Government of Canada Directory Services Architecture

Presentation to the Architecture Framework Advisory Committee
November 4, 2013
## Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topics</th>
<th>Presenters</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00–9:15</td>
<td>Opening Remarks</td>
<td>Benoît Long, <em>Chair</em></td>
</tr>
<tr>
<td></td>
<td>Objective for Today’s Meeting</td>
<td>Wade Daley, <em>Vice-Chair</em></td>
</tr>
<tr>
<td>9:15–9:45</td>
<td>Directory Services Architecture</td>
<td>Gail Eagen, Director General</td>
</tr>
<tr>
<td></td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>9:45–10:00</td>
<td>Health Break</td>
<td></td>
</tr>
<tr>
<td>10:00–11:45</td>
<td>Discussion</td>
<td>Gail Eagen, Lead</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benoît Long, Moderator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>11:45–12:00</td>
<td>Closing Remarks</td>
<td>Chair</td>
</tr>
<tr>
<td></td>
<td>Next Meeting: December 2013 or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>January 2014 (early)</td>
<td></td>
</tr>
</tbody>
</table>
The Government of Canada (GC) does not properly manage the identity information of employees and consultants, resulting in:

- increased cost through duplication of directories and authentication mechanisms across all the departments;
- slow provisioning of users, which decreases productivity;
- unreliable de-provisioning of users, which increases security risk;
- inability to share enterprise identity attributes (such as security clearances) inhibits the sharing of information or access to buildings for meetings between GC departments and agencies;
- a prerequisite component that needs to be in place for Shared Services Canada (SSC) to enable enterprise IT service delivery;
- a prerequisite component to deliver an enterprise identity credential access management (ICAM) service; and
- directory services are not well understood, and the GC does not have an agreed upon lexicon, taxonomy or common terminology to describe directory services.

*N.B.: from Treasury Board Secretariat of Canada (TBS)*
Directory Services is Foundational

A directory is a strategic component of ICAM; however, the directory in itself is at the very heart of IT service delivery. Directory objects and artifacts include people, and credential attributes required for ICAM as well as many other objects and attributes required to operate an IT service.
Directory Service: The “Information Hub” of the IT Service

- **Users**
  - Accounts
  - Environment

- **Servers**
  - Management
  - Security

- **Clients**
  - Lockdown
  - Automation

- **Applications**
  - Configuration
  - Single sign-on
  - High Availability
  - Security

- **Email Servers**
  - Mailbox Information
  - Address Book

- **Network Devices**
  - Configuration
  - Quality of Service

- **Firewall Services**
  - Configuration
  - Security Policy

- **Directory**
  - Security
  - Stability
  - Manageability
  - Compliance

- **“Directory” Lookups**
  - White Pages
  - E-Commerce
Many Different Objects with Multiple Attributes

- Many different objects
- All aspects of the IT service platform
- Many attributes per object

- Different naming conventions for objects and attributes
- Different processes, policies
Directories:
Variety of Implementations/Complex/Mission Critical

- Different schema
- Different object naming conventions
- Different attribute naming conventions
- Different vendor technology
- Critical to ‘keep the lights on’ (KTLO) for general IT service delivery
- Complex legacy implementations
- Different processes, logistics and policies
GC Directory: Current State

No enterprise directory = No enterprise services

- No data centre (DC), workplace technology devices, ICAM and network infrastructure directory, etc.
- Most directories provide a departmental view.
- The Government Electronic Directory Service (GEDS) and the Pay Modernization initiative (PayMod) are exceptions.
- Distributed directories mostly by department multiple objects (attributes)
- Designed for departmental-based service

• Over 200 directories
• Mostly Microsoft Active Directory, with lightweight directory access protocol (LDAP), Oracle, Novell and X.500
• Different objects, elements, naming conventions, vendors and schema
• Different processes, policies and logistics
Enterprise Directory Service Approach:
Option 1 – Big Bang Approach
Enterprise Directory Service Approach: Option 2 – An Incremental Opportunity-based Approach

- **Phase 5**: Next Incremental Change
- **Phase 4**: Next Incremental Change
- **Phase 3**: Next Incremental Change (ICAM)
- **Phase 2**: More People, Attributes and Services (Next Incremental Change – GCNet)
- **Phase 1**: Small Subset of People, Attributes and Services (Email Transformation Initiative)

- **Depth of Data**: (Number of Users)
- **Breadth of Data**: (Number of Attributes Synchronized)
- **Function**: (Number of Services)
Questions – Engaging Discussion

1. Can or has an enterprise directory been done before across multiple platforms and/or across multiple organizations?

2. What IT standards could be applied to fulfill the enterprise directory and the directory synchronization services described in the preceding presentation?

3. Are you aware of a state-of-the-art enterprise directories data model (conceptual and logical)?

4. Are there any lessons learned or recommended strategies to apply in reconciling various data sources that contain conflicting information to essentially “clean up” the various source systems over time?
5. What technologies or best practices can be applied to solve the problem of identical name collisions and name confusion across a diverse enterprise organization such as the GC?

6. What are the primary advantages and disadvantages of maintaining continued vendor diversity in the area of enterprise directory services across multiple GC organizations?

7. Would you recommend a “big bang” or an incremental approach to the development of a GC enterprise directory service?
Annex
“A directory service is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects. A directory service is an important component of a NOS (Network Operating System). In the more complex cases [the] directory service is the central information repository for [the IT] Service Delivery Platform. For example, looking up "computers" using a directory service might yield a list of available computers and information for accessing them.”

The directory is the enabling technology that allows us to associate all of the objects we manage; the user is just one of many. It is not enough to know your identity and authenticate you at log on. Every time you access a resource on the network, that resource has to know your identity and be able to look up attributes and values associated with it. This means that all objects must exist in a common directory or in directories that trust each other.

“Identity management (IdM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.

Identity management systems, products, applications and platforms manage identifying and ancillary data about entities that include individuals, computer-related hardware and applications.


It covers issues such as how users are given an identity, the protection of that identity and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.).”
Objects fall into two broad categories: resources (e.g., printers) and security principles (user or computer accounts and groups).

A principal in computer security is an entity that can be authenticated by a computer system or network.

Principals can be individual people, computers, services, computational entities, such as processes and threads, or any group of such things. They need to be identified and authenticated before they can be assigned rights and privileges over resources in a network. A principal typically has an associated identifier (such as a security identifier) that allows it to be referenced for identification or assignment of properties and permissions.
One identity with many attributes linked to two to three credentials and many resources.

*N.B.: from TBS*
GC ICAM Identity Management*

Identity Management
- Background investigation
- On-boarding
- Authoritative attributes
- Lifecycle management of identity and attributes

New Digital Identity Lifecycle Management

Blackberry Enterprise

Telecom PBX

Official Languages Database

Network Access Databases (e.g. Active Directory)

Facilities Databases

Pay Databases

Contractor Databases

Departmental HR Databases

People Repositories

*N.B.: from TBS
Proposed Interim Solution for Email Transformation Initiative

• SSC wants to reduce the number of directories it operates.
  • Where directories are completely integrated into a vendor product (such as an Email Transformation Initiative (ETI) proprietary directory), these directories would be provisioned from a general-purpose SSC foundational directory.
  • It is acknowledged that SSC cannot reduce this number to one.

• Hence, the GC Enterprise Directory Service project:
  • has a short-term focus – only while the GC does not have a more comprehensive identity management solution in production.
    • If approved, this project will work proactively along with TBS (Chief Information Officer Branch) to ensure that GC ICAM can consume these services as it matures.
  • The GC ICAM directory synchronization service will support standard interfaces and can be used by any SSC partner or client application maintaining identity data.
    • For example, the ETI service can synchronize identity elements of its own proprietary directory with the SSC foundational directory service.
Enterprise Directory Relationships*

*N.B.: Burton Group
Current GC Enterprise Directory Environment

- Internal applications
- External Applications
- Internal applications

- Internal CAs
- PKI X.509 Certificates
- ICM / FINDS X.500 Directory (Employees)

- Windows Network Directories (Active Directories)

- No Enterprise Directory Service
- No Directory Synchronization

- New* GC Screening Identity Repository
- Partner Messaging Directories (Exchange)
- Partner Infrastructure Directories (Exchange)

- HR Directories (PeopleSoft, SAP)

- GEDS
Proposed GC Enterprise Directory Service

- **Internal Applications**
  - NEW GC Enterprise Directory (GC ICAM)
  - Windows Network Directories (Active Directories)
  - New GC Screening Identity Repository

- **External Applications**
  - ICM / FINDS X.500 Directory (Employees)
  - ETI Messaging Directory
  - Infrastructure Directory

- **Sync**
  - Account Info
  - Identity Adds, Deletes
  - Email Address, Other info
  - Phone Number

- **Internal CAs**
  - PKI X.509 Certificates

**This Project**

**Directory Synchronization Service**

- Identity Adds, Deletes
- Email Address
- Phone Number
Directory Synchronization and Automation

- Synchronizes existing application directories with an SSC enterprise-directory service and is maintained via central and standardized business processes
- Allows consuming services to enable automated provisioning and to have automated employee and contractor lifecycle management
  - Provides required data to application directories that need it
  - Enables automated provisioning and maintenance
  - Also enables automated de-provisioning of employees and contractors in support of proper identity lifecycle management across all SSC services
- **Critical for the SSC transformational agenda**
  - Allows the provider to have one view of end-user information across all of the SSC services provided to GC partner departments/agents and clients
Enterprise Directory Data Characteristics

• The plan for the GC enterprise directory contains the following data characteristics:

  • Data is from an authoritative source.

  • Data has been referenced and audited against third-party sources.
    • Third-party sources, such as the Regional Pay System (RPS) and Internal Credential Management (ICM), can be queried for the existence of an active employee record within a particular department to augment the existing identity lifecycle processes as an SSC value add.
    • For example, if an employee has retired or changed from one department to another on a deployment, he or she will no longer be paid by the previous department in RPS, hence providing a flag to departments that this employee no longer works there and should be properly de-provisioned.
    • An employee “data” level of assurance for each record is established.
Enterprise Directory Service Dimensions

• The enterprise directory service can be thought of as three dimensional, as:
  • the depth is the number of objects for which there is data;
  • the breadth is the number of attributes for each object; and
  • multiplying these gives us the total number of pieces of data being managed and audited.

• The last dimension is the number of directory services that we support to publish/expose the data.

• SSC is to expand the service to include all federal government users, while gradually introducing additional functions/access protocols.
Enterprise Directory Service Components

- The enterprise directory service must be more than a technology service.
- There must be a set of defined service interfaces to allow suppliers and clients to interact with the system.
- The directory must contain a set of well-understood and enforced directory policies.
- There must be directory procedures in order to implement and enforce policies.
- There must be strong governance to ensure a high value to the GC.
Business Benefits to Shared Services Canada

• Demonstrated business efficiency
  • *Reduced data administration effort by application specialists, with improved data integrity and accuracy*

• Reduced costs for SSC overall
  • *Minimal lag between initial data change by the data or attribute authority and reflection in application*

• Improved security posture based on a shared information architecture
  • *Automatic revocation of services helps achieve Management of Information Technology Security compliance.*
Enterprise Directory Services Framework

End Users

Directory Clients (SSC and GC-wide Applications)

Directory Access and Synchronization Service Consumers

Standardized Access (LDAP, XML, WS*, SAML, etc.)

Publishing, Distribution, Conversion

Directory Services

Reference, Extract, Transform, Normalize, Validate, Load

Audit and Reference Data

Department-specific Feeds

Beneficiaries
(Access and Credential Management Service Providers)

Enablers
(Digital Identity Lifecycle Management)

Content Providers
(Identity Data Authorities)