

UCTrust
University of California Identity Management Federation
Service Description and Policies
March 27, 2007

1. INTRODUCTION

UCTrust is an organization that provides the basis for a unified identity and access management infrastructure for the University of California system. 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. (For the purpose of this document, the word “campus” refers to campuses, medical centers, national labs, and all other UC locations.) UCTrust is based on industry standard technologies and a common set of identity attributes and identity management practices.

2. BENEFITS of UCTrust

- UCTrust enables cost-effective, privacy-preserving collaboration among participating UC campuses. It makes it easier to share protected online resources and eliminates the need for each Resource Providers to maintain separate password-protected accounts.
- UCTrust supports individuals' access to protected resources by allowing Resource Providers to make decisions about granting access to their resources based on authoritative information offered by the individual's campus regarding that individual's status or local privileges. Authoritative information about people at a campus is maintained by a single Credential Provider
- UCTrust offers a high level of security by utilizing strong controls over secure access channels. This high level of security also provides a secure mechanism for ensuring privacy in the exchange of identity attributes.

3. PRINCIPLES of UCTrust

A fundamental principle of UCTrust is that participating campuses provide authoritative and accurate identity information about individuals in their campus community. Adherence to uniform business practices in establishing electronic credentials and maintaining individual identity information is required. Equally important is the principle that Resource Providers receiving identity information protect it and respect the privacy constraints defined by the participating campus.

The local campus may use a “single sign-on” mechanism, or any method that supports local web-based applications. The individual's campus will then send only the required information about that individual to the requesting Resource Provider application. The Resource Provider's application will make an access decision based, at least in part, on the information it receives. The Resource Provider application retains complete control over its access management.

The current version of UCTrust is based on participation in Internet2's InCommon federation, using Shibboleth[®] technology. Shibboleth makes use of whatever local authentication system the campus supports, and handles the exchange of identity information among identity management systems and participating applications. More information on InCommon may be found at <http://www.incommonfederation.org/index.cfm>

UCTrust extends InCommon by affording a higher level of identity assurance for resources (*e.g.*, employee self-service) that have higher-level requirements for access control than those resources afforded by InCommon (*e.g.*, digital library resources). UTrust achieves this by establishing minimum standards for the identification, registration, and authentication of those campus community members who require access to resources with higher-level requirements. The technical infrastructure, however, is the same for both InCommon and UTrust.

4. GOVERNANCE

The University of California IT Leadership Council (ITLC) acts as the governing body of UTrust by providing direction for its operational policies, technology, and procedures, based on input it receives from the UTrust Workgroup and the UTrust Federation Administration.

5. PARTICIPANTS

Each of the University of California's campuses, medical centers, and national labs that have joined InCommon may become participants in UTrust. Participants join UTrust by registering their Credential Providers and Resource Providers with the UTrust Federation Administration.

Certification of compliance requires completion and submission of the UTrust Member Certification of Compliance form, Attachment A. The Credential Provider or Resource Provider should follow these steps to register a new Credential Provider or Resource Provider within UTrust:

1. The participant's ITLC representative and the Credential Provider or Resource Provider shall jointly certify ongoing compliance with the UTrust policies, principles and requirements set forth in this document. The Credential Provider or Resource Provider further attest continued compliance in all material respects with such policies, principles and requirements, as they may be amended, and the requirements of any other documents governing UTrust that may be adopted in the future, at all times while a participant in UTrust.
2. The participant's ITLC representative shall submit documentation of compliance with the Minimum Requirements identified in this Service Description to the UTrust Federation Administration for integration into UTrust's documentation and technical infrastructure.

Failure to demonstrate ongoing compliance with UTrust's policies, principles and requirements in all material respects that is not resolved in a timely manner will result in removal of that participant from UTrust.

It should be noted that it may be appropriate for multiple participants to share a Credential Provider when there is a close affinity among those participants with regard to community and/or identity management. For example, a campus and its associated medical center have many community members in common; implementing separate Credential Providers could cause confusion for people who belong to both communities. Also, a campus and its associated medical center may share a common payroll system, the repository of record for employees.

6. UTrust WORKGROUP

The UTrust Workgroup, composed of UTrust's Credential Providers and Resource Providers provides a forum for communication concerning UTrust's operational issues. It also advises the governance of UTrust in the areas of technology, operations, and policy. The Workgroup's business is conducted by electronic mail with occasional face-to-face meetings.

7. UCTrust FEDERATION ADMINISTRATION

Administration of UCTrust is conducted by Information Resources and Communications at the Office of the President. Duties include:

- Facilitate participation in UCTrust
 - assist UCTrust participants to complete their required documentation
- Maintain information repository
 - UCTrust service description requirements
 - metadata describing Resource Providers
 - descriptions of UCTrust-specific attributes
 - technical support contact information for all Credential Providers and Resource Providers in a form accessible to each
- Facilitate periodic meetings of the UCTrust Workgroup to discuss operational issues and provide input to the ITLC regarding governance issues.
- Assist problem resolution between Credential Providers and Resource Providers.

8. RESPONSIBILITIES

Responsibility for participation in and administration of UCTrust lies with the following entities:

8.1 *Credential Provider*

Credential Providers are the campus organizational units that manage electronic identity information and provide identity information and authentication services for their campuses/sites.

Credential Providers are responsible for a campus's enterprise directory that is, the campus's repository of information about the members of its community. Credential Providers are also responsible for the identification, registration, and authentication processes that bind specific Community Members to the information about those members in the enterprise directory. In particular, Credential Providers are responsible for:

- *accuracy and timeliness* of information in the enterprise directory
- *privacy* of information in the enterprise directory This requires a registration process by which Resource Providers are authorized to utilize identity information.
- *availability* of the network-based services that provide access to information in the enterprise directory.
- *accuracy of the binding* of Community Members to information in the enterprise directory. This includes:
 - the identification and registration processes, which result in the issuance of electronic credentials (e.g., user ID and password) to Community Members.
 - the authentication process, which verifies possession of credentials within each session.
- *tools and procedures* for community members to update their identity information, such as passwords.

- *audit logs* that enable investigation of security incidents and misrepresentation of identity.
- *education* about standards and best practices for the campus's Resource Providers and Community Members in the use and protection of identity information
- *standards, best practices, and education*, consistent with the UTrust requirements, that guide the behavior of Resource Providers and Community Members in the use and protection of identity information.
- *help desk function* for community members to resolve issues.
- *technical support contact* for Resource Providers and UTrust Federation Administration

As part of the membership requirements for UTrust, Credential Providers provide documentation describing their compliance with these responsibilities. The UTrust Federation Administration maintains a repository of this information. (*Appendix A: UTrust Member Documentation* contains a template for the required documentation.)

8.2 Resource Providers

Resource Providers are the organizational units that manage electronic information resources that have been registered with UTrust. These services are generally, but not necessarily, network-based. (Resource Providers are also called Shibboleth Targets or Relying Parties.)

Resource Providers are responsible for the secure operation of their services. With respect to their use of identity information, they are responsible for:

- *awareness of Credential Providers' service levels*. When multiple levels are available (or negotiable), selection of appropriate service levels to meet the service's needs. When a sufficient service level is not available from the Credential Provider, the Resource Provider may need to implement its own identity management services in order to meet its service's security requirements.
- *audit logs that enable investigation* into security incidents related to information provided by Credential Providers.
- *compliance with Credential Providers standards and best practices* for use and protection of identity information.
- *technical support contact* for inquiries from Credential Providers and the UTrust Federation Administration.

8.3 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 electronic 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.

The reciprocal relationship between Credential Providers and Resource Providers affects their mutual responsibilities for security. Credential Providers must act in conformance with their stated service and assurance levels so that Resource providers may meet their policy, legal, and fiduciary requirements. Resource Providers must provide adequate protection for the sensitive identity information received from Credential Providers in order for the Credential Providers to meet their policy and legal requirements.

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. UTrust maintains an additional set of common identity attributes that are required for participation in UTrust, 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 UTrust, including data format and the URN that uniquely names the attribute. It also contains rules for governing release and use of all attributes.

UTrust 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 UTrust level of assurance, *UTrust Basic*, has been defined.

In particular, UTrust-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 UTrust policy requirements have been met. For example, `urn:mace:universityofcalifornia.edu:ucidentity:attributes:assurance:basic` must be asserted when the *UTrust Basic* requirements have been met. Credential Providers must assure that values for this attribute are asserted only when all corresponding UTrust requirements are met. At such a time that there are multiple UTrust levels of assurance, then all applicable assurance level values must be asserted.

9.1 *Specific Requirements for Credential Providers*

9.1.1 *UTrust 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 *UTrust 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. AUDIT

UCTrust Credential Providers and Resource Providers will be audited periodically to provide independent assurance of compliance with the applicable policies, principles, and requirements of UCTrust. In particular, Credential Providers will be audited at least once every two years, and Resource Providers will be audited at a frequency to be determined by the ITLC. These audits may be performed either by UC Internal Audit or other qualified independent auditors. The audit results will be reported to the ITLC, the governing board of UCTrust, and shared with Resource Providers and Credential Providers upon request.

11. 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.

12. BEST PRACTICES

12.1 *Synchronization with Repositories of Record*

- Establish processes that maintain close synchronization of Employee affiliations in the identity management repository with the corresponding records in the campus's instance of the Payroll / Personnel System (PPS). Changes should be reflected in the identity management repository within 24 hours, if not sooner.
- Establish processes that maintain close synchronization of Student affiliations in the identity management repository with the corresponding records in the campus's student information system. Changes should be reflected in the identity management repository within 24 hours, if not sooner.
- In general, when there is an existing repository of record for an identified category of users, synchronization should be maintained within an appropriate time interval.

12.2 *Multi-Factor Authentication*

- When UCTrust does not provide sufficient assurance for a particular service, as determined by the Resource Provider, the Resource Provider should use Multi-Factor Authentication to attain that higher level of assurance. For example, after receiving UCTrust's assertion of a user's identity, a high-security service could require possession of a hardware token (e.g., a smart card) or request that the user provide some shared secret.
- Possible sources for shared secrets include a) the answer to a question previously provided by the user, and b) one or more pieces of information that are well-known to the user, but not to others,
- An option for community member to use a secondary credential for validation when accessing one's own personal information may be implemented by a Resource Provider to provide the community member a choice between convenience and security. Note that this will likely require an audit log entry by the Resource Provider.

12.3 *User Interface Design*

- There is a certain amount of "bouncing" of community members between Credential Providers, Resource Providers, and the "Where Are You From?" (WAYF) server that is inherent in the technology. Care should be taken to mitigate the confusion this may cause.
- Where possible, campuses should structure login processes to occur when community members initiate network sessions. The process should also interact with the

InCommon WAYF to declare the “origin” institution without user interaction later in the session.

- Provide clear indications of the help desk that should be contacted for problems that may occur at each step.
- It is highly recommended that both Resource Providers and Credential Providers conduct usability studies to identify confusing aspects of their user interfaces.

Appendix A: UTrust Member Certification of Compliance

In order to be registered with UTrust, a Credential Provider or Resource Provider must send a certification of compliance with the requirements in the document to the **UTrust Federation Administration in the Department of Information Resources and Communications at the UC Office of the President**. This certification should contain the following language, with a name or brief description of the Credential Provider or Resource Provider provided. For example, "UC Irvine's Credential Provider," or "At Your Service Online (AYSO)."

Statement of Compliance

To: Associate Vice President, Information Resources and Communications, UCOP
Information Resources and Communications
University of California
1111 Franklin Street, 7th Floor
Oakland, CA 94607-5200
FAX: (510) 451-4340

The undersigned certify that [name or brief description of the Credential Provider or Resource Provider] _____ complies with the policies, principles, and requirements of UTrust, as described in *UTrust University of California Identity Management Federation Service Description and Policies*.

The undersigned acknowledge that compliance with the policies, principles and requirements of UTrust, as they may be amended, is subject to periodic inspection and audit. Failure to demonstrate ongoing compliance with such policies, principles and requirements in all material respects that is not resolved in a timely manner will result in the revocation of the provider's participation in UTrust.

The following information is included in this certification.

- Attached: A copy of the *InCommon Federation: Participant Operational Practices* statement that was provided when joining InCommon
- Contact information for the Credential Provider's or Resource Provider's help desk:
 - Organization Name:
 - E-mail:
 - Telephone Number:
 - Fax Number:
- The Uniform Resource Identifier (URI) that identifies this Credential Provider or Resource Provider within InCommon: _____

Signature and Title, Credential Provider or Resource Provider

Date

Signature and Title, Campus Chief Information Officer

Date

cc: Campus Controller