NC STATE UNIVERSITY

INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name *North Carolina State University*

The information below is accurate as of this date *January, 2009*

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://oit.ncsu.edu/iam*

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 *Mark A. Scheible*

Title or role *Manager, Identity and Access Management*

Email address *mark_scheible@ncsu.edu*

Phone *(919) 513-1650* FAX *(919) 513-3504*

2. Identity Provider Information

The most critical responsibility that an IdentityProvider Participant has to the Federation is to provide trustworthy and accurate identity assertions.[1] 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?

All active students, staff, faculty and approved guests of the university are eligible to receive an electronic identity. Currently, alumni and retirees do not retain credentials

[1] A general note regarding attributes and recommendations within the Federation is available here: http://www.incommonfederation.org/attributes.html

beyond a few months of transition, although retired faculty with emeritus status are allowed to retain credentials if requested.

2.2 "Member of Community"[2] 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?

All active students, staff, faculty and approved guests of the university.

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."

For Students a UnityID is created at the point applicants have fulfilled all application requirements and their status is changed to "accepted" status. This results in a student record being created in the Campus Community database (this is a joint db between Registration and Records and HR and includes students and employees).

Employees receive a UnityID on their hire date (the creation process is triggered by the hire date of their employee record). There is an exception process for special cases which allows for early creation of the account for incoming employees who need access to campus email prior to their actual start date.

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?

The electronic identity credentials currently use MIT Kerberos 5.

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

[2] "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). "Member of Community" could be derived from other values in eduPersonAffiliation or assigned explicitly as "Member" in the electronic identity database. See http://www.educause.edu/eduperson/

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 – passwords or PINs are not transmitted electronically 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.

No SSO system will be used to authenticate people for federated access to InCommon Service Providers.

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?

Yes, our UnityID and CampusID (SSN replacement) identifiers are unique for all time to the individual to whom they are assigned.

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 is provided via feeds from our HR/Student database. Initial records are created via triggers from accepted, admitted or hire transactions. Updates are handled the same way if they're as a result of a change by HR or Registration and Records. There is a self-service function which allows students and employees to update personal information related to addresses, phone numbers, emergency contacts and campus location.

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

As North Carolina State University is an agent of the State of North Carolina, most data on campus is considered subject to the Public Records Act and is therefore available to any requestor. Restricted data includes Employee personnel records (protected under the State Personnel Privacy Act) and students' academic, medical and counseling records(protected under HIPAA and FERPA regulations).. "Directory information" - as specified in FERPA - is allowed to be released unless the student has specifically requested a privacy block of that information. More information can be found in the Public Records Policy at: http://www.ncsu.edu/policies/campus_environ/REG04.00.2.php.

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.

Typical applications which are accessed by NC State's electronic identity credentials are: email systems, the campus portal (which has access to the major ERP and student LMS systems), most protected web applications (Leave, Advance, and various "secured" applications).

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?

An Attribute Release Policy (ARP) is currently being written for the university. This will cover the use of attributes released to Federation participants. This will be available in the near future. Additionally, all attributes that would be protected by HIPAA, FERPA, or any state or federal law or regulation would be restricted. However, directory information that is considered "public information" would only be restricted if it is covered by a privacy block requested by the student.

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?

Generally speaking, information subject to FERPA and HIPAA regulation won't be released to Federation participants. Special agreements might be put in place for individual Service Providers, depending on what service they are providing.

---

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.

Currently, no Service Providers will be made available to the InCommon Federation. If this changes in the future, these questions will be answered.

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. 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.

We are currently using Shibboleth V2.0.0.

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?

Any security issues involving a breach of information or release of unauthorized data should be directed to the NC State Director of OIT-Security and Compliance at (919) 513-1194.

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	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.
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 identity	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 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 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.
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.
Service 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.