Pan-Canadian Assurance Model

Final Version

Assurance, Identity and Trust Working Group
March 3, 2010

Table of Contents

Document Revisions

The following table lists the major documents revisions produced and reviewed by the AIT Working Group.

Document Date	Revision Description	RDIMS #
January 30, 2009	Working Group Draft Prepared for IMSC-AIT In-Person Meeting February 5-6, 2009	721901-v1K
February 20 2009	Work-in-Progress Draft	721901-v3
March 6, 2009	Work-in-Progress Draft	721901-v4C
April 24, 2009	Work-in-Progress Draft	721901-v5G
May 4, 2009	Work-in-Progress Draft	721901-v6A
May 19, 2009	Work-in-Progress Draft	721901-v6A
June 2, 2009	Work-in-Progress Draft	721901-v8D
June 24, 2009	Draft for Consultation	721901-v9H
February 1, 2010	Final Version for Review and Approval by IMSC Working Group	831990-v3A
March 3, 2010	Final Version for Approval at IMSC Working Group Meeting, March 3rd 2010	831990-v4C

List of Figures

List of Tables

1 Executive Summary

Identity management is required for convenient, accessible and efficient service delivery across all channels and all levels of government in Canada. When necessary, governments must have assurances confirming the identity of an individual with whom they are dealing. To standardize the approach to identity management in Canada, the federal, provincial and territorial deputy ministers established the Identity Management Steering Committee (IMSC). IMSC's mandate is to oversee the completion of the Pan-Canadian Identity Management and Authentication framework and to encourage adoption of this framework among Canadian jurisdictions.

The framework is being developed to provide a seamless, cross-jurisdictional, user-centric, multi-channel service delivery experience for all Canadians. The framework has seven specific components that have been delegated to three working groups: Assurance, Identity and Trust (AIT); Legal, Privacy and Security (LPS); and Identity Service Experience (ISE). The AIT working group has been assigned responsibilities that include developing the Pan-Canadian Assurance and Pan-Canadian Trust models, both of which are integral to the Identity Management and Authentication framework.

The assurance model outlined in this report provides the foundation for agreement and interoperability between the federal government and the provinces by establishing levels of assurance, and identifying key concepts and definitions. The Pan-Canadian Assurance model is the first step in the long road to achieving an Identity Management and Authentication framework.

The Pan-Canadian Assurance model involves a three step assessment process which allows jurisdictions to manage risk related to identity and credential assurance, and to determine what their role in a federation would be. The first and second steps are designed to help jurisdictions determine what level of assurance is necessary for them to achieve their program objectives, and what methods, safeguards or measures need to be put in place to manage possible risks. If risks are considered manageable according to the assurance standards than the third step assesses which of three roles a jurisdiction would take within a federated model; whether it be a principal, authoritative or relying party. The assessment process makes practical use of the assurance standards to allow jurisdictions to develop an interoperable and inter-jurisdictional framework for identity management.

The Pan-Canadian Assurance model is an integral part in the development of Pan-Canadian Identity Management and Authentication framework. It will support better services for all citizens of Canada regardless of where they live or work. The model brings together significant elements from established assurance models from several jurisdictions within and outside Canada. It represents a harmonization of inter-jurisdictional standards that can be used by all orders of government for their programs, irrespective of technology or service delivery channel.

2 Acknowledgements

Identity Management Steering Committee (IMSC) would like to acknowledge the members of the Assurance, Identity and Trust (AIT) Working Group for their participation and contribution to this document.

AIT Working Group Co-Chairs:
Anne Bermonte (acting co-chair), Ontario
Pierre Boucher (co-chair), Government of Canada
Jeff Evans (co-chair), Ontario
Joanne Roy-Aubrey (acting co-chair), Government of Canada

AIT Working Group Members:
Ian Bailey, British Columbia
Chris Bookless, Yukon
Tim Bouma, Government of Canada
Michael Crerar, Alberta
Myriam Cyr, Quebec
Karyn Harrison, Government of Canada
Patrick Hoger, Manitoba
Charmaine Lowe, British Columbia
Connie Michaelas, Nova Scotia
Caroloann Moisse, Ontario
Carlos Mondesir, Ontario
Shannon Roe, Manitoba
Marion Rigby, New Brunswick
Diane Tucker, Manitoba

Additional Reviewers:
Murray Rosenthal, City of Toronto
George Warren, Nova Scotia

3 Introduction

The 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 the critical ingredient to formalizing federated arrangements and is a necessary component to managing risk across the boundaries within the federation. In general, an assurance conveys confidence between different parties and leads to trusted relationships. More specifically, identity assurance is a measure of trust and confidence conveyed between parties issuing credentials and parties requiring proof of identity.

The purpose of an assurance model is to set how much or how little trust and confidence is needed against various transactions. A *Pan-Canadian* Assurance Model extends that same trust and confidence for identity-based transactions between parties located in all participating provincial, federal and municipal jurisdictions.

In jurisdictions within and outside Canada, much work has already been done on assurance models, to the extent that many of the assurance model concepts are well established. To date, however, there has been no formalized harmonization of this work. The Pan-Canadian Assurance Model, developed by the Assurance, Identity and Trust (AIT) work group, brings together the significant elements of these models into a harmonized model that has been agreed upon by the group as one that could be used by all jurisdictions for their programs, irrespective of technology or channel.

3.1 Purpose

The purpose of this document is to articulate a model that can be used to agree upon a set of standards for the model to achieve maximum interoperability between jurisdictions. Accepting common tools and guidelines will be the last step before jurisdictions formally adopt the model by way of a formalized agreement. And in order to pave the way for jurisdictions to implement the model, jurisdictions would each address any legislative barriers to implementation within their jurisdiction. Work being done at this time by a legal work group is expected to offer direction in that area.

Illustrations of End State

A fully implemented Pan-Canadian Assurance Model means that:

a) *A client from Nova Scotia notifies Service Canada that she is moving to BC. Upon the client's consent, Service Canada provides BC with up-to-date identity and change of address information. BC issues health card and drivers licenses which are ready upon her arrival.*

b) *An Ontario resident takes a vacation in British Columbia. The individual is injured while skiing and is taken to a BC Hospital. The doctor signs on to the BC health record system with his/her digital credentials which have been authenticated by the BC Government. The Ontario government, as the relying party, allows the BC doctor access to the individual's Ontario health records.*

c) *A surviving spouse is required to provide death notification of a deceased spouse. The spouse confirms death notification information with the federal government, and requests that the death notification be provided to the provinces and territories in which they had previously resided.*

Note: End-state illustrations are not necessarily representative of services that would emerge, rather, they offer hypothetical scenarios of what would be possible at maturity, assuming full pan-Canadian membership

4 Scope

The Pan-Canadian Assurance Model has a number of characteristics that have been agreed upon by the cross-jurisdictional membership of the working group. Specifically the model:

1) Articulates an understanding across provincial, federal, territorial and municipal jurisdictions of what identity assurance is, and a common language to describe it;

2) Establishes information and process requirements to attain each level of identity assurance over different service delivery channels (e.g., in-person, over the telephone, online);

3) Formalizes the chain of trust across jurisdictions so that one jurisdiction may rely upon the assurance provided by another;

4) Demonstrates alignment or equivalency with national, international, and existing provincial identity assurance standards in order to maximize the potential for all members of the Pan-Canadian federation to connect to, and be trusted by, other identity management systems.

5) Ensures a common service experience for clients of services offered in the Pan-Canadian federation.

6) Includes definitions of key terms with an eye to the future, when the document may serve as reference material for other workgroups.

What the Pan-Canadian Assurance Model, *at this stage*, does not do is as follows:

- Prescribe a set of tools for implementation, although Section 8 of this document provides some guidance.

- Provide direction on architecture, software, telephony technology, or hardware.

5 Definition of Key Terms

This section lists the key terms and definitions that are central to the assurance model.

Assurance – A measure of certainty (level of confidence) that a statement or fact is true.

Assurance Level – A specific measure of certainty (level of confidence), which may be relied upon by others. An assurance level (or *level of assurance*) is standardized to four levels (1-4).

Assurance Level Requirement – A level of assurance required to achieve a program outcome, deliver a service output, or execute a transaction.

Authentication - The process of establishing truth or genuineness to generate an assurance.

Authentication Error – A specific error that occurs when the authentication process fails thereby yielding a false assurance. [1]

Authentication Factor-- A piece of information provided by a user during an authentication process. There are three categories of information: i) something known, ii) something owned or iii) something inherent (e.g. fingerprint)

Authentication Process – The business and/or IT process that determine whether something or someone is, in fact, who or what is declared to be. The failure of the authentication process results in an authentication error.

Authentication Requirement – The level of assurance that the authentication process must provide after considering other safeguards (or security measures) that exist in the system or business.

Compensating Factor – An additional safeguard measure employed during the authentication process that further prevents or reduces the possibility of an authentication error.

Credential - A unique physical or electronic object (or identifier) issued to, or associated with, a client.

Credential Assurance - The assurance that the client (i.e. individual or business) has maintained control over what has been entrusted to them (e.g. key, token, document, identifier, etc.) and that the credential has not been compromised (e.g. tampered with, modified, etc.).

[1] A 'false assurance' is similar to a 'false positive' or 'Type I error'. A false positive occurs when a test (i.e. authentication process) claims something to be positive (true), when if fact that is not the case.

Credential Authentication (Credential Validation) – The process of establishing confidence that the client has control over their rightful credential (i.e. not stolen), and that the credential (or information contained within) has not been compromised (i.e. not tampered with or modified).

Credential Authentication Error: A false assurance that enables an individual to use a credential not rightfully theirs.

Factor – A method or mechanism used to provide a piece of information. A factor may also be used to establish the truth or genuineness of the information being provided. Factors that are specific to user authentication are considered as **authentication factors** (there are three types: i) *something known*, ii) *something owned* or iii) *something inherent*.) Factors that are employed outside of the user authentication process (e.g. back-end verification processes) can be considered as additional factor types or as **compensating factors.**

Federation - A co-operative agreement between autonomous entities that have agreed to work together. The federation is supported by trust relationships and standards to support interoperability.

Identity – A reference or designation used to distinguish a unique and particular individual, organization or device.

Identity Assurance - The level of confidence that the client really is who they claim to be.

Identity Authentication (Identity Validation/Proofing) – The process of establishing confidence in the validity of a client's claimed identity. This authentication process generates a *level of identity assurance*.

Identity Authentication Error- A false assurance that enables an individual to claim an identity that is stolen or fictitious.

Initial Authentication – An authentication process when a client has had no prior relationship with the program or service.

Ongoing Authentication – An authentication process when a client has previously enrolled/registered and wishes to gain subsequent access to the program or service.

Risk – is the effect of uncertainty on objectives. An effect is a deviation from the expected and can be positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. [21]

Safeguard – A security control (IT or business processes) that exist within the overall system that reduces or mitigate risk.

Trust (noun) - A firm belief in the reliability or truth or strength etc. of a person or thing; (verb) to place trust in, believe in, rely on the character or behaviour of.

6 Assurance Model

This section contains the description of the assurance model

6.1 Model Overview

6.1.1 Key Goals Principles and Assumptions

Key Goals

a) The primary goal of the assurance model is to establish common definitions and requirements that can be used by government departments operating in different jurisdictions and at different levels, and by commercial organizations in some relationship with government.

b) Recognizing that users have different needs, constraints, and capacities, another goal of the assurance model is to balance uniformity with flexibility in its design.

Key Principles and Assumptions

Following are the key design principles of the assurance model:

- Is independent of technology
- Employs multiple assurance levels
- Distinguishes between different types of assurance.
- Can be applied within a federation, its external clients, individuals and businesses
- Consistent with established risk management approaches and methodologies
- Uses standardized elements (i.e. impact assessment profile) and non-standardized elements (i.e. compensating factors)
- Maintains privacy
- Maintains accountabilities
- Supports an integrated approach to different methods to service access and multi-channel adaptation

The subsequent application and use of the Pan-Canadian Assurance Model should be guided by the goals, principles and assumptions described above. Given the many jurisdictional, business or program contexts into which the model may be applied, it is impossible to account for all of the unique differences across the different contexts. However, it should be kept in the mind, that the model is a general starting point to further develop models that are specific to a context, or be used a reference point that enables a useful relationship between different models.

6.1.2 The Model's Foundation Concept: Assurance

The foundation of the assurance model is based upon the concept of *assurance*. By definition, an assurance is *the measure of certainty (level of confidence) that a statement or fact is true.* An assurance is intended to answer a simple question *"How sure you are you that you are correct?"* This answer becomes critically important when it involves matters where issues of uncertainty (the opposite of assurance) carry great risk.

An assurance, when properly produced is the outcome of a sound decision resulting from the best available evidence, the proper appreciation of potential impact and its likelihood, and the appropriate level of oversight when a decision is made. Further, when an assurance (based on a sound decision) is shared between two or more parties (people, or organizations), it leads to a trusted relationship and mutual confidence. Over time this trust and mutual confidence, as it broadens to more parties becomes the essential thread that brings about a federation.

An assurance may also have a time-dependent aspect. A *static assurance* assumes that nothing changes over time (the assurance is always valid), while a *dynamic assurance* has a period of validity associated with it. Depending upon the circumstances, the period of validity may range from minutes to years. For example, an *identity assurance*, resulting from an identity-proofing process may be valid for five (5) years. In contrast, a *credential assurance* may expire after its first use (e.g. a single-use credential), which may have a validity period of only a few minutes. In all cases, an assurance should have an associated time-period of validity, during which it can be trusted.

6.1.3 Assurance and Identity

The assurance model links assurance with identity[2]. The reason is simple - the uncertainty of identity poses a great risk for the vast majority of organizations. Without the certainty of identity (i.e. assurance of the identity), the risks of providing benefits, services, and information to the wrong person could have significant and adverse impacts. Reducing and eliminating these identity-related impacts is especially crucial for public sector organizations because they can potentially undermine public trust in government as a whole. For this very reason, identity is at the heart of public administration and is at the core of most government business processes.

Identity has become a critical underpinning of many strategic government initiatives and programs, including online service delivery, integrated case management and improved information sharing. Identity is also a critical underpinning when two or more organizations, governments or jurisdictions have decided to collaborate with one another.

[2] The assurance model also links other concepts to assurance (e.g. credential). However, assurance of identity is the primary value and initial focus of the model. The assurance model will evolve over time to incorporate other types of assurances.

In this latter scenario, the uncertainty of identity (and the associated risks) becomes especially acute, because the risks are no longer confined within the set boundary of an organization or jurisdiction. The possibility of identity vulnerabilities having multiplier-effects or risks, cascading across boundaries, makes the *assurance of identity* even more important.

Due to the close link between assurance and identity*, assurance of identity* is central to the model. Assurance of identity is about ensuring that:

a) The entitled person has access to government information and services (either as employees or clients), and,
b) The information or issue is about the right person, or the service is delivered to the entitled person.

The primary value of the Pan-Canadian Assurance Model is that it enables the assurance *of identity* produced by one organization to be used by other organizations.

6.1.4 Assurance and Authentication

Authentication is generally defined as "the process of establishing truth or genuineness to generate an assurance". However, in most cases 'authentication' and the associated authentication process are very diverse and defined to meet a specific business requirement (e.g. electronic access) and enabled by a specific technology.

The authentication processes may also be 'complex'. Depending upon the business context, the authentication process may authenticate many things at once, including any combination of the following:

1) That someone is actually who they claim to be (identity authentication);
2) That someone has maintained control over a credential (credential authentication)
3) That a thing or artefact is actually legitimate (document authentication);
4) That a specific event actually took place (date-of-birth authentication); ,
5) ..Plus many more facts…

Despite the variety and complexity, there are generally two phases common to all authentication processes:

1) **Registration Phase**: the process that: i) establishes the identity of an individual (or claimant) and, ii) issues a credential to the individual. This phase is usually carried out once, or at infrequent intervals.

2) **Authentication Phase:** the process subsequent to the registration phase, where the issued credential is authenticated. This phase is carried out repeatedly, whenever an individual is requesting access to a service or system.

The authentication process for a specific system may have variations of these two phases. For example, a system issuing anonymous credentials, may issue a credential in the registration phase, but not establish identity. Similarly the authentication phase may verify that the credential is being used by its rightful owner, but ignore the identity of the credential-bearer, even if supplied.

The authentication process becomes even more complex when there is requirement to obtain a higher degree of confidence (i.e. level of assurance). The different levels of assurance require different verification methods (e.g. in-person visits, additional documents, PKI certificates, etc.). Finally, the authentication process may not be limited to an automated online process (e.g. login) but involve multiple channels (e.g. telephone, mail, and in-person) involving manual processes (e.g. officers visually inspecting documents).

Despite these complexities, the assurance model can be used to analyze and define specific requirements related to identity and credentials and help to determine which aspects can be federated.

6.1.5 Assurance within a Federation Context

In the future, the public sector at all levels of government will operate in an environment that supports the seamless delivery of services to citizens while protecting and preserving security and privacy. Underpinning this scenario are trust relationships and governance that enable government organizations to pursue interoperability goals that best align with their respective business models and IT policies, security, privacy goals and requirements. The optimal arrangement that allows for this flexibility and independence is *federation*. Federation, as defined by the model is *co-operative agreement between autonomous entities that have committed to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability*.

The practice of federated identity management informally exists today. Figure 1 illustrates an example of ‘federation’ whereby an individual uses a credential issued by one jurisdiction (e.g. a provincial birth certificate) to gain access to services or benefits from another jurisdiction (e.g. a federal benefits program). Further, the jurisdictions may have arrangements in place to share information (e.g. vital events data) which is used to maintain the integrity of a program database. These arrangements may be based on implicit trust, bi-lateral arrangements or memoranda of understanding. This approach is not scalable today and cannot support the goal of cross-jurisdictional interoperable service delivery to clients.

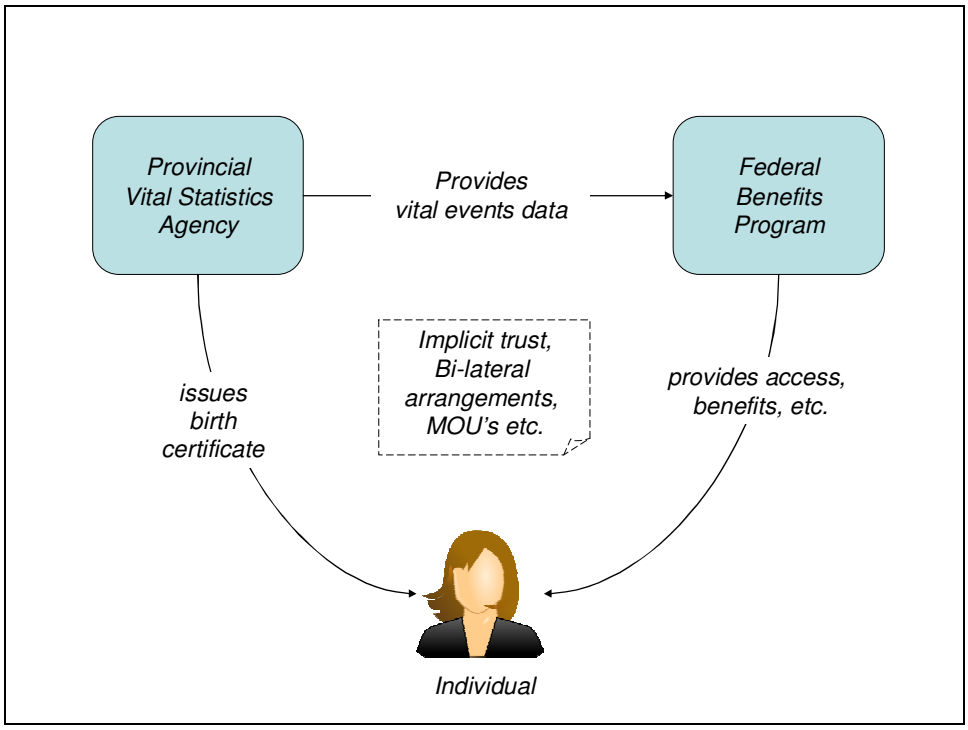


Figure 1: 'Federation' Today

The Pan-Canadian Assurance Model is intended to reinforce what informally exists today and formalize concepts of federation. These concepts, when viewed together comprise the *federation context* and can be eventually expressed in formalized arrangements such as a contractual agreement between participating parties within a federation.

Figure 2 illustrates the same scenario as in Figure 1, using federation concepts (*italicized*). The same scenario described using federation concepts: the provincial vital statistics agency is regarded as an *authoritative party* that has made a claim about a *principal* (e.g. the individual's name, date of birth, gender, etc.). In turn, the federal program is the *relying party* using an *assurance* provided by the *authoritative party* to provide access or benefits to a *principal* as a client.

The italicized terms used in this paragraph are discussed in detail below.

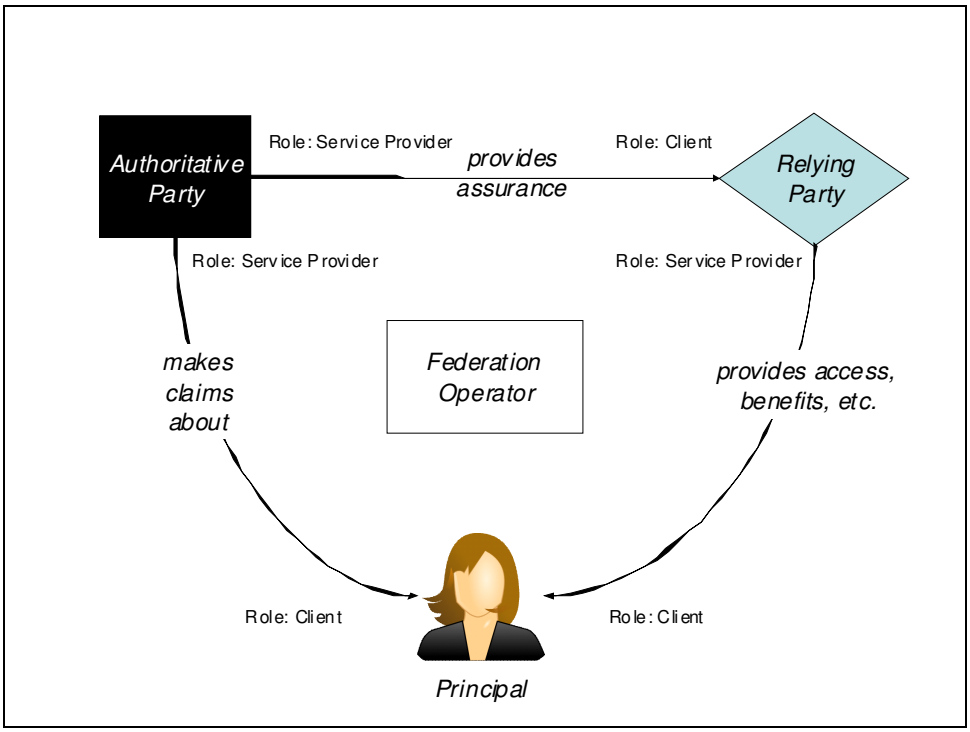


Figure 2: Federation Concepts

The federation concepts fall into four main categories:

- **Federation Actors** – (illustrated by the box, diamond, and user graphic) defines the major types of parties represented by members of a federation (authoritative party, relying party and principal);

- **Federation Roles** – (illustrated by the "Role:" label) defines the responsibilities or expected behaviours that a federation member may wish to formalize with one another by means of formal agreements or contracts; and,

- **Federation Operator** – (illustrated by the central box) defines the body (an individual, organization, group, etc.) that is responsible for standards for its respective federation, or trust community and evaluates participation in the community or network to ensure compliance with policy, including the ability to request audits of members for verification [19].

- **Federation Relationships** - (illustrated by the arrows between the actors) defines the major types of relationships that can exist between members of a federation.

Federation Actors

By definition, federation membership comprises independent actors (or entities) that have agreed to trust and interact with one another. Within a federation, there are three types of independent actors:

- **Principal**. The principal is the actor that initiates an interaction and/or is subject to an outcome. The principal is typically an individual who is providing evidence of a claim or requesting a service.

- **Authoritative Party -** The authoritative party is an entity whose authority to make claims is recognized by one or more parties. The authoritative party verifies claims to provide an assurance. Authoritative parties are in most cases government entities that have specific legislative authority and accountabilities (e.g. vital statistics agency). An authoritative party may also be *Credential Service Provider*, or *Identity Proofing Service Provider [19].*

- **Relying Party -** A relying party is an entity that receives an assurance from an authoritative party. The relying party uses this assurance to satisfy a specific risk requirement to reduce or offset the potential impact of a vulnerability or threat existing in a business process, program administration, or the provision of a service to a client (to name a few). Relying parties can be any type or organization: government or commercial organizations that depend upon the outputs of other organizations (e.g. identity documents) and which can directly impact the quality and integrity of their own programs and services.

Federation Roles

Federation roles are the formalized roles that must be assumed when one member wishes to establish a formal arrangement with another. . The model identifies two federation roles that are required in the federation context: **Client** and **Service Provider**

Client. The client is the entity that wishes to receive a service. A client is typically a principal (i.e. individual) who initiates an action (i.e. requests a service) and expects an outcome resulting from this action. Various members may take on the role of a client depending on the transaction, but it is also possible that a client can be from outside the federation.

Service Provider. The service provider is the entity that wishes to provide a service. A service provider is typically a government or commercial organization that is providing a service to a Client (as described as above). Depending upon the type and nature service, the client may be a Principal or a Relying Party.

Federation Operator

The Federation Operator is the organization that provides governance and day-to-day operational support for the federation. The Federation Operator is authorized to enter into binding contracts and agreements and to provide support for federation services. The Federation Operator is recognized by federation members as having certain roles and authority in creating a framework in which on-line identity assertions can be trusted and the privacy of identity information protected. The Federation Operator is also responsible for standards for its respective federation, or trust community and evaluates participation

in the community or network to ensure compliance with policy, including the ability to request audits of members for verification [19] [20]. For a federation operator to be effective, the federation members must agree to the following:

- **An acceptable governance structure –** Agreement is necessary on the nature and extent of the governance that will be in place for controlling and directing the federation as a whole. The governance body is dependent upon the community that is being served by the federation and may range from an informal committee to a formal organization having legal (or legislative) authorities.

- **A set of standardized assurance levels –** Agreement is necessary on the standardized levels of confidence provided by an authoritative party or required by a relying party. These standardized levels enable better decision-making as it pertains to risk management

- **Clearly defined roles –** Agreement must be reached on the roles define within the federation, how actors carry out these roles, and the qualifications needed to assume these roles within the federation.

Federation Relationships
The federation context also defines three major types of relationships within a federation (each type of relationship is represented by an arrow between the entities). Following is a description of each.

- An **Authoritative Party** in the role of a **Service Provider** makes claims about a **Principal** who is in the role of Client (leftmost arrow). An example of this relationship is a Vital Statistic Agency (authoritative party) that provides a birth certificate service (as service provider) to an individual (the client)

- An **Authoritative Party** in the role of a **Service Provider** provides an assurance to a Relying Party in the role of a Client (bottom arrow). An example of this relationship is a Vital Statistics Agency (authoritative party) providing birth validation information (the assurance as a service provider) to a Government Benefits Program (relying party)

- A **Relying Party** in the role of a **Service Provider** provides access, benefits, etc. to a Principal who is in the role of a Client (rightmost arrow). An example of this relationship is a Government Benefits Program (the service provider) providing a benefit to an individual (the client). In providing this service to the client, the Government Benefits programs uses assurance provided in the previous relationship to manage the associated risk.

6.1.6 Relationship to Identity Management Architecture

The assurance model is closely related to identity management architecture models. There are several identity management architecture models in existence having the same components described within a federated context. Figure 3 illustrates this relationship.

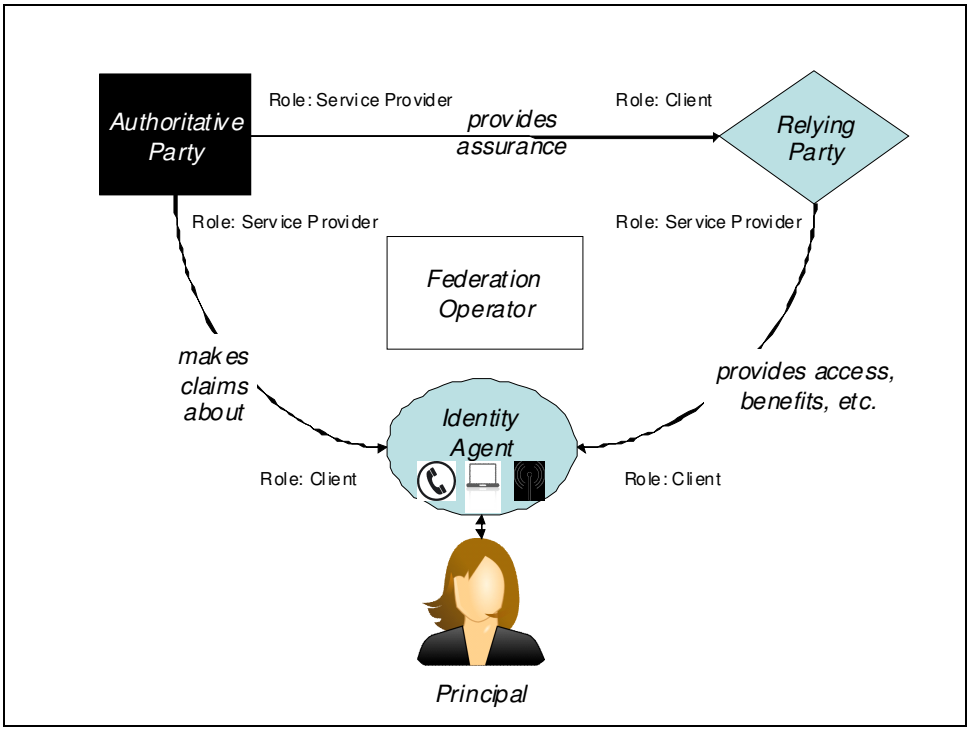


Figure 3: Identity Management Architecture

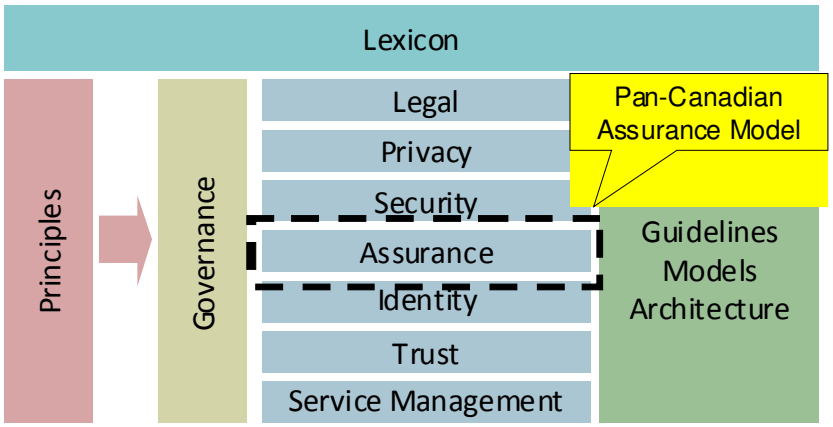
The identity management architecture is consistent with the federation context – that authoritative parties provide accurate claims to relying parties about the principals in question. These various interactions and arrangements are subject to the policies, contracts and agreements put in place by the Federation Operator.

The identity management architecture provides additional detail on how an authoritative party may issue credentials, how these credentials are associated to a principal, and how a relying party authenticates them. This is additional is expressed

The identity management architecture has the same actor types as in the federation context - authoritative party, relying party and principal, however there is one more type added: **Identity Agent.** An identity agent is not a separate actor per se. Instead, it is the software on a principal's personal computer or other device acting on principal's behalf and facilitating the flow of identity claims about an individual between the authoritative parties and the relying parties. The identity management architecture is specifically concerned about the mechanisms to convey and receive assurances between parties, including the confidentiality and integrity during these conveyances.

6.1.7 Relationship to Other Models

The Pan-Canadian Assurance Model fits into the larger Pan-Canadian Identity Management and Authentication Framework defined by the Inter-Jurisdictional Identity Management and Authentication Task Force (IATF) report *A Pan-Canadian Strategy for Identity Management and Authentication* [13] . Figure 4, below, illustrates this framework.



Developed by the Inter-jurisdictional Identity Management and Authentication Task Force (IATF)

Figure 4: Pan-Canadian Identity Management and Authentication Framework

The Pan-Canadian Assurance Model is a component within this larger framework and is being developed by the Assurance, Identity and Trust Working Group (AIT WG). In addition to the assurance model, the AIT Working Group is tasked with establishing a trust model that sets out the important requirements of trusted relationships between parties involved in identity management and authentication services. The resulting work will be used to define the standards, processes and relationships for the Pan-Canadian identity and authentication framework.

There are two other working groups contributing the development of a Pan-Canadian Identity and Authentication Framework: the Legal, Privacy, and Security Working Group (LPS WG); and the Identity Service Experience Working Group (ISE WG).

The LPS WG seeks to identify key pieces of legislation and policies among Canada's federal, provincial, territorial and municipal governments to create a common inter-

jurisdictional reference for the Pan-Canadian identity and authentication framework. The focus of the LPS Working Group is on these three areas:

- **Legal** – Provides a complete picture of laws, legislation, regulations and authorities that govern identity management and authentication within Canada;
- **Privacy** – Sets the context within which privacy requirements are applied to identity management, including consent, collection, use and disclosure of identity; and
- **Security** – Defines the environment that engenders trust through adoption of common security and protection of identity information.

The ISE WG is focused on service delivery and customer service to ensure that the end-to-end process of creating, delivering, managing and improving identity services, are client-centered. The ISE will integrate the work of the other two working groups to the customer experience across all service delivery and program channels for both business and individuals. The ISE's "Identity Service Experience Model" focuses on six customer-focused principles to support the Pan-Canadian identity management and authentication vision of a seamless, cross-jurisdictional, user centric, multi-channel service delivery experience for interacting with all levels of government:

- Client Choice, Consent, Control
- Limited Information for a Limited Use
- Client-focused, Consistent Experience
- Diversity of Identity Context and Systems
- Trusted, Secure Environment
- Transparency and Accountability

6.1.8 Assurance Categories

By definition, an assurance reflects the measure of certainty (level of confidence) that a statement or fact is true. An assurance can also be considered as a claim that is backed up by an authoritative party that has verified the claim.

The types of claims and corresponding assurances can be unlimited. However, assurances are typically concerned with claims that would represent a risk to a program, service or transaction. These types of claims fall into two categories, usually associated with individuals: claims of identity, and claims of credential entitlement and authenticity. If an individual claims the identity of another individual, and successfully accesses a secure service, this can result in real damage and this is the risk that must be managed. .

6.1.8.1 Identity Assurance and Credential Assurance

The two assurance categories used in the assurance model can be understood as follows:

Identity Assurance is the level of confidence (certainty) that the client is really who they claim to be. An identity assurance mitigates the risks (or uncertainties) associated with false or inaccurate claims around an individual's truthful identity.

Credential Assurance is the level of confidence (certainty) that the client has maintained control over what has been entrusted to them. A credential assurance mitigates the risk (or uncertainties) associated with a compromised, lost or stolen credential.

It is important to note the distinction in the model between Identity Assurance and Credential Assurance. In certain cases there may be no practical gains by separating identity and credential assurance. However, the distinction becomes useful when there are requirements to integrate within a complex system (i.e. federation) while addressing privacy and program legislation requirements. The distinction is also useful when defining specific roles and responsibilities where separation of roles is required. (e.g. credential issuance versus identity proofing).

The identity assurance is concerned with the individual's truthful identity, whereas the credential assurance is only concerned with the binding or association to the same and specific individual (anonymous binding) without necessarily knowing their 'true identity'. This distinction is desirable for programs and jurisdictions that wish to leverage an existing (i.e. federated) credential service while continuing to assign identity proofing as a program responsibility (i.e. provide their own identity assurance). This distinction is also a privacy-enabler because it allows an individual to use a credential without necessarily revealing their identity.

Table 1 provides the formal definitions of identity assurance and credential assurance as used in the assurance model.

Assurance Category
Identity Assurance - The measure of certainty (level of confidence) that an individual is claiming their truthful identity, and not a stolen or fictitious identity.
Credential Assurance The measure of certainty (level of confidence) that the client has maintained control over the entrusted credential and the credential has not been compromised.

Table 1: Assurance Categories

6.1.9 Assurance Levels

An assurance level reflects *the degree* of certainty that is given by one party (the assurance provider) or is required by a relying party. The assurance model standardizes this degree of certainty by setting four levels (plus 'zero' or 'none') of assurance.

6.1.9.1 Standardized Assurance Level Descriptions

Table 2 describes a set of standardized generic assurance levels recommended by the AIT Workgroup. The descriptors are expressed in terms of the *level of confidence required* (from the relying party perspective) or the *level of confidence provided* (from the assurance provider perspective). These descriptors apply within both identity and credential assurance categories.

Assurance Level[3]	Assurance Level Description[4]
None	**No confidence required[5]:** *No harm to any party in the event of authentication error, therefore,* authentication is typically not required nor desired.
Level 1	**Little confidence required.** *Harm from an authentication error would be nil to minimal.*
Level 2	**Some confidence required.** *Harm from an authentication error would be minor to moderate.*
Level 3	**High confidence required.** *Harm from an authentication error would be moderate to serious.*
Level 4	**Very high confidence required.** *Harm from an authentication error would be serious to catastrophic.*

Table 2: Standardized Assurance Level Descriptions

The standardized assurance levels are generic in nature[6] and are intended to map directly to requirements being defined in the emerging trust frameworks, such as the Kantara Identity Assurance Framework [23] and the Federal ICAM Trust Framework Provider Adoption Process [24].

[3] It should be noted the short descriptions (i.e. "None", "Level 1" to "Level 4") are the "normative" aspect of the model, that is, any application or derivation of the model must comply with these descriptions. The assurance level descriptions are considered as "non-normative" and can be adjusted as required to suit the audience or context.

[4] The assurance level descriptions are intended to provide an agreed upon sense of the level of confidence. As indicated in the previous footnote, these descriptions may be adjusted accordingly without affecting the relative meanings of the short descriptions. For example, "Limited" may be used for Level 1, and "Reasonable" may be used for Level 2.

[5] The assurance level description is written from the perspective of the relying party ('… confidence required'). To reflect the perspective of the assurance provider, the assurance level description may be optionally modified to read ("… confidence provided"). As stated in the previous footnotes, these descriptions may be adjusted to suit the particular audience.

[6] The 2007 *Pan-Canadian Identity Management Framework* [13] originally proposed assurance levels 0-3 with the descriptions of "Unclassified", "Low", "Medium", and "High". Since this report, the assurance levels have been adjusted to align with the emerging trust frameworks.

6.1.9.2 Credential Assurance Level Descriptions

Credential Assurance Level (CAL): The standardized assurance levels can be applied to the category of credential assurance as follows in Table 3.

Credential Assurance Level	Credential Assurance Level (CAL) Description
None	**No confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised
Level 1	**Little confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised
Level 2	**Some confidence required** that the client maintained control over the entrusted credential and the credential has not been compromised
Level 3	**High confidence required** that the client has maintained control over the entrusted credential and the credential has not been compromised
Level 4	**Very high confidence required** that the client has maintained control over the entrusted credential and the credential has not been compromised

Table 3: Credential Assurance Level Descriptions

6.1.9.3 Identity Assurance Level Descriptions

Identity Assurance Levels (IAL): The standardized assurance levels can similarly be applied to identity assurance as follows in Table 4.

Identity Assurance Level	Identity Assurance Level (IAL) Description
None	**No confidence required** that the client is or is not who they claim to be.
Level 1	**Little confidence required** that the client is or is not who they claim to be.
Level 2	**Some confidence required** that the client is or is not who they claim to be.
Level 3	**High confidence required** that the client is or is not who they claim to be.
Level 4	**Very high confidence required** that the client is or is not who they claim to be.

Table 4: Identity Assurance Levels

6.1.9.4 Comparison of Assurance Levels to Other Models

The levels defined in the assurance model are consistent with emerging industry and public sector models (NIST, Liberty Alliance, etc.), although they have been adapted slightly to suit the Pan-Canadian context. The key difference from other models is that our levels are first defined generically. These generic standards can then be applied to various categories of assurance, in the case of the Pan-Canadian Model specifically, to establish Identity **Assurance Levels** and **Credential Assurance Levels.**

The primary benefit of articulating generic, standardized assurance levels is that the assurance model can be easily extended and applied to other risk categories as they are identified (currently out of scope of this document).

Table 5 is a comparison of the Pan-Canadian assurance levels to the other major models.

Level of Assurance	Pan-Canadian Model	Liberty Alliance	OMB M04-04	eID Interoperability for PEGS[14]
None	No confidence required	N/A	N/A	N/A
Level 1	Little confidence required	Little or no confidence in the asserted identity	Little or no confidence in the asserted identity's validity	Minimal Assurance
Level 2	Some confidence required	Some confidence that an asserted identity is accurate	Some confidence in the asserted identity's validity.	Low Assurance
Level 3	High confidence required	High confidence in asserted identity	High confidence in the asserted identity's validity	Substantial Assurance
Level 4	Very high confidence required	Very high confidence in asserted identity	Very high confidence in the asserted identity's validity	High Assurance

Table 5: Comparison of Assurance Levels in Other Models

6.1.10 Relationship to Risk Management

The assurance model is consistent with classical risk management approaches and concepts.

In general, risk is the effect of uncertainty on objectives. An effect is a deviation from the expected and can be positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence [21].

Whereas risk is the *effect of uncertainty*, an assurance can be viewed as a *complementing measure of certainty that can be used to reduce risk (i.e. effect of uncertainty)*. Risk management is used by organizations to assess and decide what safeguards or measures must be put in place. In contrast, assurances are used by organizations to decide what can be relied upon *instead of* putting in safeguards and measures.

Within organizations, assurance, its relationship to risk management and the relationship to achieving objectives is well-established, although largely implicit, through organizational management standards, performance agreements, etc. However, when assurances are provided between organizations, there requires a more explicit account of the assurances being provided, the standards being followed and the risks involved.

Generally, risk management incorporates the following steps:

1. Review information and identify risks (if any) associated with it (i.e. conduct a risk assessment). This includes:
    a. Identifying what events could constitute a risk (e.g. inadvertent disclosure);
    b. Estimating the impact of the events (e.g. financial loss); and,
    c. Estimating the likelihood that the event will take place.
2. Evaluate the adequacy of the current controls and safeguards in place to protect against risk
3. Identify the acceptable risk and the additional controls needed to mitigate the risks
4. Develop an action plan to implement the additional controls.

A central component of all risk management approaches is the risk assessment methodology. The assurance model is designed to leverage existing risk assessment methodologies. Risk assessment methodologies assist in defining a level of risk by predicting the likelihood that an identified event can occur in conjunction with its impact on the parties involved. It is important to assess risks from both a consumer and government perspective.

Once risks have been appropriately assessed, including likelihood and impacts, this information can be used to determine the required levels of assurance. The question can then be asked, *what level of assurance is required to reduce or eliminate this risk?* The

level of assurance is used to determine the required controls that must be implemented to adequately mitigate risks. The following section provides a high level summary of impact assessment categories to determine the required level of assurance.

6.1.11 Impact Assessment Categories

The assurance model recommends that a program or service undergo a formal impact assessment to determine the assurance level required. . The assessment should take into account the various ways that an organization and its clients or stakeholders can be harmed by authentication errors. The table below lists eight (8) examples:

	Type of Impact
1	Inconvenience, distress/loss of standing or reputation.
2	Financial loss. Impacts are financial in nature.
3	Harm to program or public interest.
4	Unauthorized release of sensitive personal or commercial information.
5	Unauthorized release of sensitive government information (non-personal information)
6	Civil or criminal violations
7	Personal Safety
8	National Security

Table 6: Summary of Impact Categories

These examples reflect a range and degree of possible consequences that might be sustained by different parties affected by an authentication error. These parties may include:

- Principals directly involved in a transaction or service (first and second parties). This is normally a person receiving a service from a government department or agency.

- Other persons or departments (third parties) that may be harmed as a consequence of principals being harmed.

6.1.12 Compensating Factors in the Authentication Process

The assurance model defines the concept of compensating factor[7]. A compensating factor is defined as an additional measure employed during the authentication process that reduces the likelihood of an authentication error. Examples of compensating factors

[7] Compensating factor is equivalent to 'compensating control'

include:

- Shared secrets,
- Validation of identity information collected as the result of an identity assurance process (identity validation).
- Validation of program information collected as part of a program or service administrative process (program validation),
- Token/grid card challenge;
- Reverse Turing test (to determine if user is human)
- Out-of-band confirmation, etc.

A compensating factor may be employed when an input into the authentication process (e.g. credential or password) does not meet or comply with the established assurance level requirements. The compensating factor is an additional method employed to further strengthen authentication process thereby reducing the likelihood that an authentication error will occur.

Benefits of Compensating Factors

The primary benefit of a compensating factor is that it enables flexibility in the design of an authentication solution. This flexibility is required if the authentication process is subject to business or usability constraints. Flexibility is also required if the authentication process is required to dynamically adapt to a changing threat environment (i.e. consisting of new threat agents or vulnerabilities)

Examples of authentication solutions that require flexibility:

- A Level 3 transaction that must be carried out using a Level 2 credential. A compensating factor can be employed to address the risk gap arising from Level 2 assurance of the credential and the Level 3 requirement of the transaction

- An authentication process that must dynamically adapt to a different threat environment while allowing the use of the same credential. For example, a client when attempting to access the service from a publicly accessible machine (e.g. internet café, public library etc.) may be allowed to continue to use their Level 2 credential, but be challenged by a compensating factor.

- An authentication process that enables client authentication but without requiring the use a valid credential (e.g. it is has been stolen). Instead of requesting a credential (because it is lost), a client may be challenged using several compensating factors that together provide the equivalent assurance (usually a one-time process).

Drawbacks of Compensating Factors

Compensating factors also have drawbacks. Since they are essentially customized components, they increase overall costs, introduce process complexity, and require

maintenance. Compensating factors, while attractive in the short run, may be problematic over the long run. The factors used may become ineffective (i.e. threat agents adapt) and if they use program-specific or personal information, they may introduce privacy risks and impose additional security constraints. Since compensating factors are specific to a system, they should not be used to escalate the level of assurance for use elsewhere (e.g. enable a Level 2 credential be relied upon as a Level 3 credential.) If compensating factors are to be considered in an authentication solution, the trade-offs of benefits and drawbacks should be carefully weighed against one another.

7 Assurance Assessment Process

The assurance model rests on a three-step assessment process that helps organizations to answer questions regarding *managing risk in an organization* and *becoming a trusted member in a federation*. Figure 5, below, illustrates the three-step process as it unfolds with the help of the supporting tools. We also acknowledge here that the entire process is informed and enabled respectively by two other components of the Pan-Canadian model (currently under development)

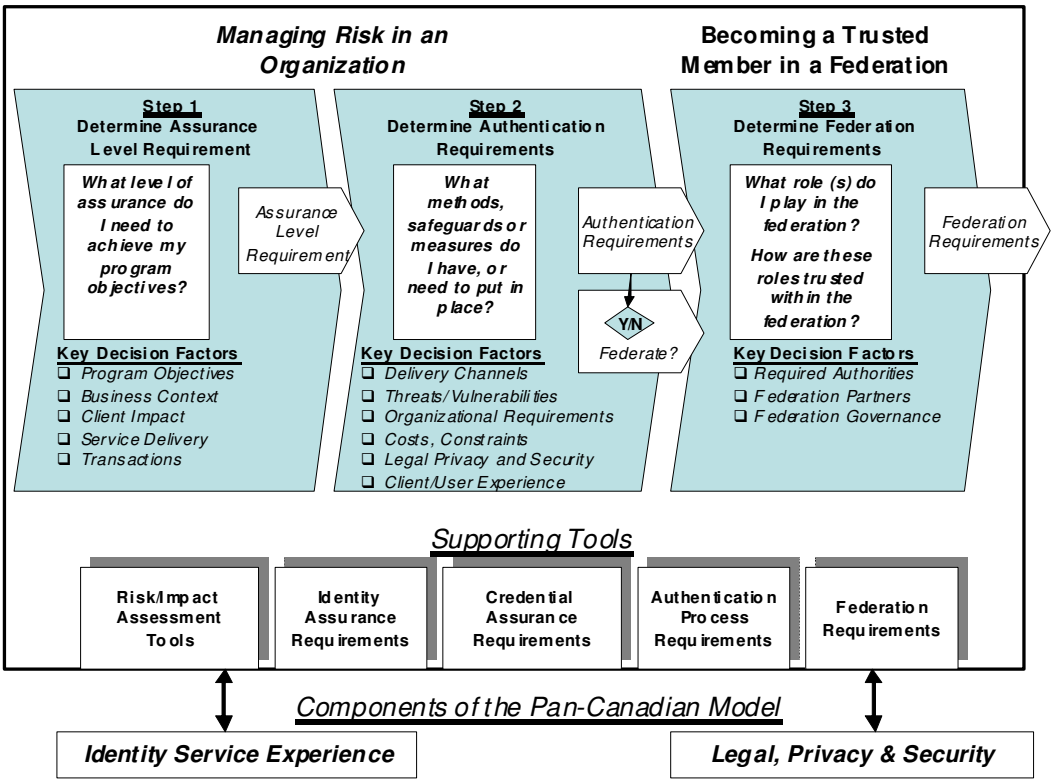


Figure 5: Three-Step Assessment Process

Tools for applying the process are found in Section 8; however a jurisdiction may use its own tools as well.

How the Assurance Assessment Process Works

The assurance assessment process is comprised of three discrete steps. Each step produces a specific output that in turn, is used as the primary input into the subsequent step. The process may be applied using a linear or iterative approach.

Steps 1 and 2 identify and manage risks within the organization. These steps are structured to leverage existing risk management tools that an organization may have already employed.

The output of Step 1 is an **Assurance Level Requirement.** The assurance level requirement is defined as the level of assurance (i.e. confidence) that is required to achieve a program outcome, deliver a service or execute a transaction. The assurance level is determined by the severity of potential impacts (refer to Table 2: Standardized Assurance Level Descriptions). Moreover, it represents the 'high watermark' requirement that must be considered for all aspects of program, service or transaction.

The output of Step 2 is the **Authentication Requirement.** The authentication level requirement is defined as the level of assurance that the authentication process must provide after considering other safeguards or controls that exist within the system or business. Step 2 also provides a decision point on whether an organization should **Federate** or do everything on its own.

If an organization has no intention to participate in a federation then Steps 1 and 2 of the assessment process are sufficient. If an organization intends to enter into a federation or trusted relationship with another party (i.e. become a relying party), then Step 3 is required.

Step 3 determines what role an organization will assume within a federation, if it has chosen to federate. Step 3 prompts decisions on the following questions:

- Will the organization become a relying party?
- Does the organization have the mandate or capability to become an authoritative party?
- Should the organization formalize business relationships to become a client or service provider?
- Once the above decisions are taken, what is necessary to achieve compliance with the required levels of assurance appropriated to the chosen roles?

The output of Step 3 - a series of decisions on how an organization wishes to collaborate with other organizations as trusted partners, or as members within a federation – is the **Federation Requirement**.

7.1 Step 1: Determine Assurance Level Requirement

The objective of Step 1 is to answer the question from the standpoint of a business owner: *What level of assurance do I need in order to achieve my program objectives, deliver my service or properly execute my transaction?* The output of Step 1 articulates a high-level business requirement that drives the balance of the assessment process. The business owner should perform this step.

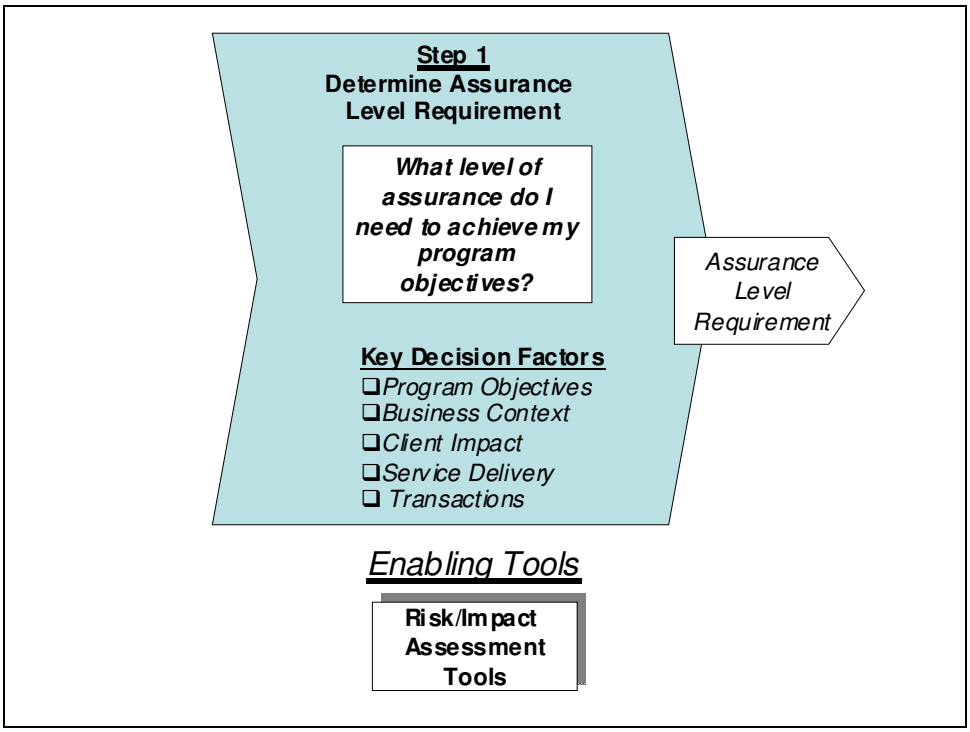


Figure 6: Step 1 - Determine Assurance Level Requirement

Guidance for Completing Step 1

The output of Step 1 is expressed as an **Assurance Level Requirement.** This represents the overall level of confidence required of a program, service or transaction. The assurance level requirement can also be regarded as the overall level of confidence required by a business or program owner to:

- Achieve program outcomes;
- Ensure that services are delivered to the right person; or,
- Ensure the legitimate execution of transactions.

The Assurance Level Requirement should be expressed in the standardized format described in **Table 2: Standardized Assurance Level Descriptions.** The assurance level

requirement represents the 'high watermark' to manage risk and is independent of a particular assurance category (e.g. identity assurance or credential assurance). As a high watermark requirement, the assurance level requirement represents the level of assurance that all inputs and processes *should achieve*. This is the ideal case. In reality this may not be possible, due costs, client requirements, service delivery requirements, or other factors. Step 2 takes into account these factors and provides options on compensating factors, or the acceptance of residual risk.

The intention is for Step 1 to be independently conducted and without regard to delivery channels, existing system safeguards, or business processes already in place. The assessment is strictly based upon the nature of the program, service, or transaction and the clients or stakeholders that these might affect.

To determine the assurance level requirement, it is recommended that an impact assessment be undertaken that employs a "what if approach"[8]. This approach compels the assessor to consider all possible impacts no matter how unlikely.

Someone with a detailed knowledge of the program or service, its outcomes, principal clients and stakeholders should perform this step. The impact assessment should draw upon this knowledge and be based upon significant business or program-related factors, including:

- The program objectives, including higher-level strategic objectives (or strategic outcomes) that program activities are intended to achieve. Consideration of impacts could include the consequences of not achieving these objectives or outcomes.
- The nature and type of program, service or transaction that is being assessed. Consideration could include the consequences to program owners and managers responsible for carrying out program activities, service or transaction.
- The clients, stakeholders, other interested parties that may be affected
- Intangible or global factors that may be relevant such as public interest or national security.

When conducting the assessment in Step 1 of the process, it is important to define "business context" and focus the assessment of program, service or transaction to this business context. The business owner must define the business context, which may include the following.

- Externally-facing (e.g. citizen-focused) or internally facing (e.g. employee-focused)

[8] This is equivalent of doing a risk assessment where likelihood is equal to '1' or probability is 100%. This approach also addresses the requirement of organizations that must account for all possible impacts however remote the possibility. The "what if approach" also greatly simplifies the Step 1 assessment process by removing the task of trying to quantify the likelihood variable which can be very difficult or subjective because it is sensitive to many inter-related factors, including threat environment, system safeguards, client behaviour, transaction volume, etc. Likelihood is considered in Step 2.

- The type and nature of clients affected by the program (individual, professional, or business)
- Legislative and/or jurisdictional considerations.

Step 1 should only consider the consequential impacts (i.e. externally visible to the program, service or transaction) and which are directly related to the specific program, service or transaction being assessed. Factors related to "methods of delivery" (i.e. online, in-person, telephone, or mail channels),"system design", likelihood, and safeguards are considered as factors in Step 2 of the assessment process.

Organizations may have separately defined their "services" on the basis of a specific channel implementation. However, when viewed from a business standpoint, these channel-specific services are usually a subset of a more generic program, service or transaction and therefore can be addressed with a single assessment. When assessing channel-specific services, the assessor should first attempt to identify the business service, and it is this business service that should be the subject of the assessment in Step 1.

Organizations are free to decide how granular they wish to conduct their assessments. Separate assessments may be conducted at a program-level, service-level (or service cluster) or at the transaction level. However, organizations must consider that the level of effort required to conduct assessments is proportional to depth and granularity.

It is important to restrict the scope of impact assessment to those impacts that can be *directly attributed to* the program, service or transaction being assessed. Although secondary or tertiary (downstream) impacts might arise (i.e. impacts resulting from a follow-on service that might be compromised due to an initial service being compromised), these impacts would be considered in separate assessments.

It is recommended that the Step 1 impact assessment should be performed at the business transaction level to ensure that all potential impacts (within a service or program) have been properly considered.

The organization must decide whether Step 1 is an informal process, or a fully-documented, evidence-based process that is formally signed-off by the organization. In cases where a risk assessment has already been completed, this information may be used as input into Step 1.

Supporting Tools

Several tools assessment tools exist to support the Step 1 Assessment process. The following tables depict an elementary toolset along with references to other recommended tools. A more detailed toolset for Step 1 can be found in the appendix.

Scope and Business Context Definition Tool

This table is intended to assist the assessor in defining the scope of the assessment.

Name of Department / Agency	
Business Owner/Contact:	
Name of Program, Service or Transaction being assessed:	
Scope of Assessment	Are you assessing separately or as a combination: ☐ A program? ☐ A service? ☐ A transaction? ☐ A group, aggregate or cluster of any of the above?
Clients	Identify the clients who are directly impacted by the program, service, and/or transaction identified above. • Are these clients: ☐ Individuals acting on their own behalf? ☐ Professionals acting in an official capacity? ☐ Businesses? Are these clients: ☐ External to the Government of Canada? ☐ Internal to the Government of Canada?
Related Parties	List any related parties that may be also impacted. • •

Table 7: Scope and Business Context Definition Tool

Summary Impact Assessment Table

Table 8 can be used to determine the assurance level requirement using injury levels determined from a risk assessment or information classification process. The table maps the injury levels as determined the risk assessment process to corresponding assurance level requirements.

Injury Level (assessed by security practitioner)	**Assurance Level Requirement** (final determination is made by business owner)
High: Could reasonably be expected to cause extremely serious personal or enterprise injury. Example impacts include any combination of: a) extremely significant financial loss, b) loss of life or public safety, c) loss of confidence in the government, d) social hardship, or e) major political or economic impact	**Level 4: Very high confidence required.** Harm from an authentication error would be serious to catastrophic
	Level 3: High confidence required. Harm from an authentication error would be moderate to serious
Medium: Could reasonably be expected to cause serious personal or enterprise injury. Example impacts include any combination of: a) loss of competitive advantage, b) loss of confidence in the government program, c) significant financial loss, d) legal action, or e) damage to partnerships, relationships and reputations.	**Level 2: Some (or Reasonable) confidence required.** Harm from an authentication error would be minor to moderate
Low: Could reasonably be expected to cause significant injury to individuals or enterprises. Example impacts include any combination of: a) limited financial losses, b) limited impact in service level, or c) performance, embarrassment and inconvenience	**Level 1: Little (or Limited) confidence required.** Harm from an authentication error would be nil to minimal
None: Will not result in injury to individuals, governments or to private sector institutions and financial loss	**None: No confidence required.** No harm to any party in the event of an authentication error, therefore, authentication is typically not required nor desired.

Table 8: Impact Assessment Table

Table 8 can be used facilitate collaboration between the security practitioners, who carry out the risk assessments to determine the injury level and the business owner who makes the final determination of the assurance level requirement. The table maps injury level assessments as defined by the *Public Sector Security Classification Guideline* [1] to acceptable options that a business owner may consider for an assurance level requirement.

For example, injury level of *Low* maps to the assurance level requirement of *Level 1* or *Level 2*. For this injury level, a business owner, using additional assessment criteria, may consider the options of Level 1 or Level 2. Similarly, an injury assessment of *Medium* enables a business owner to consider *Level 2* or *Level 3*. Finally, *High* enables a business owner to consider *Level 3* or *Level 4*.

7.2 Step 2: Determine Authentication Requirements

The objective of Step 2 is to determine authentication requirements that satisfy the assurance level requirement specified in Step 1.

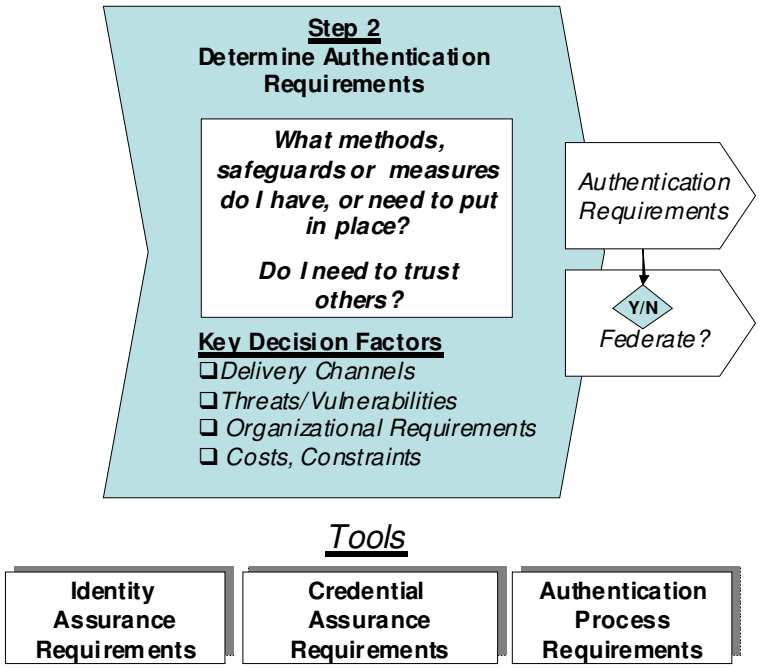


Figure 7: Step 2 – Determine Authentication Requirements

The first question that Step 2 answers is "*What methods, safeguards, or measures do I (i.e. the organization) have, or need to put into place?"* The answer to this question addresses authentication requirements as they exist *within the organization*.

The second question that Step 2 answers is *"Do I need to trust others?"* The answer to this question addresses whether the organization must collaborate with parties *outside of the organization*, through federation.

Authentication requirements emerge from an analysis within six requirements categories as follows:

1) **Credential Assurance Requirements:** These requirements are determined by several (and often competing) factors that may require trade-off decisions. These factors include: security requirements (threats, vulnerabilities), service requirements (usability, accessibility, user behaviour, adoption, etc), and cost requirements

2) **Identity Assurance Requirements:** The factors that determine these requirements are similar to the credential assurance requirements.

3) **Authentication Process Requirements:** These requirements relate to 'generic authentication' (i.e. non-program specific requirements) as defined by industry standards and familiar to federal, provincial, territorial and municipal jurisdictions Authentication process requirements are generally well-defined and standardized for the online channel and many 'out-of-the-box' vendor solutions are available to meet these requirements for online channels. However, there is little guidance for the other channels (in-person, telephone, and correspondence/mail). The authentication process requirements should address all relevant channels (not just online).

4) **Compensating Factors:** To augment the 'generic authentication' requirements, the authentication process may incorporate customized or program-specific (i.e. non-standardized) methods to authenticate the user. These are considered as compensating factors and can vary widely between programs and services. Further, many of these compensating factors use personal information, and therefore privacy requirements, may strictly limit their use within a specific program, service or transaction.

5) **Other Safeguards:** The authentication process may exist within a larger context of security control mechanisms that mitigate risk. Although a transaction may require a higher assurance level, the additional risk is mitigated by other security (non-authentication-related) controls within the system or business.

6) **Acceptable Risk Level:** The business owner may conclude that a certain amount of residual risk is acceptable and will accept any liability arising from the risk.

Figure 8, below illustrates the path of analysis across the six areas and from Steps 1 and 2. The figure uses an example Assurance Level 3 Requirement (which would be determined in Step 1).

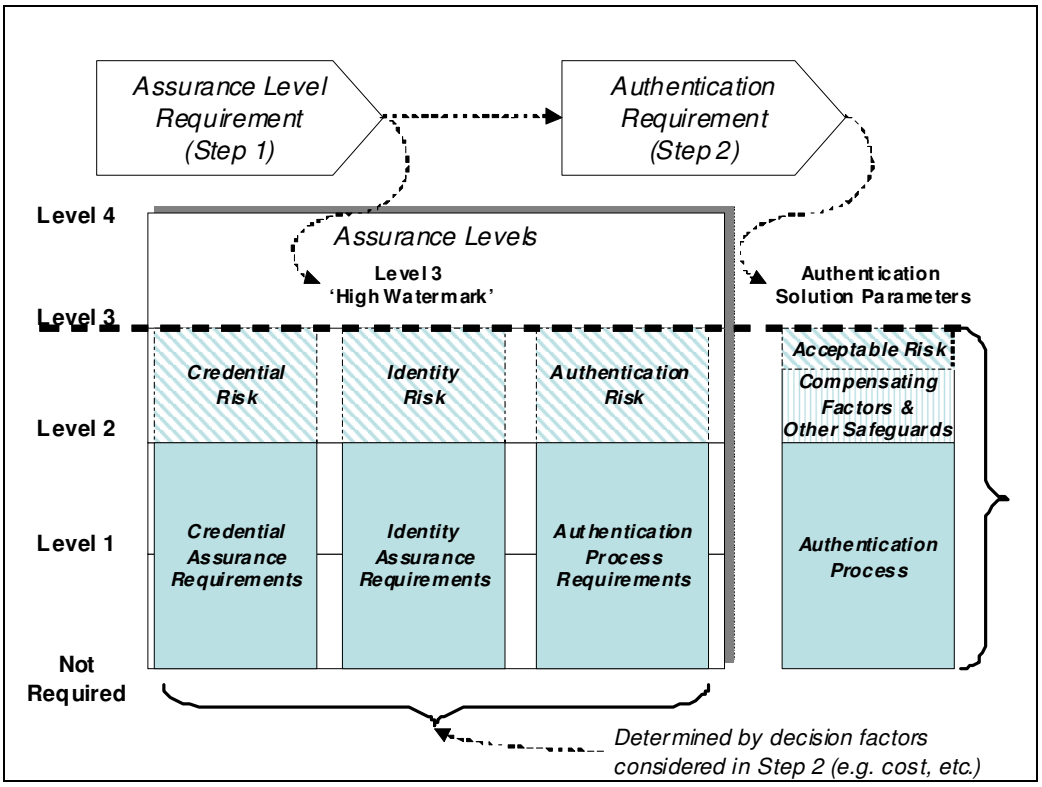


Figure 8: Step 2 Relationship between Step1 and Step 2 Requirements

In this example, the Assurance Level 3 Requirement as determined in Step 1 becomes the Level 3 'High Watermark' requirement that all inputs and processes would be required to meet. Any process or input that does not meet the "high watermark' requirement increases the likelihood that an unwanted event might occur, therefore increases the level of risk. The increased levels of risk can be considered as 'risk gaps'.

In the ideal case, the *credential assurance*, the *identity assurance* and the *authentication process* would all meet the Level 3 requirements (there are not risk gaps). However, due to constraints and limiting factors, it may not be feasible to achieve an Assurance Level 3 on all or most of these components.

The bottom line is that the organization must answer for itself the following questions:

1) What assurance levels are feasible, cost-effective or can be reasonably achieved.
2) What are the resulting 'risk gaps' (increased levels of risk)
3) How these risk gaps will be closed through alternative means, and what is the acceptable risk.

The answers to the above questions determine the **Authentication Solution Parameters.** The authentication solution parameters consist of the six requirements categories at the determined assurance levels.

In the example above, the organization may decide that is possible only to achieve (or acquire) a Level 2 assurance for *Credentials*, *Identity*, and the *Authentication Process*

(thus defining these as Level 2 requirements). However, given the Assurance Level 3 Requirement, these decisions result in risk gaps in three areas: *credential risks*, *identity risks*, and *authentication risks*[9]. These identified risk gaps must then be addressed through determining *acceptable risk*, the specification of *compensating factors*, other *safeguards* and the *authentication process*.

Decision to Federate

The major consideration of Step 2 is the decision whether an organization should federate with another organization. As defined earlier, a federation is a *co-operative agreement between autonomous entities that have committed to support a collaborative effort. The federation is supported by trust relationships and standards to support interoperability.*

In most cases, the decision to federate is an executive-level or strategic business decision rather than a decision determined within the assessment process. However, the outcome of the assessment process should inform the higher-level decision.

When considering the decision to federate, the following areas should be analyzed: 1) Federation Drivers, and 2) Benefits and Risks

Federation Drivers

The key drivers for considering the decision to federate should include:

- **Client Service Experience** - 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;

- **Security** - The desire to provide better service to clients is challenged by evolving and increasingly sophisticated threats that require 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 regards to 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

[9] The diagram is a simplification of the actual risk environment only taking into account and identifying the risk areas but not their relative magnitude. The diagram does not depict how these risk areas interact with one another to yield an overall risk.

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

Benefits and Risks

There are benefits associated with federation where each organization does not have to repeat its own set of credential management, identity management and authentication processes but instead relies upon other federation members. The following benefits that could be realized through federation include:

- Improved client service experience (e.g. increased user convenience through reduced sign on)
- Joining up and coordinating disparate service offerings;
- Reduced administration costs (identity and credential management)

However, federation may create new risks, including.

- Potential liabilities arising from failures due to other parties
- Privacy risks due to transactions and interactions that span organizational and jurisdictional boundaries;
- 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 crossover attacks possible.

Supporting Tools

Please refer to **Section 8** for additional tools and guidance.

7.3 Step 3: Determine Federation Requirements

The objective of Step 3 is to determine what role an organization will assume in a federation.

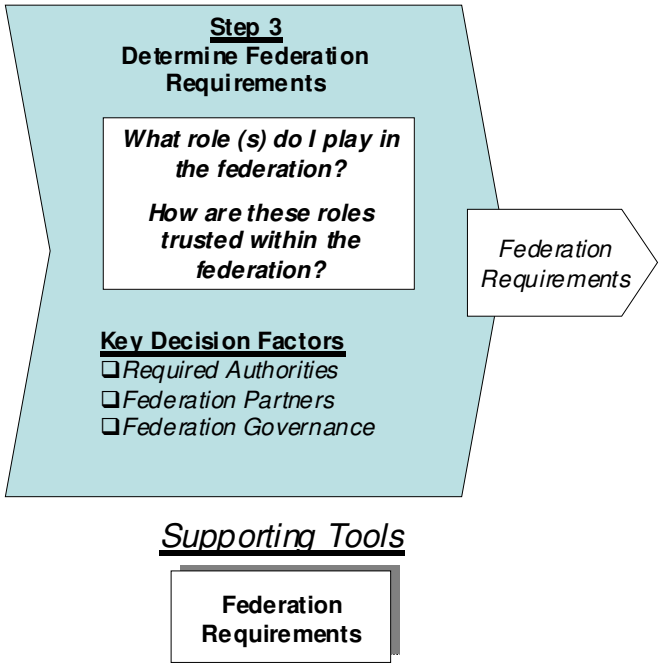


Figure 9: Step 3: Determine Federation Requirements

This step builds upon the decision in Step 2 and determines how an organization will participate in a federation. Step 3 outlines requirements for an organization wishing to enter into arrangements with other parties. The requirements cover the following areas:

- Whether the organization should become an relying party;
- Whether the organization has the mandate or capability to become an authoritative party;
- Whether the organization should formalize business relationships to become a client or service provider.
- For the above decisions, what is necessary to achieve or maintain compliance to according to the required levels of assurance?

The outputs of Step 3 are Federation **Requirements**¸ a set of decisions on how an organization wishes to collaborate with other organizations within a federation.

Formalizing Federated Arrangements

In many cases, ad hoc arrangements already exist between organizations and jurisdictions that simulate a federation. For example organizations already trust physical credentials issued by other jurisdictions as proofs of identity (e.g. driver's licence, passport, Social Insurance Number). These trust relationships are based upon accepted practice, historical precedence or in some cases, convenience. While this approach may have been sufficient in the past, the increasing risk of identity theft requires a more stringent and formalized approach to federation.

The objective of defining federation requirements is to formalize arrangements that currently are ad-hoc or undocumented. The federation requirements can be used as the starting requirements for developing contractual agreements, governance frameworks, policy instruments or legislation. It is important to note that federation of identity is a relatively recent phenomenon and only now are the supporting policy and legal frameworks beginning to emerge. Liberty Alliance has produced several conceptual and technical frameworks, most recently the Liberty Identity Assurance Framework V1.1 in June 2008. The American Bar Association (ABA) has launched a Cyberspace Law Initiative in April 2009 entitled, the Federated Identity Model Agreement and Commentary (FIMAC). FIMAC has not yet been considered within the Canadian jurisdictional context.

Federation Requirements Model

Figure 10 illustrates a simple model that that can be used to assist the formalizing federation requirements. The model is centred upon the relationship requirements between the major types of members within the federation: **principal**, **authoritative party** and **relying party**.

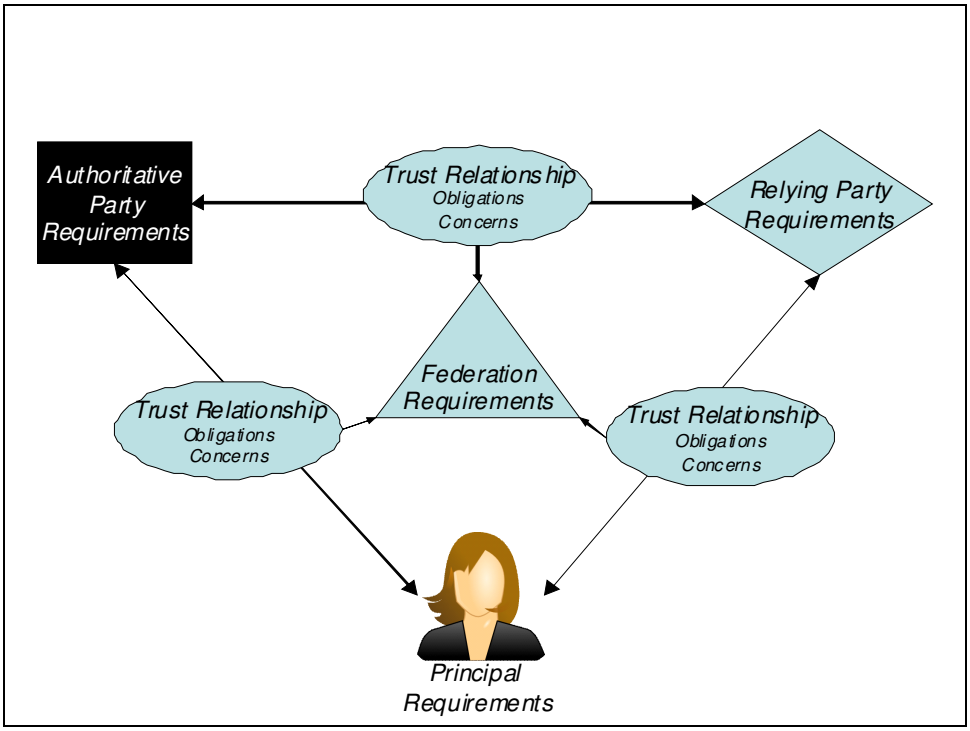


Figure 10: Federation Requirements Model

The model illustrates the necessary *trust relationship*s between the federation members. The trust relationship consists of requirements relating to the *obligations* and *concerns* necessary to maintain the relationship. Obligations are the duties that each federation member is bound to adhere to or carry out. Concerns are the issues that must be addressed before a federation member is willing to trust others. The sum total of obligations and concerns from all of the trust relationships form the federation requirements (illustrated by the central triangle)

Principal Requirements

Principal requirements relate to federation members who initiate interactions, receive a service or are subject to an outcome. Principals are typically: individuals acting on their own behalf, professionals acting in an official capacity, or employees acting on behalf of their employer. Principals interact with authoritative parties to gain recognition of a claim (e.g. legal identity, the right to an entitlement, etc.) and with relying parties to receive a service (e.g. payment).

Principal Obligations: The principal is obliged to meet the following requirements:

- Provide accurate information
- Prevent unauthorized use of credentials,
- Limit control of access to services, transactions
- Provide notification of theft, fraud, or significant change of circumstances

Principal Concerns: The principal is concerned about the other parties meeting the following requirements:

- Protecting privacy
- Ensuring security (confidentiality, availability and accessibility)
- Promoting accessibility, client choice, and mobility between providers.
- Using information only for the purposes for which it is collected.
- Disclosing information only when the principal has given informed consent

Authoritative Party Requirements

Authoritative Party requirements relate to federation members that have the authority to make claims that are recognized by one or more parties (i.e. relying parties). An authoritative party can be a public sector organization with a legislative mandate (e.g. Vital Statistics Act) or a private sector organization that has entered into a binding agreement with other parties. An authoritative party may also act in the role of a Service Provider (e.g. a credential service provider) or work together with other service provider organizations.

Authoritative Party Obligations: The authoritative party is obliged to meet the following requirements:

- Comply with applicable policies, regulations and legislation
- Ensure accuracy of information gathered about principals
- Provide accurate and timely assurances to relying parties
- Provide revocation capability or restriction of use
- Protect the privacy and security of the principal's personal information
- Properly assign or assume liabilities due to error or fraud

As an **Identity Provider**, the authoritative party would be additionally obliged to meet the following requirements

- Ensure there is a rightful need for identification that is consistent with mandate or legislation
- Administer the proper identify-proofing of principals.

Authoritative Party Concerns: The authoritative party is concerned about the other parties meeting the following requirements:

- Information disclosed to other parties is being used subject to consistent use or informed consent by the principal
- Obtaining complete and accurate description of proposed uses
- Defining or limiting the scope of use of assurances
- Limiting liability
- Detecting and reporting fraudulent use and forgery by other parties.

As an **Identity Provider**, the authoritative party would be additionally concerned that the other parties are meeting the following requirements:

- Proving prompt notification of information breaches involving identity information

Relying Party Requirements

Relying Party requirements relate to federation members that use assurances to carry out a business transaction to satisfy a risk requirement or to address a business or technical capability requirement. A relying party is dependent upon a trust relationship with an authoritative party, which if compromised, can have impacts on many related parties (notably principals)

Relying Party Obligations: The relying party is obliged to meet the following requirements:

- Conduct proper risk assessment on the relevant programs, services or transactions.
- Validate/authenticate credentials before reliance
- Limit the use and reliance of assurances provided
- Protect privacy and security of personal information that may be disclosed as the result of an assurance.

Relying Party Concerns: The relying party is concerned about other parties meeting the following requirements:

- Identifying and trusting the Authoritative Party
- Providing prompt notification due to error or fraud

Supporting Tools

The Federated Identity Management Task Force of American Bar Association is currently developing an Identity Management Legal Issues discussion paper

8 Recommended Standards, Guidance and Tools

This section provides references to recommended standards, guidance and tools that can be applied to the Pan-Canadian Assurance Model. This is not an exhaustive list and will be revised over time.

There are four categories of requirements applicable to all organizations, whether the organization intends to develop solutions independently or be part of a federation.

1. **Identity Assurance Requirements -** requirements for organizations intending to establish and/or provide assurances of identity. These requirements cover initial identity-proofing requirements that may also be part of a program enrolment or registration process.

2. **Credential Assurance Requirements –** requirements for organizations intending to issue credentials and/or provide credential management services. These requirements apply to the credential management lifecycle services (e.g. issuance, revocation and validation/authentication).

3. **Authentication Process Requirements** – requirements (primarily technical requirements) that apply to the design and development of an authentication solution (including credentials). These requirements include authentication factors, tokens, threat mitigation, cryptography and event logging.

4. **Compensating Factors and Other Safeguards** – requirements that apply to the identification and use of compensating factors and other safeguards existing within the overall system

There are two additional categories of requirements that are applicable to organizations if they intend to become part of a federation:

1. **Common Organizational Requirements –** requirements that apply to organizations that intend to become service providers within the federation. These requirements establish the general business and organizational requirements for conformity of services and service providers at all levels of assurance.

2. **Certification and Accreditation** – requirements that apply to organizations intending to become an accredited assessor within a federation. These requirements also include what is necessary to become a service provider (identity and/or credential service provider) within a federation.

8.1 Risk Assessment Tools

The Step 1 assessment process is consistent with the impact assessment of a classic risk assessment process. There are several existing tools that map impacts into assurance levels.

8.1.1 Draft Federal Guideline on Authentication

The federal government's Treasury Board Secretariat (TBS) has developed a draft guideline on authentication. The purpose of the guideline is to assist departments and agencies to articulate identity management risks, program impacts, required levels of assurance, and risk mitigation options. The draft guideline provides departments and agencies with an assessment tool to determine the Assurance Level Requirement for a program, service or transaction.

The draft document is available upon request.

8.1.2 OMB M04-04: E-Authentication Guidance for Federal Agencies

The US Office of Management and Budget (OMB) issued guidance to help US federal agencies to determining their authentication needs for electronic transactions. This guidance, referred to as OMB-M04-04, directs agencies to conduct "e-authentication risk assessments" on electronic transactions. This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. The guidance is available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

8.2 Identity Assurance Requirements

Identity assurance requirements apply to organizations that intend to establish and/or provide assurances of identity. Identity assurance requirements outline the initial identity-proofing requirements that also may be part of a program enrolment or registration process.

8.2.1 Kantara Initiative

Several of the references found within this report refer to the Liberty Alliance [25] . The Liberty Alliance Project was formed in September 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for identity management. In April 2009, the Kantara Initiative [26] was announced. The Kantara Initiative is an evolution of the Liberty Alliance Project representing a much broader mandate with a more inclusive participation and membership structure.

During the finalization of this report, several of the Liberty Alliance deliverables are being re-issued under the Kantara Initiative and are in early draft form. Where appropriate, the Liberty Alliance references have been updated to reference the Kantara Initiative deliverables currently under development.

All recommended identity assurance requirements schemes adhere to the levels as specified in **Table 4: Identity Assurance Levels** found on **Page 21**

8.2.2 Liberty Alliance Identity-Proofing SAC

The Liberty Alliance Identity Proofing Service Assessment Criteria (ID-SAC) establishes the requirements for the technical conformity of identity proofing services for the four assurance levels. The ID-SAC requirements specify criteria for each assurance level are organized into three categories each having sub-categories:

1) **Policy** – the requirement criteria that apply to the identity proofing service in general.

2) **Identity Verification** – the requirement criteria that apply to verification of an applicant's true (i.e. legal identity) identity. This category is further subdivided into the following:
    a. **In-Person Public Verification** – criteria that apply to in-person (face-to-face) identity proofing of an applicant where there is no previous relationship.

    b. **Remote Public Verification –** criteria that apply to remote (online or telephone) identity proofing of an applicant where there is no previous relationship.

    c. **Current Relationship Verification –** criteria that apply to identity proofing of an applicant that already has an established relationship with the service.

    d. **Affiliation Verification –** criteria that apply, in addition to the verification of identity, to applicants wishing to establish an affiliation.

    e. **Secondary Checks –** additional measures to deal with anomalous circumstances that can be reasonably anticipated (e.g. a recent change

address that has yet to be established as address of record).

3) **Verification Records –** criteria that apply to retaining records pertaining to identity proofing.

These requirements are being updated under the Kantara Initiative. The most recent documentation can be found on the Kantara Initiative Collaborative Site [27].

8.2.3 BC Identity Assurance Standard

British Columbia is currently developing an Identity Assurance Standard. The purpose of this standard is to:

1) Formalize the Provincial Government's Identity Assurance Model (set out in section 2.0), providing a common understanding of what identity assurance is, and what combination of information, processes and technology is involved in creating and maintaining identity assurance over time;

2) Set of information, technology and process standards required to attain increasing levels of identity assurance over different service delivery channels (e.g., in-person, over the telephone, online);

3) Provide a secure, trusted and privacy-enhancing environment in which to exchange identity claims;

4) Provide an overall framework for the supporting standards and guidelines that are necessary for achieving identity assurance including Registration and Identity Proofing Standards, Credential Management Standards, Cryptographic Standards for Information Protection, Security and Due Diligence Standards, and Federation and Claims Standards; and,

5) Ensure alignment or equivalency with national and international identity assurance standards and guidelines in order to maximize the potential for the Government of British Columbia to connect to, and be trusted by, other identity management systems.

This document provides standards in the following areas:

- Standards for establishing identity assurance levels
- Registration and Identity Proofing Standards.

8.3 Credential Assurance Requirements

Credential assurance requirements apply to organizations intending to issue credentials and/or provide credential management services. These requirements apply to the

credential management lifecycle services (e.g. issuance, revocation and validation/authentication)

8.3.1 Liberty Alliance Credential Management SAC

The Liberty Alliance Credential Management Service Assessment criteria (CM-SAC) establish the requirements for functional conformity of credential management services and their providers at the four assurance levels. The CM-SAC criteria are divided into five parts. Each part deals with a specific functional aspect of the overall credential management process.

1) **Credential Operating Environment:** Requirements that apply to the overall operational environment in which the credential life-cycle management is conducted.

2) **Credential Issuing:** Requirements that apply to the verification of the identity of the subject of a credential and with token strength and credential delivery mechanisms. They address requirements concerning; 1) Identity-Proofing, 2) Credential Creation, 3) Credential Delivery, and 4) Subject Key Pair Generation (Assurance Levels 3 and 4 only)

3) **Credential Revocation:** Requirements that apply to credential revocation and the legitimacy of a revocation request.

4) **Credential Status Management:** Requirements that apply to maintaining a current status of the credential, which may require a revocation or other change to the credential that requires notification to other parties. These requirements also deal with the provision of status information to requesting parties having the right to access such information.

5) **Credential Validation:** Requirements that apply to credential validation and identity authentication.

These requirements are being updated under the Kantara Initiative. The most recent documentation can be found on the Kantara Initiative Collaborative Site [27].

8.3.2 BC Identity Assurance Standard

The British Columbia Identity Assurance Standard defines credential management standards and provides a business-level description of four credential strength levels. The standard also provides credential strength and management standard outlining requirements in the following areas.

1) **Technology Requirements:** includes the type of electronic credentials that are acceptable at different Credential Strength Levels and the security and technical features associated with them.

2) **Credential Creation Requirements:** includes requirements for generating, unique electronic credentials.

3) **Requirements for Subject Key Pair Generation:** includes requirements for generating, storing and delivering cryptographic key pairs associate with a certificate.

4) **Credential Delivery Requirements:** includes requirements for securely delivering a credential to a subject.

5) **Credential Management Requirements:** includes requirements for maintaining a credential's status.

8.4 Authentication Process Requirements

Authentication Process Requirements are primarily technical requirements that apply to the design and development of an authentication solution (including credentials). These requirements include authentication factors, tokens, threat mitigation, cryptography and event logging.

8.4.1 CSEC User Authentication Guidance for IT Systems

The CSEC User Authentication Guidance for IT Systems is an unclassified publication issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

This document is intended for security practitioners and designers of the resulting IT infrastructure. The document provides technical guidance on the design and selection of a user authentication solution. The authentication design categories and requirements specified in the document cover:

a) **Authentication Factors.** How many authentication factors are required during the authentication process (e.g., one factor, two factor, or multi-factor);

b) **Authentication Tokens.** Which tokens are to be used to perform the authentication process (e.g., password, soft token, or hard token);

c) **Cryptographic Module Validation**. The level of validation that is required for a cryptographic module-based token;

d) **Threat Mitigation.** The threats which the authentication process must be capable of protecting against (password guessing, replay, eavesdropping, verifier impersonation/phishing, man-in-the-middle, session hijacking);

e) **Event Logging.** Defines the properties of event logging (e.g., level of detail or audit data protection) required during the authentication process in order to maintain the chain of evidence.

8.4.2 NIST SP800-63 Electronic Authentication Guideline (US)

NIST SP800-63 provides technical guidance to US Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

8.5 Compensating Factors and Other Safeguards

Presently, there are no recommended standards or guidance regarding compensating factors or safeguards. Please refer to Section 6.1.12 for guidance on compensating factors.

8.6 Common Organizational Requirements

Common Organizational requirements apply to all organizations wishing to become service providers within the federation. These requirements establish the general business and organizational requirements for conformity of services and service providers at all levels of assurance.

8.6.1 Liberty Alliance Common Organizational SAC

The Liberty Alliance Common Organizational Service Assessment Criteria (CO-SAC) establish the general business and organizational requirement criteria for an organization wishing to become a service provider at a given level of assurance. The CO-SAC requirements specify criteria for each assurance level are organized into seven (7) broad categories, described below.

1) **Enterprise and Service Maturity (ESM)** – the requirement criteria that apply to the establishment of the organization and its basic standing as a legal and operational business entity within its respective jurisdiction or country.

2) **Notices and User Information (NUI)** – the requirement criteria that address the publication of information describing the service and the manner of any limitations upon its provision.

3) **Information Security Management (ISM)** – the requirement criteria that apply to how the organization manages the security of its business, the specified service and information it holds relating to its user community.

4) **Security-Relevant Event (Audit) Records (SER)** – the requirement criteria that apply to the provision of an auditable log of all events that are pertinent to the correct and secure operation of the service.

5) **Operational Infrastructure (OPN)** – the requirement criteria that apply to the infrastructure within which the delivery of the specified service takes place.

6) **External Services and Components (ESC) –** the requirement criteria that apply to relationships and obligations upon contracted parties (e.g. suppliers or outsourced service providers) both to apply the policies and procedures and also to be available for assessment a critical parts of the overall service provision.

7) **Secure Remote Communications (SCO) –** the requirement criteria that apply to secure remote communications and the storage and protection of secrets (e.g. passwords).

These requirements are being updated under the Kantara Initiative. The most recent documentation can be found on the Kantara Initiative Collaborative Site [27].

8.7 Certification and Accreditation Requirements

Certification and accreditation (C&A) requirements as they apply to the Pan-Canadian Assurance model are in the investigative, planning and development stages. Currently, the Identity Management Steering Committee (IMSC) is considering a project to develop an understanding of the following:

- Certification and Accreditation (C&A) requirements for identity providers within a federation;
- Consideration of components of existing work on C&A can be adopted in whole or in part to support the Pan-Canadian Assurance Model.
- C&A requirements as they pertain to each of the four levels of assurance as defined in the emerging Pan-Canadian Assurance Model

8.7.1 Liberty Alliance Accreditation and Certification Model

The Liberty Alliance Identity Assurance Framework (IAF) provides an approach to establish criteria for certification and accreditation, initially focusing on Credential Service Providers (CSP) and the accreditation of those who will assess and evaluate them. The goal of this model is to provide federations and Federation Operators with the means to certify their members for the benefit of inter-federation and to streamline the certification process for the industry.

The IAF establishes the requirements that assessors must have in order to perform assessments or audits for Liberty accreditation and defines the business rules and requirements for the actual assessments. Signatories to these business rules and requirements agree that they govern the issuance, use, and validation of credentials issued by certified CSPs, the certification of such CSPs, and the accreditation of those who assess CSPs.

These requirements are being updated under the Kantara Initiative. The most recent documentation can be found on the Kantara Initiative Collaborative Site [27].

9 Conclusion and Next Steps

The Pan-Canadian Assurance model outlined in this report provides the foundation for agreement and interoperability between the federal government and the provinces. This model represents 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. To this end, the model will enable the full participation from many authoritative parties, including the federal, provincial, territorial, and municipal jurisdictions and also include commercial partners.

Much work still needs to be done, and many barriers and gaps remain. But despite these barriers and gaps, the model can be used to pave the next steps to define targeted projects for federation. By adopting a targeted approach, specific model concepts can be explored in detail. For example, pilot projects may involve applying the concepts in an operational context, or defining detailed requirements in a standard. What is learned in these pilot projects will help to address issues such as legislative barriers, legal questions or defining viable federation arrangements.

10 Glossary

This section contains definition of terms used within the document in addition to terms defined in Section 5.

Actor – an entity that can take action. Can be a principal, authoritative party or relying party.

Assurance - A measure of certainty (level of confidence) that a statement or fact is true. Assurances are typically associated with the identification of a principal and/or the integrity/rightful use of a credential.

Authoritative Party – An authoritative party is an entity whose authority to make claims is recognized by one or more parties.

Claim – A claim is an attribute (or set of attributes) regarding a principal for transactional context. Claim types are unlimited, but are typically associated with identification of a principal, organization, role and/or request context. A claim that is verified by an authoritative party is an assurance.

Client - The client is the actor who initiates an action and expects an outcome resulting from this action.

Principal - The principal is the actor that initiates an interaction and/or is subject to an outcome. The principal is typically an individual who is providing a claim or requesting a service.

Relying Party – A relying party is an entity that receives an assurance from an authoritative party.

Role – A role is a set of behaviours and/or responsibilities expected of an entity (i.e. actor). An entity may assume one or more roles.

Service Provider - A service provider is an entity that provides services to other entities. Usually the service involves formalized service agreements or contracting arrangements.

Terms - provisions that determine the nature and scope of an agreement

11 References

11.1 Canadian Public Sector References

[1] Public Sector CIO Council. *Public Sector Security Classification Guideline*. PSCIOC Review Copy, 7 September 2004

[2] Government of Alberta. *Assurance Levels*, Draft for Discussion

[3] Government of Alberta. *Identity and Authentication Standard*, Approved Version, January 30, 2006

[4] Government of Ontario. *Discussion Paper on Identity Authentication and Authorization in Electronic Service Delivery – An Ontario Perspective*, Draft Version, March 27, 2004

[5] Government of Ontario. Policy for Public Facing Electronic Identification, Authentication and Authorization, Version 8.0, March 31, 2008

[6] PSCICO/PSSDC Cross-Jurisdictional Identification, Authentication and Authorization Working Group. *Identification, Authentication and Authorization Framework Policy and Guidelines*, Release 3.0. November 26, 2004

[7] Services governementaux Québec. *Modèle de confiance pour le gouvernement du Québec*, Résultats préliminaires. Septembre 2008.

[8] Treasury Board of Canada Secretariat CIO Branch. Cyber-Authentication Renewal: Report of the future requirements of cyber-authentication for the Government of Canada, Final Version for RFI. June 2008

[9] Treasury Board of Canada Secretariat CIO Branch. *Guideline on Authentication,* Preliminary Draft. November 2008

[10] Inter-jurisdictional Identity Management and Authentication Task Force (IATF). A Pan-Canadian Strategy for Identity Management and Authentication, Final Report. July 2007

[11] British Columbia. Office of the Chief Information Officer. Identity Assurance Standard Consultation Draft, Version 0.2. April 2009.

[12] Communication Security Establishment Canada. User Authentication Guidance for IT Systems, Final Draft. March 2009

[13] Inter-Jurisdictional Identity Management Task Force. A Pan-Canadian Strategy for Identity Management and Authentication, Final Report, July 2007

11.2 International Public Sector References

[14] iDABC European eGovernment Services, eID Interoperability for PEGS. *Proposal for a multi-level authentication and a mapping of existing authentication systems.* December 2007

[15] OECD, *Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.* June 2007

[16] OMB, M-04-04. *E-Authentication Guidance for Federal Agencies*. December 16, 2003

11.3 Industry References

[17] Liberty Alliance Project. *Liberty Alliance Identity Assurance Framework*, Version 1.1. June 2008
[18] Cyberspace Law: Federated Identity Management http://www.abanet.org/dch/committee.cfm?com=CL320041
[19] Kantara Initiative. *Identity Assurance Framework: Glossary*, Version Draft 0.4. December 31, 2009
[20] Kantara Initiative. *Federation Operator Policy Guidelines,* Version Draft 0.1, October 7, 2009
[21] International Organization for Standardization, *ISO 31000:2009 Principles and Guidelines on Implementation*, November 13, 2009
[22] American Bar Association, Federated Identity Management Legal Task Force. *Identity Management Legal Issues*, Discussion Draft, November 29, 2009
[23] Kantara Initiative. *Identity Assurance Framework: Assurance Levels*, Version Draft 0.4, December 31, 2009
[24] General Services Administration (GSA), *Federal Identity, Credentialing and Access Management Trust Framework Provider Adoption Process (TFPAP) for Levels of Assurance 1, 2,, and Non-PKI 3*, Version 1.0.1 Release Candidate, September 4, 2009
[25] Liberty Alliance Project Web Site: http://www.projectliberty.org/
[26] Kantara Initiative Public Web Site: http://www.kantarainitiative.org/
[27] Kantara Initiative Collaborative Site http://kantarainitiative.org/confluence/dashboard.action