

## **Case Study: Authentication and Identity Policy at New York University**

---

Authentication services at New York University are a mix of centralized and distributed services. Central IT does not manage all computer systems and services, and many authentication contexts and implementations have arisen -- ranging in scope from individual system use of local usernames and passwords, through mid-sized school-level authentication systems, to the large-scale central authentication services provided by central IT. Even among services managed by IT, multiple authentication approaches are used.

There has been a gradual trend from distributed to centralized authentication services, as the focus of most individuals' computing use has shifted away from stand-alone services (e.g. local file service) provided at the departmental level to broader reliance on interrelated central services such as portal access, e-mail, and enterprise administrative applications.

We are now in the process of developing the next generation of university authentication services as part of an overall Identity Services Initiative: included are projects to coordinate or unify authentication practices across central systems, and to enhance single sign-on, self-service, and ease of distributed system integration -- all to be grounded in a fully worked-out framework of identity-related policies and standards.

### **AUTHENTICATION SPECIFICS**

Enterprise portal and e-mail access represent the most pervasive uses of central authentication, since they are offered to the entire community and, in the case of the portal, provide the gateway to a wide range of specific IT services. Central NetID/password authentication increasingly acts as a base-level access control mechanism and security safety net, leaving more fine-tuned authorization decisions to individual systems and applications.

The ability to authenticate is increasingly understood as a privilege that must be offered and managed in accordance with policy. Assignment of this privilege must also be carefully correlated with application requirements: if an application requiring authentication is offered to a segment of the community, then the members of that community must be eligible for the privilege; similarly, if a person is not eligible for any services requiring central authentication, then they do not need (and should not have) the privilege. Thus it is possible, and of concern, that the privilege to authenticate will be expanded more and more broadly to extensions of the core University community (e.g. to all donors to a given college because that college wishes to offer them authenticated services). Such expansions may prove difficult to plan for, may place stress on our identification, registration and authentication services or at least their underlying procedural assumptions, and may progressively dilute the degree of security provided by NetID/Password authentication.

Consequently, in the future, we can expect that central NetID/Password authentication, will increasingly need to be augmented or replaced by stricter authentication methods for many high-value services. We do not support multiple levels of assurance in a formal way at this time, but are experimenting with smart cards as 2-factor authenticators in order to be familiar with the technology and to help us identify potential deployment settings.

### **POLICY FRAMEWORK**

As part of our Identity Services Initiative, we are developing a policy framework focused on management of authentication and other identity services. Significant inspiration for this framework has been drawn from Philip Windley's book *Digital Identity* (O'Reilly, 2005) and his discussion of an Identity Policy Suite covering all of the main areas of identity-related functionality.

However, a viable identity policy framework must be tuned to the local institutional context. For example, there is strong sentiment at NYU for regarding a policy as a very general, high-level statement – so to have many specific identity policies would not fit in our larger IT policy context. So instead, we shall have one over-arching identity policy and then a set of more focused identity standards to cover such topics as identifier management, authentication, authorization, passwords and directory services. Below you will find initial versions of the overall identity policy statement and an example authentication standard.

Finally, we are also deeply concerned with elements of identity services that may need exceptions for special cases or that need to be revisited periodically – we want to be flexible in balancing service, identity management, and security goals. We also seek practices that are geared for continuous evolution and improvement over time. So in addition to development of standards governing implementations and operational procedures, we also seek to implement well-defined procedures for annual review of policies and practices and for requesting, approving, documenting and revisiting exceptions.

(Read on for NYU's Identity Services Policy and Standard examples.)

## **Identity Services Policy**

**Responsible Officer:** Associate Provost and Chief Information Technology Officer

### **REASON FOR THE POLICY**

The purpose of this policy is to provide the context and framework for standards governing central identity services offered and managed by Information Technology Services at New York University.

### **WHO IS AFFECTED BY THIS POLICY**

This policy applies to all systems and applications participating in central identity services at New York University, and to all individual users of central identity services provided by the University. Central identity services offer identity-related capabilities to systems connected to NYU-managed networks and access-related privileges to designated members of the university community under the management of NYU Information Technology Services.

### **POLICY STATEMENT**

Central identity services at New York University provide a core of highly secure and tightly managed identity-related services, providing authentication, authorization, account provisioning and related capabilities for shared use by applications and systems. These identity services are implemented, managed, and used in accordance with a strict policy and standards framework in order to maintain security, reliability and auditability across the breadth of their use. Consistent and coordinated provision of central identity services is intended to progressively encompass more and more NYU IT services, with integration priority given to those services where identity management improvements will result in the greatest security and service benefits.

Not all applications and systems will utilize central identity services in the same way or to the same degree. For example, some may use only authentication services, others may use only provisioning services. To the extent that an application or system utilizes one or more central identity services, then it must meet the standards relevant to its use.

The systems and application components themselves providing central authentication services will be managed, monitored, and reviewed in accordance with the university *Application Security Management Control Policy*. In the interest of optimizing security, information confidentiality, and preservation of individual privacy, the *minimum necessary* standard will be observed comprehensively with respect to collecting, handling, and using identity information and managing privileges for users of NYU computers and data.

Central identity services will be subject to a continual cycle of implementation, operation, monitoring, review, and improvements in the interest of being responsive to evolving requirements for managing access to NYU information resources.

The Associate Provost and Chief Information Technology Officer is responsible for interpretation, review, revision, and approval of this policy. The policy will be reviewed, revised as necessary, and re-approved on an annual basis.

The following standards covering the major functional areas and aspects of identity services will be developed, adopted, and reviewed annually:

1. **Access Control.** Guidance on access control methods used in tandem with core identity management controls.
2. **Authentication.** Guidance on management of central authentication services.
3. **Authorization.** Guidance on management of central authorization services.
4. **Directory Services.** Guidance on management and use of central directory services for identity management purposes.
5. **Encryption, Digital Signatures, and Certificates.** Guidance on use of encryption-related technologies.
6. **Federation.** Guidance on the use of federated identity technologies and services.
7. **Identifiers, Identification, and Identity Data Management.** Guidance on managing identifiers and identity-related information.
8. **Monitoring and Review.** Guidance on applying required monitoring and review practices to the context of identity services.
9. **Passwords.** Guidance on management and use of passwords.
10. **Provisioning.** Guidance on management of central provisioning services.
11. **Registration.** Guidance on assigning credentials, e.g., providing passwords, to members of the university community.

Any member of the University community found to have violated this policy is subject to disciplinary action as described in the *Policy on Responsible Use of NYU Computers and Data*.

**DEFINITIONS** – See the document *Identity Services Glossary*

## **RELATED DOCUMENTS AND RESOURCES**

Contact: Central Identity Services Architecture Committee ([its.cis@nyu.edu](mailto:its.cis@nyu.edu) )

- New York University HIPAA policies
- Policy on Responsible Use of NYU Computers and Data
- Policy on Personal Identification Numbers
- Application Security Management Control Policy
- Program Change Management Control Policy

## **Identity Services Standard on Authentication**

**Responsible Officers:** Central Identity Services Architecture Committee, Information Technology Services

### **1.0 REASON FOR THE STANDARD**

The purpose of this standard is to provide guidance concerning central authentication services at New York University.

### **2.0 SCOPE OF THE STANDARD**

This standard applies to all systems and applications participating in central authentication services at New York University, and to all individual users of central authentication services provided by the university. Use of central authentication services is a capability available to systems connected to an NYU-managed network and a privilege offered to designated members of the university community as part of central identity services operated by NYU Information Technology Services.

The Central Identity Services Architecture Committee, Information Technology Services, is responsible for interpretation, review, revision, and approval of this standard as well as for evaluating and approving requested exceptions to any of its provisions. The standard will be reviewed, revised as necessary, and re-approved on an annual basis.

### **3.0 STATEMENT OF THE STANDARD**

Central authentication provides the base-level capability of identifying an individual attempting to access a system or application participating in central identity services at NYU. It represents a key component in controlling access to NYU systems, applications, and data. Use of central authentication is a privilege specifically granted to designated members of the university community and is governed by the *Policy on Responsible Use of NYU Computers and Data*. The specific provisions of this standard govern the underlying technical management of authentication repositories and capabilities.

### **4.0 OPERATIONAL REQUIREMENTS**

#### **4.1 Authentication Methods. There are two approved central authentication methods, NetID/Password and strong authentication using a physical token.**

Approved central authentication methods are: (1) NetID/Password against an NYU enterprise authentication repository and (2) strong authentication utilizing a physical token as managed by NYU/ITS. A system or application may also require use of an additional, local username/password or other authentication technique (e.g. Biometric, digital certificate).

#### **4.2 Authentication Levels. There are two corresponding authentication levels for systems, *Basic Security* and *High Security*.**

The following authentication levels, corresponding to these two methods, are defined. Each system participating in central authentication will be categorized as operating at one of these levels.

- Basic Security – the NetID and password combination shall be used.
- High Security – a strong authentication protocol, such as two-factor authentication, shall be used

A specific form of system access, such as root access, can also be designated as requiring a *high security* approach even if normal end-user access is performed at the *basic security* level.

**4.3 Use of Authentication Repositories. The enterprise LDAP directory server is the master password repository; other NetID/password repositories represent secondary authentication repositories.**

The enterprise LDAP directory service operated by NYU Information Technology Services is the master password repository for basic authentication to NYU information systems and applications that participate in central identity services. Other centrally run services such as ITS-managed Kerberos, Radius, or Active Directory installations, if specifically designated, may operate as secondary authentication repositories and contain synchronized NetID/password information for a subset of the user community.

**4.4 User IDs. The NYU NetID is the User ID used for basic-level authentication.**

The User ID used for basic-level central authentication shall be an individual's NYU NetID. Use of the NetID is governed by the *Policy on Personal Identification Numbers*, and is created in accordance with the *Identity Services Standard on Identifiers, Identification and Identity Data Management*. Each member of the university requiring a central authentication capable login identifier is assigned a unique NetID. For special purposes, service NetIDs may be created and allocated for use by designated, sponsoring individuals. Systems and applications may also use local accounts not based on NetID for system management or other special purposes; the management of these user ids and accounts falls outside the scope of this standard.

**4.5 User Accounts. Except under special circumstances, each user account must belong to a specific individual, individuals may not possess more than a single account, and accounts may not be shared.**

Unless it is technically unavoidable, each user account using central authentication will belong to a specific individual, individuals will not possess more than a single user account, and such accounts will not be shared among individuals. Where these requirements cannot be met, strong mechanisms (such as special logging) shall be implemented to provide individual traceability.

**4.6 Permitted Systems. All systems connected to an NYU-managed network are allowed to connect to the primary central authentication repository (LDAP) for purposes of NetID/Password authentication.**

All computer systems connected to an NYU-managed network are allowed to connect to the primary central authentication repository (LDAP) for purposes of basic NetID/password authentication. Only specifically designated and documented systems and applications may participate in higher-level authentication services, such as single sign-on and federation.

**4.7 Encryption. All network transmission of authentication information must be encrypted.**

All transmission of authentication information, such as sending of NetID/Password to a system, must be encrypted. Systems collecting NetID/Password from clients should not support submission in plain-text (e.g. via Telnet, HTTP, IMAP), but should require encrypted submission (e.g. via SSH, HTTPS, IMAPS). Wherever possible, authentication repositories should be configured to support only encrypted access.

**4.8 Alternate Authentication. A system or application using central authentication for its user community may not also use an alternate authentication method for some or all of these users.**

Where central authentication is used for a defined set of users of a system or application, alternate/local authentication (e.g. fall-through to a local username/password) may not also be offered to some or all of these users.

**4.9 Authentication Proxying. A central authentication client system may not itself store user passwords in any form beyond in-memory use for the duration of a user session.**

A system or application participating in central authentication services may not itself store passwords in order to facilitate future login to itself or to other, inter-related applications that also use central authentication services. Specifically, passwords may not be stored locally in any form, including hashed or encrypted, beyond in-memory use for the duration of a user session.

**4.10 Selecting Authentication Systems. Use of LDAP is the preferred central authentication method.**

Preference will be given to using LDAP-based authentication over Kerberos or other secondary repositories, which shall only be used if LDAP-based authentication is not practical in a given situation. Compatibility with the enterprise LDAP directory shall be sought when specifying or selecting products which require authentication. Whenever an existing information system undergoes major modification, the project management shall determine whether the system can and should be brought into compliance with this standard.

**4.11 Monitoring and Review.**

Systems and application components providing central authentication services will be managed, monitored, and reviewed in accordance with the university *Application Security Management Control Policy*.

**4.12 Federated services.**

See the document *Identity Services Standard on Federation* for guidance on authentication and authorization across security boundaries.

**4.13 Enforcement**

Any member of the community found to have violated this standard is subject to disciplinary action as described in the *Policy on Responsible Use of NYU Computers and Data*.

**5.0 DEFINITIONS**

See the document *Identity Services Glossary*

**6.0 RELATED DOCUMENTS AND RESOURCES**

- Policy on Responsible Use of NYU Computers and Data
- Policy on Personal Identification Numbers
- Application Security Management Control Policy
- Identity Services Policy
- Identity Services Standard on Passwords
- Identity Services Standard on Federation

**7.0 CONTACTS**

Central Identity Services Architecture Committee, Information Technology Services, its.cis@nyu.edu

Private  
39,400 Students  
Doctoral Extensive  
Gary Chapman  
August 2006