Determining Authentication Levels Within the BC Government

March 13, 2002
Version 1.0

Table of Contents

General Approach To Authentication

Authentication is the process of verifying the claims that a person makes to establish identity, eligibility for services or authorization for payments from government, are genuine. In real world transactions it is relatively easy to collect and confirm personal information. In electronic transactions the ability to collect and verify personal information is much harder. It is possible to create electronic personas or identities which have no relationship to a person's real world identity. Authentication verifies the relationship between real world and electronic identities and defines the level of trust, or trustworthiness, of the parties involved in a transaction.

One way to deal with trust in electronic transactions is to collect and verify as much information as possible about the parties in a transaction. However, this approach is not practical because:

- more personal information may be collected than is actually need to conduct the transaction.
- data collection, however well intended, costs money to store, manage and protect. Government has a special requirement to manage personal information based on the Freedom of Information and Protection of Privacy Act;
- the impetus for electronic service delivery is based, in part, on the cost savings implicit in electronic transactions. However, the cost of authentication may not be supported by the business case for an electronic transaction.

As government expands its electronic service delivery initiatives, a framework is required to:

- consistently determine authentication requirements;
- allocate appropriate levels of technology to meet authentication requirements;
- develop a way of documenting authentication requirements so that:
  –ministry practices can be coordinated;
  –legislated protection of privacy requirements can be monitored; and
  –best practices can be identified for government.

Based on the UK Government's "Framework Policy And Guidelines For Authenticating Citizens And Businesses To Government" the BC Government's approach to authentication is to:

1. define a number of 'trust levels' which relate to the authentication requirements for particular types of transactions. Reaching high levels of trust requires a more vigorous process of verifying the information used by the parties in the transaction.
2. require Ministries will document their trust requirements by completing an authentication profile. Assign electronic service delivery initiatives to specific levels of trust using the documented requirements of the authentication profile.
3. define reference profiles for each level of trust which will assist ministries in determining the appropriate level of trust.

This paper defines the Levels of Trust and presents a template for Authentication Profiles which can be used to determine authentication requirements appropriate to the transaction.

Authentication Profile

The authentication profile is a template (see Appendix A) for ministries to document the key decisions made in choosing a cost effective method of authentication. The six sections of the Profile are divided into two parts:

Part 1 - Defining Electronic Service Delivery Requirements

The first three sections document the characteristics of the transaction and the authentication requirement for the electronic service delivery transaction. Completion of these sections of the profile should enable the user to assign a Trust Level. Reference profiles are being developed to provide a comparison standard to the profile completed by the ministry.

Section A - Transaction Requirements - defines the characteristics of a transaction which may influence the trust level. These requirements are divided into two parts:

- Evidence of a Consequential Transaction - documents the level of consequence (e.g., legal, financial, social) associated with the transaction;
- Access and Risk - documents the level of liability associated with access to an electronic service delivery application;

Section B - Authentication Requirements - documents how various components of the authentication lifecycle will be handled. Authentication covers a range of activities including: the collection of personal information; verification of that information; and, issuance of credentials for ongoing authentication;

Section C - Transaction Mode - describes how the transaction will be conducted and whether the transaction occurs on a Managed/Trusted or Unmanaged/Untrusted system.

Following completion of Part 1, the ministry should be able to assign the electronic service delivery application to a Trust Level. Part 2 of the template suggests authentication technologies, data protection and other factors which should be considered in conducting the transaction.

Part 2 - Providing Solutions

After a Trust Level has been assigned, the following sections provide some recommendations around the appropriate level of authentication for the documented requirements.

Section D - Identity Credentials - describes potential solutions for satisfying on-going authentication requirements as identified in Part 1.

Section E - Data Protection - describes data protection alternatives which can be implemented at any level of trust. Data protection solutions may be implemented to supplement an authentication technology.

Section F - Common Services - describes common support and maintenance activities which may be provided as part of the infrastructure. The presence of these common services may influence the delivery of electronic services.

Part 1 - Defining Electronic Service Delivery Requirements

Section A. Transaction Requirements

The nature of the electronic transaction is not directly related to authentication, but these key characteristics influence the level of trust required to conduct a transaction. The key transaction characteristics include:

Part 1 - Evidence of a Consequential Transaction

These are the requirements which establish the rigor that must invested in the authentication process.

- Electronic Ceremony - conveys the understanding to parties in an electronic transaction that they are performing an act that has consequences. This is the electronic equivalent of a signature.

- Evidentiary Requirements - the level of proof required to demonstrate that a transaction was conducted. Transactions can have varying requirements dependent on the parties involved, the nature of the transaction, the dollar value, etc.

  - Non-repudiation - involves the evidence required to prove that a person conducted a transaction and is provided with proof of delivery, while the recipient is provided with proof of the sender's identity. This ensures that neither party can deny having sent/received the transaction. However either party can still deny that they *intended* to conduct the transaction.
  - Receipt Acknowledgment - a message sent to the sender of a message indicating that a message or transaction has been received. The message or transaction may not be viewed or processed until a later time.
  - Integrity - assurance that information can only be accessed or modified by those authorized to do so.
  - Confidentiality - assurance that messages can be exchanged without anyone but the intended recipient accessing or seeing them.

- Privacy - documented through completion of a Privacy Impact Assessment.

Transaction Requirement	Describe Requirement	Comments
Electronic Ceremony	Does this electronic transaction need to look like a consequential act to the user?	Other factors – how are users notified that they are conducting a transaction with real life consequences?
Evidentiary Requirements	Will the transaction information be required:	Will the transaction information be used to prove:

Transaction Requirement	Describe Requirement	Comments
	- for a judicial process (e.g., to prove fraud); - for administrative purposes (e.g., order confirmation); etc.	- origination of the transaction; - submission of the transaction; - evidence of receipt. What kind of audit and security logs are available for proof? How is the evidentiary integrity of those records maintained?
Non-repudiation	What are the consequences if someone refuses to acknowledge a transaction?	Other factors - combination of electronic and real world methods for proving a transaction occurred e.g., audit trails, access logs, MOUs, contracts, data access agreements, digital certificates.
Receipt Acknowledgment	Do the parties in the transaction require acknowledgment that a message was received/sent?	Other factors – could impact non-repudiation.
Integrity	What is the evidentiary value of transaction record?	Other factors – is the cost commensurate with the transaction?
Confidentiality	What are the consequences if someone other than the sender and receiver see the transaction?	Consider the entire lifecycle of the transaction. Very high protection for electronic transactions which are left sitting at a printer for a couple of days is not good value for money.
Privacy	Privacy Principles	See the Privacy Impact Assessment

Part 2 - Access and Risk

These requirements define the limits (i.e., access, liability) that are placed on the transaction.

- Access Control – the privileges that the user has, or their ability to make commitments, enter into contracts etc.
- Liability Constraints - a measure of the amount of risk assumed by the parties in a transaction.

Transaction Requirement	Describe Requirement	Comments
Access Control	What is the user allowed to do within the transaction? e.g., Read, write, modify, delete.	Other factors – what types of commitments are allowed with the transaction? e.g., commit to buy $4M in bonds.
Liability Constraints	What are the dollar values for the transactions to be undertaken? How much risk should each of the parties be willing to assume?	Other factors - insurance limits. For example the Province underwrites all land title transactions regardless of cost.

Transaction Requirement	Describe Requirement	Comments
Transaction	Is there a limit to a particular type of transaction? e.g., Purchase cards.	
Identity Issuer	What are the liability limits of the identity issuer? e.g., negligence penalties for mis-identification.	
Relying Party	What limits are applicable?	Other factors – what transactions get 'written off', is the cost of pursuing a bad transaction cost effective.
Person	What limits are applicable?	

Non-Repudiation, Evidence and Risk

Non-repudiation is seen as a key component of public key infrastructure systems and marketed as an essential component to establishing trusted interactions for e-commerce. Technology can provide a high degree of assurance that:

- the person created the transaction (evidence of origination);
- the person sent a transaction (evidence of submission) or at least that the transaction originated from a machine that may have been under that person's control; and
- the recipient received the transaction for processing (evidence of receipt).

While technical solutions (e.g., digital certificates) can provide a great deal of assurance that a transaction was conducted, no technology can guarantee the *intent* of the other party in a transaction. Therefore technical solutions can not wholly remove the risk that a person will deny the *intent* to conduct a transaction, even when there is great deal of proof that a transaction was conducted. The assumption that simply using digital certificates, biometrics or other technology solutions will automatically protect against non-repudiation is incorrect. The ability to provide an evidentiary foundation for a transaction is based on well documented policies and procedures, and the maintenance of audit and security logs. For transactions requiring evidence it may be necessary to prove that:

- each party in a transaction has evidence that can support all the true claims it may wish to make;
- each party has evidence that can cast doubt on the all false accusations made against it;
- no party has evidence to support any false accusation it might want to make.

Finally, it is essential to balance the cost of fulfilling evidentiary requirements against the risks associated with the transaction and the nature of the transaction. What are the consequences if a transaction is denied? Is the cost of maintaining evidence and pursuing defaulters justified by the cost of the transaction? The balance between acceptable risk, the cost of evidentiary requirements, and the nature of the transaction can be expressed through the liability limits of the parties involved in the transaction. The cost of high levels of authentication and transaction evidence may be too high in relation to the business case for that transaction.

Section B. Transaction Mode

The Transaction Mode documents how the transaction is conducted. For example, a transaction over the Internet will have different authentication requirements than one which occurs over a corporate Intranet. Similarly, how the system is managed may change the level of trust associated with the transaction. If a request to buy 500 computers is sent over a virtual private network, the vendor can have some confidence (for example) in the:

- identity of the buyer;
- authorization to purchase;
- integrity of the message;
- non-repudiation of the transaction.

In contrast, if the computer vendor receives a request to buy 500 computers over the Internet from *somegoof@internet.com*, the vendor would have considerably less confidence in the validity of this transaction.

The type of system is intended to be a gross measure of how much trust can be placed in a system. The two types of systems are:

- Managed/Trusted System - typically has policies and procedures to define such activities as: verifying user identity, access control, audit trails, system security and use. These types of administrative controls elicit some level of trust in the operation of the system. Alternatively, the system could also be trusted based on the ongoing relationship between the parties in the transaction. Examples of managed/trusted systems include: BC government systems, Boeing Corporation, bank systems, etc.
- Unmanaged/Untrusted System - typically does not have policies and procedures to define the use of the system, or may define a selected set of activities. Alternatively, a system may have sufficient administrative controls and still be an Untrusted system. Thus, Extranet transactions can involve either Trusted or Untrusted systems depending on the parties involved. Examples of unmanaged systems include: the Internet, a large corporation that 4

Transaction Mode	**Managed/Trusted System**		**Unmanaged/Untrusted System**
	Intranet	**Extranet**	**Internet**
Web Transactions			
E-mail			
Document Transfer			
Application (e.g. OneStop Business Registration running on Kiosks)			

Section C. Authentication Requirements

The Authentication Requirements document each component of the authentication lifecycle that will be handled by the electronic service initiative. Steps in the authentication lifecycle would include:

- collecting personal information;
- verifying that information;
- issuing a credential which indicates that the personal information has been confirmed;
- using the credential on an on-going basis.

The Authentication Requirements include:

- Type of Registration - How do persons register for a service? Registration choices could include: self-registration, third party (e.g., Law Society, Safeway) or government. Different types of registration may influence the amount of trust invested in the transaction.
- Personal Information Collected - What specific types of personal information are collected? For example, name, address, phone number, gender, etc.
- Personal Information Verified (Initial) - How is each piece of personal information verified? What kind of documentation is the individual required to present to confirm their personal information.
- Link Between Digital and Real Identity Required - How strong is the relationship between the digital and real world identities? What are the consequences to government and to other parties in a transaction if someone is mis-identified?
- Identity Credentials (see section below) - How is the individual authenticated on an ongoing basis?

Authentication Lifecycle	Description	Comments
Type of Registration	How do persons register for a service? E.g. self-registration, government, third party.	Additional factors: contract, Memorandum of Understanding, Certificate Practice Statement
Personal Information Collected	Specify the personal information collected.	
Personal Information Verified (Initial)	What personal information is verified? How is the personal information verified?	
Link Between Digital and Real Identity Required (Low / Medium / High)	How strong is the relationship between the digital and real world identities? What happens if someone is mis-identified? What are the consequences of mis-identification?	
Identity Credentials	How is the individual authenticated on an ongoing basis? See Section D	

Part 2 - Providing Solutions

Section D. Identity Credentials

The section on Identity Credentials identifies some common methods of ongoing authentication and where they might be used within the trust levels. The credentials can be employed singly, or together to create forms of multi-factor authentication. For example, in the following table digital certificates are identified as being applicable only when 'Level 3 - Verified Transaction Access' is required. However, multiple authentication factors can also be used to achieve a higher level of trust. The combination of authentication factors provides a higher level of trust than single factors of authentication. This allows a great deal of flexibility in matching the most

appropriate level of authentication to the business case. For example, the business case may not support implementation of digital certificates, but could use its existing infrastructure to achieve an equivalent level of trust.

Authentication factors are typically described as:

- What you know – e.g., password and user id, shared secret, digital certificate.
- What you have – e.g., smart card, dongle, magnetic stripe card.
- What you are – e.g., iris or facial recognition based on an individual's physical characteristics.
- What you do – e.g., voice recognition, signature or keyboard ballistics based on what an individual does.

It is important to note that the authentication factors do not imply that one method of authentication is better than another. Multi-factor authentication is more trustworthy than single factor authentication. For example, digital certificates may be invoked by a PIN or pass phrase and thus fall prey to traditional problems associated with password and user id (e.g., people write down the password or use a phrase that can be easily guessed). Combining one form of authentication with another (e.g., shared secret, token or biometric) increases its trustworthiness. However, the trustworthiness of any other form of authentication is developed and maintained in the policies and procedures used to support the technology.

Identity Credential	**Ongoing Authentication** (identify methods)	**Recommended Use by Trust Level**
None		Level 0
User Name / Password		Level 1 and above
Shared Secret		Level 2 and above
- PIN		
- Question/answer		
- Password		
Token		Level 2 and above – Business only
- Smart Card		
- Magnetic stripe card		
- Dongle		
Biometric		Level 2 and above – Business only
- Actions - signature/keyboard ballistics		
- Characteristics - facial, voice, fingerprint		
Digital certificate		Level 3 - cost factors may limit deployment for lower levels of trust.

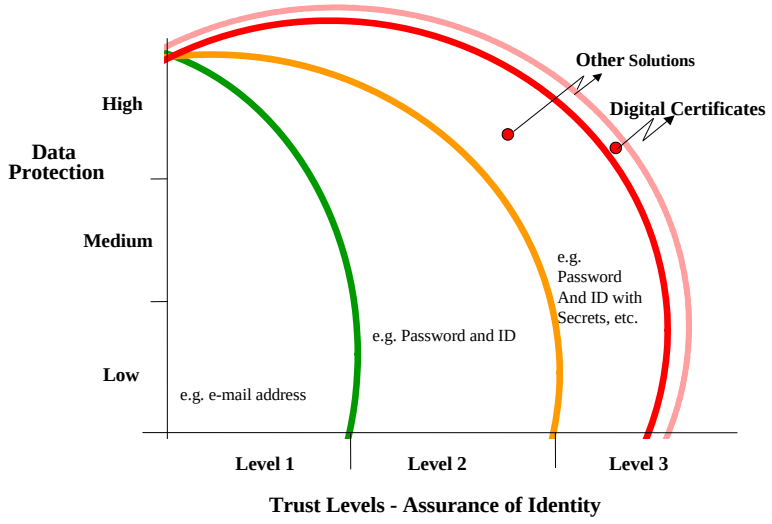
Section E. Data Protection

This section identifies methods of data protection which may be undertaken at given levels of trust. It is important to note that although they are often confused, the requirement for data protection is separate from an authentication or identity requirement. Figure 1 illustrates the relationship between data protection and identity/authentication requirements.

It is possible to have a high requirement for data protection and a low requirement for identity/authentication. The method of authentication does not protect data during transmission. For example, if personal health data is being transmitted by pseudonymous e-mail it would be prudent to protect (encrypt) that data so only the intended recipients can read the message.

Another example of the relationship between data protection and user identity is the use of a digital certificate to sign a document. A digitally signed document is transmitted in clear text and can be viewed by others unless specific measures are taken to protect the data. Differentiating between data protection and authentication requirements can provide alternative approaches to electronic service delivery initiatives.

Figure 1. Data Protection and Trust Levels



The data protection methods considered in the following table include:

- Browser certificates – for web enabled applications most browsers incorporate industry standard encryption for the data being transmitted between the user and the application. Basically any browser can 'talk' to the application;
- Virtual Private Network – allows higher levels of encryption to be set for data transmission. As the name implies only selected users can participate in the virtual network.
- Digital Certificate Encryption – allows digitally signed documents or e-mails to be encrypted regardless of the method of transmission.

Data Protection Requirement	What does it do?	Recommended Use by Trust Level
None		Level 0 to Level 2 depending on transactions
Browser Certificate for Encryption	Encrypts the data pipe between machines.	Level 1 or 2
- SSLv2 - 128 bit Encryption	Industry standard, built into most browsers	
Virtual Private Network	Encrypts the data pipe among specified partners	Level 2 or above – Business only
• Have to be known to the network to get access • Higher levels of encryption		
Digital Certificate for Encryption	Encrypts message or e-mail	Level 3
- 512 bit		
- 1024 bit		
- 2048 bit or higher		

Section F. Common Services

This section identifies services which may be delivered as part of a centralized Common Infrastructure Service. Generally these considerations are not generic to authentication or electronic transactions but involve the management of common services which may influence how a service or transaction is delivered.

Common Service	Service Requirement	Comments
Common Security Infrastructure	Is the application supported by corporate security measures?	Other factors – ministry specific security measures.
User Access Management	How often are user privileges reassessed, changed or modified? What level of Help Desk support is required?	
Service Availability	What hours is a service available for? e.g., 7 day/24 hour or other	Other factors – does the electronic service have to match regular office hours? Is there a requirement for transaction monitoring that restricts use to regular work hours.
Information Availability	Is information available at different hours than the service?	

Assigning Levels of Trust

After completing Part 1 of the Authentication Profile, a Trust Level can be assigned to the electronic service delivery initiative. The trust levels depend primarily on the amount of personal information provided and the verification process which link the digital and real world identities. However, the Transaction Requirements (Section A) may require a higher level of trust than originally indicated by the Authentication Requirements (Section C). This can be confirmed in a very subjective way by comparing the assigned Trust Level with the results of the 'Validating the Profile' checklist. If the risks and consequences of mis-identifying someone are large it to confirm that that an appropriate level of trust has been assigned.

There are four levels of trust in the Authentication Framework (See Table 1).

Level 0: Anonymous transaction – access provided for transactions that do not require or allow a person to be identified, or transactions which require protection of a person's identity. For example, access to online information about government programs or services or protecting a person's identity. Combining the transaction data with other data must not allow identification of a particular individual.

Level 1: Pseudonymous transaction – access provided for transactions that do not require a person to be identified but do require a means for further contact to deliver a product or service. For example, a note from someperson@internet.ca can not be readily translated into an individual's name, but it may be sufficient to request information, to provide some services, or on-going follow up.

Level 2: Identified transaction – access provided for transactions that require that a person be specifically identified. The nature of the transaction may require confirmation of a person's identity (e.g., name, address, birth date, etc.) and/or data linking the person to a transaction (e.g., invoice number, personal health number, etc.).

Level 3: Verified transaction - access provided for transactions that require: the person to be specifically identified; verification of the integrity of the data exchanged and the exchange itself; and, the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction. For example, a note signed with a digital certificate, audit trails and security logs may provide sufficient evidence that a specific person intended to conduct a transaction.

Table 1. Authentication Profiles And Levels Of Trust

Trust Level	Description	Authentication Requirement
0	Anonymous Transaction	Access provided for transactions that do not require or allow a person to be identified.
1	Pseudonymous Transaction	Access provided for transactions that do not require a person to be identified but do require a means for further contact to deliver a product or service.
2	Identified Transaction	Access provided for transactions that require that a person be specifically identified.
3	Verified Transaction	Access provided for transactions that require: the person to be specifically identified; verification of the integrity of the data exchanged and the exchange itself; and, the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction.

Within each trust level there will be a separate authentication profile for businesses and citizens. Business transactions may involve long standing relationships, agreements, liabilities or contractual arrangements that can create a different expectation of trust than dealing with a citizen. This is particularly relevant with Trust Levels 2 and 3. The Business Trust Level 2 must identify a business, but does not require absolute proof of the identity acting for that business. In contrast, Business Trust Level 3 requires authentication of the business, the individual and the relationship between the business and individual. Reference profiles will be prepared for each of the trust levels to serve as a comparison standard for ministry generated profiles.

As ministries complete authentication profiles for specific electronic service initiatives the comparison to the reference profiles can facilitate the use of consistent authentication practices within a ministry and across government. Similarly, as government gathers information from the authentication profiles it may be possible to:

- identify best practices; or
- develop prescriptive authentication models for use in specific circumstances.

Finally, as more ministry generated authentication profiles are gathered it will help define how the profiles are assigned to specific trust levels.

Validating the Profile

Validating the accuracy of the Authentication Profile will be problematic until government develops the knowledge base to guide electronic service delivery practices. However, one test of the Profile is to determine if the consequences of the transaction are equal to the level of trust. Table 2 defines a number of questions which assess the:

- potential risk for an incorrectly identified person to conduct a transaction; and
- magnitude or consequences associated with that risk.

The objective of this checklist is to provide a way of describing the risks and consequences associated with a transaction. Ideally the level of trust assigned to a business process based on

the Authentication Profile should adequately address these concerns. However, if the consequences of the transaction do not appear to correlate with the level of trust, the decisions made in the Authentication Profile should be re-evaluated.

Table 2. Consequences of Mis-Identification.
On a scale of 0 to 3 rate the potential risk, and magnitude of consequences of not correctly confirming the identity of parties in a transaction.

Scale: 0 (none, not appreciable), 1 (low), 2 (medium), 3 (high).

Factors	Potential Risk	Magnitude of Consequences
Incorrect Authentication may result in:		
• Inconvenience to the identity holder if someone else impersonates them		What happens if someone is impersonated within a transaction? What are the consequences for the identity holder?
• Risk to personal safety		What is the risk to personal safety if someone is impersonated within a transaction? e.g., Impersonate a doctor and provide medical advice.
• Potential release of personal or commercially confidential data		What happens if information is released to the wrong person?
• Financial loss to the relying party, the identity holder or a third party		What are the financial amounts and liabilities to be considered?
• Assists in the commission, or hinder the detection, of a criminal act		Will the transaction enable fraud or provide a stepping stone to acquiring higher level identity credentials?
• Might materially damage the identity holder's reputation or standing; or might cause significant distress to any party		For example, if someone pretends to be a member of government and endorses hate literature.
Repudiation of the transaction would result in what level of financial loss to the relying party, the identity holder or a third party.	How likely is it that the transaction would be repudiated?	What are the financial amounts and liabilities to be considered?
Repudiation of the transaction would assist in the commission, or hinder the detection, of a criminal act	How likely is it that the transaction would be repudiated?	Will denying the transaction reduce culpability for criminal activity?

Conclusion

This document defines government's general approach to authentication and specifies four levels of trust consistent with those used by the Canadian, US and UK governments. Trust levels are defined for electronic service delivery initiatives by completing an Authentication Profile.

The generic Authentication Profile described in this document is composed of six sections and describes a series of requirements or decision points which should be considered when implementing electronic services. Recommendations for technology choices are also described within the Authentication Profile. These choices provide program areas with direction, without prescribing specific methods, for conducting their business processes. As a cross-government tool, the Authentication Profile must be flexible enough to respond to a variety of business cases without slowing development.

Within each trust level there are Authentication Profiles which can be defined for Citizen and Business access to government services. Preliminary work indicates that common profiles are shared by Citizens and Business for Levels 0 and 1. Profiles for Levels 2 and 3 are different for each user group based mainly on:

- higher liability limits for transactions;
- business' ability to afford and support authentication technologies; and,
- the need to identify the business versus the individual acting for the business.

A method is also provided to test whether the risks and consequences of incorrect authentication are consistent with the level of trust defined by the Authentication Profile. This intuitive checklist provides another method of confirming that the method of authentication matches the requirements of the business case.

As government develops a knowledge base of Authentication Profiles it will be possible to refine the requirements for each of the trust levels. Similarly, it may be possible to identify best practices to standardize authentication technologies for electronic service delivery across government.

For further information contact:

Corporate Privacy and Information Access Branch
Ministry of Management Services
250-387-1992
www.mser.gov.bc.ca/foi_pop/

Appendix A. Authentication Profile Template

Defining Electronic Service Delivery Requirements

Section A. Transaction Requirements

Part 1 - Evidence of a Consequential Transaction

Transaction Requirement	Describe Requirement	Comments
Electronic Ceremony		
Evidentiary Requirements		
Non-repudiation		
Receipt Acknowledgment		
Integrity		
Confidentiality		
Privacy		

Part 2 - Access and Risk

Transaction Requirement	Describe Requirement	Comments
Access Control		
Liability Constraints		
Transaction		
Identity Issuer		
Relying Party		
Person		

Section B. Authentication Requirements

Authentication Lifecycle	Description	Comments
Type of Registration		
Personal Information Collected		
Personal Information Verified (Initial)		
Link Between Digital and Real Identity Required		
Identity Credentials		

Section C. Transaction Mode

Transaction Mode	Managed/Trusted System		Unmanaged/Untrusted System
	Intranet	Extranet	Internet
Web Transactions			
E-mail			
Document Transfer			
Application (e.g. OneStop Business Registration running on Kiosks)			

Providing Solutions

Section D. Identity Credentials

Identity Credential	Ongoing Authentication (identify methods)	Recommended Use by Trust Level
None		Level 0
User Name / Password		Level 1 and above
Shared Secret		Level 2 and above
- PIN		
- Question/answer		
- Password		
Token		Level 2 and above – Business only
- Smart Card		
- Magnetic stripe card		
- Dongle		
Biometric		Level 2 and above – Business only
- Actions - signature/keyboard ballistics		
- Characteristics - facial, voice, fingerprint		
Digital certificate		Level 3

Section E. Data Protection

Data Protection Requirement	Identify Method	Recommended Use by Trust Level
None		Level 0 to Level2 depending on transactions
Browser Certificate for Encryption		Level 1 or 2
- SSLv2 - 128 bit Encryption		
Virtual Private Network •Have to be known to the network to get access •Higher levels of encryption		Level 2 or above – Business only
Digital Certificate for Encryption		Level 3
- 512 bit		
- 1024 bit		
- 2048 bit or higher		

Section F. Common Services

Common Services	Service Requirement	Comments
Common Security Infrastructure		
User Access Management		
Service Availability		
Information Availability		

Appendix B. Validating the Profile

On a scale of 0 to 3 rate the potential risk, and magnitude of consequences, of not correctly confirming the identity of parties in a transaction.

Scale: 0 (none, not appreciable), 1 (low), 2 (medium), 3 (high).

Factors	Potential Risk	Magnitude of Consequences
Incorrect Authentication may result in:		
• Inconvenience to the identity holder if someone else impersonates them		
• Risk to personal safety		
• Potential release of personal or commercially confidential data		
• Financial loss to the relying party, the identity holder or a third party		
• Assists in the commission, or hinder the detection, of a criminal act		
• Might materially damage the identity holder's reputation or standing; or might cause significant distress to any party		
Repudiation of the transaction would result in what level of financial loss to the relying party, the identity holder or a third party.		
Repudiation of the transaction would assist in the commission, or hinder the detection, of a criminal act		

Glossary

Anonymous transaction – transactions that do not require or allow a person to be identified. For example, access to online information about government programs or services or protecting a person's identity. Combining the transaction data with other data would not allow identification of a particular person.

Authentication – the provision of assurance of a person's identity through a process of confirming or verifying information.

Authentication Profile – a set of key authentication and electronic transaction characteristics used to identify authentication requirements.

Authorization – establishes what actions or information the person is permitted to access or what goods and services the person can receive.

Confidentiality – Assurance that information is not viewed, stored or disclosed to unauthorized persons, processes, or devices.

Digital Identity (Persona) – the set of data elements (and their values) by which a person wishes to be known and thus identified in a transaction.

Eligibility – the set of data elements (and their values) used to determine if a person qualify for goods or services. For example, a person may be eligible to participate in a program, or may eligible for benefits.

Entity – any concrete or abstract thing that exists, did exist, or might exist, including associations among these things (e.g., person, object, event, idea, process, etc.).

Identified transaction – transactions that require that a person be specifically identified. The nature of the transaction may require the identification of the person (e.g., name, single business number, address, etc.), and/or data linking the person to a transaction (e.g., invoice number, personal health number, etc.).

Identity – the unique set of characteristics (data elements) by which a person is known.

Integrity – assurance that information has been maintained in a way can only be accessed or modified by those authorized to do so. Implies that an audit trail is maintained to confirm 'who did what, when and how'.

Non-repudiation – the ability to confirm the origin, transmission, receipt or processing of a transaction.

Pseudonymous transaction – access provided for transactions that do not require a person to be identified but do require a means for further contact to deliver a product or service. For example, a note from someperson@internet.ca can not be readily translated into an individual's name, but it may be sufficient to request information, to provide some services, or on-going follow up.

Relying Party – a person conducting a transaction may depend on another to provide services. For example, the BC Government is a relying party for digital certificates because it depends on an external vendor to verify the person's identity and issue a certificate. The certificates are accepted as if they were issued by the BC Government after having registered and authenticated the person.

Repudiation – the ability to deny the origin, transmission, receipt or processing of a transaction.

Verified transaction – transactions that require: the person to be specifically identified; verification of the integrity of the data exchanged and the exchange itself; and, the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction. For example, a note signed with a digital certificate, audit trails and security logs may provide sufficient evidence that a specific person intended to conduct a transaction.