

Discussion Paper on

**IDENTITY AUTHENTICATION AND AUTHORIZATION
IN ELECTRONIC SERVICE DELIVERY -
*An Ontario Perspective***

May 5, 2003

Office of the Corporate Chief Information Officer
Management Board Secretariat
Government of Ontario

Version 1.2

IDENTITY AUTHENTICATION AND AUTHORIZATION IN ELECTRONIC SERVICE DELIVERY- *an Ontario Perspective*

PREFACE

Governments across Canada face a number of complex challenges in supporting the primary or core businesses of government while promoting service delivery transformation through new technologies. Ontario has committed to a customer-centric approach to service delivery, which requires the integration of electronic services across organizational and jurisdictional boundaries.

A critical part of this service transformation concerns the development and introduction of policies, procedures and technologies that ensure the authentication of all relevant components of an electronic service transaction. The task does not involve just finding and implementing technology to address a need. It also requires a coherent policy framework that is mapped to business processes.

At the 2002 Lac Carling meeting, the Ontario Corporate Chief Information Officer made a commitment to contribute Ontario's thinking toward a national strategy on identity and authentication, to be presented at the 2003 Lac Carling meeting.

This paper will outline how Ontario is implementing its strategy for identity authentication and authorization in electronic transactions by:

- describing the fundamental building blocks of an electronic service transaction - that we have termed the **CHAIN OF TRUST** - to facilitate our discussions about service integration;
- illustrating how the Chain of Trust is integrated with an **INFORMATION CLASSIFICATION SCHEMA** to identify the levels of assurance required of each building block of a service transaction;
- providing examples of how the Chain of Trust has been applied in some of **OUR INITIATIVES** in Ontario.

Lastly, we will discuss **NEXT STEPS** that we must address in our individual jurisdictions and collectively to ensure that authentication and authorization processes continue to evolve in support of electronic service delivery.

Table of Contents

THE CHALLENGE	4
A. The Service Imperative	4
B. "Identity" in an Electronic Environment	5
OVERVIEW OF ONTARIO STRATEGY FOR IDENTITY AUTHENTICATION & AUTHORIZATION	7
THE FUNDAMENTALS	8
A. The Chain of Trust.....	8
B. Information Classification	13
C. The Analytical Framework.....	16
EXAMPLES AND ANALYSIS	22
A. Trusted Registration	22
B. Visa 3D Project	23
C. Registration, Authentication and Authorization (RAA)	25
D. Government of Ontario Public Key Infrastructure (GO-PKI)	27
E. Electronic Service Delivery for Individuals (ESDI)	29
F. Summary of Ontario Examples	31
G. The Integrated Security Interface (ISI)	33
FINAL THOUGHTS	35
PROPOSED NEXT STEPS	37
Appendix A - OTHER MODELS	38
Appendix B – Background on Registration, Authentication & Authorization Common Components	40
Appendix C - ANNOTATED BIBLIOGRAPHY	50

THE CHALLENGE

A. The Service Imperative

The Ontario government has been examining all aspects of improved service delivery to the public over a number of years. The Framework for Action 2000 outlines the plan for becoming a more customer-centered government. A key part of that plan is integrating service delivery by providing individuals and businesses with greater choice in how, when and where they access routine, high-demand government services and products. The emphasis is on “walking a mile in the customer’s shoes”, so the elements of customer autonomy, protection and choice are paramount.

While this alone would be a major undertaking in a single business or ministry, in Ontario we are deliberately restructuring service delivery away from ministry-based silos, focusing instead on “clusters” or groups of related programs with common business objectives, customers and transactional activities. This requires significant business re-engineering and new approaches to governance and accountability.

We also want to contain the costs of I & IT by carefully documenting the business architectures of our various business units in order to achieve a greater degree of standardization in approach, commonality of infrastructure and re-use of data where possible.

Historically, Ontario residents transacted with government through extensive counter service operations, supplemented by standard forms and mailed responses, and telephone service operations. Originally, when a person applied for a service his or her identity was taken for granted at face value, and a signature counted for something. More recently, we have moved to back this up with other forms of identity verification, either by asking to see a driver’s license or some proof of address, or in rare cases a birth certificate. However, time and costs have risen as authentication requirements have increased.

While this system of “authentication” appeared to suffice for many years, it was somewhat ad hoc and inconsistent. There are also reports showing how fraudulently obtained or counterfeit government documents contribute to identity theft. As we build on this authentication structure to develop e-government systems, it is important to remember that proofs of identity in current government systems are various and not necessarily reliable.

Over-the-counter approaches to service delivery are conditioned by Charter rights and provincially legislated privacy and access requirements. Fundamental to these rights are limitations on the collection and disclosure of personal information.

The shift from a known environment of bricks and mortar and paper-evidenced transactions to the new frontier of the internet requires new forms of prudence and diligence to ensure that we, our partners and our customers are in fact dealing with our respective digital representations, and not those of hackers and impersonators. The strength of assurance in service transactions and the accountability for them will need to be consistent across new and traditional channels, any of which our customers can choose at any time.

B. “Identity” in an Electronic Environment

It is also important to be clear about what we mean by the term “identity” when referring to processes such as identity authentication and registration. Individuals and businesses will legitimately have a variety of different relationships with various governmental organizations and programs. We need to remember this when we assign identity “labels” to individuals who are transacting with us in the context of each specific relationship.

A given individual may transact with government in a variety of roles:

- as a citizen engaging the government in a policy consultation or political context,
- as an individual customer executing a simple commercial transaction such as purchasing information,
- as a resident of the jurisdiction receiving public services,
- as an employee,
- as a business owner or officer transacting as a representative of the business.

Since people transact with government according to the various roles they play, the expression of their identity will vary depending on the role. 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. Entities are always singular and they exist in the real world. An “identity” however, is merely a data construct or a series of attributes that represents an

actual entity in a particular context and by extension an “identifier” is simply data signifying an identity.

Though our information systems may presume that each entity has a single identity, individuals perform multiple roles in the real world and their respective “identities” are often specific to the role they play. In fact, these distinct roles are often determined by government business functions. For example, while a passport attests to the citizenship status of the passport holder, a hunting and fishing license certifies only the bearer’s permission to hunt and fish, and a name and address provided to a government bookstore signifies only a fulfillment address, not the identity of the purchaser.

Government programs and services have traditionally treated the expression of an individual’s identity as context dependent – by establishing separate program registration functions and issuing program specific identifiers. From an information privacy standpoint, understanding that identity is contextual has ensured that we collect only the minimum amount of identifying information that is strictly necessary to effectively enable a particular transaction.

In Canadian law, and in common law countries generally, people are not precluded from expressing their identity in multiple ways or from using aliases - a not uncommon practice among celebrities or among those who need protection from others. While some people may adopt an alias with criminal intent, most people express various identities for entirely legitimate reasons that reflect the different roles they play. And in some situations governments must preserve the right of people to act anonymously, particularly in contexts such as citizen engagement where anonymous free speech is important.

In addition, governments must consider the special features of business to government services. In these transactions, the creation and use of someone’s professional electronic identity has different requirements than transactions involving his or her personal electronic identity. A business is a legal entity, but many different individuals or third party business entities can represent it. Put another way, one individual may be responsible for interacting with the government on behalf of one or more businesses. Each business entity should be able to manage (invoke and revoke) the delegation of agents who can act on its behalf, not the government.

Whether government information systems and processes will accommodate these realities, or deny them by assuming all individuals have only one

legitimate identity expression that is independent of context, and that this “single” identity must be universally and uniformly applied across our information systems, lies at the core of the privacy challenge before us. The source of this dilemma may be in the fact that the language of information architecture does not have metadata descriptions that reflect the various identities and identifiers a single entity may have.

Though these distinctions regarding “identity” are important, they are subtle and context dependent, and for that reason we won’t include them in the following general discussion that describes the three components of the Chain of Trust.

OVERVIEW OF ONTARIO STRATEGY FOR IDENTITY AUTHENTICATION & AUTHORIZATION

Simply put, our strategy is to build levels of authentication assurance into electronic service delivery systems that are consistent with over-the-counter (OTC) assurance levels and are appropriate for both the sensitivity of the information involved, the nature of the service being offered and the service delivery channel.

Ontario intends to test this strategy within Ontario and with our partners, with a view to elaborating this approach into a robust policy and service delivery framework once we are comfortable that we’ve got it right.

To guide us through these challenges, Ontario has started developing a framework for identification and authentication that includes:

- clarity about the components of the trust chain;
- guidance on how to assess the strength of assurance in any particular component;
- how to use business risk assessments to determine the level of assurance required for identification and authentication.

The basic premise underlying this framework is that a de-centralized approach is more compatible with the current legislative context where individual programs or jurisdictions have the flexibility to choose what works for them. The key to interoperability is agreeing on a common vocabulary or standard that defines the level of assurance for each component of the Trust Chain. In this environment, individual pieces of the identification and authentication puzzle

can come from various sources (municipal/provincial/federal/private sector), as long as the receiving party agrees with the level of assurance that the token reflects. We believe this pragmatic approach will give our clients and us the greatest degree of choice, flexibility and economy in meeting our business needs. We believe this approach could also provide the basis for a discussion at the federal-provincial level where there is interest in exploring interoperability issues.

The remainder of this paper will describe Ontario's strategy for Electronic Identity Authentication and Authorization and how it is being implemented with a view to stimulating discussion and possible joint action toward developing a national strategy. We anticipate that the application of these concepts will not lead us to a single solution or a one-size-fits-all response to the challenge of electronic identity authentication. Rather, this approach will likely result in a range of authentication infrastructures and processes, each of which is tailored to the specific business need and risk tolerance of participating programs and services.

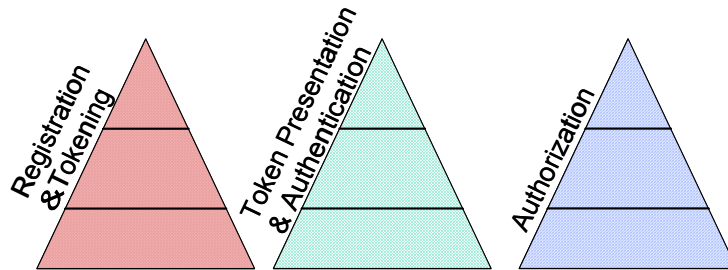
Key analytical tools in Ontario's strategy include the "Chain of Trust" and an Information Classification framework that help us think about the business processes involved in authentication and authorization and the level of assurance required. We are testing these fundamental "building blocks" in some key areas within the government. These initiatives will be described shortly, along with recommended next steps for discussions at the federal-provincial level.

THE FUNDAMENTALS

A. The Chain of Trust

Our authentication processes are modeled on a "Chain of Trust". It is composed of three discrete and independent components that are carefully linked together. These are:

- Registration and Tokening
- Token Presentation and Authentication, and
- Authorization.



The Chain of Trust model is rooted in the same rudimentary elements as any paper-based system. The elements include, firstly, the basic functions of registering identity, secondly providing a receipt or “token” of registration to verify whether an identity is known (registered) and thirdly, the final step of authorization which effectively empowers the customer to transact electronically. The model, at this level, does not represent any government program or private sector service. The term “Chain of Trust” is simply a metaphor to describe the continuum of business processes and automated steps that must be implemented to deliver electronic transactions. All or some of the activities making up the chain can be provided by the business itself or by a third party on behalf of a particular business.

The Trust Chain applies equally in the paper and electronic world. However, in the paper-based world, a large measure of trust has been placed in traditional business systems and over-the-counter services where customers may be familiar and where we expect the mail to be delivered to the right person. In electronic service delivery the security risk changes dramatically with the removal of the physical presence of one or more of the parties involved in the transaction. Digital information is also inherently easy to copy, alter, steal, transmit or delete.

In this regard, the Ministry of Consumer and Business Services in Ontario is working with a national committee on issues such as the proliferation of false “root” or “breeder” identity documents such as birth certificates and driver’s licenses that are used to acquire other documentation. These documents continue to be critical to any electronic identity initiative. It is these documents that provide evidence of identity at the assurance level required for the registration component - any weakness here weakens the electronic identity itself and weakens the overall assurance level of the trust chain.

Other factors that affect the reliability of the trust chain and its applicability include the integrity of the business processes including staff error or malfeasance, technological integrity, business and technology overhead costs and end user or sponsor manageability of processes, tokens and technologies. In addition, our system design choices will have policy implications for privacy, security and other matters such as the role of the private sector.

Table 1 provides definitions and a functional description of the core elements of the trust chain. Readers should note that the descriptions do not relate to specific products or Ontario government projects. They are just for illustration.

Table 1 - Chain of Trust Elements: Functional Descriptions

Registration and Tokening
<p>What is it? 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 registration 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.</p> <p>How is it done? Electronic Identity counter-based registration for a previously unknown person would involve the collection and scrutiny of paper or other electronic credentials. The result would be the entry in some data base(s) of a unique customer record and unique electronic identifier (token) for use in the trust chain. Only some applications like staff PKI will require this unique record to contain the subscriber's common name.</p> <p>The objective of "tokening" is to provide accepting parties in future transactions with the ability to recognize that the Electronic Identity offered in an electronic transaction is one which has been accepted through a "trusted" registration function. Examples include digital certificates, user ID, passwords, cookies, biometric templates, or data resident on a device like a smart card.</p> <p>Variations: A known person such as existing business customer can demonstrate enough confidential knowledge to prove his "identity" in a customer context. An Electronic Identity can be added to the customer registry or the data transferred to a separate Electronic Identity registry like the one described above.</p> <p>Considerations: In some cases, an unknown person can register without proof of identity for an anonymous Electronic Identity in order to utilize a trust chain for non-sequential electronic transactions, such as customizing a portal.</p>

Token Presentation & Authentication

What is it? A process that establishes the validity of the user or token before allowing access to information.

How is it done? An automated system sends information from the token and/or the user to an appropriate library that contains some of the registration data. The objective is to determine whether the token or user is in “good standing” or not.

Variations: User's possession of a valid token may be all that is required to grant access rights, e.g. when the user receives a session cookie.

Considerations: The provision of a persistent Electronic Identity is a pre-condition for moving to the next step, authorization.

Authorization or Permissions Management

What is it? Authorization is the stage when the business decision to grant access or privileges like read, write, delete, are matched to the user's authentication token. It is the step that applies the business rules to the client's permissions within the program domain.

How is it done? After registration and tokening, each accepting party often needs to create and bind a list of permissions that relate to the privileges the bearer of the Electronic Identity has in their transaction process or I&IT system.

Variations: This business specific index of read, write, delete functions may be stored only at the user program level, or can be centrally managed by the party performing registration and tokening.

Considerations: Centralized or localized permissions management is a design choice reflecting process requirements and external constraints such as privacy requirements.

Each of the above components is dependent on completion of the previous component. The level of assurance or trust in the strength of the Trust Chain as a whole is only equal to the lowest level assigned to any one of the components, or the “weakest link”.

For example, a chain with a strong registration activity requiring four pieces of primary identification that are validated at source, including two trusted

guarantors of an ID photo, but which issued only a simple password as an authentication token would rank very low over-all in its level of trust and assurance.

Similarly, a trust chain that accepts online registration in the form of self declaration, without source validation or data verification, but issues a user ID with strong password and digital certificates using FIPS 140 products with top level cryptography in which to house the authentication and authorization components, could not be seen as ranking at the highest level in strength of assurance regarding the Electronic Identity provided.

Ontario has found that the registration component, particularly for unknown persons is the most labor intensive and costly where medium to high assurance levels is required. For the authentication component, where digital certificate issuance, control and back up are part of the authentication activities, the cost of security hardening and ongoing protection can also be significant.

Generally speaking, if registration activities across two or more businesses are equal in strength, a chain that uses the authentication and authorization components of the major PKI systems are more reliable, and more costly. Reaching a determination about the relevant strengths of one chain over another requires detailed evaluation of each component on its own as well as the linkages between them.

On a practical level, since many electronic transactions are form filling with an all or none acceptance of the Electronic Identity and transaction data, models could evolve where no authorization function is included at all in the Trust Chain.

Choosing a particular trust chain for a business is a business risk management decision. This underscores the importance of carefully analyzing the actual business need in deciding the necessary level of assurance for each component of the chain when implementing electronic service delivery. Determining actual business need will involve a combination of the information classification considerations, the usability of the trust chain components from a customer perspective, and cost for the program and for government as a whole.

B. Information Classification

To address the need in the Ontario government for a common approach and common language for assessing business risk levels and potential solutions, we have been working on an Information Classification Framework to inform our IT Security planning and implementation efforts. This is one of the foundations of our Electronic Identity strategy and architecture-based approach to I&IT development.

The sensitivity of the information being exposed generally drives the stakeholder risks associated with any business or service. The Information Classification Framework guides employees to use consistent, convenient labels for information and documents to promote the implementation of reasonable security measures.

Ontario's Information Classification Framework approximates for a business or group of similar businesses the strength of assurance that will be required in any Electronic Identity initiative for those businesses.

Putting the two concepts together - the Chain of Trust and the Information Classification Framework - gives us a **Pyramid of Trust** that enables a ministry or ministry program to identify the Level of Assurance in the Chain of Trust that they should have to address their assessed level of information sensitivity (high, medium or low). The Pyramid of Trust (Figure 1) helps us look at the Level of Assurance for the Chain of Trust as a whole. As stated earlier, that Level of Assurance is established by the strength of the individual elements that make up the Trust Chain. The Pyramid makes no assumptions about what, or who, provides a given component. What is important about the Pyramid is the ranking of different offerings according to the level of assurance.

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

The Levels of Assurance on the vertical axis range from "no authentication required" at the base in response to a classification outcome of "public", up to high Levels of Assurance at the top of the pyramid according to the assessment that there is a high degree of risk with the information.

The wider base of the pyramid reflects the notion that currently the majority of public-to-government transactions, such as information dissemination, require no Identification Authentication of the client.

Following the Pyramid of Trust is a table that describes the Information Classification Framework and includes our perspectives regarding the potential user groups, size and activity levels.

Figure 1 - Pyramid of Trust

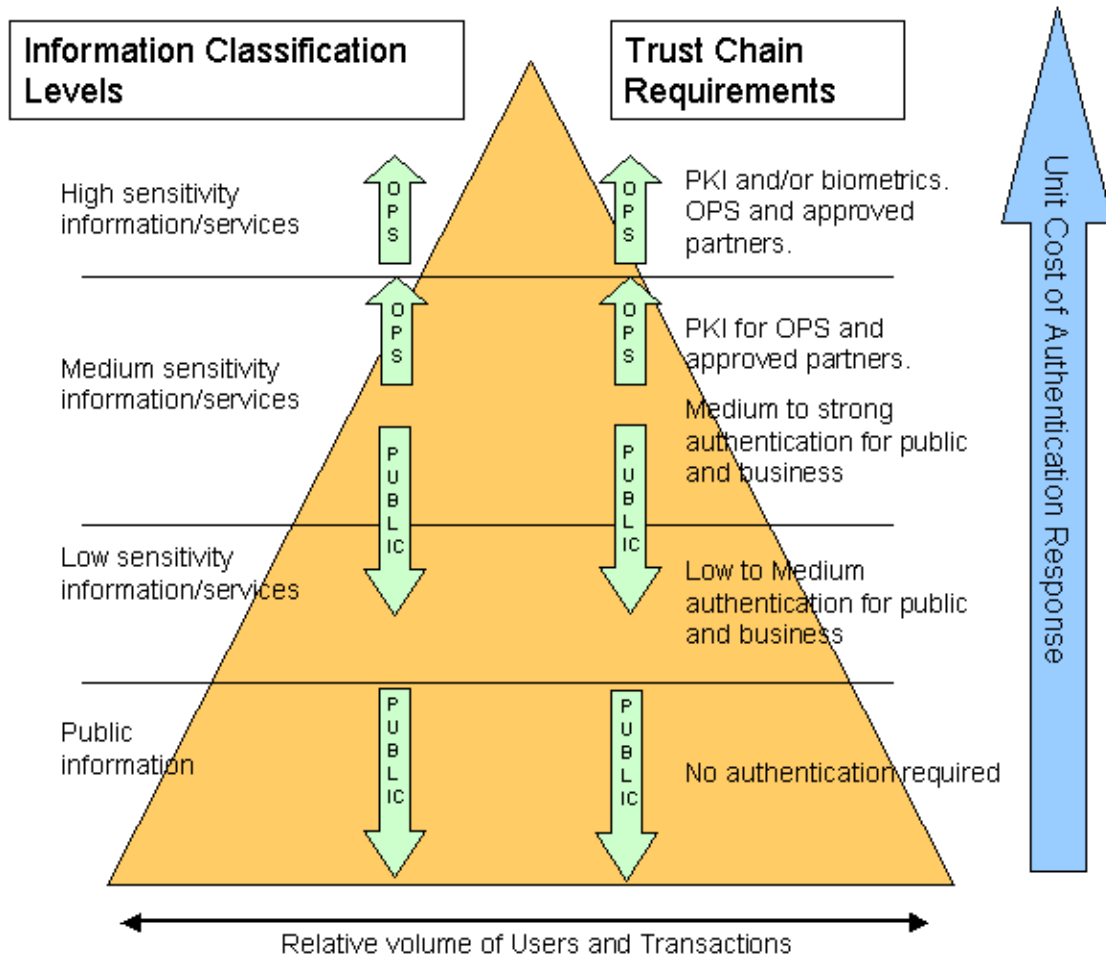


Table 2 - Information Classification

Information Classification Category	Definition	Electronic Identity customer Group potential, Asset examples	Electronic Identity product types
High sensitivity information and services	Loss or corruption could cause <u>extremely serious</u> personal, enterprise or public safety injury, economic loss, social hardship, political impacts.	Restricted access to designated PS Employees on a need to know basis only, e.g. Cabinet or law enforcement data Small number of users/transactions	PKI and/or Biometrics for PS employees only.
Medium Sensitivity Information and services	Loss, theft or corruption could cause <u>serious</u> personal or enterprise injury, economic or damage to reputation.	Public & business has access to information about themselves only. Personal and confidential business data. <100,000 PS users 11-17 million users with low annual transaction volumes	Medium to Strong authentication (PKI) for PS employees that allows viewing selected citizen information by authorized PS employees for mandated service delivery programs. Medium to Strong authentication for public and business that allows authenticated public and business users ability to access own records only.
Low Sensitivity Information and services	Loss, theft or corruption could cause persons or enterprises injury, financial loss, damage to reputation	Public and business have access to government services that may require registration and limited protected personal information like shipping addresses for order fulfillment, email distributions. 11-17 million users with low transaction volumes	Low to Medium authentication for public and business with ability to access published information and own fulfillment order information
Unclassified or Public Information Information that contains no sensitive or personal data and is meant for public availability.	No injury anticipated	Any person, with or without identification. Published documents 11-17 million users with varied average annual transaction volumes	No Electronic Identity authentication but may require financial payment authentication where fees apply

C. The Analytical Framework

Drawing from the Chain of Trust and Information Classification framework, we can construct a basic analysis framework for assessing the strengths of the components in any Chain of Trust. Similar frameworks may evolve in the future regarding other selection criteria on the vertical axis of the Pyramid of Trust, including privacy driven by PIA's, user acceptance, integration with portal structures, etc. Over time we anticipate the application of sound analysis and enterprise architecture principles will provide us with additional frameworks for analysis that will address a variety of dimensions or attributes relating to the selection of Electronic Identity systems.

For now, Table 3 presents some examples of trust chain components at three different Levels of Assurance. The overall level of assurance of the Trust Chain shown in the left column of Table 3 would match up with the Information Classification determination of high, medium or low sensitivity information. The component options for a Trust Chain that achieves a medium level of assurance, for example, is determined by reading across the row from left to right.

Table 3 - Sample Trust Chain Components at Each Level of Assurance

Estimated Component Strength	Registration and Tokening	Token Presentation & Authentication	Authorizations Permissions Management	Notes
HIGH	<ul style="list-style-type: none"> - Counter based, several photo ID, ID documents from set lists, guarantors checked, biometric samples. - Document numbers verified with issuer. Check credit or employment history. - All registration records copied to ID registry file, random checks over time. - Accountability agreement signed. 	<ul style="list-style-type: none"> - Biometric and/or high strength certificate embedded in crypto card as access requirement to facilities, PCs or networks 	<ul style="list-style-type: none"> - Controlled and managed by application owner in-house - Uses certified products 	<ul style="list-style-type: none"> - All business, HR, computer networks facilities 'hardened' to max security standards, e.g. FIPS 140 or above, all components verified and periodically audited.
MEDIUM	<ul style="list-style-type: none"> - Counter based, several photo ID, ID documents from set lists, document numbers recorded. Document numbers verified with issuer. - Periodic updates via paper or electronic means. - Accountability agreement signed. 	<ul style="list-style-type: none"> - Electronic certificate with limited access to user information or master repository, paired with User ID and strong password with enforced password standards, e.g., change frequency and length. - Distinct strong User ID-password combination to access centralized certificate or 3rd party "signed" ID validation message. 	<ul style="list-style-type: none"> - Managed by application based on policy or by service bureau according to agreement and policy. - Uses custom-built or uncertified products (software/hardware) 	<ul style="list-style-type: none"> - Key staff, e.g. CA operations, at high security level - All other components meet or exceed medium security requirements
LOW	<ul style="list-style-type: none"> -Paper based or copied from other sources such as existing customer lists or staff directories, LDAP, X.500. -Self-enrollment screens with no recording of registration data. - Potential to allow pseudonyms or anonymous IDs - Accountability declaration (not signed) 	<ul style="list-style-type: none"> - Token linked to log on security process or a distinct User ID-password combination. - Low strength ID-password combination (easily guessed or unmanaged) - Cookies 	<ul style="list-style-type: none"> - Nominal, to set display formats - Binary decisions (yes/no) to submit information to back office systems for processing or actions. 	<ul style="list-style-type: none"> - Nominal or standard office requirements.

Our work to date on this mapping of Trust Chain requirements to the Information Classification Framework demonstrates that there is an inverse relationship between the Trust Chain requirements and the complexity of issues that need to be addressed at a particular level of assurance. This is illustrated in Figure 2 below.

As we have seen with the Pyramid of Trust, we can select a level of assurance that is appropriate to the information sensitivity and our assessment of the business risk - ensuring that we assess business risk from both a consumer and government perspective. When in combination these indicate a low level of assurance requirement, the technological, legal, and policy issues and administrative overhead are relatively manageable. However, the threat/risk models change as the required level of assurance rises through Medium to High - transaction complexity and costs increase while the projected number of users fall.

Outside of law enforcement domains, we have not yet documented the business requirements for high assurance trust chains for transactions involving individuals as citizens or consumers. These may be developed in the future. For example, transactions involving the transfer of highly sensitive medical information may require a high level of assurance environment. Assuming that the Registration components of the inter-linked trust chains are equivalent, we can look at a number of options including:

- PKI managed by a specialized or dedicated Certificate Authority (CA),
- biometric templates stored only with the application provider such as voice based technologies,
- cryptographic smart cards, or
- multi-factor authentication using several of the above in combination.

A security paradox emerges with high assurance applications. While a generic CA may be cost effective in supporting low to medium assurance PKI applications, a dedicated CA with the least number of subscribers, businesses and transactions accessing an unlisted CRL or a CRL that uses only device certificates, provides much better security - at higher cost - for high assurance applications. These higher costs would include non-monetary factors such as enhanced consumer registration, use of a dedicated ID/PIN in lieu of a single sign-on for many services with varied trust requirements, less ubiquitous access, and similar minor inconvenience to achieve the level of security and trust required.

In practice, quantifying business risks will be as challenging as selecting the

correct technological response. Some business owners or groups may initially self identify the business needs as requiring a high assurance standard for electronic transactions. On occasion, this perception may be affected by media stories about security breaches and persuasive vendor marketing.

However, when a rigorous evidence-based analysis is performed, the level of assurance requirements may be quite different. Quick comparisons against industry standards or cross channel practices may help with preliminary assessments. For example, if electronic banking and securities transactions are conducted with ID/PIN combinations, or client stored cookies, then government transaction risks will have to be demonstrably higher to justify more elaborate and expensive authentication tools.

As well, complex technological approaches to high assurance electronic transactions may be seen as illogical if telephone, paper or agent-mediated versions of the same transactions do not employ similar strengths of assurance.

In addition to these business requirements, services to individuals must also comply with additional legislative and policy requirements, particularly as they relate to personal information. Consequently, schemes that were originally designed for intra-organizational, professional or commercial use may prove to be inapplicable to individual to government transactions.

Ontario's Information and Privacy Commissioner published a report in December 2002 entitled **Concerns and Recommendations Regarding Public Key Infrastructures for Citizens**, in which a number of requirements are articulated. While our respective privacy statutes may vary, and not all jurisdictions take identical approaches to privacy law enforcement, Dr. Cavoukian's report and the views of other privacy commissioners will inform the analysis and reaction by citizen groups to any authentication scheme adopted in Ontario or potentially across Canada.

Highlights of the IPC 's position include;

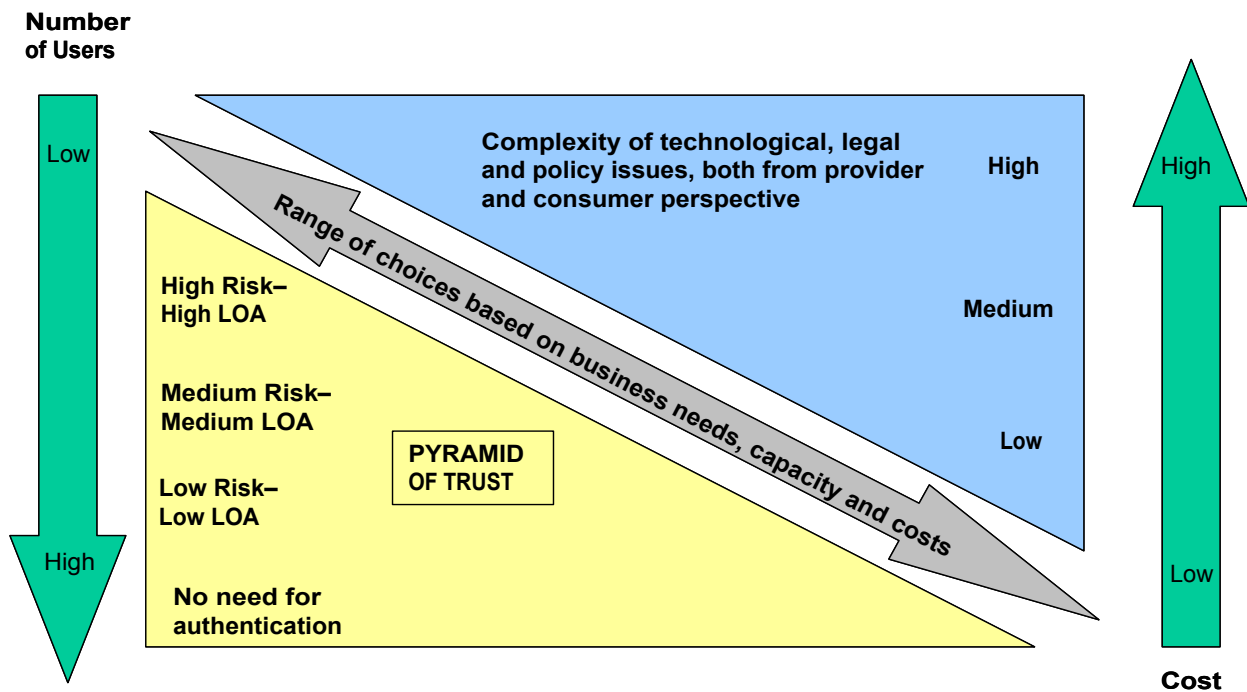
- the need for a legislative base to mandate PKI operations including roles of all parties,
- mechanisms to ensure there is no capacity for linkage of different digital certificates or role certificates linked to a primary certificate,
- citizen interactions must not be coerced in terms of "no certificate no service",
- separation of digital certificate registration information from program registration information,

- a legislatively independent operational authority and an independent oversight body with audit capacity regarding the operational authority.

Clearly we are working in a very complex and interconnected environment based on the juxtaposition of legislation and policy, business types and transaction needs, and authentication options and their costs.

Ontario's goal is to document and standardize our options to allow us to create, purchase and re-use approaches and tools to enable us to optimize choices against requirements. This is depicted by the gray diagonal in Figure 2.

Figure 2 - Levels of Assurance & Implementation Complexity



The size of this gray diagonal arrow is misleading in terms of the effort that will be required. So far, we have discussed the connotations of the Pyramid, i.e. the inverse relationship between the volume of individual users/number of distinct transactions on the one hand and the costs and complexity of trust chains required for high sensitivity assets on the other.

In practice, these connotations apply to each *distinct component* of the trust chain. To move forward on developing business driven electronic supports we need to carefully evaluate and describe the strength of assurance of each component relative to the requirements of each business. This is sometimes

referred to as decomposition, or breaking down functions into their discrete activities, allowing for more accurate comparison of their attributes. With this basis, we get a truer picture of what is really common or different across business lines that appear the same when described at a more generic level. In turn, this enables us to scope and focus intra or inter-jurisdictional projects more carefully and productively.

To advance our own integrated service delivery agenda under the **Framework for Action 2000**, Ontario has been working on a number of initiatives that target specific elements of the Trust Chain. A few of our initiatives are described below using terminology introduced in the Information Classification Framework discussion. A table is provided for each initiative to illustrate its role in Identification Authentication and its estimated overall Level of Assurance.

EXAMPLES AND ANALYSIS

Trusted Registration

Ontario's Trusted Registration project has a mandate to provide program registration at integrated service counters. There are two parts to this initiative: the first is the integration of services at common counters; the second part is a business model for the delivery of common registration and credential authentication services to customers who may be applying for one or more programs.

This registration function will be delivered through a network of public and private counters where:

- Clients may go to one counter to do multiple registrations with the same agent in one visit;
- Clients will be served by an accredited agent who is supported by rigorous standards and processes;
- Face-to-face registration will only be used for accessing programs/services requiring strong authentication;
- If identity verification is required, the agent will validate the client info against another source;
- Clients will complete their registration in one visit, where possible;
- Clients who choose to visit the counter for registration or other services available electronically will get assistance in using the onsite Public Access Terminal;
- Clients can choose any channel (counter, telephone, internet) to find out information about the registration service.
- The pilot models will not maintain customer data files after credentials are verified and sent to the program administrators for action.

The goals of Trusted Registration are to:

- Enhance trust by increasing the level of confidence in the identity attributes of each customer;
- Increase security and reduce fraud through more rigorous verification and investigation standards and processes while protecting individual privacy;
- Improve customer service and convenience so that customers are able to access a number of services in one location;
- Increase government efficiencies by delivering services using a rationalized network of counters, and;

- Promote the e-government agenda through customer assistance at public access terminals, using common infrastructure.

The integrated counters will provide a service broker function between the individual and the relevant ministry, but will not retain the registration information in any central database after the transaction is completed. This approach will facilitate improvements in service and efficiency without requiring new legislation, which would be necessary to permit the creation of a single database of identity information for use by multiple programs.

Trusted Registration

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High	★			★
Medium				
Low				
Not applicable		★	★	

The initiative does not address all aspects of the Trust Chain. Trusted Registration is always combined with other elements defined by the programs that use it.

Visa 3D Project

The Government of Ontario, Bank of Nova Scotia and VISA International are at a preliminary stage in a Proof of Concept initiative to explore the potential use of private sector authentication services for customers transacting electronically with the government.

As a result of “know your customer rules” and an evolving face to face registration standard used by the bank, VISA and the bank may be able to offer a Profile Authentication Service (PAS). This service would, upon customer’s consent through the PIN based authentication, transmit to the government application pre-determined information about the customer, such as name, address, date of birth, and other contact information.

The transmitted information could populate a government online form, or be compared to existing information held by the program as a means of validating the user.

For government agencies that only require low to medium levels of assurance regarding the authenticity of the customer engaged in the online transactions, the benefits include:

- Leveraging the bank’s PAS registration services, in lieu of a government funded or managed registration service,
- Leveraging the VISA networks robust and secure infrastructure,
- Facilitating customer ease of use by relying on the customer’s use of a PIN that is used for more frequent transactions than a government program specific PIN,
- Removing the need for any technical skills by customers in terms of loading, storing, or managing certificates or keys on personal computing devices,
- Providing ubiquitous access from any web enabled device,
- Precluding the need to centrally store basic profile data in government, avoiding new privacy issues for the government while leveraging existing privacy protection infrastructures of the banks.

Visa 3D Project

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High				
Medium	★	★		★
Low				
Not applicable			★	

The VISA 3D initiative may provide a cost-effective, common user interface and flexible consent-driven identity authentication solution to program areas with Low to Medium identity authentication requirements. The VISA 3D components could simplify authentication processes between the public and private sectors without compromising the privacy of customers. This initiative with VISA and E-Scotia illustrates the benefits of exploring identification and authorization needs and options across the public and private sectors.

Registration, Authentication and Authorization (RAA) Common Component

The Registration, Authentication and Authorization (RAA) component is a tool that provides a customer with electronic credentials to access a variety of programs in which he is already registered. This starts with a counter-based initial registration that transforms the client's paper identity into electronic credentials for the programs they wish to transact with in a privacy enhancing way. *No specific registration program or agent has been identified to date. However, any registration agent such as those above whose business processes equal a medium assurance standard could discharge that function.*

The customer goes to an authorized counter where he presents his paper credentials regarding identity. He chooses a unique memorable user-ID and password combination. This combination is encrypted in two stages, and paired only at the program application with the program-specific customer identifier. No aggregation or linking of the user ID and program identifiers is retained in the tool after registration or during subsequent use. A major benefit of this privacy enhancing authentication mechanism is that it can also serve as a single sign-on engine.

This means that the customer can conduct a variety of unrelated transactions without the government having the ability to aggregate or track his or her transactions with the government. It provides individuals with the service convenience of one-stop shopping without implementing either cross-program or universal identification.

No names or addresses are required or kept within the RAA component. All information is passed through to individual program applications where actual client information resides. This significantly reduces the risk of personal information exposure through a compromise of the RAA component, and preserves the collection of personal information, under proper legislative authority within the relevant program area.

This is a basic summary of how it works:

- The client registers at a counter, e.g. common counter as in Trusted Registration, authenticating with documents in a face-to-face process.

- The client selects a random user ID and PIN, to be used for all subsequent transactions, which is stored in a single use database. He/she selects programs he wants to access electronically, which are verified by the agent.
- The encrypted user ID, PIN, and verified program ID are sent to each program area's unique surrogate key generation component. The program will recognize the verified program ID from the program's enrollment process.
- A surrogate key is generated, leaving the user ID behind.
- The surrogate key is deposited in a privilege management component, linked with the program ID. Each program has its own instance of the Permissions Management Infrastructure (PMI).
- When the client logs on to the portal, he provides the unique user ID, which is encrypted and checked in the database, and then he provides the PIN.
- The encrypted user ID and PIN are encrypted together and sent to the program areas selected by the user.
- The program areas generate, with their own program specific algorithms, surrogate session keys, and compare them to the surrogate keys of known program users. If the program area finds one, it looks up the program ID from the pair binding established during the initial registration. Access to the requested service is granted or denied based on the user's privileges, set by the program in the Permissions Management repository.

The Registration, Authentication and Authorization (RAA) product is a ready-to-deploy component, similar to our CCPAY component for online credit card processing. These are just two of 22 common components that are being developed and delivered under the Common Components strategy. The goal of this strategy is to provide discrete transactional components that can be re-used by business lines when the business process requires them.

Password recovery and ID/Password change mechanisms conforming to the above design requirements are being conceptualized that add to overall security, prevent the excessive growth of expired Electronic Identities in the

registration database and reduce the likelihood of a customer needing to re-register due to a forgotten password.

RAA Common Component

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High				
Medium	★	★	★	★
Low				
Not applicable				

The RAA component is internally built. However, the tokening and authorization mechanisms could be replaced with commercial off the shelf products that are FIPS 140 certified if required. As a result, subject to improvements in the registration functions, this model could deliver high assurance trust chains, that meet stringent privacy design characteristics, and deliver the convenience of single sign on for unsophisticated users.

Government of Ontario Public Key Infrastructure (GO-PKI)

The Government of Ontario has deployed a traditional PKI for GO employees. It requires a central certificate store linked to individually identifiable personal information in order to provide linkages between that user and the information they touch in some way in the course of their jobs. This provides the ability to track all of the activities of an identifiable individual user throughout the PKI enabled system, and ensures the accountability of trusted employees. It is an audit mechanism that can be used to aggregate data about an individual across program and Ministry boundaries and must be handled securely as it represents a serious threat to employee privacy if abused. However, the accountability of OPS employees is a safeguard against insider abuse and data theft, from the point of view of the citizen. It will be important to manage this system well to ensure maximum security and privacy benefits for our clients, without compromising the privacy of OPS employees. Trust is established in PKI systems by a strict regime of policies and technology governed by a defined organizational structure.

At the moment, the first implementation is with an ID certificate only, which is used when the employee logs on to fill in attendance documents and electronic expense claims. It is being expanded to include use by partners in network programs, such as public health local offices in the Ministry of Health, where highly sensitive information is part of the transaction.

The GO-PKI has cross-certified with the federal government for police applications, in order that the RCMP and the OPP could share information more effectively while being absolutely assured of the credentials and identities of those accessing the system. This is a good example of where strongly authenticated and transparent systems (in terms of audit trails) are warranted and necessary.

PKI systems have come under some criticism over the past few years as they have evolved, for a number of reasons. There are privacy concerns stemming from traceability of transactions and the directories, scalability issues because the system grows in complexity as you roll it out across domains, and revocation issues, because real time revocation of certificates has not been demonstrated to be effective in a grand scale. The work factor in managing the system is significant, as soon as it grows beyond small, relatively bounded applications. Cross-certification and revocation issues remain a problem that has not really been tackled on a commercial scale as yet; we will be watching how it works in the police application.

The bulk of OPS employees PKI Electronic Identities are considered to have a low level of assurance as the registration function was executed through a bulk load process and not face-to-face registration. Where justified by job requirements, employees are also granted additional certificates for signing, non-repudiation and role privileges.

Commercially available PKI products are highly reliable and robust, from a security and interoperability point of view. However, in terms of the registration component, securing and managing certificates, PKI services are expensive to create and maintain. As a result of this, full feature PKI applications are only deployed in Ontario at the very top of the Pyramid of Trust, where there is an essential requirement for maximum security, user authentication, and non-repudiation.

Government of Ontario Public Key Infrastructure (GO-PKI)

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High	★	★	★	Determined
Medium	★			by
Low	★			registration
Not applicable				strength

Mapping PKI examples to our chart of function and trust chain assurance levels reinforces the weakest link notion. Because of the strength of the latter two functions in PKI, the level of assurance (and cost) is highly dependant upon the strengths of the registration function. Note that this addresses the Electronic Identity components only and not the other message security and non-repudiation functions that are part of a comprehensive PKI package.

Electronic Service Delivery for Individuals (ESDI)

The ESDI initiative is key in supporting the Ontario government's goals to become a world leader in delivering services on-line. It is intended to offer Ontarians increased choices in how, when and where they can access government services and aims to provide individuals with simple, seamless and speedy access to government information, products and services.

The goals of the ESDI Initiative are to:

- Provide an IT infrastructure that will accommodate ongoing expansion, modification and change to government services
- Provide electronic channels for service delivery
- Provide integrated, customer-focused service delivery
- Provide seamless access to government products and services
- Attain cost-effective, adaptable and scalable service delivery
- Improve customer service

Participating ministries are the process owners with overall responsibility for the programs offered on the ESDI infrastructure. There are currently 4 process owners, the Ministries of Transportation, Natural Resources, Health & Long Term

Care, and Consumer and Business Services. MCBS is the Service Manager with overall responsibility for the management of the ESDI contract with third party service providers and a coordination role on behalf of participating ministries.

To facilitate the translation of legal privacy requirements for the private sector partners, MBS developed the ESDI Privacy Standard. The standard was supported by the IPC and approved by the Government of Ontario as a mandatory information handling standard for project participants. The standard is a useful reference tool for similar initiatives.

The Service Provider will use authentication mechanisms comparable to other channels to verify clients for ESDI transactions, through a common electronic window.

For example, the Integrated Address Change function allows clients to change their address for multiple participating programs with one transaction. The customer enters their address update once and identifies the programs by their program identifiers that he wants the address change directed to.

Where one of the programs requires additional authentication such as a shared secret, that information can also be entered. When the customer concludes the transaction the information is parsed and transmitted to the appropriate program, with no central copy of the aggregate data retained. This application demonstrates how we can integrate services and provide the corresponding levels of authentication as specified by programs.

Such address change and similar renewal mechanisms reflect the same level of assurances that now exist in phone, kiosk or mail based transaction media. Where fees apply and are processed by credit cards there is some capacity to track back to the legal holder of the card, who may or may not be the person effecting the transaction.

In this example, the registration function action of collecting identification data is met by prior program registration.

In Integrated Address Change, program data, in the form of confidential information is also reused as shared secrets or tokens for the authentication function. Depending on the security levels attached to shared secrets, the strength of the Authentication process will vary.

Electronic Service Delivery for Individuals (ESDi)

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High				
Medium				
Low		★	★	★
Not applicable	★			

The ESDi initiative is a prime example of Ontario’s effort to restructure services that were traditionally provided by separate ministry channels into common electronic channels. The system is being carefully designed to meet participating ministries requirements, compatibility with existing channels (phone, kiosk, over-the-counter), and client privacy requirements.

We are also monitoring other initiatives to develop trust chain components that may need to be taken into account in the future. These initiatives are listed in Appendix A.

F. Summary of Ontario Examples

In summary, the key implication is that program managers have a range of choices to customize a Trust Chain to meet their requirements, as indicated in the summary chart below.

For example, to build a medium strength Chain of Trust a manager could choose between traditional PKI, Trusted Registration, VISA or use RAA for the registration activity or link.

Summary of Ontario ESD Initiatives

Estimated Component Strength of Assurance	Registration & Tokening	Token Presentation & Authentication	Authorization Permissions	Trust Chain Level of Assurance
High	Trusted Reg. GO-PKI	GO-PKI	GO-PKI	★
Medium	GO-PKI RAA Visa 3D	RAA Visa 3D	RAA	★
Low	GO-PKI	ESDi	ESDi	★
Not applicable	ESDi	Trusted Reg.	Trusted Reg. Visa 3D	

For the next link in the trust chain, the selected registration link could be paired with a PKI, RAA, or VISA authentication and tokening components. For medium strength permissions management tools, as warranted by the programs applications they could opt for either PKI or RAA.

Given this flexibility, it is possible to contemplate elements of the Chain being delivered by different jurisdictions, as long as there was consistent understanding of the Levels of Assurance for the component(s) being shared.

Often discussions within or among jurisdictions are complicated by the fact that participants use these concepts in a very product or context specific way, making comparisons of apples to apples, and oranges to oranges difficult. This is an issue we will need to resolve to facilitate inter-jurisdictional co-operation. A standardized reference framework, compatible with both industry and governmental initiatives would reduce the risk of confusion and errors.

However, policy and definitional consensus alone will not be enough to provide businesses with the ability to exercise these choices.

To enable businesses to pursue this strategy of flexibility electronic recognition, routing and transformation of a variety of electronic identity tokens from external sources will be required to be delivered to internal program

applications inside corporate firewalls and other security services.

Rather than create these mechanisms on an ad-hoc basis, in keeping with Ontario's common component strategy Ontario is planning to manage these processes through its Integrated Security Interface (ISI) initiative.

G. The Integrated Security Interface (ISI)

The ISI initiative calls for the creation of a corporate architecture within which these business and technical activities can be designed, tested and implemented based on program requirements while allowing for component reuse by other programs with similar client identity management needs.

Upon completion, the ISI will allow a program area to accept a variety of electronic identity tokens that meet a program area's requirements for user verification. These could eventually include tokens issued by different jurisdictions or levels of government, e.g., the federal government's PKI identity certificate incorporating a MBUN, VISA 3D, or the BC E-ID.

Regardless of the type of electronic identity token, the key to accepting a token for access to Ontario government electronic service (e-service) offerings will depend on whether or not the source's registration procedures are determined to be sufficient by the accepting program to allow the user access to their e-services.

It will be the role of the ISI components to receive a token, examine a set of program area business rules and make a decision on what to do with the token prior to passing it to other components of the ISI for further action.

These decisions will likely be made on the basis of whether it is an individual in their role as a private citizen seeking e-services access (which must conform to privacy standards and the legal requirements of FIPPA concerning the lawful authority to collect personal information) or whether it is an individual in their role as an employee of an organization (where information about an individual and the company they represent may be subject to disclosure).

Attributes of these two roles would be governed by different collection, use and disclosure rules, and each role would likely have different authorities with respect to accessing to different views of the same data.

One component the ISI could access on the basis of the private/public role

decision is the Registration and Authentication and Authorization (RAA) module. As previously discussed, and described in more detail in the appendix, the RAA module is intended for the creation and authentication of electronic identities used by electronic services clients in their capacities as private citizens, and has been designed with specific privacy considerations in mind.

For business transactions that require digital signatures and non-repudiation, PKI certificates could be used. These would be supplied by some other mechanism, either through the existing Ontario Government PKI infrastructure, potential service providers such as being investigated in the VISA's 3D Secure identity token proof of concept (in which the Ontario government is participating) or other 3rd party identity tokens the provincial government may be prepared to accept (such as the federal government MBUN).

In this circumstance, it will be the role of the proposed ISI interface component to accept these identity tokens and decide what to do with them based on individual programs' business rules and the requirements of provincial statutes such as FIPPA. Depending on the rules in effect, the token may be passed straight through to the program area, for example if it is a business application that requires the non-repudiation benefits of PKI.

In either circumstance, the authentication information would be routed to the authorization components, often referred to in technical terms as the Permission Management Infrastructure (PMI). These are the components that actually store and apply the data access and change rules that the programs' authorize the electronic identity to exercise.

The PMI ensures that an individual is granted a level of access appropriate to their role (private citizen or agent/employee of an organization).

To ensure privacy and the separation of the privileges appropriate to each role, a separate PMI authorization component would be used for citizen transactions with each program as well as a separate PMI authorization component for commercial transactions.

This degree of separation of business and private citizen credentials and access privileges will minimize the risks of privacy breaches. Breaches could occur by the inappropriate aggregation of transactional data, or inappropriate access to information through the application of commercial access privileges to a citizen only data store. A PMI implementation is currently undergoing trials in a pilot application in a cluster.

FINAL THOUGHTS

The Chain of Trust model and the various projects described previously test service integration and delivery options in which identity authentication and authorization issues are key factors. The projects provide an opportunity to test different technologies, architectures and program delivery schemes without committing the government to wholesale and expensive change. This approach is a measured one, recognizing that if it works and we like it after kicking the tires, we can drive it home.

In our earlier diagram of the Pyramid of Trust we illustrated our view that cost of service, complexity of registration and applied technologies and privacy risk all increase in tandem with increased levels of assurance while the volume of transactions correspondingly decreases. In other words, we see an inverse relationship between the number of users involved and the need for high assurance chains - most services being considered for electronic service delivery require only low assurance trust chains.

Similarly, the more registration and identity authentication infrastructures are centralized, the greater the liability and political accountability for the controlling institution(s), and the greater the public sensitivity to the policy, privacy and security issues raised.

For example, a highly centralized authentication and permissions infrastructure in which a single organization,

- holds identity information, customer tokens, keys or passwords, and
- has the ability or even latent capacity to trace a customer's transactions across a range of organizations

functions like a jurisdictional ID card with powerful customer surveillance capability. This would attract the most privacy concern from the general public and the press and perhaps even constitutional criticism. The organization maintaining this centralized infrastructure would inherit the primary responsibility for negative impacts of the system regardless of the contractors used to deliver sub-components. Implementing this approach at a national level will require significant legislative action to authorize a fundamental restructuring of each jurisdiction's identity verification processes. Such legislation is likely to be controversial.

Conversely, an approach where either the customer chooses, or governments provide directly, or through partners, a variety of registration and tokening services that:

- do not centralize or collectively pool registration data or authentication tokens,
- where the customer can influence or control the data elements conveyed by a token on a transaction by transaction basis,
- and each institution in the trust chain has comparable oversight or regulatory regimes regarding the use of personal information,

is less likely to attract negative public reaction due to privacy and surveillance concerns. This system is also less likely to require significant and controversial legislative action to implement. This approach will also provide us with the greatest flexibility to manage the trade-offs of cost and benefit, customer convenience and privacy protection, program/business transition and ease of implementation.

A shared understanding of the core components of the Chain of Trust is necessary to move forward with this vision of service integration. Developing a **Trust Chain Standard** will provide business or program areas with the means to decide whether a given service offering or component is suitable for integration with their own business processes. It will also facilitate practical dialogue and collaboration by providing us with common definitions that would ensure all parties are speaking a common language when negotiating and planning service integration. This will help us break down the large task of integrating services into the three components of the Chain of Trust, and allow us to build integrated services block by block.

PROPOSED NEXT STEPS

We believe that the analytical framework underpinning Ontario's Identification and Authentication strategy is generic and transferable. A standardized reference framework for analyzing respective Trust Chain components in different jurisdictions or by different providers would help us all to have a more practical, grounded discussion about opportunities to work together on ID Authentication in support of more customer-focused, integrated service delivery.

To move ahead in this, our immediate task will be to develop the standard that describes and documents our shared understanding of the trust chain and how it would apply to our respective business processes.

The standard would define each component of the trust chain and describe the levels of assurance for each component. With this standard in hand, each business or program could:

- Identify at what level of assurance their current business processes and technologies need to operate,
- Determine whether a particular component from another business process is appropriate for consideration as an alternative to one's own identification and authentication mechanisms.

We are more likely to be successful at service integration if we design our authentication models in ways that maximize the ability of each jurisdiction to resolve, through consultation with its own stakeholders, issues related to privacy, legislative authority, the role of private sector partners and technology architecture and implementation.

We propose that a working group composed of staff drawn from each jurisdiction and level of government, not unlike a Policy Management Authority, be formed to begin the work of developing a Chain of Trust Standard.

Appendix A - OTHER MODELS

The following models have not been formally evaluated in any detail but may be useful in our overall discussions. They are MasterCard's Modular On Data Storage, Microsoft's Passport and the Liberty Alliance Specification. These initiatives exemplify the growing recognition by the private sector and the I&IT industry of the importance of privacy design requirements. While traditional LDAP, directory services or X.509 standards are effective in closed enterprise systems or multi-agent commercial networks, new approaches must evolve to provide consumers with confidence regarding their control over the use and aggregation of their personal information.

Liberty Alliance

The Liberty Alliance Specification is best described as technical specification to allow a group of entities including the customer to link a series of entity specific transactions together facilitated by a single sign on with a master ID. This is accomplished by completing separate registration processes for each entity, with a set procedure for aggregating these through one entity performing the role of administrator. The administrator establishes the single sign and creates a series of pseudonyms relating to each of the other entities customer ID. Except for the administrator, each entity does not know the actual user ID the customer uses for the others participants, but may be aware of the other entities in the group the customer has a relationship with. This is a highly abbreviated description.

The value of the Liberty Alliance model is that it provides an example of a usable standard architectural framework. From the perspective of our Trust Chain, while its registration processes will vary in strength depending on each participant's internal standard, the authentication tokening and exchange mechanism may be described as a medium strength. The permissions management functions are centered within each participant's systems. For clusters of businesses a customer may frequent, it is a viable model where the customer is not concerned about the knowledge of his relationship with all participating businesses being shared, and there is trust in the administrator entity.

Compared to our internal projects, it is closest in approach to the RAA common components, but less privacy enhancing. The Liberty Alliance specification and model may have most applicability as an option for regulatory Electronic

Identity transactions with commercial entities amongst agencies and jurisdictions that often share data about a company. In this environment there is little privacy or commercial interest in the knowledge that an authorized representative of a company has dealings with agencies that have a mandatory regulatory role in that business sector. Commercial registrations, tax reporting, environmental monitoring, land and health public health administration come to mind as possible business candidates.

Microsoft Passport

Microsoft's Passport and .Net strategies are well known. This model is quite close to the directory services model we use internally and a classic PKI approach where a PKI identity cert is chained with additional attribute and identity data. A distinction from these models is the that the Passport model shifts some control to the customer to determine what if any information may be released to a site the customer is visiting through the single sign facility of Passport.

Mastercard's Modular Open Data Storage

Mastercard's Modular Open Data Storage specification is a smart card based facility for the customer to collect and store digital information for disclosure in subsequent on- or offline card-enabled transactions. EMV and ISO compliant chip processors can provide cryptographic support to data bins the customer controls access to with unique customer password. The customer can open additional subsidiary bins that a business can write data to and protect with a business PIN. It results in a storage facility that the customer has the primary key to and the business has a secondary key required to open it, not unlike a safety deposit box. Mastercard has developed metadata specifications for common data types including tombstone, financial and other data that could be mapped to in XML-based electronic transactions.

The significant features of this development is that the customer has significant control over their information as a privacy positive feature, in a standard smart card that can be used offline. For customers who do not want to maintain home technologies strong enough for many government transactions and do not want to remember numerous PINS, government businesses could utilize this model for future customers who accept card technologies and would prefer to use authorized kiosks, publicly accessible terminals or ATMs.

Appendix B – Background on Registration, Authentication & Authorization Common Components

During the past couple of years, the Ontario Government has been restructuring service delivery away from ministry-based “silos” to focus on “clusters” of ministries with related business objectives, clients and transactional activities. This new corporate strategy has meant the government needed to explore new approaches to organizing service delivery, delivering infrastructure, and managing information. The new strategy has also created the opportunity to re-engineer the way that technology is developed and implemented for use within the government to improve upon past practices.

Simultaneous to this effort by government to transform its services, software vendors have also been busy creating new tools for enterprises to use to develop distributed applications. One of the leading specifications is the Java 2 Platform, Enterprise Edition (J2EE) that can automatically take advantage of sophisticated platform services being designed into the Ontario's e-Government strategy. J2EE components can be developed according to standard guidelines, combined into applications, deployed on a variety of compatible server products and reused for maximum productivity.

Recognizing that the government frequently requires some form of ID authentication for the delivery of government services to individuals, the Economics and Business Cluster and MBS Corporate Architecture Branch, with the support of the Information and Privacy Office MBS, decided to collaborate on the development of J2EE components for Registration, Authentication and Authorization to simplify and standardize their deployment throughout the government.

Objectives

A key driver behind the development of these RAA common components was the need to preserve the right of citizens to own and control their own identity in its many manifestations when they interact with different government programs. Citizens have the right to name themselves, to change their name on their own accord, to select any name (including unorthodox syntax and formats), to maintain more than one unaffiliated name and identity when there is no intent to defraud or commit other crimes, and to eschew the use of any identity when engaging in transactions that only require payment to receive the product or service.

The RAA component was designed to address security, privacy and consumer convenience issues identified as important within the context of delivering e-government services to consumers in a secure, easy to use format that complies with Ontario provincial and municipal privacy laws.

Features include no creation of a centralized database of user information in personally identifiable form, and no aggregation or linking of the user's single login ID and program identifiers through their retention in the centralized RAA components.

Operations

The components perform the following functions in a distributed environment.

Registration Service: The Registration component is premised on the fact that the user has already been registered for the government program that the user is to be linked to electronically. It can occur as a face to face transaction at any authorized and counter equipped to communicate to the centralized Client Identification Component and Registry. RAA is not currently designed for online registration.

It is an identification process that distinguishes one user from all others. By itself, the first step of this process does not verify the identity of users beyond credential examination. It merely allows them to select a unique username and password (PIN) combination they will subsequently use to access government services.

After the user selects their unique user ID/PIN, the service stores only an encrypted version of the ID [not PIN] in the Registry . The service then communicates with the program authority to confirm the program's acceptance of the user as an individual known to and registered with the program. This can be through a program credential presented by the user or some level of shared secrets known to the user and program. The process may be automated or attended. Upon program acceptance, a variant of the user ID/PIN combination [hash] is transmitted to the program with the user's program identifier(s).

Each program runs a unique program specific algorithm on the hash of the User ID /PIN creating a program specific hash. This program specific hash is paired to the normal user program identifier and stored by the local application. This program specific hash and normal program identifier are used by the local

application in subsequent authentication and authorization activities.

The cycle repeats for each program to which the user wishes to establish an electronic linkage. Registration then ends.

Authentication: This is the centralized process of verifying the user has registered by comparing the user entered ID/PIN product with that in the repository. If a match is found the hash is forwarded to the program chosen by the user. The distributed or local program function processes the user hash to compare it against the program specific hashed version available to the application, to finalize authentication and enable permission management.

Authorization: This is a distributed local or application function that utilizes the authenticated user information to effect permission management, or the means of establishing and enforcing rights and access control for users. This program responsibility, based on the program's decisions regarding threat and risk assessment, is used to protect transaction functions, and ensure the users have been granted the privileges to use them.

The RAA implementation allows consumers to use one log-on name and PIN number for accessing any program that uses the RAA component (single sign-on from the consumer's view) or alternatively, one logon name and PIN per program at the user's choice. Users can make up a name or use their own, but real names are not encouraged.

For privacy and security purposes, no information other than the user-selected name (in encrypted format) is centrally stored. The PIN number is not stored at all. There is no centralized database of user credentials. All information necessary to identify the user to a program area is sent directly to the program itself, as only it has the authority in law to collect and use the information.

This statutory consideration is also behind the operational requirement that the distributed components be under the physical and logical control of the program authority. To centralize these functions in government would likely require legislation and give rise to concerns about the capacity to operate as a central ID or surveillance system.

For privacy purposes, a hash of the single user name and PIN is sent to a program area. The program's sub-component then converts this hash into a unique number used by the program area only. Each program has a unique hash engine in their subcomponent so that there are no common identifiers across databases to use in data matching exercises. In fact, it makes no difference from a privacy point of view if the consumer elects to use one name

and PIN for all e-government services because each program area is required to convert that information into a unique program specific identifier. It is this identifier which is unique to the individual in that specific program which the program maps in its application to the person's usual program identifier and authorities as granted by the program.

The following pages provide a data flow description and a conceptual view of the RAA Components.

Data Flow Analysis

Data Elements

Element	Source	Description	Stored
Client ID	User	User-selected identifier (encrypted)	Portal Repository
PIN	User	User-selected (password)	<i>Not stored</i>
Program ID	User	Program-assigned identifier/credential (e.g., Driver's License #)	Program Mapping Repository
Surrogate Key	Derived	A unique, program specific identifier generated at the program area. The surrogate key is created from the encrypted Client ID and PIN	Program Mapping Repository
Neutral Key	Derived	A one-time number generated at the portal repository. It is used by the program area to access the encrypted Client ID and PIN.	<i>Not stored</i>
Hash	Derived	A session specific encryption of the client ID and PIN.	<i>Not stored</i>

The following swim lane representations show, at a conceptual level, the flows of data through the RAA components. The numbers correspond to those found on the data flow diagrams after the swim lane descriptions.

Registration

Registration Application	Client Identification Component	Client ID Proxy Component
1 Present Client ID and PIN to Client Identification Component		
	2 Encrypt Client ID Create hash of Client ID and PIN	
3 Store encrypted Client ID in Portal Repository		
	4 Send to hashed Client ID Proxy Component with Program ID	
		5 Check Program ID against legacy system for validity and return message to Client Identification Component
		6 Generate Surrogate Key from Hash
		7 Add Surrogate Key and Program ID to Mapping Repository
	8 Commit or back out encrypted Client ID in Mapping Repository based on message back from Client ID Proxy Component	
	9 Return success or failure message to Registration Application	

Authentication

Registration Application	Authentication Component	Program Authentication Component
	1 Receive Client ID & PIN	
2 Look up Client ID in <i>Portal Repository</i> and return "Found" or "Not Found" status		
	3 Generate hash of Client ID + PIN	
	4 Generate Neutral Key from Hash	
	5 Pass Neutral Key to <i>Program Authentication Component</i>	
		6 Receive Neutral Key
		7 Derive Hash from Neutral Key
		8 Derive Surrogate Key from Hash
		9 Look up Program ID in <i>Mapping Repository</i> from Surrogate Key
		10 Return Program ID or Rejection

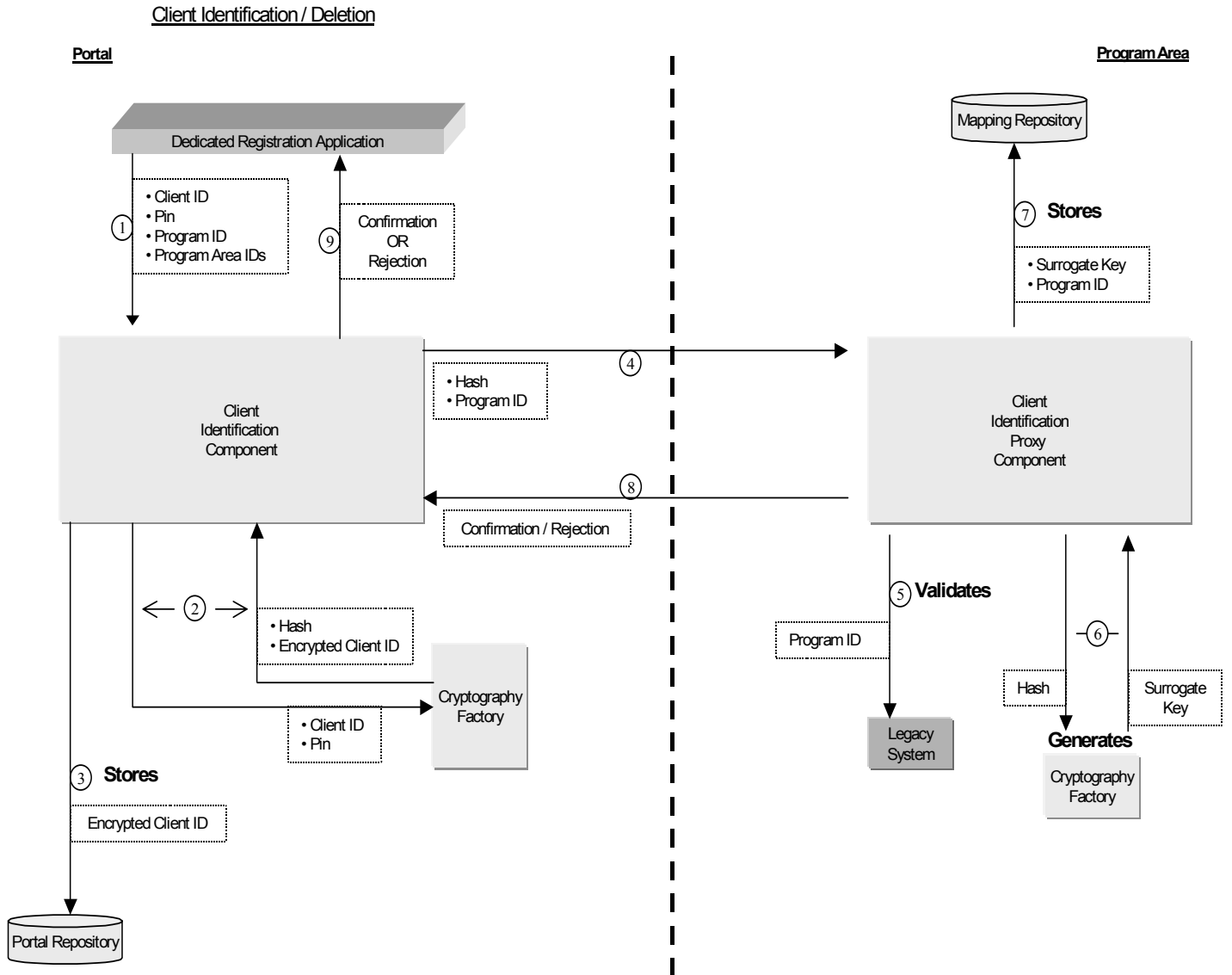
Authorization

Application Server	Authorization Component
1 Send lookup request to Authorization Component	
	2 Look up entry in <i>Program Mapping Repository</i>
	3 Return Client Information to <i>Application Server</i>

Data Flow Diagrams

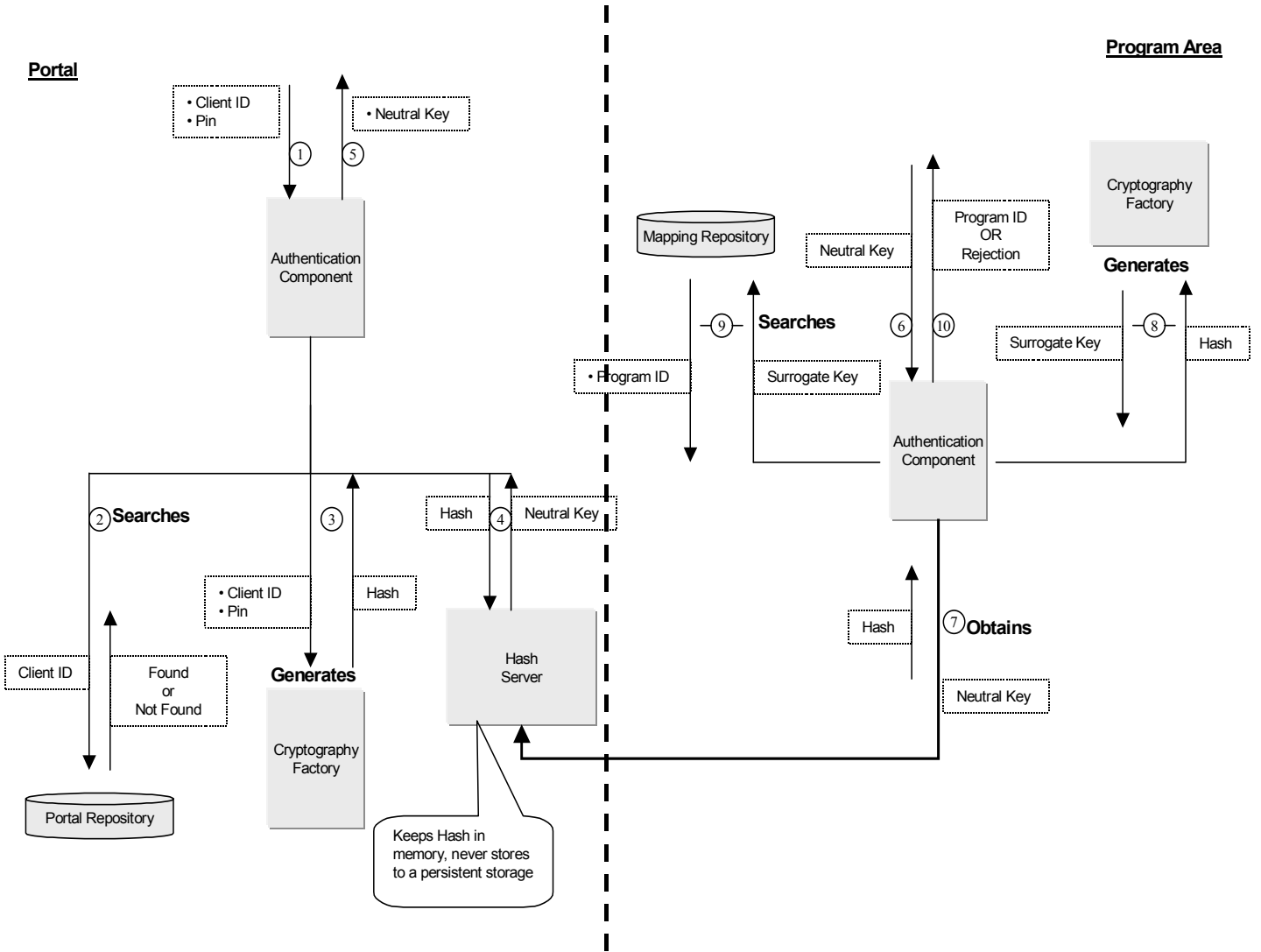
Registration

Registration Component Data Flow



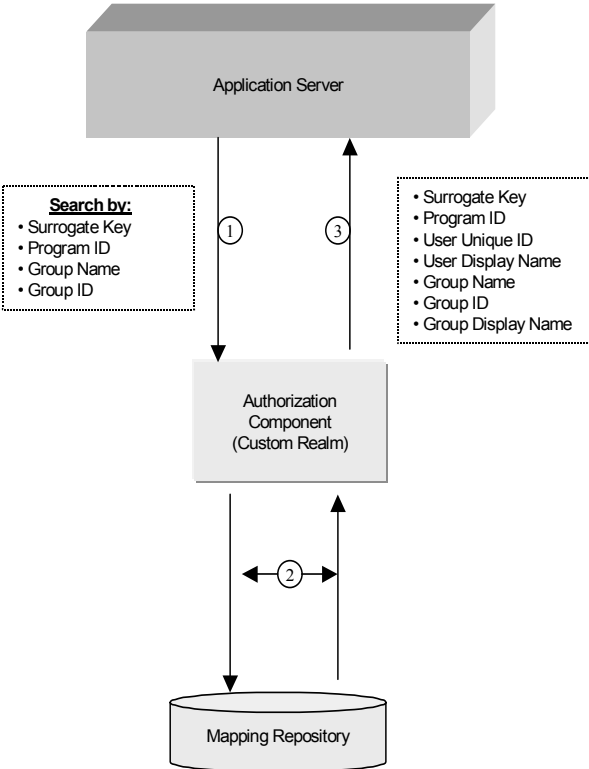
Authentication

Authentication Component Data Flow



Authorization

Authorization Component Data Flow (Program Area Side)



Status

The components exist as coded libraries. A conceptual level PIA concluded that the components, deployed as described, can operate in compliance with privacy statutes. Further work is required with respect to items such as independent vulnerability assessments, code review, and cryptographic modules certification.

Enhancements

Work is proceeding on mechanisms for user ID and Password recovery including backup surrogate keys. In addition, the ability to integrate the RAA design to utilize Commercial Of The Shelf (COTS) products for components such as authority or permissions management (PMI) is being reviewed.

Future Evolution

The potential role of the RAA Components as one of several core ID and Authentication technologies for an Integrated Security Infrastructure Architecture are under discussion.

For further information please contact:

Andreas Ott, MBS Security and Technology Integrator 416-327-6290

Peter Churchard, MBS Security and Technology Architect, 416-327-6776

Appendix C - ANNOTATED BIBLIOGRAPHY

1. **Article 29 Data Protection Working Party, "The Article 29 Working Party gives guidance regarding on-line authentication systems." The European Commission Internal Market, 10054/03/EN-WP 68 (Jan. 29, 2003): 15 pages**
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/

The document describes the Microsoft .NET Passport system and the Liberty Alliance Project. It concludes with specific guidelines to be applied by those services and by any other present or future on-line authentication system.

2. **Butler, R., D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. "A National-Scale Authentication Infrastructure." *IEEE Computer*, 33(Dec 2000):60-66.** <http://www.globus.org/documentation/incoming/butler.pdf>

The Globus project (www.globus.org) is developing tools to support an entirely new class of networked scientific applications called "grid-based applications" that are being designed to run on large-scale computational grids (the Grid). Many of the problems and solutions behind enabling Grid applications are analogous to the world of electronic service delivery. The Globus website contains an extensive list of references. The paper cited above describes a technical architecture for a Grid Security Infrastructure that lets users access resources at any participating site without authentication, while preserving a site's ability to use site-specific security mechanisms and enforce local access control.

3. **Canada-Ontario Business Service Centre (COBSC). "A Business Architecture in support of System-supported Service Management (Zachman Rows 1 & 2, Abridged)," COBSC, 4.0 (Aug 29, 2002): 27 pages.**
http://www.cobsc.org/coi/docs/COBSC_Service_Management_Architecture.doc

This paper describes a Service Management Architecture (SMA) that might be deployed in support of broadly based community of interest, or peer-to-peer implementations for information and transaction service delivery. The paper expresses the SMA in terms that approximate the artifacts of the Ontario Enterprise Information Architecture (EIA) based on the Zachman Framework.

4. **Cavoukian, Ann. "Concerns and Recommendations Regarding Government Public Key Infrastructures for Citizens." *Ontario Information and Privacy Commissioner (December 2002): 24 pages.***

<http://www.ipc.on.ca/Docs/pki.pdf>

This paper examines the potential impact of Public Key Infrastructures on the protection of personal privacy and makes several recommendations for officials establishing such systems.

5. **Clarke, Roger. "Authentication: A Sufficiently Rich Model to Enable e-Business" *Xamax Consultancy Pty Ltd. (2001): 22 pages.***

<http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html>

It has been conventional for some years to presume that e-commerce is dependent upon the parties to transactions being identified and their identities authenticated. This paper examines the concepts of identification and authentication as they apply to people and organizations. It suggests that many of the conventional presumptions are misguided, and presents a model and definitions that it is argued will lay the appropriate foundation for real progress in the e-business arena.

6. **Federal Financial Institutions Examination Council. "Authentication in an Electronic Banking Environment", *FFIEC (July 30, 2001): 12 pages***

<http://www.occ.treas.gov/ftp/advisory/2001-8a.pdf>

This interagency guidance focuses on the risks and risk management controls related to authentication in an electronic banking environment. Its principles are also applicable to the authentication of institution employees and contractors attempting to access any networked institution computer system.

7. **Ellison, Carl. "Improvements on Conventional PKI Wisdom." *Intel Labs. Presented at 1st Annual PKI Research Workshop (April 2002): 165-175.***

<http://www.cs.dartmouth.edu/~pki02/Ellison/>

This paper contrasts the use of a traditional Public Key Infrastructure for identification with the use of delegatable, direct authorization to achieve security. Ellison shows how two inter-operating PKI domains should design their policies and logical architecture to overcome the problems of traditional PKI's.

8. **Kenny, S., Korba, L. "Towards Meeting the Privacy Challenge: Adapting DRM", published in 2002 ACM Workshop on DRM, held in conjunction with the 9th ACM conference on Computer and Communications Security. Washington, DC; NRC 44956 (Nov. 2002): 17 pages.**
<http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf>

In this paper, the authors examine the prospect of adapting systems designed for Digital Rights Management for the purpose of Privacy Rights Management for European Community application. The legal requirements for privacy under the European Union Data Directive are outlined. After an overview of digital rights management systems, adaptations for transforming a DRM system into a privacy rights management system are described, concluding with strengths and weaknesses of the approach.

9. **Kent, Stephen T., Lynette I. Millet, editors. IDs – Not That Easy: Questions About Nationwide Identity Systems. Committee on Authentication Technologies and Their Privacy Implications, National Research Council (2002): 74 pages.** <http://www.nap.edu/books/030908430X/html/>

This research report prepared for the prestigious National Research Council outlines the issues the Committee believes must be addressed in any nationwide identity system. The report states it is not an exhaustive assessment. It is intended to catalyze a broader and more sophisticated discussion because the legal, policy and technological issues associated with nationwide identity systems warrant a much more detailed and comprehensive examination.

10. **National Electronic Commerce Coordinating Council (NECCC), "Identity Management – A White Paper." Presented at the NECCC Annual Conference (Dec 2002): 68 pages.**
http://www.ec3.org/Downloads/2002/id_management.pdf

This is an excellent research paper that identifies a range of questions to be asked as governments pursue electronic service delivery, such as how to balance the need for privacy and security of personal information against convenience of e-government service delivery, the need to identify and apprehend terrorists and fraud artists, and the need to interoperate across government and private systems on the other hand. The paper describes approaches to achieving identity management. The authors aim to provide a contribution to, and stimulus for, further dialogue regarding identity management and the role of government in it.

11. **Office of the e-Envoy. "HMG's Minimum Requirements for the Verification of the Identity of Individuals". *U.K. Cabinet Office, 2.0 (Jan. 2003): 29 pages.*** [http://www.e-envoy.gov.uk/oeo/oeo.nsf/sections/about-epolicy-esecurity/\\$file/securityguidelines.htm](http://www.e-envoy.gov.uk/oeo/oeo.nsf/sections/about-epolicy-esecurity/$file/securityguidelines.htm)

Guidance documents on HMG's requirement for the verification of identity as part of the UK government's drive to modernize service delivery. These documents, which are detailed technical documents supporting the Registration & Authentication Framework, describe the minimum evidence that needs to be presented by an organisation or an individual in order to be issued with a digital certificate or a password.

As they relate to the topic of identity verification, see the responses to the UK government's consultation paper on Entitlement Cards and Identity Fraud by the UK Information Commissioner (citation [17](#) in this Bibliography) and Dr. Perri 6 (citation [14](#)).

12. **Ontario Public Service Restructuring Secretariat. "Framework for Action 2000." *Cabinet Office, (Oct. 2000): 34 pages*** http://www.ontariodelivers.gov.on.ca/english/virtual_library/framework2000.pdf

The report highlights how the Ontario Public Service is moving in the direction of more integrated service deliver, strategic policy and planning. It also shows how members of the OPS have built new processes and formed new working relationships among ministries and with organizations outside the OPS to find more creative solutions to complex issues.

13. **Patrick, Andrew. "Building Trustworthy Software Agents," in *IEEE Internet Computing, (Nov./Dec. 2002): 46-53.*** <http://www.computer.org/internet/ic2002/w6046abs.htm>

This article proposes a model of the factors that determine agent acceptance, based on earlier work on user attitudes towards e-commerce transactions, in which feelings of trust and perceptions of risk combine in opposite directions to determine a user's final acceptance of an agent technology.

14. **Perri 6, Dr. “Entitlement Cards: Benefits, Privacy and Data Protection Risks, Costs and Wider Social Implications.” Office of the Information Commissioner, Response to the Government’s Consultation Paper, Annex B (2003): 54 pages.**

<http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf/24afa328dcbf83d8802568980043e730/2924d87f53cb414180256cc5003fcd96?OpenDocument>

This is an insightful analysis of the UK government’s proposals to require landed residents to register for and possess a token (smart card) for identification purposes. The paper was specially commissioned from Dr Perri 6 by the Information Commissioner as part of the commissioner’s response to the entitlement card scheme (17). Perri 6 explores the compliance of the government’s proposal with data protection principles, and the administration, cost, and wider social and public perception implications of the scheme.

He concluded that the central problem of the government’s proposal is not that no argument is available to justify compulsion for registration and possession of the entitlement card – he provides one where the government did not – nor that the argument is invalid, nor that its core premises are weak. Rather, the problem with the government’s scheme is that it does not meet the conditions of compliance with data protection and of proportionality of cost to benefit that any such scheme must meet.

15. **Perry, P., Bird, R. “Europe Smart Cards Trailblazer 8 on User Requirements for Cardholder Identification, Authentication and Digital Signatures,” *The European Commission* (2002): 22 pages.**

http://www.tiresias.org/reports/user_requirements2-2.htm

This technical report examines some of the aspects that are likely to affect the user’s ability or desire to use smart card systems. Trust is difficult to measure but will depend on the consumer’s understanding of the level of security of their personal information. Service providers need to understand the needs of their customers to ensure consumers are comfortable using smart card based systems.

16. **Reed, Archie. “The Definitive Guide to Identity Management”, (*Rainbow Technologies*) *Realtimepublishers.com*, Ch. 3 (2003): 47-71**

<http://www.rainbow.com/IDebook/index.html>

Standards and products are evolving rapidly, however the challenges faced by anyone implementing a comprehensive Identity Management

solution remain significant. This book provides IT specialists and managers with practical understanding and advice on critical Identity Management components from Web Single Sign On to resolving data issues both internal to an organization and across the Internet.

17. **Thomas, Richard. "Entitlement Cards and Identity Fraud: The Information Commissioner's Response to the Government's Consultation Paper." Office of the UK Information Commissioner (Jan. 30, 2003): 6 pages.**
<http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf/24afa328dcbf83d8802568980043e730/2924d87f53cb414180256cc5003fcd96?OpenDocument>

This is the UK Information Commissioner's response to the UK Home Office's consultation paper on Entitlement Cards and Identity Fraud (See also citation [14](#) in this Bibliography, an analysis by Dr Perri 6). The government's consultation paper can be found at: <http://www.ukpa.gov.uk/entitlement.htm>

18. **Wright, Tom. "Privacy and Electronic Identification in the Information Age." Ontario Information and Privacy Commissioner (November 1994): 11 pages.**
http://www.ipc.on.ca/scripts/index.asp?action=31&P_ID=11395&N_ID=1&PT_ID=11351&U_ID=0

This paper highlights the privacy issues that are associated with electronic relationships -- electronically identifying and interacting with public and private sector organizations in exchange for goods and services.