INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

Participation in InCommon Federation ("Federation") enables the 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 InCommon 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 that they register for use within the Federation.

Two criteria for trustworthy attribute assertions by Credential 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 (for example authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that Resource Providers, who receive attribute assertions from another organization, respect the other organization’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\(^1\) of the identity information provider.

InCommon requires participating organizations to make available to all other InCommon Participants answers to the questions below.\(^2\) 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.

\(^1\) Such permission already might be implied by existing contractual agreements.
\(^2\) Your responses to these questions must be submitted to InCommon and should be posted in a readily accessible place on your web site. If not posted, you should post contact information for an office that can discuss it privately with other InCommon Participants as needed. If any of the information changes, you must update your on-line statement as soon as possible and also resubmit it to InCommon.

Federation Overview

InCommon™ Federation
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI 48104
1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name  University of Massachusetts Amherst

The information below is accurate as of this date 1 June 2007

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 location(s).

URL(s) http://www.oit.umass.edu/accounts/eligibility/index.html

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  Christopher Misra

Title or role  Network Analyst

Email address  cmisra@nic.umass.edu

Phone  413.545.9721  FAX  413.545.3203

2. Credential Provider Information

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

Community

2.1 If you are a Credential 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?

Accounts are available to University of Massachusetts (UMass) Amherst students, faculty, staff, and retirees. Some Non-employee, Non-students (a.k.a. NENS) may, upon verification of status, obtain a Courtesy Account. We do not offer Office of Information Technologies (OIT) Accounts to alumni, students from other colleges not enrolled in a UMass course, or individuals with no formal affiliation with UMass. Courtesy Accounts require a form signed by a Dean, Director, or Department Head. Courtesy accounts also require verification of picture ID and any other supporting documentation (appointment papers, orders, contract, etc.).

---

3 The documents “InCommon: Assertion Reliability” and “InCommon: Attribute Assertion Levels of Assurance” discuss how authentication policies and practices might affect the appropriate use of identity assertions you might make. See http://www.incommonfederation.org/docs/policies/
etc.). Courtesy accounts are approved by the OIT Accounts Manager pursuant to University Policy.

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?

Active University of Massachusetts Amherst students, faculty, staff, retirees and NENS (see above).

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.”

Students: The Registrar’s Office is responsible for entering and defining a student’s affiliation with the University into the campus Student Information System (SPIRE). The student’s affiliation determines their eligibility for creation of a NetID and provisioning of services. This data provides sufficient information to provision a Kerberos authentication password and LDAP directory entry for the student. The electronic identity database has direct access to this necessary student information. Student accounts are generated at the time of enrollment in the electronic identity database. These student accounts are set with an initial password that is distributed to the students through two postal mailings. The student is required to enter the information via these mailing as well as additional personal information.

Employees: The Division of Human Resources is responsible for entering and defining an employee’s affiliation with the University. Nightly data feeds are received from the University System Human Resources system to the electronic identity database. Employees are required to apply for a campus NetID before an account is provisioned. Employees are required to show a valid picture identification in order to issue credentials.

4 "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). “Member of Community” could be derived from other values in eduPersonAffiliation or assigned explicitly as “Member” in the electronic identity database. See http://www.educause.edu/eduperson/
2.4 What technologies are used for your electronic identity credentials (e.g. Kerberos, userID/password, PKI, ...) that may be used with InCommon actions? 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?

Kerberos electronic identity credentials (username and password) are issued to all users of the University Computing and Network services maintained by OIT.

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:

No.

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 Resource 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.

The University of Massachusetts Amherst uses the Pubcookie single-sign-on, end-user web authentication system. Timeouts are enforced for maximum lifetime connections. User-initiated session termination is supported on a per-application basis. While global logout is not supported, default per-application session termination configuration procedures require termination of login credential as well as session credential. We are also beginning to deploy Shibboleth. Timeouts are enforced by the Service Provider for maximum lifetime connections and inactivity timeouts. Global logout is not supported, default per-application session termination configuration procedures require termination of login credential as well as session credential.

2.7 Are your primary electronic identifiers for people, such as “net ID,” eduPerson EPPN, 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?

No. All electronic identifiers are keyed primarily on an opaque, persistent, non-reused identifier that is NOT the ‘NetID’. NetID are guaranteed unique across the namespace at any given time. Reassignment policy requires a 3-year hiatus between final deprovisioning of services and authentication credentials before a NetID will be reassigned. Final deprovisioning of all services and is not synchronous with the loss of ‘Member of Community’ status. In practice, a NetID will not be reassigned within 5+ years of an individual severing their relationship with the University. Explicit timelines for NetID namespace lifecycle is defined by University policies and procedures and varies dependent upon the individual’s previous affiliation with the University.
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?

Acquiring and updating of information in the electronic identity database is described in Section 2.3. The specific offices designated by the University are also described in Section 2.3. Individual are allowed to update ‘directory information’ on-line including phone number and address, but NOT including name, title, status, etc.

Description of the processes used to update their own information is available at: http://umass.edu/peoplefinder/howtoupdate1.html

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

Public Information for students includes Name, Email, Phone, and Major. Public information for employees includes Name, Title, Email, Phone, Work Department, and Work Address.

All this information is subject to exclusion as described at: http://umass.edu/peoplefinder/privacy1.html

Your 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?

Members of Community use their NetID to access UMail (campus email), personal web space, networks, various computer logins, software downloads, licensed library resources, campus computing labs, Web-based file-storage, and other related OIT managed applications.

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.

---

5 Please see http://www.incommonfederation.org/docs/benefits/incommon_usecases.html
2.11 Would you consider your attribute assertions to be reliable enough to:

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

[ NO ] be used to purchase goods or services for your organization?

[ YES ] 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?

*The University of Massachusetts Amherst strongly asserts that information will only be released that is absolutely necessary for any given application. The University strongly considers the privacy implications of any data sharing. Any attribute will only be released pursuant to University Policy and relevant data confidentiality acts.*

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?

*Information protected by FERPA, HIPAA, FIPA, and relevant data confidentiality acts will be released only pursuant to University Policy.*

3. **Resource Provider Information**

Resource 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 Credential Providers. Resource 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 might make available to other Participants? Describe separately for each resource ProviderID that you have registered.

*The University of Massachusetts Amherst is not currently a resource provider for any services.*

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.?
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?

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?

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

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.

*TBD*

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, e.g., concern about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?
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 a Credential Provider in order to make an informed decision whether to accept their assertions to manage access to your on-line resources or applications?
- What would you need to know about a Resource 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 among its organizations.

- What might your central campus IT organization, as a Resource Provider, ask of a peer campus Credential 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 Credential Providers are strongly encouraged to post on their web site the privacy and information security policies that govern their identity management system. Resource 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 their student bookstore. A Resource 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 Resource 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” or “student,” etc. 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 a Credential 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, e.g. library-like materials or web sites. 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 Resource Providers need to know if 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 their 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 because 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 Resource 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 Resource 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 Resource Provider may need to know what information you are willing to make available as “public information” and what rules might apply to other information that you might release.

[2.10] In order to help a Resource 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 InCommon 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 Resource 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 site.

[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 a Credential Provider, you may wish to place constraints on the kinds of applications that may make use of your assertions. As a Resource Provider, you make 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 online 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 a Credential Provider to a Resource 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.

Credential 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.

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 a Credential 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. |
| 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. |
| Resource 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. |