Federating Identity Management in the Government of Canada: A Backgrounder

Federating Identity Management in the Government of Canada
A Backgrounder

Table of Contents

1. Executive summary
2. Introduction
   2.1 Background
   2.2 Purpose and scope
   2.3 Intended audience
3. Setting the context
   3.1 Federation today
   3.2 Need for a government-wide approach
   3.3 Thinking pan-Canadian
   3.4 Beyond Canada’s borders
4. The vision for the future
   4.1 Principles
   4.2 Benefits and risks
5. Strategy for moving forward
   5.1 Phased, incremental approach
   5.2 Policy and guidance
   5.3 Whole-of-government initiatives
   5.4 Federal, provincial, and territorial collaboration
6. Conclusion

Appendix A — Glossary
Appendix B — Recommended reading
Appendix C — References
Footnotes

1. Executive Summary
Identity is fundamental to Canadian society. It is the starting point of trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector charged with protecting the rights of citizens, ensuring privacy, and ensuring national security and public safety.

The scope of identity management is broad and affects many facets of the business of government. Given its horizontal nature, good identity management practices need to be pervasive and constantly applied to be effective. In light of identity's role as a key enabler of the business of government, it only makes sense that there be coherent identity management practices in place. Yet today within the federal government and across the provinces and territories there is no formalized basis for identity management. Without a framework, the goals of seamless and coordinated service delivery across jurisdictions and anywhere-anytime access while respecting privacy, legal, and security requirements may remain out of reach.

Federating identity management will permit trust, established by internal identity management business processes to be further extended across boundaries and enable government organizations to form trust relationships and optimally pursue interoperability goals that best align with their business model and IT policies, security, privacy goals, and requirements.

### The Vision

The vision for the future of Canada is that of a federation of organizations that trust each others' assurances of identity. The government of tomorrow will operate in an environment that supports the use of client-chosen credentials provided by multiple providers across multiple jurisdictions, through multiple service delivery channels, irrespective of the technology used. The result from the perspective of the client is convenient access to services that is secure and respects the individuals' privacy; and the result from the perspective of participating organizations is the maximization of resources and improved efficiencies. From the government-wide perspective, the results are reduced costs associated with program delivery, improved transparency, and increased client satisfaction.

While the initial focus is primarily on federating the identity management of external clients-individuals and businesses-the ultimate goal is to enable federation in support of internal clients-employees-as well.

### A phased, incremental approach is advocated

The first phase to federating identity management will be supported by the development of the next-generation online authentication services, specifically federating the management of credentials, which may contain identity attributes. In this first phase, any identity information that might be bound to a credential will not be assumed as valid or acceptable for identity-proofing purposes. The credential will essentially be treated as an anonymous credential that will allow clients to prove statements about themselves and their relationships with government organizations anonymously. The next logical phase will be to apply the lessons learned to federating identity.
The discipline of identity management will continue to evolve within the federal government, as will policy instruments to enable departments to better manage identity in support of achieving program outcomes. The timetable for realizing a federation of identity management will be influenced by priorities set within the pan Canadian arena and business pressures coming from within the Government of Canada.

By taking an incremental approach, the Government of Canada is not prescribing a solution but enabling government to respond to the changing identity landscape. This approach will enable the development of cost-effective solutions and encourage a competitive marketplace.

The Treasury Board of Canada Secretariat is working closely with federal departments and agencies as well as provincial and territorial partners to advance work on key elements required for federation. Initiatives underway include the following:

- Developing the Pan-Canadian Assurance Model in collaboration with federal, provincial, and territorial partners;
- Building trust through exploration of options for trust models;
- Federating technology-neutral credentials through the provision of central guidance and policy support for pathfinder projects to develop the next generation online authentication services; and
- Developing an Identity Assurance Model based on the model developed for federating credentials.

By approaching federation in a planned, incremental fashion, the Government of Canada believes that traction can be gained with minimal impediment. Effort will be required in order to understand how to formally interact with one another to respond to cultural, political, and legal challenges to federating identity.

2. Introduction

Three significant milestones were achieved in 2008. First, the launch of the Cyber-Authentication Renewal initiative, a federal interdepartmental activity aimed at defining a new government-wide framework to identify citizens and businesses that access government services over multiple delivery channels (in person, telephone, mail, and online). The initiative applied the work of the inter-jurisdictional Identity Management and Authentication Task Force (IATF) and expanded it through the development of a federated model of assurance that meets the needs of the Government of Canada. Also coming out of this work was the recommendation that the Government of Canada formalize and adopt a federated approach to authentication.1

Second, consensus was reached by the Federal-Provincial-Territorial (FPT) Deputy Ministers' Table on Service Delivery Collaboration to continue to develop the federated Pan-Canadian Identity Management and Authentication Framework. An inter-jurisdictional steering committee was established to oversee the completion of the framework started by the IATF, specifically the seven components: legal, privacy, security, identity, assurance, trust, and the identity service experience.

Third, the revised Policy on Government Security is undergoing the last stages of approvals. The policy will introduce a new Directive on Identity Management to address gaps and what will be needed to realize a federated approach to identity management. This is the first time within the Government of Canada that there will be a policy instrument to ensure coherent identity management practices. This will contribute to ensuring that privacy and security requirements are met and that services are developed, administered, and delivered to the right clients.
This report builds upon these successes and represents the continued evolution of thinking in the area of identity management and introduces the Government of Canada's approach to federating identity management.

### 2.1 Background

Identity is fundamental to Canadian society. It is the starting point of trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. Once an identity is established, all subsequent government activities-ranging from safeguarding assets to delivering services, benefits, and entitlements to responding to disasters and emergencies-rely upon this identity.

How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector charged with protecting the rights of citizens, ensuring privacy, and ensuring national security and public safety. It is also a concern of clients who want convenient access to government programs and services but not at the expense of the identity theft or privacy violation.

Significant work has been carried out within the federal government in the area of identity management with programs such as epass, Portageur, and development of an assurance model. Inter-jurisdictional work has produced the pan-Canadian identity management and authentication principles and initial framework, Canada Health Infoway’s electronic health records program, British Columbia's BCeID, Alberta's Alberta Secure Access Service, and Quebec's ClicSÉQR to name just a few.

The scope of identity management is broad and affects many facets of the business of government. Given its horizontal nature, good identity management practices need to be pervasive and constantly applied to be effective. In light of identity's role as a key enabler of the business of government, it only makes sense that there be coherent identity management practices in place. Yet today within the federal government and across the provinces and territories there is no formalized basis for identity management. Without a framework the goals of seamless and coordinated service delivery across jurisdictions and anywhere-anytime access while respecting privacy, legal, and security requirements may remain out of reach.

Through the provision of direction that makes identity management practices coherent across governments, organizations will have the ability to leverage each others’ identity management capabilities to better manage associated program costs and risks (e.g., sharing of costs, realizing efficiencies, and standardizing practices) while delivering improved interoperable services to clients.

### 2.2 Purpose and scope

The purpose of this report is to achieve the following:

- Introduce the concept of federation and how it could apply to identity management within the Government of Canada context;
- Present the phased, incremental approach advocated for moving forward with federating identity management; and
- Provide the starting point for government to collectively explore federation and to encourage dialogue on policy issues surrounding identity.

This report is a communications vehicle and the content presented herein is not intended as a replacement to standards and guidelines to support effective identity management. The scope of this report is limited to setting the context for the high level vision and approach for federating
Providing assurances of digital identities . . . is a complex public policy issue at the crossroads of information security, privacy and trust. Addressing it requires a comprehensive approach that would: blend the major

Identity management in the Government of Canada. While the initial focus is on secure delivery of e-government services to external clients-individuals and businesses-the intention is to evolve the vision to address federated identity management in all service delivery channels (in person, telephone, mail, and online) and to address internal clients-employees.

Identity establishment, identity-proofing, identity information sharing, access management, and internal credential management are topics of significant importance that will need to be discussed as the Government of Canada moves forward with federating identity management. They are, however, outside the scope of this report.

2.3 Intended audience

The primary audience for this report is decision makers in the Government of Canada. Other stakeholders who may have an interest in this report include the following:

- Government departments and agencies that provide common and shared products and services, deliver programs and services to Canadians, safeguard national security, and ensure public safety;
- Government policy makers; and
- Other Canadian jurisdictions that are addressing identity management through a government-wide approach, especially those involved in the creation and use of identities.

3. Setting the context

3.1 Federation today

The practice of federated identity management exists today. The Government of Canada intends to formalize the way in which trust arrangements are shaped and make explicit the accountabilities for shared assurances of credentials or identity through its policies and standards.

Presently, some programs use credentials issued by other programs as proof of identity (e.g., driver's licence, passport, Social Insurance Number); however, arrangements may be based on implicit trust, or in some cases, convenience. This approach is not scalable today and cannot support the goal of cross-jurisdictional and interoperable service delivery to clients.

Going forward, good examples of the federation of identity management within communities of governmental responsibility-such as policing, food safety, health and education-can be leveraged for lessons learned that can be applied across government.

3.2 Need for a government-wide approach

Today, different identity management practices across the Government of Canada and other jurisdictions may increase the risks of fraudulent use of identity documents, identity theft, improper granting of entitlements, benefits leakage, financial losses to individuals and governments, and invasion of privacy. Without a coherent, consistent, standardized, and interoperable approach for dealing with identity across the federal government and other jurisdictions, successful risk mitigation strategies are
increasingly difficult to develop and implement in order to manage challenges to national security while respecting privacy, program integrity, and the delivery of citizen-centred services.

Key drivers for adopting a coherent, whole-of-government approach to identity management include the following:

- **Client expectations**—Clients want convenience in accessing government programs and services, and that generally translates into asking for and providing personal information only once or at least only when necessary; they also expect a reliable, consistent user experience across all programs and services regardless of jurisdiction.\(^2\)

- **Security** — The desire to provide better service to clients is challenged by an evolving and increasingly sophisticated threat environment that requires proactive protection strategies.

- **Privacy** — Canada's socio-cultural environment (protected legislatively) places a high value on privacy. Clients are concerned about their privacy and how their personal information is used, especially with regard to the disclosure of their personal information.

- **Service delivery** — Clients expect transparency in service delivery and cost effective public services; as a result, programs are constantly challenged to deliver more and better services in a cost-efficient manner; and

- **Technology** — Adoption of new technologies and migration from traditionally siloed functions to common and shared services is driving the need for a common approach to managing identity to best achieve outcomes.

### 3.3 Thinking pan-Canadian

Federal programs that rely on evidence of identity from other jurisdictions (provinces and territories) or international bodies often incur increased risk resulting from diffusion of responsibilities and lack of clarity around identity management practices. A pan-Canadian approach to federation can amalgamate the efforts underway at all levels of government, allowing for the development of an approach that spans departmental, agency, and jurisdictional boundaries. This supports the goals of seamless and coordinated service delivery across jurisdictions and anywhere-anytime access while respecting privacy, legal, and security requirements.

The Government of Canada is working closely with the provinces and territories to extend the federally developed assurance model to a pan-Canadian model. This is discussed in more detail in Section 5.4.

### 3.4 Beyond Canada's borders

Industry watchers like the Gartner and Burton Group report a growing demand for federation across several vertical industries, with multiple enterprises federating with many partner organizations. Federations are emerging outside the typical industries such as telecom; organizations publicly talking up their federation projects include American Express, Boeing, Harvard University, Hewlett-Packard and Phillips.

International governments have also made significant federation investments in recent years. The United States’ E-Gov program and the E-Authentication initiative (the federation portion)
Identity federation is established federation as a strategic goal. Federation is also viewed as a key approach for e-government activities in Denmark, Finland, the Netherlands, Norway, the United Kingdom, New Zealand, Australia, and many European countries.

While other governments are adopting a federated approach to identity management, their solutions may not be directly portable to the Canadian context. It will be important to learn from what others are doing, adopt the best practices where appropriate and ensure the things that are important to Canada are properly expressed in the ultimate solution. Equally important will be ensuring that Canada's approach aligns with those in other countries to support the business of government that extends beyond sovereign borders.

4. The vision for the future

The vision for the future of Canada is that of a federation of organizations who trust each others' assurances of identity. The government of tomorrow will operate in an environment that supports the use of client-chosen credentials provided by multiple providers across multiple jurisdictions, through multiple service delivery channels, irrespective of the technology used. The result from the perspective of the client is convenient access to services that is secure and respects the individuals' privacy; and the result from the perspective of participating organizations is the maximization of resources and improved efficiencies. From the government-wide perspective, the results are reduced costs associated with program delivery, improved transparency, and increased client satisfaction.

Underpinning the above scenario are trust relationships and governance that enable government organizations to optimally pursue interoperability goals that best align with their respective business models and information technology policies, security, privacy goals, and requirements.

While the initial focus is primarily on federating the identity management of external clients—individuals and businesses—the ultimate goal is to enable federation to support internal clients—employees—as well.

The following elements are considered foundational for federating identity management.

**Assurance**

When establishing an identity, government departments must ensure that they are dealing with the intended client. They do this by taking into account risk and making decisions about the authenticity of the individual, business, or device with the result being an assurance of credential or identity. Within the concept of federation, this assurance is something of value that members of the federation can share with one another.

**Trust**

The formalization of identity management practices (including those resulting in assurances of credential or identity) across governments increases trust among government entities. Trust in each others' identity management practices allows the provision (or sharing) of assurances of credential or identity across the boundaries of programs, departments, and jurisdictions. This provides governments an opportunity to leverage each others' identity management capabilities to better manage associated program costs and risks (e.g., sharing of costs and realizing efficiencies standardizing practices) while delivering improved services.

Trust relationships between all members of the federation may be supported by standards and technologies that...
accomplished when trust is transferred from one organization to another.

—"Protecting and Managing Digital Identities Online"; Updated Issues Paper—February 2009, Electronic Commerce Branch, Industry Canada

Risk management

Central to the Government of Canada's approach to federated identity management is the recognition that program owners are accountable for achieving their program mandates. This includes the responsibility to authenticate the identity of clients for program delivery purposes. The selection of the appropriate assurance level for a trusted transaction is done on a risk management basis by the business owner with accountability consequences.

Shared assurances of credential or identity could enable members of the federation to share risk, thus reducing the overall costs associated with managing risk individually. This approach to risk management is aligned with the federal governments' integrated risk management process.

Federation roles

Federation members are autonomous entities that have become members of the federation. They can be individual departments, agencies, or jurisdictions that have decided to become members of the federation. Members assume one or more of these roles within the federation:

- A principal is an entity that initiates an interaction or is subject to an outcome. The principal is typically an individual who is providing evidence of a claim or requesting a service.
- An authoritative party is a federation member who provides assurances (of credential or identity) to other parties.
- A relying party is a federation member who accepts assurances (of credential or identity) from another member (the authoritative party).

The above list of key elements is not viewed as finite. It will be built upon as progress is made, and it is likely that governance, common standards, and certification and accreditation may be required to operationalize and sustain the federation.

4.1 Principles

The following principles will guide the development of the federation model for identity management:

- Achieve consensus through accepted, mutually respected assurances (of credential or identity), risk levels, and accountabilities;
- Respect program accountability—programs maintain the responsibility (and accountability) for ensuring they are dealing with the intended client in accordance with their mandate;
- Let the citizen decide—clients are provided with choices regarding which identity credentials to use to access government services which are recognized throughout the federation;
- Enable interoperability—provide direction to assist departments in implementing trusted identity management practices that support the sharing of assurances of credential or identity; and
- Promote a fair and competitive marketplace—maintain neutrality with respect to
technologies and solutions and allow multiple providers to be part of the federation. This allows for the possibility of choice and competition.

The above complement the identity principles articulated in the July 2007 IATF report, *A Pan-Canadian Strategy for Identity Management and Authentication*. As work progresses, the principles outlined above will be refined and, potentially, new ones defined.

### 4.2 Benefits and risks

There are benefits associated with federating identity management when each program does not have to repeat its own set of authentication and identity proofing mechanisms. Gartner identifies the following benefits that could be realized through federation:

- A way to join up disparate identity silos;
- A way to abstract authentication architecture differences;
- Reduced identity administration costs; and
- Improved client experience (e.g., increased user convenience through reduced sign-on).

While the benefits are typically described from the perspective of cyber authentication—the authentication of a client using an electronic credential—the vision for federating identity management is broader than electronic authentication. The concept of federation is equally applicable to managing the identity of businesses, organizations, employees of the government, and devices to which identity management practices apply. Additionally, it is applicable not only for the online channel for service delivery to clients but across all service delivery channels (online, in-person, telephone, and mail).

Federating identity management may create new risks for programs and organizations, e.g., reliance on another party for identity claims, forensics and record retention that must now span organizational boundaries, and trust failures that could proliferate, making cross-over attacks possible. According to the Burton Group, however, federated identity management can reduce other risks, such as the following:

- Accountability for identity management remains with the appropriate party;
- High-security domains can be autonomous but still interoperate; and
- Reliance on a large-scale, centralized security infrastructure is lessened (this shifts complexity).

The Government of Canada recognizes that significant work will be required in areas such as the following:

- Understanding the cultural, political, legal, and privacy concerns associated with federation;
- Establishing the governance and elements of trust necessary for federation; and
- Ensuring balance is achieved between the standards that are required and the relative independence of the participating members.

### 5. Strategy for moving forward

#### 5.1 Phased, incremental approach

The Government of Canada's position on federating identity management is not about prescribing a solution; rather it is founded on defining a few but appropriate instruments that focus on achieving results and outcomes. The proposed approach to federating identity
management aligns and supports security, privacy, information management, and service transformation outcomes, as well as, identity management initiatives within the federal government. A phased approach to implementation is advocated.

Figure 1: Phased, incremental approach to realizing a whole-of-government federation of identity management

The first phase to federating identity management will be supported by the development of the next-generation online authentication services, specifically federating the management of technology neutral credentials, which may contain identity attributes. In this first phase, any identity information that might be bound to a credential will not be assumed as valid or acceptable for identity-proofing purposes. The credential will essentially be treated as an anonymous credential that will allow clients to prove statements about themselves and their relationships with government organizations anonymously. The next logical phase will be to apply the lessons learned to federating identity. The discipline of identity management will continue to evolve within the federal government, as will policy instruments to enable departments to better manage identity in support of achieving program outcomes.

By taking an incremental approach, the Government of Canada is not prescribing a solution but enabling government to respond to the changing identity landscape. This approach will enable development of cost-effective solutions and encourage a competitive marketplace. Applying a less prescriptive approach will position the government to take advantage of future innovations while providing the opportunity to better understand and assess where the market place is going with respect to identity management, specifically the binding of identity and credential.
The timetable for realizing federation of identity management will be influenced by priorities set within the pan-Canadian arena and business pressures coming from within the Government of Canada. Progress must be swift enough to benefit from opportunities to achieve quick hits such as the federation of an anonymous credential (an opportunity to pilot federation) through the development of the next-generation online authentication services but gradual enough to allow for lessons learned to be applied and tools to affect coherency and evolution in identity management practices to have an effect.

5.2 Policy and guidance

The Directive on Identity Management, under the revised Policy on Government Security, will support the management of business processes related to identity information and will support interoperability by ensuring that consistent direction and guidance is prescribed around identity management practices. The directive will provide the foundation for developing mandatory instruments to provide departments with a coherent, consistent, standardized, and interoperable approach for identity management across the federal government. It will provide the appropriate direction to assist departments in reducing the risks of fraudulent use of identity documents, improper granting of entitlements, benefits leakage, financial losses to individuals and governments, and invasions of privacy. The directive will enable departments to better manage their business risks while meeting the challenges of national security, respect for privacy, program integrity, and service delivery.

5.3 Whole-of-government initiatives

There is significant work to be done to understand how to best federate identity management. The Treasury Board of Canada Secretariat (TBS) has been working closely with federal departments and agencies as well as provincial and territorial partners to advance this understanding, specifically in the area of key components or elements required for federation-assurance, trust, governance, and risk management. Some government-wide initiatives are described below.

5.3.1 Developing the pan-Canadian assurance model

The Government of Canada has developed an assurance model to enable departments and agencies to federate identity by assessing risks and making key authentication decisions that take into account risk, cost, and simplicity of client experience. The Government of Canada model also permits different options for authentication and supporting technologies and makes a clear distinction between the assurance of credential and the assurance of identity. Assurance of credential concerns the binding of a credential to a person (without regard to their identity). Assurance of identity concerns the claim that the individual is really who they say they are. Both assurances are necessary for a sound authentication solution.

Key aspects of the Government of Canada's new approach to authentication include a provision for multiple assurance levels commensurate with risk, standardized components and interfaces to be used as building blocks for authentication solutions, and a seamless interface for clients when they transact with Government of Canada programs and services. This model was created so that it can be applied across all service delivery channels and be extended to cover assurance of identity at a later stage. The current model covers assurance of the credential only, leaving the assurance of identity to the program to establish.

A pan-Canadian assurance model is the next step in developing a consistent assessment and decision framework that enables different jurisdictions to rely upon (i.e., trust) one another's assurances of identity and credentials as part of a federated arrangement. Central to the model is the recognition that the concept of assurance is critical to formalizing federated arrangements.
and is a necessary component to managing risk across the boundaries within the federation. To this end, the Government of Canada is working with federal, provincial, and territorial stakeholders to broaden the federally developed assurance model to a pan-Canadian model for assurance that will enable multiple credential providers and acceptance of credentials from other authoritative parties (federal government, provincial, and territorial governments, municipalities, commercial partners).

5.3.2 Building trust

Addressing trust is critical to federating identity management and achieving the cross-jurisdictional, interoperable government of the future. Evident in all the work to date is the reliance on trust as the underlying mechanism that will support the entire federated identity management network. Trust will need to be examined from various perspectives, including trends, best practices, and methods in international and private sectors, and related industries (i.e., financial and insurance) requirements, challenges, and how to apply best practices to the establishment of trust within the Canadian context as the foundation for federating identity management. Preliminary work is underway to explore options for trust models.

5.3.3 Federating credential management

The pan-Canadian assurance model is the basis on which trust in one another's assurances of credentials will be established and facilitates the federating of credentials, not only within the federal government but also across government jurisdictions. In the first phase, efforts to federate credentials will be supported by the development of the next-generation online authentication services with the result that members (of the federation) can share assurances of a credential with other trusted members of the federation. In this first phase, any identity information that might be bound to a credential will not be assumed as valid or acceptable for identity-proofing purposes. The credential will essentially be treated as an anonymous credential that will allow clients to prove statements about themselves and their relationships with government organizations anonymously.

At present, it is not general practice to share identity information outside of what is stipulated in program or jurisdictional mandates. The alternative is an anonymous credential, which is something that can be shared now with minimal privacy and legislative issues. Additionally, the clear separation of identity and credential serves the full spectrum of services. It enables transactions where the identity of the client is not essential to the transaction being carried out (e.g., census-taking) and leaves the accountability for identity assurance in the program space. Gartner states, "The separation takes into account that identity-proofing and credential services may be provided by the same or independent entities." This decision will enable progress within the existing legislative framework and allow the Government of Canada to benefit from a competitive marketplace where multiple credential providers could offer credentialing services.

5.3.4 Developing an identity assurance model

The assurance model established by the Cyber-Authentication Renewal Initiative (e.g., levels of assurance) will be leveraged and extended to address requirements as they relate to federating identity between organizations or jurisdictions. Work is underway to provide a more specific instance of the assurance model as it applies to identity within the Government of Canada and will lay the foundation for federating identity.

5.4 Federal, provincial, and territorial collaboration

The Government of Canada will continue to foster collaborative relationships within the federal
government and between the provincial, territorial, and municipal governments. The Secretariat and Service Canada are representing the federal government on the inter-jurisdictional Identity Management Steering Committee (IMSC) that reports to the FPT Deputy Ministers' Table on Service Delivery Collaboration. The IMSC is charged with overseeing the development of the pan-Canadian framework and standards for identity management, providing guidance to its working groups, and encouraging adoption of framework and standards across all jurisdictions.

Additionally, the federal government is working closely with the Joint Councils (Public Sector CIO Council and the Public Sector Service Delivery Council) and their associated sub-committees and working groups to strengthen inter-jurisdictional cooperation and leverage lessons learned and best practices with respect to managing identity. The federal government is also active on a number of national and international organizations focussed on identity management.

6. Conclusion

Federating identity management will permit trust, established by internal identity management business processes, to be further extended across boundaries and enable government organizations to form trust relationships and optimally pursue interoperability goals that best align with their business model and IT policies, security, privacy goals, and requirements. This is the direction other governments, countries, and industry are heading to address identity. It will be important to understand what federation means within the Canadian context, and this report is a first step to building a common understanding of the concept of federation and how it could apply to identity management within the context of the Government of Canada.

There is significant work to build on, such as the inter-jurisdictional work by the IATF, IMSC, and with the federal government the results of the Cyber Authentication Renewal Project, which, through extensive consultations, produced an assurance model. That model is now being extended to pan-Canadian application through FPT collaboration. As well, the introduction of a Directive on Identity Management will provide the foundation for developing mandatory instruments to provide departments with a coherent, consistent, standardized, and interoperable approach for identity management across the federal government.

A phased, incremental approach is advocated for moving forward with federating identity, and an opportunity exists to pilot federation. The proposed starting point is to learn how to federate with something simple and well understood—the anonymous credential. The first phase is to federate credential management and work is underway within the federal government with pathfinder projects that will pursue solutions for the next-generation online authentication services as part of the development of a government-wide strategy for federation. Once the trust relationships needed to make it work are in place and well understood, the next logical step is to apply that understanding to federating identity.

Traction can be gained with minimal impediment by approaching federation in a planned, incremental fashion. Effort will be required in order to understand how to formally interact with one another to respond to cultural, political, and legal challenges to federating identity.

Appendix A — Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Anonymous credential</td>
<td>Refers to a credential that, while still making an assertion about some property, status, or right of the client does not reveal the client's identity. A credential may contain identity attributes but still be treated as anonymous if the identity attributes are not recognized or used for identity validation purposes. Anonymous credentials provide clients with a means by which to prove statements about themselves and their relationships with public and private organizations anonymously.</td>
</tr>
<tr>
<td>Assurance</td>
<td>A measure of certainty that a statement or fact is true.</td>
</tr>
<tr>
<td>Assurance of credential</td>
<td>Concerns the binding of a credential to a person (without regard to their identity).</td>
</tr>
<tr>
<td>Assurance of identity</td>
<td>Concerns the claim that the individual is really who they say they are. Both assurances are necessary for a sound authentication solution.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of establishing truth or genuineness to generate an assurance (of credential or identity).</td>
</tr>
<tr>
<td>Client</td>
<td>The intended recipient for a service output. External clients are generally individuals (Canadian citizens, permanent residents, etc.) and businesses (public and private sector organizations). Internal clients are generally public service employees and contractors.</td>
</tr>
<tr>
<td>Credential</td>
<td>A credential is a unique physical or electronic object (or identifier) that is issued to or associated with a client.</td>
</tr>
<tr>
<td>Federation</td>
<td>A cooperative agreement between autonomous entities that have committed to give up some of their autonomy in order to work effectively to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability.</td>
</tr>
<tr>
<td>Federating credentials</td>
<td>Is the process of establishing a federation in which members share assurances of credentials with trusted members of the federation.</td>
</tr>
<tr>
<td>Federated identity management</td>
<td>The sharing of assurances of identity with trusted partners (members) of the federation.</td>
</tr>
<tr>
<td>Identity</td>
<td>A reference or designation used to distinguish a unique and particular individual, organization, or device.</td>
</tr>
<tr>
<td>Identity claim</td>
<td>An assertion of the truth of something that pertains to a client's identity.</td>
</tr>
<tr>
<td>Identity federation</td>
<td>Is a group of autonomous entities that have established a community to manage their clients’ identity that is based on trust.</td>
</tr>
<tr>
<td>Identity management</td>
<td>The establishment, validation, and use of identity in trusted transactions with the government, supported by a set of principles, practices, and processes and procedures used to realize an organization's mandate and its objectives related to identity.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The ability of federal government departments to operate synergistically through consistent security and identity management practices.</td>
</tr>
<tr>
<td>Risk</td>
<td>The uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.</td>
</tr>
<tr>
<td>Trust</td>
<td>A firm belief in the reliability or truth or strength, etc. of a person or thing to place trust in, believe in, rely on the character or behaviour of.</td>
</tr>
</tbody>
</table>
Appendix B — Recommended reading

The following documents are recommended to the reader as further background on some of the foundation work on identity management and authentication that led to the development of this report and for further elaboration on some concepts mentioned, but not described, in this report, such as assurance levels:


Appendix C — References


Footnotes

The credential could be loosely bound to identity; however, in the first phase the identity information would not be recognized as such.