Glossary

Who Should Read: This document is written for all users who wish to look up the meaning of technical terms used throughout this site.

Administrative Contact

During Service Provider (SP) Integration with Shibboleth, the Administrative Contact is the single individual who has over-arching authority regarding their department's application.

AIS

Administrative Information Systems (AIS) manages UCLA's campus-wide administrative computing systems and data, including student records, personnel/payroll, purchasing, ledger, data warehouse, identity management, and others. AIS is the home of the IAM UCLA program.

Apache

The Apache HTTP Server, commonly referred to simply as Apache, is a web server notable for playing a key role in the initial growth of the World Wide Web. A large number of web sites on the Internet use Apache HTTP Server. See Wikipedia's entry about Apache HTTP Server for more information.

Attribute

An attribute is a single piece of information associated with an electronic identity database record (e.g., a user record). Some attributes are general; others are personal. Some subset of all attributes defines a unique individual. Examples of an attribute are name, phone number, and group affiliation.

- definition transcribed from InCommon Glossary

Authentication (AuthN)

The security measure by which a person transmits and validates his or her association with an electronic identifier. An example of authentication is submitting a password that is associated with a user account name.

- definition transcribed from InCommon Glossary

CTS

Communications Technology Services (CTS) is a campus organization that manages critical campus communications infrastructure such as network access, telephones, campus enterprise messaging, bruin online, and the UCLA Logon ID.
EDIMI

The Enterprise Directory and Identity Management Infrastructure (EDIMI) Project (also known as the Enterprise Directory Project) is an mwidocs:UTIPP project aimed to improve user identity and access management practices at UCLA.

The initial EDIMI project focused on deploying a campus-wide logon ID (UCLA Logon), standards-based web single sign-on (Shibboleth), and the Enterprise Directory. It began in 2004.

In 2007, CITI approved the next phase of project focusing on deploying enterprise access management tools. At the same time, the project was renamed IAMUCLA/iamucla.

Enterprise Directory

The Enterprise Directory is the core of IAMUCLA services. It is where user identity and role data is collected, organized, and stored. In addition to serving the web single sign-on and access management data needs, the Enterprise Directory also feeds a variety of purpose-specific directories such as the UCLA Online Directory and the UC UDir system.

Federation

A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.

Federated sign-on allows a user to log in resources outside of using the credential she already has from her home organization.

UCLA is also a member of a US-wide higher education federation named InCommon.

Grouper

Grouper, Groups Management Toolkit, enables project managers, departments, institutions and end-users a way to create and manage institutional and personal groups. It puts the control of a group in the hands of its steward and enables the person to manage the membership and what resources it can access. This software works in conjunction with Signet to manage permissions by enriching identity attributes. UCLA is a member of a federation called UCTrust, within InCommon.

IAMUCLA is adopting Grouper.

Visit the official Grouper web site for more details.

Help Desk Contact

The people who are responsible for fielding calls, emails and questions from users regarding the operation of an application.

IAMUCLA

IAMUCLA is a set of tools helping campus applications manage the process of establishing who you are and what access you have in a way that is simplified, structured, and streamlined.

The Identity Management aspect of the framework 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. 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. 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, i.e. at the end of a staff member's employment. Click for more information.

**Identity Provider (IdP)**

An Identity Provider (IdP) is a campus or an organization that manages and operates an identity management system and offers information about members of its community to resources integrated with the identity management system.

In Shibboleth term, an Identity Provider is the software component responsible for logging in a user during authentication. It is also responsible for asserting information about the signed-in user to resources. Typically, each institution has one IdP, and it is usually operated by the institution's Identity Management Office.

AIS operates UCLA's Shibboleth Identity Provider.

**InCommon**

InCommon is a federation that creates and supports a common framework for trustworthy shared management of access to online resources in support of education and research in the United States.

InCommon eliminates the need for researchers, students, and educators to maintain multiple passwords and usernames. Online service providers no longer need to maintain user accounts. Identity providers manage the levels of their users' privacy and information exchange. InCommon uses SAML-based authentication and authorization systems (such as Shibboleth) to enable scalable, trusted collaborations among its community of participants.

UCLA is an active member of InCommon and operates an Identity Provider.

For complete details, visit the InCommon Federation web site.

**ISIS**

Integrated Security Information System (ISIS) is UCLA's web single sign-on solution. It is a home-grown system originally developed in 1996, and is currently used by over 200 web applications throughout UCLA.

ISIS is being replaced by an Internet2 standards-based solution called Shibboleth. The replacement is expected to complete by the end of 2009.

**Service Provider (SP)**

Service Provider (SP) is a campus or an organization that makes online resources available to users.

In Shibboleth term, a Service Provider is the software component installed on the resource serving application server. The SP is responsible for communicating with the Shibboleth Identity Provider to ensure that only properly authenticated individuals can retrieve the protected resource.

Click here for a Shibboleth video demonstration.

**Shibboleth**
Shibboleth is a standards-based, open source middleware software designed to provide web Single Sign-On (SSO) and user attribute exchange within or across organizational boundaries. It is the new version of ISIS and performs a similar function, but with a more enriched feature set such as detailed attribute release controls.

Visit the Internet2 Shibboleth web site for additional information.

Click here for a Shibboleth video demonstration

**Signet**

The Signet Privilege Management System enables consistent application of policy and business access rules across managed services. It places the control of a resource in the hands of its steward. This software works in conjunction with Grouper to manages permissions by better implementing access policy.

UCLA intends to adopt Signet as its enterprise permission management tool.

Visit the official Signet web site for additional information.

**Single Sign-On**

Single sign-on is the act of logging once and having seamless access to all participating resources one has access to without logging in again during the same session.

Single sign-on should not be confused with having a single, common logon ID. One can have a single logon ID capable of logging into multiple resources, but not having single sign-on across these resources. For example, when connecting to the UCLA wireless network, a student logs in using her UCLA Logon via a browser page. When she visits MyUCLA, she's prompted again to enter the same ID/password. In this case, it is said that the student has a “single logon ID”, but is not experiencing single sign-on.

**Technical Contact**

During Service Provider(SP) integration with Shibboleth, the Technical Contact are the people who are responsible for communicating with the IAM UCLA Team's Technical support regarding issues such as code changes, attribute needs and test cases.

**UCLA Logon ID**

The UCLA Logon ID is UCLA's main electronic credential. It is used to sign into most UCLA services, including over 200 web applications, the campus wireless network, Bruin Online email and VPN services, and computer lab workstations. Click for more information

**University of California Office of the President (UCOP)**

The Office of the President is the systemwide headquarters of the University of California, managing its fiscal and business operations and supporting the academic and research missions across its campuses, labs and medical centers.

*definition transcribed from the Official UCOP website*
**UCTrust**

UCTrust is the University of California's Identity Management Federation. UCTrust enables authorized campus individuals to use their local campus electronic credential to gain access, as appropriate, to participating services (Resource Providers) throughout the UC system. UCTrust is based on industry standard technologies and a common set of identity attributes and identity management practices.

UCLA is an active member of UCTrust. For additional details regarding UCLA's involvement with UCTrust, contact Albert Wu, Manager of Middleware Infrastructure Group.

The UCTrust web site contains additional information about the federation.

**UTIPP**

UTIPP is an acronym for the University Technology Infrastructure and Productivity Plan. In 2002, the plan was structured to support a core strategy that would enhance the university's existing systems, adding newer web-based interfaces and back-end database designs. It is succeeded by UTIPP2 in 2007 addressing practical upgrades to the university's financial systems.

**Where Are You From (WAYF)**

A server used by the Shibboleth software to determine what a user's home organization is.

*definition transcribed from InCommon Glossary*