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.).

[1] of the identity information providing Participant.

InCommon requires Participants to make available to all other 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 should be posted in a readily accessible place on your web site, and the URL submitted to InCommon. 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.

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?

N/A

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."

N/A

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?

N/A

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:

N/A

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

Electronic Identity Database

2.8 How is information in your electronic identity database acquired and updated?

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.

eduPersonScopedAffiliation – we accept the following affiliation types "employee", "faculty", "member", "staff", "student"

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.?

None.

3.3 What human and technical controls are in place on access to and use of attribute

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?

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	

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.