



British Columbia Broader Public Sector Identity Management Architecture Project Requirements Document

Author(s):	Paul Bryan Michael DeSandoli Sergio Fiszman Alan Harbitter Dick Hardt Stephen Skordinski
Creation Date:	March 19, 2007
Last Updated:	August 10, 2007
Version:	Draft 10.3

1 Introduction

This document contains the requirements for the British Columbia Identity Management Architecture, a key component in the Province’s drive to create a world-class system to provide “the right information, to the right people, at the right time.”

The primary deliverable of the project is to create an architecture that can be used in ongoing and future information technology projects undertaken by the Province of British Columbia and the Broader Public Sector (BPS). The goal of the architecture is to enable public servants, and eventually citizens, to easily and securely access any public sector information system required to perform a task.

This project does not deal with specific, detailed requirements of a particular organization; nor is it dealing with implementation issues. Instead it attempts to specify an architecture that will address a superset of original identity use cases describing the interaction between BPS systems and their users. The requirements in this document are therefore generic and do not detail specific Ministry or BPS names or processes.

The project team would like to acknowledge the help and involvement of the BPS of British Columbia. None of this work would have been possible without their support.

2 Lexicon

This section defines terms used in this document.

2.1 Access Control

The process by which an entity permits or denies access to a resource.

2.2 Access Control Rules

The rules used to effect access control.

2.3 Actor

An entity that can take action. Can be a principal, authoritative party or relying party.

2.4 Advertised Policies

Required claims, optional claims and terms & conditions (T&Cs) communicated by an authoritative party or a relying party as preconditions to the release of claims or access to a resource, respectively. For a relying party, advertised policies may also include authoritative parties from whom claims will be accepted.

2.5 Agent

An agent is an entity that has been authorized by another to act on the other's behalf. For example, a real estate agent represents a client in the negotiations of the sale of a home. Unlike a delegate, an agent does not generally assume responsibility or liability in place of the entity it represents.

2.6 Attribute

An attribute is a name/value pair. The name is a sufficiently unique identifier, which implies the type of attribute. The attribute type is used to define the syntax and semantics of the value. An attribute is a basic building block of claims.

2.7 Authentication

The process by which an entity's identity is determined to some accepted assurance level by another entity via the validation of claims about that entity's identity or by some other trusted mechanism.

2.8 Authoritative Party (AP)

An authoritative party is an entity whose authority to make claims is recognized by one or more relying parties. Claims made by recognized authoritative parties are used by relying parties to make access control decisions.

2.9 Authorization Policy

The policy by which an AP or relying party effects access control.

2.10 Claim

A claim is an attribute regarding a principal or transactional context. Claim types are unlimited, but are typically associated with: identification of principal, organization, user role and/or request context (network, device, location, connection type).

2.11 Delegate

A delegate is an individual who has been granted authority to act in another individual's stead. For example, a doctor going on vacation can delegate authority to another doctor to treat their patients. Unlike an agent, a delegate assumes certain responsibilities and liability for actions in place of the individual it represents.

2.12 Entity

An entity is a human person, a non-human legal entity (e.g. a company, a government), or a virtual artifact (e.g. a computer process or application).

2.13 Identity Agent

A piece of software used by a principal to invoke her identity interactions with APs and RPs.

2.14 Principal

The actor in an interaction that initiates the interaction – one who takes the deliberate action to initiate.

2.15 Relying Party (RP)

An RP is an entity that consumes claims to satisfy an authorization policy to grant a principal access to a resource.

2.16 Resource

A store of information or application needed by an actor.

2.17 Root Authority

A root authority is an entity that APs, RPs and IAs are pre-configured to initial trust. There may be multiple root authorities.

3 Requirements

3.1 Minimal Disclosure

No more than the minimal amount of information shall be required to satisfy a request.

3.2 Multiple and Alternative Claims

When a principal accesses a resource, the identity management solution must allow an RP to require multiple and alternative claims from a single or multiple APs to satisfy its authorization policy. This includes the ability to satisfy the policy with a fractional set (e.g., 3 out of 5 possible claims must be supplied and validated).

3.3 Dependant Claims

An AP may require one or more claims in order to issue a claim.

3.4 AP Discovery

An IA must be able to discover which AP(s) are considered authoritative by an RP for a given type of claim.

3.4b An RP must be able to discover which AP(s) are considered authoritative by a root authority for a given type of claim.

3.5 Claims based access may not uniquely identify user

The identity management solution must support claims provided to an RP that do not reveal the unique identity of a principal, unless such identification is a justifiable requirement for satisfying a request. For example, a claim that the principal is a university student requesting access to research may not require the specific identity of the student to allow access.

3.6 Claims based access may not identify issuer

The identity management solution must support claims provided to a RP that do not reveal the unique identity of an authoritative party, unless such identification is a justifiable requirement for satisfying a request. For example, an accredited school issues a claim about a student without identifying the name of the school.

3.7 Audit Traceable

The identity management system must be able to audit the “chain of authority” or “series of events” that occur during access attempts. The identity management system must support the ability to exclude or mask some parts of the transaction though the default is that a log will be captured. The logs must be tamper evident at minimum, with potential for tamper resistance in case of highly sensitive systems.

Note: We need the ability to audit claims issued and claims consumed, i.e., in an audit of the identity management system, an auditor should be able to trace claims through the transaction chain back to the purported APs. We also must be able to indicate we don't want an audit trail on certain transactions.

This requirement implies that APs should maintain logs of claims made, and RPs should maintain logs of claims received and transactional context. IAs should be able to maintain logs of transactions.

We also need an audit trail of changes to policies.

3.8 Directed Identity

A principal must be able to self-identify to an RP in a manner unique to that RP so that RPs cannot unnecessarily correlate activity between RPs.

3.9 Claim Integrity

The system must provide a mechanism to verify the data integrity of a claim.

3.10 Transaction Confidentiality

To ensure data confidentiality, all identity data may be transported with secured communications. It is expected that transactions with different levels of sensitivity will require associated levels of communications security.

3.11 Secure Claims

An AP must be able to prevent the disclosure of claims it makes to other than the intended recipient. That is, the AP must be able to provide a claim that is applicable/usable by certain parties only, i.e., areas of work that require secrecy where RP may need to parse the claim but none of the intermediaries including, possibly, the principal can do so.

3.12 AP knows RP

The AP may require the identity of the RP to issue a claim. For example, for audit and control reasons, an AP may be restricted to issuing the claim to certain RPs only or may need to know precisely which RPs have accessed the claim.

3.13 Secure storage of identity data and audit log

Identity data and audit logs must have the ability to be stored in such a manner that identity data is protected should the store be compromised. All identity data and audit log data must be tamper evident at minimum, with potential for tamper resistance in case of highly sensitive systems. When a system is decommissioned, all locally stored data must be scrubbed.

3.14 Access to identity data and audit data

Access to the identity data and audit data stored by any party must only be available to those that have a requirement to access the data.

3.15 Discoverable Claim Requirements – RP

The claims required by an RP to permit access and the requirements for presenting the claims should be discoverable prior to requesting access to a resource. This allows a principal to collect, in advance, the required claims and then present them when requesting access to a resource. This “claim requirement” request may itself be protected by access control.

3.16 Discoverable Claim Requirements – AP

The requirements for an AP to supply a claim should be discoverable prior to a request for the claim. This allows a principal to collect, in advance, the required claims to meet the requirements and then present them when requesting a claim. This “claim requirement” request may itself be protected by access control.

3.17 Resilient/High Availability

The identity management systems deployed must be available to supply claims and service requests with availability as high as or higher than the resources being protected. Availability includes performance/responsiveness.

3.18 Offline

For applications that are able to work in the offline mode, the identity management should support local claims processing. That is, users should be able to use the same kind of identity management mechanism whether they’re online or offline.

3.19 Principal can “authenticate” requester of claim

When a principal is requested to present claims to an RP, the RP system must support the ability for the principal to evaluate the authenticity of the RPs. Note that this might include more than one RP if a series of chained claim requests is necessary.

3.20 Principal can “authenticate” provider of claim

Before a principal is provided with one or more claims by an AP, the AP system must support the ability for the principal to evaluate the authenticity of the APs.

3.21 Conditions of Claim Release

The RP must be able to express to the principal the terms & conditions (indication of use) under which it is requesting claims so that principals can choose to release their claims under those conditions.

3.22 Terms & Conditions Bound

T&Cs of the release may be bound to the claims or resources released.

3.23 Security Gradient

The identity management solution must support a level of security appropriate for the RP and AP. For example, user-to-machine authentication may range from passwords to multi-factor, token-based and/or biometric authentication; or, the underlying network may range from unverified IP to client-side SSL certificates to private networks.

3.24 Authentication Strength Claims

The strength of principal authentication should be expressed as one or more claims, which the RP evaluates (presumably with other claims) when determining whether a principal satisfies the authorization policy to access a resource.

3.25 Trusted Device Claims

The trustworthiness of a device to manage a requested resource should be expressed as one or more claims, which the RP evaluates when determining whether a principal satisfies the authorization policy to access a resource.

3.26 Delegation Granularity

The identity management solution must allow a principal to delegate authority over accessible resources to a level of granularity that is reasonable and appropriate in the circumstances. In other words, delegation should not be a wholesale delegation of identity to another.

3.27 Agency Granularity

The identity management solution must allow a principal to grant an agent authority to represent them when accessing resources, to a level of granularity that is reasonable and appropriate in the circumstances. Like delegation, agency is not wholesale; it is relative to resources accessed.

3.28 Transparent & Opaque Policy

The identity management system must allow RPs to maintain sets of authorization requirements separate from those advertised, or even to not advertise any at all. “Requestors/claim presenters” must accept such policies to be applied by RPs and resolve, recover or gracefully fail in the event of associated authorization failures.

3.29 Claim Requirements Standardization

Claim requirements and T&Cs must be expressed in a standardized way to support interoperability between principals, APs and RPs.

3.30 Standard method of defining attributes

All interoperable components of the identity management system must adhere to a standardized method of defining and expressing attributes. Each attribute has a unique identifier and meaning and has a standard syntax.

3.31 Claim validation at authorization policy decision point

RPs must be able to acquire a valid claim at the policy decision point. For example, transactions can be long-running, requiring asynchronous communications, so the RP may need to ensure that access to the requested resource is still authorized at time of delivery.

3.32 Party Independence

An RP, AP or IA may join the identity management system without coordinating with any other party except perhaps a root authority.

3.33 Use Internet Infrastructure

Components of the identity management system can be deployed on the existing Internet infrastructure without requiring a dedicated network infrastructure.

3.34 Choice of IA

The principal may use different IAs for different transactions.

4 Desirable features

4.1 Digital Signature Service

It would be desirable if the identity management system provided a digital signature service (“digital seal”) for the principal, so that principals are able to make authenticated agreements that have data integrity.

4.2 RP Discovery

An IA and AP must be able to discover which RPs are authoritative for providing a given resource.