# INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

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

## *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?

---

2.2 "Member of Community"[4] 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?

---

## *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."

---

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.,

---

[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/

anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

---

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:

---

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.

---

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?

---

### *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?

---

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

---

### *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.

---

### *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:

[ X ] 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?

---

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?

---

# 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.

---

## 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?

---

*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~~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~~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~~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 as "public information" and what rules might apply to other information that you might release.

[2.10~~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~~2.11~~] Your answer to this question indicates the degree of confidence you have in the accuracy of your *identity assertions*.

| | |
|---|---|
| identity credential | 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. |