Office of the Chief Information Officer

CLAIMS TECHNOLOGY STANDARD

Version 1.0
April 2010

Office of the Chief Information Officer,
Architecture, Standards and Planning Branch

-- This page left intentionally blank --

Revision History

Version	Date	Changed By	Description of Change
1.0	April 23, 2010	Patricia Wiebe	

Document Purpose

This document supports the Identity Information Management Architecture Summary that describes the Province's user-centric claims-based approach to identity management. This document sets the standards and profiles related to several industry open standard protocol specifications. It also describes standards regarding security controls and logon user experience to promote secure and usable implementations.

Audience

The intended audience for this document is technical architects, infrastructure solution designers and developers. Readers are assumed to have knowledge of application development and integration, internet-based transport and security protocols, and authentication technologies.

Advice on this Standard

Advice on this Standard can be obtained from the:

Architecture, Standards and Planning Branch
Office of the Chief Information Officer
Ministry of Information Technology and Citizens' Services

Postal Address:	PO Box 9412 Stn Prov Govt
Telephone:	(250) 387-8053
Facsimile:	(250) 953-3555
Email:	asb.cio@gov.bc.ca
Web:	http://www.cio.gov.bc.ca/cio/standards/index.page

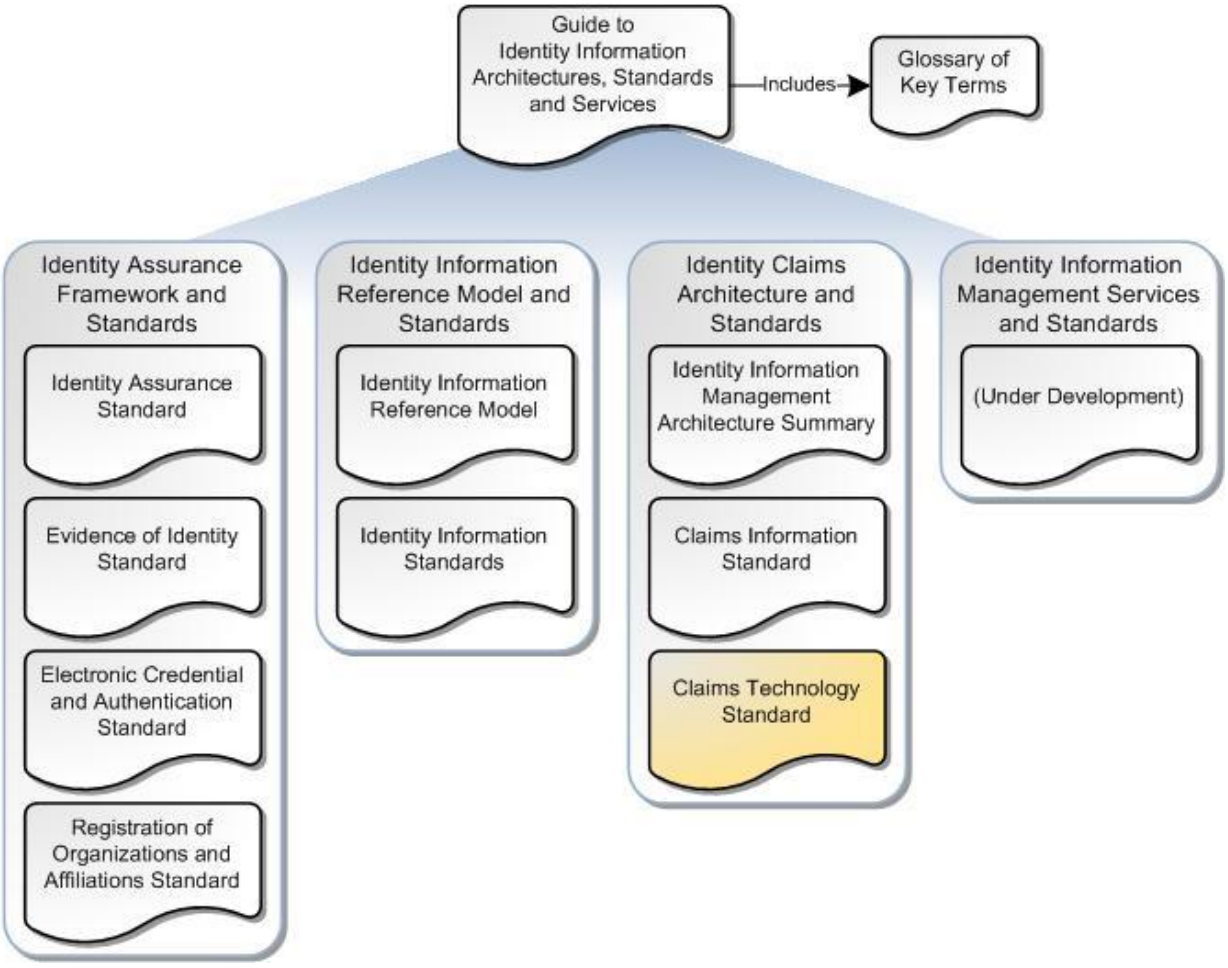
Exemptions to the standards or parts of any standard may be requested.

Identity Information Management Standards Package

This document is one of a set of standards and related documents included in the *Identity Information Management Standards Package.* The Package includes a set of architectures, frameworks, models, standards and supporting documents which, when implemented together, will result in a common, secure and trusted approach to identifying and authenticating users and subjects of government services and protected resources.

The Package can be divided into four main topic areas: Identity Assurance Framework and Standards; Identity Information Reference Model and Standards; Identity Claims Architecture and Standards; and Identity Information Management Services and Standards. The Package also contains a high-level Overview and Glossary which assist in the understanding of, and act as a navigational guide to, the other documents in the Package.

Figure 1 - The Identity Information Management Standards Package



Readers wishing to find more information on a related topic should refer to one or more of the other documents available within the package.

Table 1, below, describes the purpose of each of the Identity Information Management Standards and Documents, with the document you are currently reading highlighted. Please refer to the *Guide to Identity Information Architectures, Standards and Services* for a more comprehensive description of the documents in the Package.

Table 1 - Identity Information Management Standards and Documents

Standard/Document Name	Purpose
Guide to Identity Information Architectures, Standards and Services - *Includes Glossary of Key Terms* *(Under development)*	Provides a high-level overview of the Province of British Columbia's Identity Information Management solution and acts as a navigational guide to the supporting identity information management architectures, standards and services set out in the following four topic areas.
1. Identity Assurance Framework and Standards	
Identity Assurance Standard	Introduces the Identity Assurance Framework and sets standards for achieving increasing levels of identity assurance over multiple service delivery channels. Provides a framework for supporting standards.
Evidence of Identity Standard	Supports the *Identity Assurance Standard* by setting evidence of identity standards for registering and identity-proofing individuals to increasing levels of identification strength. Applies to both online and off-line identity management transactions and to the registration of individuals acting in multiple identity contexts (i.e., in a personal, professional or employment context).
Electronic Credential and Authentication Standard	Supports the *Identity Assurance Standard* by setting standards for issuing, managing and authenticating electronic credentials to increasing levels of strength.
Registration of Organizations and Affiliations Standard *(Under development)*	Sets information and process standards for registering organizations and affiliations between individuals and organizations.
2. Identity Information Reference Model and Standards	
Identity Information Reference Model *(Under development)*	Establishes an Identity Information Reference Model that sets out how individuals represent themselves in different identity contexts (i.e., as an employee, a professional, a student, a business representative, etc.). Provides a framework for the *Identity Information Standard.*
Identity Information Standards *(Under development)*	Sets semantic and syntactic standards for core identity and supporting information such as names, identifiers, dates and locators, as set out in the *Identity Information Reference Model*. These standards support both the *Evidence of Identity Standard* and the *Claims Information Standard*.
3. Identity Claims Architecture and Standards	
Identity Information Management Architecture Summary	Establishes a base architecture to support the exchange of identity claims between authoritative and relying parties. Introduces concepts such as user-centric claims-based architecture, authoritative parties, relying parties, identity agents, and federation, and relates these to identity assurance.

Claims Information Standard	Supports the *Identity Information Management Architecture Summary* by setting standards for the definition and use of claims. Provides definitions for the core set of claims related to the *Identity Information Standard.*
Claims Technology Standard	Supports the *Identity Information Management Architecture Summary* by setting standards and profiles related to industry open standard protocol specifications. Also sets standards for security controls and logon user experience to promote secure and usable implementations.
4. Identity Information Management Services and Standards	
(Under development)	Describes the Province's Identity Information Management Services and sets standards for their use and applicability, including: identity services, authentication services and federation services.

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

The *Claims Technology Standard* consists of a set of standards and technology profiles that, when implemented by government organizations, will provide an interoperable system that allows for the secure exchange of identity information or claims.

The *Technology Profiles Standard* sets out the specific technology profiles that describe how to implement the secure communication protocols between Relying Parties and Authoritative Parties to request claims, initiate electronic authentication, and receive the resulting claims. The *Logon User Experience Standard* sets out the user interface features to guide the user to select their choice of Authoritative Party and digital identity, and submit their credentials. These standards are meant to cover several technical architectures of Information Systems – web-based applications, desktop applications and application integration with web services.

The technology profiles set out further detail of how to implement each secure communication protocol. Profiles prescribe a subset of a base standard and specify which options are allowed or not, to make interoperability possible. They are written in a style meant to follow the style to how standards organizations write profiles of their standards. Two technology profiles are included, the *Identity Metasystem Interoperability 1.0 Profile* and *Web Services Federation Passive 1.1 Profile*, and further profiles are under development.

The *Claims Technology Standard*, with the *Claims Information Standard*, describe how to implement the claims-based architecture described in the *Identity Information Management Architecture Summary*. These standards also have direct references to the *Identity Assurance Standard* and the *Electronic Credential and Authentication Standard*.

1.1 Scope

These standards specify the technology and security controls and user interface features required to implement Authoritative Parties and Relying Parties for web-based and desktop applications. Similar standards are under development for technology and security controls related to web services.

In Scope

The *Claims Technology Standard* set specific usage of industry open standards, namely:

- Identity Metasystem Interoperability 1.0
- Web Services Federation Passive 1.1
- Security Assertion Markup Language (SAML) 2.0 Web Single Sign On (SSO)

It also sets the corresponding user experience standards on how to present user interface features related to logon, such as guiding the user to:

- Select their choice (where possible) of Authoritative Party and digital identity
- Submit their electronic credentials for their digital identity

- Consenting to send claims to the Relying Party

Out of Scope but covered in other Standards

The following are outside the scope of this Standard but, as noted, are covered by other related standards:

- specification of claims that may be exchanged (covered in the *Claims Information Standard*);
- guidance on the exchange of identity-related information within applications or web services (covered in the *Identity Information Standard*);
- specification of business rules and processes related to the data sent as claims (covered in the *Identity Information Standard*);
- specification of electronic credential technology, management and authentication processes used by Authoritative Parties (covered in the *Electronic Credential and Authentication Standard*);
- explanation of identity assurance and the information, processes and technology involved in creating and maintaining identity assurance over time (covered in the *Identity Assurance Standard*).

Out of Scope - Not covered in other Standards

The following are outside the scope of this Standard and currently outside the scope of related standards and documents:

- specification of business rules for how claims are applied to processing within Information Systems;
- guidance on how organizations may become a federation member, Authoritative Party or Relying Party;
- specification on how to establish a technical configuration between an Authoritative Party and Relying Party;
- specification of session management and controls used in an Authoritative Party or Relying Party;
- comprehensive implementation guidance.

1.2 Applicability

Applicability of this Standard

This standard applies to any BC government ministry or central agency that uses federation technology.

This standard also applies to any organization that agrees to comply through an identity federation or contractual agreement.

Organizations are responsible for ensuring that the Information Systems solutions that they build or buy are able to meet these standards. In addition, identity management shared services will be designed to comply with these standards. Where an organization uses the identity management shared services, the responsibility for complying with the standards will be devolved to the shared service.

Interpretation of this Standard

The following keywords, when used in this standard, have the following meaning:

> MUST, REQUIRED or SHALL means that the definition is an absolute requirement of the specification.
>
> MUST NOT or SHALL NOT means that the definition is an absolute prohibition of the specification.
>
> SHOULD or RECOMMENDED means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
>
> SHOULD NOT or NOT RECOMMENDED means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
>
> MAY or OPTIONAL means that an item is truly optional. (Often there is a practice to do something, however it is not a requirement.)

The definitions of these keywords are taken from the IETF RFC 2119 (See the References section). When these words are not capitalized, they are meant in their natural-language sense.

1.3 References

Normative References

The following documents are required to be read in order to understand this document.

- *Guide to Identity Information Architectures, Standards and Services*
- *Identity Information Management Architecture Summary*
- *Claims Information Standard*

Other documents are significant to this document/standard and should be read. They are required to be understood and adhered to for the implementation of the standards.

- *Identity Information Reference Model*
- *Identity Information Standard*
- *Identity Assurance Standard*

- *Electronic Credential and Authentication Standard*

Informational References

Additional documents are related and provided for informational purposes. Content within these references are generally described within this document such that it is not required to read the reference material itself for a general understanding.

- IETF RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels
  - http://www.ietf.org/rfc/rfc2119.txt
- *Cryptographic Standards for Information Protection*
  - http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf

1.4 Terms and Definitions

Key terms and definitions related to this document are set out in Appendix A and within the Terms and Definitions section of each profile. For a listing of Identity Information Management Terms and Definitions, see the *Glossary of Key Terms* in Appendix A of the *Guide to Identity Information Architectures, Standards and Services*.

1.5 Document Structure

This document has six main sections:

Section 1: The document introduction section which sets out the document's purpose, scope, and applicability.

Section 2: This section sets the requirements for which technology profiles are to be used to implement a Relying Party or an Authoritative Party based on the technical architecture of the information system.

Section 3: This section sets the corresponding requirements for logon user experience features to implement a Relying Party or an Authoritative Party.

Section 4: This section sets the requirements for how to implement the Information Card technical profile based on the OASIS Identity Metasystem Interoperability 1.0.

Section 5: This section sets the requirements for how to implement the passive (browser-based) technical profile based on the Web Services Federation Language Passive Profile 1.1.

Section 6: This section sets the requirements for communicating the results of the electronic authentication for each level in the form of an assertion to an information system or application.

2 Technology Profiles Standard

The *Technology Profiles Standard* sets out the specific technology profiles that describe how to implement the secure communication protocols between Relying Parties and Authoritative Parties to request claims, initiate electronic authentication, and receive the resulting claims.

The secure communication protocols are also referred to as federation protocols. Federation is a technical approach where one security domain has a system to authenticate users and another security domain has a system that trusts the authenticating system. This is made possible by having the authenticating domain (Authoritative Party) pass a security token to the receiving domain (Relying Party) that it understands and trusts. The security token contains claims of information about the user's identity and the authenticating domain. Often the security domains are located in different organizations connected to each other over the internet.

Federation approaches require Authoritative Parties and Relying Parties to use a common secure protocol to communicate about requests and responses for security tokens. Authoritative Parties and Relying Parties must each support the same protocol and format of security tokens in order to effectively and securely exchange messages. There are several industry open standards specifications for these. This standard adopts several specific ones, and refers to profiles that describe more specifically how to implement them.

The OASIS Identity Metasystem Interoperability 1.0 specification describes how the Identity Metasystem model is used to exchange identity and authentication data using Information Cards and Identity Agents. It builds on the Web Services Security framework and specifications, such as Web Services Trust and Web Services Security. The Identity Metasystem model is similar to the user-centric claims-based architecture described in the *Identity Information Management Architecture Summary* that the BC Government intends to use to provide the usability, privacy and security features that support the IDIM business requirements.

The Web Services Federation Language 1.1 specification describes the mechanisms to exchange identity and authentication data using web services or web browser-based methods. It is considered the earlier model of the Identity Metasystem, and also builds on the Web Services Security framework and specifications.

The Security Assertion Markup Language (SAML) 2.0 specification describes how to exchange identity, authentication and authorization data between security domains, focused on web browser-based methods.

Some implementations of federation-based secure communication protocols require the use of a web browser; these are classified as passive profiles, where the web browser is seen as a passive participant in relaying messages between two systems. The OASIS Identity Metasystem Interoperability protocol requires the use of an Identity Agent (also called an Identity Selector), which is software that resides on the user's computer. This is classified as an active profile, as the Identity Agent software actively participates in formulating and receiving messages between the Relying Party and Authoritative Party systems.

This standard promotes the use of Information Cards, making them an option for users that have Identity Agent software and Information Cards issued by Authoritative Parties; however it

recognizes that these are not yet widely deployed and permits the use of web browser-based approaches with web-based applications.

When organizations have requirements to implement the claims-based architecture, they must implement the following technology profiles.

To aid readers in navigating the standard and understanding which standards statements are applicable to their situation, this standard is divided into two sections, one for organizations acting in the role of Relying Party and one for those acting in the role of Authoritative Party. Each section is further divided into standards related to specific types of application architectures.

2.1 Technology Profiles for Relying Parties

When an organization has a requirement for claims for their Information System (also called an application), it must implement the following technology profiles for Relying Parties. These profiles describe the secure communication protocol of requesting claims and sending claims. Different profiles must be employed depending on the technical architecture of the Information System.

These technology profiles may be used for user identification and authentication at any of the identity assurance levels, unless specified otherwise below or within the profiles themselves.

2.1.1 Web-based Application

A web-based application is an Information System that is accessed by a user via a web browser over a network such as the Internet or an intranet. The application interaction is managed through a web server using HTTP or HTTPS communication. The web application may personalize the user experience or apply access control rules within the application based on the user's claims. Some examples of web-based applications are:

- Web sites for citizens or public service workers
- Web interfaces on citizen-facing electronic service applications
- Web interfaces on internal corporate, ministry or cross-organizational applications

When implementing the Relying Party interface as a web-based application, the following standard describes how to implement the secure communication protocols.

1. To implement the Relying Party interface for a web-based application, the software MUST employ the following profile:
    - Identity Metasystem Interoperability 1.0 Profile

2. The software MUST also employ one of the following passive profiles for each of the Authoritative Parties that it interacts with:
    - Web Services Federation Passive 1.1 Profile
    - Security Assertion Markup Language (SAML) 2.0 Web SSO Profile
        - (under development, contact the OCIO Architecture and Standards Branch)

The Passive Client WS-Federation 1.1 Profile is RECOMMENDED over the Passive Client SAML 2.0 SAML 2.0 Profile because it is more closely aligned with the Active Client Identity Metasystem Interoperability Profile, and thus likely to be implemented within the same software products.

3. To support the above technology profiles, the software MUST also employ the following:
    - Logon User Experience Standard

2.1.2 Desktop Application

A desktop application is an Information System that is accessed by a user through software on their computer; the client software may also interact with a server application. The desktop application may personalize the user experience or apply access control rules within the application based on the user's claims. Some examples of desktop applications are:

- Client interfaces to internal corporate or ministry server-based applications
- Smart client applications for citizen or public service workers

When implementing the Relying Party interface as a desktop application, the following standard describes how to implement the secure communication protocols.

1. To implement the Relying Party interface for a desktop application, the software MUST employ the following profile:
    - Identity Metasystem Interoperability 1.0 Profile

    It is NOT RECOMMENDED to integrate a desktop application with a web browser for the purpose of requesting claims, authenticating the user and receiving claims.

    The desktop application MUST NOT prompt the user for electronic authentication credentials for the purpose of authenticating the user with other profiles or protocols.

2. To support the above technology profiles, the software MUST also employ the following:
    - Logon User Experience Standard

2.1.3 Application Integration with Web Services

Some applications use web services technology (e.g. SOAP) to exchange information or invoke an action, either within the application or amongst a set of applications or services. This is not visible to the user and there is no user interface for web services. Web services interactions may be based on the user's claims presented through a web-based or desktop application. The web services interactions may also be based on claims made by the application itself. Some examples of application integration where this would be applied:

- One tier of an application calls another tier of the same application
- One application calls another application or service, directly or indirectly through an Enterprise Service Bus infrastructure

When implementing the Relying Party interface as a web service, the following standard describes how to implement the secure communication protocols.

1. To implement the Relying Party interface for web services integration, the software MUST employ the following profile:
    - Web Services Federation Profile
        - (under development, contact OCIO Architecture and Standards Branch)

    Further guidance will be provided in the future.

2.2 Technology Profiles for Authoritative Parties

When an organization has a requirement to receive requests for claims and send claims to Information Systems, it must implement the following technology profiles for Authoritative Parties. These profiles describe the secure communication protocol of requesting claims and sending claims. Different profiles must be employed depending on the technical architectures of the Relying Party interfaces of the Information Systems that it supports.

These technology profiles may be used for user identification and authentication at any of the identity assurance levels, unless specified otherwise below or within the profiles themselves.

Organizations implementing these technology profiles must also comply with the technology, process and management standards set in the *Electronic Credential and Authentication Standard*.

Note: These technology profiles are written from the perspective of Authoritative Parties that perform the authentication and establish the primary set of claims about a user. As described in the *Identity Information Management Architecture Summary*, some Authoritative Parties may transform or broker claims that are established by an authenticating Authoritative Party. A variation on these standards may apply. Contact the OCIO Architecture and Standards Branch for further guidance.

2.2.1 Web-based or Desktop Application

When implementing the Authoritative Party interface to support web-based or desktop applications, the following standard describes how to implement the secure communication protocols.

1. To implement the Authoritative Party interface to support web-based or desktop applications, the software MUST employ all of the following profiles:
    - Identity Metasystem Interoperability 1.0 Profile
    - Web Services Federation Passive 1.1 Profile

2. The software SHOULD also employ the following profile, to provide flexibility to support a Relying Party interface that does not implement the recommended passive client profile:
    - SAML 2.0 Web SSO Profile
        - (under development, contact the OCIO Architecture and Standards Branch)

    The Passive Client WS-Federation 1.1 Profile is RECOMMENDED over the Passive Client SAML 2.0 SAML 2.0 Profile because it is more closely aligned with the Active Client Identity Metasystem Interoperability 1.0 Profile, and likely to be implemented within the same software products.

3. To support the above technology profiles, the software MUST also employ the following:
    - Logon User Experience Standard

2.2.2 Application Integration with Web Services

When implementing the Authoritative Party interface to support web services, the following standard describes how to implement the secure communication protocols.

1. To implement the Authoritative Party interface to support web services integration, the software MUST employ the following profile:
    - Web Services Federation Profile
        - (under development, contact the OCIO Architecture and Standards Branch)

    Further guidance will be provided in the future.

3 Logon User Experience Standard

The *Logon User Experience Standard* sets out the user interface features to guide the user to select their choice of Authoritative Party and digital identity, and submit their electronic credentials.

There are several ways to logon a user to an Information System. It is desirable to have a consistent approach to presenting these logon options to the user, so that they have similar experiences within multiple Information Systems.

To support the multiple technology profiles described in the previous standard, the user interface of a website or web application needs to be adapted to accommodate logon with Information Cards as well as with one or more passive profile approaches. This standard promotes the use of Information Cards, making them an option for users that have Identity Agent software and Information Cards issued by Authoritative Parties; however it recognizes that these are not yet widely deployed and permits logon with web browser-based approaches for web-based applications.

This standard specifies the features that belong on the user interface, which focus on providing the user with choices on how to logon. This standard does not specify web page or screen layouts or specific words that need to be used.

When organizations have requirements to present a user interface in their Information Systems for the purpose of guiding users to logon, it must implement one of the following user experience standards.

This document uses the pair of terms logon and logoff; this is equivalent to the login and logout, sign on and sign off, and sign in and sign out. This standard does not specify which pair of terms must be used.

To aid readers in navigating the standard and understanding which standards statements are applicable to their situation, this standard is divided into two sections, one for organizations acting in the role of Relying Party and one for those acting in the role of Authoritative Party. Each section is further divided into standards related to specific types of application architectures.

3.1 Logon User Experience for Relying Parties

When an organization has a requirement to present a user interface in their Information System (also called an application), it must implement the following user experience approaches that describe how to guide the user to select their choice (where possible) of Authoritative Party and digital identity. Different approaches must be employed depending on the technical architecture of the Information System.

3.1.1 Web-based Application

When implementing the Relying Party interface as a web-based application, the following standard describes how to implement the user experience.

1. A Relying Party MUST display a branded web page to identify the website and the organization to which it belongs to the user before redirecting the user to logon. It MUST be provided over HTTPS to allow the user to examine the website's digital certificate.

   Extended Validation X.509 digital certificates SHOULD be used so as to instill more confidence in the user of the validity of the organization operating the website.

2. A Relying Party SHOULD display a Logon button or link that will redirect to a web page that will present the user with a set of choices on how to identify themselves. This logon options web page MAY be part of the Relying Party web-based application, or MAY be implemented by a separate web-based application such as a centralized federation or logon service. It MUST be provided over HTTPS to allow the user to examine the website's digital certificate.

3. The Relying Party's logon options web page MUST contain the following elements:

   a) A list of possible Authoritative Parties that can be used, each shown with a branded graphic image representing the organization to which it belongs and, if appropriate, the program area or distinguishing type of it. (Where there is only one possible Authoritative Party that can be used, this requirement is waived.)

      When a user selects an Authoritative Party from that list, the Relying Party MUST formulate the request message and direct the user to the Authoritative Party for authentication as described in the relevant technologies profiles.

   b) The option to logon with an Information Card, represented using the "purple i" graphic image  , consistent with the industry standard branding of Information Cards.

When a user selects to logon with an Information Card, the Relying Party MUST formulate the request message and invoke the Identity Selector software, as described in the relevant technology profiles.

4. The Relying Party's logon options page SHOULD provide a description of the required claims that a user will need to access the application.

5. The Relying Party's logon options web page MAY provide the user the option to set a preference to use the same Authoritative Party or use Information Cards on subsequent interactions with this web-based application. However, there SHOULD be a way to allow the user to change or remove their preference.

6. When a user is unable to authenticate or decides not to authenticate, the user SHOULD be able to cancel and be returned to the Relying Party interface.

7. After the Relying Party receives a security token from an Authoritative Party, indicating a successful authentication event, the Relying Party SHOULD display some of the user's identity claims, where possible, on at least the first web page of the application, so as to provide the user with visual confirmation of who they are known as. This is commonly implemented as displaying the user's name and affiliated organization in the top banner of the application.

   A Relying Party MAY also display the Authoritative Party's name on the first web page of the application, so as to provide the user with visual confirmation of the source of their identity.

8. A Relying Party SHOULD display a Logoff button or link that the user can use to end their session with the Relying Party. It is the Relying Party's responsibility to determine appropriate controls relevant to user session management, including logoff functionality.

3.1.2 Desktop Application

When implementing the Relying Party interface as a desktop application, the following standard describes how to implement the user experience.

Refer to section 2.1.2 for a description of a desktop application.

1. A Relying Party MUST provide the user the option to logon with an Information Card. This MUST be displayed using the "purple i" graphic image  , consistent with the industry standard branding of Information Cards.

   When a user selects to logon with an Information Card, the Relying Party MUST formulate the request message and invoke the Identity Selector software, as described in the technology profiles.

2. The Relying Party SHOULD provide a description of the required claims that a user will need to access the application.

3. When a user is unable to authenticate or decides not to authenticate, the user SHOULD be able to cancel and be returned to the Relying Party interface.

4. After successful authentication of the user, a Relying Party SHOULD display some of the user's identity claims, where possible, on at least the first screen of the application, so as to provide the user with visual confirmation of who they are known as. This is commonly implemented as displaying the user's name and affiliated organization in the top banner of the application.

   A Relying Party MAY also display the Authoritative Party's name on the first web page of the application, so as to provide the user with visual confirmation of the source of their identity.

5. A Relying Party SHOULD display a Logoff button that the user can use to end their session with the Relying Party. It is the Relying Party's responsibility to determine appropriate controls relevant to user session management, including logoff functionality.

3.1.3 Application Integration with Web Services

Web services do not present user interfaces to users, therefore there is no set standard for logon user experience.

3.2 Logon User Experience for Authoritative Parties

When an organization has a requirement to present a user interface for authentication to support Information Systems, it must implement the following user experience approaches that describes how to guide the user to submit their credentials for their digital identity. Different approaches must be employed depending on the technical architectures of the Relying Party interfaces that it supports.

3.2.1 Web-based or Desktop Application

When implementing the Authoritative Party interface to support web-based or desktop applications with a Relying Party interface, the following standard describes how to implement the user experience.

Refer to section 2.1.1 for a description of a web-based application and section 2.1.2 for a description of a desktop application.

1. Information Cards SHOULD be branded with a graphic image representing the organization to which it belongs, and if appropriate, the program area or distinguishing type of it.

   Other than look of the Information Card, the user experience is controlled by the Identity Agent software. The user does not directly interact with the Authoritative Party to authenticate.

2. To support the passive technology profiles (web browser-based), an Authoritative Party MUST display a branded web page to identify the website and the organization to which it belongs to the user before or while prompting the user to enter their electronic credentials. It MUST be provided over HTTPS to allow the user to examine the website's digital certificate.

   Extended Validation X.509 digital certificates SHOULD be used so as to instil more confidence in the user of the validity of the organization operating the website.

3. To support the passive technology profiles (web browser-based), an Authoritative Party SHOULD present the user with the opportunity to view the claims that are used to identify themselves to the Relying Party.

4. When a user is unable to properly authenticate or decides not to authenticate, the user SHOULD be able to cancel and be returned to the Relying Party interface.

3.2.2 Application Integration with Web Services

Web services do not present user interfaces to users, therefore there is no set standard for logon user experience.

4 Identity Metasystem Interoperability 1.0 Profile

4.1 Introduction

The purpose of this profile is to prescribe a subset of the base standard of the OASIS Identity Metasystem Interoperability 1.0 (referenced as [IMI 1.0]) specification to facilitate secure interoperability for its proposed usage within Authoritative Parties (referred to as Identity Providers), Relying Parties and Identity Agents (referred to as Identity Selectors) within the Province of British Columbia.

The IMI 1.0 specification is itself a profile of the mechanisms defined in Web Services Trust 1.2 and 1.3, Web Services Security Policy 1.1 and 1.2, and Web Services Metadata Exchange. Its purpose is to facilitate the integration of digital identity into an interoperable token issuance and consumption framework using the Information Card model. [IMI 1.0 Introduction]

The IMI 1.0 specification describes two types of Information Cards: managed Information Cards that are issued by and used to access claims within Identity Providers, and self-issued Information Cards that are issued by and used to access self-asserted claims within Identity Selector client software. This profile emphasizes the use of managed Information Cards; however it allows self-issued Information Cards where the Relying Party has a requirement for selected claims at the Low identity assurance level [BC Assurance].

The IMI 1.0 specification does not restrict the type of token used to send claims related to managed Information Cards; however this profile specifies that the only allowable token type is a SAML 1.1 assertion as described within the OASIS Web Services Security SAML Token Profile 1.1 [SAML Token 1.1]. The token profile defines the use of SAML 1.1 and 2.0 assertions as security tokens for the purpose of securing SOAP messages and SOAP message exchanges.

The IMI 1.0 specification allows for any claim type to be used. This profile specifies that the allowable set of claim types is defined within the *Claims Information Standard* [BC Claims]. This profile emphasizes the application of identity assurance as defined within the *Identity Assurance Standard* [BC Assurance].

4.2 Conformance

A Relying Party implementation conforms if it satisfies all of the MUST or MUST NOT requirements defined in Sections 4.5 and 4.9 within this profile.

An Identity Provider implementation conforms if it satisfies all of the MUST or MUST NOT requirements defined in Sections 4.6, 4.7 and 4.9 within this profile.

An Identity Selector implementation conforms if it satisfies all of the MUST or MUST NOT requirements defined in Sections 4.8 within this profile.

This profile references a number of other specifications. In order to comply with this profile, an implementation MUST implement the portions of referenced specifications necessary to comply with this profile. Conformance to IMI 1.0 is described in [IMI 1.0 Section 14].

4.3 References

Normative References

The following documents must be read and adhered to for the implementation of this standard.

[IMI 1.0] OASIS Identity Metasystem Interoperability 1.0, Jul 2009
http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.pdf

[SAML Token 1.1] OASIS Web Services Security SAML Token Profile 1.1, Feb 2006
http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

[BC Assurance] *Identity Assurance Standard*

[BC Credentials] *Electronic Credential and Authentication Standard*

[BC Claims] *Claims Information Standard*

Informational References

Additional documents are related and may be read for informational purposes.

[BC Crypto] *Cryptographic Standards for Information Protection*

http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf

4.4 Terms and Definitions

The following terms and acronyms are significant to understanding this profile.

Term	Definition
Extended Validation X.509 certificate	A special type of X.509 certificate where the Certificate Authority performs a rigorous verification of the certificate requestor's identity and authorization to obtain a certificate on behalf of their organizational and domain.
HTTPS	Secure Hypertext Transfer Protocol. A secure web communications protocol that protects information communicated to and from web servers by providing confidentiality, integrity and authentication.
Identity Provider	A service that authenticates a user and produces a security token of claims (or assertions).
Identity Selector	Software on a user's personal computer or other device that acts on behalf of the individual by facilitating the flow of claims between the Identity Provider and Relying Party. Also known as Identity Agent.
Kerberos	A computer network authentication protocol which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Term	Definition
Information Card	A digital representation of an identity card. Contains a reference to the Identity Provider that issued it where a user can get a security token containing claims about their digital identity.
Relying Party	A service that requests claims about users from one or more Authoritative Parties so that it can apply its own security or access control policies to determine whether to allow the user access to a resource or service.
SAML	Security Assertion Markup Language. An XML-based standard for exchanging authentication and authorization data between security domains.
SAML Token	A package of data that contains claims (or assertions) that follows the SAML XML format.
Security Policy	A mechanism and representation of the capabilities and security requirements for the secure exchange of messages according to the WS-SecurityPolicy specification.
Security Token	A package of data that contains claims that is typically digitally signed and encrypted to ensure security. It is used to prove identity to obtain access to information or a service.
Security Token Service (STS)	A web service that issues security tokens according to the WS-Trust specification.
Self-issued	A type of Information Card that is issued by the user themselves containing unverified identity claims. This is in contrast to managed Information Cards that are issued by a credential service and associated with verified identity claims.
SSL	Secure Sockets Layer. A communications protocol that uses digital certificates to provide security for messages sent over the internet. SSL is the predecessor of TLS.
TLS	Transport Layer Security. A communications protocol that uses digital certificates to provide security for messages sent over the internet. TLS is the successor of SSL.
URI	Uniform Resource Identifier. A string of characters used to identify a name or a resource on the internet.
Web Services Security (WSS, WS-Security)	A framework and set of specifications that extend web services (SOAP) to apply security to web service messages.
Web Services Trust (WS-Trust)	The name of an industry open standard that describes the mechanism to exchange security tokens.
X.509 Certificate	A structure and format standard for digital certificate documents based on public key infrastructure. The digital certificate binds a public key with a set of attributes about the certificate and identity of the subject of the

Term	Definition
	certificate.

4.5 Relying Party Interactions

The IMI 1.0 specification describes how a Relying Party specifies the parameters that formulate a Request Security Token message to an Identity Provider, and how the request is invoked. This profile describes the parameters that must be specified, such as the token type and required claims to satisfy the identity assurance requirements of a Relying Party.

A Relying Party MUST follow the IMI 1.0 specification with the following constraints:

1. A Relying Party MUST specify the **Token Type** of SAML 1.1 from the WSS SAML Token Profile 1.1 [SAML Token 1.1]. The token type is specified in the Identity Selector invocation parameters [IMI 1.0 Section 11.2] or as part of its Security Policy [IMI 1.0 Section 2.1]. The URI of the token type MUST be specified as:

   http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1.

2. Where **Required Claims** and **Optional Claims** are requested, a Relying Party MUST specify the claim types for the Request Security Token message from the allowable set of claim types described in [BC Claims], and NOT from the suggested claim types of commonly used personal information listed in[IMI 1.0 Section 7.5].

3. A Relying Party MUST specify its required identity assurance level [BC Assurance].

4. For a Relying Party to indicate its requirement for the **Low** identity assurance level [BC Assurance], the Relying Party MUST specify one or both of the following options:

   a. the Low Identity Assurance Level claim type as a **Required Claim**:

      http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

   b. the **Self-Issued Information Card** type as an **Issuer** [IMI 1.0 Section 2.1.1]

      http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self
      The identity assurance of claims from Self-Issued Information Cards is considered comparable to claims from Identity Providers issuing managed Information Cards at the Low identity assurance level [BC Assurance]. However, depending on claim types required from [BC Claims], self-issued Information Cards may not be suitable.

   When implementing both of the above options, they would need to be specified separately in a request to invoke the Identity Selector. These parameters cannot be combined in one Request Security Token message because the self-issued Information Card type does not understand the Low Identity Assurance Level claim type, and would yield no matching self-issued Information Card or a fault.

5. For a Relying Party to indicate its requirement for the **Medium** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as a **Required Claim**:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2

6. For a Relying Party to indicate its requirement for the **High** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as a **Required Claim**:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3

7. For a Relying Party to indicate its requirement for the **Very High** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as a **Required Claim**:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel4

8. A Relying Party MUST NOT detect and hide from the user the option to login with an Information Card based on whether an Identity Selector is enabled. [IMI 1.0 Section 11.4] Rather it SHOULD provide information to the user about obtaining the Identity Selector software.

4.6 Identity Provider Interactions

The IMI 1.0 specification describes how an Identity Provider defines its managed Information Cards, and how an Identity Provider acts upon the Request Security Token message and formulates the Security Token Response messages. This profile describes the parameters that must be specified in a managed Information Card, such as the token type and claim types to satisfy the identity assurance requirements of a Relying Party.

An Identity Provider MUST follow the IMI 1.0 specification with the following constraints:

1. An Information Card MUST specify the SAML 1.1 token from the WSS SAML token profile 1.1 [SAML Token 1.1] within the **Supported Token Types** that are offered by the Identity Provider [IMI 1.0 Section 3.1.1.3]. The URI of the token type MUST be specified as:

   http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1.

2. An Information Card SHOULD specify the set of **Supported Claims Types** that is offered by the Identity Provider [IMI 1.0 Section 3.1.1.4] appropriate for the identity assurance level [BC Assurance] associated with the Information Card. The claim types MUST be specified from the allowable set of claim types described in [BC Claims], and NOT from the suggested claim types of commonly used personal information listed in [IMI 1.0 Section 7.5].

3. An Information Card MUST specify all identity assurance levels [BC Assurance] that it can satisfy.

4. For an Identity Provider to indicate its capability to support the **Low** identity assurance level [BC Assurance], an Information Card MUST specify the following claim type in its **Supported Claim Types** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

5. For an Identity Provider to indicate its capability to support the **Medium** identity assurance level [BC Assurance], an Information Card MUST specify following claim type in its **Supported Claim Types** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2

   An Information Card SHOULD also specify the following claim type in its **Supported Claim Types** list, to allow a higher identity assurance level Information Card to be used for lower identity assurance level requests from a Relying Party:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

6. For an Identity Provider to indicate its capability to support the **High** identity assurance level [BC Assurance], an Information Card MUST specify the following claim type in its **Supported Claim Types** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3

   An Information Card SHOULD also specify the following claim types in its **Supported Claim Types** list, to allow a higher identity assurance level Information Card to be used for lower identity assurance level requests from a Relying Party:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2
   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

7. For an Identity Provider to indicate its capability to support the **Very High** identity assurance level [BC Assurance], an Information Card MUST specify the following claim type in its **Supported Claim Types** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel4

   An Information Card SHOULD also specify the following claim types in its **Supported Claim Types** list, to allow a higher identity assurance level Information Card to be used for lower identity assurance level requests from a Relying Party:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3
   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2
   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

8. An Information Card MUST **Require Token Scope** (specifically, it SHOULD include the element "RequireAppliesTo"). Requiring Token Scope reveals information to an Identity Provider about the Relying Party that an issued token will be used at. [IMI 1.0 Section 3.1.1.5, 11.7] While this is undesirable from a privacy perspective, it is necessary to identify the Relying Party for the method used to encrypt the security token.

9. An Information Card MUST specify **Require Identified Relying Parties** (specifically, it MUST include the element "RequireStrongReceiptIdentity"). [IMI 1.0 Section 3.1.1.7] This requirement prevents an Information Card from being used at Relying Parties that do not use HTTPS.

10. An Identity Provider SHOULD make the **Security Policy Metadata** of its Security Token Service endpoints available using an XML file accessible with HTTPS. [IMI 1.0 Section 3.2.2] This aids the developers of a Relying Party in configuring their Relying Party security policy.

11. An Identity Provider MUST support the **Display Token** request by an Identity Selector as described in [IMI 1.0 Section 3.3.6]. The Display Token is used to present a user-friendly representation to the user of their claims within the user interface of the Identity Selector.

4.7 Authenticating to an Identity Provider

The IMI 1.0 specification describes how an Identity Provider supports several credential types, and thus several authentication methods. These credential types are: username and password, Kerberos v5 service ticket, X.509 v3 certificate, and a self-issued Information Card. Each Information Card includes an ordered set of Security Token Service endpoints that each indicate the required credential type; this implicitly determines the authentication method to be performed when a user selects their Information Card.

This profile describes how the Identity Provider supports credential types related to the identity assurance levels requirements of a Relying Party. The Identity Provider MUST also comply with the technology, process and management standards set in the *Electronic Credentials and Authentication Standard*. [BC Credentials]

An Identity Provider MUST follow the IMI 1.0 specification with the following constraints:

1. An Identity Provider MUST act upon a Relying Party's request for a required identity assurance level [BC Assurance]. As described in this profile in section 4.5, the request is specified as a **Required Claim**.

2. For an Identity Provider to support the **Low** or **Medium** identity assurance level [BC Assurance], the Information Card MUST specify, and the Identity Provider MUST support, the **Authentication Method** for one or more of the following **Credential Types**:

    a. username and password, [IMI 1.0 Section 4.1]

    b. Kerberos v5 service ticket, [IMI 1.0 Section 4.2]

    c. X.509 v3 certificate, [IMI 1.0 Section 4.3]

    d. Self-issued information card (token) [IMI 1.0 Section 4.4] (for **Low** level only)

3. For an Identity Provider to support the **High** or **Very High** identity assurance level [BC Assurance], the Information Card MUST specify, and the Identity Provider MUST support, the **Authentication Method** for the following **Credential Type**:

    a. X.509 v3 certificate. [IMI 1.0 Section 4.3]

4. When an Identity Provider supports multiple identity assurance levels [BC Assurance], the Identity Provider SHOULD allow the user to authenticate with either of their credentials.

4.8 Identity Selectors

The IMI 1.0 specification describes how an Identity Selector enables the requests and responses for security tokens between Relying Parties and Identity Providers. Typically an Identity Selector is a free or commercially available software product that is integrated with a web browser and its operating system. Organizations MUST NOT build a custom Identity Selector.

The following describes two key characteristics that an Identity Selector must conform to for use within this profile.

An Identity Selector MUST follow the IMI 1.0 specification with the following constraints:

1. An Identity Selector MUST request an **Asymmetric Key Token** from the Identity Provider Security Token Service by default. [IMI 1.0 Section 3.3.5] This supports the security token to be encrypted before being sent to the Relying Party.

2. An Identity Selector MUST be capable of requesting a **Display Token**, and providing the option to the user to present a representation of their claims using the resulting Display Token. [IMI 1.0 Section 3.3.6]

The IMI 1.0 Section 6 specification describes how collections of Information Cards are transferred between different software implementations of Identity Selectors. This MAY be supported by Identity Selectors, however is not relevant for the near-term interoperability needs and thus is consider out of scope for this profile.

The IMI 1.0 Section 7 specification describes how self-issued Information Cards are created and used in the Identity Metasystem. This MAY be supported by Identity Selectors, however is not required in the near term as it is expected that Identity Providers will issue managed Information Cards to satisfy Relying Parties with low assurance level requirements.

4.9 Security Considerations

The IMI 1.0 specification describes how to securely interact between Relying Party and Identity Provider through the Identity Selector. This profile provides further guidance related to security controls involved in the request and response messages for security tokens.

An Identity Provider and a Relying Party MUST follow the IMI 1.0 specification with the following constraints:

1. An Identity Provider and a Relying Party MUST use the HTTPS scheme to protect all endpoints, by encrypting the transport of messages sent and authenticating the endpoints. [BC Credentials]

2. HTTPS MUST be implemented with either SSL 3.0 or TLS 1.0 or above. [BC Crypto]

3. HTTPS MUST be implemented with an X.509 digital certificate that is digitally signed by a Certificate Authority that is trusted by default by common commercially available web browsers.

4. HTTPS SHOULD be implemented with an Extended Validation type of X.509 digital certificate, so as to instill more confidence to the user of the validity of the organization operating the website. [BC Crypto]

   This also stabilizes the Common Name in the Subject field certificate attribute, used to support the calculation of the private personal identifier for the user. [IMI 1.0 Section 7.6.1]

5. The X.509 digital certificate MUST use public and private keys based on the RSA algorithm. The minimum RSA key length MUST be 1024 bits. [BC Crypto]

6. The X.509 digital certificate representing the Relying Party MUST specify a Common Name in the Subject field certificate attribute, to support the calculation of the private personal identifier for the user. [IMI 1.0 Section 7.6.1]

7. An Identity Provider MAY use the same encryption key pair for HTTPS and message security (specifically, encrypting the security token response message).

8. An Identity Provider MUST use a digital signing key pair for message security (digitally signing the security token response message) that is different than the encryption key pair.

9. An Identity Provider MUST digitally sign the security token response message that is sent to the Relying Party. [BC Credentials]

10. Digital signing SHOULD be implemented with an X.509 digital certificate that is digitally signed by a Certificate Authority (i.e. not self-signed).

11. A Relying Party MUST verify the digital signature on the security token response message, such that it is known to have come from the Identity Provider.

12. A Relying Party SHOULD perform Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) checks for certificates used in digital signing, if available. [BC Credentials]

5 Web Services Federation Passive 1.1 Profile

5.1 Introduction

The purpose of this profile is to prescribe a subset of the base standard of the Web Services Federation Language 1.1 [WS-Fed 1.1] specification to facilitate interoperability for its proposed usage within Authoritative Parties (referred to as Identity Providers), Relying Parties and web browsers within the Province of British Columbia.

The WS-Federation 1.1 specification is a framework built on Web Services Security, Web Services Trust and other Web Services specifications. It describes two profiles: the Active Requestor profile that describes the requests and responses for federated identity with a web services (SOAP) client, and the Passive Requestor profile (also called Web Requestor) that describes the same for a web browser client.

This profile is a subset of the Passive Requestor profile that is specified in [WS-Fed 1.1 Section 13].

In addition, the WS-Federation 1.1 specification does not restrict the type of token used to send claims from Identity Providers to Relying Parties; however this profile specifies that the only allowable token type is a SAML 1.1 assertion as described within the OASIS Web Services Security SAML Token Profile 1.1 [SAML Token 1.1]. The token profile defines the use of SAML 1.1 and 2.0 assertions as security tokens for the purpose of securing SOAP messages and SOAP message exchanges.

The WS-Federation 1.1 specification allows for any claim type to be used. This profile specifies that the allowable set of claim types is defined within the *Claims Information Standard* [BC Claims]. This profile emphasizes the application of identity assurance as defined within the *Identity Assurance Standard* [BC Assurance].

5.2 Conformance

A Relying Party implementation conforms if it satisfies all of the MUST or MUST NOT requirements defined in Sections 5.5 and 5.8 within this profile.

An Identity Provider implementation conforms if it satisfies all of the MUST or MUST NOT requirements defined in Sections 5.6, 5.7 and 5.8 within this profile.

This profile references a number of other specifications. In order to comply with this profile, an implementation MUST implement the portions of referenced specifications necessary to comply with this profile. Compliance to WS-Federation 1.1 is described in [WS-Federation Section 1.7].

5.3 References

Normative References

The following documents must be read and adhered to for the implementation of this standard.

[WS-Fed 1.1] Web Services Federation Language (WS-Federation) 1.1, Dec 2006
http://www.ibm.com/developerworks/library/specification/ws-fed/

[BC Assurance] *Identity Assurance Standard*

[BC Credentials] *Electronic Credential and Authentication Standard*

[BC Claims] *Claims Information Standard*

Informational References

Additional documents are related and may be read for informational purposes.

[BC Crypto] *Cryptographic Standards for Information Protection*
http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/cryptographic_standards.pdf

5.4 Terms and Definitions

The following terms and acronyms are significant to understanding this profile.

Term	Definition
Extended Validation X.509 certificate	A special type of X.509 certificate where the Certificate Authority performs a rigorous verification of the certificate requestor's identity and authorization to obtain a certificate on behalf of their organizational and domain.
HTTPS	Secure Hypertext Transfer Protocol. A secure web communications protocol that protects information communicated to and from web servers by providing confidentiality, integrity and authentication.
Identity Provider	A service that authenticates a user and produces a security token of claims (or assertions).
Kerberos	A computer network authentication protocol which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
NTLM	Microsoft's NT (New Technology) LAN (Local Area Network) Manager. A Microsoft network authentication protocol that uses a challenge-response sequence of messages between the client and server.
Relying Party	A service that requests claims about users from one or more Authoritative Parties so that it can apply its own security or access control policies to determine whether to allow the user access to a resource or service.

Term	Definition
SAML	Security Assertion Markup Language. An XML-based standard for exchanging authentication and authorization data between security domains.
SAML Token	A package of data that contains claims (or assertions) that follows the SAML XML format.
Security Token	A package of data that contains claims that is typically digitally signed and encrypted to ensure security. It is used to prove identity to obtain access to information or a service.
SSL	Secure Sockets Layer. A communications protocol that uses digital certificates to provide security for messages sent over the internet. SSL is the predecessor of TLS.
TLS	Transport Layer Security. A communications protocol that uses digital certificates to provide security for messages sent over the internet. TLS is the successor of SSL.
URI	Uniform Resource Identifier. A string of characters used to identify a name or a resource on the internet.
Web Services Federation Language (WS-Federation)	The name of an industry open standard that describes the specification of the language and mechanisms to exchange identity and authentication data using web services or web browser-based methods.
Web Services Security (WSS, WS-Security)	A framework and set of specifications that extend web services (SOAP) to apply security to web service messages.
X.509 Certificate	A structure and format standard for digital certificate documents based on public key infrastructure. The digital certificate binds a public key with a set of attributes about the certificate and identity of the subject of the certificate.

5.5 Relying Party Interactions

The WS-Federation 1.1 specification describes how a Relying Party specifies the parameters that formulate a Request Security Token message to an Identity Provider, and how the request is invoked. This profile describes the parameters that must be specified, such as the authentication level to satisfy the identity assurance requirements of a Relying Party.

A Relying Party MUST follow the WS-Federation 1.1 specification with the following constraints:

1. A Relying Party MUST specify the following parameters when requesting a security token:

    a. That the **action** to be performed is sign in, specified as "wa=wasignin1.0",

    b. The **security realm** of the Relying Party, specified as "wtrealm=<value>", where the <value> is the URI of the Relying Party,

    c. The required **authentication type**, specified as "wauth=<value>", where the <value> is the URI of the identity assurance level claim type required by the Relying Party.

    Other parameters MAY be specified. [WS-Fed 1.1 Section 13.2.1, 13.2.2] (Also, see next page.)

2. A Relying Party MUST specify its required identity assurance level [BC Assurance].

3. For a Relying Party to indicate its requirement for the **Low** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as an **Authentication Type**:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

4. For a Relying Party to indicate its requirement for the **Medium** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as an **Authentication Type**:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2

5. For a Relying Party to indicate its requirement for the **High** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as an **Authentication Type**:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3

6. For a Relying Party to indicate its requirement for the **Very High** identity assurance level [BC Assurance], the Relying Party MUST specify the following claim type as an **Authentication Type**:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel4

Other parameters, namely **Token Type** and **Required Claims**, are not easily specified by a Relying Party when requesting a security token with WS-Federation. Where it is not possible to specify these parameters, the following constraints apply:

7. The Identity Provider MUST pre-configure the following parameters on behalf of the Relying Party:
    a. That the T**oken Type** to be issued to the Relying Party is SAML 1.1 from the WSS SAML Profile 1.1 [SAML Token 1.1]. The URI of the token type is:

       http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1.

    b. The **Required Claims** to be issued to the Relying Party. These claim types MUST be specified from the allowable set of claim types described in [BC Claims].

Where it is possible to specify these parameters, the following constraints apply:

8. A Relying Party MUST use the HTTP **POST** method to submit a request security token message. This allows the Relying Party to specify parameters for token type and required claims within an XML message that cannot be specified when using the HTTP GET method.

9. A Relying Party MUST specify the **token type** of SAML 1.1 from the WSS SAML Token Profile 1.1 [SAML Token 1.1]. The token type is specified within the <wst:RequestSecurityToken> element as follows:

```
<wst:TokenType> http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1 </wst:TokenType>
```

10. Where **claims** are requested, a Relying Party MUST specify the claim types for the Request Security Token message from the allowable set of claim types described in [BC Claims]. The required claims are specified within the <wst:RequestSecurityToken> as described in [WS-Trust 1.3 Section 4.1] with a Claims Dialect as described in [IMI 1.0 Section 2.1.3], as follows:

```
<wst:Claims Dialect="http://schemas.xmlsoap.org/ws/2005/05/identity">
      <ic:ClaimType Uri="..." />
      <ic:ClaimType Uri="..." Optional="true" />
</wst:Claims>
```

Optional claims are indicated with the "Optional" attribute on the Claim Type.

The following is an example of the XML element of <wst:RequestSecurityToken> that highlights the token type and claims parameters:

```
<wst:RequestSecurityToken>
      <wst:TokenType> ... </wst:TokenType>
      <wst:RequestType> ... </wst:RequestType>
      <wst:Claims Dialect="..."> ... </wst:Claims>
      ...
</wst:RequestSecurityToken>
```

11. A Relying Party MAY use either the **Authentication Type** approach (as mentioned in 1.c.) or the **Required Claims** approach (as mentioned in 10.) to indicate its requirement for identity assurance.

5.6 Identity Provider Interactions

The WS-Federation 1.1 specification describes how an Identity Provider acts upon the Request Security Token message and formulates the Security Token Response messages. This profile describes how the responses are returned and how an Identity Provider uses a Federation Metadata document to indicate what it supports.

An Identity Provider MUST follow the WS-Federation 1.1 specification with the following constraints:

1. An Identity Provider MUST use the HTTP **POST** method to submit a security token response message. [WS-Fed 1.1 Section 13.2.3]

2. An Identity Provider MUST specify the following parameters when responding to a request for a security token:

    a. That the **action** to be performed is sign in, specified as "wa=wasignin1.0",

    b. The **security token** issued by the Identity Provider, specified as "wresult=<value>", where the <value> is the encoded and encrypted XML message.

    Other parameters MAY be specified. [WS-Fed 1.1 Section 13.2.3]

3. An Identity Provider SHOULD provide a **Federation Metadata** document describing its service offering. This aids the developers of a Relying Party to configure the requests for security token.

4. A Federation Metadata document SHOULD specify the SAML 1.1 token from the WSS SAML token profile 1.1 [SAML Token 1.1] within the **Token Types Offered** that can be issued by the Identity Provider. [WS-Fed 1.1 Section 3.1.11]

    http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1.

5. A Federation Metadata document SHOULD specify the set of **Claim Types Offered** that can be issued by the Identity Provider [WS-Fed 1.1 Section 3.1.12] relevant to the identity assurance level [BC Assurance] requested. The claim types MUST be specified from the allowable set of claim types described in [BC Claims].

6. A Federation Metadata document SHOULD specify all identity assurance levels [BC Assurance] that it can satisfy as Claim Types Offered.

7. For an Identity Provider to indicate its capability to support the **Low** identity assurance level [BC Assurance], a Federation Metadata document SHOULD specify the following claim type in its **Claim Types Offered** list:

http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

8. For an Identity Provider to indicate its capability to support the **Medium** identity assurance level [BC Assurance], a Federation Metadata document SHOULD specify the following claim type in its **Claim Types Offered** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2

   A Federation Metadata document SHOULD also specify the following claim type in its **Claim Types Offered** list, to allow a higher identity assurance level to be used for lower identity assurance requests from a Relying Party:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

9. For an Identity Provider to indicate its capability to support the **High** identity assurance level [BC Assurance], a Federation Metadata document SHOULD specify the following claim type in its **Claim Types Offered** list:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3

   A Federation Metadata document SHOULD also specify the following claim types in its **Claim Types Offered** list, to allow a higher identity assurance level to be used for lower identity assurance requests from a Relying Party:

   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2
   http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

10. For an Identity Provider to indicate its capability to support the **Very High** identity assurance level [BC Assurance], a Federation Metadata document SHOULD specify the following claim type in its **Claim Types Offered** list:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel4

    A Federation Metadata document SHOULD also specify the following claim types in its **Claim Types Offered** list, to allow a higher identity assurance level to be used for lower identity assurance requests from a Relying Party:

    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3
    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2
    http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1

5.7 Authenticating to an Identity Provider

The WS-Federation 1.1 specification describes how an Identity Provider supports multiple credential types, and thus multiple authentication methods. It does not describe all possible credential types and authentication methods, but rather describes the most common ones: username and password, NTLM and Kerberos tickets, and X.509 v3 certificates.

This profile describes how the Identity Provider supports credential types related to the identity assurance levels requirements of a Relying Party. The Identity Provider MUST also comply with the technology, process and management standards set in the *Electronic Credentials and Authentication Standard*. [BC Credentials]

An Identity Provider MUST follow the WS-Federation 1.1 specification with the following constraints:

1. An Identity Provider MUST act upon a Relying Party's request for a required identity assurance level [BC Assurance]. As described in this profile in section 5.5, the request may be specified as an **Authentication Type** or as a **Required Claim**. The Identity Provider SHOULD support both ways.

2. When an Identity Provider supports multiple credential types [BC Credentials] that could be used to satisfy a particular identity assurance requirement [BC Assurance], the Identity Provider SHOULD present the user with options and allow the user to select which of their credentials to authenticate with.

3. For an Identity Provider to support the **Low** or **Medium** identity assurance level [BC Assurance], the Identity Provider MUST support the **Authentication Method** for one or more of the following **Credential Types**:

    a. username and password,

    b. Microsoft-based NTLM v2 or Kerberos v5 service ticket,

    c. Other credential types described in [BC Credentials] suitable for **Low** or **Medium** identity assurance levels,

    d. Other credential types suitable for **High** or **Very High** identity assurance levels.

4. For an Identity Provider to support the **High** or **Very High** identity assurance level [BC Assurance], the Identity Provider MUST support the **Authentication Method** for one or more of the following **Credential Types**:

    a. X.509 v3 certificate

    b. Other credential types described in [BC Credentials] suitable for **High** or **Very High** identity assurance levels.

5.8 Security Considerations

The WS-Federation 1.1 specification describes how to securely interact between Relying Party and Identity Provider. Specifically this profile is concerned with the Passive Requestor Profile, thus the interactions go through a web browser. This profile provides further guidance related to security controls involved in the request and response messages for security tokens.

An Identity Provider and a Relying Party MUST follow the WS-Federation 1.1 specification with the following constraints:

1. An Identity Provider and a Relying Party MUST use the HTTPS scheme to protect all endpoints, by encrypting the transport of messages sent and authenticating the endpoints. [BC Credentials]
2. HTTPS MUST be implemented with either SSL 3.0 or TLS 1.0 or above. [BC Crypto]
3. HTTPS MUST be implemented with an X.509 digital certificate that is digitally signed by a Certificate Authority that is trusted by default by common commercially available web browsers.
4. HTTPS SHOULD be implemented with an Extended Validation type of X.509 digital certificate, so as to instill more confidence to the user of the validity of the organization operating the website. [BC Crypto]
5. The X.509 digital certificate MUST use public and private keys based on the RSA algorithm. The minimum RSA key length MUST be 1024 bits. [BC Crypto]
6. An Identity Provider MAY use the same encryption key pair for HTTPS and message security (specifically, encrypting the security token response message).
7. An Identity Provider MUST use a digital signing key pair for message security (digitally signing the security token response message) that is different than the encryption key pair.
8. An Identity Provider MUST digitally sign the security token response message that is sent to the Relying Party. [WS-Fed 1.1 Section 13.6.4] [BC Credentials]
9. Digital signing SHOULD be implemented with an X.509 digital certificate that is digitally signed by a Certificate Authority (i.e. not self-signed).
10. A Relying Party MUST verify the digital signature on the security token response message, such that it is known to have come from the Identity Provider.
11. A Relying Party SHOULD perform Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) checks for certificates used to perform digital signing, if available.

APPENDIX A – TERMS AND DEFINITIONS

This appendix contains definitions for the key terms used in this document.

For a listing of the terms commonly used in all the standards and documents contained in the Identity Information Standards Package, see the *Glossary of Key Terms* set out in Appendix A of the *Guide to Identity Information Architectures, Standards and Services*.

Term	Definition
Authoritative Party	An organization (or person) that is trusted to be an authority on the identity related attributes or roles associated with users and subjects of services. Authoritative Parties may issue credentials.
Active Client	Client software that is an active participant and intermediary in relaying messages between two systems. Refers to software that is capable of being a web services (SOAP) client. Also called Active Requestor. In this context, the Identity Agent or Identity Selector is an active client.
Desktop Application	An information system that is accessed by a user through software on their computer; the client software may also interact with a server application over a network such as the internet or intranet.
Extended Validation X.509 certificate	A special type of X.509 certificate where the Certificate Authority performs a rigorous verification of the certificate requestor's identity and authorization to obtain a certificate on behalf of their organizational and domain.
Federation	A technical approach where one security domain has a system to authenticate users and another security domain has a system that trusts the authenticating system.
HTTPS	Secure Hypertext Transfer Protocol. A secure web communications protocol that protects information communicated to and from web servers by providing confidentiality, integrity and authentication.
Identity Metasystem	A model and architecture that represents how existing identity management infrastructure can be leveraged to provide secure access to information and systems. Similar to claims-based architecture.
Identity Metasystem Interoperability	The name of an industry open standard that describes the specification of the negotiation and exchange of identity and authentication data using Information Cards and Identity Agents.
Identity Selector	Software on a user's personal computer or other device that acts on behalf of the individual by facilitating the flow of claims between the Identity Provider and Relying Party. Also known as Identity Agent.
Information Card	A digital representation of an identity card. Contains a reference to the Identity Provider that issued it where a user can get a security token

Term	Definition
	containing claims about their digital identity.
OASIS	Organization for the Advancement of Structured Information Standards. A standards body with technical committees that develop industry open standards related to information exchange and technology.
Passive Client	Client software that is a passive participant in relaying messages between two systems. Refers to software that is not capable of being a web services (SOAP) client. Also called Passive Requestor. In this context, the web browser is a passive client.
Profile	A prescribed subset of a base standard that specifies which options are allowed or not, to make interoperability possible.
Relying Party	A service that requests claims about users from one or more Authoritative Parties so that it can apply its own security or access control policies to determine whether to allow the user access to a resource or service.
SAML	Security Assertion Markup Language. An XML-based standard for exchanging authentication and authorization data between security domains.
SAML Token	A package of data that contains claims (or assertions) that follows the SAML XML format.
Security Token	A package of data that contains claims that is typically digitally signed and encrypted to ensure security. It is used to prove identity to obtain access to information or a service.
SSL	Secure Sockets Layer. A communications protocol that uses digital certificates to provide security for messages sent over the internet. SSL is the predecessor of TLS.
TLS	Transport Layer Security. A communications protocol that uses digital certificates to provide security for messages sent over the internet. TLS is the successor of SSL.
URI	Uniform Resource Identifier. A string of characters used to identify a name or a resource on the internet.
Web-based Application	An information system that is accessed by a user via a web browser over a network such as the internet or intranet.
Web Services	A technical approach to support interoperable machine-to-machine interaction over a network. The interaction may be to exchange information or invoke an action. It typically uses SOAP XML-based messages communicated over HTTP/HTTPS.
Web Services Federation Language (WS-Federation)	The name of an industry open standard that describes the specification of the language and mechanisms to exchange identity and authentication data using web services or web browser-based methods.

Term	Definition
Web Services Security (WSS, WS-Security)	A framework and set of specifications that extend web services (SOAP) to apply security to web service messages.
Web Services Trust (WS-Trust)	The name of an industry open standard that describes the mechanism to exchange security tokens.
X.509 Certificate	A structure and format standard for digital certificate documents based on public key infrastructure. The digital certificate binds a public key with a set of attributes about the certificate and identity of the subject of the certificate.