# TABLE OF CONTENTS

1 INTRODUCTION AND PURPOSE ........................................................................................................... 4  
1.1 PURPOSE ......................................................................................................................................... 4  
1.2 INSTITUTIONAL REQUIREMENTS FOR AND HISTORY OF THE PROJECT ............................................. 5  
1.3 PROJECT STRUCTURE ...................................................................................................................... 6  
1.4 SUMMARY OF WORK TO DATE ........................................................................................................ 9  
1.5 DELIVERABLES .................................................................................................................................. 10  

2 SCOPE .................................................................................................................................................. 12  
2.1 PROJECT OBJECTIVES ..................................................................................................................... 12  
2.2 PLANNING PROCESS ......................................................................................................................... 12  
2.3 PROCESSES / PEOPLE AFFECTED ................................................................................................... 14  
2.4 TECHNOLOGIES / SYSTEMS AFFECTED ....................................................................................... 16  
2.5 BUDGET ............................................................................................................................................ 17  
2.6 MANAGEMENT OF CHANGES TO SCOPE, SCHEDULE AND ASSUMPTIONS ..................................... 20  
2.7 EXCLUSIONS ..................................................................................................................................... 20  

3 SCHEDULE ............................................................................................................................................ 21  
3.1 LIFECYCLE MODEL ........................................................................................................................... 21  
3.2 DEPENDENCIES .............................................................................................................................. 24  
3.3 STAFFING ......................................................................................................................................... 24  
3.4 SUBCONTRACTOR MANAGEMENT ................................................................................................... 24  
3.5 RISK MANAGEMENT ......................................................................................................................... 25  
3.6 CONTINGENCIES .............................................................................................................................. 27  

4 ASSUMPTIONS ....................................................................................................................................... 28  

5 SIGNATURES ......................................................................................................................................... 33  

6 REFERENCES AND ATTACHMENTS ..................................................................................................... 34  

## LIST OF TABLES
Table 1: Original Project Budget Submitted to CITI ................................................................. 17
Table 2: Revised IAM UCLA Budget Summary ........................................................................... 18
Table 4: IAM UCLA FY07-08, 08-09 Funding Needs ................................................................. 19
Table 5: Milestones and Deliverables ......................................................................................... 23

REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Draft</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/23/2008</td>
<td>Draft 0006</td>
<td>Project team internal draft e</td>
</tr>
<tr>
<td>01/16/2008</td>
<td>Draft 0005</td>
<td>CITI funding review draft</td>
</tr>
<tr>
<td>01/15/2008</td>
<td>Draft 0004</td>
<td>Project team internal draft d</td>
</tr>
<tr>
<td>01/14/2008</td>
<td>Draft 0003</td>
<td>Project team internal draft c</td>
</tr>
<tr>
<td>01/11/2008</td>
<td>Draft 0002</td>
<td>Project team internal draft b</td>
</tr>
<tr>
<td>01/10/2008</td>
<td>Draft 0001</td>
<td>Project team internal draft a</td>
</tr>
</tbody>
</table>
IAM UCLA: IDENTITY AND ACCESS MANAGEMENT
1 INTRODUCTION AND PURPOSE

1.1 Purpose
This document describes an information technology infrastructure project aimed to increase campus productivity and to reduce IT administration overhead by establishing secure, scalable, consistent and user-friendly processes for Identity Management and Access Management. The Identity Management aspect of the project focuses on establishing a unique identity for anyone who may be part of the UCLA community, and then proving that the person is who they say they are. This is also called ‘authentication.’ The Access Management aspect addresses the policies, processes, and groups that enable us to grant the appropriate type and level of access based on the proven identity. This is called “Authorization.” In addition to streamlining the process of granting access based on the roles a person has at UCLA, it also allows us to instantly revoke all access when that access is no longer appropriate.

IAM UCLA manages the process of establishing who you are and what access you have in a way that is simplified, structured, and streamlined.

The IAM project creates the infrastructure to build, link, and implement these correlating processes. The Identity Management phase of the project was funded as part of UTIPP1 and is completed according to plan. The final phase of this entails implementation, documentation, and support beyond the early adopters. The UTIPP2 budget request focuses entirely on the Access Management process, including the key function known as “Permissions Management.” IAM UCLA intends to enable enterprise access management by:

- Deploying an enterprise-wide, 24x7 permissions management system
- Providing cross-campus integration for all applications
- Creating custom delegation tools
- Providing support for local integration
1.2 Institutional Requirements for and History of the Project

In 2003, UCLA released its Information Technology Strategic Vision, which forms the framework for the direction of IT at the University. This vision was influenced by campus academic and administrative leaders, solicited over an 18-month period. The vision yielded 5 areas of emphasis for IT: Student Integration, Research Leadership, Scholarly Interaction, Increased Productivity, and Community Interaction.

IAM UCLA primarily addresses Increased Productivity. Within the context of increased productivity, IAM UCLA intends to enhance university-wide identity management functionality. Prior to the deployment of IAM UCLA services, each campus application managed its user accounts and access to systems largely independently of each other. A user needed multiple logon IDs and passwords in order to sign onto various applications. An administrator managed user access using separate tools embedded in different systems. This practice created delays in users getting access. It caused inconsistent granting of access among systems. It also prevented the university from being able to revoke a user's access across the enterprise in a timely manner when the need arose. At the same time, requirements were emerging, calling for ways to enable collaborative learning and project management online.

UCLA needed a way to:

- Improve the end-user account credentialing experience.
- Improve account administration.
- Reduce security exposures.
- Ensure privacy.
- Improve audit and reporting
- Improve collaboration with 3rd parties

IAM UCLA addresses these issues by deploying an enterprise framework to perform:

- Consistent collection of directory information
- Unified identity across the enterprise
- Streamlined self-service account credentialing

1 http://www.oit.ucla.edu/CommonDocuments/TTPB_Brochure.pdf
• Standards-based web single sign-on
• Federated authentication and user attribute exchange
• Delegated permission management
• Enhanced security policy enforcement

In 2004, CITI sponsored the Enterprise Directory & Identity Management Infrastructure (EDIMI) project within UTIPPI\(^2\). EDIMI was in fact the first phase of the IAM UCLA initiative. The UTIPPI EDIMI project deployed the common logon provisioning and single sign-on components of the IAM UCLA framework. Today, students and employees use UCLA Logon ID to sign on to over 200 campus web applications, as well as Bruin Online mail, VPN, the campus wireless network, and the majority of student computer labs. The UCLA Logon account creation process has been integrated into the URSA Submit Intent to Register process so that a student is prompted to create her UCLA Logon at the moment she commits to attend UCLA. Behind the scene, the Enterprise Directory has been deployed to collect, organize, and distribute user identity and role data for anyone who may require online access to UCLA resources. Work is underway to transition the campus toward a Internet2 produced, standards-based single sign-on protocol called Shibboleth. Shibboleth also is the adopted protocol by UC and the general higher education community to perform federated authentication and user attribute exchange.

Due to limited funding, the permission management component of the framework was excluded from the UTIPPI EDIMI project. This project picks up where EDIMI left off by deploying the permission management portion of a complete Identity & Access Management framework.

### 1.3 Project Structure

#### 1.3.1 Executive Sponsors

The sponsorship for this project is through the Committee on Information Technology Infrastructure (CITI)\(^3\). The Office of Information Technology (OIT) is the executive sponsor on behalf the campus.

---

\(^2\) For further elaboration on the EDIMI project, please refer to the original EDIMI Project Control Document, dated June 30, 2004.

\(^3\) [http://www.citi.oit.ucla.edu/](http://www.citi.oit.ucla.edu/)
1.3.2 Functional Sponsors

Sponsorship of the functionality is through CITI. As a proxy for CITI there is a MOG. The functional sponsors are represented by the members of the IAM UCLA Management Oversight Group (MOG) which is chaired by Jackie Reynolds. The MOG consists of leaders from key campus organizations whose processes will be impacted by the IAM project, and have taken on a management role for the project. The members of the MOG include:

Jackie Reynolds, OIT (Chair)
Ross Bollens, OIT (Security issues)
Gwen McCurry, CTS (Program Manager)
Don Worth, AIS, Business and Administrative issues
Sue Abeles, Corporate Finance, Controller and Staff ID issues
Kathleen O’Kane, Student Affairs, Student issues
Julie Austin, HSSEAS, Departmental issues
Jackson Jeng, ORA, Programming issues

Ex officio: Albert Wu, Mike Van Norman
1.3.3 Organization and Management

This project is managed via the IAM UCLA MOG.

Figure 1: IAM UCLA project organization
1.3.4 Other Stakeholders

In addition to the organizations represented by the MOG, key stakeholders of IAM UCLA include the data stewards of faculty, staff and student credentials, the distributed administrative officers that will manage the authorization features, the Information Technology Planning Board (ITPB) with responsibility for policies, and CIOs and system administrators responsible for interfacing with the services.

The outcome of this enterprise-wide identity management project will impact the way each individual accesses secured UCLA online resources. It will impact a person’s eligibility for an electronic identity at UCLA, how that person creates a user account, manages her account life cycle, and controls the release of her personal information.

Further down the line, other educational, governmental, and commercial organizations who conduct business with UCLA will impact and be impacted by this project as federated authentication and access management become a reality.

1.4 Summary of Work to Date

This project builds on work done during the UTIPP1 EDIMI project. As of December 2007, the project team successfully deployed the following components outlined in the UTIPP1 EDIMI project control document:

1.4.1 UCLA Logon

"UCLA Logon" is the "common logon" described in the UTIPP1 document. The old Bruin Online Logon ID has been decoupled from BOL services and renamed "UCLA Logon". This decoupling of "identity" from "access" allows us to issue UCLA Logon ID's to individuals who previously were not eligible for BOL services. This is the first step to creating a modular identity & access management infrastructure where account creation is not restricted by an arbitrary set of service eligibility requirements.

In addition, both Bruin Online and URSA have modified their systems to improve the account creation experience for the users. A student is now automatically prompted to create a UCLA logon ID when she visits URSA to submit her intent to register. Visitors now also have a mechanism to self-register for a UCLA Logon ID.

1.4.2 The Enterprise Directory

The Enterprise Directory (ED) is the focal hub of the IAM UCLA system. ED functions as the repository and routing point of individual identity and role data. To date, version 1 of ED has been
released into production. It works in conjunction with several critical identity provisioning workflow processes such as URSA, UCLA Logon Account Management System, and CTS Directory Update Application as well as key university systems such as the UID system, the Student Records System, and the Personnel & Payroll System to collect, organize, and deliver user identity data to applications. For example, as a UID is generated within the UID system, it is, in near real-time, replicated into ED. As a user creates a UCLA Logon ID, her logon ID information is updated immediately in ED. In addition, changes in a person's student/employment status are also updated in ED. Furthermore, ED is now the source repository of campus official emails.

ED is also now the data backend serving user attribute data to ISIS and Shibboleth.

1.4.3 Shibboleth

Shibboleth, the standard-based single sign-on system has been deployed into production. It currently runs in parallel with ISIS. To support the migration effort, the IAM team also integrated ISIS and Shibboleth so that applications using either ISIS or Shibboleth have single sign-on capabilities across the two realms. Shibboleth is now being used by several early adopters such as CCLE, MyEvents, AYSO, and others. Furthermore, UCLA is now a certified member of both InCommon (US Higher Ed) and UC Trust (UC-wide) for federated single sign-on.

To date, the deployment of Shibboleth has been limited to new applications looking to integrate with IAM infrastructure. In 2008, we expect to transition a significant number of existing ISIS applications to Shibboleth and intend to terminate support for the current ISIS interface in 2009.

1.5 Deliverables

The deliverables for IAM UCLA in the UTIPP2 timeframe include:

- Create an enterprise permission management framework/tool/application built on top of the existing Enterprise Directory infrastructure. The permission management framework enables security administrators to manage access to resources from a single easy-to-use web user interface. It allows individuals to delegate access to peers. It also allows applications to reuse commonly defined roles and groups to determine user access at runtime.

- Establish a permanent Identity Management Deployment Consulting team to assist campus units with the work needed to integrate their systems with IAM services.

- Define and produce an application identity management framework within IAM UCLA. As we deploy IAM infrastructure to campus applications, we need to implement an identity management system to track applications connected to IAM. This same framework can be
scaled to a more generalized application-to-application authentication and authorization management system. The reduced funding for this project means we will need to place the generalized deployment on hold, but we will monitor and track campus demands for such system.
2 SCOPE

2.1 Project Objectives
IAM UCLA in UTIPP2 has three key objectives:

- Define and enforce common roles and access rules across the enterprise by deploying an enterprise role and permission management service. This service leverages the Enterprise Directory infrastructure developed in the UTIPP1 EDIMI project.

- Establish a permanent IAM consulting team to assist campus units with integrating their systems with the IAM services. This team will produce ongoing integration documentation and support for campus help desks. It will also help with specific technical integration efforts.

- Define the requirements for an enterprise application-to-application identity management framework. Create at least a limited production model for use within the IAM UCLA infrastructure. Funding permitting, scale such system for broader campus use.

2.2 Planning Process
The planning phase of this project occurred during the UTIPP 1 EDIMI project. This project is in fact a continuation of the UTIPP1 project. For an overview, please see the UTIPP 1 EDIMI project control document.

The IAM UCLA project divides into the following areas of focus:

2.2.1 Access Management Service
The Access Management Service of IAM UCLA will provide the tools and support materials to deploy an enterprise access management system at UCLA. Based on standards-driven systems, IAM UCLA will adopt open source group and permission management tools developed by the higher education community spear headed by Internet2.

The IAM UCLA team will provide consulting support to assist with addressing applications’ identity & access management needs and design/integrate applications with the IAM UCLA Access Management Service.
2.2.2 Identity Management Service: ISIS, Shibboleth, UCLA Logon
Also known as the "authentication" service, the identity management group focuses on the technical interface providing single sign-on, UCLA logon ID provisioning, and federation support. The bulk of the services in this area were deployed under the UTIPP1 EDIMI project.

2.2.3 Directory
The Enterprise Directory is the core of the IAM UCLA infrastructure. It is the repository of all user identity and group data. The Directory group focuses on the ongoing development and maintenance of the Directory Server as well as related data transformation and replication processes. The Enterprise Directory was deployed under the UTIPP1 EDIMI project, and will continue to be enhanced during this phase.

2.2.4 Deployment and Operational Support
IAM UCLA will provide federated help desk support by working directly with local help desks to improve their ability to help their end users. A user is likely to call the help desk of individual applications first when she encounters technical difficulties. The most efficient way to help an end user solve her issue is to provide the help desks with tools and information so that they can address the users' concerns during that first call. To that end, we will provide both online and telephone resources to the campus IT groups and help desks so they can address user needs as quickly as possible.

2.2.5 Architecture & Project Coordination
The architecture team oversees the technical implementation activities from all groups to ensure conformance with the IAM UCLA technical architecture and functional requirements. The team will continue to monitor sprouting campus and external technology development and, as needed, make the necessary architectural adjustments when resources allow. It will convey any architectural changes and consult with all working groups as well as the MOG in a timely manner. In addition, this team will also function as the project coordination team. It will track the project progress and regularly report project status to project sponsors and stakeholders.

2.2.6 Policy
The policy group, with input from the executive sponsor, the management oversight group (MOG), and the implementation working groups, is responsible for developing all relevant policies required to govern and guide the appropriate use of IAM UCLA. It must ensure that the policies satisfy all relevant university, state, and federal guidelines. It is also responsible for conveying the policies to all working groups in a timely manner.
2.2.7 Application-to-Application Identity Management
As a part of the IAM UCLA project, the team needs to create an identity management framework to provide authentication and access management service for application-to-application communications. The application-to-application framework tracks all campus systems integrated with the IAM UCLA infrastructure, and provides authentication and authorization services. It is expected that this framework will have general campus-wide application. The project team will monitor the evolving campus needs and deploy the service to a wider audience as appropriate.

2.3 Processes / People Affected
The following processes are affected:

2.3.1 Managing Online Collaboration Workgroup Resources
Instead of creating redundant system-specific groups over and over, IAM UCLA provides a common group management tool (Grouper) and access interface (Shibboleth) so that administrators can manage user groups from a single interface instead of having to repeat the process in different systems.

To implement, collaboration tools may need to make changes in order to integrate with IAM UCLA. Depending on the tools' particular technical design and implementation choice, the work required may range from simple configuration changes to creating adapter interfaces.

The IAM UCLA project will provide consulting resources to assist with the integration. The resources include documentation, design assistance, and, where we have the appropriate technical skills, selective programming help. It is expected that the application development team will provide the majority of programming resources as needed.

2.3.2 Individuals Managing the release of Personal/Sensitive Data
An individual at UCLA currently has limited ability to manage the release of her personal data. While interfaces exist (URSA, PPS, AYSO, etc.) for an individual to set data release preferences, these release restrictions are not always uniformly enforced. By integrating applications into a common access management service, we can better manage the release of sensitive data through a variety of tools.

2.3.3 Accessing Online Resources and Services at other Universities/Campuses
IAM UCLA enables members of UCLA to logon to online resources hosted by vendors, other universities, and federal granting agencies. Early examples include UC At-Your-Service and soon the UC Learning Management System.
2.3.4 Delegated Security Administration

The campus departmental security administrators (DSA) who currently use the mainframe DACSS application to manage departmental users' access to mainframe resources will get a new web-based tool. This new tool enables DSA's to manage user access for both mainframe and non-mainframe applications integrated with IAM UCLA. In addition, the new web access management tool will add significant features such as pre- and post-condition filters as well as time-limited access currently missing in DACSS.

2.3.5 Application Development and Deployment

Campus developers and IT implementers who currently manage and/or are planning to deploy applications will be expected to consider what will be necessary to adopt IAM UCLA, both technically and financially, when developing the application's system requirements.

2.3.6 Institutional Data Flow

During the UTIPP1 EDIMI project, the IAM UCLA team identified a number of redundant/inefficient identity-related data flow processes at UC. For example, there are multiple, overlapping feeds of employee directory information between UCLA and UC. The team also identified, within UCLA, a number of data-driven workflows that may be based on an outdated understanding of the relationship between a person's roles and her eligibility for service. In other cases, we have identified situations where either the data consumer misunderstands the nature of the data, or that the data consumer has begun using the data it receives in ways that were never intended. These data feeds not only cause confusion over which data feed is correct, they potentially expose the campus to security breaches.

Because having a clean, transparent data flow is critical to creating a robust and scalable identity and access management framework, the IAM UCLA team will continue to work with the data stewards and data consumers to clean up and document these data flows.

2.3.7 Medical Enterprise Single Sign-on and Access Provisioning

The IAM UCLA team recently met with the Medical Enterprise to discuss the feasibility of leveraging IAM UCLA services to address the Medical Enterprise's need for an updated single sign-on system. While the details are still pending further discussion, it appears that there may be opportunities for collaboration. At the least, the Medical Enterprise and IAM UCLA project may be able to share the directory and identity management tools software license. Second, the two groups may be able to leverage a common role and group repository.
2.4 Technologies / Systems Affected
This project is expected to significantly impact numerous campus IT services in the long term. For brevity, only key systems that will be directly impacted during the project’s development and initial deployment are described below:

2.4.1 CCLE
CCLE is expected to be the first adopter of the IAM UCLA Group Management Service. The IAM UCLA team will work with CCLE to define common collaboration roles and groups and develop the technical interface to integrate CCLE with IAM UCLA.

2.4.2 ISIS
ISIS, which has a proprietary programming interface, is being replaced by Shibboleth. ISIS and Shibboleth will run in parallel from 2007 through 2009 while applications transition to the new Shibboleth interface.

2.4.3 ISIS Enabled Applications
During calendar year 2008 and 2009, the IAM UCLA team will work with applications programmers already using ISIS to transition to the new Shibboleth protocol. The migration will take a phased approach and, to the extent possible, will work with each application's natural replacement lifecycle.

2.4.4 Enterprise Directory
The Enterprise Directory is expected to grow significantly in data storage requirements and performance demands as access management services are deployed, and Shibboleth is widely rolled out to the campus.

2.4.5 DACSS
DACSS will migrate onto the new web based access management tool. The IAM UCLA team will provide a compatibility interface on the mainframe to minimize the impact of this migration to mainframe applications.

2.4.6 URSA/Integrated Web Experience
The Integrated Web Experience is another candidate for early integration with the IAM UCLA Access Management Service. We expect to join the IWE team as the IWE enters its detailed technical design phase. The details are pending discussions with the IWE team.
2.5 Budget

The IAM UCLA project originally called for a budget of $4.77 million over 5 years. The budget included 3 temporary consulting FTE to expedite the deployment of IAM UCLA services to campus applications. These 3 FTE’s enabled the project team to engage several projects simultaneously to integrate IAM services with the applications (Table 1).

Table 1: Original Project Budget Submitted to CITI

<table>
<thead>
<tr>
<th>Main Categories:</th>
<th>FY 07-08</th>
<th>FY 08-09</th>
<th>FY 09-10</th>
<th>FY 10-11</th>
<th>FY 11-12</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>$136,800</td>
<td>$148,000</td>
<td>$148,000</td>
<td>$148,000</td>
<td>$148,000</td>
<td>$728,800</td>
</tr>
<tr>
<td>Hardware</td>
<td>$85,200</td>
<td>$109,700</td>
<td>$49,700</td>
<td>$49,700</td>
<td>$49,700</td>
<td>$344,000</td>
</tr>
<tr>
<td>Salaries</td>
<td>$775,327</td>
<td>$806,340</td>
<td>$838,594</td>
<td>$498,364</td>
<td>$518,298</td>
<td>$3,436,923</td>
</tr>
<tr>
<td>AIS Power Unit Charge</td>
<td>$52,320</td>
<td>$52,320</td>
<td>$52,320</td>
<td>$52,320</td>
<td>$52,320</td>
<td>$261,600</td>
</tr>
<tr>
<td><strong>Total Project Costs</strong></td>
<td>$1,049,647</td>
<td>$1,116,360</td>
<td>$1,088,614</td>
<td>$748,384</td>
<td>$768,318</td>
<td>$4,771,323</td>
</tr>
</tbody>
</table>

Less: Funding Offsets

<table>
<thead>
<tr>
<th>FY xx-xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>$148,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permanant</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1,140,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remaining Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>$814,647</td>
</tr>
</tbody>
</table>

Following the CITI Funding Request Review, the IAM UCLA project received a budget of $800k over 18 months to deploy core infrastructure. The reduced funding is still enough for the team to carry one consulting FTE in addition to the necessary core infrastructure development staff. As a result, the project will engage one major project at a time until its core infrastructure development is complete. Once completed, the team will shift resources as needed to work with additional applications to integrate with the IAM UCLA services.

The budget summarized in Table 2 represents the reduced scoped project following the original CITI funding presentation request. Please see the UTIPP2 CITI Investment Request document for ED Phase II for the original budget.
Table 2: Revised IAM UCLA Budget Summary

<table>
<thead>
<tr>
<th>Main Categories:</th>
<th>Development &amp; Maintenance (One-Time / Temporary)</th>
<th>Permanent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FY 07-08*</td>
<td>FY 08-09</td>
</tr>
<tr>
<td>Software</td>
<td>$16,800</td>
<td>$148,000</td>
</tr>
<tr>
<td>Hardware</td>
<td>$85,200</td>
<td>$109,700</td>
</tr>
<tr>
<td>Salaries</td>
<td>$221,520</td>
<td>$575,958</td>
</tr>
<tr>
<td>AIS Power Unit Charge</td>
<td>$26,160</td>
<td>$52,320</td>
</tr>
<tr>
<td><strong>Total Project Costs</strong></td>
<td>$349,680</td>
<td>$885,978</td>
</tr>
<tr>
<td>Less: Funding Offsets</td>
<td>$117,500</td>
<td>$235,000</td>
</tr>
<tr>
<td><strong>Remaining Balance</strong></td>
<td>$232,180</td>
<td>$650,978</td>
</tr>
</tbody>
</table>

* Budget for January through June 2008
Table 3 breaks down the first two year’s budget in greater detail:

**Table 3: IAM UCLA FY07-08, 08-09 Funding Needs**

**FY 2007-08**

**FTE's for January through June 2008**

<table>
<thead>
<tr>
<th>Position</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 FTE systems integration consultant</td>
<td>$55,380</td>
</tr>
<tr>
<td>1.0 FTE web service/infrastructure developer</td>
<td>$55,380</td>
</tr>
<tr>
<td>1.0 FTE web user interface developer</td>
<td>$55,380</td>
</tr>
<tr>
<td>0.5 FTE project outreach/support</td>
<td>$27,690</td>
</tr>
<tr>
<td>0.5 FTE administrative support</td>
<td>$27,690</td>
</tr>
</tbody>
</table>

**Hardware & Software**

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>$85,200</td>
</tr>
<tr>
<td>AIS Power Unit charge</td>
<td>$26,160</td>
</tr>
<tr>
<td>OS licenses</td>
<td>$16,800</td>
</tr>
</tbody>
</table>

Less AIS contributed funds                     $ (117,500)

**Net FY07-08 Funding Need**                   $232,180

**FY 2008-09**

**FTE**

<table>
<thead>
<tr>
<th>Position</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 FTE systems integration consultant</td>
<td>$115,190</td>
</tr>
<tr>
<td>1.0 FTE web service/infrastructure developer</td>
<td>$115,190</td>
</tr>
<tr>
<td>1.0 FTE web user interface developer</td>
<td>$115,190</td>
</tr>
<tr>
<td>0.5 FTE project outreach/support</td>
<td>$57,595</td>
</tr>
<tr>
<td>0.5 FTE administrative support</td>
<td>$57,595</td>
</tr>
<tr>
<td>1.0 FTE production/technical support</td>
<td>$115,190</td>
</tr>
</tbody>
</table>

**Hardware & Software**

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replacement servers(replace old servers deployed in phase I)</td>
<td>$109,700</td>
</tr>
<tr>
<td>AIS Power Unit charge</td>
<td>$52,320</td>
</tr>
<tr>
<td>OS licenses</td>
<td>$28,000</td>
</tr>
<tr>
<td>Directory and IdM software license</td>
<td>$120,000</td>
</tr>
</tbody>
</table>

Less AIS contributed funds                     $ (235,000)

**Net FY07-08 Funding Need**                   $650,970
2.5.1  **Formal Reporting and Reviews**
The IAM UCLA MOG meets monthly to review project progress and to discuss pending issues.

2.6  **Management of Changes to Scope, Schedule and Assumptions**
All changes in scope, schedule or assumptions will be reviewed by the MOG and submitted to CITI for approval.

2.7  **Exclusions**
Help Desk Support: While it is within the scope of the IAM UCLA project to provide support resources, the said resource is targeted at helping campus IT and help desk professionals in supporting the end users. The IAM UCLA project does not have a front-line end user help desk.

Integration Consulting: The IAM UCLA team provides consulting resources to application teams wishing to integrate with IAM UCLA services. This consulting is limited to work directly related to defining user roles and groups. As resources permit, we may also provide the necessary integration programming support. However, the project team does not provide general coding consulting.

The IAM UCLA framework is not to be used as a generic data retrieval mechanism. We only process data requirements to be used directly in making access management decisions.
3 SCHEDULE

3.1 Lifecycle Model
A common attribute of an infrastructure implementation project is the potential for a long lag between
the project's start time and the point a user realizes an appreciable benefit because of the significant
amount of research, planning, and background building-block construction work. To minimize such a
delay, this project adopts an evolutionary approach in implementing the various project objectives,
similar to the spiral development model in software engineering. In addition, where possible, this
project leverages the footprints of existing campus identity management services (Bruin Online, ISIS,
etc.) by evolving those services toward a standards-based, enterprise directory enabled infrastructure.

For information on the phases completed as part of UTIPP 1, Please see Section 3 of the EDIMI PCD.

The following phases complete the roll-out of the Identity Management project, including conversion
from ISIS to Shibboleth as we move away from proprietary tools.

3.1.1 Identity Management/Shibboleth Roll-Out
The technical pieces of this project are in place and are already being used in “early adopter”
applications for establishing identity and authenticating users. The remaining pieces needed to fully
implement the state-of-the-art solution campus-wide are full documentation of the applications,
development of support materials, developing a coordination/support process with campus Help
Desks, and promoting the Shibboleth solution to new applications needing authentication functionality
as well as the 200+ applications that currently use ISIS for authentication. As stated above, much of
this work will be done based on the life-cycle of the applications requiring modifications. All aspects
of this phase are already funded from UTIPP 1.

3.1.2 Access Management – Developing the Prototype (in parallel with 3.1.3)
Technically, there is much initial programming and development work to prepare for providing Access
management or Authorization services for a campus-wide application. The CCLE project has been
chosen as the prototype application which IAM UCLA will support. As part of this phase, the staff
and equipment funded by UTIPP2 will develop the technical workflow, implement Grouper and
Signet, and integrate the workflow with the support structure of the CCLE implementation. It is
expected that one full-time IAM programmer/analyst will work 100% with CCLE project staff to build
this complex interface and work through the delegation, workflow, and support issues. As new
UTIPP2 applications require IAM functionality, we will need to staff accordingly.
3.1.3 Access Management – Scaling for the full campus (in parallel with 3.1.2)
As the project progresses, we need to tackle the key issues that are barriers to full-campus adoption of IAM UCLA. As we learn from the prototype with CCLE, we will need to form policy workgroups that can address role definitions, how groups will be determined, what levels of proven identity are required within groups, and other non-technical decisions, as well as deciding how conflicts are resolved. We will also need to establish a process owner or oversight committee for overall Identity and Access Management, just as we have people who are ultimately accountable for financial controls, safety codes, and student discipline. During this phase, we will also create management tools that will allow local delegation and decentralized Help Desk support, and analyze the functionality needed to provide a production 24/7 environment for the entire IAM process.

3.1.4 Phase II – Full Deployment and Stabilization
The process of Full Deployment and Stabilization will take years as current applications reach a stage in their life-cycles that encourage and enable re-architecting the authentication and authorization functions. There will also be a continuing queue of new applications requiring IAM UCLA interfaces. We need to be staffed for dedicated or nearly-dedicated IAM support to these applications at the exact time that they are ready to re-architect or we may miss the window of opportunity.
Table 4: Milestones and Deliverables

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Time</th>
<th>Status</th>
<th>Major Activities</th>
<th>Associated Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch ISIS to Shibboleth Migration Program</td>
<td>February 2008</td>
<td>Production</td>
<td>officially launch program to migrate existing ISIS enabled applications to use the new Shibboleth protocol</td>
<td>Shibboleth; IAM consulting service; IAM support materials</td>
</tr>
<tr>
<td>Complete ISIS to Shibboleth Migration</td>
<td>October 2009</td>
<td>Production</td>
<td>Complete the campus migration from ISIS to Shibboleth; Terminate support for current ISIS API</td>
<td></td>
</tr>
<tr>
<td>Deploy Group Management service for pilot</td>
<td>September 2008</td>
<td>Pilot</td>
<td>Install, configure, and test Grouper and Signet systems; Update Enterprise Directory to accommodate group data; Conduct pilot with CCLE; Form policy and practices workgroups to determine best practices and procedures;</td>
<td>Grouper; IAM consulting service; IAM support materials</td>
</tr>
<tr>
<td>Deploy Permission Management Service for pilot</td>
<td>January 2009</td>
<td>Pilot</td>
<td>Install, configure, and test Signet; Conduct pilot with target to be named; Form policy and practices workgroups to determine best practices and procedures;</td>
<td>Signet; IAM consulting service; IAM support materials</td>
</tr>
<tr>
<td>Deploy Group and Permission Management Services to production/Begin wider campus rollout</td>
<td>April 2009</td>
<td>Production</td>
<td>Design and deploy help desk support procedures; Identify a list of integration targets for Phase II integration</td>
<td>Various policy and operational practices documents; Management and support tools; Continued integration plan;</td>
</tr>
<tr>
<td>Full Deployment and Stabilization</td>
<td>FY2009-10 and beyond</td>
<td>Production</td>
<td>Continue to integrate additional systems with IAM services;</td>
<td>Note: at current time, the second target after CCLE is DACSS</td>
</tr>
</tbody>
</table>
3.2 Dependencies

Beyond deploying the basic access management tools and server infrastructure, the rollout of the access management service to the end users depends on successful and timely integration with various applications.

In addition, as access management is formalized and performed outside the individual applications having a coordinated, coherent campus help desk infrastructure is key to effectively guiding a user through any access related issues.

3.3 Staffing

The IAM UCLA project requires 4 permanent additional FTE to the current IAM team. In addition, during the development phase in 2008 and 2009, another temporary consulting FTE is needed. These additional staff will work with the existing IAM team at AIS to develop all the technical and support materials. They will also work with the campus IT community to assist with development efforts to integrate applications with IAM services as well as to provide ongoing technical support.

3.4 Subcontractor Management

No subcontracting is anticipated in this project.
3.5 Risk Management

Risk
Changes to schedule or project scope of CCLE or other projects slated for integration

Priority
High

Type
Cost and Schedule

Description
The integration component of IAM UCLA deployment depends heavily on other projects' schedules. It also depends on projects to supply the appropriate level of resources in staff time to work with the IAM UCLA team to complete the necessary integration tasks.

Mitigation
In the event CCLE is unavailable, we will proceed with DACSS integration first.

Risk
The IAM UCLA project has only received funding for the first two years of the project. Successful deployment of the services covered in this project depends on continued funding.

Priority
High

Type
Cost and Service Availability

Description
While the IAM UCLA project plans to complete the implementation of its server-side components in the first 18 months of the project, deploying the permission management services to the campus requires substantial ongoing deployment and integration support as new applications appear on
campus. Without the continued support funding, it is unlikely that the service will see widespread adoption.

**Mitigation**

CITI and MOG are looking into possible alternate mechanism to fund the ongoing operations of the IAM UCLA services.

**Risk**

UCLA does not have a comprehensive help desk support environment to support the complex multi-system trouble calls likely to occur when troubleshooting issues related to user access.

**Priority**

High

**Type**

User support

**Description**

As the end user computing experience becomes increasingly provided by a distributed set of services, a typical user support call may involve the help desk to research/access multiple backend systems. It also requires the help desk to understand the overall architecture of how pieces fit together. The campus must continue to work toward providing a coherent help desk support environment to avoid creating unnecessary complexity for the end user during a trouble/service call.

**Mitigation**

IAM UCLA is staffing to provide materials and support to front line campus help desks. It will also work with the Help Desk consortium to better organize help desks across campus.

**Risk**

The open source software selected for this project may evolve away from UCLA's requirements.
Priority
Low

Type
Cost and Schedule

Description
The Grouper and Signet software selected for this project are open source collaborations among several higher education institutions. As the products evolve, the product feature set may veer from UCLA's needs.

Mitigation
To ensure that UCLA's interest is properly represented within these open source projects, IAM UCLA team plans to actively participate in the project workgroups responsible for the planning and the design of Grouper and Signet.

3.6 Contingencies
The major concern regarding this project is its integration priorities and schedule. The successful deployment of this service depends significantly on the timing of the other UTIPP2 projects. To account for unforeseen changes in plans for our initial integration targets we have identified secondary systems for integration.

Currently, we expect to integrate with CCLE first. Should that not be practical, we will work on DACSS integration/replacement next.
4 ASSUMPTIONS

4.1 Planning
In planning this project, we assume that:

- The campus leaders will continue to support moving toward adopting a common identity and access management infrastructure across the campus.
- The technology used for accessing campus electronic resources will not radically change in the next 5 years.
- On an as-needed basis, we will solicit various campus subject matter experts to help us determine best practices for data management and release. We will also raise policy issues requiring prompt attention from campus policy makers.

4.2 Third Party Commitments
UCLA has committed to participate in the UC Trust Federated Authentication Project\(^4\). The IAM UCLA project implements components that are critical in order for UCLA to be compliant with UC Trust requirements.

4.3 Expected Loads and/or Transaction Volumes
The IAM UCLA infrastructure is comprised of several technical components of varying sizes and system loads. Several components have been described in the UTIPP EDIMI PCD. The sections below provide additional details related to the deployment of the Access Management Service components:

4.3.1 Enterprise Directory
The Enterprise Directory (ED) continues to be the central repository of person identity and role data. Moving forward, ED is expected to grow significantly in size as it starts to store significant amount of user role and permission data. We also expect ED to be queried heavily as applications validate user access.

In addition, IAM UCLA is expected to carry data about traditionally non-UCLA members in 2008 and beyond. This means that ED will grow not only due to the amount of data we store for each individual, but also due to the number of individuals we track.

---

\(^4\) [http://www.ucop.edu/irc/itlc/ucfedauth/](http://www.ucop.edu/irc/itlc/ucfedauth/)
Repository Size

The Enterprise Directory carries identity, role, and entitlement data for all UCLA community members. We expect ED to carry more than 1.5 million entries with approximately 20,000 entries added annually thereafter. Each entry, depending on the person's roles at UCLA, may contain a wide range of attributes ranging from minimal user demographic data to campus identifier mappings to a full set of role and/or entitlement information based on the employee, student, alumni, and research community data. The Enterprise Directory will also carry rich meta-data such as the data's origin, data transformation processing rules, user selected privacy release preference, directory access control information, and activity logs.

Each instance of the directory repository will require up to 1 TB of storage by the end of the 2 year development phase. At least 2 instances will be required to ensure system redundancy and high availability.

Transaction Volume

Transactions in Enterprise Directory occur:

- When an authentication and/or an authorization processing engine queries the directory during a user authentication/authorization sequence;
- When data updates in the source systems trigger a near real-time and/or batch update of the directory data;
- When a user and/or an administrator updates the directory data via administration tools;
- When data updates in the directory trigger a near real-time and/or batch update of downstream systems.

The transactions handled during authentication and authorization processing will be discussed in §4.3.2 and §4.3.3 respectively. It is difficult to gauge the exact volume of the remaining transactions. However, it is expected that these activities will peak during the beginning and the end of each academic session period when massive updates occur in the source systems.

4.3.2 Authentication Processes

The majority of the authentication attempts in the IAM UCLA project will transition from ISIS to the Shibboleth-based platform. With the increased user population, we expect the authentication attempts to exceed 50,000 daily.
There are likely to be other forms of authentication such as campus lab workstations sign-in that will use the UCLA logon ID and password. However, since these authentication attempts will hit downstream directory servers outside IAM UCLA implementation scope, they are not discussed here.

4.3.3 Authorization Support Processes

The authorization support processes consist primarily of the real-time lookups of user identity, role, and entitlement information via an authorization attribute query interface such as the one offered by Shibboleth. ISIS currently offers a similar mechanism. Using it as base level measure, and considering the expected growth in the number of applications making these queries, it is expected that the service may experience anywhere from 100,000 to over 1,000,000 transactions per day. The exact numbers of these transactions will depend tremendously on the run-time behaviors of the applications taking advantage of this enterprise authorization support service.

4.4 Technologies – Hardware and Software

A significant requirement of the IAM UCLA project is to implement standards-based, platform-neutral application interfaces. When considering software solutions, the IAM UCLA project will make every attempt to offer industry standard data exchange mechanisms.

Where possible, the user interfaces in the IAM UCLA project will be web applications capable of running on standard web browsers.

Where in-house development is necessary, depending on the fit, the project team will use Java to implement the solutions.

4.4.1 Enterprise Directory

The core of the IAM UCLA infrastructure is the Enterprise Directory (ED). ED is the repository for all user authentication and identity data. UCLA uses Sun Directory Server to host ED.

4.4.2 Directory Integration Service

A Directory Integration Service enables the acquisition and publication of valuable data by integrating databases, enterprise applications, and other directories with the Enterprise Directory service. Data integration tasks typically rely on a meta-directory product. IAM UCLA currently uses a combination of custom built data replication scripts and Informatica to perform data synchronization.
4.4.3 Shibboleth
Shibboleth, an Internet2 middleware initiative, is the protocol of choice for federated authentication and authorization in the higher education realm. The University of California has adopted it as the standard federation protocol for UC. Internet2 develops and maintains an open source reference implementation of the Shibboleth server written in Java and C++. This reference implementation is widely adopted by other universities. IAM UCLA will complete the campus migration from ISIS to Shibboleth within the next 24 months.

4.4.4 ISIS Enhancements
ISIS has been integrated with Shibboleth and works with the common logon. Over the next 24 months, the campus will migrate from using ISIS's proprietary SOAP web service interface to Shibboleth.

4.4.5 Group and Permission Management (Access Management)
The IAM UCLA team intends to adopt two software packages developed by Internet2 to manage groups and user permissions. These are Grouper\(^5\) and Signet\(^6\).

4.4.6 Delegated Security Administration Tool (DACSS Web)
IAM UCLA's access management system (Internet2's Grouper and Signet) will replace DACSS's mainframe user interface. The IAM UCLA team will provide the necessary backwardly-compatible layer on the mainframe to reduce the transition cost of the mainframe applications.

4.4.7 Choice of Operating System and Hardware
IAM UCLA operates on open source software where possible. For operating system, unless required otherwise, we are using Linux running on Intel-based servers. In addition, we intend to leverage virtualization technology to reduce hardware cost and to improve system availability.

For service-specific software, we are adopting open source single sign-on, federation, and group/permission management products from Internet2. These software are widely used in the US and international higher education institutions.

There are exceptions to the preference for open source software. For example, we use Sun's Directory Server instead of OpenLDAP for its better scalability and support for high availability configurations. We use VMWare for server virtualization because there are no viable open source alternatives in that

\(^5\) http://www.internet2.edu/pubs/200704-IS-GRP.pdf
\(^6\) http://www.internet2.edu/pubs/200704-IS-SIG.pdf
market. We use Microsoft SQL Server instead of MySQL because MS SQL is a proven standard DBMS environment at AIS.

This project has the requirement to provide load balancing and redundancy for all its servers. The IAM UCLA team will coordinate the decision of specific implementation technology (OS level software load balancing and clustering or dedicated hardware load balancer) with DPNS based on AIS’s total network, systems, and operational requirements.

4.5 Non-Schedule Risks
Please refer to § 3.5 Risk Management.

4.6 Non-Schedule Contingencies
Please refer to § 3.6 Contingencies.

4.7 Deployment
Components of the IAM UCLA infrastructure have been deployed under the UTIPP EDIMI project. For details, please see the EDIMI PCD. The Access Management Service component is the main subject of this development/deployment cycle. For the Access Management Service, the IAM team will work with each application to determine appropriate strategy and timing for integration.

The first integration target is CCLE, followed by DACSS. After that, the team will work with the IAM MOG and the campus IT community to determine further integration targets.

4.8 Funding
The IAM UCLA Project is funded with UTIPP2 funds once the executive sponsor has signed off on the PCD. The UTIPP2 funding covers the first 18 months of development. Additional/permanent funding is pending further review.
5 SIGNATURES

The Committee on IT Infrastructure (CITI) has reviewed this planning document and agrees to the timing and deliverables of the Enterprise Directory & Identity Management Infrastructure.

______________________________
Chair Person, CITI

______________________________
Date
REFERENCES AND ATTACHMENTS

“The Persistent Email Model Project Control Document”.

“UCLA Enterprise Directory & Identity Management Technical Architecture”, Hyperlink TBD

“UCLA Enterprise Directory & Identity Management Functional Requirements”,

“UCLA Enterprise directory & Identity Management Planning Phase Project Control Document”,

“UCLA Enterprise Directory & Identity Management Project Control Document”,

"University of California Los Angeles Directory Services & Identity Management: Recommended Strategy"

"University of California Los Angeles Directory Services & Identity Management: Vendor Analysis and Recommendations"