INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name ______________________

The information below is accurate as of this date _________________

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) ____

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 ____

Title or role ____

Email address ____

Phone ______________________ FAX ______________________

2. Identity Provider Information

The most critical responsibility that an IdentityProvider Participant has to the Federation is to provide trustworthy and accurate identity assertions.[3] It is important for a Service Provider to know how your are issued and how reliable the information associated with a given credential (or person) is.

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an ? 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."

[3] A general note regarding attributes and recommendations wita[( )] TJET5

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?

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 ? Please identify the office(s) of record for this purpose. For example, "Registrar's Office for students; HR for faculty and staff."

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 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 in order to make an informed decision whether to accept its to manage access to your on-line resources or applications?

What would you need to know about a in order to feel confident providing it information that it might not otherwise be able to have?

It also might help to consider how within a single institution could be used.

What might your central campus IT organization, as a , ask of a peer campus (e.g., Computer Science Department, central Library, or Medical Center) in order to decide whether to accept its for access to resources that the IT organization controls?

What might a campus department ask about the central campus 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

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.

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 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 . Examples include an email address, a user account name, a Kerberos principal name, a UC or campus , an employee or student ID, or a PKI certificate.

electronic identity

A set of information that is maintained about an individual, typically in campus . 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 and corresponding associated with an . An 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 . Many technologies can be used to create an for example LDAP or a set of linked relational databases.

identity
