1.1 Authentication and Authorization

Authentication is the process by which the identity of a user, system, or service is verified.

- SUPPLIER Service must interoperate with UNIVERSITY's Shibboleth IdP (Identity Provider) that appears in and consumes InCommon Federation metadata and provides attributes as defined by the eduPerson and inetOrgPerson schemas.
- SUPPLIER must be a member of the InCommon federation service, maintain membership for the duration of the Agreement, and list SUPPLIER's SAML 2 metadata endpoints and SAML 2 signing and encryption public keys in the federation metadata. If SUPPLIER is not a current member of the InCommon federation service, then SUPPLIER will join InCommon within ninety (90) days of contract execution and maintain membership throughout the duration of the Agreement.
- SUPPLIER will perform all of the necessary actions to the application such that it properly participates in the InCommon Federation, including listing its SAML 2 metadata endpoint and signing and encryption public keys in the federation metadata. For more information on InCommon, see http://www.incommonfederation.org/.
- SUPPLIER's SAML 2 service provider software must conform to the full SAML 2 standard documented by the OASIS-Open Security Technical Committee at https://wiki.oasis-open.org/security/FrontPage.
- SUPPLIER's SAML 2 service provider must support the SAML 2 interop profile documented at http://saml2int.org/profile/current. SUPPLIER must also support encrypted assertions as documented in the SAML 2 standard.

Authorization is the determination of whether a user has permission to gain access to particular information or applications. Proper authorization for use of an application usually requires the use of the appropriate attribute, group, and/or role as defined in the enterprise Lightweight Directory Access Protocol (LDAP) service that conforms to the inetOrgPerson and Internet2 eduPerson Object Class Specification.

Authentication alone is not considered sufficient for making authorization decisions. UNIVERSITY's SAML 2 standards-compliant Shibboleth Identity Provider will be used to provide the encrypted assertions of the appropriate directory information for direct access to the externally hosted Web-based application by SUPPLIER.

- SUPPLIER shall have a SAML 2 standards-compliant Service Provider available within ninety (90) days after becoming a member and participant in the InCommon federation service.