May 31st, 2011

Trusting Identities

The IMSC Pan-Canadian approach to enabling better services for Canadians

Draft for Consultation

This paper has been prepared for consultation by the Pan-Canadian Identity Management Steering Committee (IMSC).

Pan-Canadian Identity Management Steering Committee

Table of Contents

Executive Summary

As Canadians move towards a fully digital society, trusting identities, especially in the online world, has become a critical issue. The Internet, as the preferred service delivery channel, has evolved. It has now become the critical enabler for the other service delivery channels (in-person, telephone and mail) and a major driver of change in our social, economic and cultural institutions. As Canadians conduct more and more of their lives online, the questions of whom they are dealing with and how they can trust services have become more acute.

A significant factor in trusting services is the ability to trust identities across the boundaries of systems, services and jurisdictions. In the online world, how do we as individuals, as citizens, or as governments trust each other to deliver and receive services? If identity information cannot be readily conveyed and trusted in the online world, it could impair our ability to work together as individuals, collectively as governments, or as a society.

This paper proposes an approach to trusting identities within the Pan-Canadian context – trusting identities of individuals and businesses as they are used between services, across delivery channels, across the Canadian public sector, and across the Canadian private sector. This approach, analogous to how we already organize ourselves as a country, represents the next logical step in the work that was completed in 2007 by the Identity Management and Authentication Task Force (IATF). The development of this paper was overseen by the Pan-Canadian Identity Management Steering Committee (IMSC), a multi-jurisdictional body responsible for advancing identity management within the Canadian public sector.

The Pan-Canadian approach continues to embrace the vision set forth by the 2007 Task Force: *"Citizens and businesses enjoy simple, convenient and protected access to multi-jurisdictional services in a manner they choose and control"* and *"Governments in Canada are trusted, collaborative leaders in citizen-centred service delivery"*.[1] This vision remains valid despite the rapid evolution of technology and the blurring of lines between the online and real world service delivery.

The guiding principles have been re-stated to emphasize what is appropriate to govern the trusting of identities across the Pan-Canadian context:

> **Principle 1: Interoperable, Cost-Effective and Innovative.** Trusted identities and exchange of identity information should be easily accepted across different jurisdictions,

[1] 2007 Task Force Full Report can be found at: http://www.iccs-isac.org/en/km/transformative/pdf/taskForce.asp

through multiple channels (online, in-person, telephone, mail), and enabled by cost-effective and innovative systems supporting a diverse array of services.

Principle 2: Easy to Use, Client-Focused, and Voluntary. Clients should be able to easily and voluntarily use their trusted identities online by means of a simple, consistent and intuitive experience across programs and jurisdictions.

Principle 3: Safe, Secure and Privacy Enhancing. Canada's approach should be safe, secure and privacy enhancing in a manner that respects the rights of the client while protecting them against potential abuses, such as identity fraud.

Principle 4: Accountable and Transparent. Trusted identities should be subject to clear governance, with governments accountable and transparent with respect to activities involving identity.

Four key goals were defined:

Goal 1: Improve the service delivery environment. Canada will continue to improve the service delivery environment in way that supports economic growth and the shift to a digital society.

Goal 2: Preserve the trust and confidence of Canadians. Canada and its governments will preserve the trust and confidence of Canadians as they transition to online services and transactions.

Goal 3: Create a harmonized, inclusive and interoperable framework of policies, standards and laws. Canada will develop and adopt a 'framework of frameworks' consisting of policies, standards and laws that work together through political, business, and technological means.

Goal 4: Establish a Pan-Canadian technical infrastructure for trusted identity. Canada will establish a trusted infrastructure that will enable Canadians to securely and safely identify themselves and exchange identity information regardless of where they live or work in Canada. This infrastructure would also encourage governments and industry to provide services and solutions to Canadians in new and innovative ways.

Four major actions were recommended:

1. **Establish a Pan-Canadian Trusted Identities Forum that includes an expanded membership from the public sector, broader public sector and commercial organizations.** This forum should have the mandate to lead identity management

from a Pan-Canadian perspective, carrying out the activities necessary to achieve the goals outlined in this paper.

2. **Facilitate wide-scale adoption.** Ensure that favourable conditions are in place, such as usability, cost-effectiveness, and ease of access which will encourage wide-scale adoption by all Canadians, including individuals and businesses as clients, and government and commercial institutions as authoritative and relying parties.

3. **Build a trusted identity infrastructure.** Encourage the development of solutions that can provide Canadians with simple, convenient and protected access to multi-jurisdictional services in a manner they choose and control**.**

4. **Develop an awareness and outreach program.** Help Canadians be aware of the Pan-Canadian approach to trusting identities. This also includes understanding the benefits of participating in online services, how their trust can be preserved and how they can safely and securely participate in online transactions.

To conclude, the Pan-Canadian approach to trusting identities is the next step toward improving services for Canadians and enabling the evolution of service delivery. The goals, principles, and recommendations for actions outlined in this approach can be used as the framework to move another step in the journey towards trusting identities across Canada.

Introduction

All Canadian governments – federal, provincial, territorial and municipal – share a common need to provide services to citizens and businesses. Services that were once offered separately and exclusively within the physical realm are combining and moving into the digital realm. Canadians, regardless of where they live or how they conduct business with government, are demanding that their needs be met during this transition to the "online" digital world. Despite the many transformative opportunities now possible, governments continue to have a responsibility to ensure that all services are equitably accessible, whether these services are offered online, over the counter, by phone or by mail.

Future examples of simple, convenient and protected access to multi-jurisdictional services envisioned for all Canadians

- An individual from Nova Scotia notifies Service Canada that she is moving to British Columbia. Upon her consent, Service Canada provides British Columbia with up-to-date identity information, including change of address information from her recent home purchase in BC.
- An Ontario driver renews his driver's license and selects the enhanced identity verification option. He consents that his identity information may be used to streamline his enrolment process in the federal government's trusted traveller program.
- A resident of Windsor wants to open a pharmaceutical business for which there are licensing requirements across federal, provincial and municipal jurisdictions. For the individual to be able to complete and submit these licensing requirements across jurisdictions, the identity of the individual must be trusted as the licensing information is received, reviewed and approved.

Governments are continually challenged with the rising expectations of citizens and the pace of technological change. Adding to this challenge is the blurring of lines between the physical and the online world. Boundaries between jurisdictions become invisible in the online world and Canadians expect to interact with government (or with several governments) in a seamless manner, through the channel they choose, at their convenience and at little or no additional cost. All governments must meet these new expectations, but it must be balanced with the need to protect citizens against the threats of cyberspace, such as identity theft and online fraud.

Canada has long been a leader in digital initiatives and the adoption of online service delivery to citizens. According to Statistics Canada, in 2009, 77% of Canadians, 16 years of age and older, (20.8 million) use the Internet from their home, and 44% of Canadians (11.9 million) search from their home information about Canadian municipal, provincial or federal governments.[2]

[2] 2009 Canadian Internet Use Survey, Statistics Canada

Canada continues to be successful in its commitment to be "known around the world as the government most connected to its citizens."[3]

Canada is readying itself for the next phase of evolution of service delivery. The Internet is no longer just a preferred delivery channel - it has become the major driver of change in our social, economic and cultural institutions. Canada is now shifting into the digital economy and the Canadian population is transforming into a digital society. Along with other countries, Canada is now grappling with the patchwork of online strategies and fragmented user experiences that have evolved independently of one another. This patchwork and fragmentation is also being exploited by the online criminal element. As a consequence, people's online experience is marred by security and privacy concerns when online services involving personal information have a high potential for compromise. A significant factor in trusting services is the ability to trust identities online. This erosion of trust has become a significant issue for governments and represents a major constraint limiting governments' ability to provide online services the same as what individuals expect from the commercial sector and in the physical world.

Going forward, the issue of trusting identities across jurisdictions and across channels must be solved at a national level. With the evolution of service delivery on mobile platforms occurring at a breathtaking pace along with the embrace of Web 2.0 technologies, there promises to be new social, economic, and cultural opportunities for all Canadians. Canada is becoming a truly digital society. However, the critical issue that underlies this march towards a digital society is *trust*. How do we as individuals, as citizens, or as governments, *trust* each other, especially in the online world? Trust starts with individuals trusting that governments are doing the right thing and it includes Canadian governments trusting each other and working together to benefit the country as a whole. If trust cannot be conveyed in the online world, it impairs our ability to work together as individuals, collectively as governments, or as a society.

Trust is closely related to *identity*. The first question that is asked when trust is to be established is: *Who are you?* But this question is difficult to ask and to answer in the online world. What is readily conveyed in the physical world, *trust* and *identity*, is becoming an impediment in the online world. This intertwining of trust and identity, or *trusted identity* must be solved within the broader Pan-Canadian context, rather than separately by each jurisdiction. How we collectively trust identities and how we protect and exchange identity information is the issue that must be solved if we are to embrace the next phase of the evolution of service delivery and ultimately, the long-term growth of our digital society.

[3] http://www.tpsgc-pwgsc.gc.ca/apropos-about/fi-fs/ged-gol-eng.html .

Canada is well-positioned to solve the problem of trusting identities, especially within the online context. Canadians are already among the most connected in the world and our country already benefits from a well-developed Information and Communications Technology (ICT) sector and exerts strong business leadership in the digital economy. Canadians also recognize that identity is a shared responsibility between all levels of government and a responsibility that goes beyond our borders requiring collaboration with other countries and through global partnerships.

The Changing Landscape in Canada

In 2007, the Identity Management and Authentication Task Force (IATF) published a report entitled "A Pan-Canadian Strategy for Identity Management and Authentication."[4] This report defined a Pan-Canadian identity management framework consisting of a lexicon, seven components[5] and a proposed governance and funding structure. To further this work, the Identity Management Steering Committee (IMSC) was formed in 2008 and currently oversees the continued development of frameworks.[6]

Since the completion of the 2007 IATF report, there have been major developments in the field of identity management. To name a few: the rise of identity federations, adoption of multiple levels of assurance, 'privacy by design', and the global consensus on trust-based frameworks such as the Kantara initiative. In 2010 the IMSC decided to re-visit the strategy defined in the 2007 IATF report, and produce an update, with this paper being the outcome.

While there have been several developments since the 2007 IATF report, many things have stayed the same or, rather, have become more certain. Canada requires a trust-based and de-centralized approach that respects the autonomy and the laws of the many different jurisdictions. This approach does not include a national ID card scheme, a national identifier, or a centralized identity database (such as the recently dismantled UK National ID Card Scheme).

New imperatives are forming as result of the changing landscape. As jurisdictions increasingly collaborate with one another on service delivery, trusting how individuals assert their identity online is becoming a critical issue. As citizens expect deeper engagement with government, this

[4] Available at ICCS website http://www.iccs-isac.org/

[5] The seven components are: legal, privacy, security, assurance, trust, identity and service.

[6] The framework documents are available at: http://www.iccs-isac.org/en/km/transformative/index.asp

will be prevented unless there is a way to adequately trust identities online and exchange identity information across jurisdictional boundaries. Presently, there is no Pan-Canadian solution that supports trusted identity and consequently jurisdictions are creating independent authentication solutions and frameworks 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. The issue of trusting identities online must be solved in the short run, if we are to realize benefits over the long run.

Canada's approach will consist of multiple trusted identity sources, arising from the existing programs and services already delivered to Canadians within the different jurisdictions. Canadians will retain the choice to decide which trusted identity source they can use to assure their identity regardless of which service they access. In summary, the Pan-Canadian approach for trusting identities will be built upon existing programs and services with minimal changes to enabling legislation and will facilitate seamless access to services.

Vision

The vision stated in the 2007 Identity Management and Authentication Task Force Report[7] remains valid today:

2007 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 Pan-Canadian strategy on trusted identities supports this vision by enabling identity information to be used in a secure manner that supports a seamless, user-centric and cross-jurisdictional service delivery experience for citizens and businesses when they interact with different levels of government. The initial focus of the strategy is the online channel but it can be applied to multiple service delivery channels (i.e. in-person, telephone and mail).

[7] Executive Summary and Full Report are available at: http://www.iccs-isac.org/

Trusting Identities Online

A major issue today is trusting identities online. A trusted identity, regardless of the channel used, comes from answering two questions: 1) "*Who are you?"* and, *2)" Is this you?"* When both of these questions are answered with confidence, it can be viewed as a *trusted identity*. In simple terms, a trusted identity is: 1) *knowing who you are*, and 2) *whether it's actually you* (i.e. not somebody else) who is accessing a service intended for you.

Trusted identities are used every day in the physical world. For example, when you travel to another country, your passport contains identity information and serves as your trusted identity. The passport, an internationally recognized travel document, answers the question of "*Who are you?*" by means of the identity information (surname, given name, etc.) printed on the passport page. The question of *"Is this you?"* is answered by the photograph or signature inspected by the border agent. Together, when these two questions are answered satisfactorily, the agent now trusts your identity and can move on to other questions regarding your travel.

In the online world trusted identities are problematic. Unlike the physical world with documents or cards you carry in your wallet, there is no recognized online equivalent that authoritatively answers the question *"Who are you?"* Also, the question *"Is this you?"* is equally difficult to answer because you are not standing in front of a person who can visually verify that it is you. Because you are far removed from

Did you know?
There is a difference between Identity Theft and Identity Fraud.

Recent changes to the Canadian Criminal Code have added identity offences that relate to how criminals steal and use identity information.

Identity Theft refers to the preparatory stage of acquiring and collecting someone else's personal information for criminal purposes. In committing *identity theft,* criminals steal information to answer "*Who are you?"* so that they can sell this information to others or use it themselves. Identity thieves are looking for this type of information:

- full name, date of birth ,
- Social Insurance Numbers ,
- full address,
- mother's maiden name
- username and password for online services,
- driver's license number,
- personal identification numbers (PIN) ,
- credit card information (numbers, expiry dates and the last three digits printed on the signature panel),
- bank account numbers,
- signature,
- passport number

Identity Fraud is the actual deceptive use of the identity information in connection with frauds such as the misuse of debit/credit cards or applying for loans using stolen personal information. In committing *identity fraud*, criminals exploit the difficulties of answering the question online *"Is this you?"* so that they can impersonate others. Criminals want to use your identity information to:

- access your bank accounts
- open new bank accounts
- transfer bank balances
- apply for loans, credit cards and other goods and services
- make purchases
- hide their criminal activities
- obtain passports or receive government benefits

Source: http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm other people and most likely using the Internet from your home, your business or from a public place, there are many opportunities for criminals to compromise and misuse your identity online.

Trusting identities online is especially problematic for governments. Compounding the issues stated above, governments are additionally responsible to ensure that people who have the least ability and often with the greatest need to use online services are not excluded because they lack the means to transact online. Online services should be universally accessible but this goal must be realized in the face of fiscal realities, cyber-threats and the duty to prevent harm by abusive parties. Whether accessing health records, submitting taxes, receiving unemployment benefits, or applying for visa from outside the country, the use and reliance upon trusted identities both in the physical world and the online world is an essential prerequisite to lasting service improvements.

Pan-Canadian Approach to Trusting Identities

Canada's approach to trusting identities is analogous to how we already organize ourselves as a country. Canada is "a federation, with a strong central government and Parliament, but also with an ample measure of autonomy and self-government for each of the federating communities [i.e., provinces and territories]."[8]

A good example of how we work together as a federation is our transportation system. Driver licensing and vehicle registration is a provincial or territorial responsibility. However, the design and construction of safe roads and vehicles are regulated by the federal government. You can drive across the country with your provincial or territorial drivers' license and with the knowledge that the roads and vehicles are safe regardless of where you are in the country.

Like our transportation system, *Identity federation* applies these same principles. You can present your identity information, prove your identity and receive credentials from the province or territory where you reside knowing that this trusted identity can be used across other jurisdictions. Your trusted identity, when used online ensures safe and secure access to online services across the Pan-Canadian identity federation.

[8] Eugene Forsey, How Canadians Govern Themselves, 7th Edition 2010 http://www2.parl.gc.ca/sites/lop/aboutparliament/forsey/PDFs/How_Canadians_Govern_Themselves-7ed.pdf

Figure 1 illustrates a consensus of the IMSC members of what is required for a Pan-Canadian approach to trusting identities. Central to this approach is *identity federation.* The model illustrated in this figure is consistent with identity federation models being developed and adopted by other countries and industry[9].

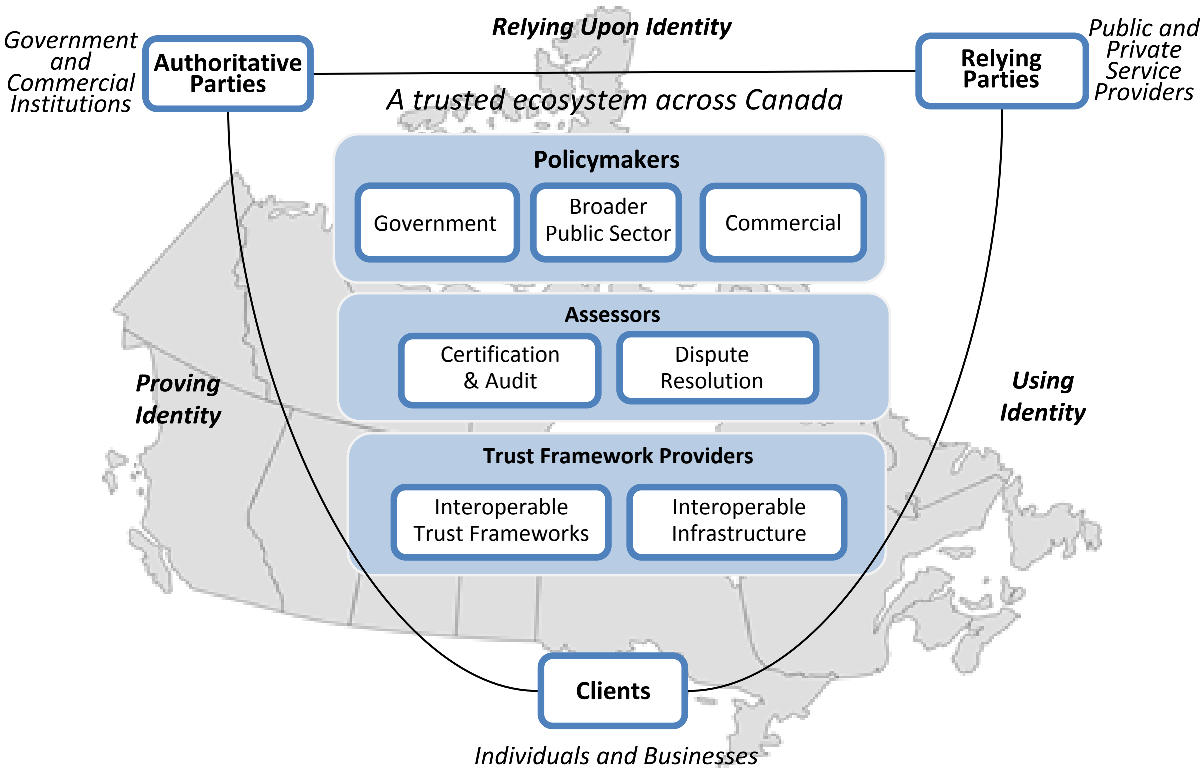
Government and Commercial Institutions
Authoritative Parties
Relying Upon Identity
A trusted ecosystem across Canada
Relying Parties
Public and Private Service Providers
Policymakers
Government
Broader Public Sector
Commercial
Assessors
Certification & Audit
Dispute Resolution
Trust Framework Providers
Interoperable Trust Frameworks
Interoperable Infrastructure
Proving Identity
Using Identity
Clients
Individuals and Businesses

Figure 1: Pan-Canadian Identity Federation Model

The Pan-Canadian approach is based upon the **Pan-Canadian Identity Federation Model** illustrated in Figure 1. This figure illustrates the main elements of what is required for a trusted ecosystem across Canada for services and transactions involving identity information.

Key Stakeholders

There are three key stakeholders (or parties) who benefit from the Pan-Canadian Identity Federation: **Clients**, **Authoritative Parties** and **Relying Parties**. The justification of a Pan-Canadian Identity Federation, including its long-term viability and success depends upon the full participation of these three key stakeholders.

[9] This includes models being developed by Kantara Initiative, American Bar Association, and the Open Identity Exchange

A **Client** is an individual or business that needs to access a service where identity is required (e.g., applying for a social benefit or a business license). An identity federation is beneficial to a client, because they can conveniently access a wide array of services without having to repeatedly prove their identity or manage a confusing mix of multiple credentials and easily-forgotten passwords. Clients, as stakeholders, expect that their privacy is protected, their identity information is secure, and they retain choice in the manner that they wish to access services.

An **Authoritative Party** is a government department or commercial organization (e.g., a bank) that is responsible for proving the identity of an individual or business, or maintaining an authoritative identity source that can be relied upon. Depending upon the business context, these departments and organizations may also issue credentials ranging from physical documents, such as a passports containing identity information to anonymous online credentials having no identity information. Presently, this wide variety of credentials are re-used and relied upon by individuals and organizations in a non-systematic fashion introducing significant vulnerabilities into the implicit system of trust that exists today. An identity federation is beneficial to an authoritative party because it introduces a systematic and accountable system of trust that allows an organization to transform its current identity and credentialing processes into formalized services for use by clients and other organizations. Authoritative parties, as stakeholders, expect that the identity information is used for the purposes for which it is provided, that there are viable economic models for providing services and that there are formalized frameworks to deal with issues such as risks and liabilities.

A **Relying Party** is an organization that provides a service to the client where the use of identity is required. In the majority of cases, a service provider is considered a relying party because it relies upon identity information that was established and verified elsewhere. The service provider also relies upon evidence that it is in fact the right client using their own identity information, and not someone else's. An identity federation is beneficial to a relying party (or service provider), because they no longer need to develop their own identity-proofing, credential management and authentication processes. Instead, they can use or *rely upon* an authoritative party that is better equipped to carry out these processes. Relying parties, as stakeholders, expect that the identity information is accurate, is being rightfully used, and that there are proper mechanisms in place for certification, audit and dispute resolution.

Key Trust Requirements

The Pan-Canadian Identity Federation, to be beneficial to all stakeholders, must fulfill three key trust requirements. These trust requirements, illustrated in Figure 1 as lines between the key participants are: 1) *Proving identity*, 2) *Using identity*, and 3) *Relying upon identity*.

Requirement 1: Proving Identity.

Clients (individuals and businesses) must be able to conveniently *prove their identity* once through an authoritative party in a manner that it can be readily trusted across the federation. When asked the question *"Who are you?",* clients must be able to securely provide identity information that once verified to a specific level of assurance, is trusted at this same level of assurance across the different channels (online, in-person, telephone, and mail) and across the different jurisdictions and sectors.

Requirement 2: Using Identity.

A client must be able to *use their identity* with many relying parties (i.e. service providers) in a manner that they can trust across the different channels and across the different jurisdictions. The trustworthy use of identity information (i.e., not being used by a fraudster) such as name, date-of-birth, etc. is assured by answering the question "Is it you?" This is achieved in the online world by means of an electronic credential (e.g., username and password/PIN) or in conjunction with a physical token (e.g., USB key). In the physical world, the trustworthy use of identity is achieved through the visual inspection of secure documents, and, in the channels of telephone and mail, access codes, caller-id, or verbal question-and-answers are used.

Requirement 3: Relying Upon Identity.

Service providers must be able to *rely upon identity*, in other words, they must be able to trust the accuracy of identity information from an authoritative party and that this information is being rightfully used by a client. This trustworthiness must be realized across jurisdictions and regardless of channel used. When the two questions are satisfactorily answered: *"Who are you?"* and, *"Is it you?"* the service provider can then focus on improving service instead of worrying if they are dealing with the right client.

Key Roles and Responsibilities

There are key roles and responsibilities that must be carried out to ensure the long-term success and sustainability of the Pan-Canadian Identity Federation. These roles and responsibilities are illustrated in the centre of Figure 1 representing what must be carried out to serve the collective interest of all participants, through an appropriate governance structure. These are the **Policymakers**, **Assessors**, and **Trust Framework Providers** that govern, assess or operate the federation. These roles and responsibilities may exist within one organization or across several organizations working together.

Policymakers

Policymakers are the organizations that define the rules by which trust frameworks are adopted, used and certified. Policymakers (or governance authorities) represent the communities of trust involved (e.g. public sector, broader public sector or commercial) which may be subject to specific legislation or legal/contractual frameworks. There may also be multiple independent policymakers that have decided to collaborate with one another (e.g. Federal/Provincial/Territorial governments, Canadian Payments Association, Interac, Canadian Council of Motor Transport Administrators, etc.). In this case, there may be requirements to harmonize standards and frameworks, and to establish umbrella agreements between policymakers, such as different jurisdictions (this is also referred to as inter-federation).

Assessors

Assessors are organizations or individuals that have been appointed to independently assess, validate and certify that member organizations are in compliance to the rules adopted by the policymakers of the trust framework. Assessors are responsible for carrying out *Certification and Audit* processes and may also be responsible for managing *Dispute Resolution* processes.

Trust Framework Providers

Trust Framework Providers are organizations that support and maintain the trust framework(s) adopted by the federation. Trust Framework Provider(s) manage the day-to-day business of running the federation, such as managing federation membership and agreements, compliance reporting, etc. Trust framework providers may be also responsible for ensuring interoperability between the adopted *Trust Frameworks* and accredited *Infrastructures* used by the federation. Examples of trust frameworks include the Kantara Identity Assurance Framework and the Open Identity Exchange. Examples of infrastructures include the Interac, Visa, or MasterCard networks.

Guiding Principles

The Pan-Canadian strategy for trusting identities is based upon the guiding principles established by the 2007 Task Force. These guiding principles remain valid today. However, for the purpose of this strategy these principles have been re-stated to emphasize the norms that will guide what is required to *govern the trusting of identities* across the Pan-Canadian context. These principles form the foundation upon which identities will be trusted across jurisdictions while adhering to the values of Canadians.

Principle 1: Interoperable, Cost-Effective and Innovative

Canada's approach should be interoperable. Trusted identities and exchange of identity information should be easily accepted across different jurisdictions, through multiple channels (online, in-person, telephone, mail), and enabled by multiple systems supporting a diverse array of services. Provinces, territories, municipalities, and the federal government should be able to benefit by leveraging existing processes involving identity verification, authentication, registration and enrolment between jurisdictions. The interoperable approach should also support the evolution towards a national infrastructure that is extensible to the broader public sector, the private sector, and other countries seeking similar benefits.

Canada's approach should also be cost-effective and innovative. By setting the right conditions to encourage a competitive and innovative marketplace, Canada can benefit from solutions built using standardized components provided by a competitive industry. These solutions should be built in proportion to the risks involved using appropriate methods and technologies. In addition, through streamlining procurement processes cost savings can be achieved.

Principle 2: Easy to Use, Client-Focused and Voluntary.

Clients should be able to easily use their trusted identities online by means of a simple, consistent and intuitive experience across programs and jurisdictions. While other channels will remain as available options, if the online approach is easiest to use, it will become the preferred method for clients in how they transact with government.

Canada's approach should consider the client as being central to all transactions where identity must be trusted online. This is referred to as a 'client-focused' approach that respects the needs, capabilities and preferences of clients. This approach includes the transfer of identity information controlled by the client and enables informed explicit consent when this information is requested by authoritative or relying parties. It also enables clients to revoke consent at a later date.

Voluntary participation means that the client should have choice whether they will participate or not. If clients decide not to participate, they should have the option to request services through alternative channels. If clients decide to participate they should have choice in the organization they choose to provide their identity information (the authoritative party) to the organization that uses the identity information (the relying party).

Principle 3: Safe, Secure and Privacy Enhancing.

Canada's approach should be safe, secure and privacy enhancing. First and foremost, it should be safe for all clients so that they can protect themselves against potential abuses, such as identity fraud. Safety also means limiting exposure to unacceptable or illegal activities such as cyber-bullying, surveillance and unwanted solicitation (e.g. spam).

Canada's approach should also be secure. This means providing clients with secure access to the wide range of available services. It also means that clients have the ability to confirm the authenticity of other participants (authoritative parties and relying parties) which is crucial when clients are accessing services remotely. They need to assure themselves that they are accessing the right website or speaking to an authorized representative**.** Finally, it means that jurisdictions must protect personal and identity information using secure mechanisms that are adaptable to the continually evolving threat environment.

Canada's approach should be privacy enhancing. Canadians demand that programs and services respect their right to privacy and preserve their ability to retain choice and consent in the manner that they choose to conduct their affairs on-line. This means that privacy should be considered proactively, as an essential component of any design, as the default mode of operation, and respecting the rights of the client[10]

Principle 4: Accountable and Transparent.
Canada's approach should be accountable and transparent. Trust is realized and maintained when citizens are confident that their governments are being accountable and transparent with respect to activities that involve their identity, including situations of dispute, redress and resolution.

Canada's approach will ensure that organizations in a position of trust regarding identity are justified by legislation, subject to clear governance holding organizations to account for duties and obligations related to identity. The use of trusted identities by a jurisdiction, department, program or service must be linked to mandates, strategic outcomes, policies or program requirements and be clearly communicated to clients.

Key Goals of the Pan-Canadian Approach

The Pan-Canadian approach to trusting identities online defines four key goals. These goals, in conjunction with the guiding principles help prioritize the recommended action items.

Goal 1: Improve the service delivery environment.
Canada will continue to be a leader in the transition to online services in a way that supports economic growth and the shift to a digital society. Canada, at the outset of the 21st century, was recognized as an innovative leader in the creation of e-government and online service offerings. In 2010, Canada remained as one of the top five countries in the e-government

[10] 'Privacy by Design' may be found at the Office of Information and Privacy Commissioner website: http://www.ipc.on.ca/

development index according to the United Nations E-Government Survey[11]. As countries recover from the global economic crisis, and re-evaluate their priorities, Canada must continue to be a leader in online initiatives.

Achieving this outcome includes the following activities:

- Emphasizing that trusted identities is a critical component of the next phase in the evolution of safe online service delivery.
- Creating a strong yet flexible governance structure that represents Canada's collective interests and is responsive to the ever-changing global environment.
- Actively participating in national and international initiatives and collaborative efforts.

Goal 2: Preserve the trust and confidence of Canadians.

Canada and its governments will preserve the trust and confidence of Canadians as they transition to online services and transactions. Canadians value their rights and freedoms and demand the protection of their privacy and security. Since this transition represents a fundamental shift in the way that governments interact with their citizens, they must be receptive to the evolving needs of Canadians, the potential (positive and negative) impacts and unintended consequences. As Canadians move online, they expect their governments to provide them with the same rights and protections that they have the benefit of today. Achieving this outcome includes the following activities:

- Promoting public education and awareness and ensuring participation of all Canadians.
- Holding governments accountable by ensuring accountability and transparency.
- Ensuring ongoing relevance to what is important to Canadians, such as safety, security, privacy and accessibility

Goal 3: Create a harmonized, inclusive and interoperable framework of policies, standards and laws.

A truly Pan-Canadian approach will be achieved through the recognition of Canada's diversity and the full participation of all jurisdictions representing the wide array of needs and priorities of Canadians. There will be no single framework, policy, standard or law that can serve the Canadian population as a whole. Rather it will be a 'framework of frameworks' consisting of policies, standards and laws working together through political, business, and technological means.

[11] United Nations E-government Survey 2010, published by UN Department of Economic and Social Affairs

Achieving this outcome includes the following activities:

- Developing the appropriate governance structures and partnership arrangements that represent the diverse needs and interests of Canadian citizens, jurisdictions and communities (e.g. health, businesses, etc).
- Ensuring that all frameworks, policies and standards adopted contribute to an inclusive, harmonized and interoperable approach.
- Engaging all interested stakeholders to ensure that what is proposed is realistic, viable and makes good sense for Canadians over the long run.

Goal 4: Establish a Pan-Canadian technical infrastructure for trusted identity.
Canada will establish a technical infrastructure for trusted identities. This infrastructure is required to enable Canadians to securely and safely identify themselves and exchange identity information online regardless of where they live or work. This technical infrastructure for trusted identities would enable Canadians to receive services from all levels of governments and conduct business with confidence in each others' identity. This infrastructure would also enable industry to provide solutions to Canadians in new and innovative ways.

Achieving this outcome includes the following activities:

- Engaging industry to ensure the development of innovative and economically viable infrastructure.
- Providing support for and development of pilot projects and sharing the lessons learned.
- Acting as a catalyst and using government as a model user to support the development of new markets and business models that can use the trusted identity infrastructure in innovative ways.

Recommendations for Action

Four high-level actions are recommended. These recommended actions represent a consensus on what needs to be done, and will form the basis for follow-on efforts.

1. **Establish a Pan-Canadian Trusted Identities Forum that includes an expanded membership from the public sector, broader public sector and commercial organizations.**

   Since its inception in 2008, the IMSC has been a central focal point for identity management within the Canadian public sector. However, the management of identity is an issue that goes beyond the Canadian public sector and requires the inclusion of the broader public sector, the commercial sector and the international community. Building upon the IMSC work to date, the Pan-Canadian priorities are shifting towards elaborating what is required (business, legal, technical, etc.) to build the right solutions for Canadians. This shift requires a broader participation beyond the public sector. A **Pan-Canadian Trusted Identities Forum** should be established consisting of a membership that extends beyond the public sector. This forum should have the mandate to lead identity management from a Pan-Canadian perspective, carrying out the activities necessary to achieve the goals outlined in this paper. Examples of activities could include:

- Creating a mandate, governance structure, and determining the required authorities that serve Canada's collective interests and is responsive to the ever-changing global environment. This includes an expanded membership that represents the diverse needs and interests of Canadian citizens, jurisdictions and communities (e.g. health, businesses, etc).
- Ensuring that all frameworks, policies and standards adopted contribute to an inclusive, harmonized and interoperable approach. Identify and, if required, coordinate amendments to existing legislation or the introduction of new legislation.
- Overseeing the conception, design, implementation and evaluation of solutions that are intended to work across jurisdictions.
- Building the necessary capacity and actively participating in national and international initiatives and collaborative efforts.
- Engaging all interested stakeholders to ensure that what is proposed is realistic, viable and makes good sense for Canadians over the long run.
- Ensuring the protection of privacy for Canadians and ongoing relevance to what is important such as safety, security and accessibility.
- Recommending appropriate mechanisms of redress and dispute resolution.

2. **Facilitate wide-scale adoption.**

Wide-scale adoption is an outcome that is achieved through the combination of many factors, such as usability, cost-effectiveness, and ease of access for all Canadians. Wide-scale adoption also requires that favourable conditions are in place, particularly for authoritative and relying parties that may have legal liability concerned.

This action includes more detailed activities, such as:

- Developing a strategy to engage industry in order to ensure the development of innovative and economically viable infrastructure.

- Engaging industry to ensure that what is proposed is realistic, viable and will be trusted by Canadians over the long run.
- Ensuring ongoing relevance to what is important to Canadians, such as safety, security and accessibility.
- Acting as a catalyst and using government as a model user to support the development of new markets and business models that can use the trusted identity infrastructure in innovative ways.
- Identifying and addressing legal and liability concerns through contractual agreements or legal frameworks.

3. **Build a trusted identity infrastructure.**
   The vision, stated earlier in this paper, will only be realized if there is a solution - or many solutions - that can provide Canadians with simple, convenient and protected access to multi-jurisdictional services in a manner they choose and control.

   This action includes more detailed activities, such as:

   - Providing support for and development of pilot projects and sharing the lessons learned.
   - Create a forum to support the development of new markets and business models that can leverage the trusted identity infrastructure in innovative ways.
   - Develop an implementation plan that coordinates the rollout of services by the public and private sector.

4. **Develop an awareness and outreach program.**
   Canadians as end users must be aware of the Pan-Canadian approach to trusting identities online. This is required to preserve their trust and confidence in online services. This also includes understanding the benefits of participating in online services and how to safely and securely participate in online transactions.

   Detailed activities include:

   - Emphasizing that trusted identities is a critical component in the next phase in the evolution of safe online service delivery.
   - Promoting public education, awareness, and participation of all Canadians.
   - Developing a public education and awareness strategy to promote the concepts and help achieve participation of all Canadians.
   - Developing awareness material to ensure continued buy-in and support from private sector, other government entities, and political leadership.

Conclusion

The Pan-Canadian approach to trusting identities is the next step toward improving services for Canadians and enabling the evolution of service delivery. The existing patchwork of systems and credentials across different channels and jurisdictions will evolve to a more seamless user experience that is easier for clients to manage and more difficult for criminals to exploit.

To enable this seamless experience, this paper provides an approach for trusting identities within the Pan-Canadian context regardless where Canadians live, or how they conduct business with the government. This approach is the result of consensus between the jurisdictions and represents a starting point for the more detailed work to come.

This paper is the next step toward trusting identities across Canada. The Pan-Canadian approach, as proposed in this paper, will enable the trusting of identities across the boundaries of systems, services and jurisdictions resulting in better services for Canadians.

For Further Reading

Additional IMSC documents may be found at **Institute for Citizen-Centred Service web site:** http://www.iccs-isac.org/en/km/transformative/index.asp