Participation in the InCommon Federation (“Federation”) enables a federation participating organization ("Participant") to use Shibboleth 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 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 and resource 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 Particip

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

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? [X] be used to purchase goods or services for your organization?

Yes

[X] enable access to personal informat

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.

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?

4.1 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 ha

may be more willing to accept your to the extent that this process can be seen as authoritative.

[2.1] It is important for a to have some idea of the community whose identities you may represent. This is particularly true for 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 , 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 .

[2.2] The 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

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 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 . If there is no limit on the duration of a SSO session, a Federation may be concerned about the validity of any you might make. Therefore it is important to ask about your use of SSO technologies.

[2.7] In some , 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 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 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 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 assess how reliable your 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 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 .

[2.12] Even "public information" may be constrained in how it can be used. For example, creating a marketing email li09 Tw[(,l li09 Tw[(ga"harv.7(h)-2.5(is -5.5(r)5005 Tc3-.0009

[3.2] As a , 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 , you may wish to place constraints on the kinds of applications that may make use of your As a , 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 information provided by an to a .
attribute	A single piece of information associated with an record. Some are general; others are personal. Some subset of all defines a unique individual.
authentication	The process by which a person verifies or confirms their association with an . For example, entering a password that is