and the corresponding Identification Level that each method might achieve.

Table 2. Relationship between Identity Proofing Methods and Identification Levels

Method of Identity proofing	Identification Level
No identification (likely anonymous)	No Identity
Claimed identity – self assertion (can be pseudonymous) – No verification	Low
Knowledge of file	Low
One shared secret match	Low
Face to face document examination (documents accepted at face-value - no verification at point of issue)	Low - Medium
Face to Face document examination (verification of documents at point of issue)	Medium
Face to face document examination (accepted at face-value) plus shared secret match	Medium
Knowledge of file or shared secret match, plus confirmation to address of record through an out-of-band mail-out	Medium
Two unrelated shared secret matches plus verification of identity information (provided remotely) through authoritative parties	Medium
Face to face document examination (plus verification of documents at point of issue) and corroboration by trusted third party professional (e.g., lawyer, notary, physician, etc.)	High

¹⁴ Identification, Authentication and Authorization Framework Policy and Guidelines – Consultation Draft – November 26, 2004

A.6.6 Identity Credentials and Authentication Factors

The second step in the registration process (once an Identification Level is established) is the issuing of Identity Credentials which can be used at a later time by an individual or business representative to authenticate his pre-established identity claim in order to conduct a transaction or obtain a service.

Identity credentials can be cards like driver's licences or smart cards, documents like passports, or, in the context of digital identities, UserIDs and passwords or digital certificates.



Identity credentials are obtained through a registration process and are attached to the identity that was established through that registration process. The registration process used to issue a credential affects the level of assurance attached to it. For example, identity credentials issued through an in-person registration process generally carry more assurance than ones issued through an online registration process.

The mere fact that an individual possesses a given credential (e.g., a User ID that has been previously registered with an authentication service) provides some level of assurance that when the credential is used, it is being used by the associated real world person. However, the level of assurance can be increased through the association of “factors” with the credential. **Factors**, like passwords, are essentially keys to credentials. Once the keys are used to unlock the credential, there is a presumption that the person that unlocked the credential is actually the person that owns the credential.

While passwords provide some level of proof of ownership, they can be lost or stolen, just like car keys. As such, in some situations, even use of a password may not provide sufficient certainty that the individual using the credential is actually who they purport to be.

The strength of credentials can be increased by using additional factors. For example, a two-factor authentication service would require the coincidence of two distinct security factors, combining two items from the following general categories:

- **Something you know** – e.g., personal history, UserID and password, PIN, mother's maiden name or other shared secret.
- **Something you have** – e.g., identification card, ID badge, hardware token, smart card.
- **Something you are** – e.g., face recognition, signature, fingerprints, retinal scan, voice recognition or other biometric.

Each of these authentication factors is vulnerable to certain threats. For example, passwords and shared secrets may be disclosed by the individual either intentionally or inadvertently through social engineering or “phishing” scams. Hardware tokens and cards may be lost, stolen or duplicated, and biometrics may be replicated. Because of these risks, authentication factors are often combined to increase the security of the authentication. For example, banks require a bankcard *and* a password to conduct an ATM transaction.

When only one factor is used (such as UserID and password), this is referred to as “single-factor” authentication. When two factors are combined (such as UserID and password plus a hardware token), this is “two-factor” authentication. If more than two factors are used, this is known as “multi-factor” authentication.

Authentication Factor Strength

Generally, the more factors that are combined, the more secure the authentication. For this reason, most people assume that two-factor or multi-factor authentication is always stronger than single-factor authentication. But such an assumption ignores the fact that authentication strength is also dependant on the quality of each individual factor. As an example, single factor authentication that relies on a strong biometric like DNA is, on its own, stronger than two-factor authentication that relies on a UserID/password and smart card combination. The strength or quality of an individual authentication factor is based on three general criteria¹⁵:

1. its **fixity** to the person (i.e., physical characteristics and biometrics are fixed to a person (or of the body), identifying numbers and professional credentials are not);
2. its **distinctiveness** (i.e., Social Insurance numbers and fingerprints are distinct or unique, birth dates, names and eye colour are not); and,
3. its **permanence** over time (i.e., DNA and birth dates do not change, hair colour and residential addresses generally do);

Based on this criteria, it is easy to see why DNA is such a strong authentication factor (it scores high on persistence, fixity and uniqueness) and why relying on names (which can change and are neither unique nor fixed to a person) is so problematic. However, the use of biometrics like DNA, fingerprints and retinal scans is an extremely controversial issue and, as an authentication method, probably vastly overqualified for the provision of services to clients.

Selection of the authentication factors to be applied to a credential depends on the level of assurance required for a given transaction. As stated above, authentication strength is a compound result of the strength of each individual factor and the number of factors used.

¹⁵ Jim Harper, *Identity Crisis: How Identification is Overused and Misunderstood*

While not an exhaustive list, Table 3, adapted from the IAAWG's Guidelines, provides examples of different types of credentials and the relative authentication strength they provide.

Table 3. Relative Strength of Various Credential Types

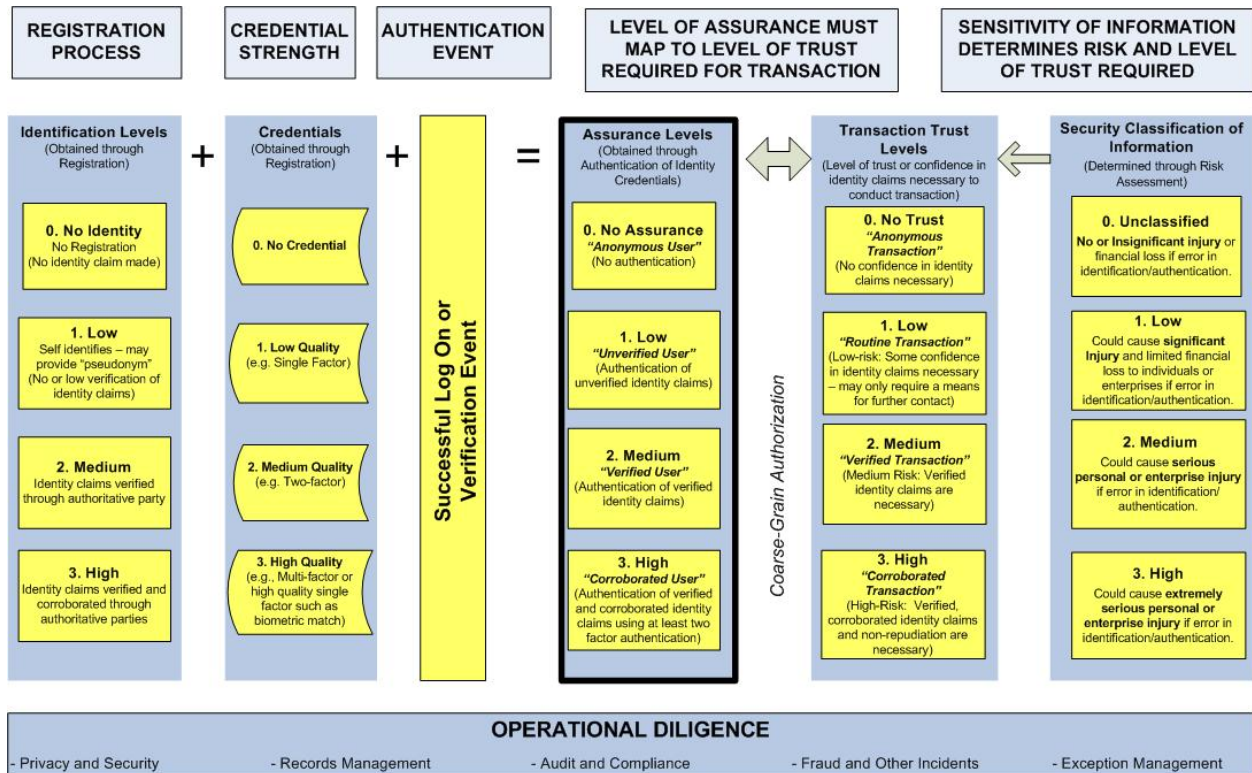
Type of Credential [i.e., authentication factor]	Relative Strength of Credential
No credential	None
Password or PIN	Low
User ID and Strong password ¹⁶	Low
Strong password with PKI certificate	Low
Strong password with PKI certificate having demonstrated user control of private key	Medium
Strong password and authentication token	Medium
Password and biometric	High
Strong password and hardware token with PKI certificate	High
Password and biometric with PKI certificate, and hardware token	Very High

¹⁶ Strong password is a generic password with strong enforced password management policies and standards for example: 6-A characters, mixed letters and numbers, upper + lower case characters, changed regularly, etc.

A.6.7 A Pan-Canadian Assurance Model

Using the concepts developed in this component, the Task Force proposes the following Pan-Canadian Assurance Model:

Figure 14 – Pan-Canadian Assurance Model



This model illustrates several key concepts about Assurance Levels, their relationship to Security Classification Levels and their dependency on registration processes, credential strength and the underlying operational infrastructure and processes (i.e., operational diligence):

1. An assessment of risk based on the Security Classification of Information sets the Level of Trust required for a related transaction or service.
2. This, in turn, dictates the Level of Assurance that is required in an identity claim before permitting access to the transaction or service.
3. Assurance is established through an authentication event (whether it is a successful logon or in-person verification) that is dependent on the rigorousness of the original registration and identity proofing process, the relative strength of the presented credential, and the operational infrastructure and diligence supporting the entire process.
4. Different levels of assurance are created using different combinations of registration processes and credential strength which are, in turn, appropriate for different types of transactions and services.

Next Steps

The Task Force has set out the main issues that it believes should be addressed in the Assurance Component and has proposed an overall Pan-Canadian Assurance Model that encompasses Identification Levels, Credential Strengths, Assurance Levels, Trust Levels and Security Classification Levels based on:

- The work of the former IAAWG;
- Assurance models and frameworks developed by various jurisdictions that were provided to the Task Force; and
- Additional research.

However, the Task Force is aware that work on Assurance Frameworks is ongoing in several jurisdictions; work that was not available to the Task Force, either because it was still in draft or it was still under development. For this reason, the Task Force recommends:

1. That the Assurance Component and Assurance Model be validated through a consultation process across jurisdictions to ensure that it can indeed serve as an inter-jurisdictional model for Identity Assurance.
2. Once this review is complete, the Task Force recommends that the Assurance Component be completed as the starting point for the development of Pan-Canadian standards and policies on identity proofing, verifying identity claims, credential issuing and registration processes over various channels, including:
 - a. Identity Assurance Requirements (including different requirements for different channels, where appropriate).
 - b. Registration Standards including:
 - acceptable registration channels for different levels of assurance (i.e., Is in-person registration necessary to obtain a high level of assurance?)
 - c. Identity Proofing Standards including:
 - acceptable methods of verification, including, criteria for what constitutes an acceptable “shared secret”.
 - acceptable evidence of identity.
 - acceptable authoritative parties for different identity attributes.
 - acceptable trusted third parties to provide identity corroboration (i.e., Do we follow the Passport Canada model?)
 - d. Credential Issuing Standards including:
 - acceptable credential issuing channels for different levels of assurance.
 - relative strength and number of factors required for different levels of assurance (including factors that are unacceptable either because they are too weak or too intrusive).

A.7 Identity Component

The Identity Component sets the framework for how individuals and businesses should be identified by governments in Canada in different contexts; and in this respect is closely related to the Legal and Privacy Components.

While the various contexts in which individuals simultaneously operate are vast (e.g., citizen, patient, parent, business representative, advocate, employee), the Identity Component simplifies these contexts by proposing broad user groups into which individuals and businesses can be categorized. It then sets out a number of identifiers or identity attributes which could be used in each case, depending on the level of identity assurance that is required and on the specific nature of the transaction.

The Identity Component also deals with the maintenance of identifying information and credentials over an identity lifecycle and with the different types of, and requirements for, agency, dependents and designates/delegates.

Based on the key issues arising out of the problem and solution analysis and on the applicable IdM&A Principles, the Task Force has identified six key areas that should be addressed in the Identity Component for the IdM&A Framework:

1. Identity Context
2. Separation of Identity Contexts or Roles
3. Identity Types or User Groups
4. Applicable Identity Attributes by Type
5. The Identity lifecycle
6. Agents, dependents and designates/delegates

A.7.1 Identity Context

From an individual or social science perspective, the notion of identity refers to both a person's image of himself and a characterization of himself with reference to a particular group, practice or ideal. For example, an individual might define themselves in terms of a family, a particular profession, gender, religion or a nation¹⁷.

As set out in problem and solution analysis of this report, people generally have several identities (as opposed to one, dominant identity), where each identity relates to a different aspect of a person's life and/or personality. For example one individual's multiple identities or "identity contexts" could be a mother, a musician, a lawyer, a Catholic and a Canadian¹⁸.

An **identity context** is the situation or context in which an identity (or person) operates (i.e., as a parent, patient, business representative, etc.).

¹⁷ Adapted from Ethical Portfolios: Supporting Identities and Values, Simon Grant and Anna Grant, available at <http://www.simongrant.org/pubs/ep2006/>

¹⁸ Ibid

Because the number of identity contexts in which an individual can simultaneously operate can be vast, many IdM&A Frameworks simplify these contexts by proposing broad user groups into which individuals and businesses can be categorized.

A.7.2 Separation of Identity Contexts or Roles

Distinct business solutions may need to be developed for each distinct “identity type” or user group, consistent with the various personas that an individual might play in their daily life. These different approaches may involve different rules, registration processes and credential management (e.g., the manner in which a patient is identified will differ from the manner in which a hospital nurse or a pharmaceutical representative is identified).

The underlying intent and rationale for this approach is the need to sever a person’s personal identity from their professional or other identities. For example, a doctor is only a doctor when she is acting as a second or third party. Her personal identity attributes and personal records should be totally separate from her identity as a doctor.

The Australian Government e-Authentication Framework suggests that grouping users into categories better supports a structured and manageable approach to deploying and managing identity management and authentication approaches. It offers the following guidelines for determining user categories (“identity types”):

- the similarity of interactions or relationships of a group with the target organization (in this case governments in Canada);
- the inherent risk profile of such groups;
- the capacity and willingness of members of a group to adopt the same approaches to e-authentication and the registration or enrolment processes; and,
- the extent to which groups already possess e-authentication credentials issued by the agency, another agency or a trusted third party.

A.7.3 Identity Types or User Groups

As stated above, grouping identities into categories based on common characteristics and on their relationship to government provides more structured and effective identity management. It also allows for the consistent application of security decisions (e.g., assurance levels).

While the numerous contexts in which individuals operate could result in many different categorizations, the Task Force recommends, as a starting point, the recognition of at least three distinct user groups¹⁹:

1. Citizen to Government (C2G)

This category which is sometimes referred to as “external individual” includes all individuals who request or receive services from government.

¹⁹ Adapted from IAAWG’s *Identification, Authentication and Authorization Framework Policy and Guidelines – Consultation Draft* – November 26, 2004

2. Business to Government (B2G)

This category which is sometimes referred to as “external organization” includes businesses and other external organizations (societies, not-for-profit organizations) that interact with government. In some jurisdictions, this may also include the broader public sector (e.g. school boards, health authorities, etc.). The business or external organization is generally accountable for all actions of individuals acting on its behalf.

3. Government to Government (G2G)

This category which is sometimes referred to as “internal individual” includes government employees, or other individuals acting in that capacity (e.g., contractors, business partners or other affiliates that provide services on behalf of government).

A.7.4 Applicable Identity Attributes by Identity Type

In keeping with the applicable IdM&A principles of using “proportional and appropriate means” and the “least amount of identity information”, an IdM&A process should only collect and verify identity claims where necessary and to a level that is commensurate with the sensitivity of the transaction or service being requested. Table 4, below, maps Identity Types to the Identity Assurance Levels established in the previous section.

Table 4. Identity Types mapped to Identity Assurance Levels

		Assurance Levels			
		Level 0 “Anonymous”	Level 1 “Unverified”	Level 2 “Verified”	Level 3 “Corroborated”
Identity Types	Citizens (C2G)	<ul style="list-style-type: none">No identity assurance is necessary – user is anonymous.No distinction of identity type necessary.	<ul style="list-style-type: none">Identity Claim is made (which provides some assurance) but not verified.Pseudonym may be used.May or may not know identity type.	Unique citizen identity verified.	Unique citizen identity verified and corroborated by trusted third party.
	Businesses (B2G)			Unique business identity verified.	Unique business identity verified and corroborated by trusted third party.
	Government Employees (G2G)			Unique employee identity verified.	Unique employee identity verified and corroborated by trusted third party.

For some services, no assurance of identity is required and there will be no need to distinguish whether a person is a citizen, business or government employee.

For other services, some identity assurance may be necessary, but only to enable further contact or to verify that this “identity” is the same “identity” that was here before. It is also possible that a service may need to know that an “identity” is part of group of identities (i.e., a government employee, business representative, or university student) but doesn’t need to link the identity to a particular individual. Identity attributes collected and verified in these

cases will vary, depending on the eligibility requirements of the service and, in some cases, may only require the provision of a contact name (which may or may not be a pseudonym).

However, some services offered by government will require the identification and verification of a specific individual or business. Where this level of identity assurance is required, identity attributes collected must be sufficient to provide a unique identity that can be linked to specific person.

Identity Attribute: a quality or characteristic ascribed to a person (i.e., citizen, business or employee) that may or may not be unique.

While there is currently no agreement across jurisdictions on how individuals and businesses should be uniquely identified, the following attributes by identity type are most commonly used, either alone or in combination:

For Citizens:

- ⇒ legal name;
- ⇒ date of birth;
- ⇒ residential address;
- ⇒ Social Insurance Number, where permitted by law or policy;
- ⇒ registration number on birth certificate, citizenship certificate, or permanent resident card;
- ⇒ driver's licence number, and/or,
- ⇒ other program specific identifiers.

For Businesses:

- ⇒ Business Number (for those agencies that are permitted to collect it);
- ⇒ Legal Incorporated or Registered Name;
- ⇒ Operating Name;
- ⇒ Incorporation Number and Jurisdiction of Incorporation;
- ⇒ Name(s) of principals, partners, or proprietor;
- ⇒ Registered Address and Mailing or Operating Address (if different); and/or
- ⇒ Other program specific identifiers.

For Government Employees:

- ⇒ legal name;
- ⇒ title, department, and ministry/agency;
- ⇒ work address, telephone number, email address, etc.;

- ⇒ employee number;
- ⇒ professional designations; and,
- ⇒ for the purpose of human resource services, date of birth, social insurance number and home address.

Identifying citizens, businesses and government employees in standard ways in similar contexts would go a long way to facilitating interoperability and engendering trust between IdM&A services and across jurisdictions, where appropriate.

Standardizing the format in which identity attributes are collected (e.g., name and date format) is also important.

The development of both semantic and syntactic data models or standards should, therefore, be considered.

A.7.5 The Identity Lifecycle

In addition to identifying and authenticating the identity claims of individuals and organizations, identity management is also about maintaining information about a person's identity or identity credentials over time (i.e., over the full identity lifecycle).

For example, the identity lifecycle establishes stages for the creation, use, termination and archival of physical and electronic credentials that apply to each identity type.

The four stages of the Identity Lifecycle are:

1. **Verification:** this includes registration, identity proofing and authentication processes.
2. **Provision:** this includes the issuing of credentials and the assigning of roles and privileges.
3. **Usage:** this includes both the first time the credential is used (which may necessitate an enrolment process and/or file matching) and all subsequent uses.
4. **Disposition:** this includes the deprovisioning and archiving of the credential.
 - **Deprovisioning** can occur through normal processes (i.e., the credential expires) or for specific causes (e.g., fraud).
 - **Archiving** the credential may be done to meet evidentiary requirements.

As part of the Identity Lifecycle, agencies may need to set up accounts associated with a client's identity credential and manage activities such as:

- Changes to identity attributes associated with a credential (e.g., name and address changes);
- Changes to roles and privileges associated with a credential;
- Expiration and renewal of an identity credential;
- Revocation of an identity credentials (e.g., because an employee leaves a company)

- Suspension of an identity credentials (e.g., due to suspicious or inappropriate use)
- Password reset or expiration.

A.7.6 Agency, Dependants, Designates and Delegates

The Identity Component should also deal with the issue of agency, dependants, designates and delegates. In some jurisdictions and situations, this is treated as an authorization issue. Each individual or business representative is identified and issued an identity credential in their own right, and then, upon being authenticated, their role and authority as an agent or delegate, etc. of a client is verified separately by each service agency. In other situations, however, the role and authority of an agent or delegate, etc. is established during the initial registration, identity-proofing and credential issuing process. For example, the role, authority and permissions of a business representative of a particular company could be built into the associated identity account and credential.

A Pan-Canadian Framework for IdM&A could provide guidelines as to when the issue of agency, dependants, designates and delegates is best left to the service agency or relying party to determine and when it is best established at the time of registration by the credential issuer. Standards for verifying agency, dependants and delegates, including acceptable evidence of the relationship, would also be helpful.

Next Steps

The Task Force has set out the main issues that it believes should be addressed in the Identity Component based on the key challenges it identified in the problem and solution analysis and on the guiding IdM&A Principles it developed.

More work is necessary to complete this component and to develop standards and models that could flow from this component. In particular the Task Force recommends the development of:

- Standards for identifying clients in different contexts and to different levels of assurance.
- Common information (e.g., semantic and syntactic) standards or models to facilitate interoperability of identity management services.
- Standards for maintaining identity information and credentials through the full identity lifecycle, including names changes, changes to roles and permissions, and the expiry, renewal, suspension and revocation of identity credentials.
- Standards for identifying agents, dependants, delegates and designates and for verifying their relationships to clients.

A.8 Trust Component

The Trust Component sets out the essential requirements for the establishment of trust relationships between parties involved in IdM&A services. It essentially deals with how one party can trust another party's identity assertions. The component also sets out the different trust roles involved in assuring identity claims and issuing and accepting credentials (e.g., client, relying party, authoritative party, etc.).

Guidelines for establishing trust between parties in a way that is commensurate with the assurance model may flow out of this component. For example, trusting another party's "high" assurance assertions likely requires more compliance-related activity than trusting their "low" assurance assertions.

Based on the key issues arising out of the problem and solution analysis and on the applicable IdM&A Principles, the Task Force has identified five key areas that should be addressed in the Trust Component for the IdM&A Framework:

1. Trust Roles;
2. Trust Models for IdM&A Services;
3. Managing Trust Relationships;
4. Transparency; and,
5. Engendering Client Trust.

A.8.1 Trust Roles

Trust Roles apply to the parties involved in the provision, verification and use of identity claims and credentials. In the Identity Lifecycle, there are a number of roles that describe the interaction (or trust relationship) between parties:

- 1 **Client** – a person (citizen or business representative) seeking service.
- 2 **Client-Agent/Delegate** – a person acting on behalf of a Client who may or may not assume responsibility or liability for the client (depending on the nature of the agency or delegation).
- 3 **Registrar** – a party that collects and verifies identity claims a client makes during a registration process.
- 4 **Credential Issuer** – a party that manufactures and issues a credential asserting identity attributes or privileges associated with a client.
- 5 **Relying Party** – a party that accepts a credential and its assertions to conduct a transaction with a client.
- 6 **Authoritative Party** - a party whose authority to make claims is recognized by one or more relying parties. Claims made by recognized authoritative parties are used by relying parties to make access control decisions.

It is important to note that there is not always a one-to-one relationship between a role and a party. A party may often perform more than one role, particularly in more traditional service models. For example, an Authoritative Party may also be a Credential Issuer (e.g., Vital Statistics, Passport Canada) and centralized IdM&A services may have one organization that is responsible for Registrar and Credential Issuing services. However, as IdM&A Services evolved, specialized trust roles performed by trusted third parties became more common.

A.8.2 Trust Models for IdM&A Services

Figure 15 illustrates a more traditional model for IdM&A services where one organization functions as registrar, credential provider and relying party. In this model, the organization provides all the trust role services for clients that present themselves for service. The organization issues the credential and provides access based on its reliance (or trust) in its own identification process.

Figure 15. Traditional Trust Model for IdM&A Services

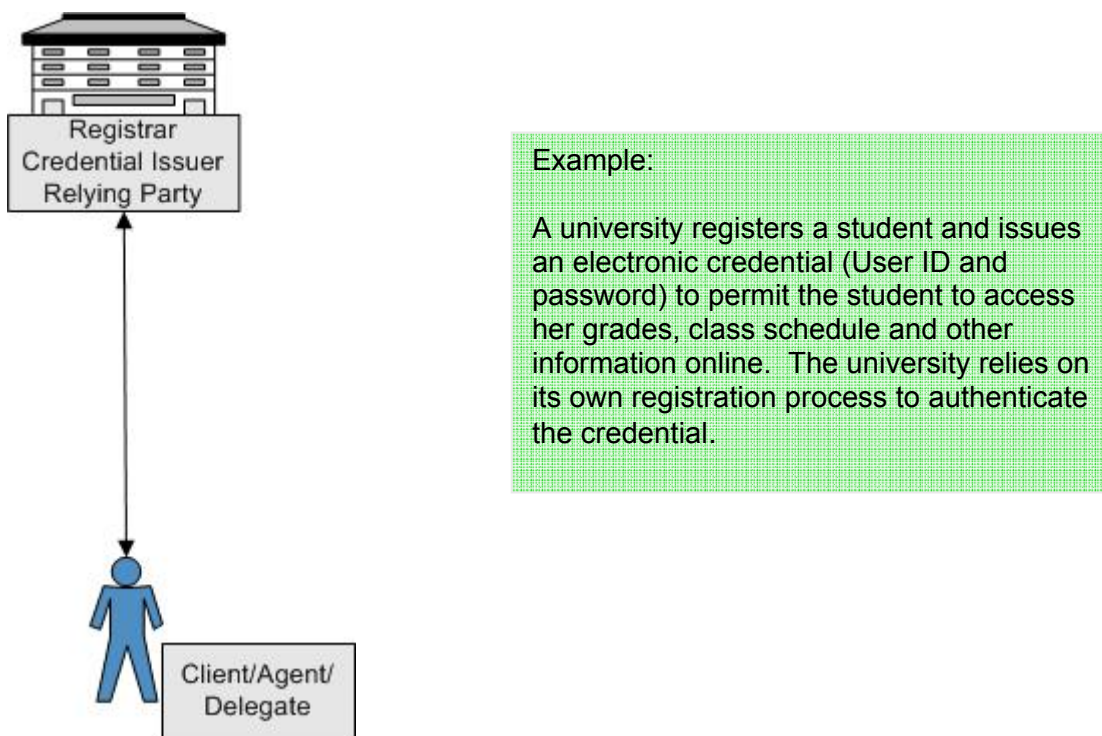
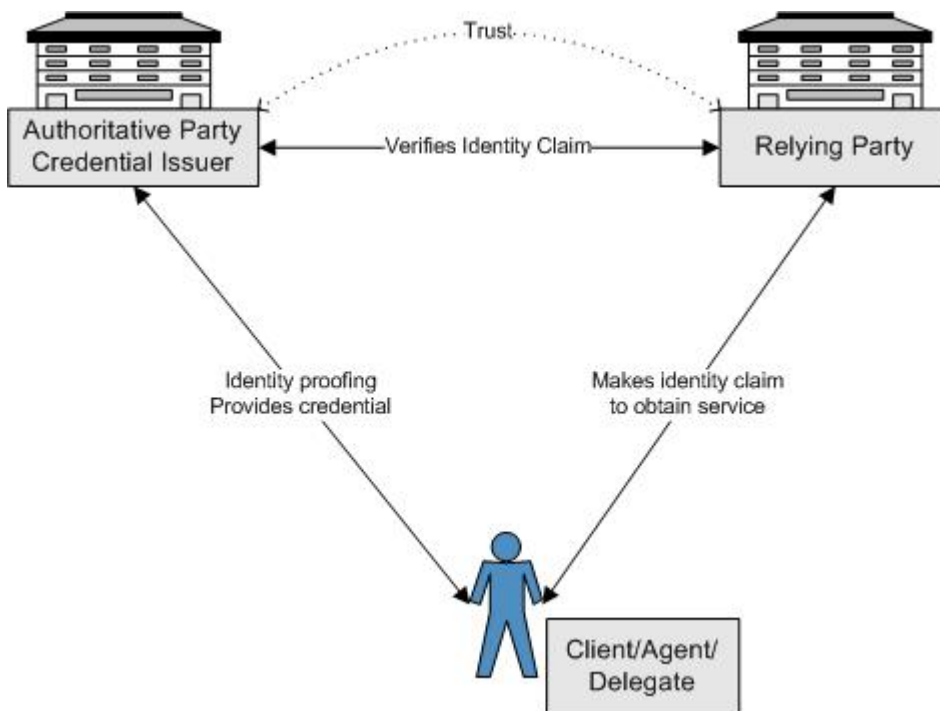


Figure 16 illustrates another common model whereby a client uses a credential issued by an authoritative party (e.g., passport, birth certificate, driver's licence) to prove his identity for the purpose of receiving a service. The Relying Party recognizes the authority behind the credential and/or accepts the assertions of the Authoritative Party. The Trust relationship may be one-way where the Relying Party accepts the authority behind the credential at face value (e.g., compares photo on driver's licence to client requesting service) or it may be two-way where the Relying Party is able to verify the authenticity of the credential or an identity claim directly with the Credential Issuer/ Authoritative Party.

Figure 16. Traditional Model for IdM&A Services with Reliance on Authoritative Party

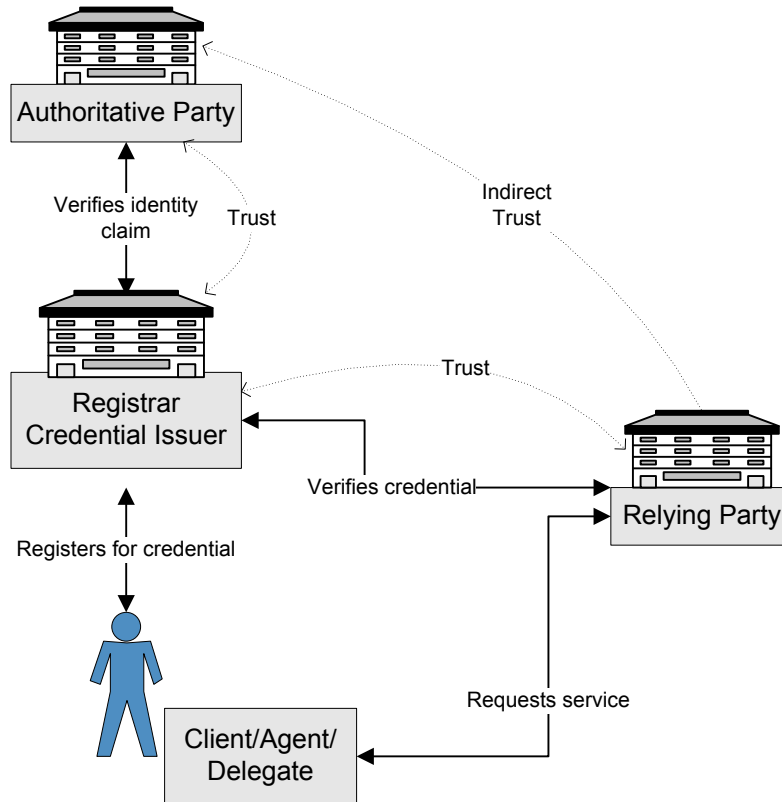


Examples:

1. A citizen uses his driver's licence (the credential) issued by a provincial driver licensing agency (the Authoritative Party) to prove an identity claim made to Elections Canada (the Relying Party) in order to be allowed to vote. In this case, Elections Canada accepts the credential at face-value.
2. A citizen uses her birth certificate (the credential) issued by a Vital Statistics Agency (the Authoritative Party) to prove an identity claim made to Service Canada (the Relying Party) for the purpose of applying for a Social Insurance Number (SIN). In this case, a two-way trust relationship exists whereby Service Canada verifies the authenticity of the birth certificate at source. Once the SIN is issued, Service Canada then becomes an Authoritative Party on the authenticity of the SIN (another credential).

Figure 17, below, illustrates a distributed trust model for the provision of IdM&A services. This is a more mature model where we see the emergence of specialized trust role services. In this example, trusted third parties provide Registrar and Credential Issuer services. E-pass, BCeID and ClicSÉQUER are examples of trusted third parties who provide centralized registrar and credential issuing services. Additionally, the Registrar trust role may rely on Authoritative Parties to provide a sufficiently high level of assurance for the proof of identity. BCeID and ClicSÉQUER rely on authoritative parties for identity assurance (e.g., Revenue Quebec, Vital Statistics, Corporate Registry, etc.) while E-pass does not.

Figure 17. Distributed Trust Model for IdM&A Services



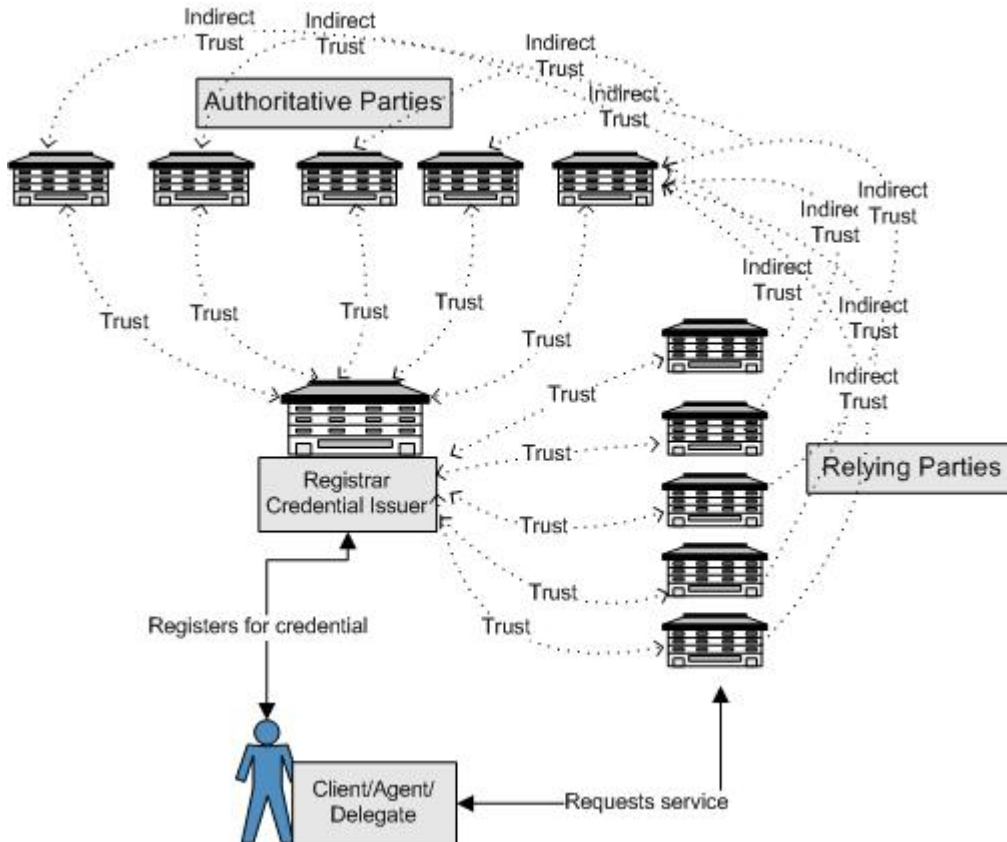
Examples:

The federal E-pass service, British Columbia's BCeID service and Quebec's ClicSÉCUR service are examples of trusted third parties who provide centralized registrar and electronic credential issuing services for their respective jurisdictions. The Relying Parties are a variety of government programs within each jurisdiction that offer online services and accept the electronic credential.

BCeID and ClicSÉCUR rely on Authoritative Parties for identity assurance (e.g., Revenue Quebec, Vital Statistics, Corporate Registry, etc.) while E-pass does not. E-pass offers an unidentified credential.

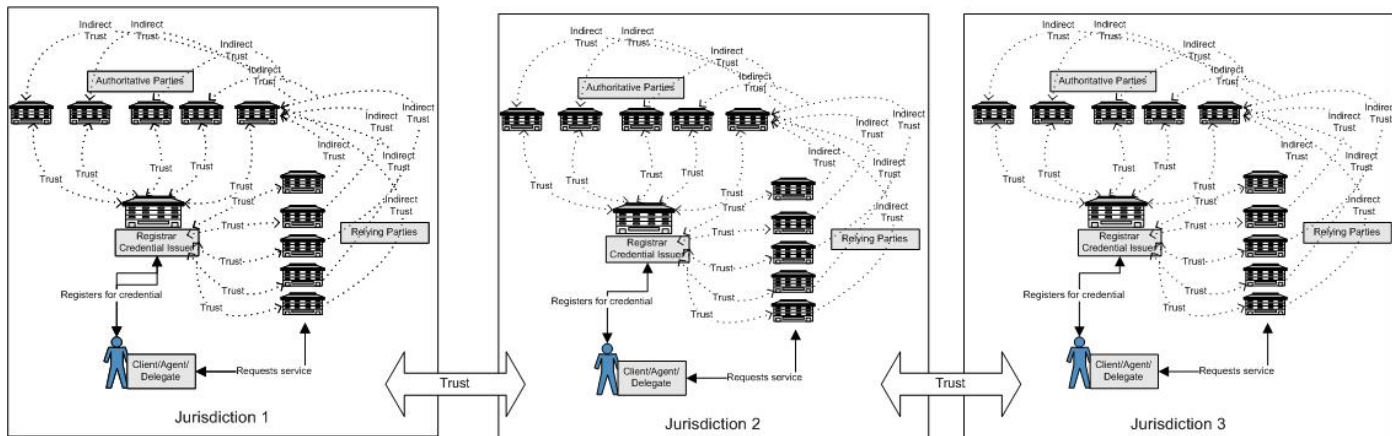
The above models offer a simplistic view of the trust relationships that exist between various parties involved in the provision and use of IdM&A services. The models are simplistic in that they only depict one relying party and one authoritative party. The real world is much more complicated in that there are commonly multiple authoritative parties and multiple relying parties involved in verifying and accepting identity claims. Figure 18, below, while still grossly simplistic illustrates the exponential growth of trust relationships with the addition of each relying or authoritative party.

Figure 18. Multiple Parties, Multiple Trust Relationships



If one were to extend this model to an inter-jurisdictional model, the complexity and number of trust relationships would grow even more as illustrated below in Figure 19.

Figure 19. Interjurisdictional Trust Model for IdM&A Services



A.8.3 Managing Trust Relationships

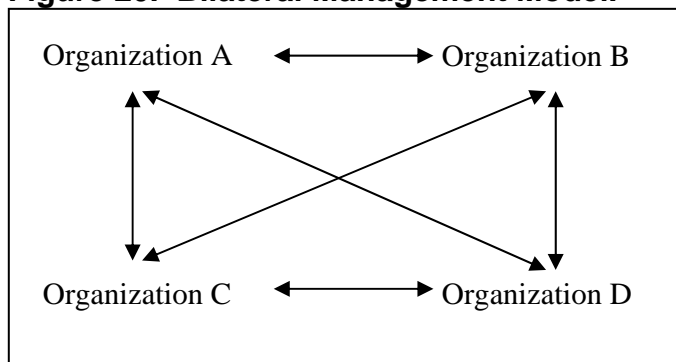
Trust Relationships are commonly managed through contracts, memoranda of understanding (MOUs), service level agreements and other tools. Information Sharing Agreements (ISAs) or other instruments may also be used to document and govern how information, including identity information, is shared between organizations and what the requirements are for its use, retention and eventual disposition.

Information sharing, particularly when identity information is involved, is problematic for a number of reasons. Concerns over the legality of the information sharing in the context of IdM&A, particularly given privacy and confidentiality regulations, are prevalent. Other barriers to the viability of information sharing include procedural uncertainties, technological barriers to systems interoperability, absence of mutual trust, and conflicting understanding of the implications of confidentiality.

In the absence of an overall strategy for delivering IdM&A services and sharing information, governments, trusted third parties and other stakeholders may establish bilateral agreements. In a **bilateral management model**, illustrated in Figure 20, below, individual program areas or organizations create contracts, ISAs, or MOUs to formalize the requirements and responsibilities needed to interact. Used extensively in government, these agreements are usually completed on an ad-hoc basis in response to specific business requirements within government. Standardizing the wording of bilateral agreements could be used to manage IdM&A trust relationships both within a jurisdiction and in a Pan-Canadian context by defining processes, standards and audit requirements.

However, the administrative burden of negotiating, maintaining and updating bilateral agreements is quite high. As illustrated in the models above, a single organization can end up managing dozens or hundreds of individual MOUs. If one considers that four organizations participating in a federation of identity services require six bilateral agreements, one can see how this could quickly become unmanageable. As new parties are added to the federation, the number of agreements increases exponentially (e.g., five organizations require 10 bilateral agreements).

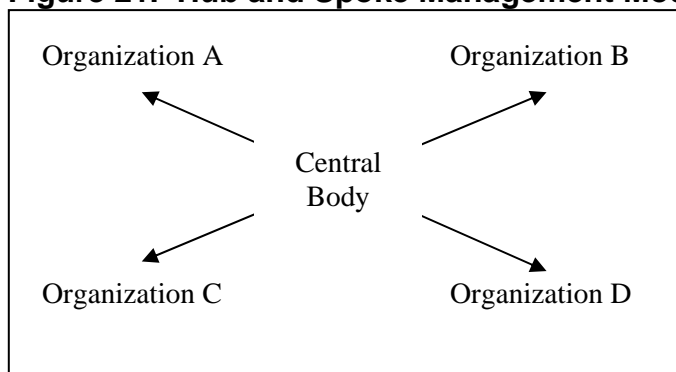
Figure 20. Bilateral Management Model.



A federation is a group of organizations that agree to a set of policies for exchanging information about users and resources to enable access and use of services. In a **Hub and Spoke Management Model**, illustrated in Figure 21, below, each organization agrees to comply with a common set of roles, responsibilities and rights. The policies and operating

procedures are imposed by the federation and enforced to ensure compliance. Government organizations use this management model for functions governed by central agencies (e.g., Human Resources, Finance, Chief Information Officer). As in the case with the Public Key Infrastructure, organizations adapt their operations to comply with the centrally defined policies, procedures and practices. Operational practices are specified and relying organizations can trust that processes carried out by other organizations are sufficient for their business process.

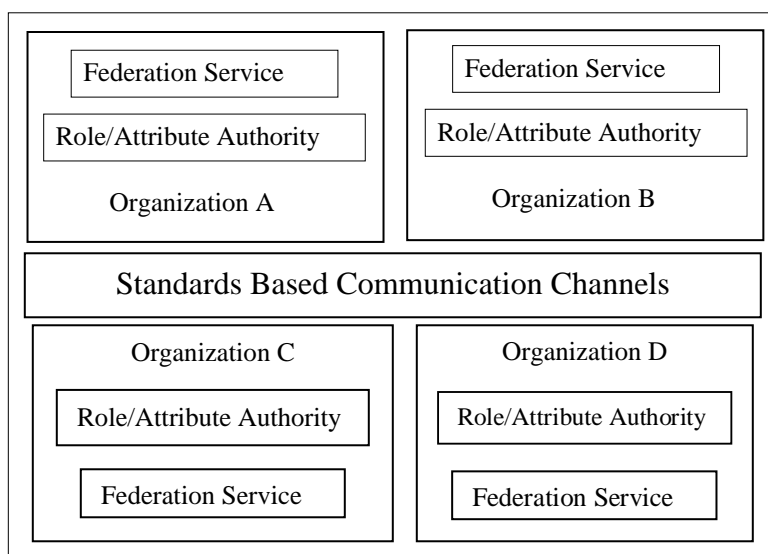
Figure 21. Hub and Spoke Management Model



In a **Circle of Trust Management Model**, illustrated in Figure 22, below, individual organizations act as authoritative sources for identification using standard data sets to exchange or verify identity information (e.g., Security Assertion Markup Language (SAML), Security Provision Markup Language (SPML)). Operational practices are based on standards, but relying organizations must determine if the processes carried out by other organizations are sufficient for their business process.

In contrast to the Hub and Spoke Model where the Central Body (or Root Authority) accepts some of the liability for partner interactions, in the Circle of Trust Model, the Relying Party accepts the risk for interacting with other partners.

Figure 22. Circle of Trust Management Model



Challenges of Wide-Scale Identity Federation

When a federation is formed with a small number of organizations, it is relatively easy to manage costs and complexity. In this case, trust is based on a common understanding of obligation and rights, and the expectation that members will act accordingly.

However, as the federation expands to include more organizations, and possibly multiple jurisdictions, cultural norms and legislation will vary and more effort will be required to confirm that organizational behaviours remain aligned with the obligations and rights of membership. Table 5, below, illustrates four areas that require process streamlining and coordination for wide scale federation adoption. For example, Business Standards should be managed through global federation requirements rather than a multitude of peer-to-peer agreements. Similarly, Certification Audits are more likely to be successful if federation members already have a high level of organizational maturity with practices based on international standards.

Table 5 - Wide Scale Federation Requirements²⁰

Trust	Liability	Risk	Compliance
Business Standards	Defined Liability	Pooled Knowledge	Privacy Legislation
Minimum Requirements	Federation Agreement(s)	Revocation Procedures	Security
Policy and Procedures	Dispute Resolution	Identity Theft and Fraud Protection	Certification Audits

A.8.4 Transparency

Transparency is another key requirement to the establishment and maintenance of effective trust relationships. Transparency in policies, processes, rules, and decision-making are all important.

A.8.5 Engendering Client Trust

So far, this section has focused solely on the trust that is necessary between organizations engaged in providing and using IdM&A services. As daunting a challenge as that is, engendering public trust in IdM&A services is perhaps even more crucial. The public's trust in an IdM&A system is an essential precondition for its successful implementation, diffusion and adoption.

As set out in the Security Component, providing a secure environment is one requirement but it is likely not enough on its own. To engender public trust, IdM&A systems have to be client, rather than government, centric. Wherever possible, clients should be provided with choice and control over the use of their identity information in order to obtain services. Client trust will also likely require transparent policies and processes and clear terms and conditions that bind how an organization may use a client's identity information. And finally, easy access to information and dispute handling processes may also help.

²⁰ Adapted from Federated Identity Management, p. A, PingID Network, Inc., 2002

Next Steps

The Task Force has set out the main issues that it believes should be addressed in the Trust Component based on a review of various trust management models that are currently used by organizations across Canada and in other jurisdictions.

While further work is required on this component, the direction of the work is dependent on the management model or models chosen and on the governance structure that is eventually set up. For this reason, the Task Force makes no recommendation on a specific trust model. However, the Task Force does recommend:

- that, regardless of the model chosen, particular attention be paid to transparency – in processes, policies, standards, rules decision-making, etc.;
- that standard templates or language be developed for MOUs, ISAs and other agreements that may be used to manage trust relationships;
- that standards and/or guidelines be developed in four key areas: Trust (including business standards, minimum requirements, policy and procedures); Defining Liability; Assessing Risk; and Audit and Compliance; and,
- that IdM&A systems be designed and operated in a client, rather than government, centric fashion.

A.9 Service Management Component

The service management component sets out the context within which service management requirements are applied to identity management and authentication. It includes both the client and government perspectives, ranging from simple, consistent client experiences to risk-based, secure, transparent processes. This component could lead to the development of common service standards and functional models that enhance the client's experience and add value for public sector partners.

Service management is concerned with the end-to-end process of creating, delivering, managing and improving services that are client driven. As a result of the problem and solution analysis and in accordance with the resulting principles, the Task Force has looked at identity management and authentication concepts and issues that are important service management considerations, to form the basis for the IdM&A Service Management component including:

- Service design driven by client needs and a common vision;
- Service delivery and management; and,
- Service standards and continuous improvement.

A.9.1 Service Design Driven By Client Needs and A Common Vision

When designing or redesigning services, it is important to consider the whole process from the client's perspective, as it crosses inter-jurisdictional (and intra-jurisdictional) lines to ensure all needs are met. The following list of design requirements have been distilled from the IdM&A Framework principles to distinguish between client and government perspectives, and to assist in the future development of service and functional models.

There are 10 client-facing IdM&A requirements that are essential to service design and should be incorporated to the extent possible, in each case. They reinforce the need to address client expectations for intuitive, responsive and consistent experiences, where clients have choice, consent and control. The requirements are that clients:

- I. Have a *choice of channels* to authenticate their identity when accessing services without being disadvantaged by doing so (Principle 2).
- II. Give *informed consent* to the collection, use and disclosure of their identity information (where consent is required); and where appropriate, be able to revoke consent at a later date (Principle 2).
- III. Are empowered to *control* their own identity credentials and the transfer of their identity information between identity providers and service providers to the extent possible. (Principle 2).
- IV. *Figure prominently* in any identity management and authentication process. IdM&A processes should be *responsive* to client needs and capacity (i.e., intuitive, convenient

and sensitive to client cultural, linguistic or disability needs). (Principle 4).

- V. Experience *simple, consistent IdM&A processes* (for services that require a similar level of assurance) that enable the separation of their different roles (citizen, employee, business) (Principle 4).
- VI. Experience *similar identification and authentication requirements over different channels* except where the unique nature of the channel or service significantly changes the risk (Principle 4).
- VII. *Exercise control over their information and credentials*, based on plain language in all communications, and sufficient information to ensure they understand the IdM&A process and the directions they receive, to maximize accessibility to services and make informed choices (Principle 4).
- VIII. Have a mechanism for confirming the *authenticity of service providers* (particularly remotely) to assure themselves that they are accessing the right website or speaking to an authorized representative of the service provider, such that transparency and trust are enhanced (Principle 6).
- IX. Have *access to their identity-related information* and know what parties have access to it and why, thereby ensuring the process is open, transparent and understandable (Principle 7).
- X. Have a clear understanding of their *role and risks* using the IdM&A process, and are accountable and responsible for their actions (Principle 7).

There are also 10 internally focused IdM&A requirements essential to service design. Generally they address governments' need for a trusted and secure environment in which to take a justifiable, risk based and cost effective approach to the collection of personal information that is limited for a specific purpose, reflects the different roles clients play, and is flexible and scaleable.

Therefore the key internal identity management and authentication requirements to base service designs on, to the extent possible, are that government processes:

- I. Have a *clear need* to collect, use, retain or disclose client identity information (Principle 1).
- II. Only use client identity information *authorized* by a jurisdiction, program or legislation (with limited exceptions). (Principle 1).
- III. Use a *risk-based approach* that balances the privacy and security of identity and other sensitive information, and is proportionate to the program goals (Principle 1).
- IV. Demonstrate *cost effectiveness*, with benefits over costs for clients and government while preserving privacy, security, program integrity and other rules (Principle 1).

- V. *Collect, use and retain the least amount of information* as possible, limited to the use it was collected for (unless the client consents to a new use) and limited to parties that have a justifiable place in the transaction (Principle 3).
- VI. *Recognize, preserve and promote the different contexts* in which clients operate (citizen, business, employee), and use inter-operable systems run by multiple identity providers to give clients choice, where possible, over their means of identification across contexts (Principle 6).
- VII. Use *secure and trusted* practices and technology and ensure accuracy and integrity of data when authenticating the identity of clients, supported by auditing processes (Principle 6).
- VIII. Are *transparent* and understandable to all parties, including the client's ability to know who has access to their information and why and to request access to their identity related information (subject to laws and exceptions) (Principle 7).
- IX. Are clear about who is *accountable* and responsible for what actions, acknowledging identity management as a collective responsibility for all parties (clients, authoritative parties, relying parties) (Principle 7).
- X. Support an *enduring solution that is* flexible and modular, technology-neutral, scaleable for the addition of clients or other parties without affecting the proper functioning of the process/principles/rules, and that does not increase administrative weight and complexity (Principle 8)

There is a need to develop common IdM&A standards, guidelines, business processes, and business architecture to guide interjurisdictional partners in conducting business for maximum efficiency and best results. Examples of IdM&A architecture models that are currently used or under development in Canada and elsewhere in the world are set out in **Appendix G**.

These standards, guidelines and processes should include IdM&A business process mapping to illustrate the most efficient flow or sequence of activities and identify duplication or areas of concern.

A.9.2 Service Delivery and Management

Given the novelty of the identity management and authentication discipline, and the significant transformation it will entail, it will be critical to define common operational models and detailed customer service, training and communication guidelines and standards.

Staff will need to fully understand and deliver what is needed and expected, including what to tell customers about how to access services involving identity management and authentication, what the processes are and what they can expect. This could be based on common models and include a front-end catalogue of life event services with intuitive screens, consistent processes, etc. Workflows will have to be developed to co-ordinate and facilitate authenticated transactions among partners and technology. Roles and responsibilities and service delivery requirements should to be defined and new standards

applied (such as level of assurance, and inter-operability needs). It will also need a clear understanding of interfaces, controls and options, and common terms to foster a consistent understanding. In this situation, the processes should be grounded in trusted, collaborative inter-governmental partnerships and coordination.

This may require the development of IdM&A operational processes, standards and measures, and systems and channels to ensure efficient, effective service delivery.

This may also require the development of generic service level agreement and memorandum of understanding templates to eliminate unnecessary duplication.

A.9.3 Service Standards and Continuous Improvement

Generally, service standards are developed for all main aspects of service management, and include specifics for areas of special interest, such as accessibility for people with disabilities. There is a need for common IdM&A performance indicators based on IdM&A desired outcomes to measure and track customer satisfaction against expectations, and the effectiveness of the service outcomes, to determine priorities for improvement.

This will require the development of IdM&A performance measures and a process to monitor their effectiveness.

Next Steps

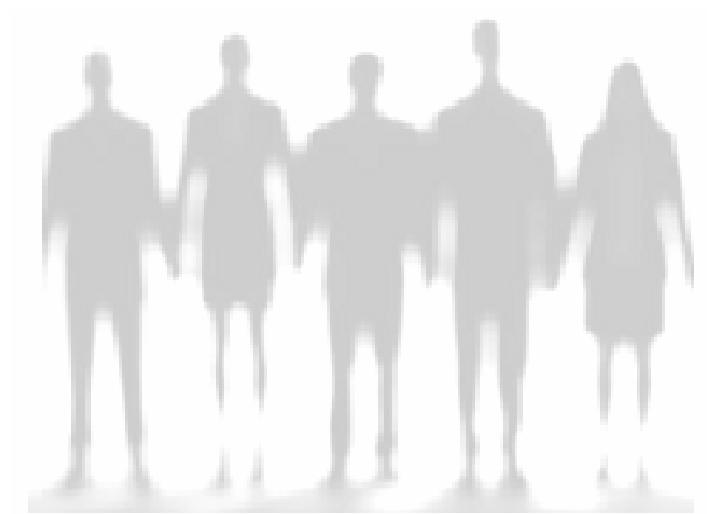
The Task Force has taken a preliminary look at the main issues it believes should be addressed in the Service Management Component based on:

- the service outcomes identified in its Interim Report;
- its knowledge of service management best practices; and
- the applicable IdM&A principles.

The Task Force believes that the work done to date on the Service Management Component would benefit from a review and completion by individuals with more experience in service management best practices and therefore recommends that:

1. The Service Management Component be reviewed by more expert bodies such as the Joint Councils to build on and confirm the content and direction.
2. Once that review is completed, IJAC consider:
 - Developing guidelines for the service design requirements.
 - Developing common IdM&A standards, business processes, business architecture, business process mapping and IdM&A performance measures which, over the longer term, could be incorporated into a Governments Strategic Reference Model (GSRM).
3. The IdM&A Vision, Framework and Principles guide future service design and delivery.
4. IJAC assess lessons learned from pilot projects to develop common Memorandum of Understanding and Service Level Agreement templates for use by partners implementing IdM&A related services, and other aspects of the Framework.

Appendices and References



Appendix A

Task Force Meetings and Consultations

To undertake the work involved, the Task Force Working Group and Steering Committee held a number of consultations and meetings.

Set up Meetings and Consultations

- December 2006: Planning meeting in Toronto
 - Established priorities
 - Developed high level work plan
- January 2007: Recruited members of IATF Working Group and Steering Committee and consulted with key stakeholders to:
 - Draft Terms of Reference
 - Establish Deliverables
- February 2007: First meeting of the Steering Committee in Edmonton.

Task Force Working Group In-Person Meetings:

- January 2007: First meeting of the IATF Working Group in Calgary
 - Developed detailed work plan, assigned tasks and deadlines.
 - Teleconference with co-chairs of the former Identity, Authentication & Authorization Working Group (IAAWG) about linkages with the National Committee on Identity Management and Authentication (NCIMA).
- February, 2007: Second Meeting of the IATF Working Group in Victoria, held in conjunction with attendance at the 8th Annual Privacy and Security Conference and Exposition on *"Identity Management and Information Protection in the Digital World. Can We Meet the Challenge?"*
 - Participated in a roundtable discussion hosted by the BC Co-Chair and attended by 35 key identity management, privacy and security experts from the province of BC.
- March 2007: Third meeting of the IATF Working Group was held in Montreal, in conjunction with a workshop on identity management principles and frameworks with key stakeholders.
- May 2007: Fourth meeting of the IATF Working Group was held in Niagara-on-the-Lake, in conjunction with Lac Carling Conference and the meetings of the PSSDC and PSCIOC. The Task Force also hosted a Governance Workshop to explore governance models and develop recommendations for the future.

Teleconference Meetings:

In addition to the aforementioned in-person meetings, weekly teleconferences for the Task Force Working Group and bi-weekly teleconferences for the Steering Committee were scheduled to assess progress, discuss outstanding issues and maintain momentum.

Briefings and Other Key Dates:

- February 2007: Update to the Joint Councils (PSSDC and PSCIOC)
- March 2007: Deputy Ministers' briefing
- April 2007: Interim Report Released
- May 2007: Steering Committee Co-Chairs present at Lac Carling Conference
- May 2007: Update to the Joint Councils (PSSDC and PSCIOC)
- July 2007: Final Report Released

Appendix B

Task Force Financial Report

Financial Contributions

Budget	\$ 200,000
---------------	-------------------

Revenue	\$ 199,484
----------------	-------------------

Expenditures	\$ 186,037
<i>Research</i>	\$ 46,037
<i>Reports (Writing - Editing)</i>	\$ 32,946
<i>Translation</i>	\$ 33,708
<i>Meetings/Workshops (incl. facilitation)</i>	\$ 23,346
<i>Secretariat</i>	\$ 35,000
<i>MISA (municipal rep on working group)</i>	\$ 15,000

In Kind Contributions

Budget	\$ 800,000
---------------	-------------------

Actual	\$ 386,850
<i>Salary</i>	\$ 323,625
<i>Travel</i>	\$ 57,725
<i>International Scan (QC)</i>	\$ 5,500

Notes:

1-Salary includes 15K matching funds from MISA for municipal rep

2-Does not include TWIKI provided by QC

Appendix C

Environmental Scan

The Task Force undertook an environmental scan to better understand the current IdM&A situation in Canada and other jurisdictions. It was aimed at existing interdepartmental IdM&A initiatives, frameworks and policies. The scan identified several important elements, which will be critical to the effectiveness of the Task Force's work:

- **Obstacles** that jurisdictions face in identifying citizens and businesses for service delivery.
- **Insights** around the capacity of each jurisdiction to deploy complex IdM&A services to a multitude of clientele.
- **Stakeholders** -- the major stakeholders in IdM&A.
- **Challenges** that all jurisdictions face *as a whole* in achieving a pan-Canadian IdM&A framework that will facilitate seamless, cross-jurisdictional, multi-channel service delivery.

A. Canadian Environmental Scan.

The Task Force developed a questionnaire that was sent to the federal government and to all provincial and territorial jurisdictions in February 2007 through the NCIMA, as well as to the joint councils of the PSSDC and PSCIOC. The Task Force also surveyed municipalities in May 2007 through the Municipal Information Systems Association (MISA).

The survey included general questions on IdM&A initiatives that have been implemented or are in development. It was directed only at inter-departmental IdM&A initiatives that cover more than one service program (or have the potential to). From the answers received, the Task Force developed a general (albeit incomplete) picture of the current Canadian situation. Table 6 provides an overview of the IdM&A initiatives currently underway in Canada.

Table 6. Existing Canadian Inter-departmental IdM&A Initiatives

Jurisdictions	Number of initiatives	IdM&A Initiative Name
Gov of Canada	4	<ul style="list-style-type: none"> • Secure Channel - ePass • Portageur (Business and citizens) • Multi-channel Authentication Initiative (Service Canada) • Record of Employment (business and employer) •
British-Columbia	5	<ul style="list-style-type: none"> • BCeID • IDIR – BC (employee ID) • One-Stop Business Registry • Identity Management Forum

		<ul style="list-style-type: none"> ID Management and authentication for citizens and health care service providers
Alberta	5	<ul style="list-style-type: none"> Employee Identification Card Netcare Identification Card ID Alberta Secure Access service Registry Agent User Authentication Token
Saskatchewan	None	
Manitoba	1	<ul style="list-style-type: none"> Internal Shared Authentication Directory Domain
Ontario	9	<ul style="list-style-type: none"> Collaborative Senior portal cross jurisdictional client case management Internet-based "My account" for EHT and RST tax clients (MOST) Integrated Birth Registration Field inspector real time check of credentials of heavy equipment operators Strengthening electronic health services authentication Transport of hazardous material; on-line real time route changes Change of Business Information (COBI); allow authorized transactions to program areas to change program legacy info Integrated Internet Address Change; change personal information with MOHLTC ASA (Apprenticeship Support Application)
Québec	3	<ul style="list-style-type: none"> ClicSÉCUR (for citizen and then business) Health ID (for health care service providers) ICPG (public servants, gov suppliers, etc)
New-Brunswick	1	<ul style="list-style-type: none"> AAA application secure access
PEI	None	n/a
Nova Scotia	2	<ul style="list-style-type: none"> Security Identity Management Initiative (SIM) Nova Scotia Business Registry (NSBR) CRA My Business Account
Newfoundland and Labrador	n/a	n/a
Nunavut	None	n/a
Yukon	None	n/a
Northwest Territories	None	n/a

As well, the municipal scan revealed the following information:

1. The Region of Peel is interested in IdM&A-related services as they support electronic service delivery initiatives on a municipality-to-municipality basis. In the short-term, the Region of Peel is interested in horizontal collaboration that cross *municipal* boundaries in support of aggregated services to identifiable target groups that include, but are not limited to, senior citizens.
2. Municipalities are interested in building their IdM&A-related capabilities such that they take advantage of, and leverage, pan-Canadian inter-jurisdictional service delivery in the future; however, the present reality is that they are reluctantly forced to implement multiple vendor-supplied identity management application solutions.
3. Most municipalities procure the vast majority of their applications from vendors. The establishment of a pan-Canadian IdM&A framework will act as a powerful inducement for vendors to deliver IdM&A-compliant applications. Over time, and as a result of the establishment of this framework, government-grade software will share the same, common security infrastructure.
4. There are limited examples of inter-jurisdictional IdM&A-related initiatives that reflect municipal-provincial collaboration:

Comparing these results with the last environmental scan conducted by the IAAWG in February 2004, several trends are apparent:

- **Consolidation of isolated IdM&A initiatives.** Provincial jurisdictions have largely consolidated isolated department or agency IdM&A initiatives into larger ones.
- **More inter-departmental and multi-service systems.** There is a clear trend away from single service program IdM&A systems to inter-departmental and multi-service systems.
- **Growth of the number of initiatives.** The number of IdM&A initiatives has grown.
- **Different approaches.** Jurisdictions are taking different approaches to IdM&A and these have a crucial impact on their outcomes. For example, in BC, BCeID was introduced first to businesses. In Québec, on the other hand, citizens were the first to use the ClicSÉCUR service.
- **Different perspectives.** Each jurisdiction has differing perspectives on IdM&A,. There is little common ground on definitions, policies or understanding of the subject.
- **Different IdM&A management models.** Current initiatives use a variety of management models (see Section 5 for a discussion of these).
- **IdM&A assurance processes.** Some jurisdictions have clear documentation defining levels of assurance, while others do not. (See section 4 for a discussion of this concept.)
- **Diverse technologies.** There are a wide variety of technologies used for identity registration and authentication.
- **Progress is being made.** Three jurisdictions have done substantial work developing inter-department authentication services for multi-service delivery: the Government of Canada with ePass-Portageur; Québec with ClicSÉCUR; and BC with BCeID. These could each be candidates for potential pilots that would leverage existing initiatives.

B. International Environmental Scan.

A limited international environmental scan was also conducted. It looked at countries that have institutional similarities with Canada, including: New Zealand; Australia; USA; and most European Union countries. The international scan is being conducted as a review of the available literature and government publications. Some countries have been directly contacted for further details on their inter-departmental and multi-service IdM&A initiatives. Table 7 provides a brief overview of the initiatives that have been studied.

Table 7. Preliminary Results of an International Environmental Scan

Country	IdM&A Initiative Name
Australia (Federal)	<ul style="list-style-type: none">▪ Australian Government e-Authentication Framework for business▪ Australian Government e-Authentication Framework for individuals▪ Smartcard Health and social services access▪ The Identity Management for Australian Government Employees Framework
New Zealand (Federal)	<ul style="list-style-type: none">▪ Government Logon
USA (Federal)	<ul style="list-style-type: none">▪ E-Authentication Federation (also known as the E-Authentication Service component)
UK	<ul style="list-style-type: none">▪ Government Gateway▪ Government Connect▪ National Identity Cards
Slovenia	<ul style="list-style-type: none">▪ Personal Registration Number▪ e-ID Card Project
Ireland	<ul style="list-style-type: none">▪ Personal Public Service Number▪ Public Services Broker▪ Public Services Cards
Germany	<ul style="list-style-type: none">▪ German Office Identity Card▪ German Health Card Project▪ e-Card Strategy

The international scan has uncovered some interesting findings:

- **Countries are at different stages in their implementation of IdM&A infrastructure.** For instance Australia is in the Design Phase; New Zealand and Belgium are in the Pilot Phase; and UK is in the Implementation Phase. Many projects are suffering from delays that are having serious impacts on implementation.
- **Assurance levels used are similar among countries.** Most use four assurance levels. Risk assessments and information sensitivity are directly linked to these levels of assurance. (See Section 4 for a discussion of assurance levels.)
- **Legal frameworks are not modified to better align IdM&A systems with security and privacy requirements.** New Zealand is the only country that intends to develop a legal framework for its Government Logon Service (GLS).
- **There is a clear trend towards smart card technologies.** In Europe smart cards are a way of life, unlike in North America. However, different approaches for presenting and storing information on the card are used.
- **Most countries opt for a centralized IdM&A management model.** This model uses a unique identifier and a central identifier databank for “citizen” and “business” clients. Exceptions are the United States and France, which favour decentralized and federated identity management with multiple identifiers; as well as decentralized databanks with citizen and business identifiers. They do however make allowances for sharing certain centralized authentication technical services. (See Section 5 for a discussion of IdM&A management models.)
- **Solution initiatives such as biometrics, tokens and multimode access remain limited** as this a sensitive issue for clients and governments. For instance in Finland, despite the existence of a national e-identification card, the government implemented a second means of authentication as its departments and agencies found the e-identification card too complex to use. In the United Kingdom, the e-identity card has not gained widespread public support and implementation has met with significant cost overruns.

Appendix D

Identity Fraud: Causes and Factors

This analysis is primarily concerned with the following causes and factors that increase or make possible identity fraud:

1. Threats such as social engineering, “phishing”, “pharming”, and “vishing”;
2. Lack of awareness about security;
3. Lack of secure technologies (e.g., web browser) and processes;
4. Unreliable identification documents or identifiers; and,
5. Lack of affordable strong authentication solutions for services that require it.

1. Threats: social engineering, “phishing”, “pharming” and “vishing”.

The following list of threats is not an exhaustive list but rather, represents the common processes or tools used by criminals for identity fraud:

a. Social Engineering

Social engineering is the art or practice of manipulating people in order to obtain confidential or sensitive data. The basic goals of social engineering are the same as those of malicious hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network

Social engineers use influence and persuasion to intimidate, deceive and manipulate people into divulging information. Social engineering works because, for the most part, people want to be helpful and trust the person requesting the information. People are also intimidated by those who purport to have some form of authority or expertise (e.g., a CEO or security expert) or they may provide information in the hopes of getting some financial reward or prize. Social engineers are experts at exploiting these basic human tendencies.

b. “Phishing”

In addition to more traditional schemes, today’s social engineer also uses technology to take advantage of people. “Phishing” is a form of social engineering that uses email to ‘fish’ the Internet in the hopes of ‘hooking’ a person into giving up their logins, passwords, credit card information or identity information. Typically, the “phisher” will use a ‘spoofed’ email address that looks like it comes from a legitimate organization. The email will direct the individual to a fraudulent website where the individual will then

be asked to provide some personal information, enter their password or update their account information, etc.

Government agencies and departments have been targeted by phishing. In February of 2005, the Ontario Ministry of Transportation warned that an e-mail impersonating the ministry was circulating with a request for recipients to confirm their driver license information by clicking on an embedded link. And recently, in May of this year, Service Canada warned its clients about emails purporting to be from Service Canada. The emails asked clients to visit a Web site fraudulently posing as the Service Canada Web site and to provide personal information, such as Social Insurance Number, date of birth and banking information.

c. “Pharming”

While alerts and education have increased the public’s awareness of “phishing” schemes, a successor threat has emerged. “Pharming” involves redirecting Internet traffic from one Web site to a different, identical-looking site in order to trick a person into entering information into the database on the fraudulent site.

“Pharming” might seem similar to e-mail “phishing” scams but “pharming” is much more insidious, because a person can be redirected to a false site without any participation or knowledge on his part (i.e., the individual doesn’t have to click on a link in an email). “Pharming” involves changing a user’s Hosts file or directly manipulating the Domain Name Server by changing the IP address of the target web site from its real IP address to the IP address of the fake website. In this way, a person can type in a perfectly valid website address but still be directed to the fake web site, that is set up to look just like that of the intended web site.

d. “Vishing”

Another relatively new threat is “voice phishing” or “vishing” which uses Voice over Internet Protocol (VoIP) to recognize and record telephone keystrokes. As knowledge about internet scams grows and the public becomes more and more cautious about clicking on links from unknown sources, “vishers” have responded by asking people to call a specified telephone number rather than click on a link. People then call the number in the mistaken belief that it belongs to their bank or trusted service provider, where VoIP is set up to record the keystrokes the unsuspecting victim uses while entering their account number or other information.

2. Lack of awareness about security

Generally speaking, citizens and government employees are either under-informed or misinformed about the security threats to their identity and personal information. As an example, employees and citizens may be repeatedly reminded that they need to protect their information by using strong passwords, by using different passwords for different transactions, and by keeping their passwords private, but without a strong understanding of why these measures are important (i.e., what is the real threat, if I don’t do this), citizens and employees may not follow this advice.

For this reason, efforts aimed at improving information technology security such as requiring longer and complex passwords (with upper and lower-case letters and special characters), sometime backfire. Because citizens and employees can't remember their complex passwords, they might write them down or adopt other insecure practices such as reusing the same password. Stronger security practices are great but when they become too onerous (i.e., having to manage multiple complex passwords for multiple programs), employees and citizens will rebel.

There is also a lot of misinformation about security, particularly internet security, that has been exacerbated to some extent by the media (news, movies and television). The media, due to time constraints or for effect, tend to either simplify or amplify beyond recognition security incidents and situations (i.e., a hacker breaks into a secure government site in 60 seconds; or the hero thwarts a hacker attack by typing a simple sentence into a computer). Information systems and technology are portrayed as either "iron-clad", or completely breakable, with no in between and no recognition of the complexity involved in both maintaining or overriding security. What we hear and see in the media is usually lacking in detail and context, with the facts either not included or not validated. In addition, the solutions suggested are always vague or over simplified. As a result citizens are ill-informed about the real threats of conducting transactions online, what security measures they should employ to protect themselves, and what they should look for in deciding whether to trust a website.

3. Lack of secure technologies (e.g., web browsers and processes)

Commonly available technologies such as web browsers that are used for accessing online government services contain vulnerabilities that may be exploited by hackers. Despite considerable efforts from the industry to overcome these vulnerabilities, software and other technologies are still the target of a considerable number of attacks, which increases the risk of identity fraud.

According to Symantec, "attackers now consider client-side vulnerabilities to be a more fruitful area of research and attacks. As part of this shift toward client-side issues, vulnerabilities in Web browsers have become increasingly prominent, which in turn poses a threat to end-user desktop computers²¹.

In particular, Zero-Day attacks do not provide any protection for the citizen as the attack is conceived to reduce or eliminate the time a software vendor or community has to react by proposing a patch or update.

4. Unreliable "identity" documents or identifiers

One of the main reasons why many documents commonly used to prove identity are considered to be unreliable, in terms of providing a high level of assurance, is that they are too easy to forge. Despite all the resources that have gone into increasing the integrity and

²¹ Symantec Internet Security Threat Report - Trends for July–December 06, Volume XI, Published March 2007.

security features of these documents, there continues to be a growing and lucrative industry producing fraudulent driver's licences and other documents.

The production of fraudulent identification cards is becoming more and more sophisticated. Criminals have access to the same type of technology that the government producers of these cards do. Government must, therefore, remain ever vigilant in its efforts to identify more and more sophisticated fakes and to improving the integrity of ID documents and processes as criminals will exploit every weakness.

This problem is exacerbated by the fact that there is insufficient information sharing and training of government employees to deal effectively with fraudulent identification documents over the counter. Ongoing education and training is needed to help all employees that are responsible for the identification of clients to recognize fraudulent documents (particularly those from other jurisdictions and countries). This is fortunately not a problem when dealing with digital identifiers as the authentication process involves automated processes and, as such, is less prone to human error.

A second, and perhaps even more problematic, issue than the production of fraudulent documents is the instance where a criminal secures a perfectly valid document or identifier by fraudulent means (i.e., by successfully impersonating another person or through employee collusion). This type of fraud is much more difficult to catch because the documents will appear legitimate, having been issued by a trusted and authoritative source.

And thirdly, there is the issue of the verifying the authenticity of foreign documents. Because we are less familiar with these documents and the processes under which they are issued, it is difficult to rely on their integrity. In addition, many of these documents do not have pictures or any of the security features that we are used to seeing in Canadian documents.

However it is also the case, that some existing identification processes or identifiers can be said to contribute to the problem of identity fraud. Some identifiers that were created in the paper world and were widely used across programs may be problematic if applied or used in a network or digital environment. For example, it is noted by the LSE Identity Project Report that "in the USA, the Social Security Number has become an identity hub and a central reference point index and link. [...] There have been countless cases of identity thefts that were enabled by first obtaining the SSN. It is arguable that the existence and ease of obtaining the SSN and its importance across private and public database is the reason why the level of identity theft in the US is extremely high. This situation applies equally in Australia where the introduction of an extensive Task File Number has also increased the incidence of identity theft beyond the levels experienced in the UK."²²

Jim Harper in his book, "Identity Crisis: How Identification is Overused and Misunderstood" also notes that the use of a single document or Identification card (single identification system) is the "root of identity theft". Indeed, as roles of a given identification document or identifier increase (i.e., in terms of the number of departments or organizations relying on the document or identifier), the more valuable that identification document becomes from a

²² LSE, "LSE Identity Project Report: an assessment of the UK Identity Cards Bill and its implications", Version 1.09, June 27, 2005. P. 100.

criminal point of view, since that one document or identifier can be used to access an increasing number of services. In other words, the more reliance we place on any one document or identifier (i.e., adopting a particular document or identifier as a universal identifier), the more lucrative it becomes to falsify that document or to hack into databases containing those key identifiers. Criminals will focus their fraudulent activities where they see the most benefit, eventually exposing and exploiting weaknesses in processes and increasing the risks and costs to government.

Solution analysis:

1. Ongoing fraudulent document recognition training for all staff who are involved in the identification and authentication of clients. Consider leveraging existing fraudulent document recognition training (FDRT) materials and programs (for example those used by Canadian driver licensing agencies).
2. Wherever possible and justifiable, agreements should be struck between agencies that are authoritative parties (and/or credential issuers) and agencies that are relying parties to permit immediate (preferably online) verification of identification documents at source so that identity reliers do not need to rely solely on the face value of the document being presented to them.
3. In addition (as a way to deal with the issue of employee collusion), consideration should be given to certifying employees who are responsible for issuing identification documents or credentials or who have the authority to manipulate identification data of clients.
4. Government should avoid adopting one identifier or identification document as a universal identifier as this does little to combat identity fraud and may even exacerbate it. Instead government should consider a system that recognizes multiple identifiers and identification documents as either offering equivalent identity assurance or providing gradients of identity assurance for different types of services.
5. Establish a committee to look at “identity” documents commonly used across Canada with the goals of improving their integrity and acceptability across jurisdictions. This committee should also look at the integrity of foreign documents with a view to recommending what foreign documents meet Canadian standards.

5. Lack of affordable strong authentication solutions for services that require it

There is a lack of affordable strong authentication solutions (i.e., two-factor and multi-factor authentication tokens and cards) for those services that require it. In contrast to European countries where smart cards are widely used and accepted by the population, in North America, strong authentication technologies are not widely deployed nor used as they are considered expensive and perceived to be a burden for clients. This considerably limits the choice jurisdictions have in authentication solutions for the short term and may prevent access to certain services online that require stronger authentication. The reality is that governments in Canada depend on industry, in particular the banking sector, for authentication technology use and mass deployment.

Appendix E

Recommended Pilot Projects

This section outlines the approach used to identify potential pilot projects, the description of pilots that are being recommended, related actions and next steps.

1. Purpose, Strategy and Outcomes

Pilot projects will test the IdM&A Framework and its components as enablers to achieve the service delivery vision of seamless client identification and authentication across governments. By doing so, governments will commence the process of building trust, capacity and a foundation for future service delivery collaboration. An important outcome is that pilots demonstrate the value of the IdM&A Framework in real service situations.

Given that the IdM&A Framework is in its early stages of development, the Task Force took an incremental approach to identifying pilot initiatives, with all pilots pushing towards the goal of a common IdM&A vision. Early pilots will provide practical short-term results that validate IdM&A principles, use and test components of the IdM&A Framework, build understanding, inform governance, and identify gaps in the IdM&A Framework. As the IdM&A Framework becomes robust and continuously improves, the pilots will test the more refined and detailed guidelines and the feasibility of draft standards. Ultimately, one broad pilot project may be proposed to test the whole IdM&A Framework across all jurisdictions.

To get the ball rolling for early results, the Task Force looked for pilots that were already funded and/or were in an early enough stage to apply the IdM&A Framework in a meaningful way. The “pilot” aspect is the inclusion of the new context within which the service will be developed, and eliminates at least the short-term need to provide seed funding until the broader inter-jurisdictional funding mechanisms are designed and implemented.

Other critical success factors for pilots included: being easy to explain and recognize; having broad potential use; being multi-jurisdictional in nature; holding value for citizens; having an on-line aspect; and complying with current legislation and policy.

2. Background

Initial Pilot Identification and Assessment Approach

When the Task Force was initiated, it was expected that pilots would be identified using an analytical approach. That included taking the results of the environmental scans and running them through the set of critical success factors as the basis for selecting a good range of services that would test all aspects of the IdM&A Framework. Discussions with program areas would follow, to help shape well defined and fully costed initiatives with clear timelines and monitoring and reporting schedules.

As the Task Force work progressed, it became clear that a problem and solution analysis was needed, on which the scope of the pilots was dependant, therefore concrete discussions with programs could only begin in earnest in the last few weeks of the Task Force's schedule. The original pilot selection approach was adjusted, where the Task Force reviewed the potential list of pilots from the environmental scans, and approached their jurisdictions directly to identify:

- Programs that were interested and willing to include the incorporation of some or all of the IdM&A Framework components into work that was approved and funded (for short term practical results); and,
- Programs that wanted to champion a significant improvement in moving the IdM&A yardstick, but may be conditional on funding or other factors (such as needing more time to work out details with potential partners).

Pilot Evaluation Tool

Initially, consideration was given to requesting potential pilot leads to develop proposals and bring them forward for approval. At that time the following evaluation tool was developed as a guide and may be helpful in the future.

Exhibit 1. Pilot Evaluation Tool

Pilot Definition	Pilot Name
	Partners
Proposed scope, deliverables	Highlight main scope and deliverables and reference to Business problems/Framework being addressed
Pilot Assessment	<input type="checkbox"/> Willingness/ability of jurisdiction to participate (direct funding, in-kind, advisory) <input type="checkbox"/> Ability to reflect Idm/a outcomes into pilot evaluation criteria <input type="checkbox"/> Business Priority <input type="checkbox"/> Readiness (conceptual stage, in development or existing service) <input type="checkbox"/> Strength of trust/history between partners (strong, new, unknown) <input type="checkbox"/> Amount of effort required to implement (minimal, moderate, major) <input type="checkbox"/> Amount of funding required (low, medium or high) <input type="checkbox"/> Business Issues (None, some or many) <input type="checkbox"/> Known IT Issues (None, some or many) <input type="checkbox"/> Pilot Size (small, medium or large) <input type="checkbox"/> Level of Risk (low, medium, high) <input type="checkbox"/> Amount of Visibility (low, medium, high) <input type="checkbox"/> Portable (not, some what or very) <input type="checkbox"/> Cross-border interoperability (not, some)
Recommendation	Project plan, deliverables, resources, funding, critical success factors, governance.

3. Recommended Pilot Initiatives

The Task Force recommends that the following potential pilots be approved as recommended. Each pilot description includes who the client is, the pilot objectives and phases of work where appropriate, as well as the type of pilot it represents (B2G, C2G, G2G). A summary of recommendations and actions is provided at the end of this section.

Pilot 1: Integrated Birth Registration (IBR) implementation assessing new Authentication and Trust Models (G2G)

The Current Situation:

This initiative involves ServiceOntario, Service Canada, and hospital agents in the broader public sector. They have successfully launched an Integrated Birth Registration (IBR) service in three cities, where parents register their child's birth on line and simultaneously apply for both their birth certificate and SIN. This enables parents to provide information once when applying for two related services, as appropriate data passes through to the provincial and federal applications and the client quickly receives their credentials by mail. Other provincial implementations are planned across the country. Authentication of the nurses, clerks and midwives is done using the province's PKI. Inter-operability is not an issue, as data flows from the e-form to the authorized application, and issues are addressed at the business level.

The Pilot Opportunity and Expected Outcomes:

The partners now want to improve upon the Integrated Birth Registration service and business processes, and are defining a new implementation solution with the following objectives:

- 1) to leverage an existing Smart Systems for Health hospital employee authentication process, in place of PKI; and,
- 2) to implement an authentication model that relies on partner authentication and trust.

The service delivery model involves authenticating hospital registration agents responsible for reporting newborn births, using a Smart Systems for Health's risk-based approach that will be trusted by ServiceOntario and Service Canada. This initiative will be implemented in November 2007, and will form the building block for other potential services to be added in the future (such as the Child Tax Benefit).

The pilot objectives from an IdM&A perspective are generally, to get quick feedback regarding the usability of the first policy version of the IdM&A Framework by an inter-jurisdictional implementation team, as additional context for DMs as they consider the Task Force's recommendations in November 07.

Specifically the IdM&A objectives are:

- 1) to help three jurisdictions use a common language and framework, to support implementation discussions in a structured way.

- 2) to understand how the implementation team dealt with trust, governance, and authentication, to inform the evolving policy IdM&A Framework components.
- 3) to build the knowledge and capacity of current participants.
- 4) to document best practices for jurisdictions that are considering adding IBR in their province and/or expanding the service to other programs.

Action:

- As ServiceOntario and Service Canada leverage and adopt Smart Systems for Health's authentication process and develop new service, trust and governance arrangements, they will assess how they dealt with these situations in order to inform the IdM&A Framework and consider how the IdM&A Framework can inform future IBR business improvements (Nov 07).

Next Step:

- ServiceOntario, Service Canada and Smart Systems for Health will provide a status report on their initial assessment of the IdM&A Framework based on implementation of a new IBR authentication process, at the DM meeting in November 2007.

Pilot 2: On Line BCeID authentication using CRA's Portageur to test shared identity proofing processes for services to individuals (C2G)

The Current Situation:

Currently individuals must register and prove their identity in-person to obtain a BCeID. A BCeID is an electronic credential that can be used to access multiple on line B.C. government service offerings. In the federal government, CRA has an on-line authentication process for their clients called Portageur.

The Pilot Opportunity and Expected Outcomes:

This pilot will test the concept of one jurisdiction (B.C.) leveraging the identity-proofing process of another jurisdiction (CRA); verifying the identity claims of B.C. residents once and providing immediate access to on-line services. In the near-term, potential BCeID clients (300,000 - 400,000) that have previously registered with CRA for a "My Account" would have the option of transferring data from CRA to BCeID for the purpose of on line registration and identity-proofing. This would offer clients a real-time fulfillment experience that facilitates access to on-line service offerings. Instead of attending a government agent's office to prove identity, the client can consent to the secure transfer of a Personal Statement of Identity from CRA that would be used to verify the identity claim of the client wishing to obtain a BCeID. The Personal Statement of Identity would be compared with identity attributes collected and verified by the BCeID service to ensure that the client is, indeed, who they claim to be.

The pilot objectives from an IDM&A perspective are:

- to test the Assurance Framework and the Assurance Model (i.e., does CRA's online registration process provide equivalent assurance to BCeID's in-person registration process);
- to test the Identity Framework with respect to whether the identity attributes provided by CRA will meet BCeID's identification requirements;
- to test the Privacy Framework (e.g., obtaining client consent to transfer the "Personal Statement of Identity" across jurisdictions, providing adequate notice of the purpose for transferring the information and how it will be used, conducting a Privacy Impact Assessment, etc.)
- to test the Security Framework in terms of ensuring a secure environment for the transfer of personal information, conducting a Security Threat and Risk Assessment, etc.;
- to establish a level of trust amongst two jurisdictions and test the Trust Framework (i.e., establishment and monitoring of bilateral agreement, requirement to comply with certain standards);
- to test the interest and willingness of clients to permit the transfer of their personal information across jurisdictions for the purpose of facilitating easier access to services; and,
- to document lessons learned and possibly expand the service.

Action:

That the Province of British Columbia and the Canada Revenue Agency immediately start discussions on how B.C. can leverage CRA's Portageur to provide a on-line registration process for potential BceID clients that provides immediate access to B.C. e-services. Details concerning business requirements, interoperability and near term opportunities have to be discussed before an agreement to proceed can be reached.

Next Step:

The Province of British Columbia and CRA will provide a status update on discussions regarding a shared identity-proofing process at the DM November 2007 meeting.

Pilot 3: Reciprocal trust agreement for authentication between Quebec (ClicSÉCUR) and CRA (Portageur) (C2G)

Current Situation:

Currently individuals residing in the Province of Quebec must authenticate separately at the provincial level as well as at CRA to gain on line access to their tax information.

The Pilot Opportunity and Expected Outcomes:

This pilot will test the concept of two jurisdictions trusting each other's authentication processes and sharing data (with consent) so clients authenticate once for on-line access to Quebec and CRA services. In the near-term, Quebec residents would be able to

authenticate using either ClicSÉCUR or CRA's process to access My Account. Then using a consent-based process (i.e., Portageur) certain identity attributes would be transferred between the two organizations to formalize the transaction. Clients would then be considered authenticated (or at least partially) and could be well on their way to enjoying immediate access to on line services. This would reduce the burden to clients of authenticating with each organization and it would offer clients a real-time fulfillment experience that facilitates on-line authentication and provides immediate access to on line service offerings.

The pilot objectives from an IdM&A perspective are:

- To test the concept of one jurisdiction trusting the authentication process of another jurisdiction.
- To test components of the IdM&A Framework Reference Model (Legal, Trust, Security, Assurance Levels, Privacy)
- To provide valuable lessons learned for the longer-term future state.

Action:

- That the Province of Quebec and the Canada Revenue Agency start discussions immediately on a reciprocal trust agreement to use each other's authentication processes and share data (with consent). Details concerning business requirements, interoperability and near term opportunities have to be discussed before an agreement to proceed can be reached.

Next Step:

- The Province of Quebec and CRA will provide a status update on discussions related to a reciprocal trust agreement for authentication at the DM November 2007 meeting.

Pilot 4: Direct validation of the Social Insurance Number (SIN) by a provincial partner(s) (G2G)

Current Situation:

In response to provincial requests and to further policy objectives, Service Canada is looking to develop a mutually beneficial pilot, which would validate the Social Insurance Numbers of provincial clients against the Social Insurance Register (SIR). The SIN is used in varying degrees by provinces as an individual client and/or file identifier; the accuracy of client authentication is, however, constrained in part by the limitations of SIN data held by the province.

Pilot Opportunity and Description:

The aim of this pilot is to develop a more in-depth understanding of the business needs of potential SIR partners, examine the range for capacity and scope growth for the SIR, explore the feasibility of an inter-jurisdictional approach to identity validation with the aim of

future integration of identity management and service delivery, and to determine which enablers would be required for pan-Canadian implementation.

Direct provincial validation of the SIN would permit provinces to address a potential identity assurance gap. Numerous provincial programs use the SIN as a client identifier, often for services that have a federal connection. However, provinces are not able to access the most up-to-date SIN information available, that is in the SIR, to ensure that the SIN does in fact belong to the identity presented.

Via this pilot, potential partners would gain access to the SIR for identity validation purposes; in this way they would be able to reduce the risk of improper access to provincial programs and reduce program inefficiencies associated with identity-related errors. In addition, through this shared identity validation tool the initial groundwork could be laid for a broader discussion of identity validation and associated risks.

Action:

- A pilot will be implemented by late 2007 to permit a province to validate the SINs of certain individual clients directly against the SIR, to increase identity authentication assurance for the province and improved integrity for the SIR.

Next Step:

- Potential pilot parameters for direct validation of the SIN by provincial partner(s) will be developed and validated within Service Canada; concurrently, initial discussions will take place with those parties who have in the past indicated an interest in direct SIR access, for implementation late 2007

Pilot 5: Integrated Multi-Jurisdictional Death Notification Service (C2G, G2G)

Current Situation:

Currently, when someone dies, a wide array of different organizations must to be contacted individually and informed of a death. Following the registration of a death with the provincial vital statistics registrar, the family of the deceased or a delegate is required to undertake numerous separate steps to:

- Cancel benefits (e.g. Canada Pension Plan, Old Age Security, Veterans' Affairs, Provincial Social Benefits, Tax Benefits, etc.);
- Deactivate Social Insurance Number;
- Cancel Passport, Driver's License, Health Card, etc.; and
- Initiate Death and Survivor's Benefits (e.g. Canada Pension Plan).

These separate steps cause significant delays for programs to be informed of deaths, which result in overpayments, recovery requirements, and delayed access to services and benefits by surviving family members or others.

Pilot Opportunity and Description:

An Integrated Multi-Jurisdictional Death Notification Service would ease the burden faced by Canadians when confronted with the death of a loved one. Through this integrated service, Canadians would only need to notify government (the provincial vital statistics registrar) once of a death and then this information would be proactively shared electronically with appropriate provincial, federal and other stakeholders to cease, and/or initiate, services and benefits as appropriate. Not only would this service respond to Canadians' needs at a difficult time by reducing the administrative burden that currently exists, it would greatly increase the timeliness, accuracy, and overall integrity of many government services and benefits and other related services.

This pilot, through the secure, electronic sharing of information between provincial vital statistics registrars, Service Canada (using the Social Insurance Register as appropriate) and other agencies, could test:

- The automatic cessation of certain benefits and access to programs and services;
- The deactivation of licenses, health cards, Social Insurance Numbers, passports and other identity documents;
- The initiation of survivor services and benefits;
- The effectiveness in reducing overpayments and recovery requirements and its impact on Canadians and programs; and,
- Potentially positive linkages for the private sector (i.e., insurance companies).

This pilot, while touching on all of the components of the Identity Management and Authentication IdM&A Framework, will primarily test the legal, assurance, and service aspects.

This pilot would build upon the existing Vital Events Linkages agreements between Service Canada and the Vital Statistics Registrars of British Columbia, Alberta, and Ontario. Preliminary discussions have occurred on this potential partnership and interest has been expressed in further pursuing this opportunity. The pilot, which would feature phased implementation, could be designed beginning in the Fall/Winter 2007-2008, for implementation beginning early in FY 2008-2009.

Action:

- Service Canada will pursue further discussions with interested provincial partners to build upon the existing vital events linkages agreements to initiate the preliminary scoping and design of an Integrated Multi-jurisdictional Death Notification pilot.

Next Step:

- Service Canada and one of its existing Vital Statistics Registrar partners (i.e., BC, Alberta, Ontario) will begin scoping and design of the pilot for an Integrated Multi-Jurisdictional Death Notification Service in Fall/Winter 2007-2008. This will allow for a phased pilot implementation: FY 2008-2009

Pilot 6: Service Canada's participation in any online identity authentication pilot and related reciprocity accords to minimize client authentication duplication (C2G, G2G)

Current Situation:

Service Canada has a mature and robust online authentication service, leveraging the Social Insurance Register (SIR). A risk-based approach to authentication of client identity is being implemented. Over 20 million transactions have been authenticated by this service in the online channel since May 2005. (*Of note, CRA, ClicSÉCUR and Service Canada are also using the SIN as one of their authentication data elements.) Service Canada also benefits from ongoing partnerships with provinces for the transmission of vital events information, enhancing the integrity of the SIR and thus the integrity of the authenticated transaction. SC has over 300 points of in-person service across Canada with Citizen Service Agents (CSAs) that are trained to perform identity document validation.

Pilot Opportunity and Description:

An opportunity exists to partner with other jurisdictions to leverage the data and integrity of Service Canada's client authentication process with that of a partner's own client authentication data source and processes. As such, each jurisdiction would rely upon each other's authentication process to grant "common" clients access to their respective programs and services. This would eliminate a client duplicating the identity and authentication process(es) when interacting with each jurisdiction. It will be critical to define trusted partners and trusted sources of data in these pilots. An understanding of a common approach to leveraging an assurance model would be key.

Action:

- Service Canada will pursue further discussions with interested partners to use each others trusted client authentication when a common client requests access to a program and/or service by August 2007 (based on an accepted trust model and testing legislation, assurance, accountabilities and consent).

Next Step:

- Partners will be confirmed by Service Canada for participation in any online identity authentication pilot and related reciprocity accords to minimize client authentication duplication, by August 2007, for discussion with DMs at their September meeting.

Conceptual Pilot to test new ideas

Pilot 7: Single identity proofing and notarization body to support extended BizPal functionality for a range of cross-jurisdictional, on-line services. (B2G, G2G)

Current Situation:

BizPal currently provides clients with an inquiry-only on-line experience. All applicable licenses and permits required for establishing a business are aggregated for clients based on the detail they provide on the BizPal website and the nature of the business to be established. Verification of identity is not required. Presently, BC has a Business Number Hub that provides verification of a business's identity by sending messages to CRA and back, but it is unknown how extensible this may be to other provinces and jurisdictions.

Pilot Opportunity and Expected Outcomes:

An authentication process could be designed to authenticate the client once. This process would be trusted by a wide range of business programs and therefore eliminate the need to re-authenticate the client. It would improve government response time, avoid development costs that would otherwise be approved for stovepipe solutions, and provide a wider choice of channels when requesting license and permit approval and fee remittances.

The authentication engine could reside in an arm's-length/independent proofing body that would vouchsafe the veracity of client credentials on behalf of all jurisdictions. This notarizing body would be the agent that brokers trust relationships between the client and governments for the license and permit transaction and, in the case of fee remittances, broker the trust relationships among clients, governments and financial institutions.

The proofing body could be a government organization like CRA and Industry Canada, or an independent body which would allow government to focus on its core businesses and the channelling of funds to service delivery initiatives that would otherwise be spent on notarization. It is acknowledged that government today, under the ægis of CRA, offers proofing services and that this service may migrate to Industry Canada. In the short term, CRA/Industry Canada could test to see if identity proofing and notarization functionality works with existing systems. In the longer-term future state, that experience could be leveraged by an independent body that could provide identity proofing and notarization services to all levels of government. It is worth noting that a centralized model for IdM&A-related services is currently operating in New Zealand (called the All-of-Government Authentication Program).

The client would access BizPal through a single-window portal experience through which government services are aggregated and individuated based on the client's authorization rights. In the single-window portal experience, BizPal is one authorized service among a set of authorized services pushed to the client at the time of authentication. All aspects of the

IdM&A Framework Reference Model would be tested. Municipal interest in this pilot opportunity would be determined through the Federation of Canadian Municipalities.

As a pre-requisite for a pilot of this nature, Industry Canada, Canada Revenue Agency and the Provincial Business Number partners (Nova Scotia, New Brunswick, Ontario, Manitoba and British Columbia) have indicated that a common business identifier should be used across jurisdictions. Several cities (Toronto and Winnipeg) are working with respective provincial partners to work around current legislative barriers. The federal government is considering the possibility of removing the existing BN legislation from the Income Tax Act and establishing new, stand-alone BN legislation. The first step toward establishing this common identifier at the federal level is the development of a Federal Business Number hub. Once the hub is established, the next step would be to encourage wide-spread use of the BN as a common identifier across all jurisdictions and programs. Along with this widespread use of the BN, a small Common Business Authentication module pilot could commence with the current jurisdictions that have already adopted the BN.

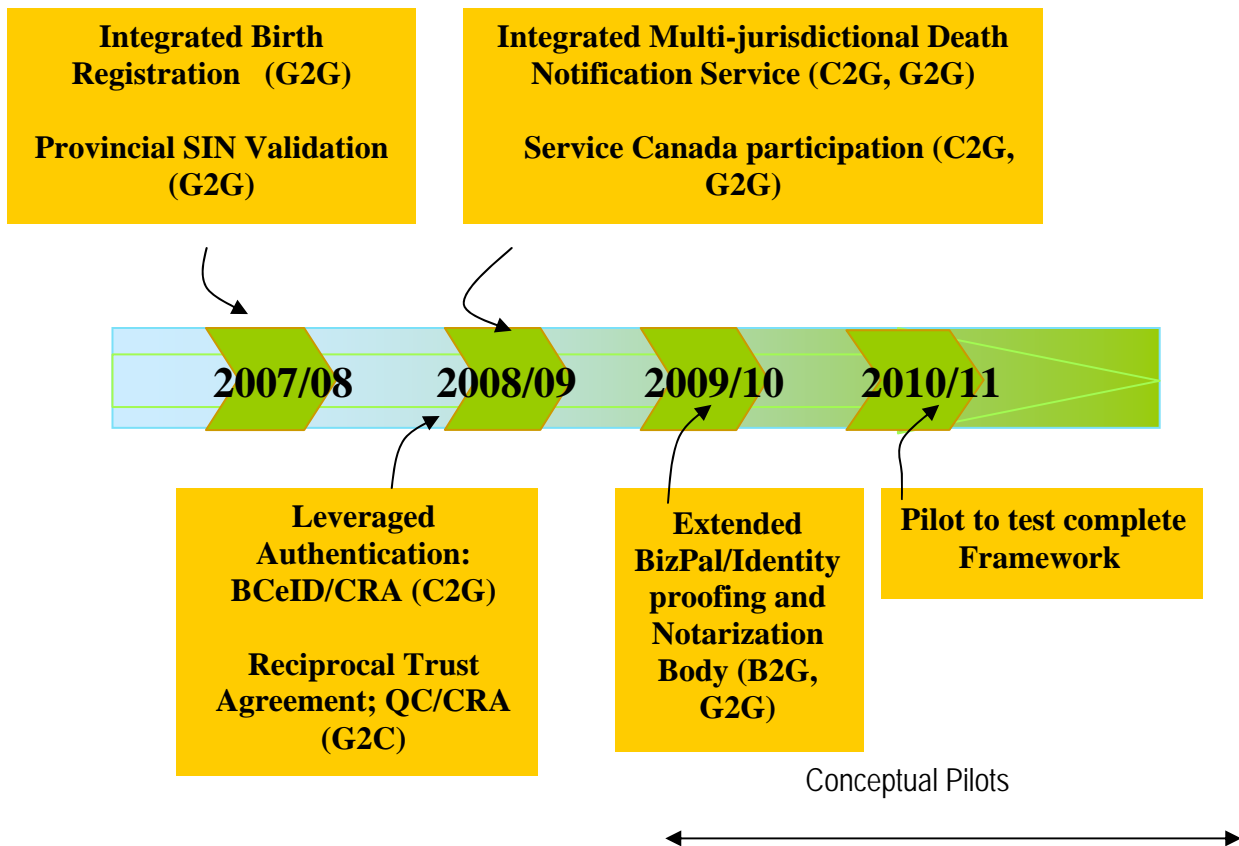
Action:

- Joint Council members will be consulted on their interest in the concept of having an independent identity proofing and notarization body to support expanded on-line business services.

Next Steps:

- In the presentation of the Final Report to the Joint Councils at their meeting in September 2007, the Steering Committee will request an expression of interest by jurisdictions in further developing the concept of having an independent identity proofing and notarization body to support business services.
- DMs will be provided with an update on jurisdictional interest in an independent identity proofing and notarization body for expanded services to business as context for their decision.
- Assuming jurisdictional interest, Industry Canada will report on its progress in determining the requirements to establish the common BN identifier, to help the Inter-Jurisdictional IdM&A Action Committee begin to understand the potential implications and timelines for the longer-term pilot to expand BizPal functionality and consider an independent identity proofing and notarization body for businesses (Mar 08).
- The Inter-Jurisdictional IdM&A Action Committee will start to identify potential partners and define the identity proofing and notarization pilot (spring 08).

4. Summary of Pilot Implementation Timelines



Summary of Action Items

- As ServiceOntario and Service Canada leverage and adopt Smart Systems for Health's authentication process and develop new service, trust and governance arrangements, they will assess how they dealt with these situations in order to inform the IdM&A Framework and consider how the IdM&A Framework can inform future IBR business improvements (Nov 07)
- The Province of British Columbia and the Canada Revenue Agency will immediately start discussions on how BC can leverage CRA's Portageur to authenticate clients on line once, and provide immediate access to e services. Details concerning business requirements, interoperability and near term opportunities have to be discussed before an agreement to proceed can be reached.
- That the Province of Quebec and the Canada Revenue Agency start discussions immediately on a reciprocal trust agreement to use each other's authentication processes and share data (with consent). Details concerning business requirements, interoperability and near term opportunities have to be discussed before an agreement

to proceed can be reached.

- Joint Council members will be consulted on their interest in the concept of having an independent identity proofing body to support expanded on-line business services
- A pilot will be implemented by late 2007 to permit a province to validate the SINS of certain individual clients directly against the SIR, to increase identity authentication assurance for the province and improved integrity for the SIR.
- Service Canada will pursue further discussions with interested provincial partners to build upon the existing vital events linkages agreements to initiate the preliminary scoping and design of an Integrated Multi-jurisdictional Death Notification pilot.
- Service Canada will pursue further discussions with interested partners to use each others trusted client authentication when a common client requests access to a program and/or service (by August 2007). This will be based on an accepted trust model and would test legislation, assurance and trust models, accountabilities and consent.

Summary of Next Steps Over Time

August –November 2007

- **Sept 07 Joint Council Meeting; Steering Committee** members will request an expression of interest by jurisdictions in further developing the concept of having an independent identity proofing body to support business services at their meeting in September 2007
- **Sept 07 Service Canada** will confirm partners for participation in any online identity authentication pilot and related reciprocity accords to minimize client authentication duplication, by August 2007, for discussion with DMs at their September meeting.
- **Nov 07 Selected pilot initiatives** will provide an update to DMs:
 - a. ServiceOntario, Service Canada and Smart Systems on their initial assessment of the IdM&A Framework based on implementation of a new IBR authentication process
 - b. The Province of British Columbia and CRA on discussions regarding a shared identity-proofing process
 - c. The Province of Quebec and CRA on discussions related to a reciprocal trust agreement for authentication
 - d. Jurisdictional interest in an independent identity proofing body for expanded services to business

December 2007 – Dec 2008

- **Service Canada and one of its existing Vital Statistics Registrar partners** (i.e., BC, Alberta, Ontario) will begin scoping and design of the pilot for an Integrated Multi-Jurisdictional Death Notification Service in Fall/Winter 2007-2008. This will allow for a phased pilot implementation: FY 2008-2009

- Potential **pilot parameters** for direct validation of the SIN by provincial partner(s) will be developed and validated within **Service Canada**; concurrently, initial discussions will take place with those parties who have in the past indicated an interest in direct SIR access, for implementation late 2007
- Mar 08: **Industry Canada** will be asked to provide a status report regarding the common identifier to the interim Action Committee, as the basis for defining the possibility of an independent identity proofing body for business
- Spring 08: **Inter-Jurisdictional IdM&A Action Committee** will start to identify potential partners and define the identity proofing pilot

Jan 2009+

- **Service Canada and one of its existing Vital Statistics Registrar partners** (i.e., BC, Alberta, Ontario) will start to implement a phased pilot for an Integrated Multi-Jurisdictional Death Notification Service (FY 2008-2009).
- **The Interim Action Committee** will determine the appropriate time to define and recommend a pilot to test all aspects of implementing the IdM&A Framework prior to a Pan-Canadian rollout.

Appendix F

Governance Workshop

On May 2, the Task Force held a one-day workshop in Niagara-on-the-Lake to explore possible governance models for a pan-Canadian IdM&A framework. In the morning, four speakers presented their thoughts and experiences about inter-jurisdictional/inter-organizational governance to the Task Force members. In the afternoon, Task Force members, members of the Steering Committee, the speakers and invited guests explored some of the challenges and critical success factors related to a governance model for IdM&A.

Three Inter-jurisdictional / Inter-organizational Governance Models

Prior to this workshop, representatives of three inter-jurisdictional /inter-organizational entities: Canada Health Infoway; Canadian Council of Motor Transport Administrators, and Interac Association, were invited to describe their governance structures. The following three caselets describe the following elements:

- The purpose of the organization
- Its membership
- Its governance structure
- Its funding
- Critical success factors and challenges
- How the organization has changed over time.

At this workshop, representatives from these organizations elaborated on these elements and answered Task Force members' questions about their governance issues.

A. Canada Health Infoway

Presented by: Stan Ratajczak, Canada Health Infoway

Canada Health Infoway (Infoway) is an independent not-for-profit corporation whose goal is to deliver electronic health record (EHR) solutions to Canadians. Its mission is:

- to foster and accelerate the development and adoption of electronic health information systems with compatible standards and communications technologies on a pan-Canadian basis.
- To build on existing initiatives and pursue collaborative relationships in pursuit of its mission.

Infoway is a *strategic investor* that works in partnership with health ministries, regional authorities, other healthcare organizations and vendors to align its investments with jurisdictional plans and to leverage existing solutions. Privacy and security are key aspects of all projects it funds. Other priorities are the potential for reuse in other jurisdictions and an interoperable approach.

The organization is “owned” by the 14 Deputy Ministers of Health of the federal, provincial and territorial governments who are its members. They meet once a year in an Annual General Meeting to review all business plans as well as the financial and compliance audits. Infoway is therefore equally accountable to all jurisdictions. The organization also has a 13 member board of directors, composed of: two members appointed by the federal Deputy Minister of Health; five members, each representing a region of the country (Atlantic provinces; Quebec, Ontario, Prairie provinces, BC), appointed by the provincial and territorial Deputy Ministers of Health; and six independent directors appointed by the Members of the Corporation. The Board meets four or five times a year and approves all projects over \$10 million. Three committees report to the Board: finance, investment and audit, which approves smaller projects; HR and compensation; and governance, which is responsible for memberships and mandates.

On a day-to-day basis, Infoway is run by a management team of eight, including a CEO, a CFO, a COO, a director of Human Resources, a Chief Technology Officer, an SVP of Investment Programs Management, an SVP of Investment Strategy and Alliances, and a VP of Innovation and Adoption. Mike Sheridan, Infoway’s Chief Operating Officer, identified seven factors responsible for the organization’s accomplishments to date.

Three factors are foundational elements on which Infoway’s programs are based:

1. **A Strategic Plan.** This outlines nine key priorities and strategies for achieving the organization’s mission, e.g., diagnostic imaging, laboratory information systems, EHR systems.
2. **A Blueprint Architecture.** This lays out how information will be accessed, as well as how the different EHR components will communicate with each other. It defines a set of common services and functional requirements for each. This architecture has also shaped a culture of what is acceptable amongst jurisdictions.
3. **Standards.** These establish ways to exchange components in a standardized fashion. They are based on 11 principles of operation, e.g., “We will commit to using international standards.” While part of the architecture, there are several standards in health care and so these are managed somewhat separately (see below). In the past, it has been challenging to establish standards in health care because there is no one coordinating body in Canada and often no dedicated staff or resources in the jurisdictions. Infoway has thus been able to add value to the provinces in this area. Standards are typically developed as part of an Infoway project, rather than in a vacuum.

Sheridan estimates that it took Infoway about 18 months to put these elements in place, but he noted that they have been critical to the organization’s ability to move forward with ever-increasing rapidity on various projects.

Two further success factors are related to collaboration:

4. **Flexibility and integration with jurisdictional plans.** Not all jurisdictions have the same priorities for EHR. Infoway’s approach to achieving collaboration and cooperation across jurisdictions is to enable each jurisdiction to set its own pace and priorities for achieving EHR. “This was a big ‘A-HA’ for us”, said Sheridan. “It means that each jurisdiction can be moving down different roads at a different pace but working towards the same goal.”

5. **Investment in EHR strategic projects.** Infoway will fund up to 75% of the costs of implementing (not operating) approved elements of its strategy. This gives all the jurisdictions a significant motivation to work with Infoway in this area.

Finally, two principles of operation have been established as guidelines:

6. **Replication.** Infoway wants to leverage its investments in more than one jurisdiction. Therefore, it tries to make strategic investments with one or more jurisdictions, which incorporate the needs of others. All software is open source but provinces can customize aspects of it as they wish.
7. **Staggered funding.** Infoway releases funding for its projects in two stages. Fifty percent is released when a project is ready for implementation; the other 50% is released when the project reaches certain adoption levels (e.g., utilization of the system, number of users). Adoption criteria are worked out with each jurisdiction and project.

Each Infoway program is headed by a Program Manager, who is responsible for establishing and managing a particular strategic area and who is accountable financially. Each Program Manager works with a set of project directors, drawn from the jurisdictions, who help set the goals and objectives in the area. "At this level, it's all about relationship management," said Sheridan. This group also works to identify and set standards for its area, which must then be approved by Infoway's Pan-Canadian Standards Committee, composed of clinicians, vendors and jurisdictional representatives. This Committee helps ensure that standards are coordinated between each strategic area and are also consistent with international standards. Once a program is ready for delivery, Executive Regional Managers work with the relevant jurisdictions on a day-to-day basis to ensure programs are implemented on time and on budget.

Sheridan noted that ideas for programs can come either from the Program group *or* from the individual jurisdictions. "We've learned there is no 'one size fits all' for EHR," he said. "Flexibility is key. As a result, we've had very positive reviews of our governance model." Ratajczek also stressed the importance of broad consultation in Infoway's work, including the participation of the Privacy Commissioners, multiple review cycles, and workshops.

B. Canadian Council of Motor Transport Administrators (CCMTA)

Presented by: *Michel Gravel, Executive Director*

CCMTA is a not-for-profit organization which acts as a neutral and independent coordination and support body for making decisions on administrative and operational matters dealing with the licensing, registration and control of motor vehicles and highway safety. As well, it manages a communications network, called the Interprovincial Record Exchange (IRE) system, which is used by governments to achieve business efficiencies in the areas of driver licensing and vehicle registration and by third parties who wish to access this type of data.

It works closely with the:

- **Transportation Association of Canada (TAC).** This is a larger, national association whose mission is to promote safe, secure, efficient, effective and environmentally and

financially sustainable transportation services in support of Canada's social and economic goals. Its 500 members include federal, provincial and territorial transportation departments, municipalities, and private-sector firms with an interest in transportation issues. Seniors and students may also join as individuals. TAC standing committees explore guidelines and best practices in various areas and make recommendations to the CCMTA.

CCMTA reports to two Councils:

- **Council of Ministers of Transport and Council of Deputy Ministers of Transport (COM-T).** These two councils set the policies and make the decisions in all matters concerning collaborative transport matters in Canada. Programs, policy matters and planning report through the DM Council, which in turn reports to the Ministers' Council. These are not a formal organizations so TAC provides all of the needed support for these Councils and also acts as the means whereby funding can be pooled for common projects.

Coordination between these three entities is maintained in several ways. First, CCMTA and TAC, share a common Executive Director, Michel Gravel, who is also Secretary to COM-T. Second, all three organizations are co-located in the same building in Montreal. Third, they share a common secretariat function and common services, such as IT, Finance, and Accounts Receivable. However, each also has its own dedicated staff, its own mandate and its own sources of funding.

The CCMTA is run by a 14 member board of directors representing each province and territory, as well as the federal government. Directors tend to be Assistant Deputy Ministers or their counterparts from vehicle registry agencies, e.g., government insurance companies. The board runs the organization and makes recommendations to COM-T, which has the final approval on all CCMTA issues. Committees of the board work on achieving consensus on various issues and then draft memoranda of understanding (MOUs) for COM-T's approval.

COM-T costs are paid for by assessments based on pre-established formulae – some equally and others by percentage of population. CCMTA has a number of sources of funding, the largest being the IRE, which charges both by utilization and assessments based on population. Some funding comes from government member assessments and other funds come from the sale of associate memberships (non-voting), its annual conference, and public sales of information. TAC's funding comes from the sale of memberships and the sale of a wide range of products and services, such as technical courses, a newsletter, and technical guides. Much of its work is also done by volunteer councils and committees.

This current structure works extremely well, according to Gravel, although this wasn't always the case. One key success factor has been the creation of "firewalls" between these three entities. "A number of years ago the organizations were always straying into each other's business," he said. "And this caused a great deal of frustration." Today, it is clear what each organization is and is not responsible for: COM-T – policy; CCMTA – vehicle, driver and regulatory matters; and TAC – technical standards and best practices. "This separation

works very well. Now everyone is satisfied with how things are working. We have the right people working on the right issues at the right level,” Gravel noted.

The success of COM-T is built on mutual respect and trust at the ministerial and deputy ministerial levels and support from good senior staff. A key factor is that this is *not* a forum for advocacy. Advocates and stakeholders are heard and consulted in the standing committees, not at the Councils. In addition, the Councils have begun to meet informally in meetings which are not recorded and these have proven to be “very productive”. Another success factor is a stable secretariat that can help orient new Council members, since turnover is fairly consistent.

Within CCMTA, Gravel identified consultation with stakeholders and open discussion as being critical to success. “Not only is it important for everyone to have a say, it is also fundamental to the credibility of the organization,” he said. Today, even board meetings are open. The same is true for TAC.

A significant challenge for the groups is getting the right people at the table. In some jurisdictions, for example, two Deputy Ministers have responsibility for transport matters or a Deputy and a provincial agency will share responsibilities. “When this happens, there is sometimes a disconnect between the two organizations involved and it can be difficult to get decisions made,” Gravel explained. Furthermore, none of these three organizations has any ability to motivate compliance on the part of their members. Sometimes, even with a signed MOU, members do not always implement what has been agreed. “There are almost always political or financial reasons for this,” said Gravel. “And there is only peer pressure between the jurisdictions to ensure that the work gets done.”

Gravel identified five key governance lessons learned:

1. Structure needs to be tailored to the organization’s mandate and strategic objectives.
2. The governing council/board needs to be designed for effectiveness, e.g., the number and type of members, committees, roles and responsibilities, the basis of representation and the role of stakeholders.
3. The organization needs to be properly supported.
4. The organization needs to be properly funded.
5. Membership needs to be determined and their roles and benefits defined.

Overall, it is extremely important for any inter-jurisdictional organization to understand what it is trying to achieve up front and to design its governance appropriately. “You must take the time to do it right,” he said. “Otherwise, it’s a recipe for disaster.”

C. Interac Association

Presented by: *Kirkland Morris, Interac Association*

Interac Association is the organization responsible for the development and operation of a national network of two shared electronic services: shared cash dispensing (ABMs) and direct payment (debit cards at the point of sale). Founded in 1984 as a cooperative venture by five of Canada’s financial institutions, today it has 85 members. Any company

incorporated in Canada can be a member of Interac Association, said Kirkland Morris, Assistant Vice President, Strategic Policy and Programs. “One of our strengths is our flexible structure that allows individual companies to choose how they want to participate with Interac.” Thus, not all companies which use Interac services choose to be members.

Contrary to the popular belief in the civil service, which holds that private sector organizations have simpler and more straightforward governance mechanisms, Interac Association²³ has just as many Byzantine complexities as most public sector collaborations. It is controlled by a host of regulations, such as the Competition Act and acts governing financial institutions, which restrict what types of collaboration are possible and what types of services can be offered by its members. “These restrictions are things we must deal with every single day,” said Morris.

Interac Association is an unincorporated not-for-profit association of members. It is headed by a Board of Directors of 14, appointed from the largest members, but whose structure ensures that both non-financial institutions and other types of members are represented. Interac Association’s members include: all major Canadian financial institutions; many foreign bank subsidiaries; trust companies; credit unions; caisses populaires; payment processing companies; “white label” bank machine operators; and some very large merchants. The board typically meets three times a year, one meeting incorporating a larger Annual General Meeting.

Members sign a Memorandum of Association (MOA), which is Interac Association’s governing document and outlines its mandate, scope and requirements of operation. Members include both Direct and Indirect Connectors, which refers to the manner in which they connect to the INTERAC network.

- **Direct Connectors**, connect directly to one another through the network. Direct Connectors operate processing systems and run special communications software to connect to the Interac network.
- **Indirect Connectors** connect to the network through a Direct Connector. A number of Direct Connectors offer these network connection services in a competitive marketplace. Interac Association is not involved in the negotiation of these network access arrangements.

Members are also free to outsource various functions and enter into business arrangements with non-members. In these instances, the member retains full responsibility for compliance with all rules and for all transactions entered into the network.

Interac Association’s network is completely decentralized with no central hub. Each Direct Connector) maintains physical links with every other Direct Connector. Interac Association manages the network itself (through outsourcers) but not the clearing and settlement of payments between members (which is done via the Canadian Payments Association). It

²³ While Interac Association is unincorporated, Interac Inc. is a formal legal entity, which handles Interac’s legal affairs and intellectual property matters. It is “subservient” to Interac Association. As well, Access Corporation owns the intellectual property underpinning the network, because of legal restrictions.

maintains management oversight and provides common services, such as fraud detection and management and establishing standards.

Policies and standards in specific areas are developed through twelve Advisory Groups (e.g., security, fraud, network operations) comprised of a number of member representatives. It is the job of these Advisory Groups to serve as a channel for consultation on issues, providing both subject matter expertise and a vehicle through which support and consensus is sought. “Originally, most of these groups had the same organizational representation as the board,” noted Morris. “However, over the years we have found that broader membership on these groups is desirable and helps us achieve more buy-in to our plans.” Advisory Group members come from a variety of organizations and work on a part-time basis (e.g., most advisory groups meet monthly), in addition to their day-to-day work. As a result, it can sometimes be challenging to get their full attention.

Interac Association’s governance critical success factors are also its most important challenges, explained Morris. Chief among these are:

- **Acknowledging the Need for Collaboration.** There are many areas where members benefit more from the critical mass and standards offered by collaborating, but there are others where individual members want to maintain a competitive edge. Interac Association tries to walk the thin line between operating as a trade association and functioning as a business. As a trade association, it has a role to play in regulating the network and representing the group’s collective interests; however, it also understands that its members are in business to sell products and services. Interac Association’s success is therefore predicated on the members’ acknowledgement that the benefits of collaboration outweigh those of “going it alone”.
- **Broad Consultation.** As the organization has evolved from one whose members had very similar interests to one with many more divergent interests, governance and decision-making practices have also had to evolve. “We are hugely dependent on consultation,” said Morris. “It’s not a trivial exercise to generate agreement.” However, while decision-making in a multi-stakeholder environment can be “arduous”, inclusivity is critical to maintaining the effectiveness of the organization. Where non-members are major players in an area, they are typically invited to participate in the work of the Advisory Groups. “Finding ways to do consultation is therefore critical to making progress in our organization,” said Morris.
- **Flexibility.** As noted above, membership in Interac Association is open to all Canadian companies. There are no fees to become a member. Interac Association’s costs are recovered on a fee-for-transaction basis. Its MOA is neither exclusive nor binding for any period of time. Members only agree to follow the parameters of the network’s operations and abide by legal and regulatory conditions. They can also choose which services to participate in.
- **Relationship Management.** Behind all the formal relationships are “myriad others”, noted Morris. “As we have evolved, we have found that informal committees and one-to-one working relationships are often where the work really gets done.” Maintaining and

supporting these relationships requires more legwork than supporting more structured groups, but the results are worth it.

Interac Association is supported by a staff of about 65, who direct all aspects of the organization's work, manage the relationships, and oversee the operation of the network.

Discussion

You have each indicated the importance of broad consultation from amongst your stakeholders. How do you select them? At Interac, consultation begins with representation that is a mirror image of the board of directors. Then, large participants in the association or constituent groups who have an interest in the subject at hand are added on a case-by-case basis. If the situation will require investment, then all possible investors are included. At Infoway, efforts are made to include thought leaders and all stakeholders with representation in the pan-Canadian space, e.g., Ministries of Health, National Health Care Providers. While these don't always truly represent the full pan-Canadian view, they are the best groups available. As well, national representatives of public groups, e.g., the Citizens Privacy Coalition, are consulted. At CCMTA, who is consulted depends very much on the issue. If there is a permanent standing committee to deal with the topic, it is usually quite easy to identify the relevant stakeholders.

It's sometimes difficult to determine which minister is responsible for IdM&A. What is your advice in this situation? At Infoway, in these situations, each jurisdiction is asked to nominate someone to represent it to the organization. This nominee is then responsible for managing communication and decision-making internally. With COM-T there is some overlap between ministers, and they tend to decide amongst themselves what they want to do. If both come to meetings, they get one vote and therefore must agree on what to do in advance. All participants agreed that since responsibilities in the different organizations/jurisdictions change continuously, it is important for a governance structure to be able to adapt to changes and restructure accordingly.

How involved is Interac with arrangements between its direct and indirect connectors? These arrangements are negotiated between the two organizations involved. Interac is responsible for doing due diligence, but it is not a broker.

What principles and standards do you have around IdM&A? Infoway would be happy to share these with the Task Force. These were established in consultation with the key stakeholders and based on common principles, e.g., "we will adopt international standards", "we will connect using international standards". If there are no standards in place at the time a project is being developed, Infoway will fund retrofitting it to standards when these are established. All jurisdictions have committed to using the standards developed by others during Infoway projects. Since standards go through several reviews, they are likely to be well-designed when finally accepted.

What models do you use for independent audits? Michel Gravel noted that the new audit requirements are onerous for not-for-profit organizations. Directors must fully understand their responsibilities and more documentation is required. In addition, the auditor has the option of appearing before the board and identifying any issues that he/she feels have not been satisfactorily addressed. At Interac, there is an annual financial audit. In addition,

members are audited for adherence to the organization's standards, including technical standards for inter-operability and security and risk management standards for confidence in the network. The organization uses a blend of centrally-managed audits and self-managed audits. Increasingly however, this function is becoming more centralized. Infoway has an annual audit regarding its spending of public funds but the systems it funds are not audited because they are a provincial responsibility. Infoway also certifies adherence to standards for vendor products and this has been very positively received by vendors because it speeds up the acceptance process in the different jurisdictions.

What are the critical success factors for your funding models? Infoway is funded by Health Canada but the organization must demonstrate the value it has delivered. At CCMTA, value for money is also critical since it is a user pay model. Interac has similar criteria. Morris noted that value must be perceived by the *individual* members as well as the collective membership.

What challenges do you face around having common terminology? All three organizations face difficulties in this area. Infoway believes that it is "immensely critical" to agree on common terms, even if a different term is used by a jurisdiction internally. Glossaries can be important documents in these cases. "We put a stake in the ground with terminology and leave the jurisdictions to map their own terms to this," stated Ratajczak. At Interac, establishing common terminology is a prolonged process that is "painful but necessary". Morris has found that it is easier to wait to draft documents until these common terms can be established. Gravel agreed, noting that even when English terminology has been agreed on, "everything can start all over again when French terminology is being worked on."

What advice do you have for establishing a governance structure for IdM&A? Before a governance structure can be established, it is essential to get agreement on *what* is going to be governed, said Gravel. Only after the key strategic objectives have been established can governance be introduced. Morris agreed. He also pointed out that it is easier to expand one's governance structure to include "those who yell and scream to be included" than to take away a voice. At Infoway, the governance framework is evolving. Ratajczak stated that whatever gets built will likely be "50% wrong" and that establishing an effective governance framework is going to be a constant and evolutionary process.

Appendix G

Identity Management and Authentication Models

This section provides a brief overview of identity management and authentication models that are used or under development in Canada and elsewhere in the world.

Identity management and authentication models can essentially be categorized into two basic groups: **Directory-Centric** (*also referred to as Enterprise, Application, Domain, or Service-Provider-Centric*) and **User-Centric**.

Directory-Centric Models

Most existing identity management and authentication models are enterprise or directory-centric. Since identity management and authentication has traditionally been viewed from the service-provider's point of view, directory-centric models are designed to be cost effective and scalable primarily for service providers. In a directory-centric model, an enterprise (or some similarly bounded set of organizational entities and/or application systems) manages identity information as a way of controlling access to electronic services within the enterprise.

Directory-centric models have evolved over the years from decentralized or silo models to more centralized and federated models. In part, this evolution has occurred to improve the user experience by providing single sign-on-like capabilities. While centralized and federated models have improved the user-experience in this regard, they have, at the same time, created other problems such as privacy concerns and complicated trust relationships. Below is a summary of the main directory-centric models and the advantages and disadvantages of each general model.

A. Decentralized or Silo Model

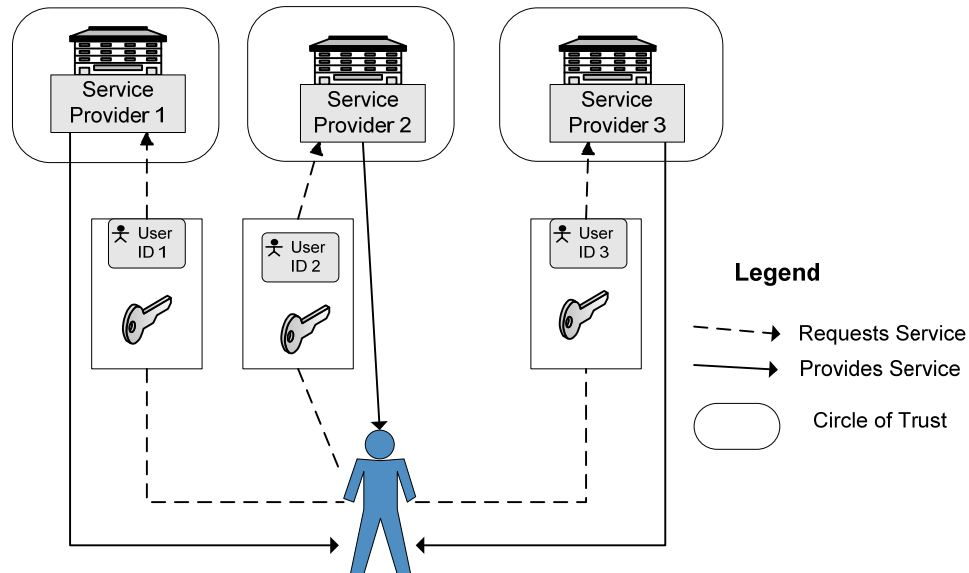
This is the most common identity management and authentication model, although it is important to note that the Environmental Scan conducted by the Task Force revealed a departure from this model towards more centralized and federated models in recent years.

In this model:

- Service providers act as both identity provider and credential provider/verifier to their clients.
- The client gets separate identifiers and credentials (such as passwords) from each service-provider he or she transacts with.

This model is illustrated below in Figure 23:

Figure 23 - Decentralized Model



Advantages of this model are:

- It provides relatively simple identity management for service providers.
- Service providers retain control and, therefore, trust in identity information. This is particularly useful where users are operating in a “work persona” and the organization wants strict control over access.
- Separate identifiers for clients provides some privacy protection, in that there is no shared identity information across departments.

Disadvantages of this model are:

- It is rapidly becoming unmanageable for users, who are overloaded with identifiers and credentials that they need to manage.
- Requiring users to memorize multiple passwords, increases the likelihood that they will not use the services, forget their passwords or adopt sloppy password practices like using reusing passwords or using insecure, easy-to-guess passwords.
 - For important sensitive services, where password recovery must be highly secure, forgotten passwords can significantly increase the cost for service providers.

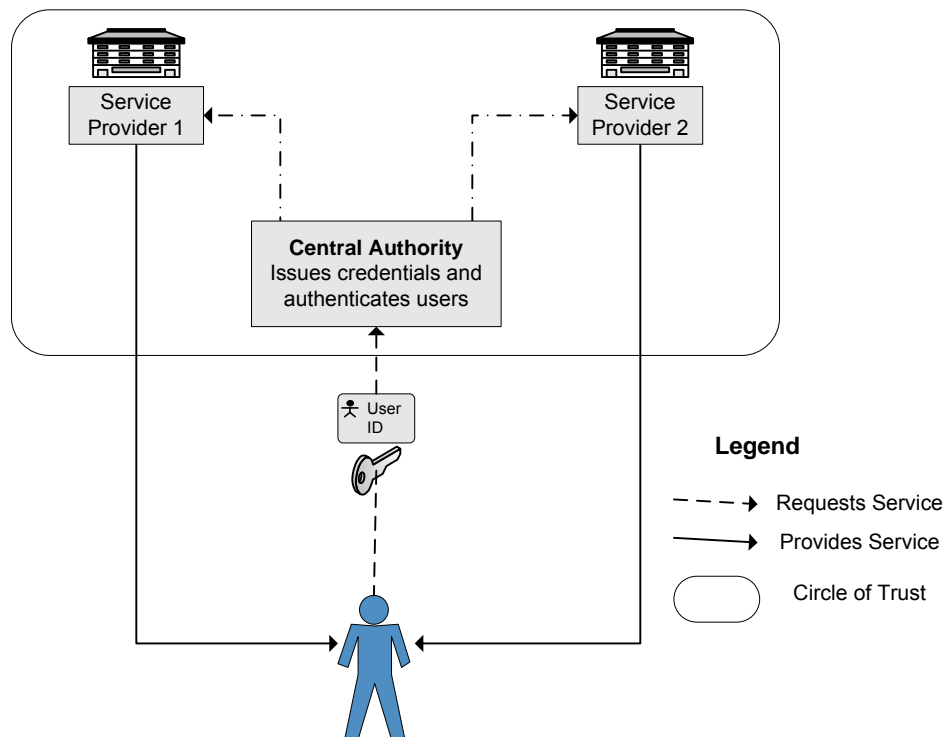
B. Centralised Model

Centralized identity management and authentication models can be implemented in a number of ways but in general:

- There is a single identifier and credential provider (Central Authority) that is used by all service providers.
- In some models, the Central Authority provides both identifier/credential issuance services and authentication or verification services for the service providers.
- The client can use the same identifier and credential to access all services.

This model is illustrated in Figure 24 below.

Figure 24– Centralized Model



Advantages of this model are:

- Clients only have to use one identifier and credential (e.g., password) for all services.
- Clients enjoy a single sign-on experience.

- Centralized account management for service providers.
- Well-suited for closed environments where multiple service providers are managed by the same organization, common policy or authority.
- It is a relatively easy model to set up.

Disadvantages of this model are:

- A central repository of identity information creates considerable privacy risks.
- The client has limited control over his identity information and identifier as it is controlled by a central authority and distributed among participating service providers.
- A centralized model is a daunting charge for the central authority who is solely responsible for the secure issuance of identifiers and credentials and for verifying clients seeking services.
- Not suitable for open environments where service providers are not governed by a common policy and authority.

C. Federated User Identity Model

Both decentralized and centralized models can be extended to multiple enterprises or jurisdictions using “federation”.

Identity federation is essentially a set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain. By establishing formal trust relationships and leveraging their respective identity information, organizations are able to set up inter-organizational or jurisdictional access to services. Examples of this model include Liberty Alliance (<http://www.projectliberty.org/>) and Shibboleth (see <http://shibboleth.internet2.edu/>).

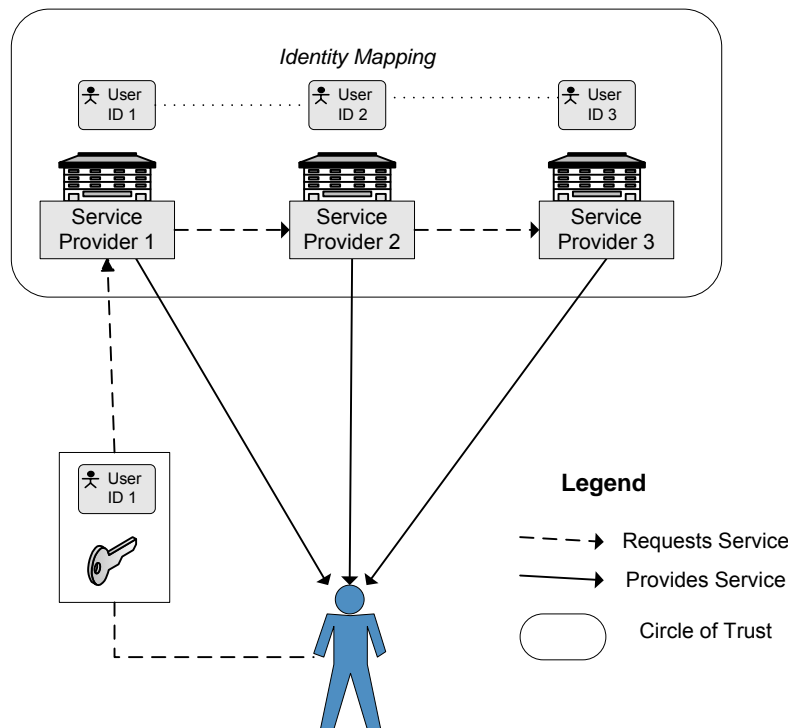
In this model:

- A mapping is established between the different identifiers that a client has from different service providers. This mapping links the associated identities which results in a single virtual identity domain.
- When a client is authenticated to a single service provider using one of their identifiers, he or she is considered to have been identified and authenticated with all the other service providers as well. This happens by passing assertions between service providers.

- Federation of identifiers gives the client the illusion that there is a single identifier domain.
 - The client can still hold separate identifiers for each service provider. However, the client does not necessarily need to know or possess them all. A single identifier and credential is sufficient.

This model is illustrated in Figure 25, below:

Figure 25– Federated Model



Advantages of this model are:

- It provides a single sign-on experience in an open environment.
 - Clients enjoy the illusion of a single identifier domain and a single sign-on experience.
- Although a client may hold a separate identifier and credential (e.g., password), for each service provider, he only has to use one to access all services within the federated domain.
- Although less privacy protective than the decentralized model, it is, if set up with the proper policy restrictions, more privacy protective than the centralized model.

Disadvantages of this model are:

- The establishment and maintenance of a large number of trust agreements creates legal and technical complexity.
- As in the centralized model, the client has limited control over his identity information and identifiers. This information is controlled by and shared with the numerous service providers within the federation.
- Without centralized control, inconsistencies of data may occur.
- Governance of multiple agreements and standards is complicated.

User-Centric Models

User-centric models turn traditional identity management and authentication models on their head, by putting users, rather than identity and service providers, in the center of the transaction.

This model is commonly referred to as “Identity 2.0” and is the focus of various industry efforts, including “Higgins” under IBM, “CardSpace” by Microsoft, and “Sxip Access” by Sxip Identity. While this model is still under development, it is seen as a likely trajectory for future identity-dependent Web services. This will mean that over the long term, Internet users will begin to expect governments to be part of such services. This will be particularly relevant within the realm of citizen identity management.

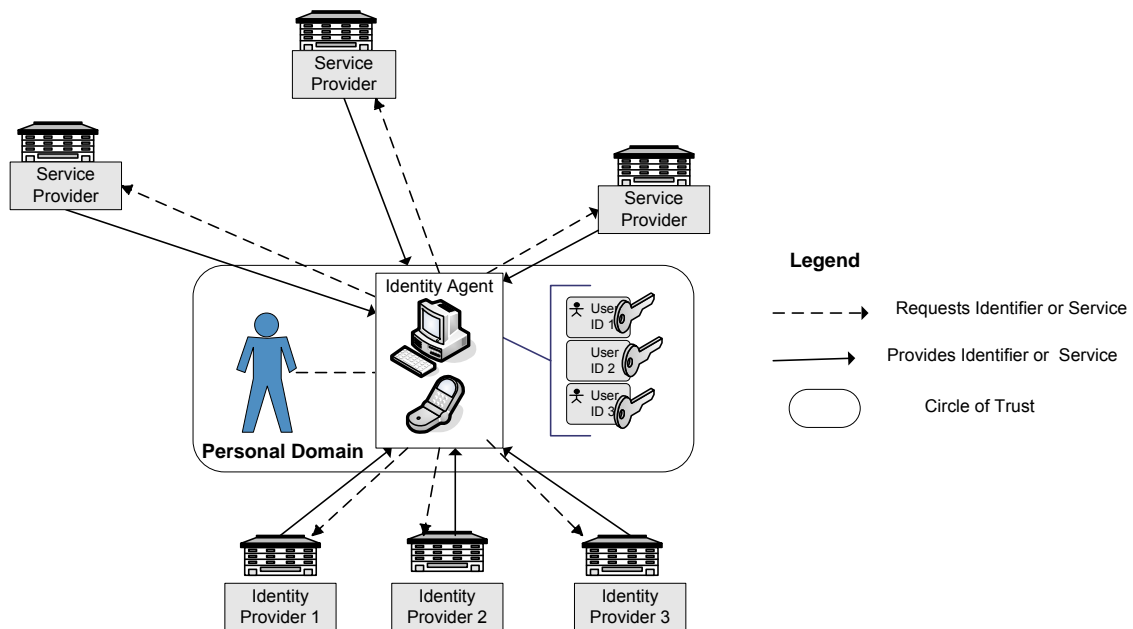
In this model:

- The client is in the middle of a data transaction.
- The client manages and shares his or her identity information using an “identity agent”. An identity agent can be a browser or it can be a portable personal authentication device (perhaps even a cell phone).
- Certificates from authoritative identity sources can be acquired by the client and associated with the client’s identity agent. These certificates can then be presented (similar to pulling a card out of an electronic wallet) when proof of identity or identity characteristics are required by service providers.

The key difference from directory-centric models is that the user is in the center of the data transaction and in control of their identity information. The data always flows through the client’s identity agent and, as such, the client is able to release information only as she sees fit. It is important to note, however, that like directory-centric models, user-centric models can be implemented in different ways (i.e., decentralized, centralized and federated).

Figure 26, below, illustrates a simple decentralized user-centric model but it is easy to envision its extension to a federated model, by the addition of federated domains of trust, each containing numerous identity and service providers.

Figure 26 – User-Centric Model



Advantages of this model are:

- It is privacy enhancing as client manages and controls his own identity information.
 - In addition, the identity provider does not know which service the client is using the identifier for. It is similar to presenting your driver's license to a store clerk – the driver's licence bureau does not know, and is not informed of, where you might use your driver's licence for identification purposes
- It is very scalable as the identity provider does not need to establish a relationship with, or have any prior knowledge of, the service provider.
 - This allows the network of sites to build up on an ad-hoc basis
- The client has a consistent user experience.
 - This does not mean that all clients have the same user experience, but that a specific client is using the same identity agent over and over for each identity transaction.
- It is extremely adaptable and can be combined with any existing directory-centric model.

Disadvantages of this model are:

- It is still in the development stage.
- It is unclear how the credentials issued by identity providers would be “certified” or accepted by service providers and how administratively complex that would be.

References

In keeping with the principle of validating, leveraging and enhancing existing work on IdM&A, the Task Force reviewed and incorporated terms, concepts and models from domestic and international public sector organizations, academic research studies, and sub-committee initiatives commissioned by the PSSDC and the PSCIOC. A selected bibliography is provided below:

1. "The politics of digital identities" by: Jeffrey Roy, **The Ottawa Citizen**, January 23, 2007
2. Available from: Corporate Information Security, Government of Alberta, ciso@gov.ab.ca
 - (a) "Identity and Authentication Standard Approved", January 30, 2006
 - (b) "Identity Theft Committees and Initiatives – An Overview", July 14, 2005
3. "Identity Management", **Government Journal**, Volume 1 Issue 2.
4. "Identity Management Initiative Charter", Treasury Board of Canada Secretariat, Chief Information Officer Branch, Government of Canada, August 2006, RDIMS# 450806
5. "Secure Driver's Licence Travel Option Conceptual Design", WHTI Province/Territories Consultative Group, Canada Border Service Agency
6. "A National Identity Card for Canada? Report of the Standing Committee on Citizenship and Immigration", October 2003, House of Commons, Canada, Joe Fontana, M.P., Chair
7. PSCIOC/PSSDC Cross-Jurisdictional Identification, Authentication and Authorization Working Group's Identification, Authentication and Authorization Framework Policy and Guidelines - Consultation Draft – Release 3.0, November 2004 at http://www.iccs-isac.org/eng/pubs/IAA_guidelines.pdf
8. Citizen Information Project Report "Better sharing of citizen data across the public sector", Office of National Statistics, UK, November 4, 2006.
9. "Strategic Action Plan for the National Identity Scheme Safeguarding your identity", UK Home Office, December 2006.
10. "Integrated Service Delivery: Beyond the Barriers", Kenneth Kernaghan, Professor of Political Science and Management, presentation at Brock University, May 31, 2003
11. "Modinis Study on Identity Management in eGovernment"
Prepared for the eGovernment Unit, DG Information Society and Media, European Commission, Identity Management Issue Report, Deliverable: D.3.9 June 2006
12. "Canadians' Views on Privacy, Security, Information Sharing and Identity Management", Cathy Ladds Research and Analysis Division, CIOB Treasury Board of Canada Secretariat, Prepared for Federal and Provincial and Territorial Deputy Ministers, December, 2006

13. "Service québécois d'authentification gouvernementale", Ministère des services gouvernementaux, Avis d'appel d'intérêt, 30 octobre 2006
14. "Authentification des citoyens et des entreprises dans le cadre du gouvernement électronique", Orientations et stratégie, Août 2004
15. "Information technology — Security techniques — A framework on identity management" American National Standards Institute: New York, Secretariat ISO/IEC JTC 1, December 2006.
16. Roadmap for Identity Assurance in the UK , Information Assurance Advisory Council, July 2006 v1.0 at <http://www.iaac.org.uk/Default.aspx?tabid=105>
17. An Introduction to Identity Management (Hp), Written by Jan De Clercq and Jason Rouault June 2004.
18. BTEP Identity Management: Mapping the Continuum, prepared by Team BCE, Secure Channel Project, Government of Canada.
19. The Laws of Identity, Kim Cameron's Identity Weblog at http://www.identityblog.com/?page_id=354
20. 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age, Information and Privacy Commissioner, Ontario, 2006 at <http://www.ipc.on.ca/index.asp?navid=46&fid1=470&fid2=4>
21. Focusing on Identity in the Government of Canada, Treasury Board of Canada Secretariat
22. The CDT preps new authentication and ID policies (The Center for Democracy and Technology will introduce a 10-point set of authentication and identity management guidelines to the FTC next week), by Matt Hines, April 18, 2007, InfoWorld at http://www.infoworld.com/article/07/04/18/HNcdtschwartz_1.html
23. CAN ID? Visions for Canada's Identity Policy. Understanding Identity Policy and Policy Alternatives, Draft Version 2.2 – June 2007, Information Policy Research Program, Faculty of Information Studies, U of T in partnership with Policy Engagement Network, LSE at <http://www3.fis.utoronto.ca/research/iprp/publications/PDFs/CAN-ID/CAN-IDreportv2gaJul3.pdf>
24. Identity Project Report, London School of Economics and Political Science, June 2005 at <http://identityproject.lse.ac.uk/identityreport.pdf>
25. Australian Government e-Authentication Framework (AGAF) for Individuals Discussion Paper December 2005
26. National CIO Council Subcommittee for Information Protection (NCSIP), Public Sector Security Classification Guideline, Public Sector CIO Council (PSCIOC), September 7, 2004 www.iccs-isac.org/eng/pubsec_security_class.htm
27. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management, June 2005

28. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, October 2005
29. Working documents: Security Component Narrative and Storyboard, Murray Rosenthal, City of Toronto, June 2007
30. Jan De Clercq, Jason Rouault, "An Introduction to Identity Management," HP, June 2004
31. Jason Rouault, Jan De Clercq, "Identity Management Architectures," HP, July 2004
32. Laurence Millar, "Authentication to Access Government Services: What Might the Future Hold," State Services Commission, Government of New Zealand, March 30, 2006, <http://www.privacy.org.nz/filestore/docfiles/71275093.ppt#1>
33. "Authentication for e-government: Government Logon Service Design Overview," State Services Commission, Government of New Zealand, n.d., <http://www.e.govt.nz/services/authentication/library/docs/authent-blueprint-0605/index.html>
34. "Authentication for e-government: Best Practice Framework for Authentication," State Services Commission, Government of New Zealand, April 2004, <http://www.e.govt.nz/services/authentication/library/docs/authentication-bpf/index.html>
35. "On-line Authentication for e-government Blueprint," State Services Commission, Government of New Zealand, July 2003, <http://www.e.govt.nz/services/authentication/library/docs/authent-blueprint-200307/index.html>