INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

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[1] of the identity information provider.

InCommon requires participating organizations to make available to all other InCommon Participants answers to the questions below.[2] 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] Such permission already might be implied by existing contractual agreements.

[2] Your responses to these questions must be submitted to InCommon and should be posted in a readily accessible place on your web site. If not posted, you should post contact information for an office that can discuss it privately with other InCommon Participants as needed. If any of the information changes, you must update your on-line statement as soon as possible and also resubmit it to InCommon.

Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name ***American University of Sharjah***

The information below is accurate as of this date *Mon 13-Jun-2016*

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) *https://itfaq.aus.edu/incommonpop*

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 *Naji M. Nujumi*

Title or role *Information Security Officer*

Email address *systems@aus.edu*

Phone *+971 6 515 2135* FAX *+971 6 515 2120*

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.[3] 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?

Faculty (full-time and part-time), staff (full-time and part-time), and students (undergraduate level, graduate level, and outreach) are eligible to receive electronic identities. Alumni retain their electronic identities when they graduate. In addition, visiting scholars, consultants, and affiliates may receive identities that will grant limited access to a small subset of services (e.g. wireless access.) Any exceptions must be approved by the Director of Human Resources (HR) and the Director of Information Technology (IT).

[3] The documents "InCommon: Assertion Reliability" and "InCommon: Attribute Assertion Levels of Assurance" discuss how authentication policies and practices might affect the appropriate use of identity assertions you might make. See http://www.incommonfederation.org/docs/policies/

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."

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 full-time and part-time faculty and staff, currently registered students, and alumni.

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."

The information source for a person in the University is Ellucian's Banner ERP. HR maintains records for all employees (full-time and part-time faculty and staff,) while the office of the Registrar maintain all student records.

The office of enrollment management (OEM) populates details for new students into Banner and indicates when a record is ready for account generation. An hourly process extracts data from Banner and automatically generates electronic identities on Active Directory, creates mailboxes, and grants access to the self-service Banner system. The office of the Registrar then assumes maintenance of the student records. Once students are registered, they are automatically granted access to additional university resources.

HR populates the details about all new Employees into Banner and indicates when a record is ready for account generation. Electronic or paper forms are then submitted to IT requesting the generation of electronic identities. IT confirms that the status of the account indicates that it is ready for creation, then initiate a process that automatically generates electronic identities on Active Directory, creates mailboxes, and grants access to resources requested in the form.

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?

Active Directory UserIDs and passwords for all students and employees. Teaching faculty who have access to change grades are also issued Yubi-Keys for added security and protection against password theft.

[4] "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/

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:

We do not allow passwords to be transmitted across the network 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 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.

We use a Gluu IdP for SSO. Session timeouts and user-initiated session terminations are both deployed, and use with public access sites is protected with TLS encryption.

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?

*The university's primary electronic identifiers for people are Banner IDs (EmployyeID and StudentID), which are unique for each individual, are permanently assigned, and are never reallocated. Active Directory user accounts (specifically the sAMaccountName attributes) that are tied to these individual Banner IDs are also unique and are never reassigned**.***

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?

Banner is the primary source of information for Active Directory user accounts. HR maintains Banner information for Employees, and the office of the Registrar maintains Banner information for students. Except for a personal emergency contact number, individuals are not allowed to directly update their information on Banner or Active Directory and will have to do so through HR or the office of the Registrar.

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

No information in this database is considered "public information".

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?

Webmail, Learning Management Systems, Self-Service Banner, Library systems, wireless access, workstation logins, VPN… etc.

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:

[✓] control access to on-line information databases licensed to your organization?

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

[✓] 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?

Attribute information may only be used for the specific purpose for which it is provided-- typically to validate authorized use of resources- and may not be used for any other purposes.

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?

Any attribute information that fall under HIPPA, FERPA, or articles 7 and 22 of the UAE's Federal Law no.5 of 2012 must not be disclosed.

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.

N/A, the university does not currently have any Resource Providers.

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.?

N/A, the university does not currently have any Resource Providers.

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?

N/A, the university does not currently have any Resource Providers.

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?

N/A, the university does not currently have any Resource Providers.

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

N/A, the university does not currently have any Resource Providers.

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 IdP 2.4.5 (we use Gluu as our IdP.)

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?

N/A