[NOTE: This document should be considered a DRAFT as MIT is still in the process of "spinning up" its participation in InCommon.]

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^ ^ of the identity information provider.

InCommon requires participating organizations to make available to all other InCommon Participants answers to the questions below. 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. Federation Participant Information

1. The InCommon Participant Operational Practices information below is for:
   InCommon Participant organization name _ Massachusetts Institute of Technology_

The information below is accurate as of this date _ December 2008_

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) _ TBD_

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: Paul B. Hill
   Title or role: Consulting Architect within Information Services and Technology
   Email address: pbh@mit.edu
   Phone: (617) 253-0124 FAX: (617) 258-8736

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?

MIT faculty, students and staff are entitled to obtain MIT credentials. These are in the form of Kerberos principals, X.509 Certificates, and MIT ID Cards. Additionally a sponsored guest account is available to any voucher or temporary employee working for an MIT department. Guests and visitors who are working on Institute projects in a way that requires an MIT electronic identity are also eligible for a sponsored guest account. Finally, former MIT students or staff who are continuing their work with their department for a period of time after their departure can have their account sponsored by their supervisor.

Accounts can be sponsored by any current member of the MIT faculty or staff. Students are currently not eligible to sponsor guest accounts. An account's sponsor will be the primary contact for problems related to the account and renewal questions.

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?

We view "Member of Community" as a broad category that includes all holders of a valid MIT Kerberos ID or X.509 certificate. In addition to faculty, staff, and students, this will include visiting scholars, contractors, and voucher employees. It will not includes people that have an MIT ID number but do not have a valid MIT Kerberos principal or X.509 certificate.

We are able to provide finer granularity for other negotiated assertions.

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 office of record is the Registrar's Office.

When a student is accepted, an acceptance package is sent to the student. The acceptance package includes a unique six word pass phrase that the student must use, in addition to their MIT ID number to complete the account registration process. At that time the account will appear as an affiliate. Later in the process, the account will be transitioned from MIT Affiliate to MIT Student. Picture based identity proofing is later performed when the MIT ID Card is issued to the student.

Faculty and Staff:

The office of record is Human Resources.

It is possible for new hires to obtain MIT electronic credentials prior to their date of hire. However the account will be marked as an affiliate until the starting date of record has occurred. At that time the account will transition from MIT Affiliate to MIT Employee. Identity proofing with third party picture IDs is performed when an MIT ID Card is issued.

Affiliates:

The office of record is Information Services and Technologies.

A sponsored guest account is required for voucher or temp staff, former students or staff who are no longer eligible but need continuing access to their account, as well as visitors who need an MIT electronic identity.
Accounts can be sponsored by any current member of the MIT faculty or staff. Students are currently not eligible to sponsor guest accounts. An account's sponsor will be the primary contact for problems related to the account and renewal questions."

Guest accounts are valid for up to two years and are easily renewable with approval of the account's sponsor.

The sponsor is able to provide the information about the guest via an authenticated self service web form. The guest will then be contact via email and given instructions on how to complete the account registration process. Holders of guest accounts are not necessarily issued MIT ID Cards.

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 credentials form the basis of our electronic identity. Anyone with a valid Kerberos name, matching password, and matching MIT ID number may also obtain an X.509 certificate.

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 clear text passwords are required to access any services operated by Information Services and Technology or any mission critical service operated by other business units.

It is possible that individual users have established identities on some systems which use the same username and password as the primary Kerberos realm, and that they occasionally send the password in the clear. If and when we become aware of such a

situation we educate the user and typically require a password change.

If an InCommon Participant believes that an active attack is originating from MIT then security@mit.edu should be contacted.

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.

Our Primary Single Sign On is "Kerberos" for client server systems. Kerberos tickets have a default expiration time measured in hours, though they can be renewed as needed up to a defined limit (about 24 hours).

For web authentication we make extensive use of X.509 Client Certificates. Because certificates must be installed on an individual person's computer, they are not recommended for access from "public" facilities such as Internet kiosks. Our "Touchstone" system may be used by websites that expect significant usage from public terminals. It permits Kerberos authentication as well as supporting X.509 Client certificates. After an initial sign-on with Touchstone, it is up to the individual web application to perform its own session management which includes session expiration.

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?

At this time the Kerberos user principal names are not recycled. In the past they were allowed to be recycled, and we may change this policy in the future, any such change would be reflected in this document.

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?

Information Services and Technology (IS&T) acts primarily as a consolidator and redistributor of identity data. The MIT ID number creation is centralized in one database and some business units are delegated to create new IDs in the database. IS&T also operates the primary Kerberos realm and the MIT CA. Information about individuals,

which affects provisioning and categorization, comes from various data sources including Human Resources, the Registrar, MIT Card Services, and IS&T Accounts.

There are some self service applications which enable individuals to update their own information. Individuals are not empowered to change their username, MIT ID number, name, or MIT affiliation.

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

Note users may choose to suppress some of this directory information.
Full Name
Given Name
Sirname
Username
MIT email address
MIT phone number
MIT room number
Preferred unix login shell type
Path to AFS home directory
Department affiliation
Job title if an employee

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?

Classes B, C, and D are applicable.

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?
[X] be used to purchase goods or services for your organization?
[X] enable access to personal information such as student loan status?
Note that each of these answers require more context to fully answer. We do have reliable data sources which can be used to generate such assertions, but there needs to be agreement about the exact nature of the assertion and the context in which it will be used in order to be fully confident in the response to the question.

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 answer is context dependant.

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?

The answer is context dependent on the specific attribute information and how it will be used.

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.

First, our understanding is that this information must be provided even to join the federation which will certainly precede the registration of a ProviderID hence this question appears to be a bit premature.

Overall the answer to this question will evolve as individual business units create applications for use within the federation. We imagine that some applications will require the eduPerson EPPN or eduPersonTargetedID. Other applications will simply need to know that the user has some affiliation with a participant, still others may need to distinguish the affiliation between student, faculty, staff, and other.

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.?

We do not envision aggregating session access records or records of specific information accessed based on attribute information at this time. Nor do we envision sharing such

information with other organizations at this time.

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?

No single blanket statement can be made in response to this question. The answer will vary for each application and line of business that creates an application that can be used by federation participants.

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?

No single blanket statement can be made in response to this question. The answer will vary for each application and line of business that creates an application that can be used by federation participants.

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

No single blanket statement can be made in response to this question. The answer will vary for each application and line of business that creates an application that can be used by federation participants.

As an example, if the information were simply which individuals made changes to a wiki page, or posted to a blog, over time, we would likely make no effort to notify the affected individuals.

However, if we felt that an information disclosure could potentially be used by someone to perform identity theft we would take steps to notify the affected individuals. We would also follow all applicable laws and regulations.

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.

This has yet to be determined.

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?

No.

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 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	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

identity	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.