# Identification and Authentication Systems

**Authority** This policy was approved by the Vice President for Business Affairs and Chief Financial Officer.

**Summary** This Guide Memo states requirements for identifying and authenticating users of Stanford computer systems and networks, and describes centrally-supported identification and authentication facilities. Section headings are:

## 1. IDENTIFICATION AND AUTHENTICATION POLICY

To ensure the security and integrity of both University data and data belonging to individuals, all owners of Stanford computer systems and networks must develop and implement access control policies. This Memo does not describe possible policies nor specify how to choose one; however, systems with non-public resources to protect should have policies that base access control on user identities.

Authentication is the secure identification of system users. The system owner is responsible for determining which authentication method to use among those that may be available for a particular system. However, system owners are strongly encouraged to rely on the authentication services provided by Stanford's central computing organization rather than using system-specific authentication methods. This service provides secure authentication and consistent campus-wide identification.

It is University policy that all University business for which computer-based forms and actions have been released will be done using those computer-based systems; paper forms are no longer accepted. This policy applies to all aspects of qualifying transactions, including initiation, routing, processing by Schools and VP Area offices, and transmission to and processing by central administrative offices. Secure identification of the participants in all such transactions is crucial to the successful conduct of University business. The centrally-supported authentication service described in this Memo is designed to support University business requirements.

## 2. IDENTIFICATION: GENERAL

a. **Linked Identifiers —** Stanford maintains a set of linked records identifying all employees, students, and others who use the University's computing resources. These records correlate SUNet ID, University ID, and Stanford Identification Card records.

b. **Management of Identifiers**

(1) **Uniqueness** — Each identifier (University ID or SUNet ID) is unique; that is, each identifier is associated with a single person or other entity.

(2) **One Identifier per Individual** — An individual may have no more than one University ID number and one personal SUNet ID.

(3) **Non-Reassignment** — Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity. Alternative IDs (that is, alternative names registered along with a personal SUNet ID) may be reassigned after a waiting period.

## 3. IDENTIFICATION: SUNET ID

a. **Stanford University Network Identifiers** — SUNet IDs consist of alphabetic characters and digits, and are chosen by their users. Personal SUNet IDs are from three to eight characters in length. Other SUNet IDs may be up to 256 characters in length.

b. **Types of SUNet IDs**

(1) **University-eligible Personal SUNet IDs**

(a) **Full (University-eligible) Personal SUNet IDs** are available to:

- Authorized, registered students, as defined by the Registrar; and
- Regular faculty and staff, and emeritus faculty and staff, including SLAC staff, as defined in Guide Memo 23.1, Definitions, http://adminguide.stanford.edu/23_1.pdf.

(b) **Base (University-eligible) Personal SUNet IDs** are available to:

- Temporary and casual faculty and staff, as defined in Guide Memo 23.1, Definitions, http://adminguide.stanford.edu/23_1.pdf.
- Recent alumni and current hospital staff.

(2) **Sponsored Personal SUNet IDs** are available to all others, subject to the following conditions:

- The ID is to be used by a specific, named individual requiring access to University computing resources in support of legitimate University work.
- The ID is sponsored by:
  - **Full, sponsored Personal SUNet IDs** must be sponsored by a member of the University's regular faculty or staff possessing requisitions or financial signature authority.
  - **Base, sponsored Personal SUNet IDs** may be sponsored by a member of the University's regular faculty or staff.
- The sponsor accepts responsibility for ensuring that the sponsored ID is used in support of work consistent with the University's mission of instruction, research, and public service, and in a manner consistent with the University's policies.

c. **Establishing a SUNet ID** — SUNet IDs are established and maintained via on-line procedures. See http://www.stanford.edu/services/sunetid for more information. Note that employees and students must have a University ID number in order to obtain a SUNet ID.

## 4. IDENTIFICATION: UNIVERSITY ID

An eight-digit University identification number is automatically assigned to regular, continuing employees by the PeopleSoft HRMS system and to students by the PeopleSoft Student Administration system. This number appears on the printed Stanford Identification Card (see Guide Memo 28.4, Stanford Identification Cards, http://adminguide.stanford.edu/28_4.pdf).

## 5. IDENTIFICATION: OTHER ID

IDs are available to identify other kinds of entities such as groups, departments, mailing lists, roles, computer-based services, etc. For more information, submit a HelpSU request at http://helpsu.stanford.edu or phone the Stanford IT Help Desk at 650-725-4357.

a. **Wireless Guest Account** allows a Stanford visitor only to connect a wireless computer to Stanford's wireless network and provides no other network rights or services. The Wireless Guest Account must be sponsored by a member of Stanford's community and can be obtained at http://wirelessguest.stanford.edu/.

b. **Group IMAP Account** is a mailbox with more than one user, each user using his or her own SUNet ID and password to connect to the mailbox. For more information, go to http://www.stanford.edu/services/imap/group.html.

## 6. AUTHENTICATION: GENERAL

a. **Authentication Methods** — Authentication methods involve presenting both a public identifier (such as a user name or identification number) and private authentication information, such as a Personal Identification Number (PIN), password, or information derived from a cryptographic key. Authentication methods currently supported by Stanford's central computing organization include:

- Kerberos authentication, which uses SUNet IDs and passwords.

b. **Eligibility for Authentication Entry** — A user must be associated with an entry in the authentication service to be able to use most centrally-supported systems and services.

(1) **University ID and Regular Personal SUNet ID** — Eligibility for an entry in the authentication service begins when the individual accepts the offer of student registration or employment. Eligibility ends when a person's active association with the University ends; i.e., when an employee is no longer employed (and does not have emeritus status) or a student is no longer registered. A grace period may be allowed as a courtesy after eligibility ends.

(2) **Sponsored SUNet ID** — A sponsored SUNet ID is sponsored for a specific period of time. The sponsor determines the length of sponsorship; sponsorship must be renewed to keep the ID valid. There is no grace period: the entry becomes invalid immediately at the end of the sponsorship period.

(3) **Reactivation** — An entry may be reactivated if the individual subsequently rejoins the University, either via regular association or sponsorship.

(4) **Suspension** — The use of an authentication entry may be revoked if it is used in a manner inconsistent with Stanford policies or if an individual is subject to other administrative action that denies them University privileges.

c. **User Responsibilities**

(1) **Official Actions** — Use of the authentication service to identify oneself to an on-line system constitutes an official identification of the user to the University, in the same way that presenting an ID Card does. Users can be held responsible for all actions taken during authenticated sessions.

(2) **Integrity** — Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use; i.e., must never identify themselves falsely as another person or entity.

(3) **Confidentiality** — Regardless of the authentication method used, users must keep their authentication information confidential; i.e., must not knowingly or negligently make it available for use by an unauthorized person.

(4) **Reporting Problems** — Anyone suspecting that their authentication information has been compromised should contact the information security office at security@stanford.edu or by entering a HelpSU request at http://helpsu.stanford.edu or by phoning the Stanford IT Help Desk at 650-725-4357.

(5) **Security Precautions** — Users are strongly encouraged to change their password regularly (at least once every three months), to limit possible abuse of passwords that may have been compromised without the user's knowledge. Passwords should be chosen so that they are not easily guessable; e.g., not be based on the user's name or birth date.

(6) **Disciplinary Action** — Individuals who are found to have knowingly violated one of these provisions will be subject to disciplinary action. The possible disciplinary actions for violations, which can include termination of employment or student status, will depend on the facts and circumstances of each case.

## 7. AUTHENTICATION: KERBEROS

Kerberos, a sophisticated cryptographic authentication system, is the preferred authentication method for use with centrally-supported systems and services at Stanford.

a. **Identifiers** — Stanford's Kerberos system uses personal SUNet IDs to name its entries for people. Other entities, such as network-based services, also have Kerberos entries.

b. **Use** — Each Kerberos entry is associated with a srvtab or keytab based on a password hash maintained by the user. Kerberos software, installed on end-user computers, allows users to authenticate to network services using their SUNet ID and password.

c. **Changing a Password** — Password changes may be made using standard Kerberos software or via http://www.stanford.edu/services/sunetid. The Kerberos system checks proposed new passwords and rejects those that are likely to be easily guessable.

d. **Reissuing Passwords** — When a SUNet ID holder forgets the password associated with a Kerberos entry, or if it is compromised and no longer private, he or she should immediately try to reset it themselves at http://sunetid.stanford.edu or contact the Stanford IT Help Desk at 650-725-HELP [725-4357] for assistance in having a new password issued.

## 8. IDENTIFICATION AND AUTHENTICATION: LOCAL SYSTEMS

This section contains recommendations and requirements for systems and services that use local identification and authentication methods rather than the centrally-supported methods.

a. **Use SUNet IDs** — Systems should use personal SUNet IDs to identify their users. This will be less confusing for users, and will ease future transition to centrally-supported authentication.

b. **Avoid Clear-Text Passwords** — Systems may not transmit reusable passwords across the network unencrypted. Such passwords are vulnerable to capture and abuse.

c. **Support Password Quality** — Systems should check proposed passwords and reject those that are likely to be easily guessable.

## 9. SOURCES FOR MORE INFORMATION

### a. SUNet IDs

(1) **Cognizant Office** — The office responsible for implementing policy on SUNet ID system is Administrative Systems.

(2) **Support** — Support information is available at http://www.stanford.edu/services/sunetid or submit a HelpSU request at http://helpsu.stanford.edu or phone the Stanford IT Help Desk at 650-725-4357.

### b. Kerberos

(1) **Cognizant Office** — The office responsible for implementing policy on the Kerberos authentication system is IT Services.

(2) **Support** — Support information is available by submitting a HelpSU request at http://helpsu.stanford.edu or phone the Stanford IT Help Desk at 650-725-4357.

### c. University IDs

(1) **Cognizant Office** — The offices responsible for implementing policy on University IDs are Human Resources (for employees) and Registrar (for students).