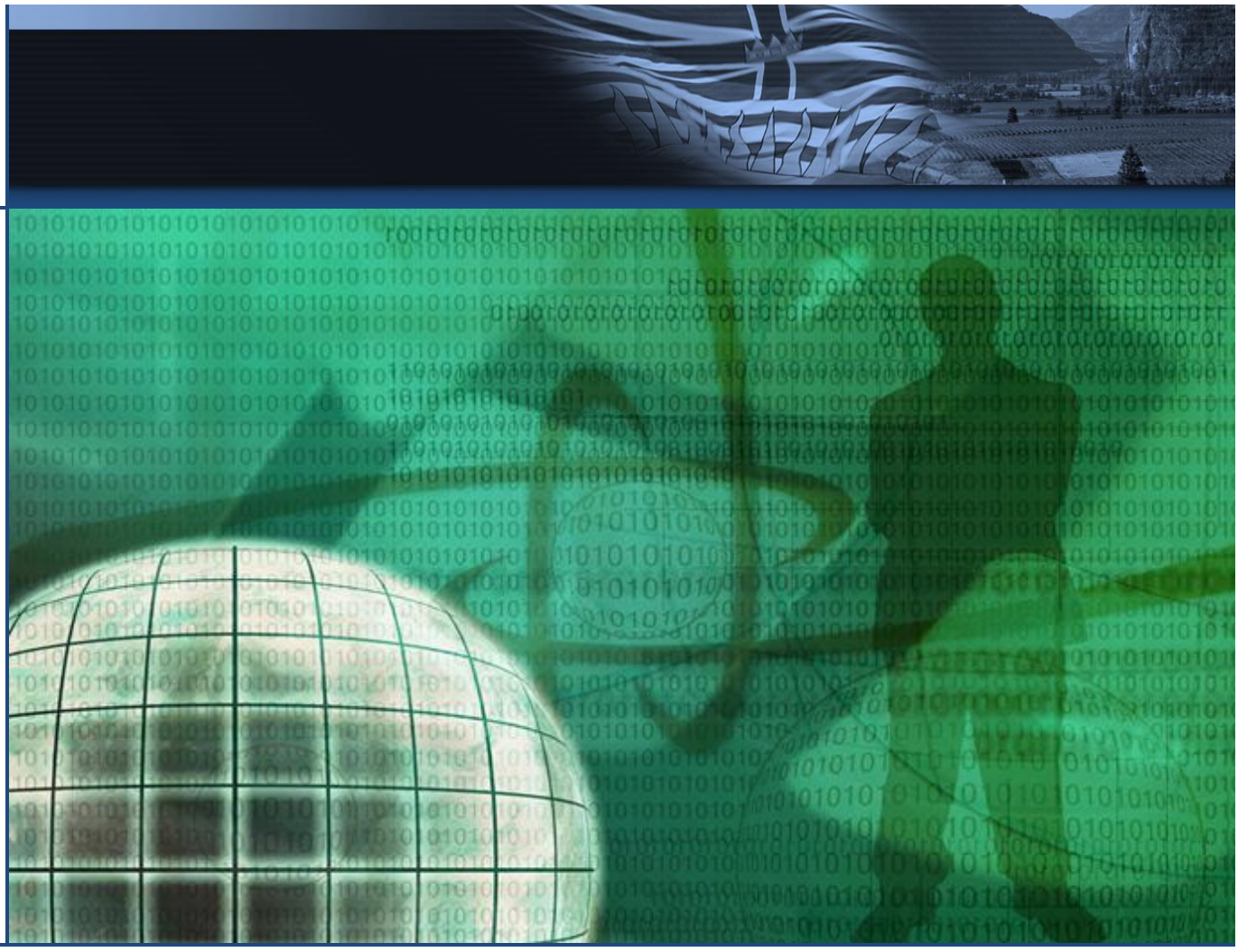
Office of the Chief Information Officer

CLAIMS INFORMATION 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 regarding how to define and use claims, and provides definitions for the core set of claims related to the Identity Information Reference Model.

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

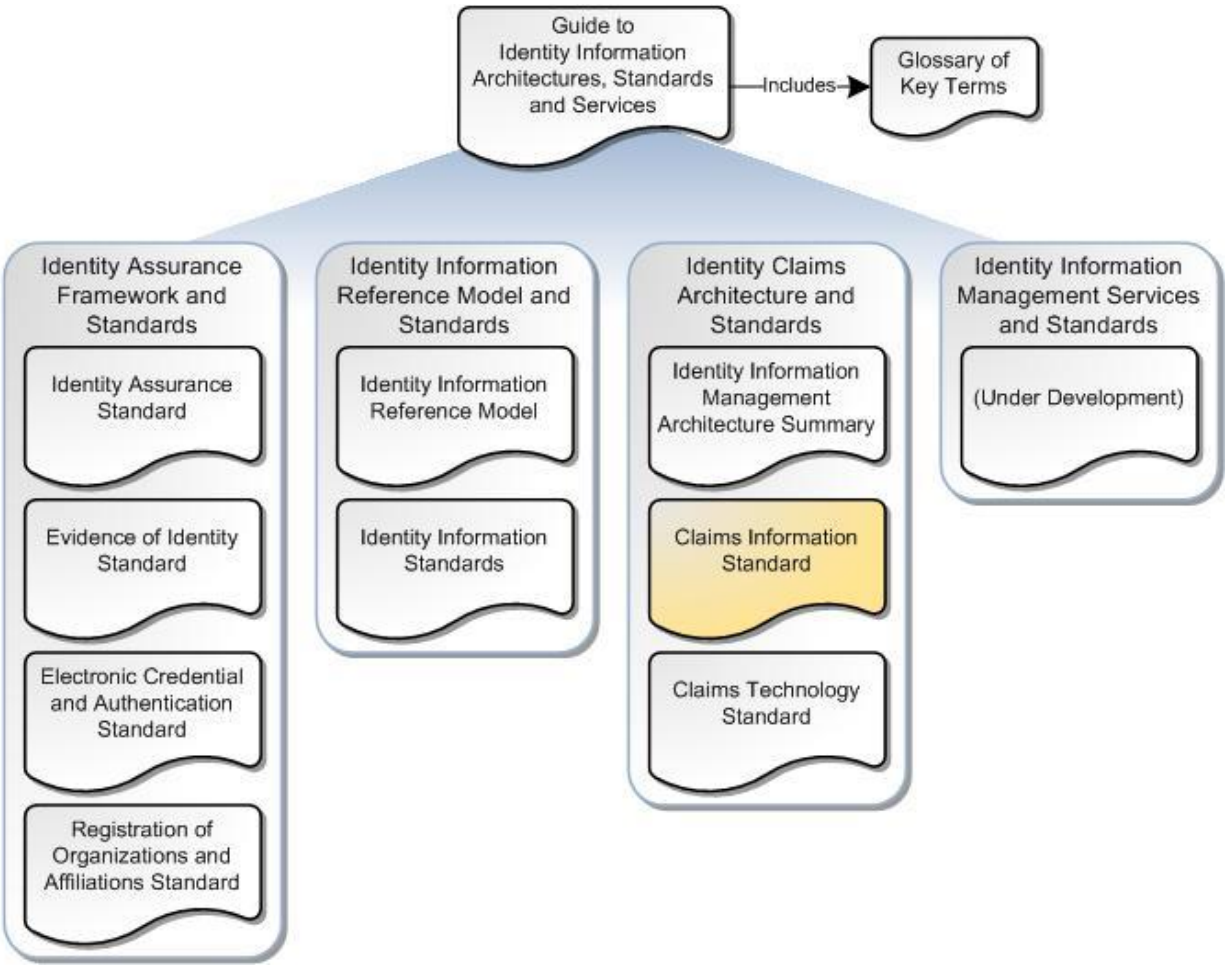
Exemptions to the standards or parts of any standard may be requested.

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 documents in the Package, with the document you are currently reading highlighted. Refer to the *Guide to Identity Information to 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 Information Standard* consists of a set of standards, guides and definitions of claims that, when implemented by government organizations, will support an interoperable system to securely exchange identity information or claims.

The *Claims Information Guide* describes the concept of a claim, how it relates to the claims-based architecture, how claims are intended to be used (such as for user access control or personalization), and how a claim is described. The *Claim Usage Standard* sets out the specific rules about which claims are appropriate to be used in accordance with the level of identity assurance requirements of the Relying Party.

The *Claim Definitions* provides definitions for the core set of claims related to the Identity Information Reference Model. These definitions focus on identity information about individuals representing themselves in different identity contexts (i.e. as an employee, a professional, a business representative). Additionally, the definitions include claims about identity assurance and the Authoritative Party that is issuing the claims.

The *Claim Definition Lifecycle Guide* describes the rules and processes about how additional claims can be defined for use within Information Systems that implement the claims-based architecture.

The *Claims Information Standard*, with the *Claims Technology 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*, the *Identity Information Reference Model* and the *Identity Information Standard*.

1.1 Scope

These standards describe the claims information model, how it relates to the Identity Information Reference Model and specify appropriate use of a core set of defined claims.

In Scope

The *Claims Information Standard* define a core set of claims about:

- individuals acting in a personal context
- individuals acting in affiliation-related identity contexts, specifically
    - employment context
    - professional context
- organizations to support the above affiliation-related identity contexts
- the identity assurance level attained
- the Authoritative Party system issuing the claims

Specifically, this first set of defined claims express the data about:

- names
- identifiers

Future versions of this standard are expected to define claims for

- birth date
- place of birth
- locators such as addresses, telephone numbers, email addresses

Additional analysis is needed to further develop claims about organization and business identifiers, and to develop additional claims such as employment and professional identifiers, and roles.

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 secure communication protocols that may be used to exchange claims (covered in the *Claims Technology 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*);
- 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 to become a federation member and how to establish a technical configuration between an Authoritative Party and Relying Party;
- specification of defined claims about a system, application or other technical environment characteristics, or about a user's authorization and entitlements;
- 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*
- *Identity Information Reference Model*

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 Standard*
- *Identity Assurance 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
- *Claims Technology Standard*

1.4 Terms and Definitions

Key terms and definitions related to this document are set out in Appendix A and within section 2.1. 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 five main sections:

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

Section 2: This section sets context and describes core concepts related to claims, how they are used, and the information model of a claim definition.

Section 3: This section sets the requirements for how claims are issued by an Authoritative Party for use by a Relying Party.

Section 4: This section lists the claim definitions, organized by claims about individuals, organizations, affiliations, Authoritative Party systems and identity assurance.

Section 5: This section describes how claims are defined and managed through their lifecycle.

2 Claims Information Guide

The guide describes the concept of a claim, how it relates to the claims-based architecture, how claims are intended to be used (such as for access control or personalization), and how a claim is described. This sets the context for the *Claim Usage Standard*, which sets out the specific rules about which claims are appropriate to be used in accordance with the level of identity assurance requirements of the Relying Party. It also provides the background for the *Claim Definitions*, which define a core set of claims.

2.1 Claims Information

As described in the *Identity Information Management Architecture Summary*, a claim is an assertion that something is true or factual.

Claims may be assertions of core identity information such as a name and birth date; they may be roles and privileges that have been granted to a user or subject. Claims may also indicate the level of assurance that a consumer of the claims (Relying Party) should consider. Also, claims may be derived from other claims, such as a claim that an individual is over 18 years of age (derived from birth date) or a resident of a municipality (derived from residential address).

There are many authorities for claim information. Government is an authority for personal identification claims, through organizations such as Vital Statistics. Government is also an authority for business identity claims, through corporate and business registries. Organizations are an authority for claims about their employees, and professional bodies are for their members. Also, individuals are the authority for some claims about themselves.

Technically, a claim is an attribute related to an identity in a particular context. A set of claims are packaged into a security token which is sent from Authoritative Party to Relying Party using one of the secure communications protocols described in the *Claims Technology Profiles*. Claims are pulled from data stored about identities within directories and databases.

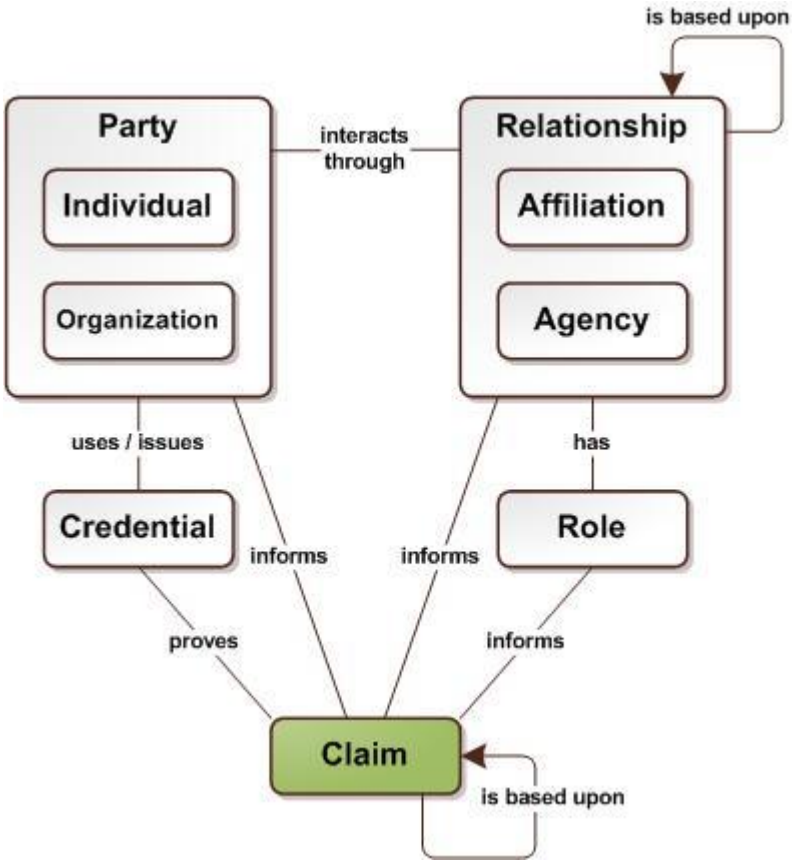
An identity is commonly described by many different claims. The *Claim Definitions* in section 4 define a core set of claims about individuals acting in a personal context or an affiliation-related context, specifically employment and professional contexts. Also included are claims about the identity of the affiliated organizations. To support the consumer of the claims (Relying Party), the identity assurance claim is used to communicate the amount of confidence that should be placed in the identity, based on earlier identity proofing processes and electronic credential issuance and authentication events.

Additional claims will be defined, as needed, to further describe identities beyond the core information. For example, claims may be developed to support an individual's contact information like address, phone number and email address, in their personal or affiliated contexts. The processes related to defining claims are described in *Claim Definition Lifecycle Guide*.

2.2 Claims Information Model

The *Identity Information Reference Model* sets out how individuals represent themselves in different identity contexts (i.e. as an employee, a professional, a student, a business representative, etc.). The document includes the following diagram which illustrates the associations of significant things in the model. Claims (shown highlighted in green) can be made about a party's identity, relationship, role or possession / ownership of a credential.

Figure 2 - Identity Information Reference Model



Some claims may come from information not shown in the above model. For example, information about the Authoritative Party and Relying Party are not shown in this model. Claims could be defined in the future to describe and identify the systems interacting or other contextual information related to the systems environment in which the information is being sent.

2.3 Claims Usage

Relying Parties consume claims as a form of input data that can then be used a variety of ways. Claims are commonly used for

- Identity resolution, to uniquely link an authenticated individual with previously stored information about them,
- Access control, to determine whether an individual should be authorized to access resources within Information Systems, and
- Personalization, to provide a customized user experience based on information about the user.

Given that Relying Parties consume claims for a particular use, they also are in control of requesting the claims that are needed from an Authoritative Party. The mechanism to specify which claims are to be requested from the Authoritative Party is described in the *Claims Technology Standard*. The standards and rules about how claims are requested and sent is set out in the *Claims Usage Standard* in section 3.

There are several general characteristics of claims that will be described here to elaborate their meaning and set the context for the *Claim Definitions* in section 4.

As already described in the previous section, claims are descriptive of specific entities like individuals, organizations and affiliation relationships.

Claims describe different types of information. In alignment with the core set of identity information described in the *Identity Information Reference Model*, claims are defined primarily for names and identifiers. Additional claims may be developed to exchange information about dates, addresses, numbers and codes.

A claim generally contains one piece of information; a Relying Party typically requires a set of claims to collectively describe an identity. For example, the name of an individual may be described by a “Surname” claim and a “Given Name” claim. To uniquely describe an individual, for the purposes of identity resolution, a Relying Party generally needs to request claims about core identity information (full legal name, date of birth and place of birth) plus possibly some additional information on file to support linking the individual to their records.

As a claim is a statement or assertion that something is true or factual, it is important to also understand how that assertion is made and what it is based on. There are often varying levels of trust in the quality or correctness of the information.

Some claims are self-asserted by an individual, thus the trust in the information depends on the trust that a Relying Party has in the individual themselves. A common example of a self-asserted claim made by an individual is their contact information (such as personal email address); it may change often and is not required to be registered or verified with an authority.

An organization may facilitate the storage of self-asserted data and issuing of those claims for the convenience of the individual. For example, an individual may able store their self-asserted contact information within an Authoritative Party and allow it to be shared as claims.

Most claims are verified through some process so as to instil trust in the quality and correctness of the information. It is also very important that an Authoritative Party is responsible to provide

reliable up-to-date information. An individual's core identity information is verified through the identity proofing business processes described in the *Identity Assurance Standard*. This results in a measure of confidence of the identity information about an individual which contributes to the identity assurance claim.

The trust in claims is also inferred by the trust that a Relying Party has that the source of claims is authoritative on the information. For example, the Vital Statistics organization is widely recognized to be the authority on birth names because of their significant involvement in the birth registration business process. For some information, the authoritative source is unclear.

Sometimes an organization is able to assert claims without being the original authority for the information conveyed in claims. These organizations may be considered "proxy" Authoritative Parties based on trust in their verification processes and links back to the original authority. For example, the driver licensing authority verifies an individual's legal name and date of birth through verification processes and links to the individual's birth certificate.

2.4 Claim Definition Information Model

A claim needs to be well-defined in order for an Authoritative Party and Relying Party to have a common understanding of the meaning and format of the information being sent in a claim. A claim definition is composed of several pieces of information:

- Claim name
- Claim type (which is also the claim definition's unique identifier)
- Claim business description
- Claim technical description
- Owner

The owner of the claim definition represents the organization and contact person who is responsible for ensuring correctness and maintaining the descriptions.

Claim definitions also specify business and technical constraints about what is an allowable value. For example, a "Surname" claim may be constrained to a 30 characters in length, and an "Age" claim may be constrained to a positive integer value.

Some claim definitions constrain the claim to specific defined values. For example, an "Is Over Age 18" claim may be constrained to a choice from a set of "True", "False", or "Unknown". A "Business Role" claim may be constrained to be chosen from a set that includes common roles such as "Licensed Physician", "Lawyer", "Social Worker" and "Accountant". (There may also be other types of role claims, such as application-specific roles.) A set of defined values may grow incrementally, and requires well-defined business descriptions, specific owners of those definitions and clear change management processes.

The following diagram shows that claim definitions are generally composed of several describing attributes, and that a claim definition may be constrained by a set of claim values. Claim values are also composed of several describing attributes:

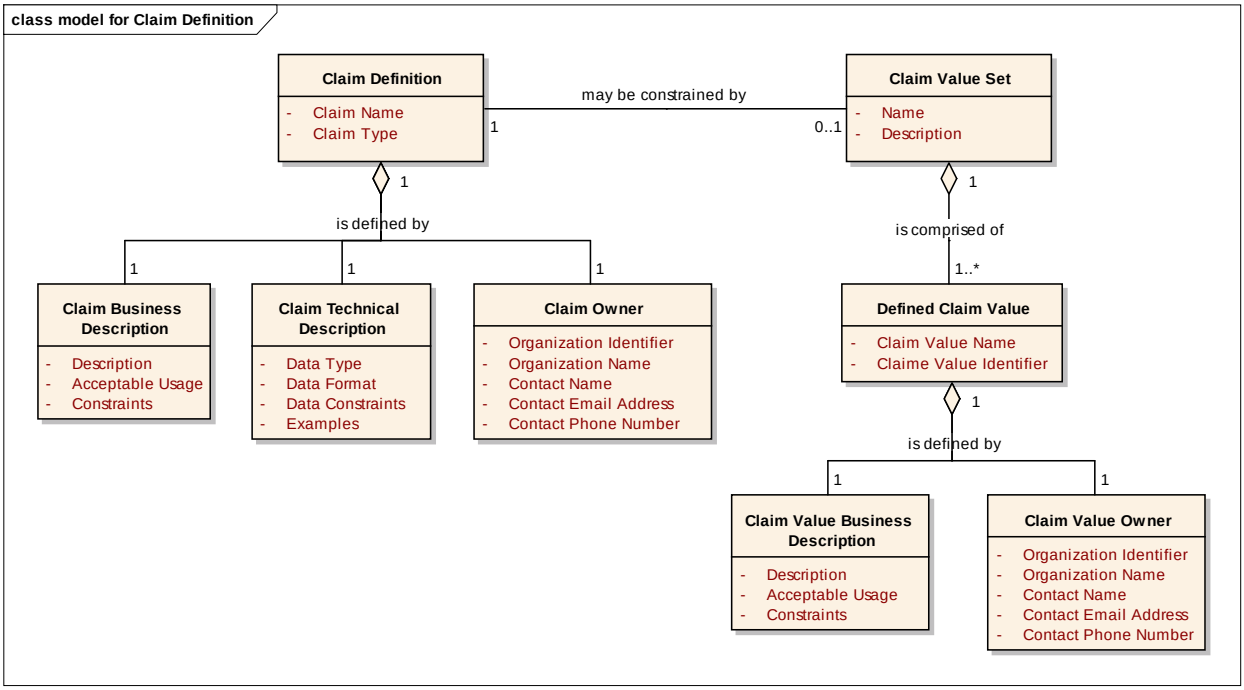
- Claim value name
- Claim value type (which is the claim value's unique identifier)
- Claim value business description

- Owner

A claim value does not have its own technical description, as it inherits what is described in the claim definition's technical description.

Each claim value may have a distinct owner that is responsible for ensuring correctness and maintaining the business description.

Figure 3 - Class Diagram of Claim Definition



The technology profiles within *Claims Technology Standard* require that each claim be described with a Claim Type in the syntax of a Uniform Resource Identifier (URI). The *Identifier Standard* within the *Identity Information Standard* provides guidance on how URIs are defined.

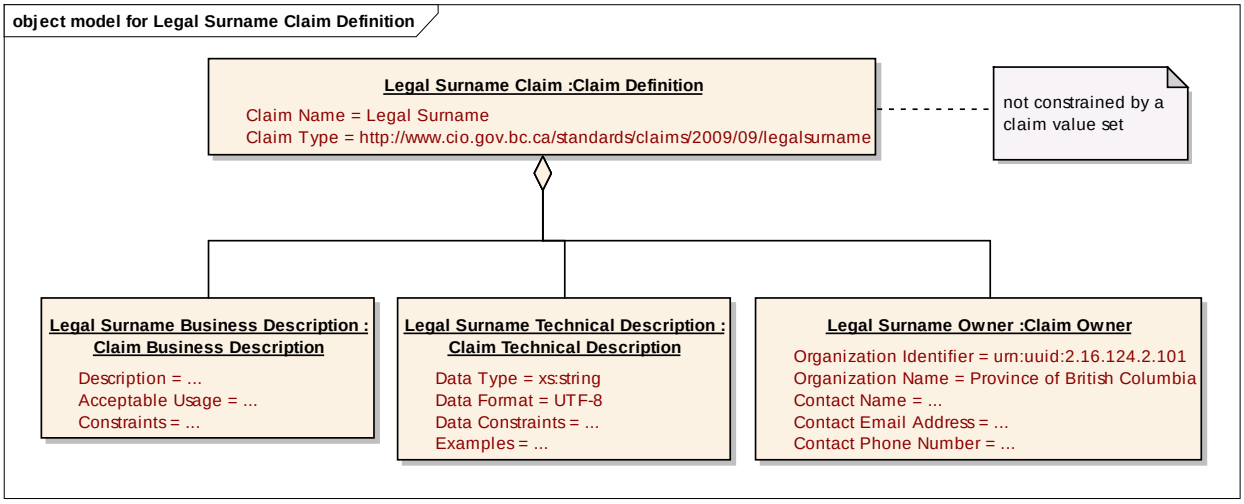
The above model is not a strict data model, as it does not describe the specific data types of each attribute, nor does it represent metadata attributes for change management and audit purposes. The implementer of the information model may adapt the model for implementation.

To reinforce the concepts in the above diagram, two examples will be presented in the following sections to represent instantiations of the information model. The first example shows the claim definition for a "Legal Surname" claim, and the second example shows how a claim value set is relevant for a "Business Role" claim.

Example Claim Definition for "Legal Surname"

The following diagram shows an instantiation of the Claim Definition Information Model for a "Legal Surname" claim. The claim definition is composed of a business description, technical description and owner.

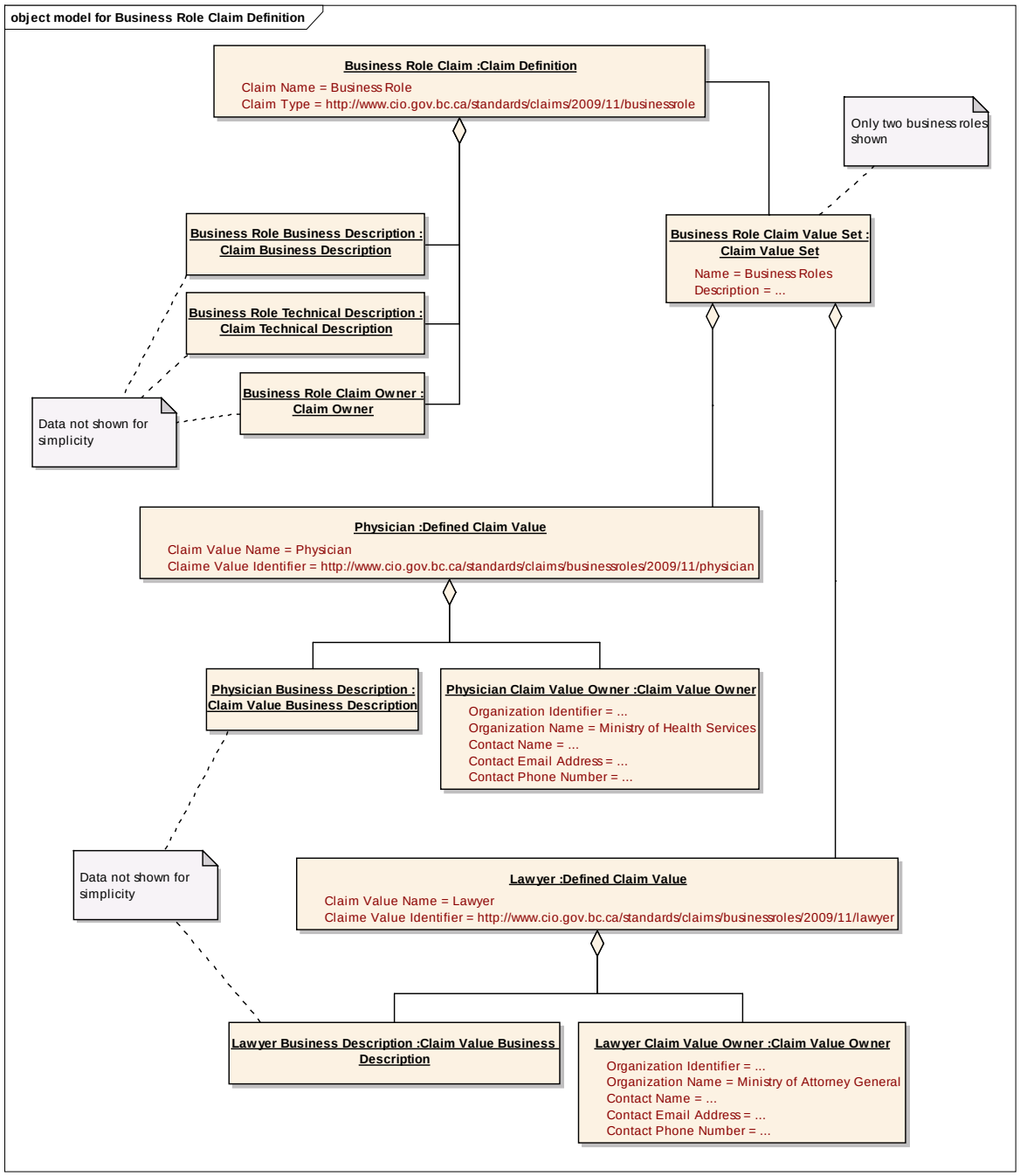
Figure 4 - Object Diagram Showing Example of Claim Definition



Example Claim Value Set for "Business Role"

The following diagram shows an instantiation of the Claim Definition Information Model for a "Business Role" claim, with emphasis on how a claim value set is composed.

Figure 5 - Object Diagram Showing Example of Claim Value Set



3 Claims Usage Standard

When an organization has a requirement for claims for their Information System (commonly called an application), it must implement the following standards about the use of claims.

3.1 Privacy Considerations

In requesting and sending claims, Relying Parties and Authoritative Parties MUST ensure that they uphold their responsibility to protect the privacy of personal information and follow best privacy practices. Privacy responsibilities for BC government organizations and the broader public sector are set out in the *Freedom of Information and Protection of Privacy Act.* Privacy responsibilities for private sector organizations in BC are set out in the *Personal Information Protection Act*.

While not an exhaustive list, the following privacy best practices are particularly relevant to the requesting and sending of claims that involve personal information:

1. Relying Parties SHOULD only request personal information claims that they are authorized to collect and that are necessary for the operation of their program or service. Where the provision of certain personal information claims is optional, it SHOULD clearly be communicated as such.

2. Relying Parties MUST notify individuals of the purposes for which they are requesting personal information claims and inform individuals of how their personal information will be used and, if applicable, disclosed. Relying Parties MUST also provide individuals with a contact name or position to whom questions or concerns about the collection, use or disclosure of their personal information may be directed.

3. Wherever possible, Relying Parties and Authoritative Parties SHOULD provide individuals with the maximum amount of choice, consent and control over the credentials they use and the transfer of their personal information from one party to another.

4. In determining what personal information claims they need for a particular service, Relying Parties SHOULD ensure that they request the least amount of personal information possible to meet the requirement of the service. Where the provision of some personal information is optional (i.e., not necessary for the provision of the service) a decision by the individual to not provide that information SHOULD NOT result in the denial of the service.

5. In determining what personal information claims they need for a particular service, Relying Parties SHOULD consider the identity context of the individuals accessing their service and limit the amount of personal information they collect accordingly. For example, if the individual accessing the service is acting as an employee of an organization, personal information claims

SHOULD be limited to that individual's affiliation with the organization and SHOULD NOT include personal information that is only relevant to the individual's personal context (such as date of birth and residential address).

6. Where an Authoritative Party is responsible for sending personal information claims about individuals operating in multiple identity contexts (e.g., as a private citizen, employee, professional), it SHOULD ensure that it sends claims in such as way that a Relying Party cannot easily link these different identity contexts together.

7. Authoritative Parties SHOULD ensure that the personal information claims it sends about an individual cannot be easily linked by Relying Parties operating unrelated programs and services (i.e., the ability for Relying Parties to create cross-program profiles of individuals SHOULD be limited and strictly controlled).

8. After receiving personal information claims from an Authoritative Party, a Relying Party MUST ensure that the personal information is protected from unauthorized access or disclosure and only used and disclosed for the purposes for which it was originally collected (unless the individual consents to a new use). If the Relying Party received the personal information claims subject to an information sharing (or similar) agreement, it MUST also comply with any requirements set out in that agreement.

3.2 Required Claims

Different sets of claims may be used depending on the level of identity assurance required by the Relying Party. Identity Assurance Levels are explained in the *Identity Assurance Standard*, and are summarized here:

- **Low** identity assurance (Level 1) means that there is little to no confidence in the identity claims about this user.
- **Medium** identity assurance (Level 2) means that there is some confidence in the identity claims about this user.
- **High** identity assurance (Level 3) means that there is high confidence in the identity claims about this user.
- **Very High** identity assurance (Level 4) means that there is very high confidence in the identity claims about the user.

When a Relying Party has a requirement for the **Low** identity assurance level, the following constraints MUST be followed:

1. The Relying Party MUST require the following claims:
    - Identity Assurance Level 1

- Authoritative Party Identifier
- Authoritative Party Name

2. When a Relying Party requires claims about the user, it MUST only use those in the following set of claim definitions:
   - Private Personal Identifier
   - User Identifier
   - Surname
   - Given Name

   Other claims require a higher level of identity assurance to be meaningful. A user cannot have an affiliation or agency relationship at this level, thus claims about an affiliation or organization are not appropriate to be requested.

   Additional claims may be defined in the future, at which time this list may be expanded.

3. The Authoritative Party SHOULD send the claims required by the Relying Party, where it does not violate the business rules of the Authoritative Party. If the Authoritative Party is not able to send the claims, it MUST reject the request and require the Relying Party to send requests for claims to another Authoritative Party.

When a Relying Party has a requirement for the **Medium**, **High** or **Very High** identity assurance level, the following constraints MUST be followed:

4. The Relying Party MUST require and the Authoritative Party MUST send the following claims:
   - Identity Assurance Level 2, 3, or 4
   - Authoritative Party Identifier
   - Authoritative Party Name

5. When a Relying Party requires claims about the user, it MAY use any of the claim definitions, except for Identity Assurance Level 1.

6. The Authoritative Party SHOULD send the claims required by the Relying Party, where it does not violate the business rules of the Authoritative Party. If the Authoritative Party is not able to send the claims, it MUST reject the request and require the Relying Party to send requests for claims to another Authoritative Party.

4 Claim Definitions

This section of the document describes specific claim definitions for use within Information Systems implementing the claims-based architecture. These claims are the core set of claims that are expected to be commonly used in the majority of Information Systems.

The claim definitions presented in this section are represented as a collection of business and technical descriptions. The structure of a claim definition is described in the Claim Definition Information Model, in the previous section of this document. The status and processes related to maintaining a claim definition are described in the *Claim Definitions Lifecycle Guide*, in the next section of this document.

The claim definitions are organized and presented in the following order:

- Claims about Individuals
- Claims about Organizations
- Claims about Affiliation Relationships
- Claims about Authoritative Party Systems
- Claims about Identity Assurance

Guidance on which claims may be used for the various identity assurance requirements is described in the *Claims Usage Standard*, as well as indicated within the claim definitions themselves.

The following diagram illustrates most of the defined claims relative to the *Identity Information Reference Model*. However, it does not represent the claims about an Authoritative Party because that is not explicitly drawn in that model.

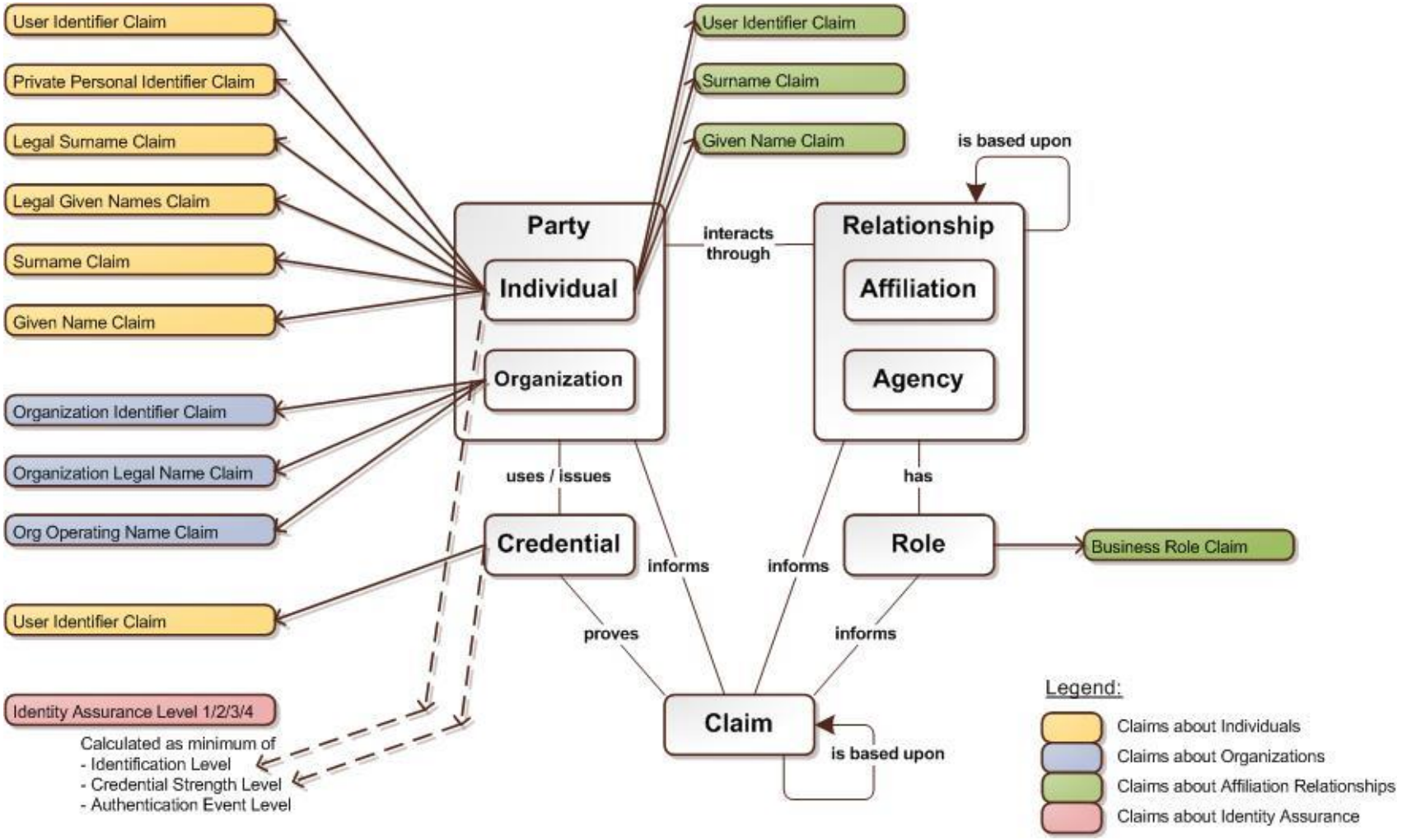
Note that claims are defined for only a subset of all data elements in the model. Some data elements are not appropriate to be shared as claims, as described in the *Identity Information Standard*.

Some claims are yet to be defined; refer to the *Claim Definition Lifecycle Guide* in section 5, or contact the Architecture and Standards Branch of the Office of the CIO (see the fourth page of this document).

Also, some claim definitions are shown multiple times in the model, because they are relevant to multiple identity contexts. For example, a user's name ("Surname" and "Given Name" claims) are relevant to both acting in a personal context as well as for an employment context. That individual's name may even be different, such as when a person goes by a different name at work than at home.

Most Authoritative Parties implementing the claims-based architecture will only be authoritative in one identity context. The most common scenario will be an organization being authoritative for a set of claims about its employees. Few Authoritative Parties would implement all defined claims.

Figure 6 - Identity Information Reference Model with Associated Claims



4.1 Claims about Individuals

The following claims are about an individual person, whether acting in a personal context or in a relationship with another organization or individual.

User Identifier Claim

Claim Definition	
Claim Name:	User Identifier
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/11/useridentifier
Business Description	
Description:	This claim represents the unique identifier associated with the user, specific to an Authoritative Party. It is a general purpose user identifier.
Acceptable Usage:	This claim may be used when required to represent the individual as a unique identifier. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. Use name claims for display purposes. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified as one of the following globally unique identifier schemes: - object identifier (OID), - universal unique identifier (UUID/GUID), and - universal principal name (UPN) When using the object identifier, the OID value must correspond to a registered object identifier that is uniquely associated with the user. When using the universal unique identifier, the UUID (or GUID) value must correspond to an existing object within a directory associated with the user. When using the universal principal name, the UPN value must correspond to an existing account within a directory associated with the user. An Authoritative Party may send multiple “User Identifier” claims, thus allowing flexibility for Relying Parties to work with either identifier provided.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding, URN syntax - urn:oid:<value>

	- urn:uuid:<value> - urn:upn:<value> URN syntax is defined in IETF RFC 2141 OID syntax is defined in ITU-T X.660 and ISO/IEC 9834-1 OID URN syntax is defined in IETF RFC 3001 UUID syntax is defined in IETF RFC 4122 UUID URN syntax is also defined in IETF RFC 4122 UPN syntax is defined in Microsoft documentation UPN URN syntax is not defined by may be used
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the above specifications. The common ones are colon, @, period and hyphen. Maximum 255 characters
Examples:	An example of this claim in UUID URN syntax is "urn:uuid:BB578593878A4E70AB3A262F98ED583F". An example of this claim in UPN URN syntax is "urn:upn:pwiebe@idir"
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Private Personal Identifier (PPID) Claim

Claim Definition	
Claim Name:	Private Personal Identifier
Claim Type:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
Business Description	
Description:	This claim represents the unique identifier associated with the user, specific to a given Relying Party. It is privacy protecting because it is not shared amongst a broad set of Relying Parties.
Acceptable Usage:	This claim may be used when required to represent the individual as a unique identifier. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. Use name claims for display purposes. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified as described in the OASIS Identity Metasystem Interoperability (IMI) specification. The value is expected to

	be calculated by software implementing that specification.
Technical Description	
Data Type:	Binary
Data Format:	64-bit encoded binary
Data Constraints:	When this claim is sent, it must not be empty or null. As described in the Identity Metasystem Interoperability specification.
Examples:	An example of the display encoding of a (binary) private personal user identifier is "VAS-NFKR-4AT".
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Legal Surname Claim

Claim Definition	
Claim Name:	Legal Surname
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/legalsurname
Business Description	
Description:	This claim represents the legal surname (or last name or family name) of the individual represented by the user.
Acceptable Usage:	This claim may be used when required to represent the individual. This claim may be shown to the user, usually in combination with the "Legal Given Names" claim. This claim may be used in combination with other core identity claims to uniquely identify an individual with identity information within an Information System. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use an identifier claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and

	French accent characters. Maximum 255 characters
Examples:	An example of this claim is “MacDonald”.
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Legal Given Names Claim

Claim Definition	
Claim Name:	Legal Given Names
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/legalgivennames
Business Description	
Description:	This claim represents the legal given names (or first name plus middle names, if any) of the individual represented by the user.
Acceptable Usage:	This claim may be used when required to represent the individual. This claim may be shown to the user, usually in combination with the Legal Surname claim. This claim may be used in combination with other core identity claims to uniquely identify an individual with identity information within an Information System. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use an identifier claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is “Mary Annabelle”.
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Surname Claim

Claim Definition	
Claim Name:	Surname
Claim Type:	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Business Description	
Description:	This claim represents the surname or family name of the individual represented by the user. This may be a pseudonym or the preferred surname that the individual uses and is known as within the context, which may or may not match the legal surname.
Acceptable Usage:	This claim may be used when required to represent the individual. This claim may be shown to the user, usually in combination with the "Given Name" claim. This claim may be used to link an individual with identity information within an Information System. When used with the requirement of Low identity assurance, this claim should not be considered accurate as it is not verified. Use higher identity assurance levels and/or the "Legal Surname" claim for matching purposes where possible. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use an identifier claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is "MacDonald-Smith".
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Given Name Claim

Claim Definition	
Claim Name:	Given Name
Claim Type:	http://www.schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Business Description	
Description:	This claim represents the given name (or first name) of the individual represented by the user. This may be a pseudonym or the preferred first name that the individual uses and is known within the context, which may or may not match any of the legal given names.
Acceptable Usage:	This claim may be used when required to represent the individual. This claim may be shown to the user, usually in combination with the "Surname" claim. This claim may be used to link an individual with identity information within an Information System. When used with the requirement of Low identity assurance, this claim should not be considered accurate as it is not verified. Use higher identity assurance levels and/or the "Legal Surname" claim for matching purposes where possible. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use an identifier claim for access control purposes. This claim may be recorded in user tales and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is "Anna".
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

4.2 Claims about Organizations

The following claims are about an organization that an individual person has an affiliation with.

Organization Identifier Claim

Claim Definition	
Claim Name:	Organization Identifier
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/organizationidentifier
Business Description	
Description:	This claim represents the unique identifier associated with the organization.
Acceptable Usage:	This claim may be used when required to represent the organization that an individual has an affiliation with. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. Use the "Organization Operating Name" claim for display purposes. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified as one of the following globally unique identifier schemes: - object identifier (OID) - universal unique identifier (UUID/GUID), and - domain name (DNS) When using the object identifier, the OID value must correspond to a registered object identifier that is uniquely associated with the organization. When using the universal unique identifier, the UUID (or GUID) value must correspond to an existing object within a directory associated with organization. When using the domain name identifier, the DNS value must correspond to an internet-registered domain name that is uniquely associated with the organization. An Authoritative Party may send multiple "Organization Identifier", thus allowing flexibility for Relying Parties to work with either identifier provided.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding, URN syntax - urn:oid:<value> - urn:uuid:<value>

	- urn:dns:<value> URN syntax is defined in IETF RFC 2141 OID syntax is defined in ITU-T X.660 and ISO/IEC 9834-1 OID URN syntax is defined in IETF RFC 3001 UUID syntax is defined in IETF RFC 4122 UUID URN syntax is also defined in IETF RFC 4122 DNS syntax is defined in IETF RFC 1034 OID DNS syntax is undefined but may be used
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the above specifications. The common ones are colon, @, period and hyphen. Maximum 255 characters
Examples:	An example of this claim in OID URN syntax is "urn:oid:2.16.124.2.101.100.1" (where 2.16.124.2.101 represents the Province of British Columbia). An example of this claim in UUID URN syntax is "urn:uuid:3ECD39BED1D744568FA17A1A24E0AD2D". An example of this claim in DNS URN syntax is "urn:dns:gov.bc.ca".
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Organization Legal Name Claim

Claim Definition	
Claim Name:	Organization Legal Name
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/organizationlegalname
Business Description	
Description:	This claim represents the legal business name (or registered name) of the organization.
Acceptable Usage:	This claim may be used when required to represent the organization that an individual has an affiliation with. This claim may be shown to the user; alternatively, use the "Organization Operating Name" claim for display purposes. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use the "Organization Identifier" claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the

	Identity Information Standard.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is “ABC Consulting, Inc.”
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Organization Operating Name Claim

Claim Definition	
Claim Name:	Organization Operating Name
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/organizationoperatingname
Business Description	
Description:	This claim represents the operating name (or “doing business as” name) of the organization. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Acceptable Usage:	This claim may be used when required to represent the organization that an individual has an affiliation with. This claim may be shown to the user; alternatively use the “Organization Legal Name” claim for display purposes. This claim should not be used on its own to determine whether a user is allowed to access information or perform functions within an Information System. Use the “Organization Identifier” claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified in the *Name Standard* in the *Identity Information Standard*.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding

Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard*. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is "ABC Consulting, Inc"
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

4.3 Claims about Affiliations

The following claims are about an affiliation that an individual has with an organization.

Business Role Claim

Claim Definition	
Claim Name:	Business Role
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/11/businessrole
Business Description	
Description:	This claim represents the business role of an individual in an affiliation relationship with an organization.
Acceptable Usage:	This claim may be used when required to represent the business role that an individual has in relation to their affiliation with an organization. This claim may be shown to the user, however because the value is in URI syntax, it is better to show the user a simplified display of the name of the business role derived to the value. This claim should be used to determine whether a user is allowed to access information or perform functions within an Information System. (This claim is defined to facilitate role-based access control. Other types of role claims may also support this approach, such as application-specific roles.) This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is constrained to a defined claim value set of Business Roles; however this set is not yet specified. It is expected to contain common roles such as "Licensed Physician", "Lawyer", "Social Worker" and "Accountant". Each business role would be assigned a unique identifier in URI syntax, similar to claim type. When a user is associated with multiple business roles, an Authoritative Party may send multiple Business Role claims to a Relying Party.
Technical Description	
Data Type:	String

Data Format:	UTF-8 encoding, URI syntax
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in URI syntax. Maximum 255 characters
Examples:	Suppose there was a business role for "Licensed Physician". It could be specified as a URN "urn:ca:bc:gov:cio:standards:businessroles:2009:11:physician" or a URL "http://www.cio.gov.bc.ca/standards/businessroles/2009/11/physician"
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

4.4 Claims about Authoritative Party Systems

The following claims are attributes about the Authoritative Party systems that issue the claims.

Authoritative Party Identifier Claim

Claim Definition	
Claim Name:	Authoritative Party Identifier
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/authoritativepartyidentifier
Business Description	
Description:	This claim represents the unique identifier of the Authoritative Party system.
Acceptable Usage:	This claim must be used by an Authoritative Party in the required set of claims. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. Use the "Authoritative Party Name" claim for display purposes. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim is constrained to have values specified as one of the following globally unique identifiers schemes: - domain name (DNS), and - object identifier (OID) When using the domain name identifier, the DNS value must correspond to an internet-registered domain name that the Authoritative Party system is accessed by users. When using the object identifier, the OID value must correspond to a registered object identifier that is published in a publicly accessible registry that is uniquely

	associated with the Authoritative Party system. When desired, a claim for each identifier type may be sent by an Authoritative Party, thus allowing flexibility for Relying Parties to work with either identifier provided.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding, URN syntax - urn:dns:<value> - urn:oid:<value> URN syntax is defined in IETF RFC 2141 OID syntax is defined in ITU-T X.660 and ISO/IEC 9834-1 OID URN syntax is defined in IETF RFC 3001 DNS syntax is defined in IETF RFC 1034 OID DNS syntax is undefined but may be used
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the above specifications. The common ones are colon and period. Maximum 255 characters
Examples:	An example of this claim in OID URN syntax is “urn:oid:2.16.124.2.101.200.1” (where 2.16.124.2.101 represents the Province of British Columbia). An example of this claim in DNS URN syntax is “urn:dns:bceid.ca”.
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Authoritative Party System Name Claim

Claim Definition	
Claim Name:	Authoritative Party Name
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/authoritativepartyname
Business Description	
Description:	This claim represents the common name of the Authoritative Party system.
Acceptable Usage:	This claim must be used by an Authoritative Party in the required set of claims. This claim may be shown to the user to express where they authenticated and where their claims were sent from. This claim should not be used to determine whether a user is allowed to access information or perform functions within an Information System. Use the “Authoritative Party Identifier” claim for access control purposes. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were

	using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim should be the branded name or acronym of the Authoritative Party system that the user should recognize and associate with.
Technical Description	
Data Type:	String
Data Format:	UTF-8 encoding
Data Constraints:	When this claim is sent, it must not be empty or null. Special characters are allowed as described in the *Name Standard* in the *Identity Information Standard* for an organization's operating name. The common ones are space, hyphen, apostrophe, and French accent characters. Maximum 255 characters
Examples:	An example of this claim is "BCeID"
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

4.5 Claims about Identity Assurance

The following claims are attributes about the identity assurance relevant to the person that the user is representing. There are four identity assurance level claims.

The identity assurance level represents the measure of confidence that should be placed in the identity of the user. This level is based on the identity proofing and registration processes, the strength of the credentials used, and the success of the authentication event. Refer to the *Identity Assurance Standard* for further explanation.

Identity Assurance Level 1 Claim

Claim Definition	
Claim Name:	Identity Assurance Level 1
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel1
Business Description	
Description:	This claim represents identity assurance level 1, which means "Low". There is no to some confidence in the identity claims about this user.
Acceptable Usage:	An identity assurance level claim must be used by an Authoritative Party in the required set of claims. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. It is not recommended to show this claim to the user, as the user is unlikely to

	understand its meaning. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim represents the default level for identity assurance. If the identity assurance level is not level 2, 3, or 4, or the identity assurance level is unknown, use this claim of level 1.
Technical Description	
Data Type:	Boolean
Data Format:	True or False
Data Constraints:	When this claim is sent, it must not be empty or null. When this claim is sent, it is expected to have the value of True, otherwise it would not be sent.
Examples:	An example of this claim is “True”
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Identity Assurance Level 2 Claim

Claim Definition	
Claim Name:	Identity Assurance Level 2
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel2
Business Description	
Description:	This claim represents identity assurance level 2, which means “Medium”. There is some confidence in the identity claims about this user.
Acceptable Usage:	An identity assurance level claim must be used by an Authoritative Party in the required set of claims. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim represents level 2 for identity assurance. If the identity assurance level is unknown, use the level 1 claim.

Technical Description	
Data Type:	Boolean
Data Format:	True or False
Data Constraints:	When this claim is sent, it must not be empty or null. When this claim is sent, it is expected to have the value of True, otherwise it would not be sent.
Examples:	An example of this claim is “True”
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Identity Assurance Level 3 Claim

Claim Definition	
Claim Name:	Identity Assurance Level 3
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel3
Business Description	
Description:	This claim represents identity assurance level 3, which means “High”. There is high confidence in the identity claims about this user.
Acceptable Usage:	An identity assurance level claim must be used by an Authoritative Party in the required set of claims. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim represents level 3 for identity assurance. If the identity assurance level is unknown, use the level 1 claim.
Technical Description	
Data Type:	Boolean
Data Format:	True or False
Data Constraints:	When this claim is sent, it must not be empty or null. When this claim is sent, it is expected to have the value of True, otherwise it would not be sent.
Examples:	An example of this claim is “True”

Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

Identity Assurance Level 4 Claim

Claim Definition	
Claim Name:	Identity Assurance Level 4
Claim Type:	http://www.cio.gov.bc.ca/standards/claims/2009/09/identityassurancelevel4
Business Description	
Description:	This claim represents identity assurance level 4, which means “Very High”. There is very high confidence in the identity claims about this user and non-repudiation.
Acceptable Usage:	An identity assurance level claim must be used by an Authoritative Party in the required set of claims. This claim may be used in combination with other claims to determine whether a user should be allowed to access information or perform functions within an Information System. It is not recommended to show this claim to the user, as the user is unlikely to understand its meaning. This claim may be recorded in user tables and audit logs for an Information System to represent the set of information known about the user when they were using an Information System.
Constraints:	This claim is not constrained to a defined claim value set. This claim represents level 4 for identity assurance. If the identity assurance level is unknown, use the level 1 claim.
Technical Description	
Data Type:	Boolean
Data Format:	True or False
Data Constraints:	When this claim is sent, it must not be empty or null. When this claim is sent, it is expected to have the value of True, otherwise it would not be sent.
Examples:	An example of this claim is “True”
Owner	
Organization Name:	Architecture and Standards Branch, Office of the CIO, Province of BC

5 Claim Definitions Lifecycle Guide

Many claim types have already been defined and published for use within Information Systems (Authoritative Parties and Relying Parties) implementing the claims-based architecture. These are described in the *Claim Definitions*, in the previous section of this document. It is anticipated that new claims will be needed. This guide describes the lifecycle of claim definitions.

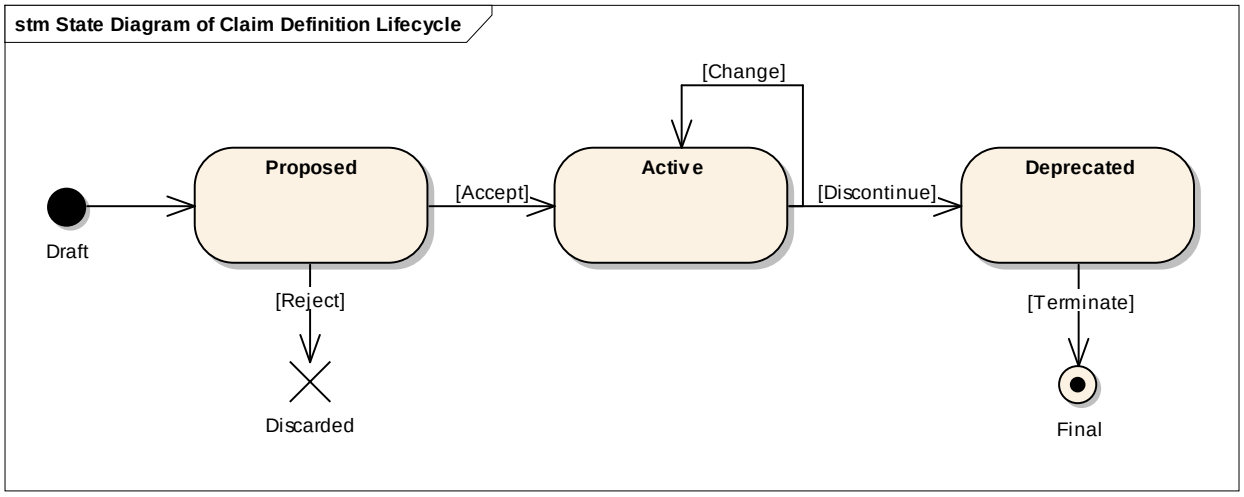
5.1 Claim Definitions Lifecycle Model

The lifecycle of claim definitions is represented as a series of states that a claim definition can be in, and processes that change between these states.

The following diagram shows that a given claim definition is in one of three states: Proposed, Active and Deprecated. Information Systems should only use claim definitions that are in the Active state. Deprecated claim definitions may be used for a period of time to allow for transition to some other claim definition(s). A claim definition may then be terminated and removed from use.

Organizations should not create their own claims without following the below processes, and they should not use Proposed claims until they have been reviewed and made into Active claims.

Figure 7 - State Diagram of Claim Definition Lifecycle



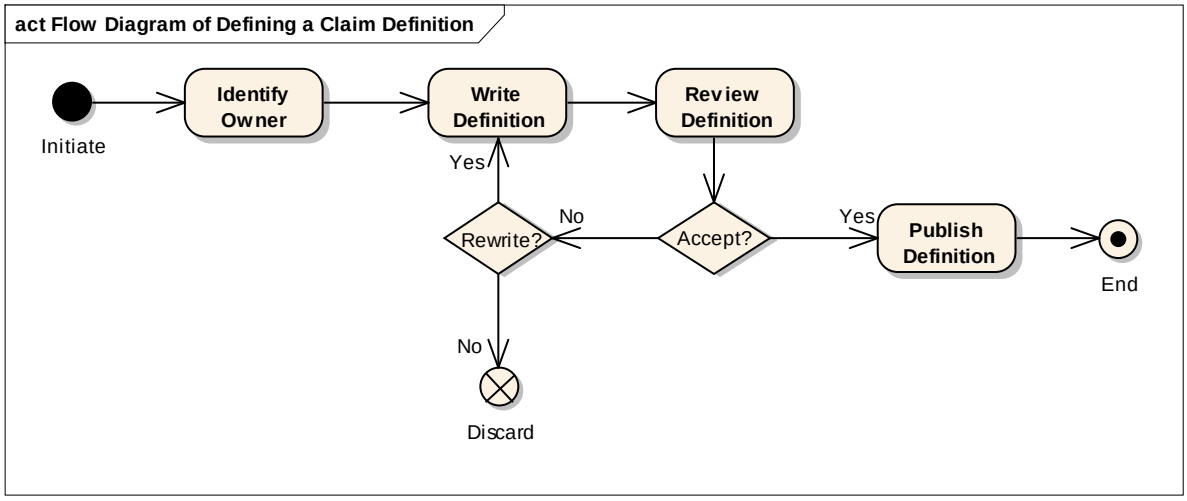
5.2 Defining a new Claim Definition

The following diagram shows the general activities or steps involved in defining a new claim definition. At this time, requests for claim definitions will be facilitated through the Office of the CIO.

First, an owner must be identified for the proposed claim definition. The claim definition must be written, capturing the business and technical definitions, as described in Claim Definition Information Model. Some analysis work is expected to ensure a stable and complete definition is produced.

The claim definition is then reviewed for correctness and appropriateness by a set of reviewers, and may be formally approved depending on the situation. If the definition is accepted it is then published, considered in an Active state, and able to be used by Information Systems. If the definition is not accepted, it may be sent back for revisions, or not pursued further.

Figure 8 - Activity Diagram of Defining a Claim Definition



The process also includes defining a set of claim values, if that is required for the claim. The claim definition and a corresponding set of claim values may be defined, reviewed and published at the same time. Alternately, the claim definition and an initial set of claim values may be defined, reviewed and published at one time, then later claim values could to be added to the set as needed.

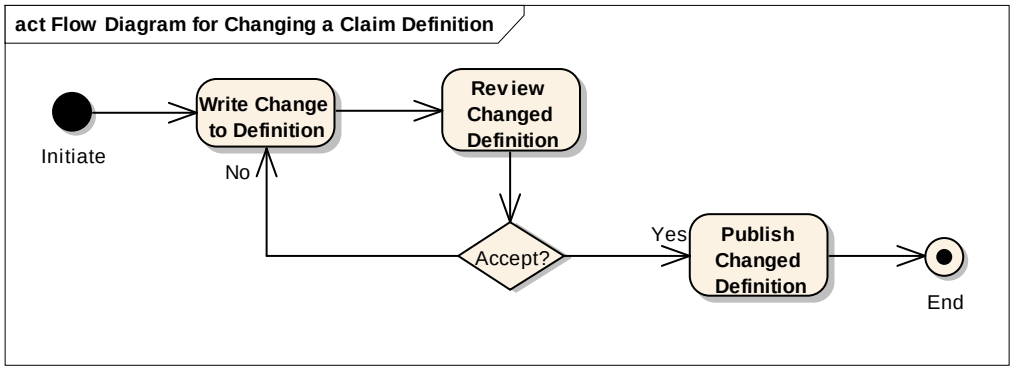
5.3 Changing a Claim Definition

The following diagram shows the general activities or steps involved in changing an existing claim definition. This allows for minor changes to be made, however it is not recommended to significantly change a definition, as people and Information Systems may already be relying on its meaning. When significant changes are needed, it is recommended to define a new claim.

The activities involved in changing a claim definition extend to changing a claim value definition or adding or removing claim values. It is expected that requests for changed claim definitions will be facilitated through the owner of the claim definition or owner of specific claim values.

Similar to defining a new claim definition (and if appropriate claim values), the definition must be written, with some analysis of its current usage to ensure that changes do not adversely affect those relying on it. The changed definition is then reviewed and, if acceptable, published.

Figure 9 - Activity Diagram of Changing a Claim Definition



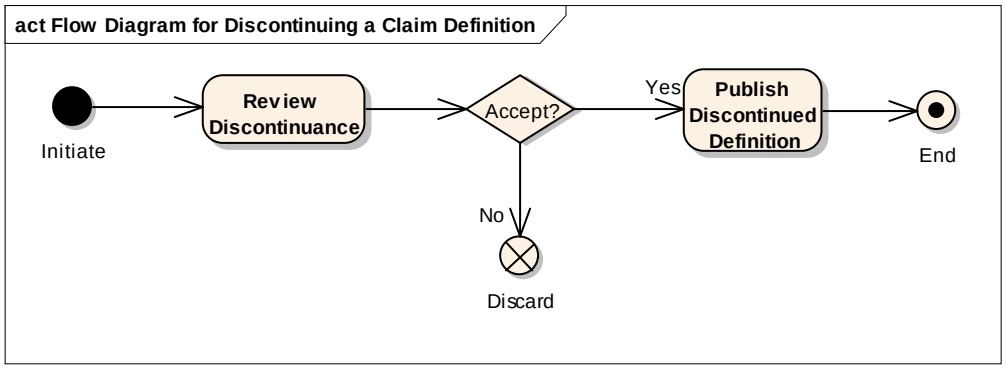
5.4 Discontinuing a Claim Definition

The following diagram shows the general activities or steps involved in discontinuing an existing claim definition. Discontinuing a claim definition makes it clear to those people relying on it that they must transition away from using a claim definition, and instead use a newer superseding claim definition or another approach to receiving the data. The claim definition is then marked as being in Deprecated state, which means it is not recommended for further use.

The activities involved in discontinuing a claim definition extend to discontinuing one or more claim value definitions. It is expected that requests for discontinued claim definitions or claim values will be facilitated by the owner of the claim definition. It is expected that the current usage of a claim definition is analyzed before a claim definition is discontinued.

A claim definition (and, if relevant, claim values) may be in a discontinued state for a period of time to allow sufficient time for people and Information Systems to transition. The owner should indicate the length of time of the transition.

Figure 10 - Activity Diagram of Discontinuing a Claim Definition

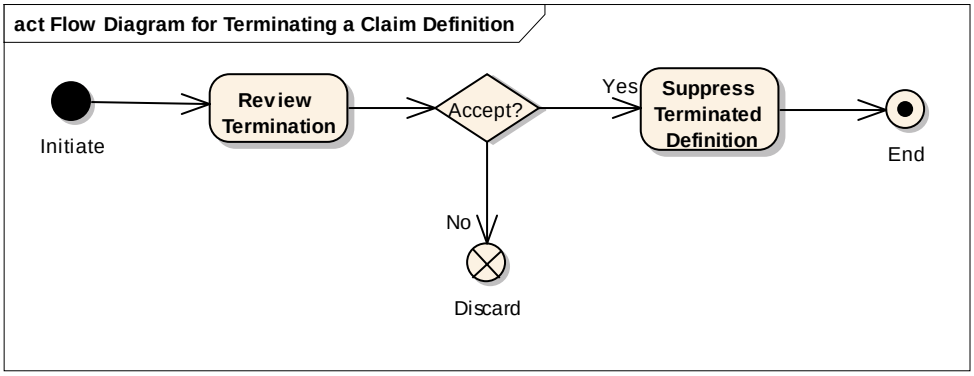


5.5 Terminating a Claim Definition

The following diagram shows the general activities or steps involved in terminating an existing claim definition. The claim definition must be discontinued before terminating it to allow some period of time for people and Information Systems to transition away from its use. Termination should only occur when it is known that Information Systems no longer rely on it.

The activities involved in terminating a claim definition extend to terminating one or more claim value definitions. It is expected that the owner of the claim definition or claim value definition will facilitate the termination. The claim definition should then be suppressed from being displayed where claim definitions are published, to prevent people and Information Systems from reading about it or using it.

Figure 11 - Activity Diagram of Terminating a Claim Definition



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.
Authoritative Party Proxy	An organization or system that acts on behalf of the original authoritative source.
Claim	An attribute related to an identity in a particular context.
Claim Type	An identifier of a claim definition specified as a URI.
Claim Value	The data portion of a claim.
GUID	Unique Identifier. A Microsoft implementation of UUID
OID	Object Identifier. An identifier described by walking the tree of nodes form root to leaf, represented as a string of numbers delimited by periods. Refer to ITU-T X.600 or ISO/IEC 9824-1 for more information. Refer to IETF RFC 3001 for the how to specify OID data in URN syntax.
Relying Party	A party that controls access to a resource or service and relies on an Authoritative Party to provide identity assurance and identity related attributes about a user or subject.
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 a resource or service.
UPN	Universal Principal Name. A Microsoft syntax combining user account name and Windows domain name.
URL	Uniform Resource Locator. A syntax to specify where an identified resource is located and the primary mechanism for accessing it.
URN	Uniform Resource Name. A syntax to encode a name, intended to serve as a persistent, location-independent resource identifier. Refer to IETF RFC 2141 for more information.
URI	Uniform Resource Identifier. A string of characters used to identify a name or a resource on the internet. A URI may be specified as a URN or

Term	Definition
	URL
UTF-8	8-bit Unicode Transformation Format. An character encoding used to represent written text in many human languages.
UUID	Universal Unique Identifier. An identifier generated by an algorithm focused on uniqueness across the set of all UUIDs and time. Refer to IETF RFC 4122 for more information and for the how to specify UUID data in URN syntax.