Northwestern University User Authentication Requirements  
Revision 2.0  
July 2007

This document is intended for use as an attachment, exhibit, or appendix to bid specifications for acquisition of software systems or services to be used at Northwestern University. All systems must operate effectively within the authentication environment defined in this document. The University will not customize or tailor authentication services to an application.

These requirements are subject to change. The most recent version is on the Web at: http://www.it.northwestern.edu/about/departments/isa/isa-spec/isa-bidspecs/index.html

I. **General statements concerning identity management and services available for authentication**
   1. The University uses a single identifier for use by all University systems as the basis for user authentication. This identifier is created by a central identity management system operated by Northwestern University Information Technology (NUIT). Within the University community, this identifier is called the “NetID”. University management processes ensure that NetIDs are never reused. The application software system should make no assumptions about the format or length of the NetID, as it may be either a short alphanumeric string or a complete e-mail address. The vendor must specifically highlight any restrictions its software places upon the identifying token.
   2. The University requires that all new software systems acquired and deployed use the NetID to identify users.
   3. Authentication of users must use the NetID and its associated password. The University will not manually assign other user identifiers and/or passwords within a specific software system.
   4. The University will not bulk transfer groups of user NetIDs into software systems in order to pre-populate a user profile database. User profiles are either built manually by the software system administrator, constructed at initial access (“first-access provisioning”), or rendered unnecessary by dynamic session construction from attributes of the user. The vendor must clearly describe the options and favored practices supported by the software system.
   5. The University makes available four authentication methods for use by software applications.
      a. Web Single Sign-On (via SUN Access Manager)
      b. LDAP version 3 (via SUN Enterprise Directory 5.2)
      c. Microsoft Active Directory (via Windows 2003 Server R2)
      d. Federated authentication (via Internet2 Shibboleth)

II. **General statements about personal information, security and privacy**
   1. Regardless of the method of authentication, applications may have need for additional information about the user for authorization decisions and customization of the user
experience. This information is housed in the LDAP Registry database and a subset is mirrored in the central Active Directory forest. This information is considered private and access to it must be requested and granted to the application. The LDAP Registry schema is on the Web at http://www.it.northwestern.edu/isa/.

2. Due to government regulations, the University closely monitors how information is collected, stored, exposed, and used in its academic, research, and administrative processes. This affects the use of software systems in at least the following ways:
   
e. If the central database (LDAP Registry or Central AD forest) holds relevant demographic information for a person, an application should request access to and retrieve that information when it is needed. Demographic information should not be cached within the application’s own databases.
   
f. Depending upon the demographic information requested, the application may have to conform the University privacy policies about how data is exposed to classes of users or the Internet at large. Determination will be made when access to the information is requested.
   
g. Information collected by the application within its intended function may fall under governmental regulation. In this case, the University may have specific operational and audit requirements.

III. Authentication options for software systems hosted within the University network

1. Web SSO authentication via SUN Access Manager
   
a. Web SSO is the preferred authentication method for applications within the University network. Single Sign-On is most effective if it is adopted by the largest number of applications. It is also a more secure method of handling of the NetID password, since the application itself never sees it.
   
b. Web SSO is the only method which provides two-factor authentication.
   
c. Vendors must highlight their ability to operate within this Web SSO environment. If the standard product cannot operate in this way, the vendor must provide a cost estimate of the necessary customizations required.
   
d. Web SSO authentication service must be approved and Web server agent credentials issued prior to installation.
   
e. More information about the Northwestern implementation of SUN Access Manager may be found at http://www.it.northwestern.edu/isa/.

2. LDAP authentication via SUN Enterprise Directory 5.2
   
a. Access to LDAP Registry authentication services are by request only and are limited to specific application credentials at specific IP addresses. Anonymous binding to the LDAP Registry is not supported.
   
b. Northwestern’s specifications and practices for authenticating against the NUIT LDAP Registry are on the Web at http://www.it.northwestern.edu/isa/. Vendor software must be able to comply with the University’s stated practice for authentication as described.
   
c. Vendor software must not require superuser or write access to the LDAP Registry in order to authenticate users and retrieve attributes.
   
d. Connection to the LDAP Registry must be over an LDAPS (SSL protected) protocol link.
   
e. The definition of the LDAP Registry schema is managed by NUIT and the vendor should not assume that it may be extended to accommodate additional data elements. Any aspect of a proposed software system or service that
   a. Northwestern’s specifications and practices for authenticating against the NUIT Active Directory forest are on the Web at http://www.it.northwestern.edu/isa/.
   b. The definition of the central Active Directory schema is managed by NUIT and the vendor should not assume that it may be extended to accommodate additional data elements. Any aspect of a proposed software system or service that requires such accommodation must be clearly called to the University’s attention for evaluation.
   c. Schools and divisions may operate a dedicated AD forest for authentication and to hold unique user schema attributes. These forests are provisioned with a subset of the University’s total identities and passwords in accordance with agreements between the units and NUIT.
   d. Vendor software must not require superuser or write access to the Active Directory in order to authenticate users and retrieve attributes.
   e. Any aspect of a proposed software system or service that requires AD authentication must be clearly called to the University’s attention for evaluation.

IV. Authentication requirements for services outside the University network.
1. All services outside the University must be accessed through the Web. Federated authentication is the preferred method for authenticating and authorizing users. The University will not expose any other authentication method outside of its network.
2. The University supports Internet2 Shibboleth 1.3 federation and is a member of the InCommon Higher-Education Federation. The vendor should describe any and all federation protocols the software system or service will support.
3. If federated authentication is not possible, then authenticated access should rely upon a secure session-key technology to designate a persistent session with the service point. Because session-key techniques must be coordinated, any aspect of a proposed software system or service that requires such accommodation must be clearly called to the University’s attention for evaluation.
4. The University does not export or bulk transfer identities, passwords or personal information to third parties for authentication or any other purpose.