

**PSCIOC/PSSDC
Cross-Jurisdictional
Identification,
Authentication and
Authorization Working
Group**

**Identification, Authentication and
Authorization Framework Policy and
Guidelines**

- Consultation Draft –
Release 3.0

November 26, 2004

Identification, Authentication and Authorization Framework Policy and Guidelines

Release History

Version No.	Version	Date
Release 1.0	IA&A Working Group Initial Draft	July 29 th , 2004
Release 2.0	PSCIOC / PSSDC Submission	September 28 th , 2004
Release 3.0	IA&A Working Group Consultation Draft	November 26 th , 2004

Table of Contents

1.0	Introduction	5
1.1	Invitation to Comment	6
2.0	Previously at Lac Carling	7
3.0	Objectives of the Working Group	7
3.1	Out of Scope Determinations	8
4.0	Terms Used in this Document.....	9
5.0	What is Identification Authentication and Authorization?.....	10
6.0	Why is Identification Authentication and Authorization Important? .	11
7.0	General Approach to Registration and Authentication.....	12
7.1	Developing an Analytical Framework	12
7.2	The Chain of Trust	12
7.2.1	Trust Chain Components.....	13
7.2.2	Strength of Assurance for Trust Chain Components	14
7.3	Levels of Assurance	15
7.3.1	Basis for Levels of Assurance	15
7.3.2	Levels of Assurance Mapping	15
7.3.3	User Category Definition	16
7.3.4	Adoption of the NCSIP Classification Guideline	17
8.0	Risk Management.....	20
8.1	Principles for Electronic Authentication Risk Management	21
8.2	Risk Assessment.....	21
9.0	Registration and Tokening Guidelines.....	23
9.1	Enrolment vs. Registration	23
9.1.1	Two Identity Verification Models.....	24
9.2	Background for Registration and Tokening Guidelines	24
9.3	Unclassified Level	24
9.4	Low Level.....	25
9.5	Medium Level.....	25
9.6	High Level	25
9.7	Summary of Registration and Tokening Guidelines	26
9.8	Identity Verification.....	29
10.0	Authentication Guidelines.....	31
10.1	Background for Authentication Guidelines	31
10.2	Unclassified Level	31
10.3	Low Level.....	31
10.4	Medium Level.....	32

10.5	High Level	32
10.6	Credential Values and Validation	33
11.0	Identification and Authentication Guidelines Supplemental.....	35
12.0	Issues.....	36
12.1	Privacy	36
12.2	Security	36
12.3	Governance.....	37
12.4	Liability	37
12.5	Transferable Model	37
13.0	Moving Forward	38
13.1	Joint PSCIOC - PSSDC Meeting, 2004.....	38
13.2	Governance for Cross-Jurisdictional IAA	38
13.3	Privacy	38
13.4	Liability	39
14.0	In Closing.....	39
A.	Partnerships	40
B.	References.....	41
C.	Glossary.....	43
D.	Acronyms.....	47
E.	List of Figures and Tables	48
F.	Practice Assessment Statement Guidelines	49

1.0 Introduction

To deliver on service delivery transformation that is customer-focused, seamless and convenient there is an urgent need to find ways to enable interoperability between governments by recognizing and accepting electronic credentials across jurisdictions. This initiative has Federal, Provincial and Municipal governments working jointly to address common priorities and simpler, more integrated access to government information and services.

The results of this work will have broad implications for access and privacy, information classification and security, as well as being a key enabler to leverage each jurisdiction's information technology infrastructure for the secure exchange of information.

The intent of the approach undertaken for the development of this framework policy and guidelines is to leverage international and industry standards as much as possible. These are cited throughout the document as well as in Appendix C.

The framework and guidelines in this document are meant to complement legislative and regulatory requirements within each jurisdiction. The document presumes that participants involved in developing identification and authentication processes are not only aware of their obligations, but are also in compliance with any and all applicable legislation, regulations and policies within their jurisdiction.

1.1 Invitation to Comment

This consultation paper was tabled with the joint PSCIOC - PSSDC councils at the joint council meeting in Winnipeg in September 2004. This consultation draft is now being circulated to a number of key stakeholders to seek their input and feedback. Key stakeholders are invited to submit written comments about this document by December 20th, 2004 to:

Jeff Evans

Chair, Cross-jurisdictional Working Group on Identification Authentication and Authorization

I&IT Strategy, Policy and Planning Branch

Office of the Corporate Chief Strategist

Management Board Secretariat

Government of Ontario

Jeff.evans@mbs.gov.on.ca

All comments will be considered. From the compiled responses the IA&A Working Group will prepare a revised document for release in February 2005. .

2.0 Previously at Lac Carling

As a result of the input received from previous Lac Carling congresses, the Public Sector CIO Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC) agreed that a multi-jurisdictional working group (Identification Authentication and Authorization (IAA) Working Group) was required to develop common terminology and to identify, develop and propose identification, authentication and authorization standards that facilitate seamless, cross-jurisdictional electronic service delivery.

At the Lac Carling VII and PSCIOC and PSSDC meetings held in Saint Sauveur, Québec in May 2003 the governments of Ontario and Canada had presented an overview of an identification authentication and authorization framework for service delivery that is generic and transferable. This framework was intended to provide the underpinnings for further discussions on the components of IAA systems, the goal being the development of a standard that all jurisdictions could use to simplify the work to build cross-jurisdictional IA&A systems and to provide a consistent and coherent client experience.

It was agreed that the IAA Working Group would develop common cross-jurisdictional language to describe the components and related levels of trust for identification authentication and authorization systems. It was also agreed that the Working Group should recommend an on-going governance structure for the standard.

Membership to the Working Group was constructed to bring the right balance of expertise in line business, information and information technology, privacy and security from across federal, provincial, municipal interests.

PSCIOC/PSSDC gave final approval to the Terms of Reference and the Draft Work Plan on September 30th, 2003.

3.0 Objectives of the Working Group

As per the IAA Working Group's terms of reference, the ultimate objective is to develop identification authentication and authorization standards that facilitate seamless, cross-jurisdictional electronic service delivery and leverage each jurisdiction's IT infrastructure. It is envisioned that standards will be maintained by a permanent governance body.

As an interim step towards the long-term goals, the Working Group is undertaking to:

- Develop guidelines containing a common set of definitions and vocabulary for identification authentication and authorization processes for inter-

- jurisdiction application, including trust levels related to each component of the Trust Chain;
- Develop recommendations with respect to next steps, including an on-going governance structure and the role of Third Parties.

3.1 Out of Scope Determinations

During the course of its work the IAA Working Group has had to address many issues and areas for consideration. In some of these cases the Working Group has arrived at consensus that some of these issues are outside of the scope of its mandate. These are listed below:

- 1) While the IA&A Working Group is focused on technical interoperability and dealing with those end-to-end issues, the Working Group is not meant to deal with the technology specific aspects of Identification, Authentication and Authorization architectures, technologies and services.
- 2) The Working Group is not developing Threat Risk Assessments for cross-jurisdictional authentication but rather guidelines on how and when they should be used.

4.0 Terms Used in this Document

The following are definitions of key terms used throughout this paper. Additional terms are included in Appendix D.

Client	In the context of this discussion paper, a client refers to an individual or business wishing to transact with government. In the case of business it could be represented by an individual or an agent.
Credential	Evidence provided to prove a claimed identity and present related contextual information in order to access electronic resources.
Identity Proofing	A process that “proves” the identity of the client that is attempting to access information or resources. Proof is based on a set list of criteria that are previously established and measured based on Levels of Assurance.
Level of Assurance	The level of confidence in confirming an identity required for an electronic transaction. Levels of assurance are categorized by the Working Group into four levels – unclassified, low, medium and high. Further treatment on levels of assurance are found in this document.
Originating Party	A government entity that performs the original identity proofing and provides the authentication information forwarded to or shared with a relying party.
Registration	A process by which a client provides information to gain a credential for subsequent authentication.
Relying party	A government entity that relies upon the client’s credentials, as passed through by the originating party, to process a transaction or grant access to information or a system.

5.0 What is Identification Authentication and Authorization?

The rewards of electronic service delivery implementation hold great promise, not only in terms of service delivery improvement through increased accessibility, both in hours of operations and better service connections with remote regions, but also the possibility of significant cost reduction as well. However once the services provided go beyond being informational to being transactional, especially with personal information being contained within those transactions, it is imperative that the government has assurance that those clients accessing services are who they say they are. This is the role of online identity authentication.

Thus authentication is an enabler for integrated, cross-jurisdictional service delivery through multiple channels that is customer-focused, seamless and convenient. In the world of Identification, Authentication and Authorization this means:

- Creating and issuing a persistent verified electronic identity (based on assessment of evidence that has been presented to support the claimed identity)
- Establishes at the start of each online session the validity of that identity where appropriate- based on assurance level
- Grant or deny access to online information or services based on the transaction or program specific business rules of the online service

Individuals transact with government according to various roles they play (citizen, customer, driver, student, resident, employee, business owner, etc.). While each individual is a single physical entity, each individual does not necessarily have a single identity or, put another way, a single and uniform expression of identity. An electronic "identity" is merely a data construct or a series of attributes that represents an actual, physical entity in a particular context.

To uniquely identify their clients for the purposes of service delivery, government programs have generally issued program identifiers through some enrolment process. While many programs focus on Individual Authentication, i.e.: the process of establishing to an understood level of confidence that an identifier refers to a specific individual, consideration also needs to be given to authenticating the role or attribute as well.

Practically speaking all electronic transactions are merely concerned with establishing that a proffered credential refers back to an attribute such as a name or account number. The authenticated credential may not need to be linked to a

physical individual by every organization in the delivery chain for a service to be performed.

Attention to identity authentication issues is required to realize the significant dividends in terms of designing a system that delivers services to the right individual while earning the trust of the clients who use the system. The overall solution will be a combination of technical, policy, legal, physical and procedural controls.

6.0 Why is Identification Authentication and Authorization Important?

Trusted registration and electronic authentication of individuals and businesses to receive government services will become increasingly important as a vital enabler as we move to electronic delivery of government services and to integrating services across program lines.

Electronic service delivery and the promotion of service delivery transformation through the use of new technologies requires some rethinking of traditional approaches to identification authentication and authorization. There are a number of drivers that would suggest the need to collaborate and cooperate on a cross-jurisdictional basis. The key drivers are:

- a client is typically the same in multiple jurisdictions and must interact with those jurisdictions;
- that same client is a taxpayer in those same jurisdictions and there is an interest in reducing duplication of effort and investment; and,
- there is a need to increase security and reduce identity fraud.

In addition, collaborating on identity standards for authentication to respond to these drivers will leverage the shift to customer-centred service delivery, focussing on improved government services and creating a more efficient means to deliver services. To meet the customer demand (from both citizens and businesses) for more seamless services from all levels of government, it becomes more imperative to find ways to recognize and accept electronic credentials across jurisdictions and to leverage the various identification and authentication infrastructures that already exist.

7.0 General Approach to Registration and Authentication

7.1 Developing an Analytical Framework

An analytical framework under which registration and authentication guidelines can be developed, analysed and evaluated is key to enabling interoperability between one jurisdiction and another. To serve this purpose, an analytical framework was developed that contains two key components:

1. Chain of Trust
2. Levels of Assurance based on an information classification schema.

Each level of assurance, while based on the classification schema, will need to be defined in terms specific to that component of the trust chain. This means guidelines on how to assess the strength of assurance for each component of the Trust Chain.

It is clear that for cross-jurisdictional authentication to work, distributed registrations of identities must be enabled and supported. When the Trust Chain components can be provided by various sources (e.g. municipalities, Federal or Provincial Governments or the Private Sector), it is essential for the participating parties to not only agree with defined standards, procedures, and processes, but also committed to following them.

Thus, the key to interoperability is agreeing on an analytical framework that includes common vocabulary and standards that define the level of assurance for each component of the Trust Chain, but still allows for some flexibility for jurisdictions for specific service delivery design.

7.2 The Chain of Trust

The term “Chain of Trust” describes the continuum of business processes and automated steps that must be implemented to deliver electronic transactions. Trust is a function of People, Processes and Technology involved in issuing, handling, and using tokens at each step in the delivery of electronic services. The individual steps to enrol clients in a program and to deliver services to them electronically map to fundamental processes that describe the flow of a client’s information to different agents during the transaction.

Although within cross-jurisdictional initiatives there are different requirements due to differing policies or technologies, when unbundled, there is an opportunity to develop a framework for describing actions that are ubiquitous and necessary and to establish a common understanding of each component of the trust chain.

7.2.1 Trust Chain Components

All Trust Chains can be said to have the same three fundamental components. For the purpose of this paper they are:

Identification - includes the registration process (creating an electronic label or name for a person, based on the review of evidence, and creating a record of these events in a database) and tokening (providing the client with a receipt and transfers data from the registration process into a usable digital format).

Authentication - the process that establishes the validity of the user or token before allowing access to information.

Authorization - validating that a user has the right to use a protected resource (services, information resources).

Figure 1 below illustrates the continuum of business processes in providing electronic service delivery as building blocks to establishing trust.

Figure 1: Chain of Trust model presented at Lac Carling 2003

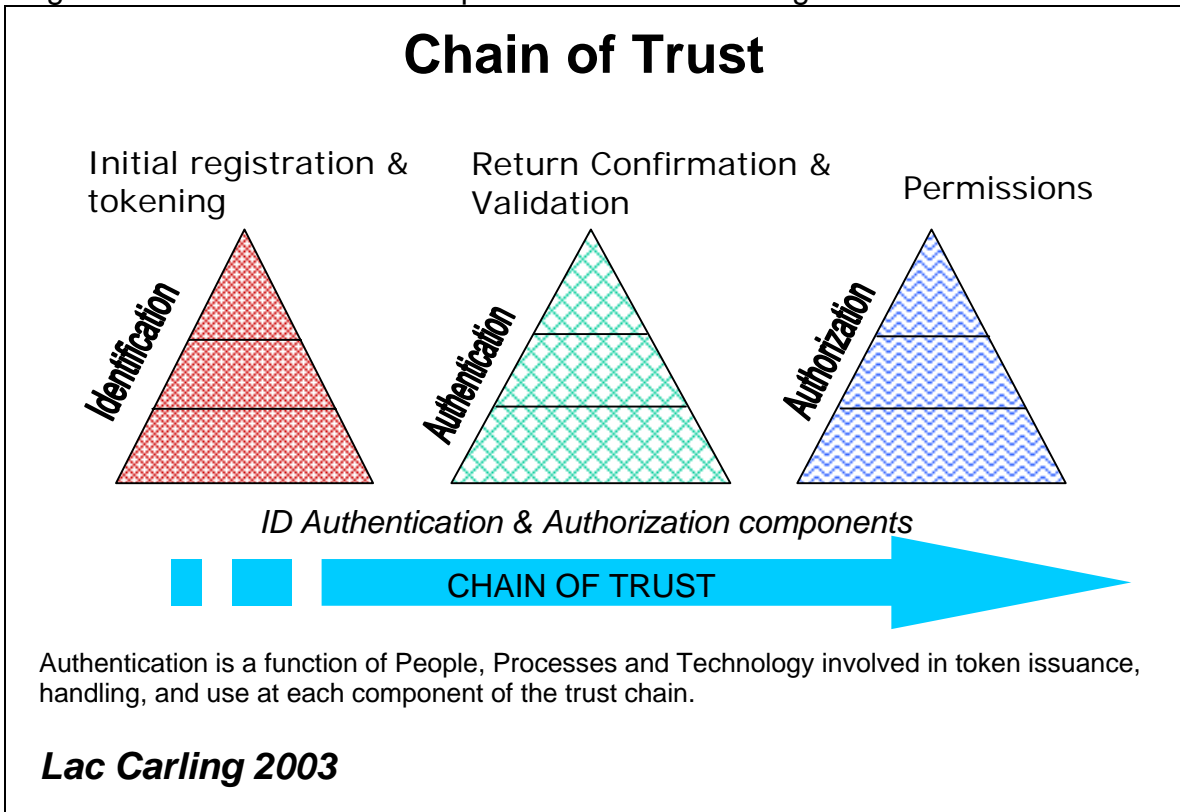


Table 1 expands upon the model in Figure 1 to describe the functionality of each individual component of the trust chain.

Table 1: Description of Trust Chain Components

	Chain of Trust Components		
	Identification	Authentication	Authorization
Function	Creating and issuing a persistent electronic identity based on assessment of evidence that has been presented to support the claimed identity	Establishes at the start of each online session the validity of the accessor before granting access to information or online services	Grant or deny access to online information or services based on the authenticated electronic identity of the accessor and on whether the user's access request conforms with the business rules of the online service
Presupposes	Registration infrastructure	technical and administrative management	locally made program or service business rules enrolment
Core Processes	<ul style="list-style-type: none"> • registration • tokening / issuance • establishing attributes • mapping • first time service registration 	<ul style="list-style-type: none"> • credential presentation • Presentation of authentication factors • Identity verification 	attribute verification
Ancillary Processes	<ul style="list-style-type: none"> • Provision to re-establish identity • Revocation • Chronicle • Shared secret set up • Attribute verification • Attestation • Audit 	<ul style="list-style-type: none"> • Revocation • Recovery • Renewal • Transaction mgmt • Long term records management • Periodic system testing • Audit 	Delegation

7.2.2 Strength of Assurance for Trust Chain Components

The level of assurance or trust in the strength of the Chain of Trust as a whole is only equal to the lowest level assigned to any one of the components, or the “weakest link”. For example, a trust chain with a strong registration component but a weak authentication component may, as a whole, be considered low in terms of its level of trust and assurance.

As a trust chain is only as strong as its weakest link, choosing a particular trust chain therefore becomes a business risk management decision. **Thus it is important to carefully analyze the actual business need in deciding the necessary level of assurance.**

7.3 Levels of Assurance

Level of assurance refers to the level of confidence or trust in confirming an identity required for an electronic transaction. The level of trust associated with an identity is determined by the level of due diligence performed during the registration process and the levels of service provided. Currently level of assurance definitions are being created independently in many jurisdictions and convergence in definitions is needed to greatly facilitate interoperability efforts.

Lac Carling indicated that to achieve interoperability, there is a need for clarity of the components of the trust chain and for cross-jurisdictional agreement on the levels of assurance for each component of the trust chain.

A prospective level of assurance framework to address these needs is outlined below.

7.3.1 Basis for Levels of Assurance

Establishing the level of confidence in an identity must be done in the context of the sensitivity of the information and services that will be accessed by the business process and the associated risk to the jurisdiction.

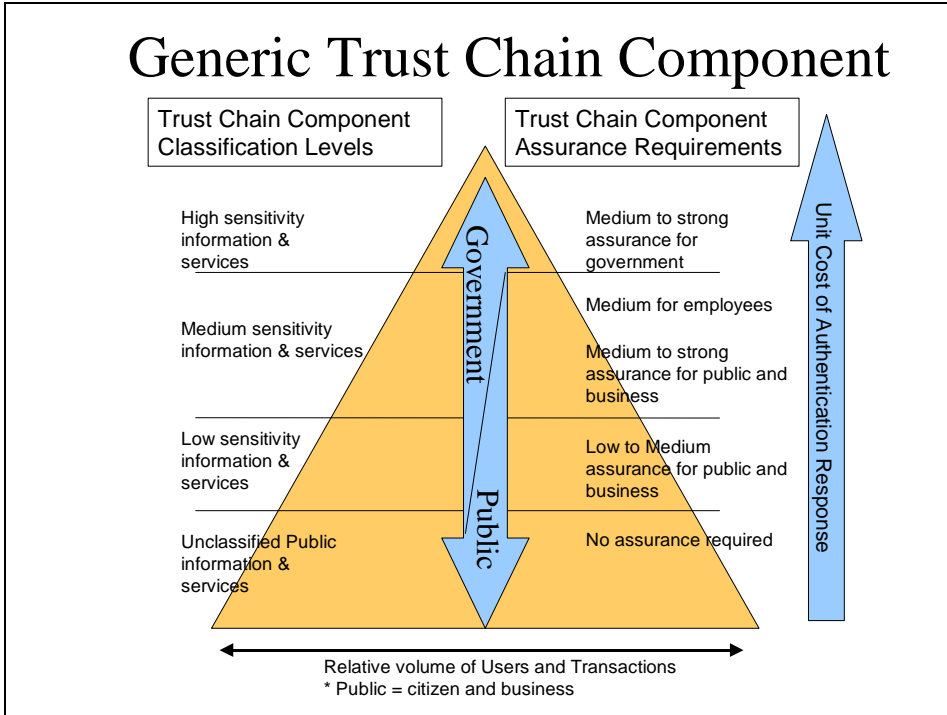
As a starting point in defining levels of assurance, the sensitivity level of the information is analysed and the risks associated with providing access to increasingly sensitive information helps to define the level of assurance required for a transaction. Thus it is the information classification schema of a jurisdiction becomes a foundation for defining its levels of assurance.

7.3.2 Levels of Assurance Mapping

There is a direct relationship between the level of sensitivity of information and services and the level of assurance classification. If information is classified at a high level of sensitivity, then accordingly, the level of assurance required for the electronic service is also high. In other words, the more sensitive the information or service, the higher the level of assurance is required to complete a transaction.

Figure 2 illustrates the relationship between sensitivity of information, levels of assurance and cost of authentication. In general, there is a one to one mapping of classification levels to levels of assurance.

Figure 2: Levels of Assurance Schematic



The authentication triangle is a simplified representation of the information produced, handled and stored, associated with the security level required for privacy and confidentiality.

7.3.3 User Category Definition

The definitions for user categories relate to the differences in their relationship with government rather than being defined user groups.

7.3.3.1 Business to Government (B2G)

The relationship between this category and the government is founded on an organization-to-organization basis rather than an individual-to-organization basis. This category includes businesses that interact with government programs and the organizations included in the Broader Public Sector (School Boards, Health Authorities, etc.). The external organization is accountable for all actions of the individual user acting on their behalf. Permissions are allocated to the individual and can be role-based.

7.3.3.2 Government to Government (G2G)

This category includes employees, contractors, business partners or other affiliates that interact with government sponsored or operated resources or applications to provide services on behalf of the government. The relationship for this category of user is between the user and the government. When information and services are being provided across jurisdictions the authority for registration will be provided through the Originating Party and associated security decisions through the Relying Party. All individual G2G users are personally responsible for their actions while using this identity however it is likely liability will accrue to government organization for whom the individual is acting on behalf of. Permissions are allocated to the individual or are role-based.

7.3.3.3 Citizen to Government (C2G)

This category includes all individuals who request or receive services from the government. These are individuals who require an identified relationship for the purpose of receiving government goods / services. The individual is individually responsible for all actions associated with an electronic identity.

7.3.4 Adoption of the NCSIP Classification Guideline

Where possible, international and industry standards have been leveraged with a view to identify commonalities among jurisdictions to facilitate cross-jurisdictional adoption of levels of assurance and ultimately, interoperability.

The IAA Working Group agreed to leverage the work already done by the National CIO Council Subcommittee for Information Protection (NCSIP) in the development of the Public Sector Security Classification Guideline. This guideline was approved by PSCIOC and is to be applied by governments on a voluntary basis to facilitate the sharing of electronic information between government jurisdictions that is not classified in the national interest (i.e. Confidential Secret, Top Secret). The NCSIP levels of assurance generally align with those of Australia, the UK and the USA.

7.3.4.1 NCSIP Unclassified Sensitivity of Information and Services

The Unclassified Sensitivity level may be appropriate for transactions where the impact of any loss, damage, or harm resulting from an error in identification authentication and authorization processes will not result in injury to individuals, governments or to private sector institutions and financial loss would be **insignificant**. At this level, little confidence in the entire process is required. The loss, damage, or harm that may result at this level is summarized in Table 2.

Table 2: Unclassified Sensitivity and Impact from Loss, Damage, or Harm

Definition	Examples
<p>Will not result in injury to individuals, governments or to private sector institutions and financial loss will be insignificant</p>	<p>The type of information, if lost, changed or denied would not result in injury to an individual or government organization</p> <p>Confidentiality example is:</p> <p>a) information of public knowledge that can be found on most government web sites and would include such information as the government telephone books, advertisements for job opportunities in the various ministries, government-wide initiatives such as Government-On-Line, public health information, job classification level and range of pay scale.</p> <p>Availability example is:</p> <p>a) certain delay to access the information is tolerable</p> <p>Integrity example is:</p> <p>a) internal information of an organization with no legal effect</p>

7.3.4.2 Low Sensitivity of Information and Services

The Low Sensitivity level may be appropriate for transactions where the impact of any loss, damage, or harm resulting from an error in the identification authentication and authorization processes could reasonably be expected to cause **significant** injury to individuals or enterprises. At this level, some confidence in the entire authentication process is required. The loss, damage, or harm that may result at this level is summarized in Table 3.

Table 3: Low Sensitivity and Impact from Loss, Damage, or Harm

Definition	Examples
<p>Could reasonably be expected to cause significant injury to individuals or enterprises including any combination of:</p> <p>a) limited financial losses,</p> <p>b) limited impact in service level, or</p> <p>c) performance, embarrassment and inconvenience</p>	<p>Confidentiality examples include:</p> <p>a) basic or "tombstone" personal information,</p> <p>b) status of a government evaluation of a company product, and</p> <p>c) unauthorized release of the job applicant's names.</p> <p>Availability example is:</p> <p>a) denial of service resulting in status of social assistance application not being available.</p> <p>Integrity examples include:</p> <p>a) information assets relating to administrative information such as volume and type of customer orders, and</p> <p>b) operational procedure assets relating to non-critical activities.</p>

7.3.4.3 Medium Sensitivity of Information and Services

The Medium Sensitivity level may be appropriate for transactions where the impact of any loss, damage, or harm resulting from an error in the identification authentication and authorization processes could reasonably be expected to cause **serious** personal or enterprise injury. At this level, high confidence in the entire process is required. The loss, damage, or harm that may result at this level is summarized in Table 4.

Table 4: Medium Sensitivity and Impact from Loss, Damage, or Harm

Definition	Examples
<p>Could reasonably be expected to cause serious personal or enterprise injury, including any combination of:</p> <ul style="list-style-type: none"> 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. 	<p>Confidentiality examples include:</p> <ul style="list-style-type: none"> a) compromise of personal medical or health information, b) information on a completed tax return form, c) information describing personal finances, d) eligibility information for social benefits, and e) disclosure of trade secrets or intellectual property. <p>Availability examples include:</p> <ul style="list-style-type: none"> a) payments of benefits to Canadians, and b) financial and management information systems. <p>Integrity examples include:</p> <ul style="list-style-type: none"> a) information assets relating to food or water supply that would not meet expected standards of quality and would not cause illness, b) information assets relating to non-emergency health care, c) financial transactions and payments, and d) information that could be used for criminal purposes (e.g., false identity or impersonation)

7.3.4.4 High Sensitivity of Information and Services

The High Sensitivity level may be appropriate for transactions where the impact of any loss, damage, or harm resulting from an error in the identification authentication and authorization processes could reasonably be expected to cause **extremely serious** personal or enterprise injury. At this level, very high confidence in the entire process is required. The loss, damage, or harm that may result at this level is summarized in Table 5.

Table 5: High Sensitivity and Impact from Loss, Damage, or Harm

Definition	Examples
<p>Could reasonably be expected to cause extremely serious personal or enterprise injury, including any combination of:</p> <ul style="list-style-type: none"> 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 	<p>Confidentiality examples include:</p> <ul style="list-style-type: none"> a) information on a police informant or witness protection subject, b) cabinet confidence, c) exploration data in the mineral or oil industry, d) information relating to a sex offender, and e) information relating to the case files of a major crime. <p>Availability examples include:</p> <ul style="list-style-type: none"> a) crisis communications during emergencies, b) essential police communications information, and c) emergency health information services. <p>Integrity examples include:</p> <ul style="list-style-type: none"> a) information systems used for testing food or water supplies that could result in loss of life or severe illness, b) information systems related to emergency health care, c) law enforcement information, d) extremely large financial transaction transfers, and e) extended loss of service resulting in the need to institute manual processes.

8.0 Risk Management

"The risks associated with electronic authentication processes should be identified, assessed and managed in a reasonable, fair and efficient manner.

Source: Industry Canada Principles for Electronic Authentication
Principle 2 - Risk Management

Determining levels of assurance related to each component of the trust chain is based on the level of sensitivity of the information or services provided during the transaction, and the associated risk. Section 7 above described four information classification levels based on potential risk of loss, damage or harm. Next, those risks need to be assessed and guidelines developed as a means to mitigate the risks.

Generally, risk management incorporates five broad steps:

1. review information and identify risks (if any) associated with it
2. evaluate the adequacy of the current controls in place to protect the information
3. identify the level of risk by conducting a risk assessment
4. identify what additional controls are needed to control the risks
5. develop an action plan to implement the additional controls.

8.1 Principles for Electronic Authentication Risk Management

The risk management process for electronic authentication encompasses a number of generic steps, including identifying risks, assessing their likelihood and impact and developing and implementing mitigation strategies.

Industry Canada developed principles for electronic authentication to help guided organizations in confirming the identities of online parties and in ensuring that electronic communications are kept confidential and unaltered. A component of these overarching principles relate to risk management and incorporate the following:

- The responsibilities of participants concerning risk management are proportionate to the degree of knowledge and control that each participant can reasonably be expected to have and to exercise
- Risks should be identified to the extent possible
- Risk should be assessed as to seriousness and potential impact. In assessing risk, special attention should be paid to where and when reliance is placed on the authentication process
- Resulting risks should be managed to the point of greatest economic efficiency by being assumed, avoided, re-allocated or mitigated
- Regardless of the means used to allocate risk, the resulting allocation should be reasonable and fair and take into account the ability of participants to manage risk and/or absorb losses. It should also create incentives for those developing and implementing authentication processes to ensure that their products and services are secure and reliable.

For further information please see the document http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html which is listed in the appendix to this document

8.2 Risk Assessment

As the risk management covers an end-to-end process, a key component within risk management is risk assessment.

Risk is the possibility that an event occurs causing unwanted results. Risk assessment is about defining a level of risk by predicting the likelihood that an identified event can occur and its impact on the parties involved. It is important to assess risks from both a consumer and government perspective. Steps to defining the level of risk are:

1. identifying what events could constitute a risk (e.g. inadvertent disclosure)
2. estimating the impact of the events (e.g. financial loss), and
3. estimating the likelihood that the event will take place.

Once risks have been appropriately assessed, levels of assurance can be assigned and controls to adequately mitigate risks can then be identified and implemented. Table 6 provides a high level summary of risk assessment factors and levels of assurance.

Table 6: Risk Assessment Summary

Level of Assurance Risk Assessment Factors				
Level of Assurance	Unclassified	Low	Medium	High
Identification, Authentication, and Authorization Threshold	Self assertion Minimal records Little / no Confidence	Some confidence Assurance for low risk, routine transactions More or less immediate access	High confidence in the asserted individuals identity Number of Authentication factors dependent on people, places, and processes also in place	Very high confidence in the asserted individuals identity
Potential Loss, Damage, or Harm	insignificant financial loss; no injury to individuals, or enterprises	significant injury to individuals or enterprises	serious personal or enterprise injury	extremely serious personal or enterprise injury
Risk Assessment Factors	<ul style="list-style-type: none"> • insignificant financial loss • no injury 	Any combination of: <ul style="list-style-type: none"> • limited financial losses, • limited impact in service level, or • performance, embarrassment and inconvenience 	Any combination of: <ul style="list-style-type: none"> • loss of competitive advantage, • loss of confidence in the government program, • significant financial loss, • legal action, or • damage to partnerships, relationships and reputations. 	Any combination of: <ul style="list-style-type: none"> • extremely significant financial loss, • loss of life or public safety, • loss of confidence in the government, • social hardship, or • major political or economic impact

9.0 Registration and Tokening Guidelines

This section describes generic requirements for registering claimants and the issuing tokens which are the basic processes of the identification component of the trust chain. The guidelines take into account the sensitivity level of the information and services provided during a transaction, as well as the associated risk. Here the focus is the strength of registration and the tokens issued through meaningful measures and proof points for business, government and personal uses.

Registration is the process of creating an electronic label or name for a person, based on the review of evidence, and creating a record of these events in a database. Registration activities can be for the sole purpose of creating an Electronic Identity or integrated with program enrolment where data is collected once, parsed and managed by different entities. Tokening provides the client with a receipt and transfers data from the registration process into a usable digital format or other formats.

Depending on the level of assurance, registration and tokening can be done in-person or remotely through various channels such as browsers, telephones, mail or on-line. Approaches to electronic transactions should employ similar strengths of assurance as well as be aligned with the standards and protocols of other channels such as telephone, paper or agent-mediated versions.

9.1 Enrolment vs. Registration

It is important to note the distinction between program enrolment and registration within the context of this document.

Enrolment is the process by which a client obtains authorization for a specific online service. The authenticated electronic identity is then recorded as having authority to engage in relevant transactions. Enrolment may also entail registration of additional information relevant to the service in question. If appropriate, asserted information may be checked against available records. A client is only required to enroll once for each service and may only use those services for which he/she/it is enrolled. Requirements for enrolment need to be set on a service-by-service basis.

Registration, on the other hand, is the process by which a claimant provides information to gain a credential for subsequent authentication. As enrolment applies to specific service or program, registration can apply to multiple services or programs that are accessed multiple times.

9.1.1 Two Identity Verification Models

Two Identity Verification models are given where trust in a real-world identity needs to be established to a level appropriate for a particular transaction:

- 1) A client registers with a Registration Authority (RA) and is issued with a credential after examination of relevant documentation. Evidence of real-world identity is securely embedded in the credential, or accessible securely *via* a look-up database or equivalent. The registration process thus establishes trust in the real-world identity of the client. This may be augmented during enrolment if further trust or additional client information is required for service delivery.
- 2) A client registers with an RA and is issued with a credential. The credential either does not contain or point to any information on real-world identity or the information is not releasable (e.g. privacy constraints prevent the release of relevant information for use other than for its original purpose). In this case, no trust is established in the real-world identity; trust would be obtained during enrolment or built up through a history of successful transactions.

9.2 Background for Registration and Tokening Guidelines

To assess registration and tokening processes two components need to be evaluated - the strength of the identification and the strength of the credentials issued to users. The strength of the identification is evaluated on the basis of the level of evidence through the type and sophistication of documents presented. The strength of credentials refers to the level of confidence in that the claimant is who they say they are.

9.3 Unclassified Level

A significant amount of government business can be conducted between external individual Users and various government programs without the need for an identity assigned or used by that user.

The unclassified level of assurance for the identification component of the trust chain is commonly assigned to transactions that require little or no confidence in asserted identity and a minimal level of evidence. Identity assertions of claimants are accepted without verification and there is no requirement to maintain a record of the facts of registration. For example, transactions of a unclassified level may be accessing information that is already public.

Successful registration and tokening does not require the claimant to prove his/her identity or that he/she controls the token. Unclassified level type transactions may be done anonymously.

9.4 Low Level

The low level of assurance for the identification component of the trust chain is commonly assigned to transactions that require some confidence in asserted identity and sufficient level of evidence in establishing the claimant's identity. Establishing the identity of claimants can be accomplished on-line and immediately for cases that are of relatively low risk and are routine in nature. For example, transactions of a low level may be requesting specific program related information.

Registration and tokening at the low level can be done in person or remotely. Low level type transactions may be done pseudonymously.

9.5 Medium Level

The medium level of assurance for the identification component of the trust chain is commonly assigned to transactions that require high level of confidence in asserted identity and a substantial level of evidence in establishing the claimant's identity.

For example, transactions at the medium level may be filing a tax return online. As well Government employees would likely need an individual electronic identity at an identity assurance level of Medium or higher to be able to carry on interaction with government applications.

This level generally requires some of the credentials or records used to validate an identity to be confirmed as valid and current. It also requires confirmation of a physical address or phone number of record or database at the time of registration.

Registration and tokening at the medium level can be done in-person, or remotely if other suitable authentication factors are in place.

9.6 High Level

The high level of assurance for the identification component of the trust chain is assigned to transactions that require a very high level of confidence in asserted identity and an extremely significant level of evidence in establishing the claimant's identity. For example, transactions at the high level may be submitting health information online.

This level requires identity proofing of identity documents that contain a picture of the applicant (and may include a background check) and a biometric (such as a photograph or fingerprint) is taken and retained on record. Applicants are required to sign their application with a handwritten signature.

Registration at the high level can only be done in person and the delivery of tokens is also linked to the in-person appearance at the site of the registration agent.

9.7 Summary of Registration and Tokening Guidelines

Table 7: Identification Practice Guidelines Summary

Level of Assurance	Registration and Tokening Guidelines		
	Comments	Remote Registration	In-Person Registration
Unclassified	Self assertion Minimal records Little/no Confidence	N/A	N/A
Low	<ul style="list-style-type: none"> • Some confidence • Assurance for low risk, routine transactions • More or less immediate access 	<ul style="list-style-type: none"> • Personal Statement (e.g. name, address, etc.) • Some currently verifiable ID (e.g. credit card, gov't ID) • Database/credit record confirmation • Close loop in token issuance by phone or e-mail 	<ul style="list-style-type: none"> • Personal Statement (e.g. name, address, etc.) • Some currently verifiable ID (e.g. credit card, gov't ID) • Database/credit record confirmation, OR • Relies on existing customer or employee relationship • Close loop in token issuance by mail, phone or e-mail

Table 7: Identification Practice Guidelines Summary continues for medium level of assurance on the following page.

Table 7: Identification Practice Guidelines Summary (continued)

Level of Assurance	Registration and Tokening Guidelines		
	Comments	Remote Registration	In-Person Registration
Medium	<ul style="list-style-type: none"> • High confidence in the asserted individuals identity • Number of Authentication factors dependent on people , places, and processes also in place 	<ul style="list-style-type: none"> • personal statement (e.g. name, address, etc.) • one primary gov't issued ID verifiable through current database check • Verify some currently valid ID (e.g. credit or bank card) and one of • evidence of established "significant" relationship, (e.g. employment, business registration) of at least one year duration; OR • shared secrets • Issue token in manner that confirms either postal address or wire-line phone number of record 	<ul style="list-style-type: none"> • personal statement (e.g. name, address, etc.) • Current gov. issued primary photo-ID verified by live records check; and one of, • significant" relationship, (e.g. employment, medical licences, substantial credit, insurance, payment of taxes, business registration...) of at least a one year duration; OR • other ID verified by live records check (e.g. credit card, student ID...) • Issue token/credentials either in person or in manner confirming either postal address or wire-line phone number of record

Table 7: Identification Practice Guidelines Summary continues for high level of assurance on the following page.

Table 7: Identification Practice Guidelines Summary (continued)

Level of Assurance	Registration and Tokening Guidelines		
	Comments	Remote Registration	In-Person Registration
High	Very high confidence in the asserted individuals identity	N/A	<ul style="list-style-type: none"> • In-person proofing only • personal statement (e.g. name, address, DOB, etc.) with third party corroboration • two pieces of documentary evidence (originals) • one primary gov't issued ID with biometric (e.g. photo) • one secondary gov't issued ID verified through current database check • biometric (e.g. photo or fingerprint) during registration • Issue token/credentials in person

9.8 Identity Verification

A key component to the registration and tokening process is the rigour attached to identity proofing. Identity proofing encompasses both the method of identity verification and the strength of the evidence used. Table 8 below provides examples of methods of identity proofing and their relative value. Table 9 below describes the types of evidence that may be used for verification.

Table 8: Overview of Identity Verification

Method of Identity proofing	Relative Value of Process
No identification (likely anonymous)	Unclassified
Claimed identity – self assertion (can be pseudonymous)	Low
Face to face (document examination no verification at source of document issuance)	Low
Knowledge of file -(shared secrets no verification to address of record)	Low
Face to Face (document examination) verification of documents -verification of documents from point of issue	Medium
Knowledge of file -(shared secrets) plus confirmation to address of record	Medium
Face to face (document examination) verification of documents plus shared secrets	Medium
Face to face (document examination) verification of documents and guarantor by trusted agent	High
Knowledge of file -(shared secrets) plus OOB to address of record and guarantor by trusted agent	High

Table 9: Testamentary Evidence for Identity Verification

Evidence that may be used for validation and verification	
For organisations	
Official registration documents	Refers to publicly available information registered with an official body.
Evidence of dealings with government	Should be recent and not publicly available
Membership of official or recognised bodies	
Trading/operational documents	Evidence is generated in the normal course of business
Third party corroboration	This type of evidence comprises information from a trustworthy third party, obtained by direct contact or as published information. The registrant should not be directly involved, apart from to give consent.
General published material	
Existing relationship	With the RA
For individuals	
Personal statement	The registrant or his/her agent provides details on his/her real-world identity and history in order to uniquely distinguish the individual and provide material to be checked against other classes of evidence. May request attributes of the real-world identity like name, DOB, etc.
Documentary evidence	Refers to documents in the possession of the registrant which fall into two main categories i) Evidence of real-world identity or ii) Evidence of 'activity in the community'
Third party corroboration	This type of evidence comprises information from a trustworthy third party, obtained by direct contact or as published information. The registrant should not be directly involved, apart from to give consent.
Biometrics.	
Existing relationship	With the RA
Shared secrets	
Closed Loop	Token issuance by phone, mail, or email address

10.0 Authentication Guidelines

10.1 Background for Authentication Guidelines

This section describes generic requirements for the four authentication levels associated with the levels of assurance. As for the registration guidelines above, these authentication guidelines take into account the sensitivity level of the information and services provided during a transaction, as well as the associated risk.

These guidelines recognize that the assurance level assigned to the authentication depends on the process and requirements for validating the accessor. This includes the type of authentication technologies or tokens used.

10.2 Unclassified Level

The unclassified level of assurance for the authentication component of the trust chain is commonly assigned to transactions that require little or no confidence in asserted identity. For example, transactions of an unclassified level may be requests for information that is already public.

Unclassified level of assurance allows for a wide range of available authentication technologies to be employed and permits the use of any token methods, including PINs.

Successful authentication does not require the claimant to prove his/her identity and may be done anonymously or that he/she controls the token.

10.3 Low Level

The low level of assurance for the authentication component of the trust chain is assigned to transactions where some level of confidence is required in the asserted identity. Pseudonymous identity proofing is allowed at this level. For example, participating in an on-line learning course may require low level authentication.

Low level of assurance allows for a wide range of available authentication technologies to be employed and permits the use of any of the token methods of Medium or High level, as well as passwords.

Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token.

10.4 Medium Level

Medium level of assurance for the authentication component of the trust chain is assigned to transactions where a high level of confidence in the asserted identity is required. For example, medium level authentication may be required when an individual or business wants to access tax records which he/she filed on-line.

Medium level of assurance allows a wide range of available authentication technologies to be employed and permits the use of any of the token methods, as well as passwords.

Authentication assurance at the medium level can require one or two factors, dependent on the relative strength of those factors. For example, authentication is based on proof of possession (for example, of a key and password) through a cryptographic protocol. The primary authentication token (secret key, private key or password) requires cryptographic strength mechanisms that protect it from being comprised.

Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token.

10.5 High Level

High level of assurance for the authentication component of the trust chain is assigned to transactions where the highest practical remote network authentication assurance is required. For example, high level authentication may be required for transactions involving health records on-line.

High level of assurance requires strong cryptographic techniques to be used for all operations. All sensitive data transfers shall be cryptographically authenticated using keys derived in the authentication process.

Authentication at this level is based on proof of possession of a key through a cryptographic protocol. This level is similar to medium level except that a tangible device (token, smart card, portable, etc) is required.

Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token.

Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant. When used, session (temporary) shared secrets may be provided to verifiers or relying parties by the Credential Service Provider.

10.6 Credential Values and Validation

As with any other component of the trust chain the strength of authentication is a function of People, Processes and Technology involved.

The three factors often considered as the cornerstone of authentication are:

- *Something you know (for example, a password)*
- *Something you have (for example, an ID badge or a cryptographic key)*
- *Something you are (for example, a voice print or other biometric)*

NIST. *Electronic Authentication Guideline, Special Publication 800-63*, June 2004

Combining two or more of these factors creates stronger authentication.

As shown in the example above, each factor can be represented by a variety of tokens which taken together become the credential being proffered for authentication.

Not all credentials are equal. Each type of credential has a relative value for the strength of its particular method of authentication which contributes to the determination of the level of assurance provided.

Thus the strength of the credential that represents any particular factor is determined by both the relative value of the credential employed and its processes of validation.

So while authentication systems are often categorized by the number of factors that they incorporate, strength of assurance is dependent not only on the number of factors employed but also on the relative strength of each.

So to arrive at credential values and validation we must use a multi-layered approach.

Table 10 provides examples of credentials that may be issued to a claimant and their relative value based on the number and type of factors used. Table 11 provides examples of validation processes for credentials during authentication.

Note: User ID is not considered an authentication credential in these examples because it is generally too easy to guess.

Table 10: Example Credentials and Relative Values

Credential Issued	Relative value of Credential
No credential	Unclassified
Password or PIN	Low or Unclassified
Strong password ¹	Low
Strong password with PKI certificate	Low
Strong password with PKI certificate having demonstrated user control of private key	Medium
Strong password and authentication token	Medium
Password and biometric	High
Strong password and hardware token with PKI certificate	High
Password and biometric with PKI certificate, and hardware token	Very High

1 = Strong password is a generic password with strong enforced password management policies and standards for example: 6-8 characters, mixed letters and numbers, upper + lower case characters, changed regularly, etc

Table 11: Credential Validation Examples

Authentication process for validating the credential	Relative value of Authentication process
No verification of credential	Unclassified
Password or PIN match	Low
Password match with retry limit and strong password edits	Low
Password match, soft PKI certificate validation	Low
Password match, PKI certificate validation – user has demonstrated control of private key	Medium
Password match, authentication ² token present	Medium
Password match, biometric validation	Medium
Password match, PKI certificate validation - hardware token present	High
Password match, PKI certificate validation - biometric match, hardware token present	High

² Authentication tokens such as smart cards, USB tokens, one-time passwords

11.0 Identification and Authentication Guidelines Supplemental

These guidelines are not intended to be comprehensive in defining “how to assign” relative values to credentials or in articulating methods of authentication to the appropriate level of assurance. They are simply meant to provide guidance to jurisdictions involved in cross-jurisdictional identification authentication and authorization.

Authentication guidelines do not function on their own, but rather, work in concert with other key components:

a) Ongoing governance with arbitration capabilities

As governments get involved in cross-jurisdictional identification authentication and authorization for electronic service delivery, there will be the need for a cross-jurisdictional governance body with responsibility for developing and revising standards to which the jurisdictions can follow and for resolving disputes as they may arise between participating jurisdictions.

Effective public sector electronic service delivery closely resembles a Business-to-Business (B2B) model of electronic service delivery, whereby discrete enterprises/ministries cooperate to develop and share common information management and technologies to defray the costs of the underlying infrastructure and improve service (AITSF, 2003). An ongoing governance body can facilitate this work.

The IAA Working Group is currently looking at the issue of governance that is expected to address cross-jurisdictional relationships and the authority of one jurisdiction to react appropriately to another. The results of this exercise will feed into the evolving cross-jurisdictional authentication architecture, product and/or service selection, and implementation.

b) Practice Assessment Statements

Practice assessment statements enable a relying party to evaluate an originating party's processes and protocols against its own in order to validate that the IAA system has achieved the required level of assurance. It is important to note that practice assessment statements do not replace the need for memoranda of understanding, legal agreements, liability clauses and audit regimes that may be put in place between two jurisdictions. Practice assessment statements merely set out the steps and requirements a jurisdiction follows for identification authentication and authorization. See Appendix F for practice assessment statement guidelines.

12.0 Issues

12.1 Privacy

The issue of privacy remains one of the single most significant and undefined, determining factors in arriving at a workable solution (or set of solutions) to implementing cross-jurisdictional authentication. It would be useful to understand the impact that privacy legislation, regulation and policies will have on designing acceptable business and technical architectures for delivering all the functional elements of cross-jurisdictional authentication. This is particularly necessary in both the Initial Registration and the Authorization/Permission Management functions of an IAA system.

In order to design architectures and evaluate solutions, criteria will need to be developed. These criteria could take the form of a set of requirements for compliance that would be used to arrive at an acceptable design or a few variations of high-level design. The evaluation of strengths and weaknesses could result in a hybrid of a number of options or a range of options that would meet the criteria.

When considering Business Clients, there are some special features that need to be addressed by a definitive review of privacy legislation, regulation and policy. These include the use of professional versus personal credentials when acting on behalf of a business entity; the need for sophisticated privilege management capability (Self-managed Delegation from the business client point of view); and the role of third party agents performing business registrations. Accommodating these requirements will have privacy considerations that need considerable analysis and are distinctly different from individual privacy concerns.

The third area affecting privacy is user acceptability. User acceptability should also be a major influence to balance against cost and policy drivers. Any sensitivity analysis will certainly need to consult business representatives to engage their perspective on what is both necessary and acceptable. Ultimately, there needs to be a balance between privacy, security and providing a level of customer service that is appropriate to the level of assurance.

12.2 Security

As with privacy, security requirements help identify levels of assurance based on a number of factors, including the information system being used, connection to other systems, information sensitivity, probability of harm and value to the organization. Security requirements must be assessed against these factors and the security applied should be commensurate to the value of the information assets to the organization and sufficient to minimize risks.

As with privacy, the level of security must be linked to the level of information sensitivity and level of assurance. Security requirements complement privacy in that they, in part, ensure that privacy and personal information are protected. Therefore, there needs to be a balance between privacy, security and providing a level of customer service that is appropriate to the level of assurance.

12.3 Governance

As previously stated, IAA systems that enable interoperability must be accompanied by an ongoing governance structure that is responsible for developing and updating standards, auditing compliance with standards and overseeing arbitration of disputes between jurisdictions.

12.4 Liability

The potential liability with cross-jurisdictional identification authentication and authorization is, at this point, unknown and will have to be examined. Given that cross-jurisdictional authentication involves multiple parties (e.g. the client, the originating party and the relying party), the responsibilities and obligations will need to be clarified and agreed upon mechanisms to address potential liabilities will need to be developed. This work should include an identification of which party is liable, to whom is that party liable and for what and under what circumstances is that party liable.

Interoperability may be impeded if responsibilities and obligations of each of the parties are not clearly defined. This will have to be accompanied by strong standards and a governance structure.

12.5 Transferable Model

Interoperability suggests a model for IAA that is transferable from one jurisdiction to another. The IAA framework policy and guidelines are intended to consist of a well-developed and uniform set of business processes for initial registration of businesses and for authentication and authorization practices. The advantage of a transferable model is that it could save partner jurisdictions from “reinventing the wheel” by repeatedly re-engineering the same set of processes. A transferable model would include common terms and perhaps broad agreement on the level of security to be provided. Eventually it would include business processes such as delegation and access by third parties, as well as agreement on the use of a uniform, unique and persistent business identifier.

13.0 Moving Forward

13.1 Joint PSCIOC - PSSDC Meeting, 2004

A presentation was made to the joint PSCIOC / PSSDC council meetings in Winnipeg on September 28, 2004 by the chair of the IA&A Working Group. This presentation outlined the progress made to date and reviewed proposed next steps. Specifically the joint councils accepted this document, entitled as *"Identification, Authentication and Authorization Framework Policy and Guidelines"*, brought forward as a deliverable as per the IA&A Working Group Terms of Reference. At the same time the joint councils approved an extended Working Group mandate to manage consultation / promulgation, and subsequent change management, to the current version of definitions and standards.

This work is underway with the broader release of this document soliciting suggestions for the next pragmatic and tactical areas to be addressed. It is anticipated that this work will conclude its next phase in early February 2005.

13.2 Governance for Cross-Jurisdictional IAA

The IAA Working Group was tasked in its terms of reference with developing recommendations with respect to an on-going governance structure for review by PSCIOC and PSSDC. To this end the Working Group has brought forward an initial paper entitled *"Governance for Identification, Authentication and Authorization"*. It is expected that any proposed cross-jurisdictional authentication governance model will need to go through several iterations due to the range of issues to be addressed and that this work will be an ongoing exercise.

13.3 Privacy

As previously stated, there is an urgent need to provide a definitive analysis that will clarify the constraints imposed on cross-jurisdictional authentication by privacy legislation, regulation and policy. The focus of this work will be on the requirements for privacy compliance. The IA&A Working Group has developed an initial discussion paper on privacy issues related to Cross-Jurisdictional Identification, Authentication and Authorization. Specifically, it aims to define the privacy issue, identify an approach to addressing the issue and proposing next steps.

While this is an overview paper, it is recognized that the issue of privacy has great breadth and complexity. Thus, it is recommended that the document be taken as a starting point for a more comprehensive and fully nuanced analysis to be conducted by an appropriate cross-jurisdictional committee with expertise on these issues.

13.4 Liability

Liability has been identified as a key issue to be addressed in order to enable interoperability. Ontario is leading the development of an issues paper that will identify the areas where liability could be incurred, the associated risks and possible models to address or limit liability. Input from the IAA Working Group will be sought as this work is undertaken. It is expected that the issues paper will be completed and presented to Lac Carling in 2005.

14.0 In Closing

In order for cross-jurisdictional identification authentication and authorization to successfully take place, there are a number of component pieces that will need to be developed, addressed and put in place. This identification authentication and authorization framework policy and guidelines document is meant to be one of those components. The framework and guidelines set out a structure that jurisdictions can follow that, when used consistently by participating jurisdictions, will enable interoperability. The standards set out in this document are neutral - politically, legally and technologically. This neutrality allows for individual programs or jurisdictions to choose what works best for them within the defined, standardized framework.

This document also identifies other key components for cross-jurisdictional identification authentication and authorization such as the need for an ongoing governance structure, privacy and liability issues to be addressed. A supplemental guideline is included outlining requirements for the development of practice statements.

A. Partnerships

As the IAA Working Group has moved forward on achieving its mandate, it has drawn on the resources with a number of parties, including:

- Government of Ontario, Management Board Secretariat (Chair)
- Government of Canada Treasury Board Secretariat
- Government of British Columbia, Ministry of Management Services
- Government of Alberta, Office of the Chief Information Officer
- Government of Saskatchewan Information Technology Office
- Government of Manitoba Information Communication Technology
- City of Winnipeg Corporate Information Technology
- City of Toronto, Information and Technology Planning
- Québec L'inforoute gouvernementale et aux ressources informationnelles
- Government of Nova Scotia Service Nova Scotia
- Government of Newfoundland & Labrador, Executive Council
- Integrated Service Delivery for Business (Ontario)
- Government Authentication Project (British Columbia)
- National CIO Council Subcommittee for Information Protection
- National CIO Council Privacy Subcommittee
- PSCIOC/PSSDC XML National Subcommittee

As the work of the IAA Working Group continues, engaging more municipalities as key stakeholders will become increasingly important.

B. References

Industry Canada. *Principles for Electronic Authentication - A Canadian Framework*, April 23, 2003

UK Government. *Modernizing Government - E-Government Strategy Framework Policy and Guidelines: Registration and Authentication*, v2.1 November 2, 2001

Management Board Secretariat. *Discussion Paper on Identity Authentication and Authorization in Electronic Service Delivery – An Ontario Perspective*, V. 1.1 March 27, 2003

Government of Canada, *Challenges and Requirements of On-Line Authentication: The “epass” Solution*, May 2003

Federal/Provincial/Territorial Council on Identity in Canada, *Identity in Canada: A Policy Framework*, Version 3, November 2002

Government of British Columbia, Office of the Chief Strategist and Government CIO, Ministry of Management Services, *Government Authentication Project, 2004*

Government of Alberta, *Government of Alberta Enterprise Architecture*, 2002

Province of Ontario, Management Board Secretariat. *Control and Risk Self-Assessment Over Information Security*, 2003-04

Government of Quebec, *Summary of Government Policies for the Authentication of People Using E-Government by Level of Assurance*, December 2003

Province of Nova Scotia, *Framework for Registration, Authentication and e-Signatures*, (Version 1.3, May 2003)

National Electronic Commerce Coordinating Council, E-sign Interoperability Work Group. *Framework for Electronic Signature Reciprocity: A White Paper Exposure (Draft)*, December 2001

Government of Canada, Communications Security Establishment. *Government On-Line PKI Identity Proofing and Authentication Guideline (Draft)*, Version 1.6, May 5, 2004

U.S. Department of Commerce, National Institute of Standards and Technology. *Recommendation for Electronic Authentication, Special Publication 800-63*, January 2004

Asia-Pacific Economic Cooperation, eSecurity Task Group. *Electronic Authentication: Issues Relating to its Selection and Use*, 2002

U.S. Department of Justice. *Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies*, November 2000

Australian IT Security. *Forum PKI Interoperability through scheme-based PKI Version 3.0*, November 2003

National Institute of Standards and Technology. *Electronic Authentication Guideline, Special Publication 800-63*, June 2004

C. Glossary

The following are working definitions of key terms used for the purposes of this paper.

Anonymous Access	Refers to access that is provided where the identity cannot be linked to a real-world identity or can be tracked.
Assertion	A statement from a verifier to a relying party that contains identity or attribute information about a subscriber.
Attribute	Information concerning the identity, privileges or rights of a participant or other authenticated entity.
Authentication	A process that attests to the attributes of a participant or entity and then attests to them to other participants in the electronic communication.
Authorization	Validating that a user has a right to use a protected resource (services, information, resources).
Certification	The administration of a measure or process designated to establish the identity of attributes of an entity.
Certification Authority	A trusted entity that issues and revokes public key certificates.
Chain of Trust	Refers to the continuum of business processes and automated steps that are implemented to deliver electronic transactions.
Claimant	A party whose identity is to be verified using an authentication protocol.

Client	In the context of this discussion paper, a client refers to an individual or business wishing to transact with government. In the case of business it could be represented by an individual or an agent.
Credential	Evidence provided to prove a claimed identity and present related contextual information in order to access electronic resources.
Credentials Service Protocol	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may include a Registration Authority (RA).
Enrolment	The process by which a customer obtains authorization to access a program or service. The authentication identity is then recorded as having authority to engage in relevant transactions. Enrolment may also entail registration of additional information relevant to the program or service.
Entity	Any concrete or abstract thing that exists, did exist, or might exist, including associations among these things (e.g. person, object, event, idea, process, etc.)
Identity	A set of information that uniquely identifies a customer to a computer system. Examples of an electronic identity are a username or digital certificate identifier.
Identity Proofing	A process that “proves” the identity of a client that is attempting to access information or resources. Proof is based on a set list of criteria that are previously established and measured based on Levels of Assurance.
Identification Authentication and Authorization	The process a jurisdiction uses to ensure a client who is accessing services remotely over the Internet is who they say they are.

Integrity	Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication or storage.
Level of Assurance	The level of confidence in confirming an identity required for an electronic transaction. Levels of assurance are categorized by the Working Group into four levels – unclassified, low, medium and high. Further treatment on levels of assurance are found in this document.
Level of Evidence	Used within the context of establishing an identity, refers to both the number of pieces of documentation and their degree of integrity and reliability.
Originating Party	A government entity that performs the original identity proofing and provides the authentication information forwarded to or shared with a relying party.
Participant	An individual or organization participating in an authentication process.
Password	A shared secret character string used in authentication protocols.
Permissions	The rights granted to an individual or entity on presentation and validation of their credentials/identity to access resources.
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g. RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Pseudonymous Access	Refers to access that is provided where the identity cannot be linked to a real-world identity but can be tracked.
Real-world Identity	A set of attributes that uniquely discriminates between clients.

Registration	A process by which a client provides information to gain a credential for subsequent authentication.
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying party	A government entity that relies upon the client's credentials, as passed through by the originating party, to process a transaction or grant access to information or a system.
Revocation	The process of withdrawing a certificate prior to its normal expiry date.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Trusted Token	A program token that has been issued as the result of the trusted registration process.
Validation	Establishing that the claimed identity exists (the attributes actually belong to a real person).
Verification	Establishing that the registrant is who he/she claims to be (rightfully possesses those attributes)
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.

D. Acronyms

B2G	Business to Government
C2G	Client to Government
CA	Certification Authority
CSP	Certification Service Provider
ESD	Electronic Service Delivery
G2G	Government to Government
IAA	Identification, Authentication and Authorization
NCSIP	National CIO Council Subcommittee for Information Protection
PIN	Personal Identification Number
PSCIOC	Public Sector Corporate Information Officer Council
PSSDC	Public Sector Service Delivery Council
RA	Registration Authority

E. List of Figures and Tables

	Page
Figure 1: Chain of Trust Model Presented at Lac Carling 2003	13
Figure 2: Levels of Assurance Schematic	16
Table 1: Description of Trust Chain Components	14
Table 2: Unclassified Sensitivity and Impact from Loss, Damage or Harm	18
Table 3: Low Sensitivity and Impact from Loss, Damage or Harm	18
Table 4: Medium Sensitivity and Impact from Loss, Damage or Harm	19
Table 5: High Sensitivity and Impact from Loss, Damage or Harm	20
Table 6: Risk Assessment Summary	22
Table 7: Identification Practice Guidelines Summary	26
Table 8: Overview of Identity Verification	28
Table 9: Testamentary Evidence for Identity Verification	29
Table 10: Example Credentials and Relative Values	33
Table 11: Credential Validation Examples	33

F. Practice Assessment Statement Guidelines

[placeholder]