



IS-11 Identity and Access Management

Date

Refer questions to Information Resources and Communications

DRAFT – FOR COMMENT ONLY

Table of Contents

I.	Purpose	2
II.	Definitions	2
III.	Introduction	2
IV.	Identity Management Concepts and Core Functions	3
	A. Identification	3
	B. Credentialing and Registration	3
	C. Authentication	4
	D. Authorization	4
	E. Levels of Assurance (LOA)	4
	F. Enterprise Directory Services	4
	G. Single Signon Systems	5
V.	Roles and Responsibilities for Identity and Access Management	5
	A. Credential Providers	5
	1. Identify Proofing	6
	2. Registration	6
	3. Authentication	7
	4. Enterprise Directory	7
	B. Resource Providers	8
	C. Accountability	8
VI.	Federated Identity and Access at UC	9
VII.	Major Responsibilities	10
	A. Systemwide	10
	B. Campus	10
	C. Divisions and Departments	10
	D. Individuals and Community Members	10
VI.	References	11
	Appendix A - Definitions	12
	Appendix B – UTrust Requirements	12

I. Purpose

Access to and use of University electronic information resources must be performed in a manner that ensures the integrity, availability, privacy, and confidentiality of University resources and such actions must be conducted in full compliance with federal and state law and University policies. Access to University resources may be granted only to those individuals who have been authorized to have such access, and access must be accomplished by means of physical and/or technical access controls in conformance with University security policy and standards.

A summary of identity and access management requirements are described in the Guidelines for Stewardship of Electronic Information Resources, in support of the University of California Policy on Stewardship of Electronic Information Resources. This bulletin provides more specific recommendations for identity and access management.

These guidelines apply equally to all University campuses, medical centers, UC-managed national laboratories, and the Office of the President. Additionally, all faculty, staff, students, and authorized guests or visiting scholars are responsible for conformance with these guidelines as appropriate to their roles and assigned responsibilities.

II. Definitions

The following terms used in these Guidelines are defined in Appendix A.

Authorized Individual
Credential Providers
Electronic Information Resource (Resource)
Resource Providers

III. Introduction

Identity management describes the integration of workflow, process, and technology that enables the tracking of individual community members throughout their affiliation with the University. Identity and access management (IAM) employs critical security-based technology components and process that simultaneously utilize centralized management of information about community members and automate the processes that enable reliable authorized access to services and resources, while protecting confidential information from unauthorized access. A carefully constructed IAM system enables the University to effectively achieve its security objectives and auditable compliance with regulations regarding authorized access.

Identity and access management should be based on a set of principles and control objectives:

- to ensure exact identification of members of the University community and assignment of access privileges,
- to allow access to Resources only by Authorized Individuals,
- to ensure periodic review of membership in the community and review of their authorized access rights,
- to maintain effective access mechanisms through evolving technologies.

Secure and compliant operations rely on a well-managed IAM system that protects online resources and user privacy while enabling ease of use. Identity and access management should answer questions such as:

- Are the individuals using these services who they claim to be?
- Are they members of our campus community?
- Have they been granted permission to access these specific services?
- Is their personal information adequately protected?
- Do their authentication credentials meet established security standards?

Identity and access management applies a set of business rules to this total view of community to make decisions about identity and rights of access for each member of the community.

Access to Resources that have been determined to be *restricted* or *essential* may have specific access control requirements. See IS-2, Inventory, Classification, and Release of University Electronic Information for guidelines regarding classification of *restricted* and *essential* Resources. See IS-3, Electronic Information Security, section III.C.2, Operational and Technical Controls for access control guidelines.

IV. Identity Management Concepts and Core Functions

IAM systems typically include the following functions.

A. Identification

Identification is the process by which information about an individual is obtained. The nature and reliability of the identification process supports some level of assurance that individuals are who they claim to be. Generally, this identity verification takes place within the office (e.g., Human Resources or Student Services) that first encounters the individual and creates their record within the institutional system(s) of record.

B. Credentialing and Registration

Credentialing is the process whereby an individual is issued digital credentials (identifier and authentication credential) for the individual's use to access Resources. Registration describes the binding of the digital credentials to data maintained about the individual in the repository that supports the authentication process (see IV.F. Enterprise Directory Services).

C. Authentication

Authentication is the act of confirming the identity of an individual by verification of the digital credentials presented by the individual when accessing a Resource. An *authentication credential* may be:

- something the individual knows, such as a password, passphrase, or other secret information,
- something the individual has, such as a smart card with a public-key certificate,
- something that is biologically part of the individual, such as a fingerprint or a retina.

D. Authorization

Authorization is the process of controlling an individual's access to resources. Initial decisions regarding rights of an individual's access to Resources may be determined by administrative procedures or role-based privilege management. See IS-3, Electronic Information Security section III.C.1 Administrative Workforce Controls.

E. Levels of Assurance (LOA)

The term "level of assurance" describes the degree of certainty that the individual who uses digital credentials (identifier and authentication credential) is who he/she claims to be at the time of the authentication event. Assurance may be determined by factors such as:

- the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued,
- the degree of confidence that the individual who uses the credential is the individual to whom it was issued,
- the degree of confidence of the security of the data exchange, and
- the degree of confidence that the authentication credential has not been shared with untrusted services.

Resource Providers may implement requirements for meeting specific LOA requirements for Authorized Individuals to access their services.¹

F. Enterprise Directory Services

Enterprise Directories contain identity information about individuals who have been authorized to join the campus community. Enterprise directory services provide an essential infrastructure component that supports authentication and authorization to Resources. Enterprise directories may serve as repositories for digital credentials or may be integrated with systems that inform authentication or authorization events.

¹ See Section 7 in the NIST Special Publication 800-63, Electronic Authentication Guide.

G. Single Signon Systems

Single Signon (SSO) describes the process that allows an individual to enter one set of digital credentials for access to multiple Resources. This may be accomplished either through

- portal technologies, which, for a period of time, passes the digital credentials to another service or
- by use of a single set of digital credentials for access to multiple resources.

Use of SSO in portals may remove the need for an individual to enter further authentication credentials when switching from one Resource to another, but it may also increase security risks. When appropriate, Resource Providers should consider the need to implement a higher level of assurance or two-factor authentication to add a measure of greater security for access to their Resources.

V. Roles and Responsibilities for Identity and Access Management

Identity and access management systems serve as a critical component of the campus security infrastructure. Campuses should work toward the development of systems and procedures to provide core automatic mechanisms that:

- insofar as possible, capture identity information from institutional repositories of information,
- ensure timely provisioning and de-provisioning of access rights,
- offer self-service to facilitate individual's timely update of personal information and authentication credentials,
- ensure compliance through logging, auditing, and reporting.

A. Credential Providers

Credential Providers are the campus authorities responsible for the management of electronic identity information and for providing identity information and authentication services for their campus locations.

Each of the UC campuses, medical centers, and UC-managed national laboratories should designate an authorized Credential Provider to be responsible for the campus IAM system that provides identity information and authentication services for its location.

When there is close affinity between locations, such as a campus and its medical center, it is recommended that they share a Credential Provider since implementing separate Credential Providers could cause confusion for individuals who belong to both communities.

Credential Providers are responsible for protection and authorized release of personal identity information consistent with law and University policy.

See [RMP-8, Legal Requirements on Privacy of and Access to Information](#). For guidelines governing release of student information, see Policies Applying to Campus Activities, Organizations, and Students, [Section 130.00](#).

Credential Providers are responsible for the following elements.

1. Identity Proofing

Verification that individuals can prove who they say they are is fundamental to identity and access management since conducting the business of the University is ultimately about who is authorized to take certain actions.

- Individuals' identity information may be entered into institutional repositories through a variety of processes, such as during an application process, but insofar as possible, identification procedures should require that individuals present a government issued ID containing their picture and including an address or record of nationality, e.g., driver's license or passport, before the individual is authorized to become a member of the campus community.² Note that the degree of confidence that the individual is who he/she claims to be influences the level of assurance of digital credentials.

2. Registration

Since the process for vetting identity is closely related to the credentialing or registration process, the process for coupling credentials to an identity should ensure accurate binding between the individual and the credentials.

- Registration procedures should ensure that the *identifier* of an individual, that is the electronic name (e.g., nickname, handle), is accurately associated with directory information about the individual.
- Registration procedures should ensure that the *authentication credential* (e.g., password) meets campus standards as required in IS-3, Electronic Information Security, section III.C.2.B Access Controls.
- Registration procedures should ensure that the electronic *authentication credential* is accurately bound to the individual's identifier and is issued by secure means only to the correct individual.

² Identity of employees must conform with UC hiring policies and practices.

- Credential Providers should provide mechanisms that allow Resource Providers to implement timely provisioning and de-provisioning (termination) for Authorized Individuals' access to Resources.
- Where appropriate, Credential Providers should manage role information for Resource Providers who grant access based on predefined roles, such as "student," "staff," "faculty," or "guest."

3. Authentication

- Credential Providers should document their authentication service. Documentation should include the level of assurance associated with their authentication credential and the practices used to achieve that level of assurance.
- The act of verification of the digital credentials presented by the individual when accessing a Resource should be adequately protected.
 - Appropriate encryption must be used to protect the privacy of the exchange when digital credentials are transmitted during authentication.
 - Measures should be established to prevent resource providers from having access to authentication credentials without prior authorization.

4. Enterprise Directory

Although derived from distributed sources, the enterprise directory should be managed centrally. Principles that enable the tracking of individuals through each phase of their affiliation with the campus, such as applicant to student, student to staff, or student to alumni, should be observed. Procedures that ensure accurate life cycle management of community members are a necessary component of enterprise directory management.

- Wherever possible, electronic information about individuals, including guests, in the enterprise directory should be maintained according to established business practices that ensure the proper verification of identities, facilitate automatic role assignment, and facilitate automated provisioning and deprovisioning of services.

- Procedures should be established that enable timely and accurate update of directory information and authentication credentials.
 - The process of maintaining employee information should be integrated with University employment processes.
 - The process of maintaining student information should be integrated with student registration processing.
- Granting access rights must be consistent with University policy regarding allowable users (see section III.C, Electronic Communications Policy).

B. Resource Providers

Resource Providers are the organizational units that manage electronic information resources that are accessed by Authorized Individuals. These resources are generally network-based, but may not necessarily be so.

1. Resource Providers are responsible for appropriate protection of the information resources over which they have jurisdiction or control. For example:
 - Resource Providers should establish procedures ensuring that only Authorized Individuals are permitted access to their Resources. For authorization management guidelines regarding workforce controls see section III.C.1, Administrative Workforce Controls in IS-3, Electronic Information Security.
 - Resource Providers should ensure appropriate access control measures consistent with IS-3, section III.C.2, Operational and Technical Controls.
2. Resource Providers are responsible for protecting identity information they receive as part of the authorization and authentication processes.
3. Resource Providers may also implement additional measures to enhance credential provider's level of assurance if Resource Providers require a higher level of assurance than that given by the Credential Provider.

C. Accountability

Administration of IAM systems requires that:

1. Credential Providers implement procedures that ensure the documentation and appropriate retention records linking individuals' names with their identification information in enterprise directories.

2. Resource Providers implement appropriate audit logs that document individual access to Resources and the authorization permissions granted to individuals

Retention of audit logs

Log records provide essential detailed information that document many activities supporting information resources, such as the creation or editing of identity records, or recording of process transactions. Procedures for the retention of log records should be well-defined to provide an appropriate balance among the following:

- confidentiality of specific individual's activities,
- the need to support investigations,
- the cost of retaining the records.

When logs document or contain valuable information related to activities of the University's information resources or the people who manage those resources, they are University *Administrative Records*, subject to the requirements of the University Records Management Program. See [RMP-2, Records Retention and Disposition](#) and IS-3, Appendix C, Log Management.

VI. Federated Identity and Access at UC

At the University of California, there may be need for community members from one campus to access services from another UC campus. Federated identity systems offer considerable benefits in efficiency and security.

- convenience: individuals can access services of participating institutions using their local campus electronic credentials.
- efficiency: federated systems reduce the overhead of maintaining multiple administrative tasks required for account maintenance since they utilize automated authentication and authorizations mechanisms.
- privacy: federation reduces the need for creating multiple data stores of personal information. Participating campuses must ensure the protection of personal information through secure access channels.

The University of California [UCTrust](#) service utilizes a federated approach to allow access to another campus by the use of authoritative identity information from the home location. It enables authorized campus individuals to use their local campus electronic credentials to gain access, as authorization permits, to participating services throughout the UC system.

See Appendix B for UCTrust participation requirements for both Credential and Resource providers.

VII. Major Responsibilities

A. Systemwide

The Associate Vice-President – Information Resources and Communications, Office of the President is responsible for these Guidelines.

The Information Technology Leadership Council, whose membership is appointed by Chancellors, medical center directors, and UC managed national laboratory directors, works in partnership with the UC academic and administrative leadership to identify systemwide and common campus implementation strategies.

B. Campus

Chancellors, and for the Office of the President, the Senior Vice President, Business and Finance, are responsible for delegating responsibility for implementation of these Guidelines at their respective locations.

C. Divisions and Departments

Division deans, department chairs, and appropriate administrative officials are responsible for establishing pertinent procedures and identifying appropriate practices to achieve departmental compliance with campus implementation recommendations.

D. Individuals and Community Members

Community Members are the individuals who have officially established an affiliation with a campus. They are the individuals who use the Resource Providers' services and whose electronic identity is managed by Credential Providers.

Community Members are responsible for protection of the digital credentials provided to them by their Credential Provider. In particular, they are each individually responsible for:

- assurance that their credentials are not held by other people.
- compliance with Credential Providers' standards and best practices for use and protection of identity information.

Community Members are also responsible for conformance with Resource Providers' standards and best practices.

Community members are expected to comply with campus policies and procedures and to exercise responsibility appropriate to their position and delegated authorities. Each individual is expected to conduct the business of the University in accordance with the Statement of Ethical Values and the Standards of Ethical Conduct, exercising sound judgment and serving the best interests of the University.

VI. References

- Policy on Stewardship of Electronic Information Resources
- Guidelines for Stewardship of Electronic Information Resources
- IS-2, Inventory, Classification, and Release of University Electronic Information
- IS-3, Electronic Information Security
- Policies Applying to Campus Activities, Organizations, and Students, [Section 130.00](#).
- [RMP-2, Records Retention and Disposition](#)
 - [RMP-8, Legal Requirements on Privacy of and Access to Information](#)

Appendix A - Definitions

Authorized Individual

A University employee, student, or other individual affiliated with the University who has been granted authorization by the Resource Proprietor, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the University. The authorization granted is for a specific level of access to the Resource as designated by the Resource Proprietor, unless otherwise defined by University policy.

Credential Providers

Credential Providers are the campus authorities responsible for the management of electronic identity information and for providing identity information and authentication services for their campus locations.

Electronic Information Resources (Resource)

An electronic information resource used in support of University activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer server, desktop (workstation), communications and other hardware used to conduct activities in support of the University’s mission. These resources may also be called “information assets.”

Resource Providers

Resource Providers are the organizational units that manage electronic information resources that are accessed by Authorized Individuals. These resources are generally network-based, but may not necessarily be so.

APPENDIX B – UCTRUST REQUIREMENTS

A complete description of UCTrust: The University of California Identity Management Federation is available at <http://www.ucop.edu/irc/itlc/ustrust/>.

9. MINIMUM REQUIREMENTS AND SERVICE LEVELS

Members must join InCommon.

InCommon maintains a table of Common Identity Attributes, which are recommended for participation in InCommon. UCTrust maintains an additional set of common identity attributes that are required for participation in UCTrust, such as UCnetID, at <http://www.ucop.edu/irc/itlc/ustrust>. This list contains a description of each attribute assertion of identity information to be used in UCTrust, including data format and the URN that uniquely names the attribute. It also contains rules for governing release and use of all attributes.

UCTrust implements different *levels of assurance* from InCommon. A level of assurance describes the policies and practices that have been applied to a particular identity assertion. This level of assurance can be used by Resource Providers to determine their confidence in the identity information they received. As of this writing, one UCTrust level of assurance, *UCTrust Basic*, has been defined.

In particular, UCTrust-conforming identity assertions must include a multivalued attribute, `urn:oid:2:16:840:1:113916:1:2:1:1`, along with associated values of the form `urn:mace:universityofcalifornia.edu:ucidentity:attributes:assurance:*` to indicate when specific UCTrust policy requirements have been met. For example, `urn:mace:universityofcalifornia.edu:ucidentity:attributes:assurance:basic` must be asserted when the *UCTrust Basic* requirements have been met. Credential Providers must assure that values for this attribute are asserted only when all corresponding UCTrust requirements are met. At such a time that there are multiple UCTrust levels of assurance, then all applicable assurance level values must be asserted.

9.1 Specific Requirements for Credential Providers

9.1.1 UCTrust Basic

- 9.1.1.1 Authentication, attribute, and other application services provided by the Credential Provider must be operated according to the requirements in Business and Finance Bulletin IS-3 for *restricted* and *essential* information resources. (IS-3 is available at <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>.)

- 9.1.1.2 The identity of individuals must be verified either by presentation of a government-issued photo ID as part of an established process of the Credential Provider, or through the University's official hiring process.
- 9.1.1.3 If campus identities exist that have not been verified according to current *UCTrust Basic* requirements, those identities must be re-verified prior to those individuals' use of UTrust.
- 9.1.1.4 If shared secrets, such as passwords, are transmitted during authentication, appropriate encryption must be used to protect the privacy of that exchange. These shared secrets are considered to be *restricted* information in the context of Business and Finance Bulletin IS-3.
- 9.1.1.5 In order to provide interoperability with Resource Providers, Credential Providers must implement the specific attributes identified in UCTrust: Common Identity Attributes (separate document)
- 9.1.1.6 The registration process for issuing credentials may be either in-person or remote:
- In-Person
 - A government or University issued ID with a picture must be presented to and verified by an officer of the Credential Provider as belonging to the registrant.
 - Remote
 - The registrant must be prompted for at least two identifying attributes that are verified as belonging to the registrant. The attributes should be chosen to be relatively accessible to the registrant, but not to others. Examples include employee or student ID, birth day and month, Social Security number, date of hire, *etc.*
 - The process should include a step to confirm existing records of the registrant's electronic mail address, telephone number, or postal address. For example, a confirming email or a letter sent to registrant's postal address requiring a response would suffice. This step should either precede issuing credentials or be capable of revoking already-issued credentials in a timely manner.
- 9.1.1.7 The registration process must include provisions to avoid the use of easily guessed passwords.
- 9.1.1.8 If a single sign-on system is utilized to alleviate the need for a user to provide a password for each application, session timeouts must be utilized to mitigate the risk presented by unattended workstations being used by unauthorized people.

- 9.1.1.9** Credential Providers must publish in a format accessible to participating Resource Providers:
- description of each attribute assertion of identity information that is available to UCTrust, including data format and the URN that uniquely names the attribute
 - rules for governing release and use of UCTrust attributes
 - description of the identification process that the campus uses to manage the repository of identity information for the campus community, linking the individual with the electronic identity and electronic credential, e.g., password, etc.
 - description of the registration process used to issue electronic credentials
 - description of authentication technology, e.g., Kerberos
 - description of the maintenance procedure used to ensure that identity information is current and synchronized with repositories of record, particularly as it relates to de-provisioning and revocation of permissions
 - a service level statement covering issues such as availability, responsiveness, security, timeliness and accuracy of information, log record maintenance, *etc.*
- 9.1.1.10** Credential Providers must provide a help desk function for problem resolution related to identity management and authentication.
- 9.1.1.11** These *UCTrust Basic* requirements for Credential Providers are identified in Shibboleth's SAML assertions as
`urn:mace:universityofcalifornia.edu:ucidentity:attributes:assurance:basic`

9.2 Specific Requirements for Resource Providers

- 9.2.1** Applications that utilize UCTrust must be compliant with all University policy regarding privacy, security, and application development.
- 9.2.2** Resource Providers are responsible for the security of their services; they must implement any additional authentication measures required for the criticality or sensitivity of the application or the data accessed by the application.
- 9.2.3** Resource Providers must address appropriate usability concerns prior to registration with UCTrust Federation Administration.
- 9.2.4** Resource Providers must provide a help desk function for problem resolution related to the application.

It is anticipated that higher levels of assurance will be implemented for UCTrust in the future. Those higher levels of assurance will include different sets of requirements.

10. TECHNICAL SPECIFICATIONS

Each Credential Provider and Resource Provider within UCTrust must be capable of exchanging attribute information with other members' Credential Providers and Resource Providers through the use of the protocols, formats, and software required by InCommon. The use of the Internet2 implementation of Shibboleth is highly recommended.