

InCommon Federation: University of Alaska Participant Operational Principles

Participation in the InCommon Federation ("Federation") enables a federation participating organization ("Participant") to use Shibboleth identity attribute sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system fall under the purview of the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that Service Providers, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below. Additional information to help answer each question is available in the next section of this document. There is also a glossary at the end of this document that defines terms shown in italics.

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name *University of Alaska*

The information below is accurate as of this date *2009-06-25*

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following URLs

UA Board of Regents Policy and University Regulation: <http://www.alaska.edu/bor/policy-regulations/>

UA Student & Enrollment Services documentation on FERPA compliance: <http://www.alaska.edu/studentservices/ferpa/>

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name *David Bantz*

Title or role *Chief Information Architect; Manager, Identity & Access Management Services*

Email address *Q@alaska.edu*

Phone *+1 907 450 8314*

2. Identity Provider Information

The most critical responsibility that an Identity Provider Participant has to the Federation is to provide trustworthy and accurate identity assertions. It is important for a Service Provider to know how your electronic identity credentials are issued and how reliable the information associated with a given credential (or person) is.

Community

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an electronic identity? If exceptions to this definition are allowed, who must approve such an exception?

Records of current employees and students are extracted from our institutional Human Resources and Student Information Systems (both are components of SunGardHE's Banner) and provisioned unique identities in UA's IdM. Business practices routinely discover and flag instances of multiple ("duplicate") records for a single individual and mark those records as "bad." Identities based on "bad" records are removed from our IdM. An employee's identity is inactivated upon termination; a student's identity is inactivated after three sequential terms with no course registration. "Guests" may have identities created in our IdM through sponsorship by a recognized department. Only those granted specific administrative role in our IdM are technically able to add guests. Those roles are in turn granted through designated "security coordinators" at each institution. Departments are annually provided the names of people they are sponsoring and must explicitly request renewal for those identities to be retained.

2.2 "Member of Community" is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to anyone whose affiliation is "current student, faculty, or staff." What subset of persons registered in your identity management system would you identify as a "Member of Community" in Shibboleth identity assertions to other InCommon Participants?

Non-terminated employees and students registered in the current term.

Non-terminated employees include some who do not have a current assignment (for example, faculty on sabbatical or other leave). While some calendar days on the University calendar are not in any term, for purposes of determining whether a student is registered "in the current term", a date between terms designates the change from one term to the next. For some purposes, such as maintaining access to email and portal accounts, we allow students to authenticate and maintain access to accounts up to three terms after their last registration; we would consider using this extended subset for "member of community" for specific services or resources.

Electronic Identity Credentials

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database? Please identify the office(s) of record for this purpose. For example, "Registrar's Office for students; HR for faculty and staff."

As described in 2.1, current employees (faculty and staff) and students in our HR and Student information system of record (Banner) are automatically provisioned identities (currently via a once/day extract, but potentially more frequent data exports or database triggers). Employee records are entered only by the institutions' offices of human resources. Students may register in person through registrars, or entirely online; payment is required to complete registration. Unlike employees and students, identities of guests are typically not vetted; in addition to being designated a sponsored person with a responsible official sponsoring department in our IdM, their username and id are prefixed with the string "uaguest_" [which prefix may be changed but will retain distinguishability from any identifier of students and employees].

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

Entities in the IdM have passwords that are stored in MIT Kerberos KDC, which is the backend credential store of the UA Enterprise LDAP directory; we use the Duke University Kerberos plug-in for using the external KDC. Prior to October 2008 passwords were stored in the internal LDAP database; as these passwords are reset by users, their accounts are "kerberized." All active accounts should be kerberized by the end of CY2009.

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by

encryption (i.e., "clear text passwords" are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

We require connections to our LDAP and IdM web interfaces to use encrypted (https) sessions, so clear text passwords are not sent for LDAP authentication, for our CAS-like web central authentication service, nor, obviously, to the Kerberos KDC. We expect applications using LDAP or our web authentication service to receive and send passwords using encrypted communications only, but realistically cannot guarantee compliance.

Contacts:

*UA OIT Chief Information Security Officer Kerry Digou, sxkmd@email.alaska.edu or
UA OIT Chief Information Architect David Bantz, Q@alaska.edu*

2.6 If you support a "single sign-on" (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with "public access sites" is protected.

UA's central authentication service for web-based applications is not strictly speaking an SSO service; each application requests authentication. However, it is possible to authenticate to the service itself and then launch multiple subscribing services without explicitly re-authenticating. This SSO-like function will not be used for or available to InCommon Service Providers. Session time-outs are not in place. Sessions are terminated with close of browser window(s) for that service.

2.7 Are your primary electronic identifiers for people, such as "net ID," eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

Locally assigned identifiers and used within UA's IdM are intended and controlled to be unique for all time to the individual to whom assigned. (We do have legacy identifiers in use on some systems that have in the past been re-issued, but these are not used as unique identifiers within UA's IdM.) UA assigns a name-based "UA Username" and a number-like string "UA ID#" and a UID meaningful only internal to the IdM. Kerberos principals are UAID#@ALASKA.EDU. Sponsored accounts (guests) receive UA Username and UA ID# prefixed with the string "uaguest". UA Usernames may be changed if the person's legal name changes, but the old UA Username is not available for re-issue. UA ID# is intended and controlled to be permanent (does not change regardless of status of the person).

Electronic Identity Database

2.8 How is information in your electronic identity database acquired and updated? Are specific offices designated by your administration to perform this function? Are individuals allowed to update their own information on-line?

- *For employees and students: A person's legal name, preferred first name, student registration data (campus and program of each course, declared major and minor, credit hours), employment information (home department, employee type), assigned UA Username and UA*

ID# originate in and are updated from Banner only. These data in Banner may generally be edited only by UA's HR offices (for employees) and Registrar's offices (for students. Some employee data may be updated by the employee's departmental administration. Students may register and change registration on line.

- Information about email accounts assigned to an individual may be entered and updated by other individuals with the IdM role of email administrator. Email administrators are responsible for entering assigned email account information (address, authentication method, protocols supported) and may edit the mailRoutingAddress and advertised email address (each of which may have a different value).*
- Data not actively maintained in Banner HR or Banner SIS may be entered and updated by individual users; this includes: employee working title, secretary, office location, phone, advertised email address, URL, USPS mailing address. In addition, individuals may edit their mailRoutingAddress, assign themselves vanity email addresses routed to their mailRoutingAddress, and edit the email addresses advertised in the public directory.*

2.9 What information in this database is considered "public information" and would be provided to any interested party?

- For students who elect confidentiality of their records under FERPA: no data is public information; not even the existence of the record is public or would be confirmed even if an inquirer provides a identifier.*
- For other students: UA has designated "directory information" that includes name, campus, major or program of study, email address; this is the data that would be provided and is available via our public electronic directory.*
- For employees: name, home and other departments or units with which affiliated, working title, email, campus (office) location(s), phone(s), mailing address, administrative contact ("secretary" attribute).*
- Note that not all this data is automatically populated so may not be present for some employees.*

Uses of Your Electronic Identity Credential System

2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.

- web applications, including MyUA portal*
- Blackboard Course Management System*
- Online Directory ("phonebook") also used to publish printed directories*
- Wireless network access (currently not used, but has been and may again)*
- Document imaging and management system*
- Help Desk (Service Center) incident tracking*
- Student Health Service application*
- Google Apps for Education*

Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another

Federation participant concerning the identity of a person in your identity management system.

2.11 Would you consider your attribute assertions to be reliable enough to:

control access to on-line information databases licensed to your organization?

be used to purchase goods or services for your organization?

enable access to personal information such as student loan status?

Privacy Policy

Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?

Non-public information could be released only under explicit agreements reviewed and approved by appropriate UA executive authority; such agreements would spell out restrictions on use. Member of..., current student, current employee, and departmental affiliations are public information. However, we could not release the name or other uniquely identifying attributes of students electing to retain complete confidentiality of their educational record under FERPA.

2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?

Non-public information could be released only under explicit agreements reviewed and approved by appropriate UA executive authority; such agreements would spell out restrictions on use. Member of, current student, current employee, and departmental affiliations are public information. However, we could not release the name or other uniquely identifying attributes of students electing to retain complete confidentiality of their educational record under FERPA.

3. Service Provider Information [UA is not currently a service provider via InCommon]

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

N/A

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

N/A

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

N/A

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

N/A

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

N/A

4. Other Information

4.1 Technical Standards, Versions and Interoperability Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

Our intention is to deploy Shibboleth 2.x; Shibboleth 2.0 IdP is running currently in a proof-of-concept, non-production implementation.

4.2 Other Considerations Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

No.

Additional Notes and Details on the Operational Practices Questions

As a community of organizations willing to manage access to on-line resources cooperatively, and often without formal contracts in the case of non-commercial resources, it is essential that each Participant have a good understanding of the identity and resource management practices implemented by other Participants. The purpose of the questions above is to establish a base level of common understanding by making this information available for other Participants to evaluate. In answering these questions, please consider what you would want to know about your own operations if you were another Participant deciding what level of trust to place in interactions with your on-line systems. For

example:

- What would you need to know about an Identity Provider in order to make an informed decision whether to accept its assertions to manage access to your on-line resources or applications?
- What would you need to know about a Service Provider in order to feel confident providing it information that it might not otherwise be able to have? It also might help to consider how identity management systems within a single institution could be used.
- What might your central campus IT organization, as a Service Provider, ask of a peer campus Identity Provider (e.g., Computer Science Department, central Library, or Medical Center) in order to decide whether to accept its identity assertions for access to resources that the IT organization controls?
- What might a campus department ask about the central campus identity management system if the department wanted to leverage it for use with its own applications?

The numbered paragraphs below provide additional background to the numbered questions in the main part of this document.

[1.2] InCommon Participants who manage Identity Providers are strongly encouraged to post on their website the privacy and information security policies that govern their identity management system. Participants who manage Service Providers are strongly encouraged to post their policies with respect to use of personally identifying information.

[1.3] Other InCommon Participants may wish to contact this person or office with further questions about the information you have provided or if they wish to establish a more formal relationship with your organization regarding resource sharing.

[2] Many organizations have very informal processes for issuing electronic credentials. For example, one campus does this through its student bookstore. A Service Provider may be more willing to accept your assertions to the extent that this process can be seen as authoritative.

[2.1] It is important for a Service Provider to have some idea of the community whose identities you may represent. This is particularly true for assertions such as the eduPerson "Member of Community." A typical definition might be "Faculty, staff, and active students" but it might also include alumni, prospective students, temporary employees, visiting scholars, etc. In addition, there may be formal or informal mechanisms for making exceptions to this definition, e.g., to accommodate a former student still finishing a thesis or an unpaid volunteer. This question asks to whom you, as an Identity Provider, will provide electronic credentials. This is typically broadly defined so that the organization can accommodate a wide variety of applications locally. The reason this question is important is to distinguish between the set of people who might have a credential that you issue and the subset of those people who fall within your definition of "Member of Community" for the purpose of InCommon attribute assertions.

[2.2] The assertion of "Member of Community" is often good enough for deciding whether to grant access to basic on-line resources such as library-like materials or websites. InCommon encourages participants to use this assertion only for "Faculty, Staff, and active Students" but some organizations may have the need to define this differently. InCommon Service Providers need to know if this has

been defined differently.

[2.3] For example, if there is a campus recognized office of record that issues such electronic credentials and that office makes use of strong, reliable technology and good database management practices, those factors might indicate highly reliable credentials and hence trustworthy identity assertions.

[2.4] Different technologies carry different inherent risks. For example, a userID and password can be shared or "stolen" rather easily. A PKI credential or SecureID card is much harder to share or steal. For practical reasons, some campuses use one technology for student credentials and another for faculty and staff. In some cases, sensitive applications will warrant stronger and/or secondary credentials.

[2.5] Sending passwords in "clear text" is a significant risk, and all InCommon Participants are strongly encouraged to eliminate any such practice. Unfortunately this may be difficult, particularly with legacy applications. For example, gaining access to a centralized calendar application via a wireless data connection while you are attending a conference might reveal your password to many others at that conference. If this is also your campus credential password, it could be used by another person to impersonate you to InCommon Participants.

[2.6] "Single sign-on" (SSO) is a method that allows a user to unlock his or her electronic identity credential once and then use it for access to a variety of resources and applications for some period of time. This avoids people having to remember many different identifiers and passwords or to continually log into and out of systems. However, it also may weaken the link between an electronic identity and the actual person to whom it refers if someone else might be able to use the same computer and assume the former user's identity. If there is no limit on the duration of a SSO session, a Federation Service Provider may be concerned about the validity of any identity assertions you might make. Therefore it is important to ask about your use of SSO technologies.

[2.7] In some identity management systems, primary identifiers for people might be reused, particularly if they contain common names, e.g. Jim Smith@MYU.edu. This can create ambiguity if a Service Provider requires this primary identifier to manage access to resources for that person.

[2.8] Security of the database that holds information about a person is at least as critical as the electronic identity credentials that provide the links to records in that database. Appropriate security for the database, as well as management and audit trails of changes made to that database, and management of access to that database information are important.

[2.9] Many organizations will make available to anyone certain, limited "public information." Other information may be given only to internal organization users or applications, or may require permission from the subject under FERPA or HIPAA rules. A Service Provider may need to know what information you are willing to make available "public information" and what rules might apply to other information that you might release.

[2.10] In order to help a Service Provider assess how reliable your identity assertions may be, it is helpful to know how your organization uses those same assertions. The assumption here is that you are or will use the same identity management system for your own applications as you are using for

federated purposes.

[2.11] Your answer to this question indicates the degree of confidence you have in the accuracy of your identity assertions.

[2.12] Even "public information" may be constrained in how it can be used. For example, creating a marketing email list by "harvesting" email addresses from a campus directory web site may be considered illicit use of that information. Please indicate what restrictions you place on information you make available to others.

[2.13] Please indicate what legal or other external constraints there may be on information you make available to others.

[3.1] Please identify your access management requirements to help other Participants understand and plan for use of your resource(s). You might also or instead provide contact information for an office or person who could answer inquiries.

[3.2] As a Service Provider, please declare what use(s) you would make of attribute information you receive.

[3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g., "member of community," should be protected while resident on your systems.

[3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?

[3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?

[4.1] Most InCommon Participants will use Internet2 Shibboleth technology, but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.

[4.2] As an Identity Provider, you may wish to place constraints on the kinds of applications that may make use of your assertions. As a Service Provider, you may wish to make a statement about how User credentials must be managed. This question is completely open ended and for your use.

Glossary

access management system

The collection of systems and or services associated with specific on-line resources and/or services that together derive the decision about whether to allow a given individual to gain access to those resources or make use of those services.

assertion

The identity information provided by an Identity Provider to a Service Provider.

attribute

A single piece of information associated with an electronic identity database record. Some attributes are general; others are personal. Some subset of all attributes defines a unique individual.

authentication

The process by which a person verifies or confirms their association with an electronic identifier. For example, entering a password that is associated with an UserID or account name is assumed to verify that the user is the person to whom the UserID was issued.

authorization

The process of determining whether a specific person should be allowed to gain access to an application or function, or to make use of a resource. The resource manager then makes the access control decision, which also may take into account other factors such as time of day, location of the user, and/or load on the resource system.

electronic identifier

A string of characters or structured data that may be used to reference an electronic identity. Examples include an email address, a user account name, a Kerberos principal name, a UC or campus NetID, an employee or student ID, or a PKI certificate.

electronic identity

A set of information that is maintained about an individual, typically in campus electronic identity databases. May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used.

electronic identity credential

An electronic identifier and corresponding personal secret associated with an electronic identity. An electronic identity credential typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.

electronic identity database

A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email address, affiliation, and electronic identifier(s). Many technologies can be used to create an identity database, for example LDAP or a set of linked relational databases.

identity

Identity is the set of information associated with a specific physical person or other entity. Typically an Identity Provider will be authoritative for only a subset of a person's identity information. What identity attributes might be relevant in any situation depend on the context in which it is being questioned.

identity management system

A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.

Identity Provider

A campus or other organization that manages and operates an identity management system and offers information about members of its community to other InCommon participants.

NetID

An electronic identifier created specifically for use with on-line applications. It is often an integer and typically has no other meaning.

personal secret (also verification token)

Used in the context of this document, is synonymous with password, pass phrase or PIN. It enables the holder of an electronic identifier to confirm that s/he is the person to whom the identifier was issued.

Service Provider

A campus or other organization that makes on-line resources available to users based in part on information about them that it receives from other InCommon participants.