Ministry of Labour and Citizens' Services

# IDENTITY INFORMATION MANAGMENT ARCHITECTURE SUMMARY

## Architecture and Standards Branch
## Office of the CIO ● Province of BC

*People ● Collaboration ● Innovation*


**Author:** I. Bailey



**Creation Date:** May 28, 2008
**Last Updated:** March 23, 2009
**Version:** 0.7

## Reviewed By

| Name | Organization & Title |
|---|---|
| | |

## Revision History

| Version | Date | Changed By | Description of Change |
|---|---|---|---|
| 0.1 | May 28, 2008 | Ian Bailey | Initial draft |
| 0.2 | December 12, 2008 | Ian Bailey | Updated as per IDIM conceptual model |
| 0.6 | January 27, 2009 | Ian Bailey | Updated as per IDIM conceptual model 2 |
| 0.7 | March 23, 2009 | Herb Lainchbury | Incorporated into Connected Systems Architecture Package |

## Document Purpose

This document is intended to provide a summary overview of the base architecture for the BC Provincial Identity Information Management System (IDIM) for the benefit of system integrators and other IT service providers in the preparation of responses to Request For Proposal opportunities. It captures and conveys the purpose of the IDIM and the services it provides. As such this document is not a general description of architecture principles and patterns to be followed by provincial ministries, nor is it an enterprise architecture blueprint for government. It is rather focused on an overview of the logical architecture of the IDIM as designed to support the development of Provincial IM/IT services. Readers should also refer to the Information Access Layer Architecture Summary document as IDIM is a component of the Information Access Layer architecture.

# Connected Systems Architecture Package

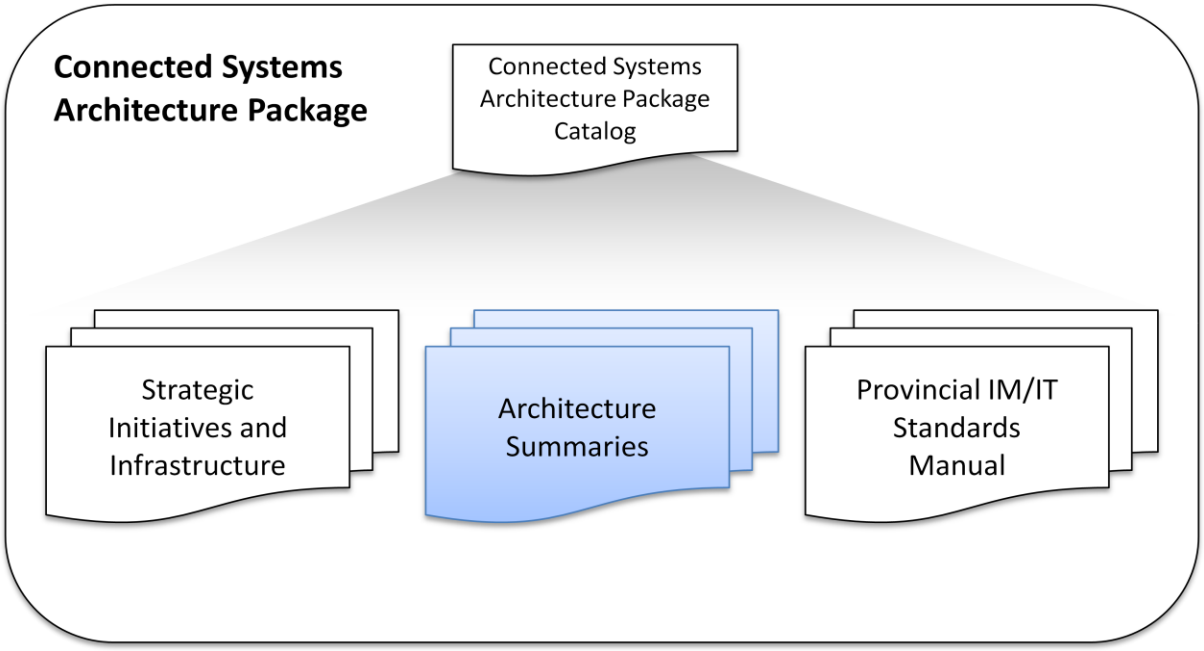
This document belongs to a set of documents called the Connected Systems Architecture Package. The Connected Systems Architecture Package includes materials on strategic Information Management and Information Technology (IM/IT) initiatives and infrastructure relating to the Connected Systems Strategy and features a broad range of concepts including architecture, standards and technical specifications.

The Strategic Initiatives and Infrastructure sub-package informs readers of key strategic initiatives and infrastructure through a collection of brief one page summaries.

The Architecture Summaries provide background material for the development of provincial information sharing services, in an attachment to a RFP for example.

The Provincial IM/IT Standards Manual provides official documentation regarding provincial IM/IT standards and policies.

The diagram below gives a high level overview of the types of documents available in the Connected Systems Architecture Package with the document you are currently reading highlighted. Please refer to the **Connected Systems Architecture Catalog** for a complete list of documents in the Connected Systems Architecture Package.



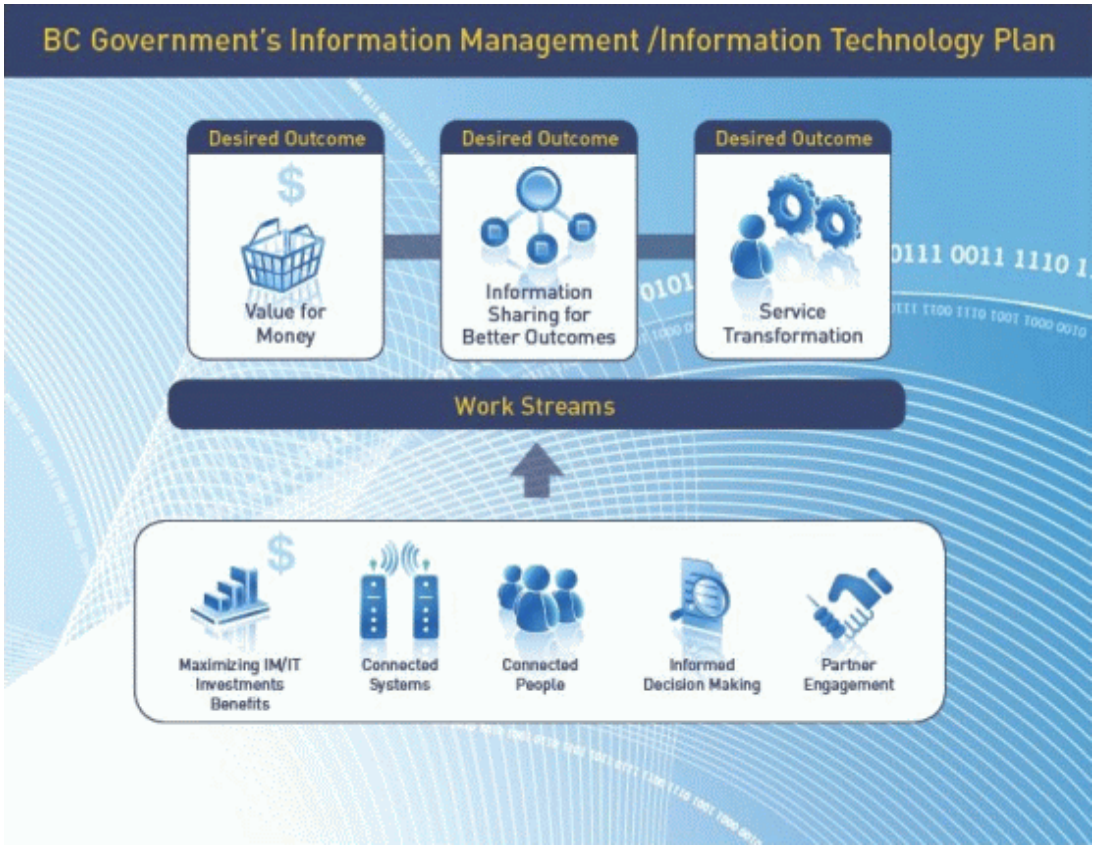
# TABLE OF CONTENTS

# TABLE OF FIGURES

# 1 Overview

## 1.1 Business Context

The OCIO is implementing an Information Management/Information Technology (IM/IT) plan for government to improve information sharing to better achieve citizen outcomes. The IM/IT plan is about securely connecting systems and people, identifying evidence-based outcomes and making sound investment decisions, all supported by a next generation information structure.




A key enabler of the next generation information structure is the Province's Identity Management Program (IDIM). At the heart of information sharing, connecting people, and providing access to information systems is the knowledge of who we are sharing the information with, what organizations they we are working for, what roles and privileges they have been granted, and, for many public services, assurances of whom the information is about. The Identity Management Program provides this knowledge and assurances so that we can securely, and respecting privacy, share information, connect the workforce, and provide appropriate access.

## 1.2 Core Concepts

The architecture of the IDIM is based on two foundation bodies of work: the Claims and User Centric Identity Management Architecture and the Pan Canadian Identity Management Framework. The architecture and framework are published on the OCIO website at http://www.cio.gov.bc.ca/idm.

### *1.2.1 Claims and User Centric Identity Management Architecture*

The Claims and User Centric Identity Management Architecture was developed by the Province collaboratively with representation from the broader public sector of British Columbia and industry leading vendors of identity management technologies. This technical architecture describes a scalable and secure way to exchange identity information (claims) between parties using electronic services.

The diagram below shows the core components of the architecture and the simplest case where a single authoritative party, identity agent, and relying party interact to provide secure access to an electronic service. These three core entities can be combined into more complex scenarios. See the Architecture document for a more complete description.

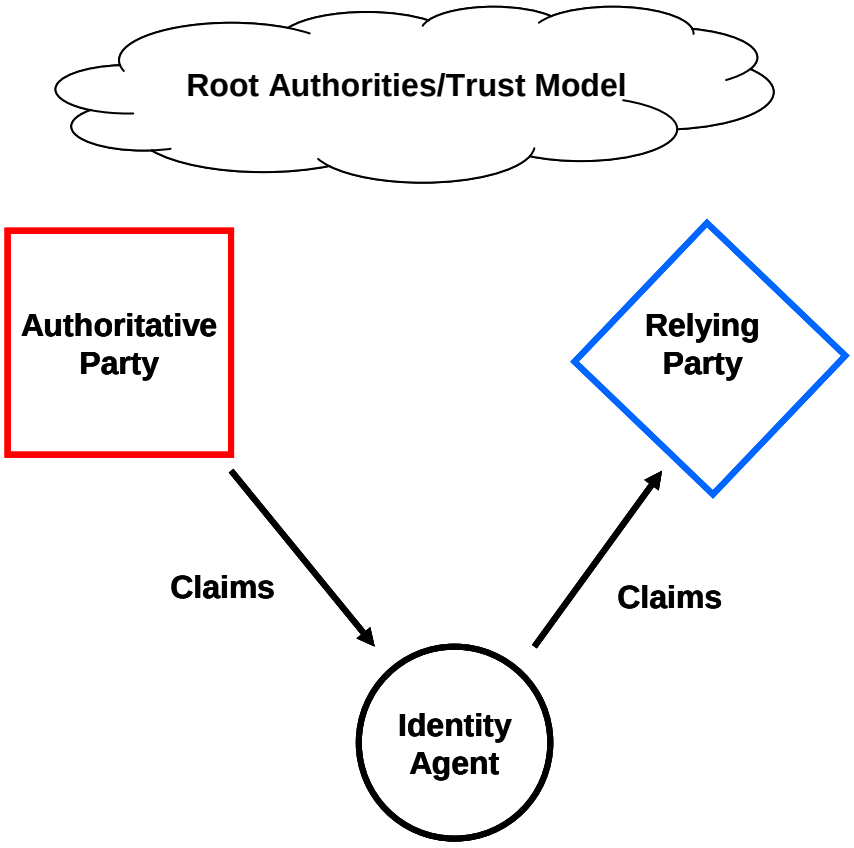



**Figure 1 Claims and User Centric Architecture**

### *1.2.2 Pan Canadian Identity Management Framework*

The Inter-jurisdictional (or Pan-Canadian) Identity Management and Authentication Task Force was established by a council of Deputy Ministers across provincial, territorial and federal governments with responsibility for service delivery and supported throughout its six month term by the Public Sector CIO Council and the Public Sector Service Delivery Council. The Task Force was established to develop a pan-Canadian strategy for identity management and authentication (IdM&A) that would facilitate seamless, cross jurisdictional, citizen-centric, multi-channel service delivery. The framework provides a policy and service model for an Identity Management Program.

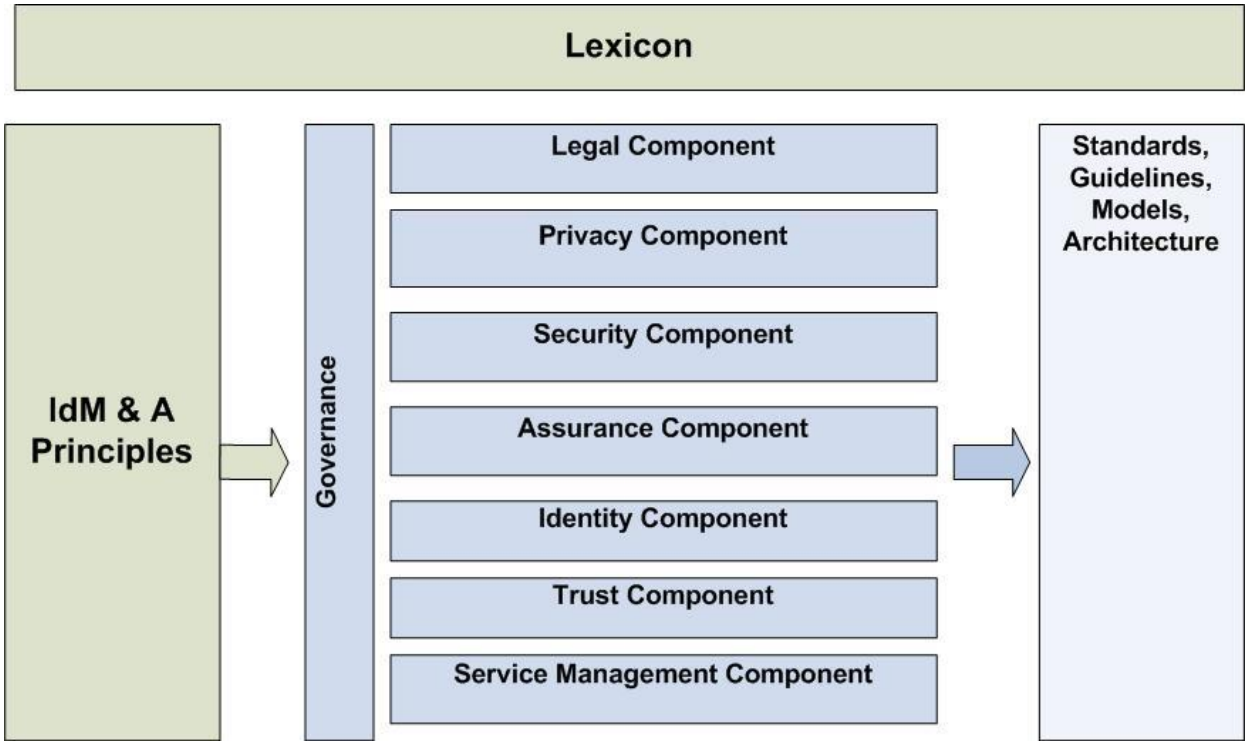



**Figure 2 Pan Canadian Identity Management Framework**

### *1.2.3 Users and Subjects*

The IDIM is fundamentally about information management for the identity attributes of people using public services, and the people that are the subjects of the public services. In some cases the user and subject are the same person, as in citizen self service applications, and in other cases the user and subject are different persons, as in a doctor using an electronic service to access information about a patient. In latter case the doctor is the *user* and the patient is the *subject*. If the patient was accessing their own medical records then they are both the *user* and *subject*.

### *1.2.4 Personas*

The IDIM recognizes the different identity contexts when people use or are a subject of public services. A person may be an employee of a public service organization and an individual citizen referenced in that public service. A medical professional can be a patient, a licensed provider of medical care, and a business owner. We call these identity contexts (citizen, public servant, medical professional, business owner) "personas". We recognize these separate personas in the IDIM so that, where appropriate, the differing contexts are separated.

The IDIM supports personas in three different contexts. These contexts are: a person as an individual; a person as an employee or principal of an organization, and a person as a licensed professional. Note that a person may have multiple business personas or professional personas but only one individual persona.

### *1.2.5 Root Authority, Trust, and Federation*

Identity management is fundamentally of a distributed nature. Our identity information comes from many different sources (or parties), some from legislated government bodies, some from organizations, and some from ourselves. Any party that needs to rely on identity information from another party will (mostly) require some level of trust in that other party (providing the identity information). When one party has trust in another party and will accept identity information from another we call this *federation*. The IDIM is a federation of public sector and private sector parties that trust each other for identity information. The root authority is the party that provides the governance of the federation, in our case the Province of British Columbia is the root authority.

### *1.2.6 Authoritative Parties*

An authoritative party is an organization (or person) that is trusted, and hence part of the federation, to be a source of the identity attributes about the users and subjects of our public services. The authoritative party may be recognized because of legislation, a government policy, a contract, or naturally as in an organization being recognized as an authority for its employees. In the architecture an authoritative party is recognized to make claims (see below) about the identity attributes of users and subjects. Authoritative parties usually make claims about a single type of persona.

### *1.2.7 Claims*

The identity information that authoritative parties provide are called claims. These claims may be tombstone type information such as name and birth date, or 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 claim should consider. An assurance claim could indicate that the user has been identified via a rigorous process and has signed on using a strong authentication technology such as smart card. Claims may be derived from other claims, such as a claim that a person is over 18 years of age (derived from birth date) or a resident of a municipality (derived from residential address).

### *1.2.8 Relying Parties*

A relying party is any electronic service provider that requests claims about users or subjects from one or more authoritative parties. Public service organizations that provide electronic services are relying parties. For users accessing an electronic service, the relying party requests claims via a security token service so that a local access policy can be checked and appropriate access granted. For managing records about subjects, a relying party requests claims via a registry service, often via a web services interface (see the IAL Architecture Summary document).

### *1.2.9 Identity Agents*

In the user centric architecture, the Identity Agent (also known as Identity Selector), is software that acts on behalf of the user, usually in combination with a web-browser or other user client software. Microsoft Cardspace is an example of an Identity Agent. The Identity Agent manages the movement of claims from an authoritative party to a relying party and provides user experience, security, and privacy functions.

*Note: Legacy identity management systems (access management technologies) such as CA Siteminder and Sun Access Manager or OpenSSO can act as a "non user centric" identity agent to pass claims from an authoritative party to a relying party, typically using proprietary single-sign-on technology or a federation technology (such as SAML 2.0). In this case the user experience, security, and privacy functions of an identity agent are limited or unavailable.*

### *1.2.10 Anatomy of an Authoritative Party*

Authoritative parties provide claims about their users and/or subjects via multiple distinct interfaces. An authoritative party may provide all or some of these interfaces, depending on the type of identity information they are managing.

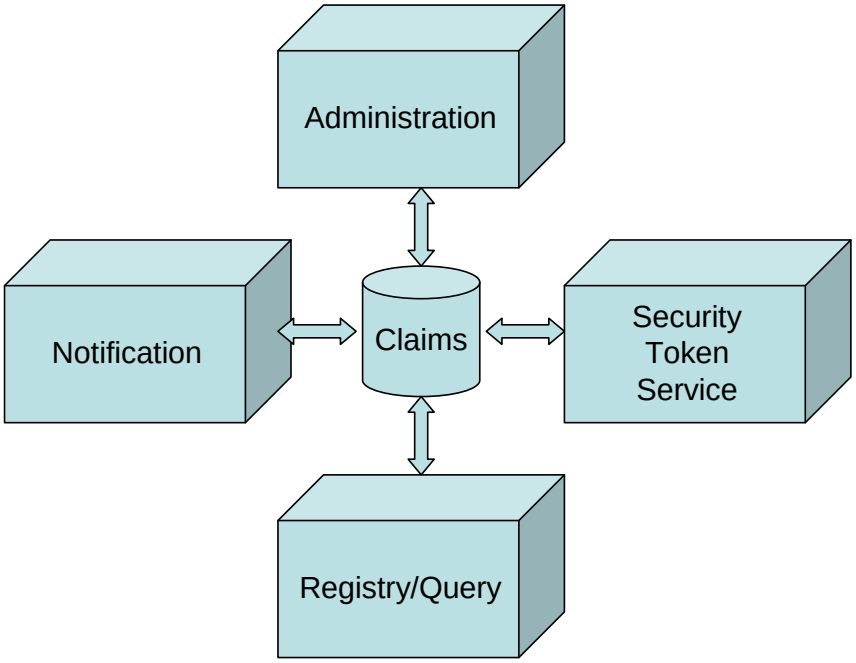



**Figure 3 Interfaces for an Authoritative Party**

#### 1.2.10.1 Registry or Query Interface

For claims about subjects (who may also be users), a Registry or Query interface is provided so that other systems can look up or verify the claims about a particular subject. Interestingly, the registry interface for an authoritative party is itself a relying party and may require claims from another authoritative party to satisfy its access policy and provide claims. The registry or query interface is usually implemented as a SOAP interface and hosted on the Information Access Layer.

#### 1.2.10.2 Security Token Service

For claims about users, a Security Token Service (STS) is provided so that systems receive claims information about the user accessing the service. A security token is a tamper proof electronic document containing claims about a user, usually complying with the Security Assertions Mark-Up Language specification. The STS is usually compliant with the Ws-Trust protocol.

#### 1.2.10.3 Notification Service

An authoritative party can provide a notification service that relying parties and other authoritative parties can subscribe to. The notification service can provide claims to indicate

add/change/delete events for subjects and users, usually for automated provisioning. Security Provisioning Mark-up Language specification is usually used as the vehicle for these claims.

#### 1.2.10.4 Administration Interface

Authoritative parties also typically provide a relying party interface to allow for the management of the claims information, usually as web site that allows for add/change/delete transactions. SOAP interfaces can also be provided to allow for automated provisioning, usually relying on Security Provisioning Mark-up Language specification.

### *1.2.11 Registration, Authentication, and Assurance*

An important aspect of claims is the level of assurance that a relying party should place in the claims. The other way to look at assurance is the probability that the claim is true. If the entire life cycle of the claim information held by an authoritative party and passed to a relying party is rigorous and well protected then a relying party can have a high level of assurance in a claim and probability is high that the claim is true. By providing the assurance level as a claim, a relying party can then tie access policy to the assurance level. The following diagram from the Pan Canadian framework shows the relationship of registration, authentication, and operational rigor in establishing assurance. Readers should consult the most recent government standard for assurance.

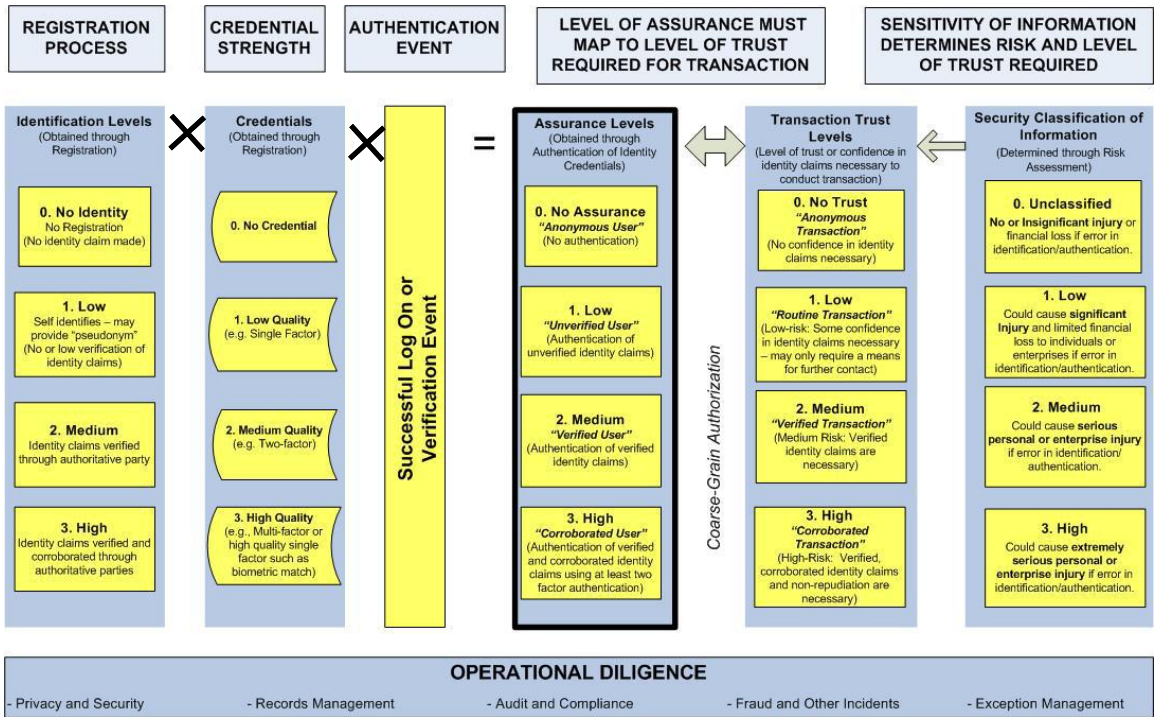



**Figure 4 Pan Canadian Assurance Levels**

### *1.2.12 Authentication Credential Strength*

The assurance model described above includes the concept of credential strength which is a measure of the ability of the credential to withstand attack or compromise. For example, the use of shared secrets to authenticate a person is considered low strength because they are

shared and therefore difficult to control which people have access to the secrets. Conversely, hardware cryptographic tokens with asymmetric private keys and PIN are extremely difficult to compromise and there is very high probability that the only the rightful owner is in possession of the credential and able to authenticate with it.

Another aspect of the credential important to the architecture is the compatibility of the credential to the products available that support the user centric architecture. The WS-Trust protocol supports four authentication methods, username/password, Kerberos, SAML, and x509.3 certificate. Readers can consult the government standards for these authentication methods for further details.

### *1.2.13 In Person Identification*

IDIM includes the provision of identification cards for in person identification of people using public services. The identification cards conform to government standard and ensure that subject registration processes result in high quality subject data within the public services. Readers can consult government standards for the format and content (claims) of the identification cards. Systems builders should ensure that processes and tools conform to the identification standards.

The identification cards may be combined with user authentication credentials such as smart card chip, again consult government standards for details.

### *1.2.14 Program and Domain Identifiers for Individuals*

IDIM does not rely on or promote the concept of a universal identifier for individuals that authoritative parties and relying parties would all record and use as subject/user linkages. The IDIM program considers a universal identifier to be unacceptable from a privacy and security perspective.

Programs and domains (e.g. Health domain) may create domain level identifiers (such as PHN) to better serve their clients and manage their information. This prevents public services from inappropriately linking information together and creating a complete profile of an individual's services.

This policy principle creates a challenge in ensuring that our public service workforce has appropriate access to information from other programs and domains. To solve this problem IDIM is creating an Identity Resolution Service to broker the translation of one program identifier to another in a privacy enhancing way. The service design is in the requirements stage at the time of this writing.

# 2 BC Government Identity Management Architecture

## 2.1 Root Authority for Federation

The root authority and governance body for the federation of authoritative parties is the Province of British Columbia. The root authority establishes legislation, policy, and governance for the design and operation of the federation. The root authority establishes the trust criteria and operation of membership (authoritative parties and relying parties) in the federation.

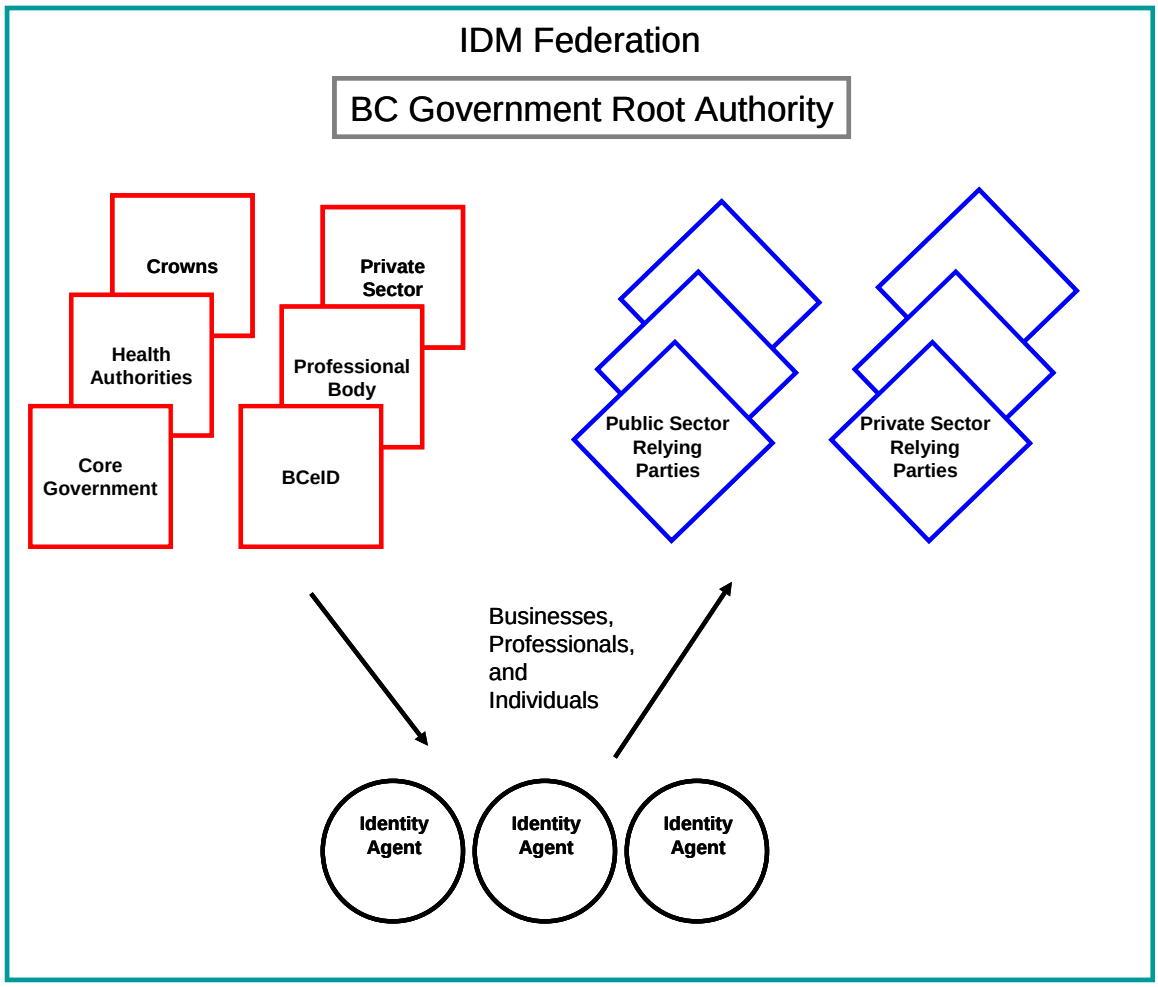



**Figure 5 IDIM Federation**

## 2.2 Authoritative Parties

The authoritative parties in the federation are any public or private sector organizations that meet the criteria established by the root authority.

### *2.2.1 Public Sector Organizations (business personas) as Trusted Enterprises*

Most public sector organizations are trusted to make claims about their employees, to enable access to relying parties in the federation. The following are examples of public sector organizations that make claims about their employees:

- Core Government (Ministries)
- Crown Corporations
- Health Authorities
- Universities
- School Districts

### *2.2.2 Private Sector Organizations (business personas) as Trusted Enterprises*

Private sector organizations, that meet the criteria established by the root authority, are trusted to make claims about their employees. Private sector organizations, unable or unwilling to establish themselves as authoritative parties, can register with the BCeID authoritative party.

### *2.2.3 Licensed Professionals (professional personas)*

Professional licensing bodies that meet the criteria to join the federation can establish their own authoritative party functions or they can register with the BCeID authoritative party.

### *2.2.4 BCeID (all personas)*

The BCeID authoritative party is a common service authoritative party that is trusted to make claims about individuals, and private and public organizations that are unable to provide their own authoritative party functions. BCeID has identification, registration, and authentication services to manage the claims of individuals, professionals, and organizations (businesses).

## 2.3 Claims

Claims are normally in the form of SAML 1.1 or 2.0 documents, however, for legacy systems integration the claims may be in other forms. The federation has a base set of standard claim types for the three personas and custom claim types can be defined for an application or set of applications (domain). Readers should consult the latest government standards manual for claim standards.

## 2.4 Registries

Authoritative parties provide registry services via a web services (SOAP) interface and public sector AP's may provide these services using the Information Access Layer (IAL) common infrastructure. See the IAL Architecture Summary for additional information about providing services via the IAL.

## 2.5 Security Token Services

Authoritative parties provide token services using a WS-Trust protocol server, usually connected to a directory server or DBMS repository. Most public sector AP's will have the token server connected to their Windows Active Directory service.

## 2.6 Notification Services

Authoritative parties provide notification services via a web services interface, usually with a COTS user provisioning solution. Public sector bodies may provide these services using the IAL common infrastructure.

## 2.7 Relying Parties

Relying parties must be constructed to accept claims from appropriate authoritative parties in the federation. This integration is best implemented using a Federation Gateway device provided by the Federation. Additionally, access management products such as CA Siteminder, Sun Access Manager, and Microsoft ADFS, can provide this integration, or may be available directly with some COTS products. Custom coding to accept claims is possible but not encouraged. Readers should consult the IM/IT Standards Manual for additional information about integrating relying parties with the IDIM services.

## 2.8 Identity Agents

Any identity agents that support the Information Card technology are able to participate in the federation. Most public sector employees will use Microsoft CardSpace to control the flow of claims from AP's to RP's.

Web browsers and non-user centric (Information Card) federation technologies can participate in the federation , provided authoritative parties and relying parties provide these services, such as SAML 2.0 or WS-Federation.

# 3 Identity Management Architecture Design Patterns

This IDIM architecture enables the construction of a rich identity management eco-system using the three base components: authoritative party (AP), relying party (RP), and identity agent (IA). This eco-system allows identity information (or claims) to be securely passed so that at all times we know who is accessing a service and who the service is be about. We can construct models with multiple RP's and AP's to match the use cases involved in delivering public services.

Design patterns for representative use cases are presented below.

## 3.1 Use Case: Citizen Access to e-Health Portal

In this example we show a design pattern for a citizen accessing their Health record via an e-Health portal. We assume the citizen has already registered with the BCeID authoritative party and can login with their username and password (or smart card).

Step 1: The citizen accesses the E-Health portal with their web browser. The portal requests identity claims from the BCeID AP. The IA requests these claims from the BCeID security token server, authenticates, and receives the claims as a security token.

Step 2: The IA sends the claims (token) to the portal. The portal checks its access policy and grants access to the application.

Step 3: The portal sends a request to the IAL enterprise service bus with the claims attached. The IAL checks its access policy and allows the request.

Step 4: The IAL forwards the request (with the claims) to the Health back-end application for processing. The Health application finds the Health record for the patient identified in the claims.

Step 5: The Health record is returned to the IAL.

Step 6: The Health record is sent to the E-Health Portal for processing/display to the citizen.

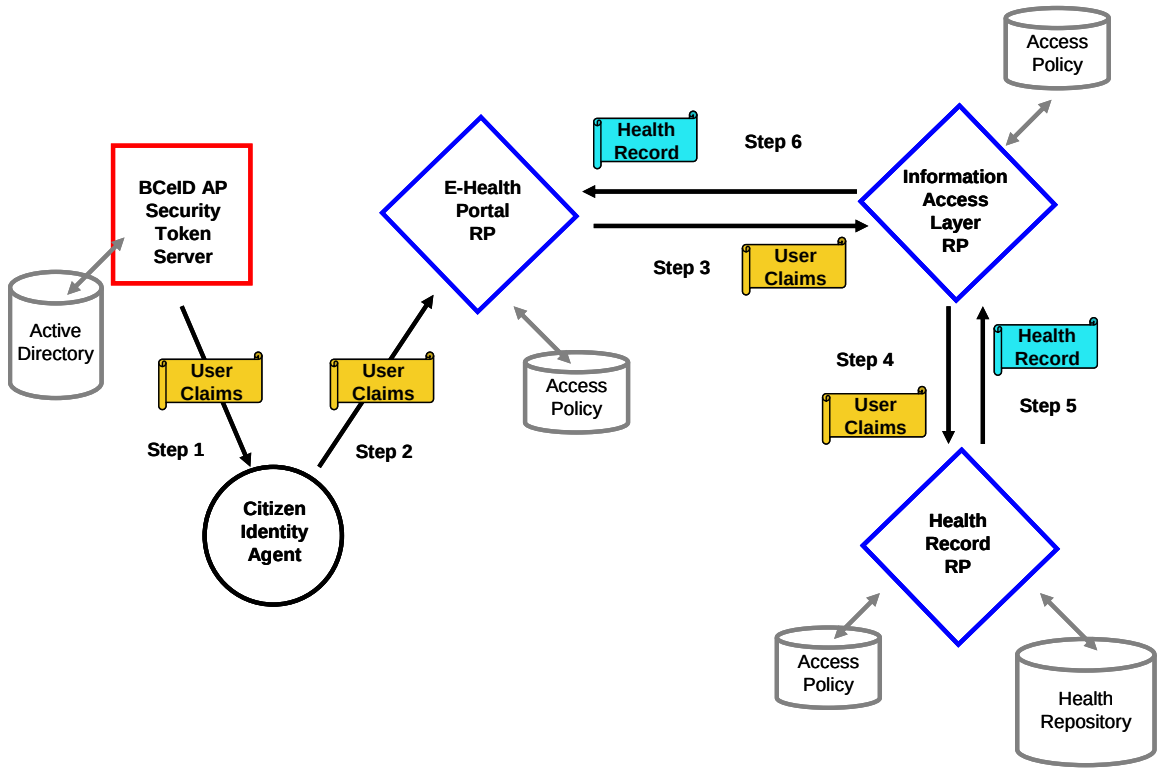



**Figure 6 Citizen Access to e-Health Portal**

## 3.2 Use Case: Social Worker Access to Case Management

In this use case we construct a moderately complex example involving a government employee social worker accessing the Case Management Application (CMA) using their normal workplace logon id and password. The Case Management application will need to send messages to the Information Access Layer (IAL) to get information about a subject from the Client Registry (CR).

Step 1: The social worker connects to the CMA RP. The CMA requests user claims to satisfy its policy that only social workers are allowed to access the application. The identity agent (IA) requests these claims from the Employee AP security token server. The token server authenticates the social worker using the desktop Kerberos session and provides the required claims (as a SAML token) back to the IA.

Step 2: The IA sends the claims to the CMA RP. The CMA compares the claims to its access policy and grants access.

Step 3: To lookup the details of person relevant to the case, the CMA sends a message to the IAL RP to query the client registry AP, along with the claims. The IAL compares the claims to its access policy and grants access.

Step 4: The IAL sends the query and the claims to the CR. The CR compares the claims about the social worker to its access policy and grants access. The Client Registry sends the client details as subject claims to the IAL.

Step 5: The IAL sends the subject claims to the CMA.

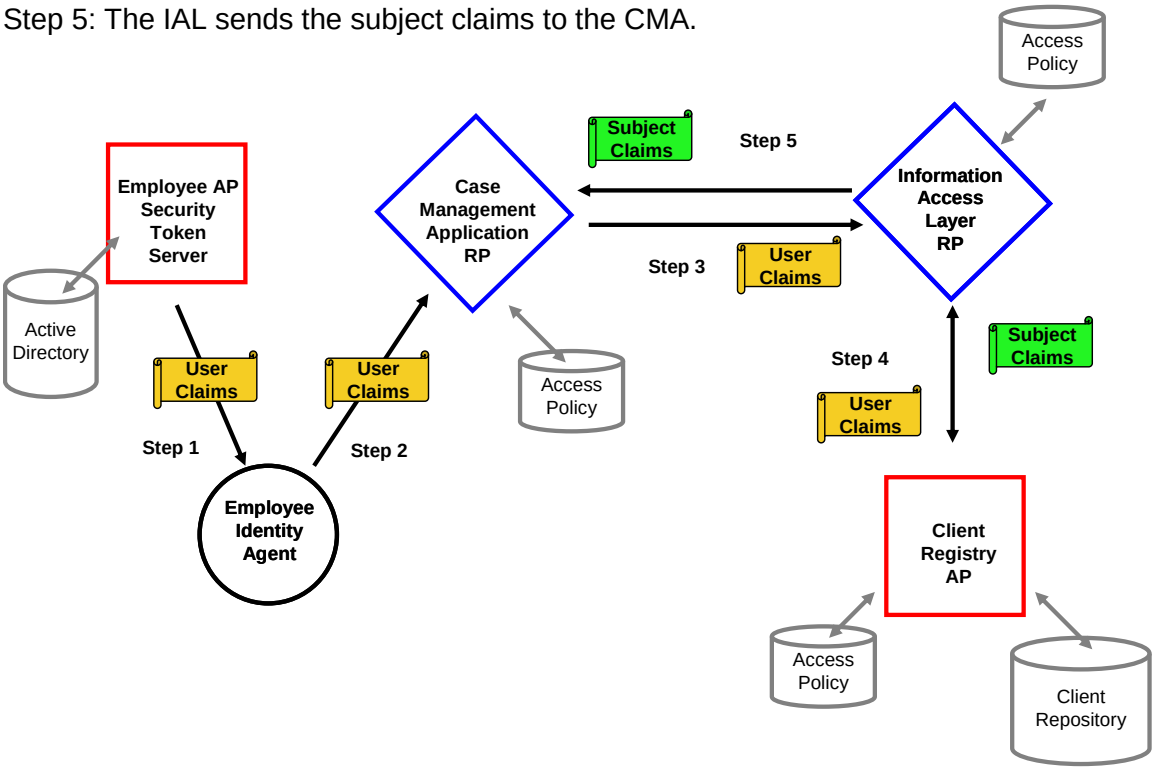



**Figure 7 Social Worker Access to Case Management**

## 3.3 Use Case: Custom Application Integration with BCeID

In this use case we show application integration with the registry and security token services of the BCeID authoritative party. A ministry employee uses the registry services to grant a BCeID user access to the custom application and the BCeID user accesses the application.

Step 1: The ministry employee connects to the administrative interface of the custom application RP. The IA requests claims from the Employee AP, authenticates the user with their desktop logon session, and receives the claims.

Step 2: The IA sends the user claims to the custom RP. The custom RP compares the claims to its access policy to ensure the user has administrator access.

Step 3: The ministry employee uses the "add user" function of the application RP. The RP sends a request to the registry interface of BCeID AP to find the subject claims for the BCeID user. The employee claims are attached to the request.

Step 4: The BCeID registry compares the employee claims to its access policy, grants access, and sends the subject claims of the BCeID user back to the custom application. The custom application updates the access policy to grant access .

Step 5: The BCeID user requests access to the custom application RP. The RP requests user claims from the user.

Step 6: The IA receives the claims from the user and sends the claims to the RP. The RP compares the claims to its access policy (recently updated by the government employee) and grants access.

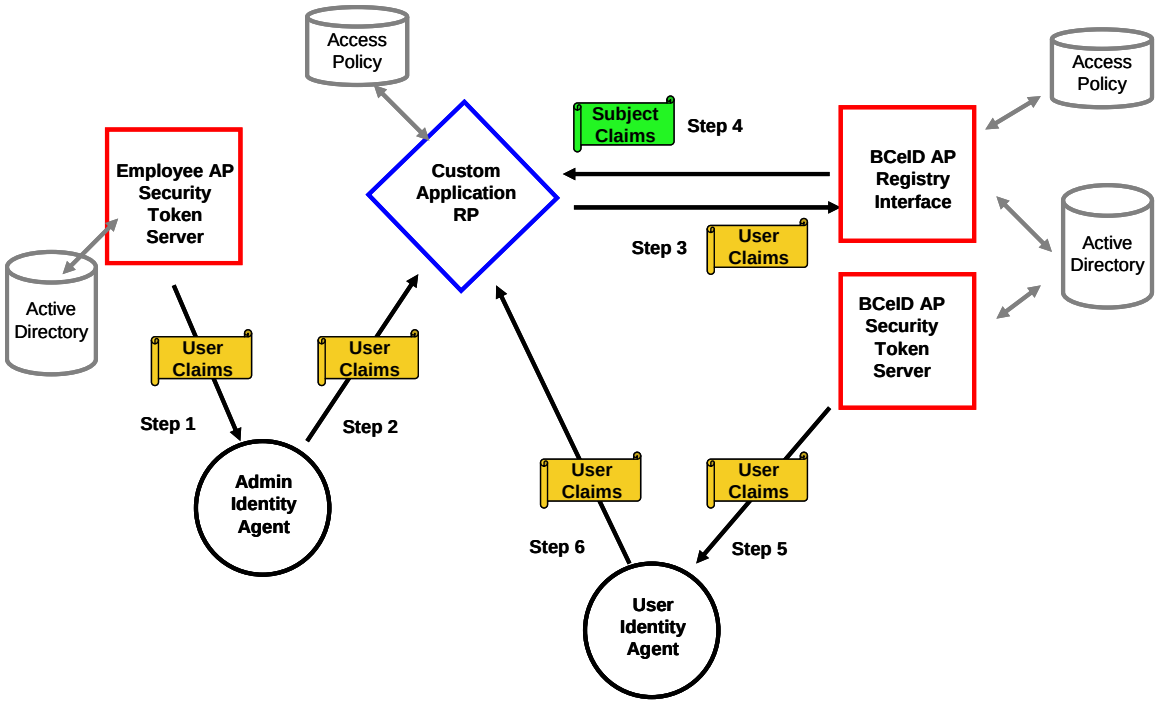



**Figure 8 Custom Application Integration with BCeID**

## 3.4 Use Case: Claims Transformation

In this example we show how authentication claims can be transformed into authorization claims. In this scenario the custom application RP is part of a domain with a shared role repository. A custom security token server transforms the authentication claims from the BCeID security token server into authorization claims. The IA then presents the authorization claims to a custom application to get access.

Step 1: User (IA) requests access to the custom application and receives a request for authorization claims. The IA requests authorization claims from the custom security token server and receives a request for user claims from the BCeID AP.

Step 2: The IA requests claims from the BCeID AP, authenticates the user, and receives the claims from the AP.

Step 3: The IA sends the user claims to the custom security token server. The server compares the user claims to the role repository.

Step 4: The custom security token server converts the user claims to authorization claims (using the role information) and sends the claims back to the IA.

Step 5: The IA sends the authorization claims to the custom application RP. The RP compares the authorization claims to its access policy and is granted access.

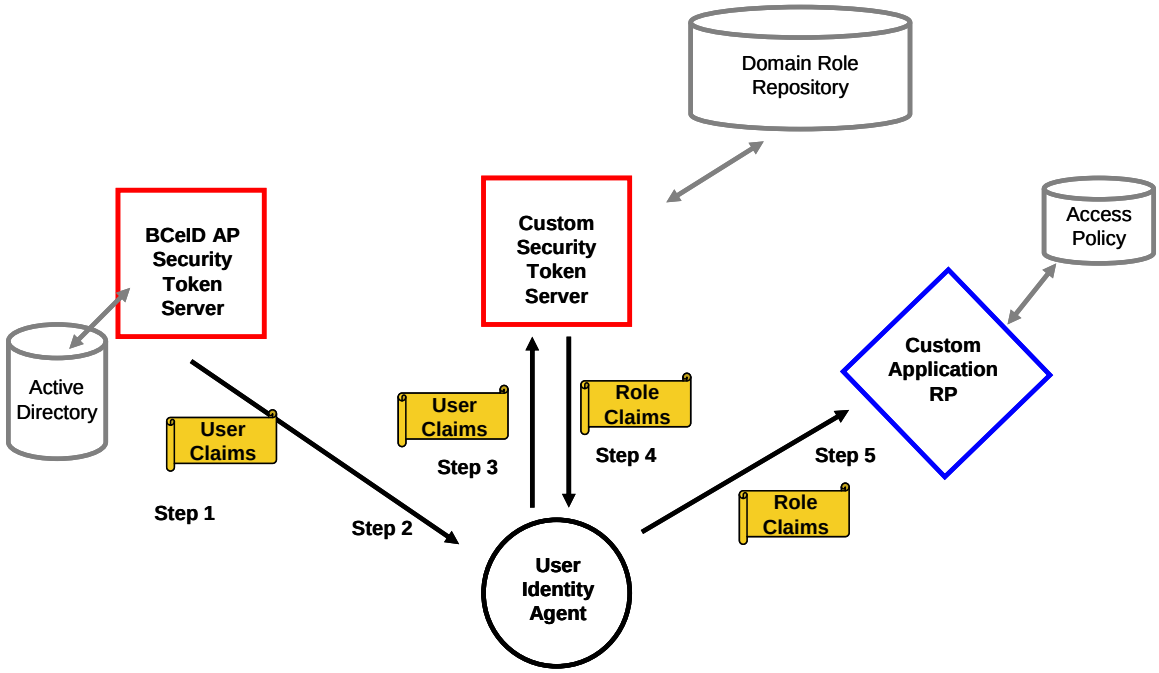



**Figure 9 Claims Transformation**