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 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 providing Participant.

InCommon requires Participants to make available to all other 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

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name *Bucknell University*

The information below is accurate as of this date *5/23/12*

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)
<http://www.bucknell.edu/documents/lit/policies/InCommonPOP.pdf>

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 *Chris Weber*

Title or role *Director of Technology Infrastructure and User Services*

Email address weber@bucknell.edu

Phone *570-577-1795* FAX *570-577-1790*

2. Identity Provider Information

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

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?

Students, faculty, and staff automatically receive electronic identities. Alumni retain their identities following separation from the university. In addition, trustees receive electronic identities, as well as some vendors, academic collaborators, and contractors on an as-needed basis as determined by an appropriate director or assistant director.

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?

Students, faculty, staff, and retirees in good standing

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."

Nightly data extracts from Registrar and HR information cause new electronic identities to be created automatically for students and faculty/staff. Similarly, departing employees automatically have their electronic identities rescinded. Students leaving the university in good standing retain their identities as alumni. Electronic identities for trustees and other validated individuals are established using data from either the Registrar's office or HR, whichever is appropriate.

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?

UserID/password

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:

There are no circumstances under which passwords are transmitted in clear text

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.

Bucknell uses Jasig CAS for single sign-on, the security aspects of which are well known. The campus Shibboleth deployment uses the CAS service for user authentication. Idle sessions are automatically timed out.

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?

New userIDs are unique and never reassigned. It is possible on rare occasions for an individual to have a new userID assigned. In these cases, the original userID is deassigned and never reused.

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?

In the overwhelming majority of cases, the electronic identity database is automatically updated using database information entered by the Registrar's office or Human Resources. In cases involving trustees, vendors, contractors, and other validated users, the electronic identity database is updated via a manually run process and the data used are first vetted for accuracy by appropriate IT staff. Electronic identity holders are not able to update their own database information.

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

Any data considered public information are made available through Bucknell's public online directory. Non-public information is protected via ACLs or other appropriate controls.

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.

Campus portal/intranet, network login, email, ERP system, workstation login

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?

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?

May only be used for the ostensible purpose for which it is provided, typically to validate authorized use of resources

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?

Will not release/provide information subject to FERPA, HIPAA, or other pertinent privacy laws or institutional policies.

3. Service Provider Information

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.

Bucknell University does not currently act as a Service Provider

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.?

Bucknell University does not currently act as a Service Provider

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?

Bucknell University does not currently act as a Service Provider

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?

Bucknell University does not currently act as a Service Provider

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

Bucknell University does not currently act as a Service Provider

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.

Shibboleth 2.3.x

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?

None