UBC Identity Management

Proof-of-Concept Report

V1.0a September 30, 2005

Jens Haeusser
Paul Zablosky
Sergiu Petrescu
Gerald Boersma

The Authors

Gerald Boersma *is a Consultant with Brighton Consulting*

Jens Haeusser *is Manager of the UBC IT Security Office*

Sergiu Petrescu *is a Principal with Brighton Consulting*

Paul Zablosky *is a Senior Technical Analyst with UBC IT*

Table of Contents

1 Executive Summary

Accomplishment of Objectives: Within the defined scope of the proof of concept and its terms of reference, all of the objectives for the exploration of concepts within the UBC landscape and the Sun identity management suite have been met. As with any study in an area of such broad scope, many issues for future exploration and progress were identified. These are classified and listed in the body of the report.

A Role for the Sun Java ES Identity Management Suite: While it is clear that in an institution with the internal diversity of UBC there is a need for a variety of different products and solutions – many have already been adopted and are integral to established processes – there is a significant and central role for the Sun Java ES product suite. It has been shown that the Sun products can interoperate with existing services and complement their functionality. It is expected that the products can be deployed to replace some functions, complement others, and provide new areas of functionality in the evolution of a unified identity management infrastructure at UBC.

Continuing Partnership with Sun: The established relationship with Sun Microsystems is productive and mutually beneficial. Sun should continue to act as a partner in UBC's implementation of its long term identity management strategy.

Long Term Architecture and Road Map: A long term architectural model for unified identity management at UBC needs to be created. Sufficient information and understanding now exists for this to be undertaken. The model will provide context and principles for all strategic initiatives for the evolution of identity management at UBC. In addition to the architecture definition, a road map is needed to specify the appropriate paths to realization of the architecture as an institutional service.

Central Identity Management Practice: There is a need for a centre of expertise, support, and operational services in identity management at UBC. This can be serviced by the establishment of an identity management practice within UBC IT. As well as supporting central identity management services operating on UBC IT platforms, the practice would provide leadership and consultation, as well as engaging in partnerships with other campus units.

Proposed Projects: There are projects which can be done now to advance identity management at UBC. Some of these are the first steps to the desired unified service and some address areas of immediate need and urgency. With careful planning, steps can be taken now to service critical needs without compromising long term directions and strategies.

Governance and Partnerships: Identity management is an institution-wide concern which goes far beyond the technology challenge. Responsibility for direction and policy should reside in a body that represents the interests of major stakeholders and users. Partnerships between campus units will be essential to our success. Also, there is a need for partnerships with other members of the higher education community for UBC to take its place in the world of inter-institutional identity management.

2 Assessment Summary

2.1 Project Initiation

An Identity and Access Management Proof of Concept (IDAM POC) has been completed jointly by the UBC IT Department (UBC IT) and the Sun Client Services team (Sun CS, between February 28 and June 22, 2005.

The project was initiated by the UBC IT Strategy team and intended to provide a "service proof"[1] by evaluating the value and feasibility of using the Sun JES Identity and Access technology stack, previously licensed by UBC IT, in conjunction with existing IT infrastructure, for the delivery of new and improved campus services.

A joint team from UBC IT and Sun CS resources has been established for the performance of the POC project:

Role	UBC IT	Sun CS
Sponsor	Richard Spencer	Tri Chiem
Project Manager	Jens Haeusser	
Engagement Manager		Nancy Campbell
Direct Contributors	Paul Zablosky CWL team myUBC team William Craven (SI) Gordon Chan (CA)	Gerald Boersma Dan Razzell Rick Zimbelman Sergiu Petrescu

A team from UBC Finance led by Chris Michaud provided a PeopleSoft test integration environment.

In addition, a wide range of IT staff, both from within UBC IT and from many other departments also participated in the POC, both as contributors and evaluators of the project. Multiple presentations, demonstrations and training sessions engaged a large cross-section of IT staff at UBC, and specific feedback on UBC's Identity Management needs was gathered from various key departments and units.

Sun Microsystems, as a partnership contribution, has provided the funding for the professional services team, access to Sun Support services and the loaner equipment.

2.2 Objectives and Scope

Sun's JES Identity Management suite has been proposed as potentially capable of meeting UBC's enterprise identity management needs. The proof of concept was designed to test the feasibility and value of using the JES IDAM technology in the effective delivery of UBC IT services for campus Identity, Access, and Policy Management

Specifically, the project has been structured to directly address the following objectives:

[1] This is a service-level proof, to be distinguished from a technology-level proof.

- Evaluate the JES stack's support for UBC's long term services strategy and our conceptual models for Identity and Access Management (IDAM) services
- Demonstrate the JES stack functionality for the delivery of IDAM services, primarily in the areas of Provisioning, Role Management, Workflow Management, Self-Service and Audit Reporting
- Explore the ability of the JES stack to provide customized services, and evaluate the effort required to integrate new applications
- Demonstrate integration and interoperability between the JES stack and representative key UBC systems and applications/services, including CWL, myUBC, PeopleSoft and Active Directory
- Estimate the resources required for a full, enterprise implementation of JES, including ongoing operational costs

The project has also been structured to facilitate the implicit objective of exploring of the broad needs for identity management at UBC, both centrally and within distributed departments and units. An additional topic of consideration is the ability of the JES suite to support federation with external entities.

Based on the initial scope definition, the project was not intended to provide a technology evaluation, an operational evaluation or a demonstration of the federation, auditor or other features of the JES suite, unless specified in the project statement of work. In addition since this is explicitly a proof of concept and not a pilot, no work product other than various documents and recorded demonstrations will survive the project.

2.3 Methods and Deliverables

The project has delivered the functional fit and usability assessment through multiple work methods, reflecting the project scope bounds and the UBC IT priorities:

- Demonstration of the Product Features
  The JES products are installed and configured as an integrated stack. The key product features are practically demonstrated to the UBC stakeholders, in their base, generic configuration.
  This method is mainly used for the key features with general applicability.
- Exploration of the UBC Landscape
  The existing UBC identity management landscape is explored through examination of previous studies, designs, and requirements documents; interviews with key stakeholders and departmental representatives; and review of existing identity management solutions and practices (e.g. CWL).
- Assessment of UBC Concepts and Practices
  The UBC landscape is assessed through the consolidation and itemizing of testable concepts. A synthesis of major concepts and practices is documented. Use cases are created.
- Demonstration of Customization
  The JES products are installed, configured and customized for the UBC POC

requirements. The key customizations are the interfaces to the external UBC systems/applications, such as PeopleSoft, Active Directory, Campus-wide Login, and the myUBC Portal. The customized services are practically demonstrated to the UBC stakeholders.
This method is mainly used for features critical and/or highly specific to UBC.

- Features Presentation
  The JES product features, potential capability and/or recommended use are presented during a demonstration session, through slides, to the UBC stakeholders or the core team.
  This method is used for non-key features (to the POC), of general interest.
- JES product - UBC Concept Review
  Key concepts and practices are reviewed with respect to product features and capabilities. Observations are documented for each relevant product.
- myUBC Portal Proving
  The myUBC portal is used as an example enterprise application to demonstrate JES-based authentication and single signon to the JES web interfaces.
- Dynamic Organization Assignment
  Multiple organization structures are created. Users are assigned to one or more nodes in these organizations through a dynamic process.
- Report References
  The JES services capability and/or recommended use are presented to the core team through a reference in the closure report.
  This method is used for features outside the scope of the project, but identified as capability of potential interest to the stakeholders

Key to Scope Documents:

SOW University of British Columbia Sun Microsystems Identity Management Proof of Concept Project

POV Sun Identity Management Proof of Concept Project Overview

Method	Features (Deliverables)	Scope Comments
Demo Product features	Authentication	SOW
	Authorization (coarse grained)	
	Identity (virtual) model	SOW
	Roles model	SOW
	Provisioning	SOW
	Self-Service	SOW
	Password Mgmt	SOW
	Distributed Admin	
	Audit Reporting	SOW
Explore UBC Landscape	Requirements Documents	SOW, POV
	Interview Reports	

	Design Documentation (CWL)	SOW, POV
Concepts Assessment	Consolidated Testable Concepts Listing	
	Distilled Concepts and Practices Document	
	Use Cases	SOW
Demo Customization	Active Sync interface of IDM with PeopleSoft-HRMS as an authoritative source	SOW
	Sync interface of IDM with Access Mgr, Active Directory, and Sun Portal as managed resources	SOW
	Coexistence of IDAM (JES stack) services with the IT-stack services	
Features Presentation	Workflow Mgmt	SOW
	Reconciliation	
	Policy Management	
Product/Concepts Review	Recorded Observation of Concept by Product	
myUBC Portal Proving	JES Authentication	SOW, POV
	Single Signon to JES Products via myUBC	SOW, POV
	Self service and delegated administration	POV
Dynamic Org Assignment	Multiple organizational views created	SOW
	Users assigned dynamically	
Report References	Proxy/Delegation	
	Federation	
	Identity Life-Cycle Mgmt	
	Multi-Factor Authentication	
	Privacy & Security of ID information	
	Fit with existing infrastructure and services	
	Technology strength and maturity	
	Standards Support	

2.4 Findings

2.4.1 Implementation Findings

At the closure of the project, a feasibility scorecard (High, Medium, Low) for the key objectives has been defined by the Sun team, with agreement from UBC IT:

Method	Features (Deliverables)	Conceptual Support	Stack Functionality (pre-built)	Customizability
Demo Product features	Authentication, SSO	H	H	H
	Authorization (coarse grained)	H	H	H
	Identity (virtual) model	H	H	H
	Roles model	H	H	variable
	Provisioning	H	H	H
	Self-Service	H	H	M-H
	Password Mgmt	H	H	M-H

	Distributed and Delegated Admin	H	H	H
	Audit Reporting	H	H	H
Demo Customization	Active Sync interface of IDM with PeopleSoft-HRMS as an authoritative source	H	H	H
	Sync interface of IDM with Access Mgr, Active Directory and Sun Portal, as managed resources	H	H	H
	Coexistence of IDAM (JES stack) services with IT-stack services	H	NA	function of integration
Features Presentation	Workflow Mgmt	H	H	H
	Reconciliation	H	H	M
	Policy Management	H	M-H	H
Report References	Proxy/Delegation	TBD	L	variable
	Federation	H Further validation required	Federation Mgr to be tested	TBD
	Identity Life-Cycle Mgmt	H	H	M
	Multi-Factor Authentication	H	H	M-H
	Privacy & Security of ID information	TBD Further validation required	M-H	M
	Fit with existing infrastructure and services	H Shibboleth support to be validated	H	NA
	Technology strength and maturity	TBD	NA	NA
	Standards Support	H	LDAP, SAML SPML XML	NA

In summary, the IDAM stack has been assessed to provide:

- A high level of support for the tested components of UBC's conceptual model for Identity and Access Management (IDAM) services
- A high level of pre-built IDAM functionality primarily in the areas of Provisioning, Identity and Role Management, Workflow Management, Self-Service and Audit Reporting
- A high level of customizability, through:
    - Configurable pre-built services, such as audit reporting
    - Customizable forms and workflows
    - Customizable synchronization Interfaces

- Application programming interfaces

Further evaluation is recommended to be done for areas which were not fully in scope for this project, such as federation, privacy and security of identity information, support for Internet2 Shibboleth, and the effectiveness of development, and operations for production services.

2.4.2 Services Fit

The following services were demonstrated to interoperate with the JES products:

- Campus-wide Login Provisioning:
  CWL integration was achieved through a shared database table. Accounts created in Identity Manager were reflected in the shared table, triggering the creation of corresponding accounts in the CWL service.
- PeopleSoft (HR) Provisioning:
  A standard adapter was used to retrieve information from the PeopleSoft resource and create an account in Identity Manager. The account was then updated through and Active Sync process.
- Active Directory Provisioning:
  Through Identity Manager, an account was created on an Active Directory resource. The account was used for login to a service, and then later updated by Identity Manager.
- myUBC Authentication:
  The myUBC portal was modified to authenticate using the Access Manager API. Channel access was controlled by Access Manager roles. Single signon to Identity Manager and Access Manager was enabled through a myUBC channel, demonstrating both self-service and delegated administration capabilities.
- Organization Structure Administration:
  Multiple views of simulated UBC organizations were set up in Identity Manager. Dynamic assignment of people to these organizations was demonstrated, using Identity Manager rules.

2.4.3 Open Issues – In Scope

Within the specific scope of the POC, there are no critical open issues.

2.4.4 Issues Arising

In the general domain of the capabilities and services demonstrated within the POC, the following additional features are considered important to be evaluated through follow-up activities:

- Integration with SunONE and JES email services
- Two-way integration with Campus-wide Login
- Name space synchronization with Campus-wide Login
- Updating of Campus-wide Login accounts
- Role provisioning to Campus-wide Login accounts

- Access Manager policy-based authorization for myUBC channels
- Attribute-based dynamic organization assignment
- Automated end-to-end provisioning – e.g. PeopleSoft to Active Directory
- Support for login to commercial applications software – e.g. PeopleSoft

The following generic issues were explicitly outside of the POC scope, and remain to be evaluated:

- Current software version characteristics
- Version compatibility with products from other vendors
- Robustness
- Ease of installation for production
- Ease of upgrading
- Scalability
- Development environment management issues
- Operational management issues
- System administration management issues
- Operational independence and interdependence of products
- System level security, resistance to corruption and mass disclosure
- Continuous availability characteristics
- Demonstrated federation capability
- Operational maturity of products
- Custom adapter development – e.g. for UBC SIS
- Platform sizing for production
- Specification of an institutional identity repository

The following issues were outside of the POC scope, and are specific to the UBC environment. They are listed here because they arose during the POC study and are worthy of further investigation.

- Comprehensiveness and utility of the Identity Manager API's
- A central contact information resource
- Single logout
- Identity key capability
- Mutable login names
- Shibboleth federation
- Multiple personas and role sets

2.5 Conclusions

2.5.1 Role for JES Identity Management Suite at UBC

The JES Identity Management suite addresses key areas of UBC's critical identity management service requirements, and could be used as a core component of UBC's overall identity and access management implementation.

2.5.2 Further Study

There are areas where further investigation is required. These are outlined under Issues Arising (section 2.4.4) and reflected in Recommendations (section 2.6).

2.5.3 Long Term and Near Term Initiatives

There are a number of actions which UBC can take to progress to a unified institutional identity management infrastructure. Some of these are long term, and some of them address specific challenges in the near term.

2.6 Recommendations

Given our observations and conclusions, we recommend the following actions:

1. Establish a long term high-level architecture for institutional identity management.
    - Establish principles based on models and standards, independent of technology.
    - Establish rules for conformance, so that identity management initiatives can demonstrate compliance.
    - Outline a roadmap for evolving identity management services and practices within the architecture.
    - Conduct a planning study to determine the implementation nature of an institutional identity repository most appropriate to UBC's needs.
        - Investigate the contents and semantics of primary identity information holdings within the university, focusing on Systems of Record including SIS, PS-HR, CWL, Tracc-II, Mercury and others.
        - Develop a comprehensive set of use cases where cross-holding attributes are involved across multiple Systems of Record.
        - Assess potential implementation models for the institution-wide resource, focusing on practical and operational issues.
        - Consider forming an operational merge team to support the synchronization of identities and attributes across multiple Systems of Record.
        - Recommend a model for an institutional repository, supported by a high-level implementation plan.
        - Specify any derived resources required to support the model, including a definition of the "directory information tree".

2. Proceed toward the implementation of the JES technology products in production services to address key areas by the following steps:
    - Define an initial services portfolio and an evolution roadmap.
    - Define a services-oriented target architecture for identity and access management.
    - Identify lead opportunities and lead users for the services.
    - Identify key partnerships within UBC and facilitate interaction between identity providers, as well as between identity providers and identity consumers.
    - Create a UBC governance body to oversee the evolution of identity management within the university, and to foster federation partnerships with other institutions.
3. Ensure progress to identity and access management production services, through additional assessments and practice implementation.
    - Conduct a set of pilot projects to extend the assessment of identity and access management services, focusing on:
        - Federation: Liberty Alliance and Shibboleth, investigating federation technology appropriate to partnerships and service providers
        - Privacy and security of identity information, including regulatory compliance
        - Technology performance and operational profiling
        - Development effectiveness benchmarking
        - Operational conformance
    - Build an identity and access management practice, adopting and incorporating best practices from Sun.
    - Build an initial service technology platform.
    - Conduct service-targeted pilot projects to address particular areas of need and urgency.
    - Continuously develop the identity and access management practice through evaluation and adoption of lessons learned from other academic implementations of JES-based IDAM.

2.7 Opportunities for Action

Based on our investigations into the UBC identity management landscape and our conversations with multiple stakeholders, both internal to UBC IT and throughout various other departments and units, we have identified various short and longer term opportunities for enhanced services.

2.7.1 Target Internal Services

The following internal IT services are identified as potential candidates for integration with JES IDAM:

- Role Management and Distributed Administration for CWL accounts
  The implementation of Identity Manager and integration with CWL would provide a composite CWL+IDM service for the campus. This composite service would provide value in rapidly addressing known identity management challenges surrounding:
  - Role Management
  - Distributed Administration
  - Provisioning synchronization with authoritative sources such as SIS and PS-HRMS
- Central Campus Directory Service
  The implementation of a centralized, web-based, user-updatable contact information service, synchronized with various identity providers and consumers would provide a large benefit for UBC Faculty, Staff and Students in streamlining and simplifying the process of providing and updating contact information.
- JES Messaging integration with the IDAM services.
  The implementation of Identity and Access Manager, in conjunction with the migration to JES Messaging and Calendar would provide a strong, coherent set of core services. In addition, the potential for the JES Unified Address Book to meet the needs of a Central Campus Directory service should be explored.
- TRACC-II enhancement/replacement.
  The implementation of Identity Manager and integration with TRACC-II would allow the transfer and enhancements of the provisioning features from TRACC-II to IDM, while TRACC-II would continue to provide the inventory management and billing support for its current services.

2.7.2 Target External Services

In the larger context of campus requirements and initiatives, the following IDAM services are identified as early opportunities:

- Improved provisioning to departmental account management services from various Systems of Record
- Extended Authentication and Authorization capabilities for departmental account management services beyond what is now provided by CWL
- PeopleSoft/HR Common Address Book, required for the PeopleSoft Phase II rollout of eProfile and ePay in February of 2006
- Business Operations “Throw Away the Key” initiative, providing identity management based secure access to buildings, offices and labs
- Shibboleth Federation within the Canadian Higher Education community, targeting integrated wireless access at CANHEIT 2006
- Federation with the BC Health Authorities to streamline the integration of third year medical resident students in September, 2006.

2.8 Action Proposals

Based on our recommendations and the identified opportunities, we propose that UBC IT undertake the following actions over a 6-9 month time frame:

1. Develop a central identity management practice, enabling UBC IT to provide leadership, service, assistance, and support to UBC units.
2. Approve, plan, and initiate a coordinated set of projects to:
    a. Define plans for the long term future of identity management at UBC
    b. Resolve issues arising from the proof of concept study, but not within its scope
    c. Take the first steps to developing a coherent identity management infrastructure for the institution
    d. Address areas of greatest need, deficiency, and immediacy

    There are varying degrees of interdependence between the proposed projects. Some can be done as independent undertakings, whereas others must be coordinated so that the results of one can be used as the foundation for another. These are issues to be resolved during the preparation of project proposals, overviews, and charters. Proposed projects are listed in section 6 to inform decisions regarding selection, priority, timing, and resource assignment.
3. Work toward the establishment of a governance body to give direction on policy and institution-wide issues. Foster the formation of partnerships within the University to enable the creation of a unified identity resource, and outside of the University to enable federated access to externally provided services.

The first two initiatives are complementary and mutually sustaining. UBC IT must develop an identity management practice to implement a wide range of identity and access management services, but it must also undertake pilot projects to extend its understanding of the issues and technologies involved. The last initiative provides institutional context and furthers the buy-in and support of the other efforts.

The proposed projects should also build on and strengthen the partnership between UBC IT and Sun in order to deliver a comprehensive set of identity and access management services for the UBC community. A wide range of resources from within UBC IT will need to participate in the projects, along with staff from the broader UBC community. Sun resources will be instrumental in providing training and knowledge transfer to help establish the UBC identity management practice, as well as providing hands-on installation assistance and support in the implementation of an enterprise identity management infrastructure at UBC.

Further details surrounding practice development, proposed projects for the initial pilot, and governance and partnerships can be found in section 6.

3 Overview

The purpose of the proof of concept study was to examine both the existing identity management situation at UBC and specific Sun products that might be employed in solutions at our institution.

To clarify our approach we sought a definition for the word "proof" as it is used in the phrase "proof of concept".

> **Proof** Determination of the quality of something by testing – *The American Heritage® Dictionary of the English Language, Fourth Edition*

Our approach, therefore, was to identify and test important concepts in both the UBC environment and the candidate products. Our objective was to identify correspondences between concepts derived from UBC requirements, and concepts expressed and supported by candidate products from Sun.

3.1.1 Foundation Documents

We took our direction from two documents:

1. Sun Identity Management Proof of Concept Project Overview
   [File: Sun ID Pilot overview a]
2. University of British Columbia Sun Microsystems Proof of Concept Project
   [File: UBC IdM POC 05-02-24]

3.1.2 Other References

Other reference sources are cited within the relevant sections.

3.2 Survey of the UBC Landscape

Foundation document 2 requires that the capabilities of the Sun products be demonstrated within the UBC environment. To determine the nature of that environment, we did a survey of the existing knowledge and current practices at UBC. This included:

- A review of the comprehensive and detailed material prepared by Richard Spencer
- Interviews and meetings with departmental representatives
- A review of major identity sources in UBC's Systems of Record, derived repositories, and secondary sources of identity (accounts)
- Examination of current practices in UBC departments

Our research was extended and informed by interactions at JA-SIG[2] and Internet2 workshops – these provided perspective on how UBC's challenges are aligned with those of other higher education institutions.

[2] JA-SIG is the "Java Architectures Special Interest Group. Its purpose is "to provide education and research in the applied use of open technology architectures and systems in higher education". See http://www.ja-sig.org.

3.3 Exploration of Sun Products

Our study focused on the three products which comprise the identity management core of Sun's Java Enterprise System collection:[3]

1. *Identity Manger:* A comprehensive provisioning tool, formerly known as Lighthouse from Waveset
2. *Access Manager:* Sun's authentication, authorization, and WebISO product, formerly known as Identity Server
3. *Directory Server:* Sun's LDAP server product. Directory Server handles information storage for Access Manager

To explore the concepts expressed and supported by these products, specific technical experiments were performed. These experiments can be categorized into three groups.

1. *Out of the box:* Initial tests and demonstrations were performed with the products installed as delivered by Sun, with no local customization or integration. This served to demonstrate "out of the box" capabilities.
2. *Integrated with UBC Services:* Small projects were created to integrate the products with test implementations of prominent UBC services. The target services were:
    - UBC Human Resources PeopleSoft service
    - ITServices Active Directory service
    - Campus-wide Login
    - The myUBC portal
3. *Organization Modeling:* A model was created, representing multiple independent organizational hierarchies across a diverse set of UBC people – staff, students, and faculty.

3.4 Useful Definitions of Common Terms

The following terms are useful in describing the UBC identity management problem space. The definitions are taken from NSF Middleware Initiative documents and presentations.

- *System of Record:* An authoritative source for information in an institution. Often resides in an ERP service and database. UBC examples include the SIS and the HR PeopleSoft service.
- *Provision:* Push identity and access management information out to systems and services (applications) as required. Contrast with *Relay*.
- *Relay*: Make access control / authorization information available to services and resources at run time.
- *Reflect*: Track changes to institutional data from changes in Systems of Record and other identity management components.
- *Join*: Establish and maintain person identity across Systems of Record.

[3] See section *5.3 Products* for a more detailed description of the Sun product set.

3.5 The Identity Management Marketplace

While Sun has had a strong directory product for many years (Directory Server, originally acquired from Netscape in 1997), it has only recently become a strong player in the identity management marketplace with the acquisition of Waveset in December of 2003. Before the acquisition, Gartner had just added Sun to the Magic Quadrant for Extranet Access Management, 2H03, as a niche player. After the acquisition, Gartner moved Sun to the axis between niche player and challenger in the Magic Quadrant for Extranet Access Management, 1H04. Most recently, Gartner has moved Sun solidly into the challenger quadrant, with no identified leaders on the Magic Quadrant for Extranet Access Management, 2H05.

3.5.1 Other Identity Management Vendors

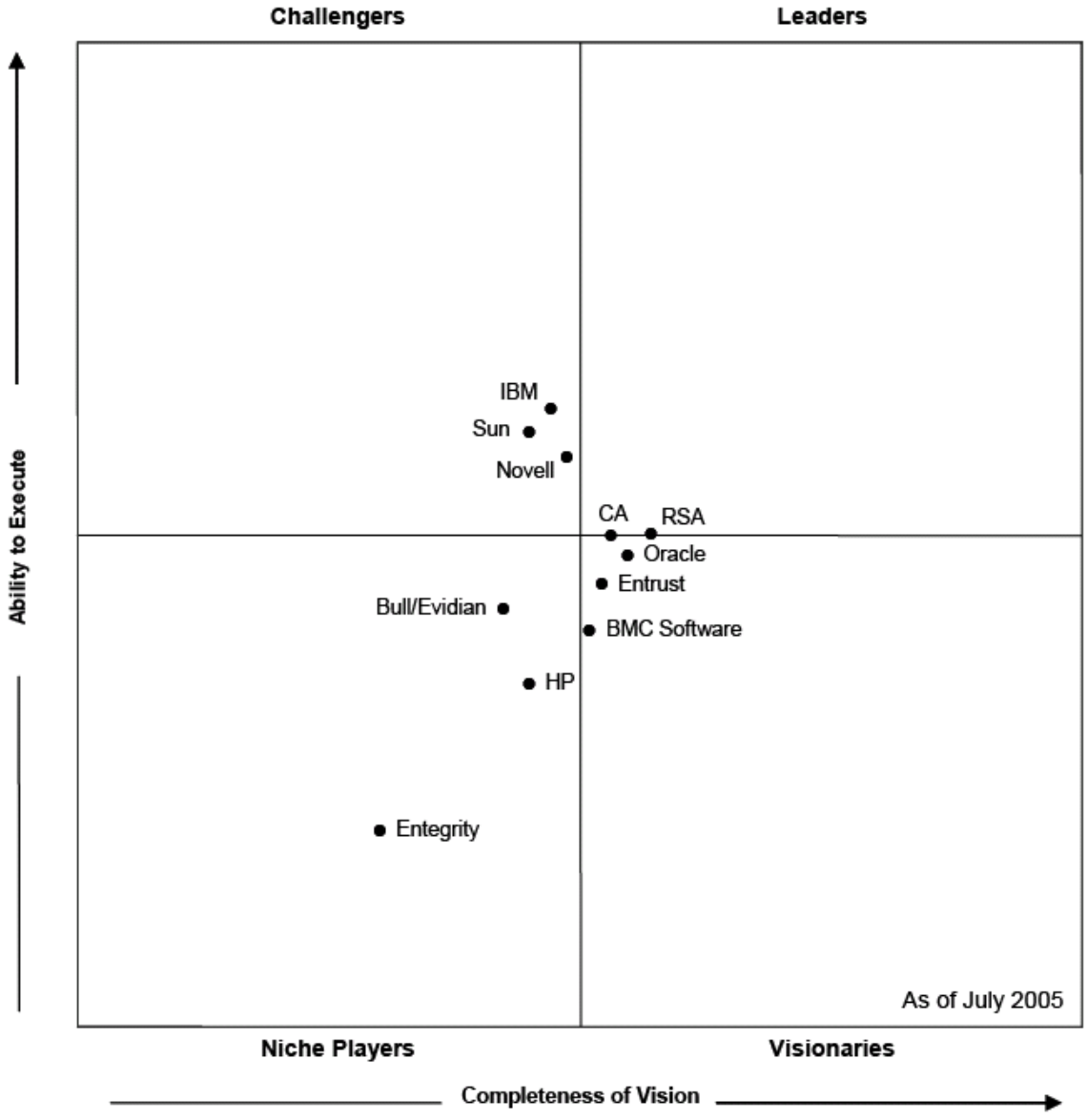
The identity management marketplace has recently undergone a round of consolidation. Previous leaders in the space have been purchased by large companies who are integrating those offerings as part of larger software suites. In particular, previous leaders Waveset, Netegrity and Oblix were purchases by Sun, Computer Associates, and Oracle respectively. This has lead to an changing marketplace where Gartner has identified no current leaders in its Magic Quadrant for Extranet Access Management. IBM, Sun and Novell are all currently placed strongly in the challengers' quadrant, while CA and RSA are straddling the visionary and leader axis.

3.5.2 Sun Identity Management in Higher Education

While Waveset had very little penetration into higher education with their Lighthouse product (the precursor to Sun Identity Manager), Sun has made a strong commitment to deploying Identity Manager within the higher education sector, both as part of their complete Sun Java Enterprise System and as part of the Sun Java Identity Management Suite. There are few current higher education deployments of Identity Manager, but Sun is actively working on deployments with a number of sites including Western Michigan University and the University of Victoria. With the initial round of deployments well underway, UBC would not be a bleeding-edge adopter of Sun's Identity Management suite, but would still benefit from Sun's willingness to partner with early adopters.

Sun has recently been a more active player in the identity management space within the higher education community. They have openly expressed a strong commitment to providing identity management solutions to the higher education community, and seem to have identified this sector as a strong growth area for Sun. Sun representatives have participated in a variety of higher-education identity management conferences and workshops including JASIG and the Internet2 NSF Middleware Initiative. Sun is also starting a discussion forum and mailing list for higher education users of its Identity Management suite.

3.5.3 Gartner Magic Quadrant for Extranet Access Management, 2H05



Key to Vendor Names:

BMC = BMC Software
CA = Computer Associates
Entegrity = Entegrity Solutions
RSA = RSA Security
Sun = Sun Microsystems

Source: Gartner (July 2005)

4 The UBC Landscape

This section gives details of the exploration of the UBC landscape.

4.1 Reference Sources from Richard Spencer and Bruce Jolliffe

Our primary sources for UBC requirements were the following documents authored by Richard Spencer:

- A. Identity and Access Management at UBC – General Objectives DRAFT FOR DISCUSSION v1.3 *March 3, 2005*
- B. Creating a UBC Identity and Adding Identity Attributes DRAFT FOR DISCUSSION v1.0 *March 3, 2005*
- C. Identity Management Strategy – DRAFT FOR DISCUSSION – v1.03 *February 8, 2005*

We also reviewed the design and architecture behind UBC's current institutional authentication and authorization service – Campus-wide Login (CWL).

- D. Campus-wide Login Design and Specification Version 3.00 *Bruce Jolliffe, June 30, 2004*

4.2 Derived References

Our first step was to consolidate the information from the three sources into a single document, identifying and highlighting all the testable cases. Our result was a list of 133 concepts.

- E. Identity Management Proof of Concept – Unified List of Testable Concepts Version 1.01 *March 16, 2005*

We synthesized a list of principal ideas to use in evaluating potential solutions. The ideas were derived from the source documents and our observation of embedded practices at UBC.

- F. Identity Management Proof of Concept – Concepts Practices and Products *April 27, 2005*

We also created a number of high level use cases to give focus our experiments.

- G. Identity Managent Proof of Concept – Use Cases *April 27, 2005*

4.3 Interviews and Meetings with Campus Stakeholders

Interviews were held with members of campus stakeholder departments:

Department or Group	Respondents
SNAG	Dave Hermon (Land and Building Services), Robert Bruce (Education), Jason Carter (Arts), Pat Darragh (Sauder), Michael Sanderson (CS), Luca Filipozzi

	(ECE), Steve Atwal (Student Systems)
Human Resources/Finance	Niran Subramaniam, Chris Michaud, Shawn Chaput
Library	Darrell Bailie, Anna Lee, Joerg Messer
Student Systems	Audrey Lindsay, Paul Hill
Forestry	Larry Carson
Office of Research Services	Brent Sauder
Agricultural Sciences	Cyprien Lomas
Peter Wall Institute for Advanced Studies	Markus Pickartz
Office of Learning Technologies	Michelle Lamberson, Novak Rogic
Business Operations	Ken Leighton, Bruce Lovell, Kevin Chow
ICICS	Luca Filipozzi, Michael Sanderson

4.4 Identity Sources

The following is a list of UBC's major identity resources, many of which include the concept of a user account with login credentials. The list includes major identity sources, derived resources, and secondary sources we are aware of. The primary authoritative Systems of Record are flagged.

Identity Source	**Concept of Account with Credentials**	**SoR**
HR PeopleSoft Service	Yes, for admin access and user access	Yes
SIS	Yes, also uses CWL for authentication	Yes
UBC Directory	No	
CWL	Yes	Yes
Tracc II	Yes	
Interchange Mail	Yes	
Exchange (Active Directory)	Yes	
myUBC	Profile only, uses CWL for authentication	
UBC Library	Yes, can use CWL	

4.5 Ancillary Information Sources

During the proof of concept project, we had the opportunity to gain an understanding of what other members of the higher education are doing to address identity management needs.

4.5.1 JA-SIG uPortal Conference

The need for comprehensive identity management infrastructure is being acknowledged by those members of JA-SIG who are developing enterprise-level portal services. Discussions in "Birds of a Feather" (BOF) meetings and presentations revealed that UBC is not unique in its need for multiple organizational views, multiple personas, and mutable login names.

Contact was made with Stuart Sim from Sun, who is active in JES Identity Management deployment in North America and the UK. He has promised us a list of sites (email).

4.5.2 Internet2 NMI Campus Architecture Middleware Planning Workshops

In the last week of June, Paul Zablosky participated in the Internet2 Middleware Planning workshops held in Denver. From this experience, we have gained:

- Standard nomenclature and diagrammatic approaches for modeling of our identity management problem space
- An understanding what other sites are doing, including their level of interest in Sun solutions
- Knowledge of other sites' approaches to identity repositories
- A better understanding of international federation issues

The program included presentations from vendors. The representative from Sun mentioned that there were 24 higher education sites, 9 of which should be available as references. We have requested a list.

4.5.3 University of Victoria Visit and Training

In the first week of July, Paul Zablosky attended a five-day technical course on the Identity Manager product. This contributed to:

- A clearer understanding of Identity Manager capabilities
- Better understanding of what is required to support and maintain an Identity Manger service

There was also the opportunity to exchange information on key issues with some of the technical members of University of Victoria's Nova project.

4.5.4 CANHEIT

In the last week of June, Jens Haeusser attended CANHEIT, the Canadian Higher Education IT Conference, in Montreal. This provided an opportunity to explore the identity management landscape within other universities in Canada, both by attending presentations on identity management given by McGill, Dalhousie, Calgary, and Saskatchewan, as well as participating in a hands on session on installing and configuring Shibboleth. The presentation slides from CANHEIT are available at http://canheit2005.campus.mcgill.ca/sessions.html . In addition, Jens chaired a Birds-of-a-Feather session on Identity Management where a wide range of different approaches within the higher education community in Canada were discussed. This lead to Jens establishing a mailing list where Canadian Universities can further discuss both the high-

level technical and the operational issues surrounding identity management in higher education in Canada.

It is interesting to note that identity management was a topic of much discussion at CANHEIT. Many Canadian universities are either about to start, in the middle of, or just completing substantial identity management projects within their own institutions. There was also a high degree of interest in exploring Shibboleth as the method of federating identities between higher education sites in Canada. In particular, many universities have agreed to install Shibboleth and enable federated wireless authentication for the next CANHEIT conference, taking place at Dalhousie in June, 2006.

4.6 Major UBC Concepts and the Sun Suite

In preparation for the proof of concept study, we created a list of the major concepts observable in the existing UBC landscape.[4] With some of these concepts we were able to identify a clear correspondence within the Sun products. With others it was not possible to determine if they can be fully realized within the Sun suite, given the limitations of our study.

In the following sections, we list each concept, and describe our observations of how well it is addressed by the Sun products.

4.6.1 Multiple Organizational Views

From an identity management standpoint, UBC is a diverse organization with multiple intersecting and non-intersecting hierarchies. A person may simultaneously occupy positions in any or all of the formal organizational structures. It is possible for a person to be a student, a staff member, a faculty member and an alumnus; all at the same time. One may also be a member of a loosely affiliated set, such as parent, prospect, visiting scholar, or institute member. A person on the staff may belong to more than one department. There is no useful single hierarchy that includes everyone. For this reason, it is necessary for the organizational model to be able to represent many different views, each with its own member set, but all based on the same identifiable individuals. A person's identity may comprise many affiliations, but the person should only be represented once.

POC Observations: Identity Manager can represent multiple non-intersecting hierarchical structures. A person's identity can be associated with one or more nodes in one or more hierarchies. The model appears to be sufficiently flexible to represent the existing structures and relationships at UBC. Our main purpose in these representations is to model the responsibility and authority relationships for identity administration. Access Manager does not support the same flexibility of representation.

4.6.2 Authorization and Roles

A primary goal of and identity management services is to handle authorization decisions. These decisions may be based on combinations of identity attributes and role membership. Users may have one or more roles. Associated with roles are rules and

[4] See reference F: Concepts Practices and Products.

policies, which can be used to limit and extend access to services. Every role must be managed to ensure that it is assigned to only those users entitled to it, and removed from those who are no longer eligible.

POC Observations: Identity Manager supports the notion of named roles or groups to which users can be assigned. Roles are commonly associated with "resources", i.e. managed accounts on other services, so that the membership in a role results in the creation of an account on another service – this is the described purpose of roles in the Identity Manager documentation. Along with the assignment of an account, a role can determine the value of attributes in the managed account, including roles as defined in the managed service. For example, the assignment of a role within Identity Manager can result in the assignment of a role in CWL or Access Manager. Within Identity Manager, a role is always associated with a node in the organization structure which determines its visibility for assignment.

4.6.3 Universality Within and Federation Without

All members of the university as well as all those with an affiliation with the university are candidates for inclusion in the identity management service. Outside of UBC, federation with other identity services at other institutions will enable certification and access privileges for UBC's members. Federation between institutions of higher education requires compatibility with standardized shared attribution sets.

POC Observations: Access Manager supports Liberty Alliance Federation. There is currently no support for the Shibboleth-style federation being adopted by some Canadian institutions. Federation was not formally investigated or demonstrated – our report is based on product documentation. This is a topic for further investigation.

4.6.4 Self Service and Global Immediacy

Wherever possible, interactions with the identity management service should be of a "self service" nature. This includes all aspects of provisioning and updating. Any step requiring actions by an administrator should be considered for refactoring with self-service alternatives. Any approval steps required in workflow should be deferrable if policy allows. Any transactions should be realized immediately in their full global effect. There should be no discernable propagation delays, or production cycle latency. For example, if I alter my home mailing address through the SIS, the effect should be immediately recognized for mailings from the HR system.

POC Observations: Actions taken within Identity Manager have immediate effect on all resources, subject only to approval steps defined by workflow. Synchronization takes place at defined polling intervals (Active Sync), or at scheduled times (Reconciliation).

4.6.5 Decentralized, Distributed, and Delegated Administration

For administrative tasks that cannot be handled through end-user self-service, it should be possible to spread authority and responsibility across the various UBC units, reflecting the multiple organizational views:

- ***Decentralized:*** Responsibility need not be handled centrally; responsibilities can be handed off other units.
- ***Distributed:*** Authority can be passed on to a number of different actors.

- ***Delegated:*** Authority can be passed down through a hierarchy.

A very important area of decentralized function is the ability to create and manage roles. Administrators are authorized to create roles and assign them in a particular segment of the organization, usually through descending levels of hierarchy.

POC Observations: Identity Manager supports a sophisticated model for fine-grained delegation of administration tasks, particularly role assignment..

4.6.6 Interface Symmetry

Anything a user or administrator can do through the user interfaces to the IDAM should be able to be done by an application or service through standard APIs. The reverse should also be true.

POC Observations: Access Manager has sophisticated API's providing access to most of its functionality. These were exercised, in part, during myUBC integration. Identity Manager supports its own internal programming environment and scripting language, and does not provide Java API access to its internal functionality. It does, however, support SPML access as well as the ability to call methods within external Java objects. Identity Manager's APIs were not exercised during the proof of concept. Our observations are based on Sun product documentation and interviews with Sun's Identity Manager course instructor.

4.6.7 Distributed Identity Repositories

A user's identity is the sum of all the information in all the identity repositories. This includes all the information stored in the mandated repositories such as the HR and SIS resources, as well as the contact information resource and the all "domain controller" components such as CWL, and Active Directory.

POC Observations: The notion of identity information being distributed across multiple repositories is fundamental to Identity Manager. It is realized through a sophisticated provisioning capability, as well as the ability to update attributes from authoritative to managed instances.

4.6.8 Central Contact Information Resource

A primary deliverable for identity management at UBC is a contact information repository. This will appear as a directory of all the identity service members, containing postal and geographical addresses, telephone numbers, email addresses, and other electronic contact information. Entries will be flagged to indicate use semantics, such as "home address", "work telephone number", etc. Authorized applications will have retrieval and update access to the entries. A central interface will provide self-service maintenance access to the members. The central interface will also be accessible from authorized core services such as the SIS, HR, Library, and institutional portal (myUBC).

POC Observations: A contact information repository can be organized as a directory. Directory Server is an obvious choice of platform for this service. Using Identity Manager, it should be possible to populate the repository with contact information from the SIS and HR services once suitable adapters are created. Updating, reconciling, and synchronizing might also be accomplished with Identity Manager, but this will depend on

the complexity of requirements. This topic was not deeply explored during the proof of concept. Our observations are based on our experiments with Access Manager, and the use of Directory Server elsewhere within UBC IT. This service would be a good candidate for a pilot project.

4.6.9 Privacy and Security

There will be fine-grained access control for applications which reference the identity repositories, especially those that contain personal information such as resides in the contact information resource. For example, an application may be allowed to retrieve the "home address" for a designated set of users – e.g. "registered students" – but it may not be allowed to reference email addresses or telephone numbers.

POC Observations: Privacy and security concerns are addressed with two different mechanisms: the first is the capability to define and enforce access policy; the second is the capability to audit all access to identity repositories, down to the attribute level if required. Identity Manager allows management of access policy based on role assignment or specific to individual users. Identity Manager also supports audit of changes to identity repositories, down to the attribute level if necessary. The topic of system-level security – i.e. resistance to penetration or corruption through snooping or spoofing – was not formally explored, since we used open protocols (e.g. HTTP) in our investigations.

4.6.10 Single Signon and Single Logout

Single Signon: Once a user has authenticated through a central authentication service, access should be enabled to all authorized services without further authentication steps by the user. Services may be local or remote, central, or decentralized. Single signon sessions must expire after a settable interval. Services may need to inquire how long it has been since authentication took place.

Single Logout: A user should be able to cleanly terminate all authorized active sessions with a single action.

POC Observations: Access Manager supports single signon for web services. Single logout was not addressed within the scope of the proof of concept. It is a topic for further exploration.

4.6.11 Coexistence

UBC already possesses a number of authoritative identity repositories such as central student records and human resources databases, as well as authentication and authorization services such as Campus-wide Login and Active Directory. It is important that future identity management solutions interoperate with this existing infrastructure and practice. Applications now using Active Directory or CWL may continue to do so. Development of new identity management solutions must take the direction of harmonizing, synchronizing, integrating, and building upon the existing services.

POC Observations: Much of the work done in the proof of concept exercises was aimed at demonstrating interoperability and the potential for co-existence of current solutions with new capabilities. None of our results indicate a need for replacement of existing working solutions.

4.6.12 Identity Keys

Identity repositories are referenced through attributes called "identity keys" in CWL terminology. Examples are Student Number and Employee number. An identity key is the identifier that a core application uses to specify the record for a particular individual. A person may have any number of identity keys associated with their record.

POC Observations: As delivered, Identity Manager keeps very little information about the user, assuming (like CWL) that most of the data will be maintained in authoritative repositories. The schema for the Identity Manager user object should be able to be extended to include attributes for the identity keys maintained by CWL. This was not formally addressed within the scope of the proof of concept. It is a topic for further exploration.

4.6.13 Mutable Login Names

A login name is a handle used to identify a user to the authentication service. It is the "ID" part of the "ID and password" authenticator that the user types during the authentication process. No application needs to know the value of the login name except for trivial display or reporting purposes. No application should preserve the value of a login name or employ it as a key. No application may rely on a user using the same name at subsequent authentications; a user may change the value of their login name without affecting their access to any application.

POC Observations: All Identity Manager attributes are mutable. There is a special process for changing *accountid* – the value normally used for login name – but the value is not normally exposed for user modification. The Access Manager attribute for *accountid* cannot be changed through the existing interfaces. This was not formally addressed within the scope of the POC. It is a topic for further exploration.

4.6.14 Login Keys

Associated with each login name is an immutable attribute known as the login key. Applications may use this value as a key to store user profile information. Its value will remain constant as long as the login exists in the user's identity.

POC Observations: Our experiments were limited to the basic schemas that Identity Manager and Access Manager support. These do not include an immutable key at either the identity level or the login level. It should be possible to extend the schemas to include such keys Assignment of key values would also be a problem to be solved locally. This was not formally addressed within the scope of the POC. It is a topic for further exploration.

4.6.15 Multiple Personas per Identity

A user's identity account may have several *personas*[5] associated with it. Each persona comprises a login name, a unique login key, and credential set. In effect, the user can

[5] In a larger sense, our use of the term *persona* is intended to be consistent with the Sxip network implementation, as well as Dave Kearn's assertion that your identity is the sum of all your personas.

have several login names, but only one identity account. A user may, for example, create a unique persona for use with a particularly sensitive application.

POC Observations: The concept of multiple personas is not expressed in any of the JES products. Access Manager does allow multiple aliases for an account ID, but there is no support for separate 'logins' with different credentials with the same identity, for use with the same service. It should be possible to extend the Identity Manger schema to include multiple login names and login keys. It is likely that we could support the concept between Identity Manager and Campus-wide Login, but it is unclear whether we can usefully support the concept with Access Manager. It is important to weigh the value of personas without associated role subsets (discussed in the next section). This is a topic for further exploration.

4.6.16 Roles Associated with Personas

A user's roles may be associated with specific personas, so that particular roles are active when a particular login name is used for authentication. Authenticating with a given persona causes a role set to come into effect. This is the mechanism that users may employ to limit their role set during access to particular services. Assignment of roles to personas is a self-service activity performed by the user through an account management interface.

POC Observations: Roles may be associated with persons or groups, but there is nothing in the JES products that supports the assertion of a particular set of roles for a particular session, based on how the user logs in. It should be possible to extend the Identity Manger schema to include multiple login names and login keys, but associating these with roles while maintaining Identity Manager's strong role administration capability would require substantial development work. It is likely that we could support the concept between Identity Manager and Campus-wide Login, but it is unclear whether we can usefully support the concept with Access Manager. More design and experimentation will be required to determine if we can usefully support the notion of multiple personas completely within the Sun products. We must be careful not to extend Identity Manger's schema and role model beyond its original intent. This is a topic for further exploration.

4.6.17 Independence of JES Components

While it is important that the JES components interoperate smoothly and seamlessly in an enterprise-level identity management solution, it is also important that the individual components be able to run standalone or in various combinations in a variety of environments if they are to be deployed by UBC's departments. Loose coupling is essential. JES components should not depend on the use of any particular container. Tomcat is widely used at UBC and the ability to run reliably and robustly under Tomcat would contribute to the adoption of JES at UBC.

POC Observations: The JES components all run standalone, with no apparent inappropriate bindings. Identity Manager runs well in the Tomcat container. This, in fact, was the container recommended by the instructor of the Identity Manager training course. We did not have the opportunity to experiment with Access Manager running under Tomcat.

4.6.18 Operational Maturity of JES Components

We need to be able to assess the maturity and reliability of JES releases to determine when and how to install them or phase them in to a running enterprise implementation. Installability, configurability, patching practices, and ability to perform clean back-outs are all part of such an assessment. Ideally, we can phase in new releases with minimal risk and zero user-visible impact, using zero-design processes.

POC Observations: Our limited test platform gave us no opportunity to assess the operational maturity of the Sun products. This topic was clearly outside of the scope of the proof of concept, and is only included here because it appeared in the reference document.

4.6.19 Scalability and Continuous Availability

UBC targets continuous availability for all enterprise-level services. This means that all hardware and software components exhibit full redundancy with clean failover on failures. Continuous availability means that there are no single points of failure, and there are no reasons for scheduled outages. Solutions should also exhibit zero-design scalability – capacity can be expanded by simply adding hardware and/or instances of the service. Changes or upgrades are designed for run-time compatibility so that they can be introduced instance-by-instance with no user-visible outages or service interruptions.

POC Observations: We have been told that it is possible to run multiple instances of Identity Manager with a shared or clustered database. Experiments in this area were beyond the scope of our study. To assure ourselves that we can create a service that will scale up for all types of activity – continuous reconciliation of attribute values across all resources through Identity Manager Active Sync comes to mind – we will need to investigate through a formal pilot study.

4.7 Major UBC Problem Areas

We considered current practices and needs, and identified major problem areas.

4.7.1 Identity Fragmentation

Identity fragmentation occurs when more than one System of Record can create a “person record”. At UBC there are two Systems of Record (HR and SIS) which can create authoritative institutional person records, as well as many systems which independently create accounts and store identity-associated attributes such as contact information (addresses and telephone numbers). The challenge of bringing these distributed fragments together to form a consolidated identity is called the *Join* problem. The join problem is easy to address if there is a dependable and unique common attribute shared between the Systems of Record. This is lacking at UBC.

4.7.2 Centralized Contact Information

Among the information most fragmented across the UBC systems is contact data: postal addresses, location addresses, email addresses, and telephone numbers. These are maintained independently in the major Systems of Record, and in many other services as well. There is an electronic directory for faculty and staff, but it shares no keys with the other Systems of Record. Here the *Join* problem is extreme.

If a person's contact information changes, all these systems must be updated independently. There are few mechanisms for ensuring consistency across the Systems of Record or derived copies of the information. This is known as the *Reflect* problem – ensuring that changes made to information in Systems of Record are *reflected* in all places where the data is viewed or retrieved.

In an ideal solution, people would see their contact data as information shared between themselves and the institution. They would be able to update that information for specific purposes – "this is the place to send my marks" or "this is the place to send my Library notifications". The administrative departments would see the information as part of their mandated data holdings within the Systems of Record. To achieve such a solution, we must address both the *Join* and the *Reflect* problems.

4.7.3 Departmental Access Control – Authentication and Authorization

Academic departments need to identify students and staff for the purpose of authorizing the use of resources. Student computer labs are a good example. A faculty needs to know that a student is registered in a particular course or program to grant access to lab facilities. In practice, this means retrieving up-to-date registration information from the SIS (*Reflect)*, and creating lab account with credentials for the student. This is called *Provisioning.* It is the process of pushing out identity and credential information to account management services so that they can perform the tasks of authentication and authorization.

Computer labs are not the only facilities where this type of solution applies. Electronically-managed building access is another example.[6]

4.7.4 Delegated Responsibility to Appropriate Areas of Authority

UBC's institution-wide authentication and authorization service – the Campus-wide Login – is currently administered centrally within the UBC IT department. This includes the creation and assignment of roles – named groups of users to which privileges are granted. This is inappropriate, since the authority to assign roles rests with service owners and service providers, and should not be the responsibility of UBC IT.

There are two problems to be solved here. One involves *Provisioning* and *Reflection* – for example, pushing out CWL role membership to students who have the right attributes in the SIS, and keeping roles up to date as the attributes change. The other is distribution of authority to departmental administrators, so that they can create roles and manage role membership on behalf of the applications they support.

4.7.5 Federation

Even if we solve the problems of identity fragmentation, there is a limit to how far we can proceed with integration. Once that limit is reached, we must resort to *federation*, the linking of identities administered in different domains. It is unlikely that we will need to support federation within UBC – full integration across the institution should be achievable. But when members of UBC require access to resources at other institutions,

[6] See the "Throw Away the Key" initiative mentioned in section 2.7.2.

their situation is much simplified if UBC can act as a guarantor of their identity through a pre-established fabric of trust with the other institutions.

There are several potential partners that have expressed an interest in pursuing Federation with UBC. At the national level, the discussion has centered around Shibboleth, particularity for shared wireless authentication between universities. Many Canadian universities have endeavoured to provide Federated authentication back to their home institutions from the wireless network at Dalhousie during the next CANHEIT conference in June, 2006. It looks as if CANHEIT will be the coordinating body for inter-institutional Federation within the higher education community in Canada.

At the provincial level, there has been a high degree of interest in identity management within BCNet. There is an active Identity Management working group chaired by Lionel Tolan from SFU which is quickly ramping up to discuss identity management issues both within and between BCNet institutions. As at the national level, Shibboleth looks to be the Federation technology of choice. The working group is currently organizing a one day identity management conference to be held in Vancouver in September or October of 2005.

There have also been a number of non-university partners who have expressed an interest in Federation with UBC. In particular, the various Health Authorities within BC have expressed a keen interest in some kind of Federation, potentially using Liberty-Alliance as the Federation technology. There is a strong desire to have some form of Federation in place in time for the 3rd year medical residents to enter the Health Authorities in the fall of 2006.

In addition to the Health Authorities, other organizations such as BC Campus have also mentioned the possibility of Federation with UBC.

Federation issues are further discussed under Proposed Action Details – *Federation Partnerships* in section 6.1.2.3.

4.7.6 The Main Challenge – an Identity Repository for UBC

As the requirement for uniform, consistent, and ubiquitous identity management grows within institutions of higher education, the need for a central repository of identity information becomes more apparent. In some respects a monolithic, centralized, single repository appears to be the needed solution, but the flexibility requirements of multiple stakeholders favour a distributed approach.

If we consider UBC's three main sources of identity information, we find that each is authoritative in a particular domain:

Service	**Authoritative for**
Human Resources	Faculty and Staff
Student Information System	Students
Campus-wide Login	Others

Closer examination reveals that while the HR and SIS repositories are each responsible for a particular population, neither is absolute as an authority. At particular times of the

year, the SIS may have more up-to-date information on faculty members than HR, for example. There is also the problem that there is no dependable matching attribute between the two services. A person may appear in both, but there may be no unambiguous linking of the records. Campus-wide Login *does* have a set of dependable attributes for matching to the other two repositories – the identity keys – but there is no guarantee of uniqueness in the CWL: a person may have separate accounts for employee and student affiliations.[7]

Coming back to the problem of unification, we are faced with two choices: do we try to bring all identity information together in one place, making *that* our institutional repository, or do we create a virtual repository with links to the Systems of Record where information is originally stored. In our POC investigations we have come to appreciate the theoretical advantage of the virtual approach – information is only stored in one place, and is fetched as needed. In discussions with other sites, however, we haven't encountered any who have made this choice. A derived repository stored on an LDAP server is the common approach.

There is no purely technical solution to the problem. A cooperative partnership between all of the major repository holders will be necessary if UBC is to achieve unification and consistency of its identity information. Governance of the undertaking will need to be managed by a high-level coordinating body.

[7] This is likely, in fact, because the self-service interface for creating CWL identities does not provide an easy mechanism for unifying a user's "student number account" with their "employee number" account.

5 Summary Report

The POC consists of three demonstrated activities:

- Integration between Java ES IDAM stack components.
- IDAM pre-built services.
- Integration with UBC systems.

This report describes what has been demonstrated, identifies any discovered issues, and discusses any required capabilities not explicitly demonstrated as part of the POC.

5.1 Feasibility Scorecard

The following table is reproduced from the feasibility scorecard from section 2.4.1 that details the implementation findings for the POC, and also maps each item to the corresponding items in the proof matrix (section 5.9).

The proof matrix is a set of concept and feature statements expressed at the start of the POC that identifies the working scope of the POC. Refer to section 5.9 for the proof matrix, which includes the mapping of proof matrix items to product features and POC activities.

Method	Features (Deliverables)	Conceptual Support	Stack Functionality (pre-built)	Customizability	Proof Matrix Items
Demo Product features	Authentication, SSO	H	H	H	2, 6, 7
	Authorization (coarse grained)	H	H	H	3, 4, 5, 12, 13, 25, 31, 32, 34, 35, 39
	Identity (virtual) model	H	H	H	1, 22, 23, 33, 38, 41
	Roles model	H	H	variable	4, 11, 12, 13, 18, 24, 31, 32, 33, 34
	Provisioning	H	H	H	6, 10, 19, 20
	Self-Service	H	H	M-H	27
	Password Mgmt	H	H	M-H	12, 16, 25
	Distributed and Delegated Admin	H	H	H	9, 28, 33, 37
	Audit Reporting	H	H	H	13, 30, 31, 32, 34
Demo Customization	Active Sync interface of IDM with PeopleSoft-HRMS as an authoritative source	H	H	H	17, 21, 22, 23, 26, 45, 46, 52
	Sync interface of IDM with Access Mgr, Active Directory and Sun Portal, as managed resources	H	H	H	17, 23, 24, 26, 38, 45, 46, 47, 51

	Coexistence of IDAM (JES stack) services with IT-stack services	H	NA	function of integration	45, 46
Features Presentation	Workflow Mgmt	H	H	H	19, 20, 40, 49
	Reconciliation	H	H	M	22, 23
	Policy Management	H	M-H	H	12, 13, 25, 32, 39
Report References	Proxy/Delegation	TBD	L	variable	5, 8, 29, 36
	Federation	H Further validation required	Federation Mgr to be tested	TBD	14, 15, 42, 56, 57
	Identity Life-Cycle Mgmt	H	H	M	49
	Multi-Factor Authentication	H	H	M-H	2
	Privacy & Security of ID information	TBD Further validation required	M-H	M	13, 30, 32, 54, 55
	Fit with existing infrastructure and services	H Shibboleth support to be validated	H	NA	45, 46, 47
	Technology strength and maturity	TBD	NA	NA	
	Standards Support	H	LDAP, SAML SPML XML	NA	14, 15

5.2 References

The following are supporting documents delivered as part of the POC. These provide more detail of what was covered off in the demonstrations and implementation details.

- Proof Matrix. Identifies concepts and features proven as part of the POC.
- Integrated IDAM Java ES Product Capabilities Demonstration. Demonstrates capabilities of and integration between components of the Sun Java ES IDAM product suite (Identity Manager, Access Manager, Directory Server, Portal Server). This demonstrates the “out-of-the-box” capabilities in context of the UBC objectives.
- UBC JAVA ES IDAM Integration. Demonstrates integration between components in the UBC environment (PeopleSoft, Campus-Wide Login, Active Directory, and myUBC) and elaborates key capabilities. This demonstrates capabilities that were implemented and tested in context of the UBC objectives.

- Demonstration Scripts. All demonstrations are captured as animated AVI files with voice-over explanations.

5.3 Products

The products evaluated within the POC are part of the Sun Java ES Identity and Access Management (IDAM) product suite, specifically Identity Manager, Access Manager, Directory Server, and Portal Server.

5.3.1 Identity Manager

Identity Manager connects to applications within the enterprise using adapters, allowing Identity Manager to provision users into these applications (i.e. PeopleSoft, SAP, LDAP, Oracle, etc.) as well as into other Java ES components (i.e. Access Manager, Directory Server, etc.).

This allows Identity Manager to provide a central repository of user identity across the enterprise, along with services to manage users within the repository. Identity Manager also provides features that provide a high degree of customizability of the product including forms and workflow (such as the provisioning workflow).

5.3.2 Access Manager

Access Manager provides authentication and authorization services that provide capabilities for Single Sign-On (SSO) and Federated Identity.

5.3.3 Directory Server

Directory Server is an LDAPv3 compliant directory that provides LDAP-enabled services.

5.3.4 Portal Server

Portal Server provides portal capabilities including self-registration, channel content management, and personalization.

5.4 Integration

The POC demonstrates technology integration between Java ES IDAM components (Identity Manager, Access Manager, Directory Server, and Portal Server) and with sample UBC systems (Campus-Wide Login, Active Directory, PeopleSoft, and myUBC Portal).

5.4.1 JAVA ES IDAM Components

The demonstration of integrated JAVA ES IDAM components shows how the product components provide unified services.

Identity Manager provides services for identity management (such as identity discovery and synchronization, provisioning, password / profile / role management, delegated administration, self-service, provisioning workflow, and reporting).

Access Manager provides services for access management (such as authorization, authentication, policy management, single-sign on, audit, and federation).

Directory Server provides services of an LDAP-based enterprise directory.

Portal Server provides portal capabilities (portlets, self-registration, and personalization).

Identity Manager is integrated with Access Manager in two ways:

1. A resource adapter allows Identity Manager to provision and manage identities, provide password and role management capabilities into Access Manager.
2. A web/J2EE policy agent intercepts authentication requests to Identity Manager and authenticates with Access Manager. It also intercepts requests for web pages (via URLs) and authorizes against Access Manager policy.

Access Manager stores all user and policy information in the Directory Server (it does not have another data-store of its own). The user entries are stored in standard LDAP schema, where the entries to be managed by Access Manager are marked with special object class tags. This allows the Directory Schema to be used as a directory integration point within the enterprise.

Portal Server is integrated with Access Manager through the API for authentication and authorization to portlet content.

5.4.2 UBC Components

PeopleSoft HRMS is integrated with Identity Manager through a resource adapter. PeopleSoft is configured according to support Active Synchronization, where the PeopleSoft resource provides details of the deltas in identity information. Identity Manager periodically polls and acts on these deltas to update its own identity store.

Campus-Wide Login (CWL) is integrated with Identity Manager through a resource adapter that provisions into a shared database table. The implementation of the test version of CWL has been updated so that the insertion of the record into the table triggers CWL to provision the identity into CWL.

Active Directory is integrated with Identity Manager through a resource adapter that provisions into the Active Directory domain. The resource adapter communicates with the IdM gateway, installed on a host in the Active Directory domain, which translates IdM actions into Active Directory commands.

The test instance of myUBC is instrumented to authenticate with Access Manager through the API and to retrieve the roles for a user. Since Identity Manager also authenticates against Access Manager, SSO between myUBC and Identity Manager is also enabled. A user clicks on a link to launch the Identity Manager admin interface from within a myUBC channel, and is not required to authenticate to Identity Manager.

5.5 Deployment

Identity Manager, Access Manager, Portal Server, and Directory Server are deployed on the same machine. Access Manager and Portal Server are deployed in one container under the Sun ONE Application Server; Identity Manager is deployed in another. This separation is required because of conflicts in required libraries. Identity Manager stores its data-store in an Oracle database, also deployed on the same machine.

In a production deployment, all communication paths between the components must be secured using SSL; HTTPS should be deployed as the protocol to the browser. This level of security was not deployed for the POC.

5.6 Provided Services

The POC demonstrates the services of the Java ES IDAM product suite in the following areas (refer to the Integrated IDAM Java ES Product Capabilities document for more detail):

Identity Management

- Identity Discovery and Synchronization.
- Provisioning.
- Profile Management (including self-service).
- Password Management (including self-service).
- Role Management. Admin roles (RBAC-type roles for authorization within IdM), User roles (for role management across external systems).
- Resource Management. Integration with external systems.
- Provisioning Workflow. Custom workflow, notifications, approvals.
- Reporting. Reporting for provisioning-related events within IdM.

Access Management

- Authentication.
- Authorization.
- Policy Management.
- Single-Sign On (SSO).
- Logging. All authentication and authorization requests.

5.7 Implemented and Tested

The POC demonstrates the integration between the components tested with the following functionality (refer to the UBC JAVA ES IDAM Integration document for more detail):

Identity Manager and

- **PeopleSoft HRMS**. Discover identity in PeopleSoft HRMS using activeSync.
- **CWL**. Provision identity into CWL.
- **Active Directory**. Provision identity into Active Directory. Manage identity in Active Directory. Change password in Active Directory. Disable account in Active Directory. De-provision identity from Active Directory.
- **myUBC (through Access Manager).** Provision identity into myUBC. Change password for myUBC. Assign roles for access to myUBC channels.

Access Manager and

- **myUBC.** Authenticate user for access to myUBC. Authorize for access to channel content (with roles). Single-sign on (SSO) access to Identity Manager.

5.8 Other Concepts

There are a number of concepts identified in the feasibility matrix that are identified as report items. These items are elaborated as part of this report, rather than a demonstration. Refer to the feasibility matrix in section 5.1 for the corresponding mapping to the proof matrix

5.8.1 Proxy / Delegation

Proxy or Delegation is where a user can authenticate to a system on another user's behalf with their own credentials. This allows the credentials of the proxied user to be kept private. An example of its use would be a help desk person proxying as a user that is calling in for support; the help desk person can then see exactly what the end-user is seeing without requesting the user's credentials. Another example would be an administrative assistant accessing an executive's account with their privileges in order to complete administrative tasks on their behalf.

Proxy authentication is provided by authentication services of Access Manager. Proxy authorization is provided by role-based definition of privileges, which allows authorization for proxy access by temporarily assigning the roles to the proxy user for the session. This would some customization on the client application in order to introduce the semantics of proxy access.

5.8.2 Privacy and Security of ID Info

Once a user is registered, credentials and identity profile information must be kept private and secure. It is especially important for the user's credentials.

Privacy and security is ensured through the use of two mechanisms: access policy definition and enforcement, and audit logging of access to identity profiles. Access policy can be defined in terms of roles or in terms of individual users.

Other aspect of privacy and security relates to the level of encryption of data within Identity Manager and the security of the connections between the components. Identity Manager encrypts all users' passwords with a triple-DES algorithm and a private key. Identity Manager does not store the attributes that are maintained by resources; rather, it requests and updates the attributes directly on the resource as needed.

If SSL is enabled for the connection between IdM and the resources, then all information (credentials and attributes) is also encrypted for communication over these connections.

Passwords for Access Manager are stored in Directory Server using the salted SHA hashing algorithm. Attributes for users can be accessed from the directory only by users that have permission to see the entries, which is controlled by ACLs within the directory, as maintained by Access Manager.

If the https protocol is enabled between Identity Manager / Access Manager and the browser, then all communication between the browser and Identity Manager / Access Manager is also encrypted and secure.

5.8.3 Multi-Factor Authentication

Access Manager supports a number of authentication methods. Multi-factor authentication is used to strengthen authentication by requesting something the user knows (password) along with something the user has (such as RSA token id).

Access Manager supports the following types of multi-factor authentication:

- Certificate-based. Allows a user to log in through a personal digital certificate (PDC). The module comes with an Online Certificate Status Protocol (OCSP) which can determine the state of a certificate.
- SecurID. Allows for authenticating users using RSA's ACE/Server authentication server.
- SafeWord. Allows for authenticating users using Secure Computing's SafeWord™ or SafeWord PremierAccess™ authentication servers, which support a number of multi-factor authentication approaches (including passcode-generating tokens, digital certificates, smart cards, biometrics, and text-messages to wireless devices).

Other supported authentication methods include Kerberos, LDAP, Radius and NT / Unix authentication. In addition, custom authentication models can be written and plugged in to Access Manager.

5.8.4 Federation of Identities and Standards Support for Identity

The Liberty Alliance project is a standard developed in co-operation with a number of vendors that allows federation of identity information within a Circle of Trust, supporting SSO and identity information sharing (using the SAML protocol).

The Security Assertion Markup Language (SAML) service defines a framework for exchanging security assertions among security authorities. This makes interoperability across different platforms possible, enabling authentication and authorization, and attribute services.

Access Manager supports the Liberty-Alliance specifications (Identity Federation Framework 1.2 specifications) and the SAML protocol.

5.8.5 Identity Life-Cycle Management

Identity Manager provides support throughout the life-cycle of an identity. As identities are provisioned, managed, or de-provisioned- either from within Identity Manager or from an external resource- events are triggered within Identity Manager that can then trigger custom workflows at that point in the identity life-cycle. This allows customized, consolidated handling of events through-out the life-cycle of the identity.

5.8.6 Fit with Existing Infrastructure and Services

As the POC demonstrated, it is possible to selectively migrate external resources and systems to be managed by Identity Manager and Access Manager. It is also possible to selectively implement the services provided (e.g. first password change, then delegated administration, etc.). The POC also shows that Identity Manager and Access Manager can co-exist with other Domain Controllers (such as Active Directory or CWL).

5.8.7 Standards Support

The Java ES IDAM stack implements and supports a number of standards, including LDAP (Directory Server), SAML (Access Manager), SPML (Identity Manager), and XML (Identity Manager, Access Manager).

5.9 Proof Matrix

The following table shows concepts identified in the proof matrix, the method for addressing that concept, and the pointer to features / project activities that provide the proof. Refer to the references for more details of how the proofs were carried out.

#	Requirement / Objective	Scope	Proof Result (Feature, POC Activity)
	Framework Capability (platform)		
	Organization Model Administration		
1	A central registry of identity, roles, and access information	Demo	Identity Manager – user, role model Access Manager – access policy Directory Server
11	Role creation and management	Demo	Identity Manager – roles
9	De-centralized (delegated) administration	Demo	Identity Manager – admin roles
8	Delegation of authority (proxy)	NIS – Report	Access Manager – authentication and authorization plus customization
12	Policy enforcement	Demo	Identity Manager - account id and password policy; role-based access to resources Access Manager - access policy
18	Role definition and Role Based Access Control (RBAC)	Present ation	Identity Manager – admin roles
	User Provisioning		
10	Flexible (central) provisioning	Demo	Identity Manager – provisioning model
19	Automated, distributed provisioning workflow	Demo	Identity Manager – provisioning model
20	Automated, distributed deprovisioning workflow	Demo	Identity Manager – provisioning model
	Protected Resource Provisioning		
10	Flexible (central) provisioning	Demo	Identity Manager – provisioning model
19	Automated, distributed provisioning workflow	Demo	Identity Manager – provisioning model
20	Automated, distributed deprovisioning workflow	Demo	Identity Manager – provisioning model
	Identity Life-Cycle Management		
13	Privacy and security of ID info	Demo	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role

			assignment capabilities.
	Authentication (user) and Session Management		
2	Authentication, with support for multi-factor	Demo	Access Manager – authentication (multi-factor not demonstrated)
	Authorization (resource)		
18	Role Definition and Role Based Access Control	Present ation	Identity Manager – role model
3	Authorization – individual, course-grained	Demo	Access Manager – access policy
4	Authorization – role-based, fine-grained	Demo	Access Manager – access policy
5	Authorization – Anonymous (proxy), coarse-grained	Report	Access Manager – authentication and authorization plus customization
	Password Management		
16	Password Management	Demo	Identity Manager – password policy
	Integration		
6	Unified login name and password	Demo	Identity Manager – user model
7	SSO using unified login name and password	Demo	Access Manager - SSO
17	Identity synchronization	Demo	Identity Manager – identity synchronization and linking
15	Federation of identities	Present ation	Access Manager – authorization; support for SAML and Liberty Alliance
14	Standards support for identity	Present ation	Access Manager – authorization; support for SAML and Liberty Alliance
	Identity Consolidation		
21	Discovery of distributed identities	Demo	Identity Manager – reconciliation, active sync
22	Discovery of distributed profiles	Demo	Identity Manager – reconciliation, active sync
	Services Capability		
	Organization Model Administration		
28	Distributed (delegated) administration	Demo	Identity Manager – organization model, admin roles
36	Implement delegation of authority	Report	Access Manager – authentication and authorization plus customization
29	Delegation / proxy rights	Report	Access Manager – authentication and authorization plus customization
25	UBC-wide policies control	Demo	Identity Manager – account id, password policy Access Manager – access policy management
37	Allow simple, effective, decentralized support of users	Demo	Identity Manager – delegated administration
38	Enable easy creation and management of groups	Demo	Identity Manager – resource management
39	Enforce applicable policies for access to service and resource	Demo	Access Manager – access policy
	User Provisioning		
40	Enable the automation of business processes and the routing of related information	Demo	Identity Manager –provisioning model

	Protected-Resource Provisioning		
40	Enable the automation of business processes and the routing of related information	Demo	Identity Manager –provisioning model
	Identity Life-Cycle Management		
27	Community-wide self-service	Demo	Identity Manager – self-service interface
32	Maintain personal privacy and security of information	Present ation	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role assignment capabilities.
41	Eliminate the need to enter and update the personal info in multiple systems	Present ation	Identity Manager – user, role model Access Manager – access policy Directory Server
	Authorization (resource)		
31	Enable secure, reliable access to IT resources and services for all roles	Present ation	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role assignment capabilities.
34	Make it easy for staff and systems to authorize and mange user's access to on-line resources	Present ation	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role assignment capabilities.
35	Prevent inappropriate or unauthorized access	Demo	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role assignment capabilities.
	Logging, Audit Trail, Reporting		
30	Audit log to the individual	Demo	Identity Manager - reporting
	Integration		
42	Support the federation of identity	Report	Access Manager – authorization; support for SAML and Liberty Alliance
33	Reduce overall admin costs and improve effectiveness	Report	Identity Manager – delegated administration
	Identity Consolidation		
22	Identity consolidation	Demo	Identity Manager – user model, resource reconciliation / synchronization of identities
23	UBC-wide identity consolidation	Demo	Identity Manager – user model, resource reconciliation / synchronization of identities
24	UBC-wide roles consolidation	Demo	Identity Manager – role model, resource mapping
26	UBC-wide profile consolidation	Demo	Identity Manager – user model, resource reconciliation / synchronization of identities
	Implementation Efficiency		
45	Co-existence of frameworks	Demo	Integration with Campus-wide Login, Active Directory
46	"Transparent" migration of applications to the new framework	Demo	Integration with myUBC, PeopleSoft
47	Integration of domain controllers	Demo	Integration with Campus-wide Login, Active Directory

48	Identification of the effort and resource for a PROD implementation	Report	Identified as pilot activity
	Life-Cycle Operations Efficiency		
49	Support for identity life-cycle management	Report	Identity Manager – user model, provisioning workflows
50	Identity framework support UBC IT operational targets	Report	POC provides functional coverage; load-testing identified as pilot activity
	UBC Implementations Support and IT Challenges		
51	Active Directory integration	Demo	Integration with Active Directory
52	PeopleSoft HRMS integration	Demo	Integration with PeopleSoft HRMS
53	Support incremental implementations and adoptions	Report	Recommend staged approach (e.g. pilot)
54	Highly secure	Report	Identity Manager, Access Manager – Support for SSL, https protocols Identity Manager – Credentials encryption methods
55	Support privacy on identity information	Report	Identity Manager – role assignment Identity Manager – audit Access Manager - access policy, role assignment capabilities.
56	Support Federation	Report	Access Manager – authorization; support for SAML and Liberty Alliance
57	Conform to Federation standards	Report	Access Manager – authorization; support for SAML and Liberty Alliance
	Deliverables		
	Install technology stack	Y	Provided environment and installation.
	Integrate technology stack	Y	Access Manager + Identity Manager integration (provisioning, SSO) Directory Server
	Configure base services	Y	As part of base services demonstration
	Load test data	Y	As part of demonstrations
	Design demo scenarios, roles, groups, organizations, identities	Y	As part of demonstrations
	CWL interface	Y	CWL integration
	AD interface	Y	AD integration
	PeopleSoft interface	Y	PeopleSoft integration
	Radius integration	NIS	
	POC Report	Y	This report
	POC Presentation to IT	Y	Demonstrations
	POC Presentation to Campus stakeholders (SNAG, etc)	Y	Demonstrations
	Test cases demo	Y	Demonstrations

5.10 Open Issues

Within the specific scope of the POC, there are no critical open issues.

This section discusses additional features and extensions to investigated features that are considered important to be evaluated through follow-up activities.

This section provides more supporting detail to the issues identified in section 2.4.4.

5.10.1 Integration with SunONE and JES Email Services

Integration with the SunONE email service was deferred until UBC IT moves to the appropriate release.

5.10.2 Two-way Integration with Campus-wide Login

The CWL integration effort was limited somewhat by the availability of the CWL development team, whose efforts were focused on critical deliverables – SIS support in particular. It had been our intention to view CWL both as an authoritative resource, where identities and accounts originated, and as a managed resource, where accounts created elsewhere could be provisioned. Within the timeframe and with the staff available, we were only able to demonstrate the latter.

5.10.3 Name Space Synchronization with Campus-wide Login

Campus-wide Login manages the name space in which user accounts are created. It synchronizes with Tracc-II to ensure that the same account name is not used for two different identities. If accounts are to originate with both CWL and Identity Manager, they must each check with the other for every account creation to ensure that they don't both create an account with the same name. This level of sophistication of interaction was beyond the scope of what we could do with the supplied adapter.

5.10.4 Updating of Campus-wide Login Accounts

With the simple one-way shared-file strategy we used, we were not able to retrieve account attributes from the CWL service, nor were we able to update them.

5.10.5 Role Provisioning to Campus-wide Login Accounts

The account-creation interface we used for our CWL integration does not permit the assignment of roles. It just supplies basic information to the CWL account-initialization modules, which only assign basic affiliation roles.

5.10.6 Access Manager Policy-based Authorization for myUBC Channels

We were only able to perform authorization at the role-name level with our myUBC integration. In this setup, authorization is done within the application, based on the role name supplied by Access Manager. We were not able to test a scenario where channel access was controlled through an Access Manager policy instead of the uPortal permissions engine.

5.10.7 Attribute-based Dynamic Organization Assignment

Our test of dynamic assignment of users to organizations is based on rules programmed within Identity Manager. Our rules were simplistic, referring to lists of predetermined account names rather than evaluating attributes. In a more authentic test, assignments would be based on retrieved attribute values such as roles.

5.10.8 Automated End-to-end Provisioning

In our provisioning demonstrations, information was retrieved from the PeopleSoft resource to Identity Manager. A manual step was then performed to provision the corresponding Active Directory account. A more complete demonstration would have included an automated script (workflow) to perform the complete process.

5.10.9 Support for Login to Commercial Applications Software

While we demonstrated authentication to the JES components and myUBC, we didn't show authentication to any commercial applications such as PeopleSoft.

5.11 Gaps

This section discusses gaps between what we learned in the proof of concept, and what we need to know to move forward.

As this was a proof of concept, and not a technology test or a product evaluation, there were many things we did not explore. Compressed into a single host, our test platform was far from production hardness. Our integration tests were necessarily performed with sandbox versions of other services. Our operating system was used as delivered from Sun, without any local hardening or enhancement. As a result there were many things we could not assess.

The following sections expand on the topics listed in section 2.4.4, indicating activities for future studies and pilot projects.

5.11.1 Current Software Version Characteristics

We did not use the most recent versions of the Sun products – our JES components came from the 2004Q2 release, and our Identity Manager work was done primarily on a version without any service packs applied. For a production implementation, we would expect to use the most recent JES release.

5.11.2 Version Compatibility with Products from Other Vendors

It is important that versions of the JES products be certified compatible with those of other major products such as PeopleSoft. We should be able to plan for upgrades of either without suffering from version skew.

5.11.3 Robustness

We need to perform load, volume, and stress tests to determine how the JES products will behave under extreme conditions within the context of the UBC environment.

5.11.4 Ease of Installation for Production

Considerable planning will be required for production installation. We need to ensure a clean fit to the UBC operational environment.

5.11.5 Ease of upgrading – Assessment of when to patch or upgrade

We need to exercise the JES upgrade process and understand how clean back-outs can be achieved without impact on production processes or disrupting user practices. We also need to be able to assess when it is appropriate to apply a patch or an upgrade.

5.11.6 Scalability

We need to explore strategies for scaling up the capacity of JES products in production. This should be a zero-design solution. It should be one of the deliverables of our production implementation design.

5.11.7 Development Environment Management Issues

While it supports a rich set of development and configuration options, Identity Manager provides little in the way of production infrastructure, such as support for staged instances or clean promotions and back-outs. Almost all development is GUI-based, which makes repeatable promotions and back-outs problematic. We will have to design a development environment with the usual stages (devl, test, verf, prod), and a CVS code repository.

5.11.8 Operational Management Issues

We have not explored any of the operational issues associated with the JES products. How are products started, stopped, and monitored? How do we monitor the user experience? How do users report problems, and what should the operational response be? What are the appropriate availability targets?

5.11.9 System Administration Management Issues

We need to understand the installation and patching cycle, capacity planning, and performance assessment. For example: What are the criteria for deciding to install a new release? What is the impact on users?

5.11.10 Continuous Availability Characteristics

An institutional identity management service must exhibit continuous availability to its end users. This will affect platform architecture design. Patching and upgrading are important considerations. For example, can we go through a version upgrade change without imposing an outage on our users?

5.11.11 Federation Capability

Within UBC we can integrate across all identity sources. To extend the use of UBC identities to service providers outside of the institution, we must federate. This will entail establishing federation partnerships with other institutions and services providers, and agreeing on a protocol for certified authentication and attribute exchange. The two common standards are Shibboleth and Liberty Alliance. We may need to support both.

5.11.12 Operational Maturity of Products

Our investigations within the proof of concept gave us no opportunity to assess the operational maturity of the JES products. This evaluation step should be part of a pilot project.

5.11.13 Custom Adapter Development

All of the resource adapters used in the proof of concept were from the set included with the Identity Manager distribution. We will need to gain experience with custom adapter

development for integration of the SIS. We may also find a need to modify the provided adapters. This could be done within a pilot project.

5.11.14 Platform Sizing

Our investigations within the proof of concept did not include any measurements which would provide a basis for initial platform sizing. Interviews with Rick Zimbelman and Guy Pensa indicate that we should be considering something on the order of a 4 processor Sun server with 8 gigabytes of memory.

6 Proposed Action Details

6.1 Action Plan Proposal

Based on the conclusions, recommendations, and opportunities for action arising from the proof of concept, the following actions are proposed as components of a 6-9 month initiative to further the implementation of an enterprise identity and access management infrastructure at UBC. They are broken into three main areas of focus, namely practice development, potential components for pilot projects, and governance and partnership issues.

6.1.1 Practice Development

UBC IT needs to establish and sustain a centralized, ongoing identity management practice.

To grow its practice, UBC IT must conduct and attend training sessions and engage in technology studies. It must maintain awareness of developments in the higher education community as well as what is being done within UBC. These steps will enable the establishment of an identity management practice within UBC IT. The eventual size, staffing, and resource requirements of the practice will depend upon the size and number of identity management initiatives undertaken by UBC.

6.1.1.1 Training

UBC IT must train staff in the principles and use of the technology products recommended in the projects section. Specifically, staff should attend courses on:

- Identity Manager
- Access Manager
- Directory Server

Training must cover relevant system administration, service administration, and development techniques and practices. Training plans should driven by the selection and timing of the proposed pilot projects.

6.1.1.2 Technology Pilot Studies

An important deliverable of the proposed pilot studies is the acquired understanding of the technology in an ongoing operational environment. In selecting staff members for the pilot studies, it is important to consider their long term involvement in UBC IT's identity management practice. Practice development may also be a driver in the prioritizing of pilot projects.

6.1.1.3 Higher Education Initiatives

UBC IT must continue to participate in ongoing higher education initiatives such as the Internet2 Campus Architecture Middleware Planning (CAMP) workshops.

6.1.1.4 Community Awareness

UBC IT needs to maintain awareness of information resources, practices, and technology products within the institution.

6.1.2 Governance and Partnerships

6.1.2.1 Governance Body Formation

Identity management is an institution-wide concern which goes far beyond the technology challenge. Responsibility for direction and policy should reside in a body that represents the interests of major stakeholders and users. As well providing governance such a body could assist in the establishment and coordination of cooperative partnerships amongst the campus units who hold identity information.

Establishing a governance body will give credibility to UBC IT's identity management initiatives and ensure that they are consistent with institutional needs and directions.

6.1.2.2 Partnerships within the Institution

Achieving the identity management capability that UBC needs will require that UBC IT form partnerships with other campus units, particularly those who are large holders or consumers of identity data. There will also be a need for partnerships between various System of Record owners and other stakeholders. As mentioned above, a governance body could assist in the formation and coordination of such partnerships.

6.1.2.3 Federation Partnerships

UBC needs to identify the set of service providers with which it needs to form partnerships. UBC IT should work through BCNet, CANHEIT contacts, UBC departments, and the identity management governance body to make this happen. The objective is to set up appropriate trust relationships. Once the necessary relationships are identified, agreement can be reached on the appropriate technology for federation implementation.

Federation partnerships are driven by members at one institution needing to make use of services at another, but they are actualized through the establishment of a "fabric of trust" between identity providers and service providers. The trust fabric is based on mutually agreed-upon standards[8] for such things as level of security, quality of attribute information, and thoroughness of credentialing procedures. The process is usually managed through an organization which administers a certificate authority to create a common assurance level based on identity proofing of member institutions.[9] There are implications here for both the proposed governance body and UBC IT's identity management practice. Standards must be met not only at the technology level, but for authority and responsibility distributed across UBC departments and individual staff

[8] Sometimes the standards are based on legislation. In the United States, higher education institutions will need to comply with a federal "Credential Assessment Framework" (CAF) standard for secure interactions with government departments.

[9] In the United States the InCommon organization performs this role. It is our understanding that InCommon membership is not at present available to Canadian institutions.

members. New designations of responsibility and authority may be required. Issues of governance that will arise include the following:

- Ownership and Stewardship: Who are the identity information proprietors? Who is responsible for collecting and maintaining identity data?
- Data quality: How certain are we that digital identity information is associated with the correct person? How certain are we of the correctness of attribute values? Can we associate a "level of confidence" value with each attribute?
- Policy and Authority: Who has the authority and responsibility to make policies regarding identity information?
- Certification: How can we certify the quality of attribute data to guarantee appropriate levels of trust?
- Process Quality: Are our processes appropriate to the desired level of trust? E.g.: What is the quality of our credentialing processes?

6.1.3 Proposed Projects

In the following sections we give a brief description of skills, dependencies, deliverables, and benefits for each project. Details of effort and resource assignment will be dealt with in the project proposal and project charter processes. The entries for effort and time frame are rough targets, and should be viewed as a guide to the relative sizes of the projects.

6.1.3.1 Project: Create a Long Term Architecture Plan

This project implements the action proposed in recommendation 1 in section 2.6. It is closely aligned with the next project (section 6.1.3.2) which focuses on specification of the repository architecture.

The result of this project will be a clear description of the architectural model on which UBC's unified central identity management capability will be based. The underlying model and its principles[10] are the focus. While the main deliverable will not be implementation-specific, it must be implementable. It will not be technology-specific, but will be capable of accommodating evolving and future technology products.

It is not expected that the architecture can be specified in its ultimate final form at this stage – it will evolve through time. The expectation is a sufficiently clear draft for UBC's major stakeholders to agree on goals and directions, and to provide a foundation for implementation projects to proceed.

Target Effort:	2 FTE months
Time Frame:	3 months elapsed
Skills:	UBC identity landscape expert Identity management expert

[10] An example of a principle is "Users should be in control of their own identity attributes and there should be no central repository of their personal data controlled by a third party". Adopting a user-centric approach would strongly influence the nature of the resulting architecture. The example is taken from an article written by Dave Kearns *[Network World, August10, 2005]*. Kim Cameron's "Laws of Identity" (which includes the user-centric concept) is a good source for principles to be considered.

	System architect
Dependencies:	None
Deliverables:	A first draft of a high-level architecture specification for identity management at UBC
Benefits:	The architecture specification will set a clear context and framework for identity management initiatives, both within UBC IT and amongst other UBC units. It will provide a basis for consistent direction and goal setting. It will set the foundation for partnerships and cross-unit projects.

6.1.3.2 Project: Define the Repository Technical Architecture

This project creates the detailed description of what will constitute UBC's identity repository. It will focus on defining the extent to which a virtual repository is appropriate, and what derived repository elements are required. It will determine the ongoing support and maintenance activities that will be required (e.g, an operational merge team), and the necessary departmental agreements and partnerships.

The result will be a high-level technical architecture definition: the platforms, the data stores, the interfaces, the services, the external entities, and the context within which the entities interoperate.

Target Effort:	4 FTE months
Time Frame:	3 months elapsed
Skills:	UBC identity landscape expert SIS semantics and structure expert PS-HR semantics and structure expert CWL semantics and structure expert Oracle/LDAP/AD experts Identity management product expert (trained in Sun products) Business analyst
Dependencies:	Input from the Long Term Architecture Plan is desirable Input from the Gaps studies would be useful
Deliverables:	High-level technical architecture definition for the "repository" component of UBC's identity management infrastructure
Benefits:	The repository, whether virtual or monolithic, is the centre of any identity management service. Having this aspect of the service defined will give clarity to all other identity management initiatives, especially those based on inter-departmental partnerships.

6.1.3.3 Project: Create an Implementation Road Map

The Road Map document will be a description of the path or alternative paths to realization of the architecture and services outlined by the architecture definition project described in section 6.1.3.1.

Target Effort:	2 FTE months
Time Frame:	2 months elapsed

Skills:	Business analyst UBC identity landscape expert Identity management product expert (trained in Sun products) System architect
Dependencies:	Draft of architecture plan Draft of repository definition
Deliverables:	High level directions document outlining the necessary steps to a full implementation of unified institutional identity management at UBC
Benefits:	A coherent public plan for identity management for the institution will provide a framework for leadership, departmental planning and initiatives, central services, and partnerships within UBC.

6.1.3.4 Pilot: Establish a Technology Platform

This project puts in place the technology platform to be used by the other pilot projects, and where the gap studies will be performed.

The project can be viewed as phase 1 of a 3-phase process. We build a pilot platform based on our current expertise and understanding of what is needed (phase 1), perform the gap studies (phase 2), and then create a final production service based on what we learn (phase 3).

The initial implementation will be of production quality according to UBC IT standards. It will include distinct development, test, verification, and production environments and may comprise multiple hosts. It will be scalable and robust. It will employ appropriate technologies (redundancy, clustering, failover, etc.). The expectation is that this platform will evolve into a secure, reliable, continuously available, scalable, and robust institutional service – this will be a guiding principle in all design choices.

The following initial product set will be installed:

- Identity Manager
- Access Manager
- Directory Server

Target Effort:	1 FTE month
Time Frame:	1 month elapsed
Skills:	System Architect (familiar with UBC IT standards) Identity management product expert (trained in Sun products) UBC identity management landscape expert Hardware platform installer Software platform installer Operations representative/analyst
Dependencies:	None critical Input from long term architecture plan is desirable Input from repository project is desirable
Deliverables:	A robust production environment for identity management pilot projects Robust environments for development, testing and verification of identity

management services at UBC

Benefits: A ready and efficient operational environment for identity management work will enable pilot projects to proceed effectively and efficiently. Experience gained with this platform will enable the creation of a fully function operational service in the UBC IT identity management practice

6.1.3.5 Pilot: Develop Campus-wide Login Identity Manager Adapter

Campus-wide Login serves UBC both as a System of Record and an account management system. This project integrates the CWL information resource with the Sun Identity Manager. The result of the project is an adapter that will enable enhanced administration of the CWL as well as provisioning, discovery, and synchronization with other information sources. The adapter will support 2-way synchronization and update, as well as role and identity key management.

Much of the work for this project will need to be done within the CWL development team.

Target Effort: 6 FTE months

Time Frame: 4+ months elapsed

Skills: CWL architect/designer
CWL developer
CWL DBA
Identity Manager adapter developer
Identity management expert (trained in Sun products)

Dependencies: Pilot technology platform

Deliverables: A production-capable CWL adapter for the Sun Identity Manager

Benefits: Completion of this project will provide the key component for integration of CWL with other Systems of Record through Sun's Identity Manager, enabling other CWL pilot projects to move forward.

6.1.3.6 Pilot: Campus-wide Login Service – Role Administration

This project extends the utility of UBC IT's Campus-wide Login service, by introducing complementary capabilities with Identity Manager. Specifically, it adds distributed administration, allowing departmental authorities to manage roles and other account attributes relating to services under their control. This has been a long-requested feature of the CWL service.

Much of the work for this project will need to be done within the CWL development team.

Target Effort: 5 FTE months

Time Frame: 3 months elapsed

Skills: Identity Manager developer
CWL DBA
Identity management expert (trained in Sun products)
CWL architect/designer

	CWL developer Computer accounts operations expert
Dependencies:	Pilot technology platform CWL Adapter
Deliverables:	Delegated, distributed, decentralized, management of CWL accounts for UBC departments with fine-grained control of authority
Benefits:	Fills a significant gap in UBC IT's current CWL service, making it much more useful to other units. Relieves UBC IT of the responsibility for of a large portion of CWL administration tasks.

6.1.3.7 Pilot: Develop SIS Identity Manager Adapter

UBC's Student Information System is one of its most critical Systems of Record. It is the authoritative repository for student identity information. To move forward with UBC IT's identity management plans requires that this resource be integrated, and this implies the creation of an Identity Manager adapter for provisioning and synchronization of account information.

The results of this pilot will provide the basis for CWL role synchronization and departmental provisioning proposed as other projects. It will also be the first step for reconciliation between the SIS and other Systems of Record.

Target Effort:	6 FTE months
Time Frame:	4 months elapsed
Skills:	SIS architect/designer/schema authority/data semantics expert SIS developer SIS DBA Identity management expert (trained in Sun products) Identity Manager developer UBC IT identity management architect
Dependencies:	Pilot technology platform SIS partner availability
Deliverables:	Skills and understanding of Identity Manager adapter development Detailed knowledge of Identity Manager interacting with a complex full-size authoritative resource. Detailed knowledge of provisioning and synchronization issues in UBC's virtual repository environment An SIS adapter which can be used for CWL role synchronization and departmental account provisioning
Benefits:	Integration of the SIS into UBC's institution-wide identity architecture Deeper understanding of Identity Manager's potential in UBC's virtual repository environment

6.1.3.8 PeopleSoft-Human Resources Identity Manager Adapter

The PeopleSoft-based Human Resources system is one of UBC's primary Systems of Record. It is the authoritative repository for faculty and staff identity information. To

move forward with UBC IT's identity management plans requires that this resource be integrated, and this implies the creation of an Identity Manager adapter for provisioning and synchronization of account information.

The results of this pilot will provide the basis for CWL role synchronization and departmental provisioning proposed as other projects. It will also be the first step toward reconciliation between the PS-HR service and other Systems of Record.

Target Effort:	2 FTE months
Time Frame:	2 months elapsed
Skills:	PS-HR architect/designer/schema authority/data semantics expert PS-HR developer PS-HR DBA Identity management expert (trained in Sun products) Identity Manager developer UBC IT identity management architect
Dependencies:	Pilot technology platform HR partner availability
Deliverables:	Skills and understanding of Identity Manager adapter development Detailed knowledge of Identity Manager interacting with a complex full-size authoritative resource Detailed knowledge of provisioning and synchronization issues in UBC's virtual repository environment A PS-HR adapter which can be used for CWL role synchronization and departmental account provisioning
Benefits:	Integration of the PS-HR service into UBC's institution-wide identity architecture Deeper understanding of Identity Manager's potential in UBC's virtual repository environment

6.1.3.9 Pilot: Campus-wide Login Service – Role Synchronization

This project will create a mechanism for synchronizing the values of service roles (e.g. those enabling wireless access) in the CWL with the students' current status in the SIS and faculty/staff status in the PS-HR service. This addresses a deficiency in the current CWL service – the deterioration of the quality of role information. Currently, roles can be set when a person enrols in the CWL, but there is no automatic mechanism for maintaining role membership consistent with persons' actual status.

This project consists of creating a process by which Identity Manager senses changes in the SIS and PS-HR systems through its "Reconciliation" or "Active Sync" features, and performs appropriate updates to service roles in the CWL.

Target Effort:	8 FTE months
Time Frame:	4 months elapsed
Skills:	SIS architect/designer/schema authority/data semantics expert SIS developer SIS DBA

PS-HR architect/designer/schema authority/data semantics expert
PS-HR developer
PS-HR DBA
CWL architect/designer
CWL developer
Identity management expert (trained in Sun products)
Identity Manager developer
UBC IT identity management architect

Dependencies: Pilot technology platform
Identity Manager SIS adapter
Identity Manager PS-HR adapter
Identity Manager CWL adapter

Deliverables: A mechanism for maintaining consistency between CWL roles and status in the SIS and PS-HR services

Benefits: Correct and consistent service role information for students, faculty, and staff will be available to services which use CWL.
UBC IT will have achieved a deep and detailed understanding of how information in the SIS and PS-HR services may be reflected to other services through the use of Identity Manager.

6.1.3.10 Pilot: Departmental Account Provisioning

Academic departments rely on information derived from the SIS to create student accounts for access to computing facilities. The current processes which provide the data are non-uniform and insufficiently dynamic. This project creates a common Identity Manager-based service to provision departmental accounts and keep them up-to-date with changes to the SIS and PS-HR services.

Target Effort: 6 FTE months

Time Frame: 4 months elapsed

Skills: Departmental technical expert
Departmental business expert
Identity Management expert (trained in Sun products)
SIS architect/designer/schema authority/data semantics expert
PS-HR architect/designer/schema authority/data semantics expert
Identity Manager adapter developer

Dependencies: Pilot technology platform
Identity Manager SIS adapter
Identity Manager PS-HR adapter
Pilot department partner

Deliverables: An adapter and a process for provisioning departmental accounts for students, faculty, and staff, capable of being used as model for many departments

Benefits: A standard mechanism for departmental account provisioning will enable a uniform approach across many departments

6.1.3.11 Gaps Study 1 – Platform Study and Planning

This project is a study of the systems management and operational issues identified in section 2.4.4 and discussed in section 5.10. It will be done by systems infrastructure experts and applications support staff who have been trained on the Sun identity management products. It will include appropriate training for systems infrastructure and operations staff.

The result will be a detailed specification for a production platform, as well as a staff prepared to manage, maintain, and operate it. The knowledge gained will contribute to the development of UBC IT's identity management practice. This should be a consideration in the selection of participants.

Of particular importance is the requirement for system level security. The service will deal with masses of potentially sensitive identity data and UBC needs to be prepared to guard against potential large-scale exposure or compromise of this information.

Target Effort:	4 FTE months
Time Frame:	4 months elapsed
Skills:	Identity management expert (trained in Sun products) UBC IT systems infrastructure analysts UBC IT operations analyst UBC IT operators UBC identity management landscape expert
Dependencies:	Pilot technology platform
Deliverables:	Understanding of the practices and techniques for reliable support and maintenance of Sun Java ES products, and for the identity management suite in particular A technical architecture specification for a production quality identity management service platform, conforming to UBC IT's standards for reliability, scalability, availability, and security. Trained system administrators who are prepared to install, manage, and upgrade Sun's identity management products in a full production setting Trained operations staff who are prepared to operate and manage identity management platforms and services
Benefits:	The deliverables provide UBC IT with the operational base of its identity management practice

6.1.3.12 Gaps Study 2 – UBC-specific Issues

This project is a study of the UBC-specific issues identified during the proof of concept, but outside of its scope. See section 2.4.4 (Issues Arising) for a listing. Details are discussed in section 4.6.

Target Effort:	3 FTE months
Time Frame:	3 months elapsed
Skills:	Business Analyst familiar with UBC identity management practices Identity management expert (trained in Sun products) UBC identity management landscape expert

Dependencies:	Pilot technology platform
Deliverables:	Clarification of unresolved issues arising from then POC Thorough understanding of identity management issues specific to UBC Assessment of UBC-specific needs, recommended solutions, and report on how the Sun (or other) products can provide for them
Benefits:	Strengthening of UBC IT's identity management practice Improved prioritizing of identity management initiatives

6.1.3.13 Pilot: Liberty Alliance Federation

This project assumes that institutional partners or service providers who have adopted (or are willing to adopt) Liberty Alliance protocols have been identified.

The project involves configuring an Access Manager service with account federation support. An early step will be to find target service and a target set of users.

The project may include the installation of the Sun Federation Manager Product.[11]

Target Effort:	2 FTE months
Time Frame:	2 months elapsed
Skills:	Identity management expert (trained in Sun products) UBC identity management landscape expert Business analyst familiar with federation principles
Dependencies:	Pilot technology platform Pilot partner or service provider Initial set of service users
Deliverables:	A working prototype of Liberty Alliance Federation for UBC users A pilot service for a defined constituency of users
Benefits:	An understanding of Liberty Alliance Federation in operation for UBC users, contributing to the competency of UBC IT's identity management practice A working service for the users, giving them federated access to outside service providers Demonstrated federation capability which can evolve to a institution-wide production service

6.1.3.14 Pilot: Shibboleth Federation

This project assumes that institutional partners or service providers who have adopted (or are willing to adopt) Shibboleth protocols have been identified. A potential candidate is integrated wireless services for CANHEIT 2006 (see section 2.7.2).

The project involves installing Shibboleth software on the pilot technology platform, and integrating it with an authentication service and a source of attribute information. An early step will be to find a target service and a target set of users.

[11] The Federation Manager product was announced by Sun in June 2005. It was not available for study during the proof of concept exercise.

Target Effort:	2 FTE months
Time Frame:	2 months elapsed
Skills:	Identity management expert (trained in Sun products) UBC identity management landscape expert Business analyst familiar with federation principles Analyst familiar with Internet2 Shibboleth
Dependencies:	Pilot technology platform Pilot partner or service provider Initial set of service users
Deliverables:	A working prototype of Shibboleth Federation for UBC users A pilot service for a defined constituency of users
Benefits:	An understanding of Shibboleth Federation in operation for UBC users, contributing to the competency of UBC IT's identity management practice A working service for the users, giving them federated access to outside service providers and facilities at other institutions Demonstrated federation capability which can evolve to a institution-wide production service

6.1.3.15 Pilot: A Centralized Contact Information Resource

This project creates a prototype version of a central contact information resource or campus directory as mentioned in section 2.7.1 and discussed in section 4.7.2.

The result will be a service will can be viewed as a single point of contact by users for viewing and updating all of their address information maintained by central UBC units (HR, Student Services, Library, etc)

Target Effort:	9+ FTE months
Time Frame:	6 months elapsed
Skills:	UBC identity management landscape expert Identity management expert (trained in Sun products) SIS architect/designer/schema authority/data semantics expert SIS developer SIS DBA PS-HR architect/designer/schema authority/data semantics expert PS-HR developer PS-HR DBA CWL architect/designer LDAP expert/DBA Identity Manager developer UBC IT identity management architect Business analyst familiar with identity management Computer accounts operations expert
Dependencies:	Repository technical architecture definition Pilot technology platform Identity Manager SIS adapter Identity Manager PS-HR adapter

Identity Manager CWL adapter

Deliverables: A prototype central directory where users can view and manage their contact information
A mechanism for synchronizing contact information across all Systems of Record
A pilot service which can evolve to institution-wide production

Benefits: Members of the institution will be able to maintain all of their addresses and other contact data through a single centralized facility, with a significant saving of time and effort
Contact information will be more uniform across Systems of Record

6.1.3.16 Pilot: Integrated Java ES Email

This project will explore the issues associated with migration of our SunONE-based mail service to the Java ES platform and its integration with identity management services. The first phase of the project will investigate issues of architecture, platform, and identity management integration. In a second phase, a prototype will be constructed. Sun's Unified Address Book will be studied, especially in how it relates to the construction of a Contact Information Resource (see section 6.1.3.15).

The result of the project will be a clear understanding of what will be required to migrate UBC's production email service to the Java ES platform.

This project will involve considerable involvement by the Mail Project Team, and may be driven by them.

Target Effort: 3 FTE months

Time Frame: 2 months elapsed

Skills: Java ES Mail expert
UBC IT mail service expert
UBC identity management landscape expert
Identity management expert (trained in Sun products)

Dependencies: Pilot technology platform
Email development environment

Deliverables: A prototype of an Email service integrated with other facilities
A planning document outlining a reliable path for an upgrade and migration to Java ES mail

Benefits: Improved planning ability, based on a thorough understanding of what will be required to migrate to Java ES mail
A substantial reduction in the risks to our user population in a mail service migration

6.1.3.17 Pilot: Tracc-II Enhancement/Replacement

This project investigates the integration of Identity Manage with Tracc-II with the objective of replacing Tracc-II components and services with Identity Manager functions. Identity Manager's main strength is its provisioning capability, and there is a potential for using it in place of a number of Tracc-II's internal processes. This will include the

employment of Identity Manager to provision the LDAP directory with Tracc-II information. The project will require the development of an Identity Manager Tracc-II adapter.

Tracc-II's relationship with CWL will be explored, with the objective of deprecating Tracc-II functionality in favour of CWL. Prototype versions of reconciliation processes will be created.

While this is primarily an exploration project, it is expected that the pilot processes developed here can evolve into a production service in subsequent projects.

Target Effort:	2 FTE months
Time Frame:	2 months elapsed
Skills:	Tracc-II designer/architect Tracc-II developer Tracc-II DBA LDAP expert/DBA UBC identity management landscape expert Identity management expert (trained in Sun products) Identity Manager adapter developer Business analyst familiar with UBC account management practices
Dependencies:	Pilot technology platform Identity Manager CWL adapter
Deliverables:	Pilot versions Documented detailed plans for the retirement and replacement of Tracc-II functions
Benefits:	A better understanding of how Tracc-II services can be refined and improved with Identity Manager Ultimately: A more robust, more effective, and operationally more tractable Tracc-II service and a more coherent service offering across CWL/Tracc-II functionality

6.1.3.18 Pilot: CWL LDAP Updating/Synchronizing

This project uses Identity Manager to replace the current process for updating the CWL LDAP directory from its Oracle database.

Target Effort:	3 FTE months
Time Frame:	3 months elapsed
Skills:	UBC identity management landscape expert Identity management expert (trained in Sun products) CWL architect/designer CWL DBA LDAP expert/DBA Identity Manager developer
Dependencies:	Pilot technology platform Identity Manager CWL adapter

Deliverables: A prototype process which can evolve to full production

Benefits: A more reliable process for creating the derived LDAP CWL resource
Improved service to UBC IT's user's of LDAP-based CWL authentication
Improved efficiency through the use of a standard solution

6.1.4 Project Interactions

Many of the projects depend on results and deliverables from other projects. In some cases, there are looped dependencies – a project requires a result from a dependent project. The recommended approach is to run the projects in parallel, feeding early results across project boundaries. This will also contribute to the ongoing development of the identity management practice.

6.1.5 Project Dependencies Diagram

The diagram illustrates dependencies across the proposed projects. Dashed lines indicate situations where early or incomplete results from one project can contribute to another. Solid lines indicate required project deliverables.