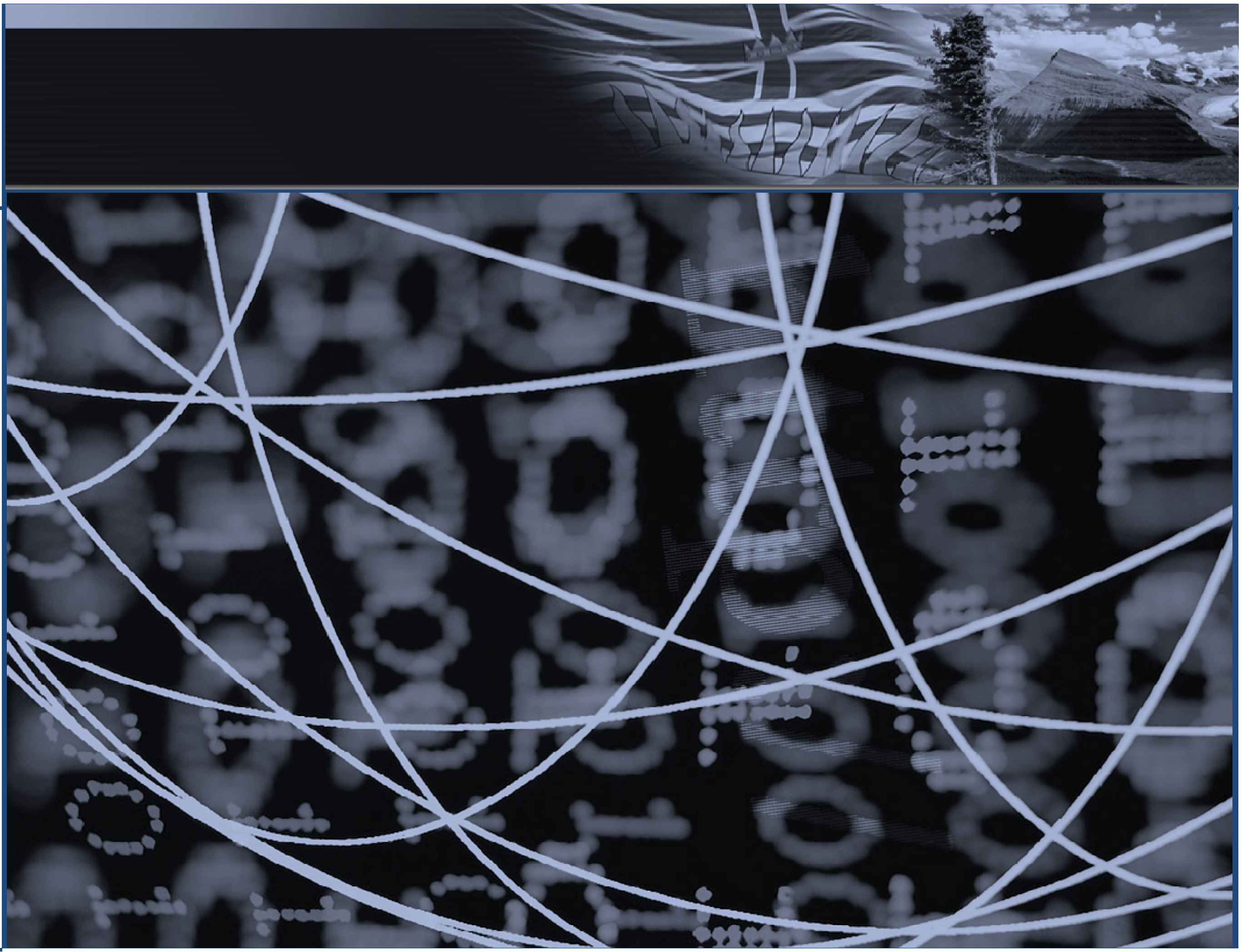
BRITISH COLUMBIA
The Best Place on Earth

Ministry of
Citizens' Services

IDENTITY INFORMATION REFERENCE MODEL

Version 1.0
Nov. 2010



Office of the Chief Information Officer,
Architecture and Standards Branch

-- This page left intentionally blank --

Revision History

Version	Date	Changed By	Description of Change
1.0	November 19, 2010	Charmaine Lowe	

Document Purpose

This document is part of the Identity Information Management Standards Package.

It introduces an Identity Information Reference Model that describes the key identity-related elements that are common in identification processes across government and illustrates how those elements can be related and combined to represent individuals acting in different relationships or identity contexts (such as in a professional, business, or employment context).

In describing and illustrating the relationship between common identity-related elements, the Identity Information Reference Model:

- sets the context for semantic interoperability and the development of identity information standards;
- informs the registration and communication of affiliation and agency relationships; and,
- guides the development of logical and physical identity data models.

Audience

The intended audience for this document is business and technical analysts, data architects, and developers.

Advice on this Document

Advice on this document can be obtained from the:

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

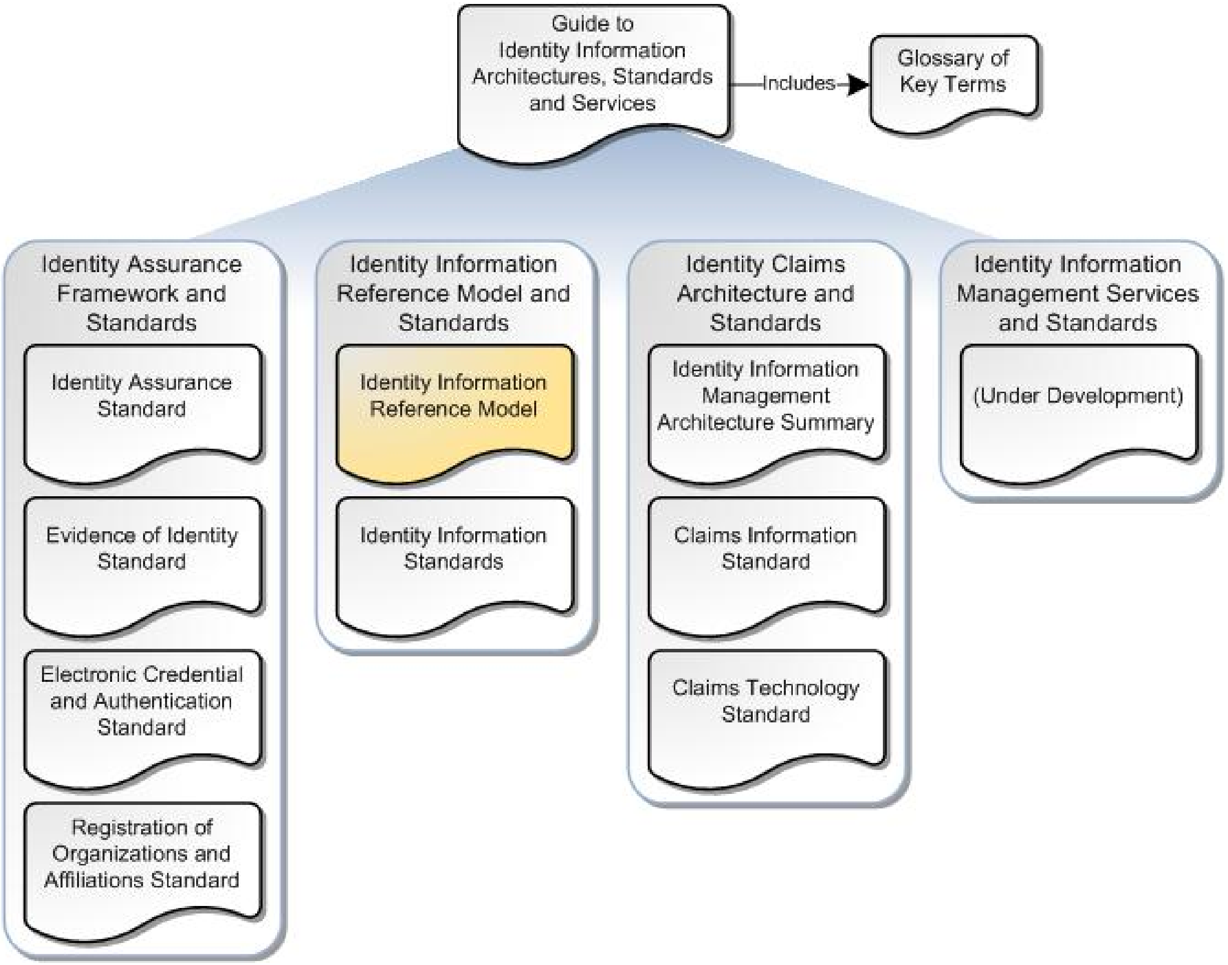
Postal Address:	PO Box 9412 Stn Prov Govt
Telephone:	(250) 387-8053
Facsimile:	(250) 953-3555
Email:	asb.cio@gov.bc.ca
Web:	http://www.cio.gov.bc.ca/legislation/standards

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


Guide to Identity Information Architectures, Standards and Services
Includes
Glossary of Key Terms
Identity Assurance Framework and Standards
Identity Assurance Standard
Evidence of Identity Standard
Electronic Credential and Authentication Standard
Registration of Organizations and Affiliations Standard
Identity Information Reference Model and Standards
Identity Information Reference Model
Identity Information Standards
Identity Claims Architecture and Standards
Identity Information Management Architecture Summary
Claims Information Standard
Claims Technology Standard
Identity Information Management Services and Standards
(Under Development)

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, listed below.
Evidence of Identity Standard	Supports the *Identity Assurance Standard* by setting evidence of identity and operational diligence standards for registering and identity-proofing individuals to increasing levels of identification strength. Applies to both online and offline (i.e., real world) identity management transactions.
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 identifying and registering organizations and establishing affiliations between individuals and organizations.
2. Identity Information Reference Model and Standards	
Identity Information Reference Model	Introduces an Identity Information Reference Model that describes the key identity-related elements that are common in identification processes across government and illustrates how those elements can be related and combined to represent individuals acting in different identity contexts (such as in a professional, business, or employment context). Sets the context for *Identity Information Standards.*
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 Standards.*
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

In conducting routine business and evidence of identity processes, government organizations collect, record, verify and exchange identity-related data about individuals, organizations and the multiple relationships they have with one another. Individuals have relationships with other individuals (e.g., this individual is that individual's parent, agent or guardian); individuals have relationships with organizations (e.g., this individual is a principal or employee of that organization), and organizations have relationships with other organizations (e.g., this organization is a subsidiary of that organization).

Without a systematic way to organize the information associated with these relationships, government's ability to control data and identity proliferation, improve data integrity and availability, and facilitate authorized information sharing is limited.

The *Identity Information Reference Model* is a first step towards bringing some order and consistency to how information about individuals acting in different relationships (or identity contexts) is understood, recorded and communicated. It describes the key identity-related elements that are common in identification processes across government and illustrates how those elements can be related to represent individuals acting in different identity contexts.

Identity Context is the environment or circumstances in which identity information is communicated and perceived. Individuals operate in multiple identity contexts (e.g., legal, social, employment, business, pseudononymous) and may identify themselves differently based on the context.

Each identity-related element in the model is additionally associated with core identity data (such as name and date of birth) and/or supporting data (such as contact information and relationship types). By illustrating how this identity and supporting data is combined to support multiple relationships, the *Identity Information Reference Model* informs the *Registration of Organizations and Affiliation Standard*. It also sets the context for the *Identity Information Standards* where definitions, rules and formats are specified for core identity data such as name, date, and identifier.

When implemented by government agencies, the *Identity Information Reference Model* and the *Identity Information Standards* will provide a common language and approach for the collection and exchange of identity information about users and subjects of government services and resources.

1.1 Scope

The *Identity Information Reference Model* describes the key identity-related elements that are generally useful in establishing identity and identity-related relationships. It also illustrates how identity and supporting data can be associated with these elements to support identity and relationship claims.

In Scope

This model describes and associates the following identity-related elements which are introduced and defined in section 2.1:

- Party (Individual and Organization)
- Credential
- Relationship (Affiliation and Agency)
- Role
- Claim

Out of Scope but covered in other Standards

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

- Prescription of the minimum set of data elements to uniquely identify individuals (covered in the *Evidence of Identity Standard*);
- Prescription of the minimum set of data elements to identify organizations and organizational affiliations (covered in the *Registration of Organizations and Affiliations Standard*)
- Verification of the data elements (covered in the *Evidence of Identity Standard and Registration of Organizations and Affiliations Standard*);
- Definitions, rules and data formats for identity-related and supporting data elements (covered in the *Identity Information Standards*);

Out of Scope but not covered in other Standards

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

- Additional data elements that some government agencies may wish to collect in order to enable or enhance their own specific internal processes and services including program-specific identity and entitlement information.

1.2 Applicability

This document applies to British Columbia Government Ministries and Central Agencies (hereafter referred to as government organizations). Other organizations may choose to apply this reference model or may agree to apply it for the purpose of fulfilling contractual, federation or other legal agreements.

It should be read by any organization that needs to identify, and associate identity-related data to, individuals and/or organizations.

1.3 References

This document is recommended pre-reading for any organization implementing the *Evidence of Identity Standard,* the *Registration of Organizations and Affiliations Standard,* and/or the *Identity Information Standards.*

For an overview of the Identity Information Management solution and a complete list of related documents and standards see:

- *Guide to Identity Information Architectures, Standards and Services*

1.4 Terms and Definitions

Key terms and definitions related to the *Identity Information Reference Model* are set out in Appendix A. For a listing of all Identity Information Management Terms and Definitions, see the *Glossary of Key Terms* in the *Guide to Identity Information Architectures, Standards and Services*.

1.5 Document Structure

This document has three main sections:

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

Section 2: This section introduces the Identity Information Reference Model, provides definitions of the key elements in the model and provides examples of how these key elements can be related to represent individuals in different relationships or identity contexts.

Section 3: This section expands on section 2 by including the core identity-related and supporting data elements associated with different relationships or identity contexts.

2 Identity Information Reference Model

The purpose of the *Identity Information Reference Model* is to set the context for the *Identity Information Standards* and to inform the registration and communication of affiliation and agency relationships.

The Reference Model sets out the key identity-related elements that are common across services and illustrates how these elements can be related and combined to represent individuals in different relationships or identity contexts (such as in a professional, business, or employment context).

The *Identity Information Reference Model* is high-level and conceptual. It is not meant to be an implementable data model. However, the concepts outlined and discussed here will guide the development of logical and physical identity data models.

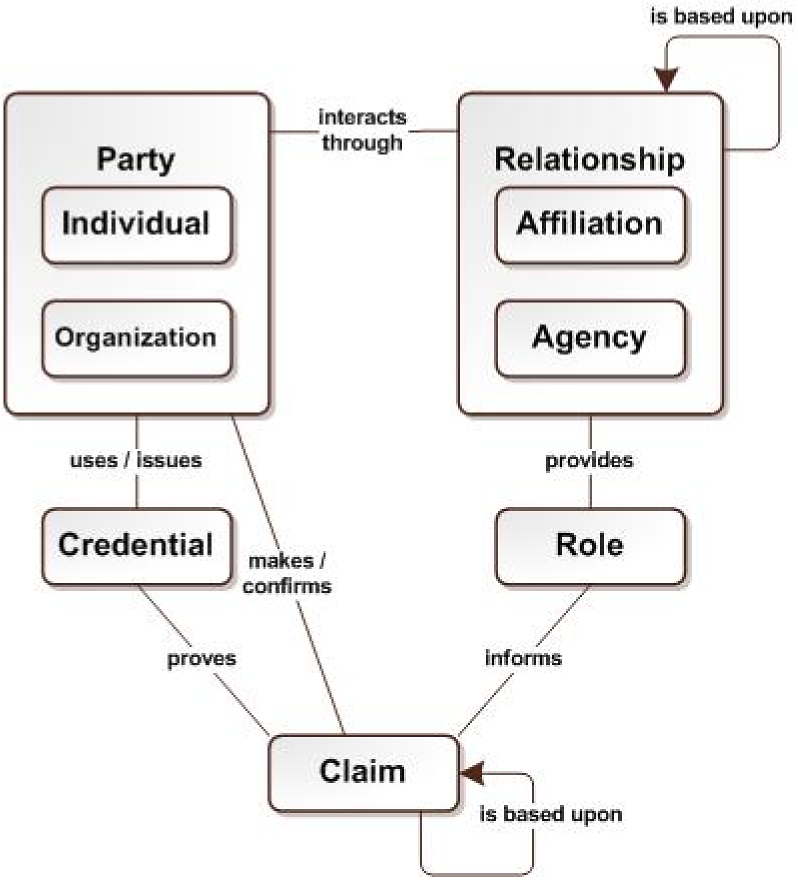
2.1 Defining the Reference Model

Individuals make claims about themselves in the real and online world. They make claims about their own identity, their relationships to other individuals and to organizations they represent or with whom they are affiliated. They also make claims about the personal and business roles they hold based on relationships they have with another individual (e.g., guardian) or an organization (e.g., employee). Often, they use credentials (both physical and electronic) to prove the claims they make about themselves and their relationships.

The Identity Information Reference Model, set in out in Figure 2, below, applies to both real world and online identity management transactions, as do the definitions supporting the model. This supports the goal of the Province's Identity Information Management solution to improve the quality of, and trust associated with, identity management transactions across all service delivery channels, not just the online channel. It also highlights an important design principle of the solution which is to mimic and align online identity and authentication processes as much as possible with real world processes and paradigms that are trusted and familiar to citizens.

Data elements associated with the Reference Model, which are set out in section 3.0, are also applicable across all service delivery channels (unless otherwise noted). This highlights a key consistency principle that core identity and supporting data should, as much as possible, be the same, mean the same and be collected according to the same rules and in the same structures, regardless of the service delivery channel.

Figure 2 - The Identity Information Reference Model



Definitions

1. A **Party** is an individual or organization. Parties interact with, and have relationships with, other parties.

   Parties make claims about themselves and use credentials to prove those claims. Certain parties, known as authoritative parties, are trusted to confirm claims made by other parties. In some cases, authoritative parties issue credentials that may be used by these other parties to indirectly confirm (or prove) claims.

2. An **Individual** is a human being.

3. An **Organization** is a group of people that work or associate together. An organization may be a legal entity like a business or government agency, a subsidiary or division of a legal entity or it may be an informal association such as a working group.

Organizations are represented by individuals through party relationships (e.g., this individual has an employment relationship with that organization).

4. A **Credential** is a physical or electronic object (or identifier) that is issued to, or associated with, one party by another party and attests to the truth of certain stated facts and/or confers a qualification, competence, status, clearance or privilege.

   Identity credentials can be cards, like a driver’s license or smart card; documents like a passport; or, in the context of digital identities, a User ID and password or digital certificate. These credentials are generally issued by organizations to individuals for the purpose of proving claims.

5. A **Relationship** is an association or connection between two parties. In this model, relationships are of two general categories: Affiliation and Agency (see definitions below).

   Relationships may be based upon, and therefore dependent on, other relationships. For example, an agency type relationship (such as a delegation) can exist between two employees of an organization. In this case, the agency relationship is based on two affiliation (e.g., employment) relationships. If one of the employment affiliations is severed, the agency relationship is severed as well.

6. An **Affiliation** is a relationship between two parties (usually an individual and an organization) that can be verified by an authoritative party. Typical affiliations include membership, employment or ownership/directorship. For example, an individual may be a member or employee of a particular organization. Another type of affiliation is where one organization is a subsidiary of another organization. In these examples, the employing or parent organization would be the authoritative party for the affiliation.

7. An **Agency** is a specialized type of relationship where one party is empowered to act for another party in some capacity. For example, one individual may be another individual’s delegate or one individual may have power of attorney over another individual’s affairs.

   Generally speaking, the first or principal party is the authority (or authoritative party) on who may act for him in a particular situation and no third party verification is necessary. However some types of agency (e.g., custodial parent, committee) are granted by third parties such as a Court and require verification directly with the issuing authority or through the presentation of evidence.

8. A **Role** is a set of responsibilities, activities and authorizations assigned to an individual based on an affiliation or agency relationship.

Some roles are automatically provided as a result of a relationship and are commonly understood and non-specific (e.g., an employment relationship automatically generates the role of "employee"). Other roles are assigned specifically to an individual or position and are unique to particular sector or business.

While the examples used in this document are common, non-specific roles which do little more than communicate the nature of a particular affiliation or agency relationship, the model does support the additional assignment and communication of more specific roles and entitlements.

9. A **Claim** is an assertion that something is true. Individuals make claims about themselves and about their relationships and roles (e.g., "I am John Smith" or "I am a Physician").

   Some claims are based on (or derived from) other claims. For example, the claim "I am over the age of 18" is based on a date of birth claim and the claim "I am a resident" is based on an address claim. Derived claims are important from a privacy perspective because they meet program needs (e.g., age and residency requirements) without exposing more information that is necessary (such as one's actual age or home address).

2.2 Application of the Reference Model

The Identity Reference Model applies to both real world and online identity management transactions. It applies to the identification or registration of individuals representing themselves in different contexts (e.g., as a private individual, an employee, a student, a professional, etc.) and to the ongoing authentication and verification of claims that individuals make in those multiple contexts (e.g., "I am a UVIC student", "I am a BC government employee", "I am a licensed physician"). It also supports authorization and data matching scenarios where identity, relationship or role information is a critical part of the decision-making process.

The following scenarios illustrate how the model applies to multiple identity contexts and situations. While these scenarios could easily be turned into online registration, authentication or access use cases, they have intentionally been described in a non-specific way to highlight the universality of the Reference Model.

A1. Individual Context

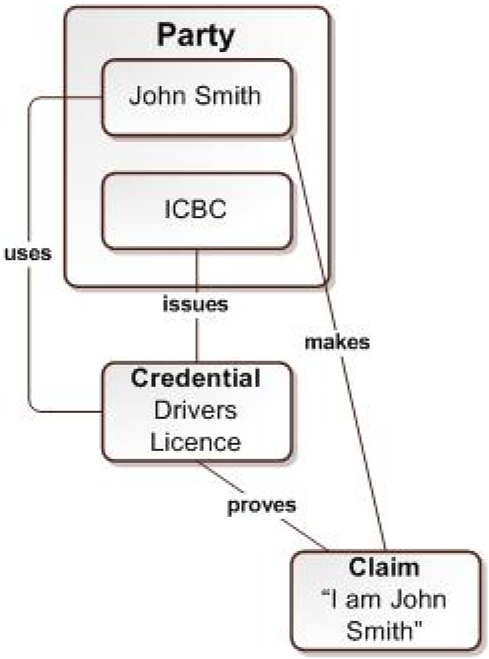
Individuals make all kinds of claims about themselves. Often those claims are identity-related such as: “My name is John Smith”; “I am 42 years old”; “I live at 123 Elm Street”. In some cases, an individual may need to prove an identity claim. For example, proof may be required when an individual is requesting a government service or benefit. Identity claims are proven or verified in one of two ways:

- Direct verification by an Authoritative Party (i.e., an individual or organization that is trusted to be the authority on the identity claim); or,
- Indirect verification through the presentation of a credential issued by an Authoritative Party.

Scenario:

In this scenario, John Smith uses his BC Driver’s Licence to prove his claim that he is John Smith. Because ICBC - the issuer of the credential - is trusted by the agency viewing the credential, John’s identity claim is accepted as true.

Figure 3 - Individual Context



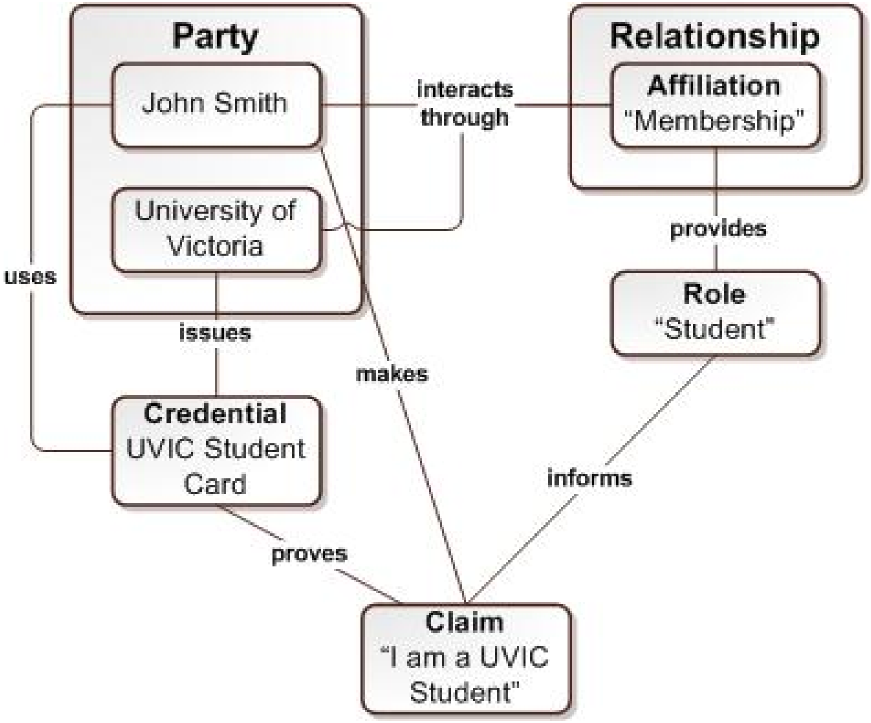
A2. Individual (Student) Context – University Affiliation

Individuals also make claims about their relationships or affiliations to organizations, such as to a university. These affiliations are often expressed as common role claims such as “I am a student”. Where an individual is purporting to have such a role or affiliation, evidence or verification of that affiliation may be required. That verification may be sought from an authorized representative at the organization itself, from another party trusted to be an authority on the affiliation or through the presentation of a valid credential that proves the affiliation, such as a student card.

Scenario:

John Smith is a student at the University of Victoria (UVIC). In this scenario, John proves his affiliation with the university and his student role by producing his university student card. Because UVIC – the issuer of the student card – is trusted to be the authority on who is a UVIC student, John’s claim that he is a UVIC student is accepted as true.

Figure 4 - Student Context – University Affiliation



The above scenario is an example of real world identity verification. However, this scenario could just as easily take place over the internet using electronic credentials issued by the University.

A3. Individual Context – Agency Relationship

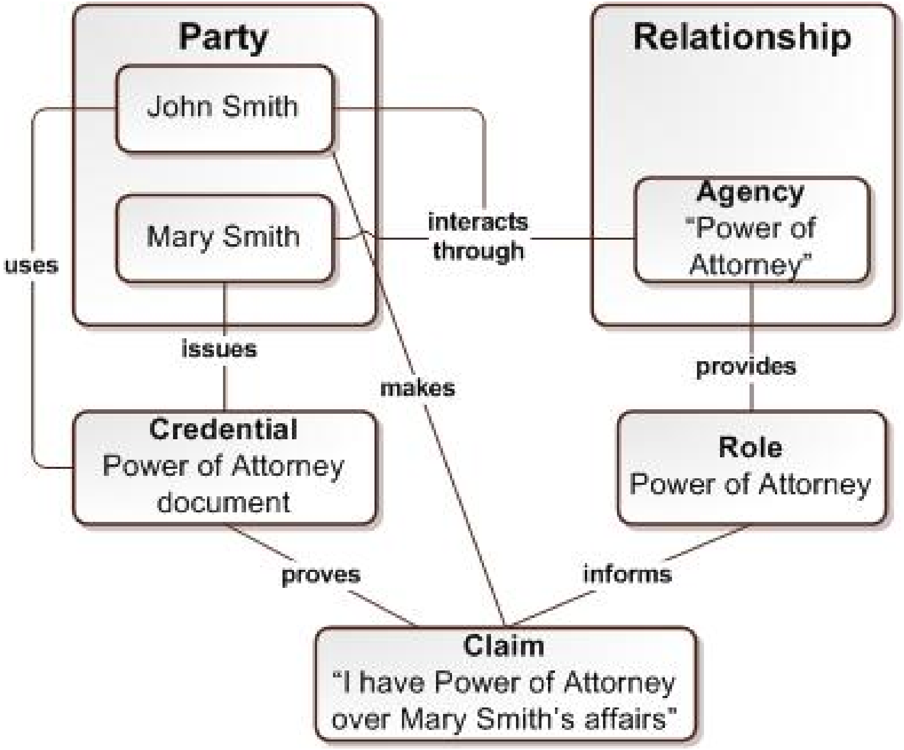
In addition to making claims about themselves and their organizational affiliations, individuals make claims about their relationships to other individuals. Common relationship claims include: “parent”, “custodial parent”, “power-of-attorney”, “advocate”, etc. These relationship claims are often made when one individual is representing another individual in some transaction.

Third party verification of a personal agency relationship is not generally required. Any capable individual can generally authorize another individual to act on her behalf when it comes to her personal affairs. However, where an individual is not capable, a court order may be required to authorize the agency relationship. In these cases verification by an Authoritative Party or by the presentation of evidence (e.g., custody or committee order) may be necessary. Different verification methods will be appropriate in different situations.

Scenario:

John Smith has power-of-attorney over his mother’s affairs. In this scenario, John is able to conduct business transactions on behalf of his mother by presenting his power-of-attorney document. This document, signed by Mary Smith and notarized, proves John’s agency relationship with his mother and provides authority for him to act on her behalf.

Figure 5 - Individual Context – Agency Relationship



B1. Business Context – Principal Affiliation

Business owners, representatives and employees make claims about themselves, their relationship to a business organization and the roles they have within that business. Where an individual is purporting to have authority to represent a business in some transaction, evidence or verification of that relationship may be required. That verification may be sought from an authorized representative at the business itself or from another party trusted to be an authority on the business relationship.

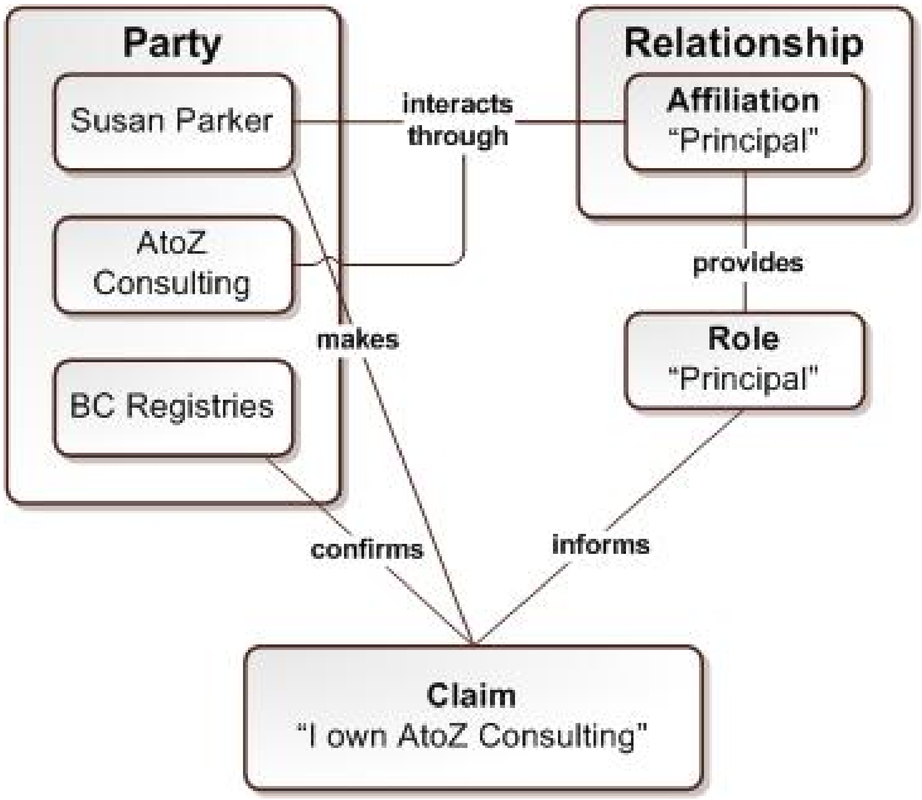
Scenario:

Susan Parker is the sole proprietor (or principal) of AtoZ Consulting. While Susan can prove her individual identity through the presentation of photo ID (See Scenario A1), the identity of the business, AtoZ Consulting, and Susan's relationship to it, requires additional verification.

In previous scenarios, individuals produced credentials to prove their claims. While Susan could produce business registration documents to prove her ownership of AtoZ Consulting, there is an alternative and more direct verification method available for online transactions.

BC Registries is trusted to be the authority on registered businesses in British Columbia. In this scenario, Susan Parker makes her claim online and BC Registries is able to electronically verify both the identity information associated with AtoZ Consulting and the fact that Susan Parker is the listed principal.

Figure 6 - Business Context – Principal Affiliation



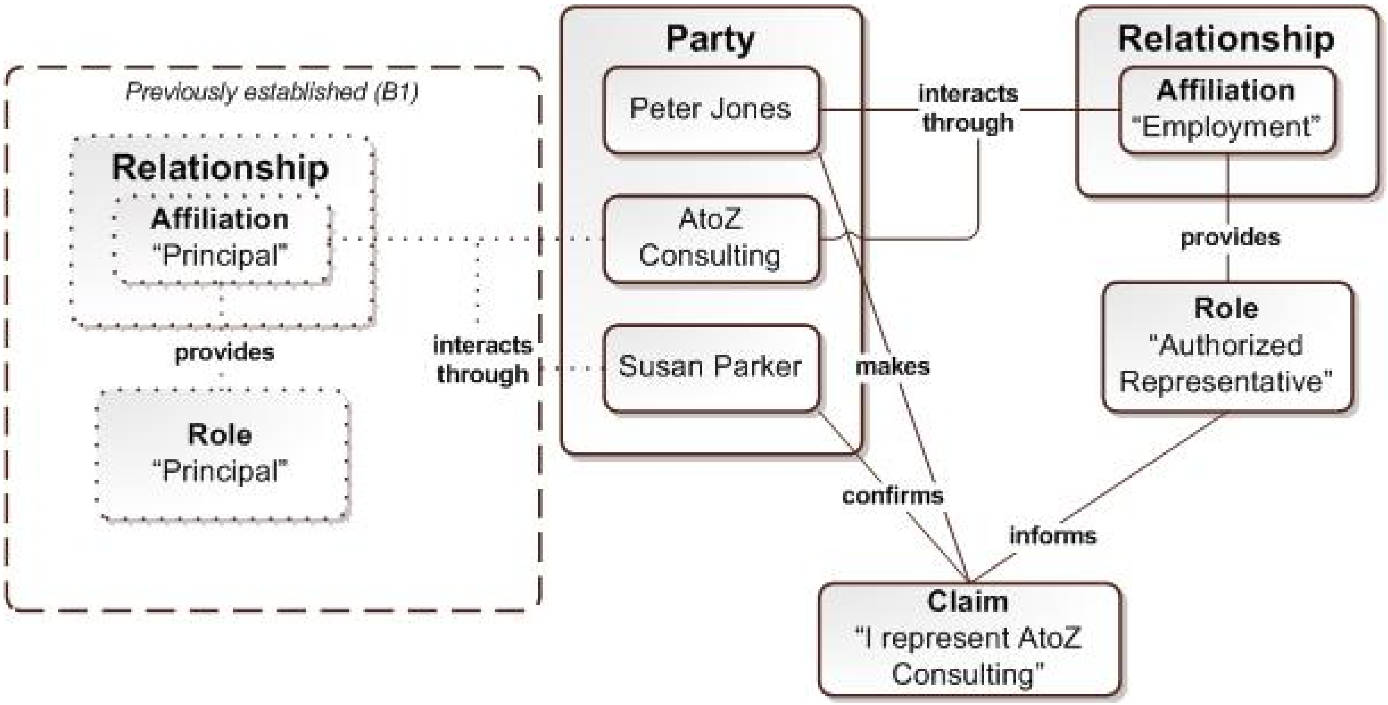
Once Susan Parker's role as principal of AtoZ Consulting is established, she can be used as an Authoritative Party for verifying who is an authorized representative of her business. (See Scenario B2, below.)

B2. Business Context – Employment Affiliation

Scenario:

Peter Jones is an employee of AtoZ Consulting. In this scenario, his claim that he is an authorized representative of AtoZ Consulting can be verified by Susan Parker whose role as principal of AtoZ Consulting has already been established. (See Scenario B1, above.) Because Susan Parker is the principal of AtoZ Consulting, she is trusted to be the authority on who is an employee of her business and who is authorized to represent her business.

Figure 7 - Business Context – Employment Affiliation



As in previous scenarios, Susan Parker can confirm Peter's authority to represent her business in person or online if the appropriate registration and authentication mechanisms are in place.

C1. Professional Context – Member Affiliation

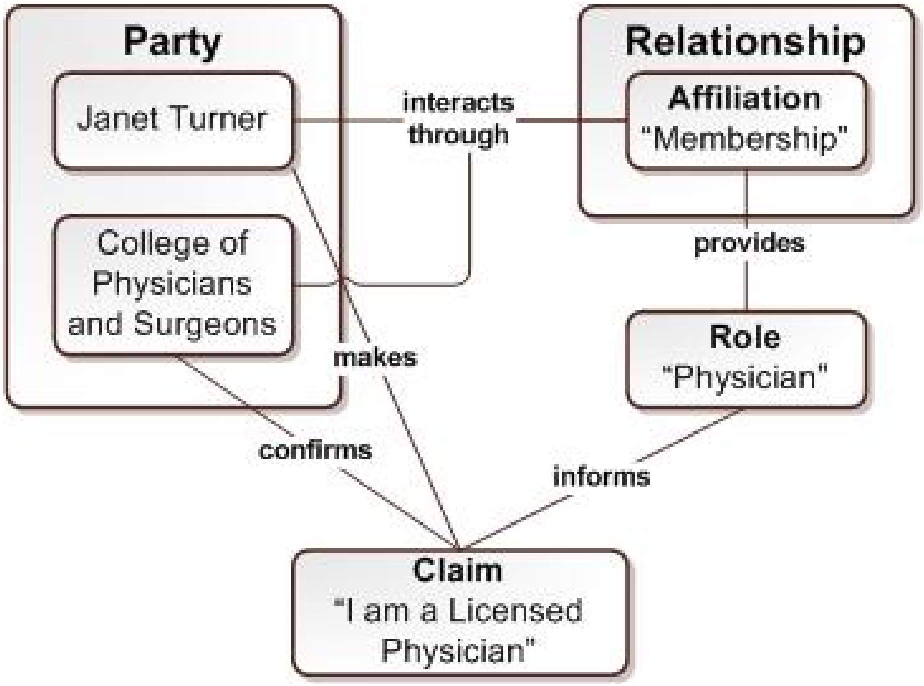
Professionals (such as health, legal and educational professionals) make claims about themselves, their professional accreditations, and the roles they have based on their professional accreditations.

Where an individual is purporting to have a professional role, evidence or verification of the affiliation upon which that role is based may be required. Professional accreditations are granted by professional associations such as the College of Physicians and Surgeons, the College of Teachers and the Law Society of BC. These organizations are trusted to be the authority on whether or not an individual has professional accreditation and is a member in good standing. Verification may be sought from an authorized representative at the organization itself or from another party trusted to be the authority on the professional relationship.

Scenario:

Janet Turner is a member of the College of Physicians and Surgeons. Her membership affiliation with the College provides her with the role of "physician". Because the College is trusted to be the authority on who is licensed to practice medicine in British Columbia, Janet's claim that she is a licensed physician is accepted as true.

Figure 8 - Professional Context – Member Affiliation



Once Janet Turner's role as a "physician" is established, she may wish to delegate some of the responsibilities, activities and authorizations associated with that role to another professional or to an assistant. (See Scenario C2, below.)

C2. Professional Context – Agency (Delegate) Relationship

Professionals often designate or delegate some of the responsibilities, activities and authorizations associated with their professional role to another professional (e.g., a locum) or to an assistant (e.g., delegate).

This is an example of a relationship that is built upon, and is therefore dependent on, other relationships. For example, a physician can only have a designate or locum relationship with another physician. The designate (locum) relationship is dependent on both individuals having a membership affiliation with the College of Physicians and Surgeons which provides both individuals with the role of “physician”. If one of those individuals loses their “member in good standing” status with the College, the designate relationship is similarly invalid.

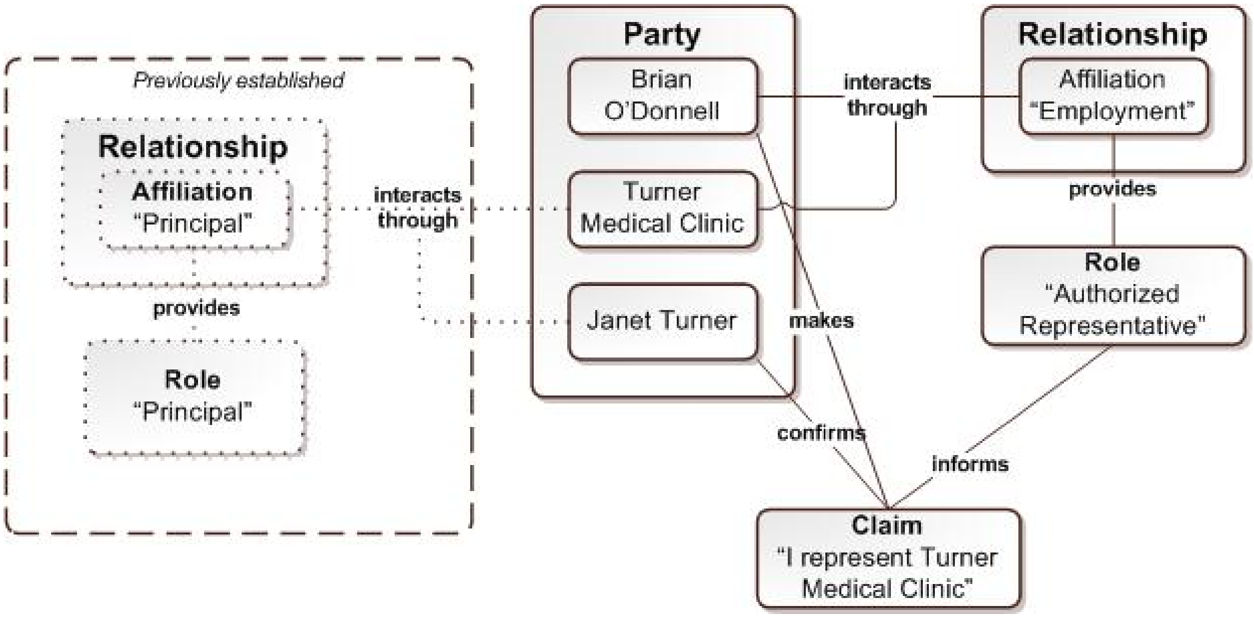
Similarly, a physician may be permitted to delegate certain responsibilities and activities to an employee or assistant. The delegate relationship is therefore dependent on one individual being a physician (i.e., a member of the College of Physician and Surgeons) and the other individual having an employment relationship with the physician or the physician’s business. If the employment relationship ends, the delegate relationship also ends.

Scenario setup: Establishing an Employment Affiliation with a Professional

This scenario builds on Scenario C1, above, where Janet Turner’s role as a “physician” is established. Before she can delegate authorizations associated with her “physician” role to an assistant, the assistant’s employment relationship with her clinic must be established

Brian O’Donnell is a Medical Office Assistant at Turner Medical Clinic, which is where Dr. Janet Turner runs her medical practice. In this scenario, Brian O’Donnell’s employment relationship and his role as her authorized representative are verified by Janet Turner the principal of Turner Medical Clinic (This scenario is similar to scenario B2 under Business Context – Employment Affiliation)

Figure 9 - Establishing an Employment Affiliation with a Professional



Scenario (Delegate Relationship):

Dr. Janet Turner's member affiliation with the College of Physicians and Surgeons and Brian O'Donnell's employment affiliation with Turner Medical Clinic form the basis for the agency or delegate relationship between Dr. Turner and Brian.

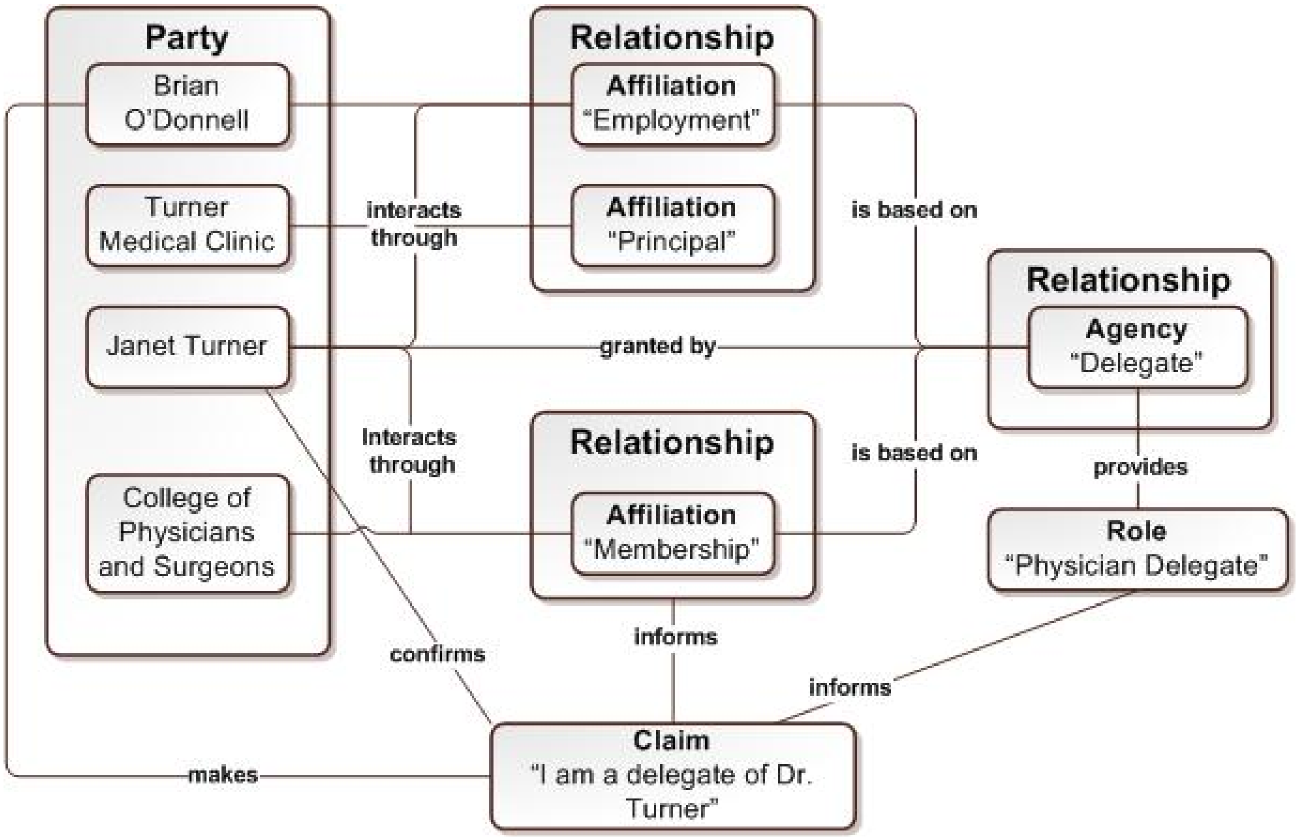
In this scenario, Dr. Turner delegates the authorizations associated with her "physician" role to her assistant, Brian. This is a type of agency relationship which requires no independent verification. Dr. Turner is fully accountable for any actions taken by her delegates and, as such, is the authority on who is permitted to act for her.

In establishing Brian as her delegate, Brian is provided the role of "physician delegate" which he can now use to access systems and perform functions on behalf of Dr. Turner.

Dr. Turner may rescind the delegation at anytime, even if Brian continues to work at her clinic. Brian's employment at the clinic does not automatically entitle him to be Dr. Turner's delegate – this is a separate role and relationship which is granted at the discretion of Dr. Turner.

However, since Brian's employment with the clinic is a precondition of his delegate role, the delegate role and relationship would end when his employment ends. Alternatively, should Dr. Turner lose her member affiliation with the College of Physicians and Surgeons, Brian's role as her delegate would no longer be valid.

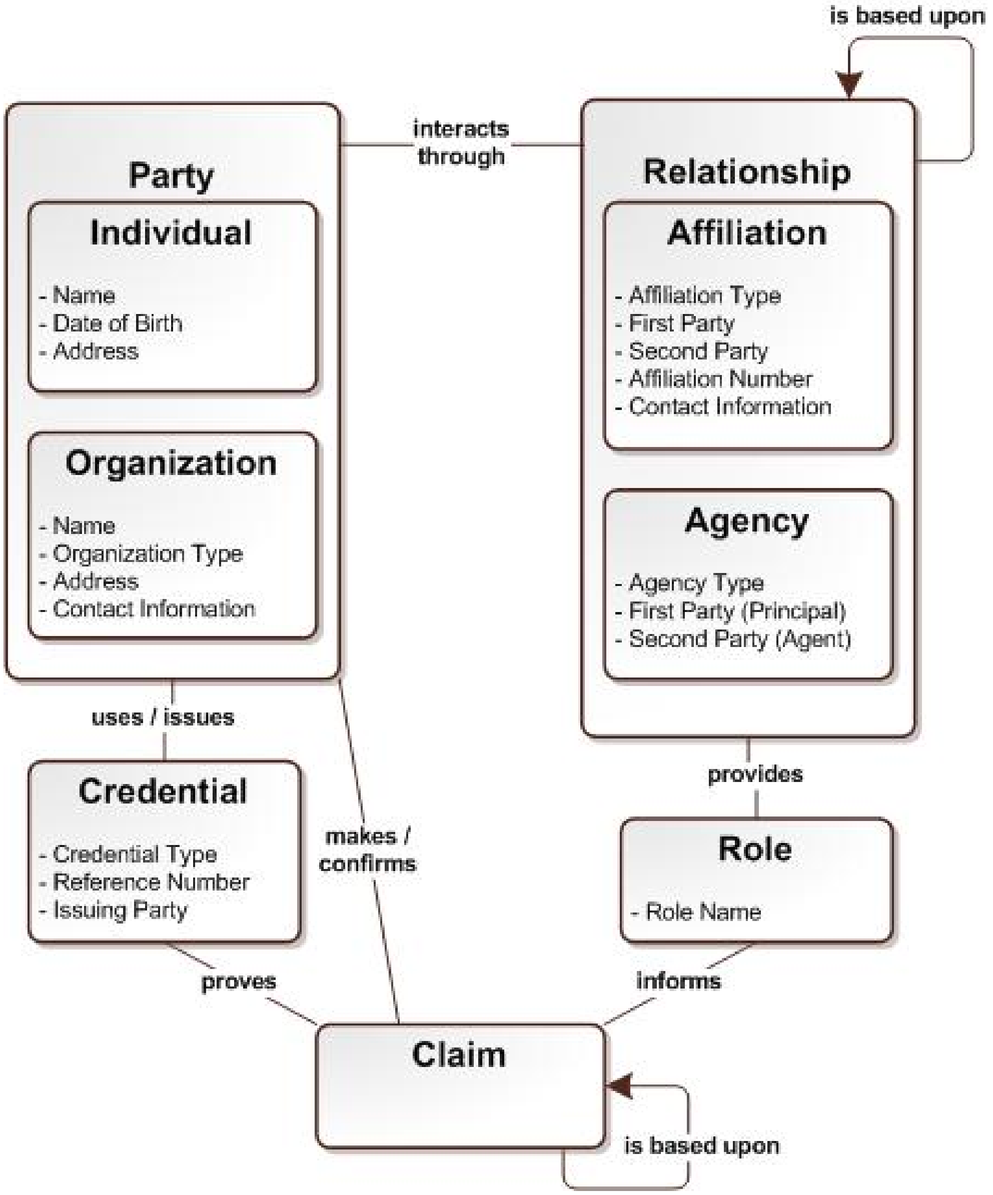
Figure 10 - Professional Context: Agency (Delegate) Relationship



3 Core Data Associated with the Reference Model

Each identity-related element in the Reference Model can be associated with a set of core data (e.g., name, date of birth) and supporting data (e.g., contact information). Figure 11, below illustrates associated data which is generally useful in establishing identity and identity-related relationships.

Figure 11 - Identity Information Reference Model with Associated Data



It should be noted that the set of data associated with each element in the model is not complete. Additional data may be required depending on the situation and/or the service delivery channel utilized. For example, establishing identity to higher levels of assurance may require additional data, such as “place of birth” and online transactions may require additional data such as unique identifiers.

In addition, where data is included in the model, it is described in a simplistic way. For example, name and address are described generally, rather than as specific types of names and addresses (such as Legal Name, Preferred Name, Residential Address, Operating Address).

A full set of required and specific data attributes is included in the *Identity Information Standard.*

3.1 Definitions for Data Elements

Data elements (e.g., name, address) associated with the Reference Model are not defined here. The examples provided in this document are meant to be illustrative rather than prescriptive and utilize general terms rather than specific terms commonly found in standards documents. As such, where data is referenced in this document, it should be assumed to have its ordinary, everyday meaning. Definitions for more specific data elements are set out in the *Identity Information Standards.*

3.2 Identity Scenarios with Associated Data

The following scenarios illustrate how identity and supporting data is associated with individuals, organizations and the multiple relationships they have with one another. These scenarios build on the previous scenarios presented in section 2.2.

The purpose of the scenarios is to illustrate generally how data about parties is linked in different types of relationships and used to support identity claims. The data examples used are not specific and may not reflect a true application (e.g., this document does not purport to use actual role names recognized by organizations and systems). These examples are provided for illustrative purposes only and should not be read as setting specific data requirements.

Specific application of the model and associated data elements are set out in the *Identity Information Standards.*

A1. Individual Context with Associated Data

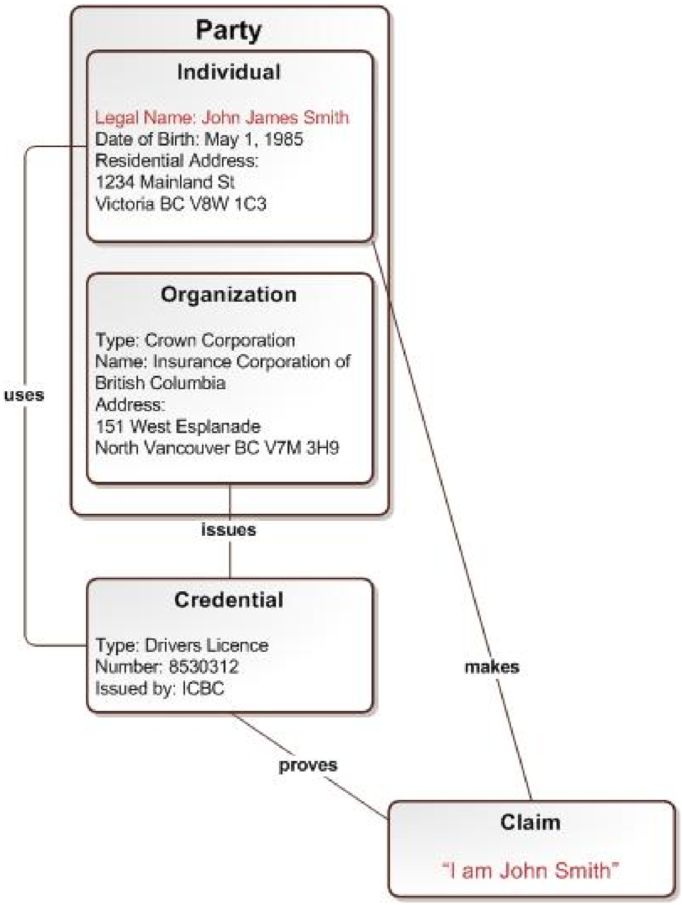
Scenario:

In this scenario, John Smith uses his BC Driver's Licence to prove his claim that he is John Smith. This scenario involves two parties and one credential. ICBC is the issuer of the credential – a BC Driver's Licence – and John Smith is the user of the credential. There is identity data associated with both John and ICBC and supporting data associated with the credential (i.e., data that may support a verification process).

In this scenario, John only needs to prove the claim that he is John Smith. Therefore the only data relevant to this claim is his individual name (appears in red in the model). His birth date and address are irrelevant to the transaction as is the identity information of ICBC. Since John proves his claim by presenting his licence, the supporting data associated with it is also irrelevant in this case.

If the scenario was different and John was making his claim online, supporting data from the credential might be relevant to the transaction in order to support online verification.

Figure 12 - Individual Context with Associated Data



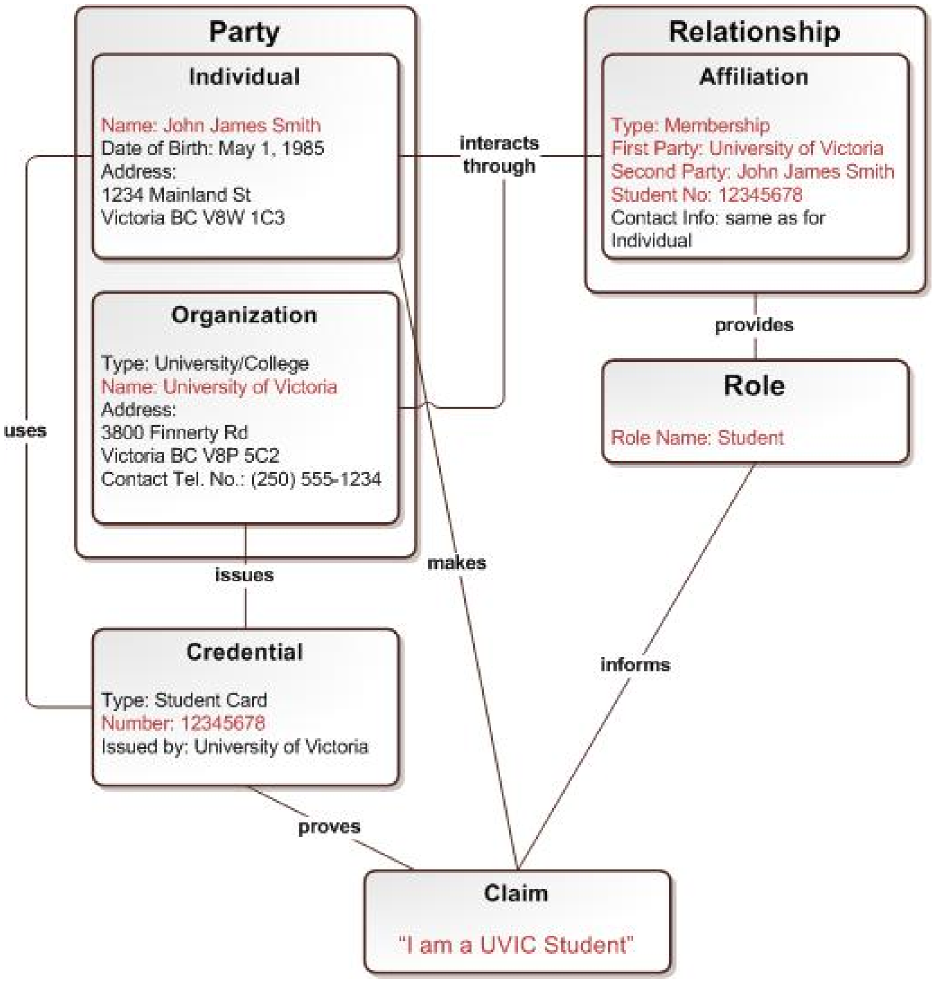
A2. Individual (Student) Context – University Affiliation

Scenario:

In this scenario, John proves his affiliation with the University of Victoria (UVIC) and his role as a student over the internet. This scenario involves two parties, one relationship with an associated role and one credential. UVIC is the issuer of the student card and the Authoritative Party on who is a student at UVIC. There is identity data associated with both John and UVIC and supporting data associated with the relationship and the credential (i.e., data that may support a verification process).

In this scenario, John enters information to support his claim online. The online service electronically verifies the information with UVIC. John's name, UVIC's name and the data associated with the affiliation are all relevant as is his role as a student (this data appears in red in the model). Because John is using the online channel, the student number that appears on his student card is also relevant to this transaction for verification purposes. Other data such as John's birth date and address are not relevant in this scenario.

Figure 13 - Student Context with Associated Data



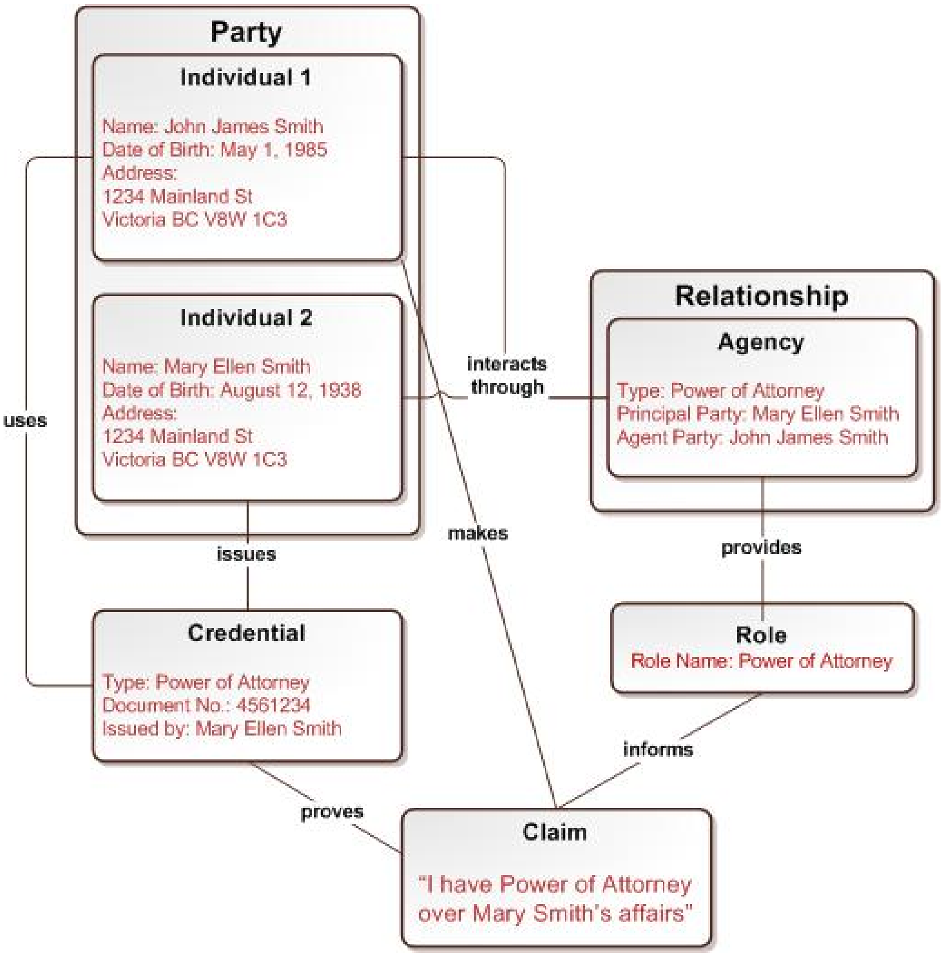
A3. Individual Context – Agency Relationship

Scenario:

In this scenario, John Smith proves his claim that he has power-of-attorney over his mother's affairs by presenting a power-of-attorney document. This scenario involves two parties (John Smith and his mother, Mary Smith), one relationship with an associated role and one credential. Mary Smith is the principal party in the agency relationship and is the authority on who may act on her behalf as an agent. The power-of- attorney document she signed can also be used as evidence. There is identity data associated with both John and Mary and supporting data associated with the relationship and the credential.

In this scenario, John decides to register his power-of-attorney relationship with a government service his mother receives. This will enable him to act for his mother on an on-going basis without having to present the power-of-attorney document repeatedly. To support the registration event, much more data is relevant than was the case in scenarios A1 and A2. John's name, birth date and address are relevant as is his mother's name, birth date and address. As well, all the data associated with the agency relationship, his role and the power-of-attorney document are relevant. (All of this data appears in red in the model).

Figure 14 - Agency Relationship with Associated Data



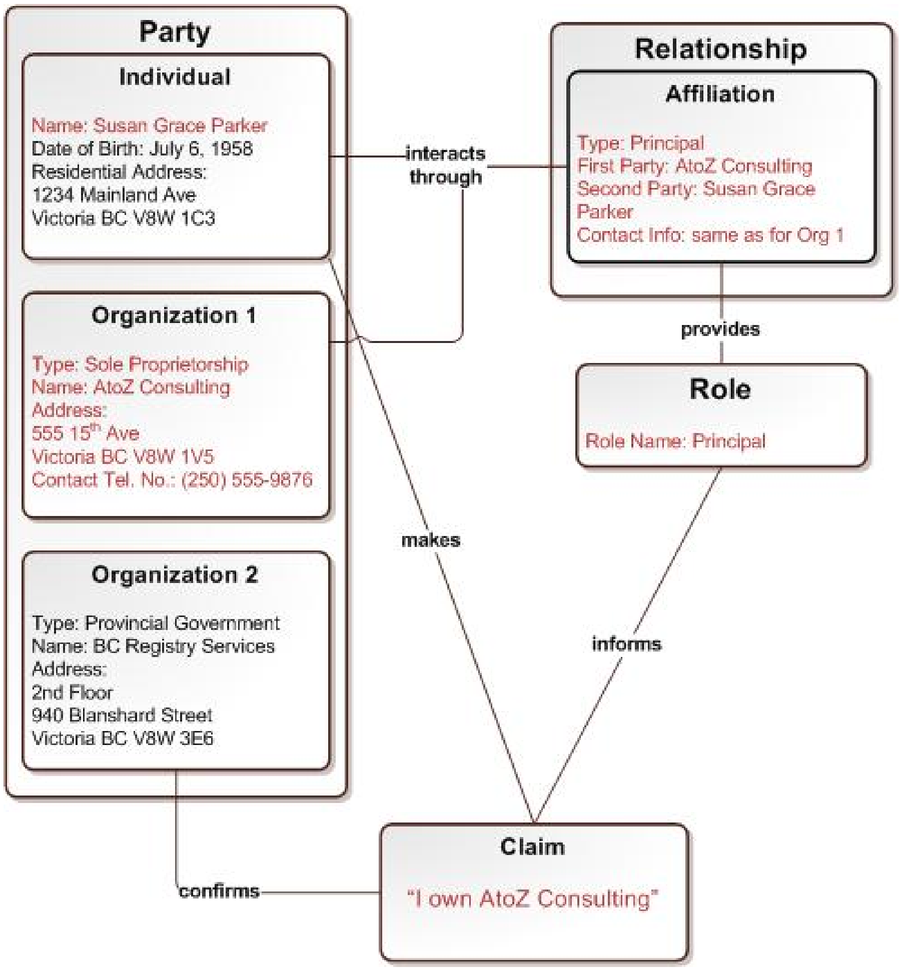
B1. Business Context – Principal Affiliation

Scenario:

In this scenario, Susan Parker's claim that she is the sole proprietor (or principal) of AtoZ Consulting is verified by BC Registries. This scenario involves three parties (Susan Parker, AtoZ Consulting, and BC Registries) and one relationship with an associated role. BC Registries is the authority on both the identity information associated with AtoZ Consulting and the fact that Susan Parker is the listed principal. There is identity data associated with Susan, AtoZ Consulting, and BC Registries and supporting data associated with the affiliation relationship and associated role. The presentation of, or reference to, a credential is not relevant to this scenario.

In this scenario, Susan's claim that she is the principal of AtoZ Consulting is made and verified online. Susan's name, identity data associated with AtoZ Consulting and the data associated with her affiliation are all relevant as is her role as a principal. (This data appears in red in the model). Other data such as Susan's birth date and home address are not relevant in this scenario nor is the identity data associated with BC Registries.

Figure 15 - Principal Affiliation with Associated Data



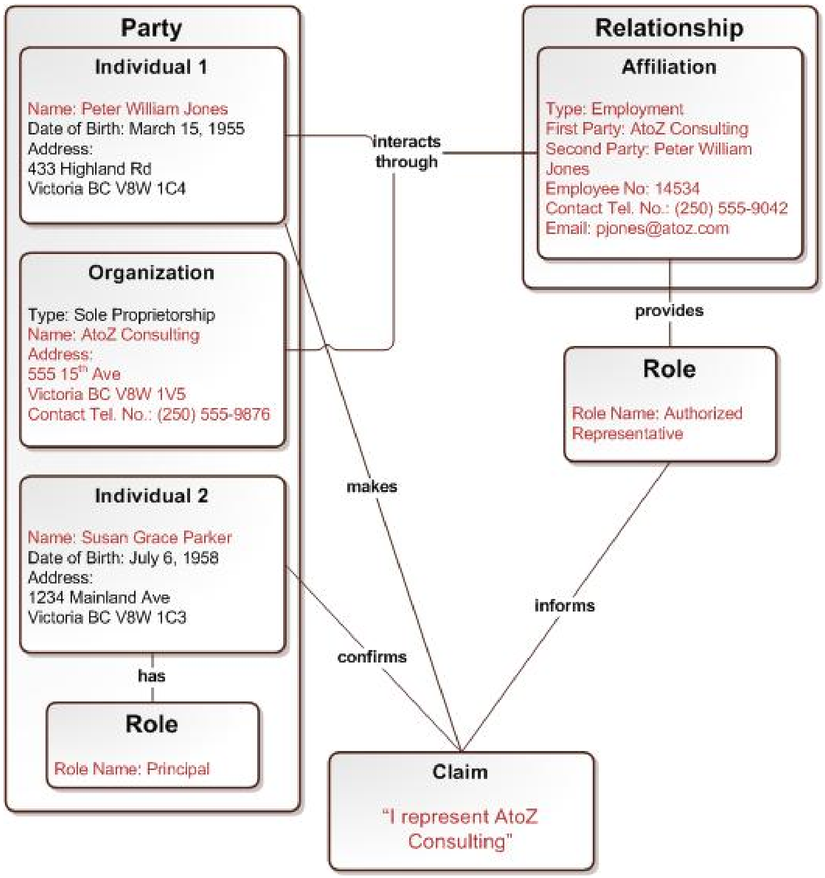
B2. Business Context – Employment Affiliation

Scenario:

In this scenario, Peter Jones' claim that he is an authorized representative of AtoZ Consulting is verified by Susan Parker, whose role as a principal of AtoZ Consulting has already been established (See Scenario B1, above). This scenario involves three parties (Peter Jones, AtoZ Consulting, and Susan Parker) and one relationship with an associated role. Susan Parker is the authority on who is an employee of her business and who is authorized to represent her business. There is identity data associated with Peter Jones, AtoZ Consulting and Susan Parker and supporting data associated with the affiliation relationship and associated role. The presentation of, or reference to, a credential is not relevant to this scenario.

In this scenario, Peter's claim that he is an employee and authorized representative of AtoZ Consulting is verified by Susan Parker online. Susan, whose identity and role as a principal was already established, uses a registered UserID and password to log onto a service and confirm Peter's information and affiliation to her business. Peter' name, identity data associated with AtoZ Consulting, and the data associated with his affiliation are all relevant as is his role as an authorized representative. Because Susan is verifying this information online, her name and role as principal are also relevant to the transaction. (All this data appears in red in the model). Other data such as birth dates and home addresses for both Susan and Peter are not relevant in this scenario.

Figure 16 - Employment Affiliation with Associated Data



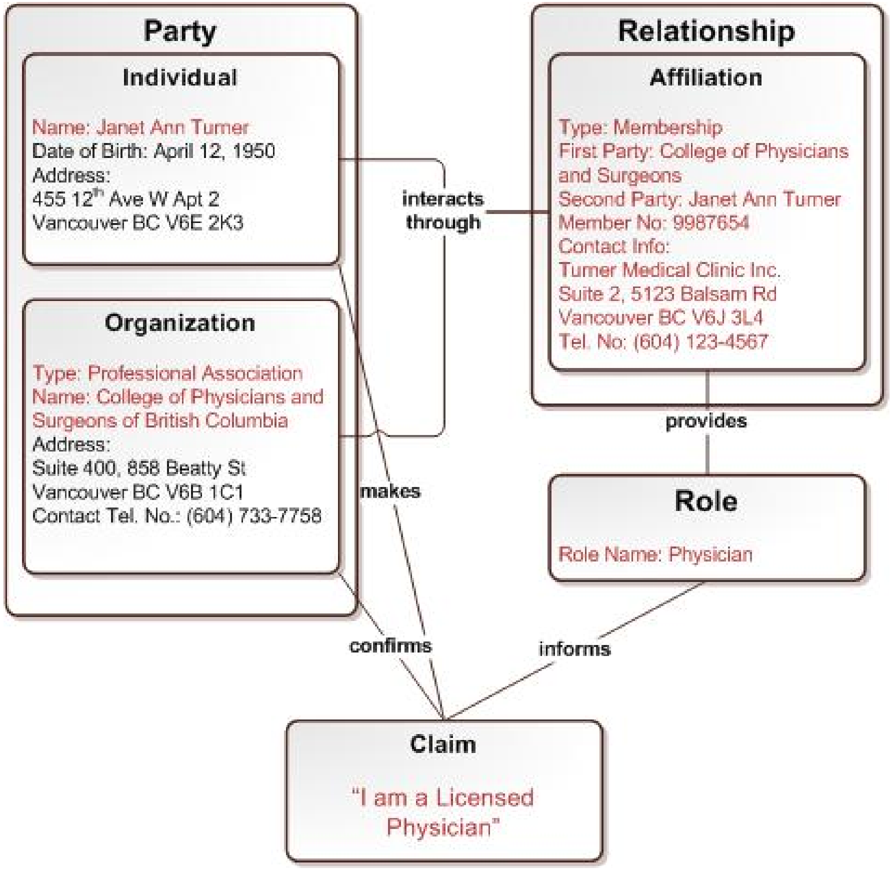
C1. Professional Context : Member Affiliation

Scenario:

In this scenario, Janet Turner's claim that she is a licensed physician is verified by the College of Physicians and Surgeons for British Columbia. This scenario involves two parties (Janet Turner and the College of Physicians and Surgeons) and one relationship with an associated role. The College is the authority on who is licensed to practice medicine in British Columbia and maintains a registry of who is a member in good standing with the College. There is identity data associated with Janet and the College and supporting data associated with her member affiliation and role as a "physician". The presentation of, or reference to, a credential is not relevant to this scenario.

In this scenario, Janet's affiliation with the College and her role as a "physician" are registered with a health services system. This will enable Janet to use her role as a "physician" to access necessary health information about her patients on an as-needed basis. To support the registration event, Janet's name and the College's name and organization type are relevant as is the data associated with Janet's role and membership affiliation (such as her member number and business contact information). (This data appears in red in the model). Other data such as Janet's birth date and home address and contact information for the College of Physicians and Surgeons is not relevant in this scenario.

Figure 17 - Professional Context with Associated Data



C2. Professional Context – Agency (Delegate) Relationship

Scenario Setup:

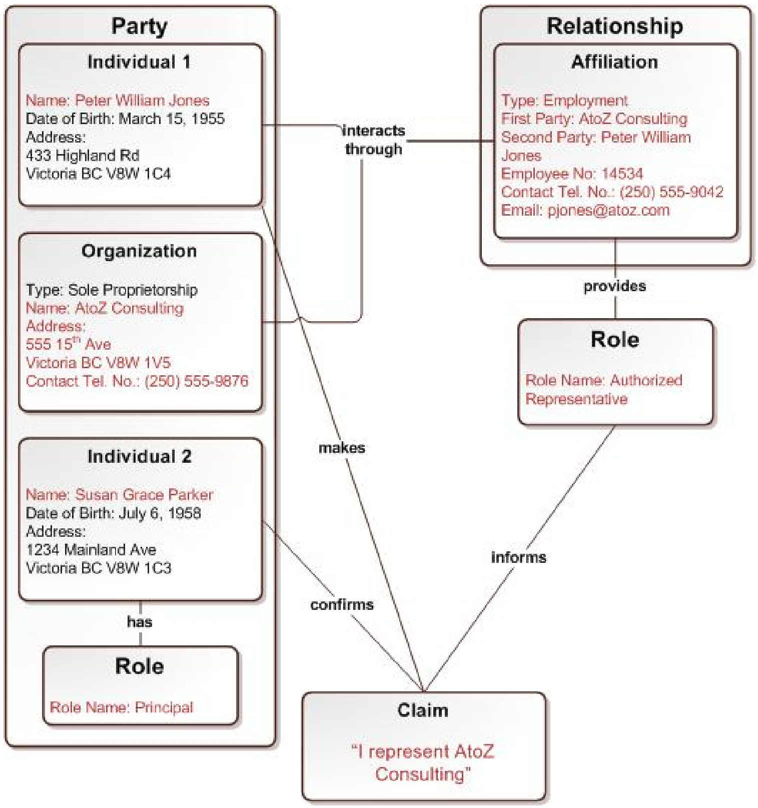
In this scenario, Brian O'Donnell's employment relationship with Turner Medical Clinic and his role as an authorized representative are verified by Dr. Janet Turner, the principal of Turner Medical Clinic.

This scenario is similar in nature to scenario B2 under Business Context – Employment Affiliation, and is only provided here to setup the following scenario where Dr. Turner establishes Brian as her delegate.

As in scenario B2, this scenario involves three parties (Brian O'Donnell, Turner Medical Clinic, and Janet Turner) and one relationship with an associated role. Janet Turner, as a principal of Turner Medical Clinic, is the authority on who is an employee of her clinic. There is identity data associated with Brian, the Medical Clinic and Janet Turner and supporting data associated with the employment relationship and associated role. The presentation of, or reference to, a credential is not relevant to this scenario.

In this scenario, Brian's claim that he is an employee of Turner Medical Clinic is verified by Janet Turner through the submission of a signed form. Peter' name, identity data associated with the Clinic, and the data associated with the employment relationship are all relevant as is Brian's role as an authorized representative. Janet's name as the authorizing principal is also relevant to the transaction. (This data appears in red in the model). Other data such as birth dates and home addresses for both Brian and Janet are not relevant in this scenario.

Figure 18 - Employment Relationship with Associated Data

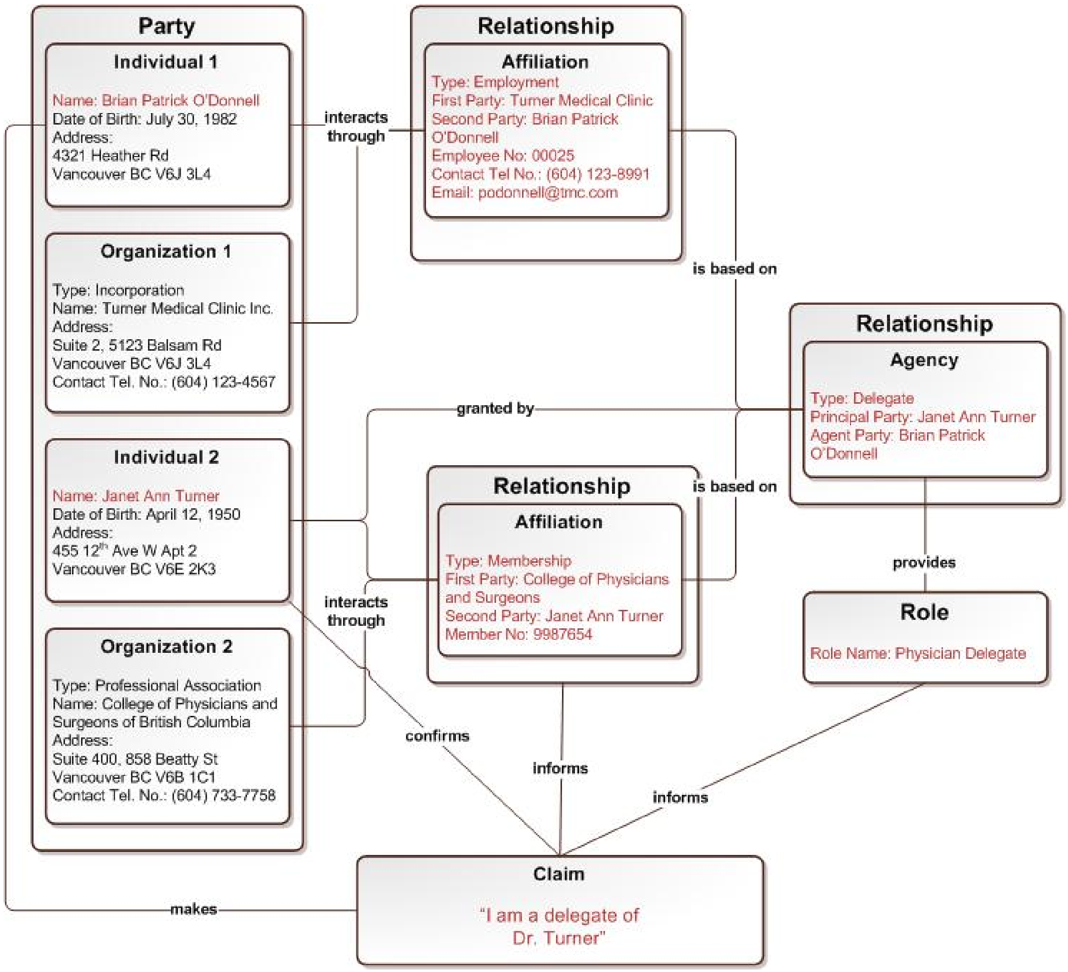


<u>Scenario:</u>

In this scenario, Dr. Janet Turner delegates the authorizations associated with her “physician” role to her assistant, Brian.

As illustrated in the figure below, the establishment of this agency relationship is built on the relationships previously established between: 1) Janet Turner and the College of Physicians and Surgeons; and, 2) Brian O’Donnell and the Turner Medical Clinic. As a result, this scenario involves four parties and three relationships with associated roles. The College is the authority on Janet Turner’s membership and Janet Turner is the authority on both Brian’s employment with Turner Medical Clinic, and his role as her delegate. There is identity data associated with all four parties and supporting data associated with all three relationships and associated roles. The presentation of, or reference to, a credential is not relevant to this scenario.

Figure 19 - Professional Delegate Relationship with Associated Data


Party
Individual 1
Name: Brian Patrick O'Donnell
Date of Birth: July 30, 1982
Address:
4321 Heather Rd
Vancouver BC V6J 3L4
Organization 1
Type: Incorporation
Name: Turner Medical Clinic Inc.
Address:
Suite 2, 5123 Balsam Rd
Vancouver BC V6J 3L4
Contact Tel. No.: (604) 123-4567
Individual 2
Name: Janet Ann Turner
Date of Birth: April 12, 1950
Address:
455 12th Ave W Apt 2
Vancouver BC V6E 2K3
Organization 2
Type: Professional Association
Name: College of Physicians and Surgeons of British Columbia
Address:
Suite 400, 858 Beatty St
Vancouver BC V6B 1C1
Contact Tel. No.: (604) 733-7758
interacts through
Relationship
Affiliation
Type: Employment
First Party: Turner Medical Clinic
Second Party: Brian Patrick O'Donnell
Employee No: 00025
Contact Tel No.: (604) 123-8991
Email: podonnell@tmc.com
is based on
Relationship
Agency
Type: Delegate
Principal Party: Janet Ann Turner
Agent Party: Brian Patrick O'Donnell
granted by
is based on
Relationship
Affiliation
Type: Membership
First Party: College of Physicians and Surgeons
Second Party: Janet Ann Turner
Member No: 9987654
provides
Role
Role Name: Physician Delegate
interacts through
confirms
informs
informs
Claim
“I am a delegate of Dr. Turner”
makes

In this scenario, Brian’s relationship with Dr. Janet Turner and his role as her delegate are registered with a health services system. This will enable Brian to access certain information and perform certain functions in the system on behalf of Dr. Turner. To support the registration event, Brian’s name, Janet’s name, data associated with Janet’s membership and role, and data associated with Brian’s agency relationship and role are all relevant. (This data appears in red in the model). Other data such as birth dates, home addresses, and identity data associated with the College of Physicians and Surgeons and Turner Medical Clinic are not relevant in this scenario.

APPENDIX A – TERMS AND DEFINITIONS

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

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

Term	Definition
Agency	A specialized type of relationship where one party is empowered to act for another party in some capacity. For example, one individual may be another individual's delegate or one individual may have power of attorney over another individual's affairs.
Affiliation	A relationship between two parties (usually an individual and an organization) that can be verified by an authority. Typical affiliations include membership, employment or ownership/directorship. For example, an individual may be a member or employee of a particular organization.
Authentication (Business)	The act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the thing are true.
Authoritative Party	An organization or individual 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.
Business Role	Users may be associated with one or more "business roles" which describe the business function of the user. For each business role there is an Authoritative Party that manages the definition and use of the business role.
Claim	An assertion that something is true. Some claims are based on, or derived from, other claims. For example, the claim "I am over the age of 18" is based on a date of birth claim and the claim "I am a resident" is based on an address claim. Derived claims are important from a privacy perspective because they meet program needs (e.g., age and residency requirements) without exposing more information that is necessary (such as one's actual age or home address).
Contact information	Information used to contact an individual or organization.
Context	see **Identity Context**
Credential	A physical or electronic object (or identifier) that is issued to, or associated with, one party by another party and attests to the truth of certain stated facts and/or confers a qualification, competence, status, clearance or privilege. Identity credentials can be cards, like a driver's license or smart card; documents like a passport; or, in the context of digital identities, a User ID and password or digital certificate.

Term	Definition
Identification	The process of associating identity-related attributes with a particular person.
Identity	A set of characteristics by which a person or thing is definitively recognized or known.
Identity Assurance	A measure of confidence that an identity claim or set of claims is true.
Identity Claim	An assertion of the truth of something which pertains to a person's identity. An identity claim could convey a single attribute such as an identifier (e.g. a student number) or it could convey that a person is part of a certain group or has certain entitlements (e.g. I am over 18, I am a company employee). A set of identity claims could provide sufficient identity attributes (e.g. name, date of birth address) to permit the identification of a person.
Identity Context	The environment or circumstances in which identity information is communicated and perceived. Individuals operate in multiple identity contexts (e.g., legal, social, employment, business, pseudonymous) and identify themselves differently based on the context.
Identity information	A set of attributes used to describe a person and may be used to distinguish a unique and particular individual or organization.
Identity Information Management	A set of principles, practices, policies, processes and procedures that are used within an organization to manage identity information and realize desired outcomes concerning identity.
IDIM	see **Identity Information Management**
Individual	A human being.
Organization	A group of people that work or associate together. An organization may be a legal entity like a business or government agency, a subsidiary or division of a legal entity or it may be an informal association such as a working group.
Party	An individual or organization.
Personal Information	Recorded information about an identifiable individual other than business contact information.
Relationship	An association or connection between two parties.
Role	A set of responsibilities, activities and authorizations assigned to an individual based on an affiliation or agency relationship. For example, an individual that is a member of the College of Physicians and Surgeons may be assigned the role of "Physician" and a medical office assistant who is employed at a health clinic and is an authorized delegate of a "Physician" may be assigned the role of "Physician Delegate".