The intent of this document is to describe the various electronic authentication services offered and supported by the Office of Information Technology (OIT), define boundaries of such services, and identify levels of services all users should expect.

Authentication is a verification process that substantiates a person’s identity. Specific to information technology, authentication is the process of verifying the digital identity of the sender of an electronic communication, such as a request to log in to a system.

Authentication Services are used to provide credentials for access to services offered not only by OIT, but also through other service organizations at the University of Minnesota. Multiple types of authentication services are supported to accommodate the needs of the various types of software.

**Definition of Services Provided**

The following authentication types are supported by OIT:

**Central Authentication Hub (CAH)**
http://www1.umn.edu/is/cookieauth/aboutcah.html

Also known as “Internet Login” and “cookieauth,” Central Authentication Hub (CAH) is a web-based, single sign-on system providing centralized authentication services for web applications at the University. The Application Programming Interface (API) is based on standard web redirects and thus, is not dependent on a particular software, server, hardware platform, or language. There are two components to the CAH service: the log-in service and the validation service. Detailed information about how CAH works, as well as instructions for service providers who wish to take advantage of the service, is available on the web at http://www1.umn.edu/is/cookieauth/aboutcah.html

**LDAPAUTH**

LDAPAUTH is an authentication method that may be useful for providing central authentication for vendor-provided applications. Many packaged software products can be configured to reference an LDAP directory for authentication. LDAPAUTH provides an SSL-protected LDAP interface to the x.500 directory.

**RADIUS**
http://en.wikipedia.org/wiki/RADIUS

RADIUS is an authentication protocol for controlling access to network resources. It is commonly used for managing access to the Internet or internal networks across an array of access technologies, including wireless and Virtual Private Networks (VPNs).

**Kerberos**
Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. It is implemented using a suite of software published by the Massachusetts Institute of Technology (MIT). Its designers aimed primarily at a client-server model, for which Kerberos provides mutual authentication (both the user and the server verify each other’s identity). Kerberos protocol messages are protected against eavesdropping and replay attacks. UMN Active Directory is an example of a service that uses UMN central Kerberos.

Kerberos will sunset in the near future. Very few University applications use Kerberos now, and there are no plans to enable new applications to use it in the future.

**Shibboleth**

Shibboleth is Internet2 middleware that supports a federated identity-based authentication and authorization infrastructure based on Security Assertion Markup Language (SAML). Federated identity allows for information about users in one security domain to be provided to other organizations in a common federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain user names and passwords. Identity providers (IdPs) supply user information while service providers (SPs) consume this information and gate access to secure applications. Shibboleth also allows services hosted off campus to utilize Central Auth Hub (CAH). UMN GoldPass is an example of a service that uses UMN Shibboleth.

**MKey**

MKey is a two-factor authentication method that uses two separate forms of identification: something you have and something you know (similar to an ATM card – you *have* the card, and you *know* the PIN). Two-factor authentication is stronger than a simple userID/password system. At the University of Minnesota, the two-factor authentication is achieved using a token that provides a unique code at the push of a button and is completed with a user’s secret passcode. (You *have* the unique code from the token, and you *know* your secret passcode). Applications can use a RADIUS, LDAP or vendor-proprietary protocol for MKey authentication.

**Internet ID / X.500**

All of the above-stated services use the central Internet ID (X.500) electronic directory services system for user IDs and passwords. (More information about X.500 can be found on the web at: http://en.wikipedia.org/wiki/X.500.)

**Service Performance**

**Hours of Operation**

It is OIT’s goal to provide authentication services 24x7x52. Normal work hours for Authentication staff are between 8 a.m. and 5 p.m., Monday through Friday, with on-call staffing for after-hours.
emergencies. Systems are monitored 24x7x52. System status is available at: [http://systemstatus.umn.edu](http://systemstatus.umn.edu).

**Change Management**
Change Management is the structured approach OIT uses to manage changes to the University of Minnesota IT environment via formal request and approval mechanisms. By employing a consistent, structured approach to change management, we are able to ensure that all changes are efficiently and promptly handled, thereby minimizing the impact of change-related incidents on service delivery. Changes are approved before they go into production as part of the project management (ITGP) process. Authentication does not go through the CAB process.

**Scheduled Maintenance**
Redundancies built into authentication services will ensure availability of service during scheduled maintenance periods. Maintenance activity is typically done during the business week.

**Service-Impacting Maintenance**
If a scheduled maintenance activity is expected to impact service, OIT intends that information regarding that maintenance activity will be communicated via the System Status page, the EMAIL-L and NET-PEOPLE mailing lists, and other appropriate venues no fewer than 10 business days in advance of the maintenance activity. Redundancies built into authentication services ensure availability of service during scheduled maintenance periods, therefore service impacting maintenance is rarely scheduled.

**Communications**
Communications about maintenance will include the start time, anticipated end time, and a description of the maintenance to be performed (upgrades, patches, etc.).

**Dependencies**
Authentication services are dependent upon the University data center power, network, and related systems. The availability of those systems will have a direct impact on the availability of this service.

<table>
<thead>
<tr>
<th>Service</th>
<th>Dependency on Service</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>There must be power to servers that provide authentication services and the X.500 servers</td>
<td>OIT</td>
</tr>
<tr>
<td>Network</td>
<td>There must be network connectivity to servers that provide authentication services and the X.500 servers</td>
<td>OIT</td>
</tr>
<tr>
<td>Environment</td>
<td>A room temperature environment is required for servers that provide authentication services and the X.500 servers</td>
<td>OIT</td>
</tr>
</tbody>
</table>

**Service Provider and Customer Responsibilities**

**Staffing**
OIT monitors, maintains, and repairs Authentication Services systems and manages the MKey system.
OIT Duties and Responsibilities

OIT's Internet Services group provides support to IT staff in local units in addition to the support offered by the University’s 1-HELP service. OIT's Internet Services group is available to handle support requests during normal business hours (8 a.m. – 5 p.m. weekdays, excluding official University holidays).

Any University unit that wishes to use one of these authentication services is encouraged to consult with the Identity Management group to determine the appropriate mechanism to deploy for the proposed service and to provide assistance with implementation. For several of the authentication services, registration of the server and service is required. If special validation (based on criteria that are kept in the X.500 directory) is required, OIT will work with the requesting unit to implement the authentication.

For assistance in setting up authentication services for use with specific software or services contact the OIT via email at idm@umn.edu.

The OIT Identity Management team will be expected to:
- Communicate about configuration or service changes to minimize disruption to end users
- Work with customers to set up authentication services
- Meet response and resolution times associated with service-related incidents

Customer Duties and Responsibilities:
- Adhere to any related policies, processes and procedures
- Report problems using reporting procedures described in this service statement
- Provide input on the quality and timeliness of service

Problem Management

The operational status of University systems is available online at: http://systemstatus.umn.edu. Whenever possible, users are encouraged to check the System Status page before contacting technical support.

Users are strongly encouraged to contact technical support resources in their local unit if they are experiencing problems with computers or applications. Local technical staff will be able to resolve many problems or escalate them to the appropriate levels, helping to increase the speed and effectiveness of the service response. Response time is dependent on the local unit's technical support processes and policies.

If local technical support resources do not exist or are not available (e.g., outside of normal work hours) users are encouraged to contact the University's 1-HELP service (http://www.oit.umn.edu/help):
- On-campus – 1-HELP (1-4357)
- Off-campus – (612) 301-HELP (4357)
- Email – help@umn.edu

1-HELP hours are found at:
http://www.oit.umn.edu/help/contacts/

Monday-Friday: 7:30 a.m. - 8:00 p.m.
Saturday: Noon. - 5 p.m.
Sunday: closed

Outside of these hours, or on University holidays, callers may leave a message, which will be responded to the following business day.

1-HELP will escalate incidents, when necessary, to appropriate service providers. All incidents and changes reported to 1-HELP will be logged into Service Center, a tracking tool.

**Disaster Recovery**
Authentication services are considered critical services. In the event of a disaster, recovering authentication services is at the highest level of importance. High levels of redundancy, with auto fail-over capabilities are built into the authentication systems to minimize outages and to ensure that service is restored as quickly as possible in the event of a disaster. Degraded or failed service receives immediate attention and all available resources are brought into force to recover full operations.

Reduced throughput, or reduced authentication speed, would be worst case scenario, unless all three data centers were involved in an outage.

**Communication**
In the event of unexpected service interruption, OIT will update the System Status page and send notification of service interruption to subscribed individuals via the EMAIL-L and NET-PEOPLE mailing lists within 15 minutes of a service loss being identified. A post mortem analysis will be released after the resolution of the interruption.

**Policies**
University of Minnesota Information Technology policies are available on the web at:
http://www.policy.umn.edu/Policies/it/index.htm
Policies related to this statement include:
- Acceptable Use of Information Technology Resources
  http://www.policy.umn.edu/groups/ppd/documents/Policy/Acceptable_Use.cfm
- User Authentication for Access to University Computer Resources
  http://www.policy.umn.edu/Policies/it/Use/SECUREDATA_PROC01.html#authentication

**More Information**
For more information about this and other OIT services, visit the OIT service catalog.

**Service Statement Maintenance**
This statement of service will be reviewed annually
Last revision: August 2010
File Name: Authentication.doc