UCHastings/UCTrust MINIMUM REQUIREMENTS AND SERVICE LEVELS

Among the requirements for our joining the UCTrust identity management federation, we are required to post and maintain our responses to a series of questions in Section 9 of the **University of California Identity Management Federation Service Description and Policies (March 27, 2007).**

The following are up-to-date responses by UC Hastings to the Section 9 questions.

. . .
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/uctrust. 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.)
UC Hastings' procedures are generally in accord with Business and Finance Bulletin IS-3.

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.
This is true for all employees given UCTrust Basic Assurance status by us. Adjuncts, for instance, don't go through this procedure. Contract employees and temps do not. They do not receive "basic" status. Student IDs are verified through LSAC processes (http://www.lsac.org/jd/lsat/day-of-test.asp). Also, they are required to show official IDs to both the Fiscal Department and the Records Department in order to get the Hastings ID card. They receive "basic" status.
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 UCTrust.
No such employees will receive a UCTrust Assurance level of "basic" from us. The UCTrust Assurance attribute value will be empty.
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.
All Shibboleth/SAML and CAS communications are encrypted (over SSL). We are using encrypted connections (SSL) to Hastings AD. But note that the Shibboleth IdP is not handling the password itself, since we have it layered over CAS. So the CAS Server is checking the user's password against AD by using an encrypted connection (LDAPS). The Shibboleth IdP receives the user identity from CAS over an encrypted channel, and then the Shibboleth IdP itself connects to the campus AD through an encrypted connection (LDAPS) to retrieve the additional attributes about the person.
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.

This approach is used for faculty and staff who receive the UCTrust Assurance status "basic" from us.

- 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.

These approaches are used by the Admissions Department, the Fiscal Department and Records Department prior to the students arriving on campus, and we create accounts at the Admissions

Department's order. Additionally, if the IT Department has to issue a new password to a student, staff or faculty member, we use either the "in-person" or one of the two "remote" methods described above to verify the identity of the requester.

9.1.1.7 The registration process must include provisions to avoid the use of easily guessed passwords.

The password rules that are being phased in for all new students are the following: password must not contain spaces, be 8 characters or longer, must contain an upper and lower case letter, at least one number, and one symbol (e.g. one of ?!@#$%&&*). Example: 5eR%1seuj. In the near future we will be bring these rules into effect for all existing users.

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.

Almost all the school's unattended workstations are in the Library Learning Resource Center. Via Windows Group Policy, there is automatic session timeout enforced after 15 minutes of inactivity. There are several other unattended workstations that need to be integrated into this session timeout system. Hastings is running two single sign-on systems, a Shibboleth Identity Provider and a CAS Server. The Shibboleth Identity Provider relies on the CAS Server for SSO session management, and maintains no SSO session itself. The CAS Server restricts user sessions to both a maximum lifetime and to an "idle timeout" (no activity within a specific amount of time will cause the session to expire); once either of those cause the user's session to "expire", the user will need to re-authenticate to access a service.

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

"urn:oid:2.16.840.1.113730.3.1.241"= "displayName"
"urn:oid:2.5.4.3"= common Name
"urn:oid:2.5.4.4"= surname
"urn:oid:2.5.4.42"=givenName
"urn:oid:2.16.840.1.113916.1.1.6"=employee ID
"urn:oid:2.16.840.1.113916.1.1.5"=UCTrust Assurance
"urn:oid:1.3.6.1.4.1.5923.1.1.1.6"=EPPN
"urn:oid:0.9.2342.19200300.100.1.3"=email Address
"urn:oid:1.3.6.1.4.1.5923.1.1.1.1"= eduPersonAffiliation
"urn:oid: 1.3.6.1.4.1.5923.1.1.1.5 "= eduPersonPrimaryAffiliation

As defined in document: internet2-mace-dir-eduperson-201203;
http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html

• rules for governing release and use of UCTrust attributes
Depending on the needs of the particular UCTrust Service Provider, we may release any of the above attributes to them. We require that they not release this information to third parties.
• 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.

o Accounts given the UCTrust Basic Assurance status by us are created by the IT Department at the request of the HR Department or the Admissions Department. The HR Department is responsible for verifying the identity of staff and faculty upon hiring, following the rules of the Department of Homeland Security, and the Admissions Department utilizes the LSAC processes plus bank deposits to verify the students' identities.
o For accounts that are not given the UCTrust Basic Assurance status, other means of identification are utilized, and they do not meet the rigorous standards in effect for staff, faculty and students.

• description of the registration process used to issue electronic credentials

For staff and faculty, the hiring department sends to the IT Department the name and credential requirement. The IT Department creates the electronic credential and delivers it personally to the staff or faculty person upon being introduced to the person by lead staff of the hiring department. For students, the Admissions Department transfers the data from LSAC to our SIS, and sends confirming letters and then the credentials, etc., after payment of deposits by students. Once on campus, the students must identify themselves to the Fiscal Department and the Records Department in person with government IDs. They are then sent to the Public Safety Department for a photo ID. If any of these stages are missed, the departments can tell us to revoke the credentials.

• description of authentication technology, e.g., Kerberos

We use the Kerberos-based authentication technology built into Windows Server 2008R2. We also access the Active Directory authentication technology using secure LDAP (LDAPS), and are using the two SSO systems mentioned above, CAS and Shibboleth. CAS leverages AD for authentication using secure LDAP (LDAPS), and the Shibboleth Identity Provider leverages CAS for authentication.

• 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.

The hiring department and the Records Department (registrar) send out notices of every change of status or coming change of status for staff, faculty and students (i.e., those holding the UCTrust Basic Assurance level). Any change that would remove UCTrust Basic Assurance status is applied so that UCTrust Basic Assurance status for that person shall be removed within 24 hours of taking effect.

• a service level statement covering issues such as availability, responsiveness, security, timeliness and accuracy of information, log record maintenance, etc.

Hastings computer help personnel are available 24 hours/day, 7 days/week, 365 days/year for network emergencies (contact via the Hastings Public Safety Department). Routine help is available 5 days/week, 50 weeks per year at the Hastings IT Department, helpdesk@uchastings.edu, room 379, 200 McAllister Street, San Francisco. Logs are kept of the Shibboleth and CAS servers. We do not have a “high availability” structure for our identity systems. Malfunctions in the Shibboleth or CAS servers would result in some downtime in Shibboleth services or CAS single sign on services.

9.1.1.10 Credential Providers must provide a help desk function for problem resolution related to identity management and authentication.

All staff, faculty and students report their identity management problems to the IT Department’s helpdesk, which handles all these problems.

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.