Minutes (available on web and already distributed by listserv)

**ITPB Attendees:** Chair Chris Foote, Kathy Atchison, Russel Caflisch, Alfonso Cardenas, Brian Copenhaver, Jim Davis, Adam Harmetz, David Kaplan, Greg Kitch, Adrienne Lavine, Sam Morabito

**Guests:** Mike Lee (PDP participant), Larry Locher (OID), Nick Reddingius (OIT), Mike Schilling (CTS), Kent Wada (OIT), Esther Woo-Benjamin (OIT), Don Worth (AIS)

**Agenda:**

1) **Alternative pricing models for technology (non-voice services)**

   In June this year, CTS introduced a new telephone bill format which disaggregated technology from voice. CTS has recently completed preliminary analysis of proposed alternative models for funding those technologies with a campus ‘technology infrastructure fee’ which will be separate from the voice services charges. Mike Schilling presented a comparative analysis of six models: 1) active switched ports, 2) ip address space, 3) knowledge worker head count, 4) knowledge worker FTE, 5) UCLA head count, and 6) UCLA FTE. These models were developed with input from campus workgroups and have been vetted with the CSG. The goal is to select a model where data can be easily retrieved in an automated fashion and the charging algorithm can be kept as simple as possible. Other models being explored include those based on usage and expenditures. There was a question of whether the technology infrastructure fee could be paid for from research grants. The preliminary answer is that it can but CTS will research this in more detail.

2) **Enterprise Directory and Identity Management Infrastructure (EDIMI) project update and policy considerations**

   The discussion surfaced questions on project objectives and overall value to UCLA. Subsequent to the meeting, the project team prepared a non-technical explanation of the project to address those questions. The document: ‘Institutional View of Enterprise Directory and Identity Management Infrastructure (EDIMI)’ is attached as Appendix 1. A document prepared for the Committee on IT Infrastructure (CITI) that summarizes the schedule of project deliverables: ‘Summary of what to expect from EDIMI’ is attached as Appendix 2. If there are additional unanswered questions, they may be directed to Jim Davis.
The EDIMI project is designed to address the ITPB priority for ‘Confident Electronic Business’ established last year and reiterated in the May 2003 Cost Reduction Memo to the Chancellor. Over 18 months ago, the CITI approved development of pilot systems and detailed planning. Earlier this Fall Quarter, final project plans, deliverables and timelines were reviewed in great detail. The review team and the Office of Information Technology (OIT) strongly support moving forward. Subsequent to the ITPB meeting, the Common Systems Group (CSG) voted to support the project with 14 supporting and 1 abstention (not because of problems with the project).

A discussion on the policy implications of the EDIMI project is planned for the next ITPB meeting.

3) Progress on Repositioning IT Initiative

   a. **Network Review** – The information request to the campus was distributed to Deans and Vice Chancellors with copies to CIOs and their designated Network Coordinators on 11/19. The external review team has been finalized: Ron Johnson, University of Washington; John Silvester, University of Southern California; Ken Klingenstein, Internet2 and University of Colorado, Boulder; and Charles Wellford, University of Maryland. The site visit is planned for March 28, 29, and 30. In the next few weeks the ITFOC will begin planning for the structure for the site visit.

   b. **Email Consolidation** – Documentation on progress of the project is being prepared for communication to the campus.

   c. **Data Centers Data Gathering** – This project has just started. The purpose of the project is to identify campus-wide applications and the server rooms that house them. The intention of the survey is to understand how these applications are protected. The project has been scoped to gathering information about administrative applications. Research and instructional applications will be covered in future phases of the project.

4) Future Meetings

   - Tuesday, December 14, 2-4 p.m. @ 2121 Murphy
Appendix 1

Institutional View of Enterprise Directory and Identity Management Infrastructure (EDIMI)

As the broadest statement of objective, the Enterprise Directory and Identity Management Initiative (EDIMI) addresses UCLA's ability to 'confidently' do 'business' electronically with an individual through web-base applications and email. We will refer to this objective as 'Confident Electronic Business.'

'Business' refers to any web-based instructional, research or administrative transaction or managed access activity that an individual might engage in or any transaction or official communication that the university may wish to engage in with an individual.

'Confident Electronic Business' refers to an individual conducting a managed electronic activity with a high degree of assurance that the activity will be secure and that personal identity and information will be protected. 'Confident business' also refers to UCLA having assurances that an individual accessing an application is who the individual claims to be and that an electronic communication will in fact reach a particular individual.

Confident Electronic Business is an ITPB priority reiterated in the May 2003 Cost Reduction Memo to the Chancellor. There are both potential cost savings as well as increased productivity by increasing the ability of the campus to do business confidently with an individual through electronic applications.

What is EDIMI?

EDIMI is a SUITE of campus identity management applications that can be used by distributed web applications. The EDIMI applications together represent a single leveraged investment that will avoid the costs of managing and maintaining replicated individual identify information in many distributed directories and the high cost of replicating accepted security practices for each web application. Additionally EDIMI provides identity management capabilities that are not possible with a distributed identity management and it is the underpinning for next generation network-based services. EDIMI is consistent with the consolidation goals of the Repositioning IT Initiative.

What does EDIMI do for UCLA?

1. Addresses the validity and currency of identity and contact information

Creates a single campus directory containing accurate and up-to-date email address and identity information for an individual. This includes the tools to manage self-service and university authorized changes to this information on each individual in the UCLA community. Changes to an individual’s information are managed and maintained in one place and need to be made only once.
2. Expands the community that can engage in UCLA electronic business to include affiliated individuals

Creates an ID space that allows the campus to conduct confident electronic business with a large base of individuals who are affiliated with UCLA but are not in the payroll system or registered students.

3. Provides robust security tools that increase the protection of personal information and avoid the cost of replication

Provides standards based tools (program modules) for managing individual access to distributed web applications. Organizes security tools centrally so they can accessed by applications and do not need to be replicated. Evolving standards are maintained in one place. Security is raised by providing more robust tools for greater security than many individual applications could afford individually. The incremental investment of web-based applications can be lowered, i.e. it is very costly to replicate and then maintain these kinds of tools.

4. Creates an identity management data service providing authentication and authorization information to distributed applications

Makes identity information from the directory readily available to distributed applications that cannot yet use access management tools, again avoiding replication of information. Provisions identity information for authorization to distributed applications to facilitate authorization and positions the campus for an authorization application in a later phase.

5. Creates an identity credential that will support common logon and single sign in by the individual user

Provides common logon (accessing applications with the same credentials) and single sign on (moving through multiple applications with one use of a credential) both a convenience and a necessity to the end user that will increase in value as the number of applications increase (clear trend). Security is enhanced by doing security right once.

6. Positions UCLA for secure and managed access to resources across UC campuses and UCOP

Provides federated authentication across UC campuses making it possible for the UCLA community to more readily access resources at other UC campuses and at UCOP with greater access security and likewise for secure access to UCLA resources by other UC campus individuals. This capability is not possible without the EDIMI project.
Appendix 2

Summary of what to expect from EDIMI

REQUIREMENT: Common fields describing each person in the UCLA community will be identified, collected from various sources (Payroll, Student Systems, the CTS Phone Directory Update application & self-registration) and carried in the Enterprise Directory. These will include name, mailing address, email address, phone, etc.

PLANNED: This is going to be an ongoing process over the next 2 years. However, we know we will identify at least various variations of name, mailing address, office location, email address, and phone in Phase I (due Summer 2005)

REQUIREMENT: Two online "white page" directories will be published - one that is accessible only within UCLA, and one that is accessible to anyone, including external visitors. Individuals will be able to specify whether they want their directory information listed on in one, both, or neither.

PLANNED: This will be available in Phase I (Summer 2005)

REQUIREMENT: A new "Persistent Person ID" - or unique number - will be assigned to everyone in the campus community. Mapping will be provided between this number and the UID for those persons who have a UID, but there will be the ability also to assign a PPID to persons who do not have a UID.

PLANNED: This will be available in Phase I (Summer 2005)

REQUIREMENT: Registration mechanisms will be created to permit the creation of new identities ("rows") in the Enterprise Directory - one for each person in the community. Persons added to Payroll or Student Systems will be added by those systems. Others may be added by other applications or via a self-service registration web application.

PLANNED: The first set of rollout will be available in Phase I (Summer 2005). First set includes PPS and SIS driven identities and identities created via a CTS-maintained administrator-use tool. Complete self-registration of identities is pending.

REQUIREMENT: Anyone with a PPID (and a row in the Enterprise Directory) may create a "Common Logon ID" or UCLA Logon ID and password. This will replace Bruin OnLine IDs and passwords and can be used by any web application by calling the ISIS authentication service.

PLANNED: This will be available in Phase I (Summer 2005)
REQUIREMENT: Students will be prompted to create a UCLA Logon ID when they file their Statement of Intent to Register (SIR). Others may create it using a self-service web application. URSA will honor the new UCLA Logon ID (replacing the use of UID/PIN).

PLANNED: Students - Fall 2005, Others - Summer/Fall 2005

REQUIREMENT: Single Sign On: Persons will be able to authenticate once to one ISIS-enabled web application, and have that session passed from web application to web application without the need to re-logon.

PLANNED: This already exists for any application that uses ISIS today.

REQUIREMENT: A Microsoft Active Directory will be established with all UCLA Logon IDs such that departments or student labs that use Microsoft networks may create an account for a person that matches his/her UCLA Logon ID.

PLANNED: CTS plans to implement this sometime during calendar year 2005.

REQUIREMENT: Replication of accounts with matching logon IDs on other systems (eg. UNIX, etc.) will also be supported through an account provisioning service.

PLANNED: This is likely a part of Phase III (summer 2006)

REQUIREMENT: The Shibboleth authorization protocol will be implemented to allow authorization for UCLA library patrons wishing to access content that is hosted by external publishers.

PLANNED: We will have a Shibboleth server running by summer 2005, but real implementation of Shibbolized library access depends on vendor support as well.

REQUIREMENT: Staff will be able to authenticate themselves using the UCLA Logon ID to UCOP's benefit applications (UC4Yourself, Benefits OnLine).

PLANNED: A UCFY pilot is slated to begin in December 2004/January 2005. Production implementation is pending.

REQUIREMENT: Data will be provided to applications to assist them in making decisions about authorization based on user attributes or membership in a group. For example, information will be provided about whether someone is a student, faculty, or
staff.

PLANNED: Data will be added gradually over the next 2 years. We expect the first set of authorization type data to appear in ED by Winter 2005.

REQUIRED: A delegated, explicit authorization system will be developed that expands on the concept now represented by DACSS on the AIS mainframe, but extends it to web applications. AIS will explore the use of the new SIGNET open-source application for this purpose.

PLANNED: Signet is in early Alpha. We will follow along and launch select pilot and early adoption programs during the next 2 years. However, we do not expect full deployment till after summer 2006.

REQUIREMENT: One or more email addresses will be collected for all faculty, staff and students and stored in the Enterprise Directory. Each person will designate which address is to be used for "official" university business. And they will indicate which will be published in the online directories.

PLANNED: This is summer 2005

REQUIREMENT: Students will be required to obtain and publish a persistent email address that will continue to exist beyond graduation and could be forwarded to future email accounts.

PLANNED: This is summer 2005