Executive Summary

A University System Architecture must address near-term and long-term goals for supporting University enterprise applications for administrative, academic, and research. The explosive growth in Northwestern’s information technology capabilities has contributed to advancing these areas; however, the collection of applications is becoming complex. The isolation of some systems leaves blind spots in planning resources. Proliferation of multiple identities confuses system users and leads to inconsistent security. These negative effects have been manageable.

Increased governmental requirements for security and privacy, plus the recent decision to replace the financial system, have driven a re-evaluation of the current Northwestern system architectures. The result is a sweeping plan to change enterprise applications and introduce methods for sharing information, passing transactions, and protecting privacy through industry standard software. This plan radically centralizes identity management and security, defines methods for application integration and accessing central data resources, and recommends a extendable University service portal.

Due to the broad and ambitious nature of the goals for a new University System Architecture, many service units will have to relinquish certain local controls that they have enjoyed over
University System Architecture for Integrated Enterprise Systems

the past 20+ years at Northwestern. This will not result in loss of flexibility or business control, but will increase capabilities and confidence in security and data integrity.

Because so many facets of University activities involve the financial system, this is the ideal time to adopt an architecture to which all enterprise systems will conform. Implementation and deployment of the plan could take place in parallel with, and on approximately the same timeline, as the new financial system.

Planning Assumptions

The University System Architecture is concerned with deployment of enterprise applications and other applications that are reliant upon core institutional information. These applications can be administrative, academic, or research oriented. The University System Architecture defines a framework of identity, authorization, access control, and information sharing based upon a set of explicit assumptions about future functionality and desirable capabilities.

Self-Service Is the Best\(^1\) Method for Improving the Effectiveness of University Services

Persons at Northwestern engage in business and academic work by using systems of administration and collaboration. This use is transactional – a person requests assistance; requests a change; responds to required tasks; etc. For traditional service models, the person contacts a staff expert who uses information bases to deliver service. Service availability is limited by staff work hours and the accessibility of the information base.

New service models have taken hold through Internet-based commerce. Many Northwestern faculty and staff, and virtually all students, have experienced using the Internet to purchase goods and services directly. Over the Internet, it is now possible to purchase books, tickets, vacations, and even cars; file taxes; shop for groceries; and tour homes for sale. Effective and intuitive Web sites assist persons to make decisions in the same way as the staff expert, but at lower cost and with continuous availability. This experience of “self-service” through the Internet prompts an expectation that University transactional functions should also be moving to this model.

There are several advantages of self-service for enterprise applications. Taken together, these advantages are compelling.

- **Availability** – Internet-based applications can be accessed virtually at any time. This is particularly important for persons in other time zones.
- **Reach** – The Internet is a global resource. Self-service applications are available anywhere in the world.
- **Capacity** – Self-service applications are engineered to give service simultaneously to hundreds, if not thousands, of persons. Staff-based service models cannot scale to this degree.
- **Immediate feedback** – A self-service application interacts with the person to immediately signal request completion, the need for additional information, or problems with information provided. Very quickly, the transaction can be refined and completed with clear notice to the person.

\(^1\) When comparing approaches, the “best method” is one that maximizes user satisfaction, confidence, and privacy; provides the strongest authentication, security and regulatory compliance; is compatible with industry standards and can make information available reliably; minimizes service times, errors, and manual intervention; eliminates duplication of data in multiple systems; and can be easily modified or extended.
The University System Architecture is designed to support deployment of self-service applications.

**The Best Method to Implement a Self-Service Model Is Through Real-Time Messaging Between Applications to Share Changes Continuously**

Self-service applications must represent relevant decision information as the most up-to-date available. Some services will require that information be aggregated from more than one data source and transactions will affect them. The appearance of an integrated service can only be accomplished by continuous sharing of information in real-time.

A self-service purchasing function might interact both with a supplier and with the financial system. Supplier information includes pricing, inventory, delivery options, etc., while the financial system presents funds available and enforces policies on their use. When a purchase is made, the supplier is signaled in real-time to ship the goods while the computed total cost is encumbered in the financial system. Without real-time messaging, the information about the two requests (ship and encumber) could be unavailable to the next person assessing financial data.

Currently, real-time messaging between applications is not used at Northwestern. This is an important part of the University System Architecture and will rely upon adoption of industry-standard communication methods. Major vendors in enterprise applications are supporting these methods and are implementing services today.

**Centrally-Managed Digital Identities Is the Best Method to Deploy Secure Services**

Digital identities are the tokens persons present to computer applications to identify themselves as a particular individual. The Northwestern NetID is an example. Rather than one token for each application requiring identification, it is more convenient and secure to have a single identifying token for each person. Security is further enhanced by central management of this token, authentication and the permissions granted to it.

The University System Architecture requires reliable identification of persons using enterprise systems. Most administrative systems manage information which is confidential, should be kept private, or is mandated protection by law. It is essential that business processes and technical systems cooperate to deliver the highest confidence in identities and authentications. Current practices apply different business practices for many systems, leading to multiple tokens and confusing passwords – which weakens security. As new applications are deployed, including new authentication services, a unified identity can be realized.

**The Best Method to Allow Secure Access to Institutional Data or Business Functions Is With Established Technical Standards**

The University System Architecture addresses a long-standing institutional need to make centrally-governed administrative information available to division and school applications for integration with local business data. This is an internal business use that parallels self-service for individual needs.

A discussion of how access to information should be governed is outside the scope of this paper; however, data stewards should adjust their thinking about data. Instead of assuming that central data should not be given to divisions and schools, the University should
assume that opposite – that all data should be available – and then determine the exceptions.

The means to make central information available must be secure and capable of implementation by a distributed technical work force. Both of these requirements are met by the same technical standards that will be used for inter-application real-time messaging. Therefore, the University System Architecture will rely upon these technical standards to be the basis for exposing central data as requested.

Goal and New University Service Environment

The goal of the University System Architecture is to create an integrated, secure service environment that supports distributed management, and users open standards for data access and software development. This environment will operate on the Internet using the Web. University business functions are migrating quickly to be Web-based self-service applications. The University System Architecture must support effective use of these functions, promote additional extensions and leveraging of information, and maintain excellent security.

Create a University Service Portal to Organize Access to All Enterprise Applications

The most visible aspect of the future University business environment will be a portal Web site that will organize access to available services. Beyond being a navigational device, the portal will use attributes of the individual, such as employee status, permission to access financial information, or research interests, to offer a range of alternatives.

The basis of the portal will be “roles” derived from status information known from authoritative systems. Each individual will have multiple roles that will reflect the different tasks performed. Roles of “student”, “faculty”, “researcher”, “financial”, and “employee” are examples. Each role will appear in the portal as a separate tab upon which relevant applications will reside. The individual will be able to customize which services will appear from a list of applications.

The portal will give the individual a window (a “portlet”) into the service available and allow the individual to click through to that application. For example, a window may summarize that three new e-mail messages are waiting and list a portion of the subject line for each. Clicking on the window would launch the Webmail utility.
Create Tools, Services, Etc., to Enable Schools and Divisions to Deploy Portlets within the Service Portal

An important goal for the University service portal is to distribute the authorship of portlets (the applications that control windows) to schools and divisions. Each school and division has business and academic functions that would be of value in the service portal. NUIT must make it possible to create applications within the portal with the distributed resources across the University. This will speed development and deployment.

Addressing this goal will require a mix of hardware and software to allow programmers to author portlets, test them off-line, authenticate users, and manipulate data securely. Final testing and installation of portlets will fall under NUIT for security reasons.

For portlets to be valuable, they will need access to certain key administrative information. This might include retrieving Registry data (such as emplid or e-mail address) for the individual user. Programming methods for this will fall under the same Web Services framework as will be favored for application-to-application communication generally. Therefore, portlets will participate in the same governance and technical portability to be favored across the network.

Require Use of Central Digital Identities for All Administrative and Academic Services

A unified presentation of administrative and academic functions in the portal will require that all applications agree on individual identifications. Today, the NetID is the de facto standard for identification but it is not universally accepted. This will be essential in the future.

Because the central identities are linked from authoritative data sources, such as Human Resources and Registrar information, changes in the standing of an individual could have immediate effects on access rights. The moment a person separates from the University, access to all systems could end. Transfer of a person between University units could trigger restructuring of what information was then visible within administrative systems. Such changes will be expected by persons who move within the University, and by their supervisor, to preserve accountability.

Standardize Identity Management Processes to Increase Security ofAuthenticated Services

A concern that should arise about central digital identities is that the processes for identifying individuals and assigning them credentials (e.g. NetID and password) must be well managed. Using NetIDs for administrative system access, to the exclusion of local authorization databases, must be deployed with confidence in identities and the ability for service units to implement specific means to grant access.
Processes for creating identities for individuals must pass audit standards. What forms of identification are required? What means of communication can be used to convey a NetID and password to an individual? Methods in use today may be too lax for future identities that will have administrative powers.

Significant attention must be paid to “role-based” authorizations, where the individual’s standing at the University defines default capabilities. For example, the role of “Department Assistant” as defined from Human Resources information might give any identity the ability to view the financial information for the department funding the position. Individuals with a role of “Student” may be barred from any access to the financial management system. The definition of roles, including business rules for determining membership in the role, is a critical success factor for identity management services.

![Diagram](Figure 2 – Role-based Authorization)

In opposition to “role-based” are “rule-based” authorizations. In rule-based authorizations, an application applies specific tests against an identity’s entitlements to determine if services should be delivered. The entitlements could be defined from authoritative source information or added manually by an authorized administrator. Returning to the example of the department assistant, the financial management system might require the entitlement “purchaser = true” before allowing the identity to transfer funds or issue purchase orders. By default, this entitlement would not be present; however, an office process within Financial Services might interview and train a new staff person before granting the entitlement to enable access. Through rule-based authorizations, service units can establish strong controls.

**Deploy Web Single Sign-On to Reduce the Number of Passwords**

An important benefit of centrally administered digital identities will be Web Single Sign-On. Those systems accessed through Web browsers will share one initial authentication step across a session and eliminate the need for multiple password entering.

A common password across applications will improve security because individuals will have only a single password to remember. Concerns that compromise of a single

---

2 The application must request this attribute from the LDAP Registry. Whether this occurs at initial access to the application and or occurs when the more-secure function is requested is a design issue of the application and is outside the scope of this discussion. Either approach has advantages and disadvantages.
password will give access to all applications can be addressed through strong authentication techniques such as swipe cards or biometrics.\(^3\)

**Deploy Web Services as the Integration Infrastructure**

Another goal of the University System Architecture is to minimize data errors, manual handling, and service times through improving the collaboration between enterprise systems. At this time, the most promising and affordable means to realize this goal is through Web Services.

The attractions of Web Services are many. As a Web-based communication method, it can be universally deployed both within the University and with trading partners and collaborators. Second, commercial interest in Web Services is so great that development will far outpace Northwestern’s need for local development (PeopleSoft has already deployed Web Services within the systems at Northwestern).

Web Services standards are under active development, although there are already strong deployments available. By mid-2005, standards bodies will have completed work on the most important aspects for Northwestern, the secure transaction protocols. Before that time, additional local security methods will be needed.

**Create Web Services for Access to Administrative Information**

Web Services should be the basis for access to administrative data as requested by division and school applications. Convenient access to administrative data also reduces data duplication in “shadow systems.” Rather than creating custom data extractions for each request, or forcing local double entry of transactions into a local database, administrative information should be exposed through Web Services. Thereafter, approved applications can call upon those services to access up-to-date information for analysis and reporting.

Security would be controlled by the data owner through NUIT tool sets. This will allow creation of security policies with individual Web Services to support them. For example, different security requirements could exist for services such as “Is this person a student?” versus “Which class(es), if any, is this person registered for in school <…>?” versus “Please return all classes this person is registered for” versus “Please return all students registered for class <…>”.\(^4\)

---

\(^3\) The decision to deploy strong authentication can be made on a function-by-function basis within single applications. Thus, NetID and password could be sufficient to deal with e-mail or to read financial information, but a swipe card might be needed by that same person to access financial functions that spend or transfer funds.

\(^4\) These services are hypothetical and are intended to show both the types of queries schools are likely to propose as well as the wide range of security requirements. The query “Is this person a student?” could be answered through the online directory – so security requirements might low. The other examples are show queries for which security and privacy are increasing concerns and could each be implemented with different authorization requirements.
Anticipated Benefits

The University System Architecture will deliver many benefits as enterprise applications are brought into compliance. The range of benefits can be appreciated by considering the resulting service and technical environment from three viewpoints: the user, the service providers, and the system administrator.

The User’s Experience

All members of the Northwestern community will be users of enterprise systems and will experience improved convenience and integration of services. This will result from the following frameworks.

- The portal environment will support effective work. All administrative and enterprise academic functions will be deployed through the University portal, thus providing a single location for finding services. A full description of portal software features is outside the scope of this document; however, the functions available to the user will be tailored by identity information (faculty, staff, student, researcher, financial manager, etc.) and may be customized for appearance. The user will have a full range of relevant services at hand.

- Each session will have a single authentication step. Through the portal or any separate application, user authentication will be handled once and preserved over the session. This will be necessary for portal functions and will be valued by users as a convenience. Service providers may require additional authentication steps within applications, perhaps involving swipe cards or thumbprint readers.

- Self-service will increase convenience and confidence. Availability will increase both in time and locations. The user will see results immediately and can be comfortable that transactions have been completed. Depending upon the application, progress of work flows could also be seen.

- A single transaction will yield multiple results across systems. Rather than the user interacting with two or more systems to complete a transaction in all its details, collaborating applications will pass information. Each application will have full knowledge of the user’s roles and entitlements should it be necessary to change processing rules.

The Service Administrator’s Experience

Directors of University administrative services will also see benefit from the new architecture, including savings in staff time.

- Reduction in paper-based work flow between administrative services. Once central applications are linked through an integrated messaging infrastructure, manual steps between service units can be replaced by real-time functions. An immediate benefit will be reduction in paper handling and staff time. Staff time can be routed to handling service exceptions and increasing user satisfaction. Service times will be reduced, will require fewer manual checks, and will use information gathered at any prior transaction to assure consistency.

- Information will be captured as close to the source as possible and then used from single database sources. This will minimize the chance of errors and thus need to
University System Architecture for
Integrated Enterprise Systems

rework transactions. For self-service applications, the user becomes the source directly into central applications.

- Central identity management and authentication will give confidence in who is accessing systems and data. As stewards of institutional data, service directors will have more options open for defining how users will be authenticated. This can include authentication trust rules, secondary strong authentication through swipe cards or biometrics, and user-by-user entitlement control. Further, policies for user management can be constrained by the granted entitlements.\(^5\)

- The time to develop and deploy new functions will be reduced. With a standards-based infrastructure between applications, the service managers can expect to offer new services faster. In most cases, vendors will implement software within the standard infrastructure. Where local development is warranted, the Web Services framework will support rapid creation and testing of software using published libraries of other services.

**The System Administrator’s Experience**

The task of system administrator will be assisted by the University System Architecture in at least the following ways.

- Through the use of standards-based messaging infrastructure (Web Services and XML), the University will expose functions at several levels of granularity. This will enable system administrators to rapidly determine what information and functions are available to support new services or fulfill functional needs of purchased software. By the nature of Web Services, the specifications will be largely self-describing to developers.

- Inter-application messaging will be logged and may be analyzed to improve performance. Administering a service, or several services, will be simplified through this logging or real-time transaction flow tracing. In some situations, transaction logs can serve audit purposes.

- Because vendors will use the identical Web Services infrastructure for inter-application messaging, new software will rapidly merge into the enterprise. A high degree of functionality can be delivered quickly. Testing of both vendor services and locally-authored services will occur under controlled conditions with standard tools and test environments.

**Summary**

For the user, service administrator and system manager, the University System Architecture will result in a more unified and consistent service experience. This will be reflected in:

- Portal organization and navigation that will reduce confusion and save time
- User self-service, reduced manual interfaces, and easier deployments that will save effort and reduce errors

\(^5\) For example, the NUIT Information Center could be barred from resetting the password of an identity with access to Human Resources information.
University System Architecture for Integrated Enterprise Systems

- Unified identity management that will promote consistency of services and strong security across the University
- Vendor adoption of service methods and less-difficult local development that will speed deployment of new functions

Realizing the Goal – Eliminating Application Silos

The stated goal of creating an integrated and secure service environment requires changes within the University service units. The term “integrated” conjures images of single-vendor solutions or fragile custom “connector” software between each pair or applications. Under the University System Architecture, this will not be the case.

Most complex systems are perceived to be “integrated” because the consumer of services only sees his interface and the results. In fact, a system of any size is built of sub-systems that cooperate to accomplish the integrated whole. The University System Architecture will define, an “integrated system” to include a set of separately administered systems linked together to deliver convenience, speed, and accurate of transactions.

The most apparent barrier to any integration of enterprise services is the historical separation of applications under their service units. These isolated application systems are a natural result of past business justifications, funding techniques, administrative priorities, and narrow user communities served. The systems are isolated from one another because integration between applications was not a priority and vendor support for integration has been lacking. In most literature, these isolated administrative functions – both organizations and in application systems – is called “silos.”

Application silos are usually self-sufficient. Since a system was developed or purchased for a single administrative unit, that unit naturally feels responsible for all aspects of operation and planning. As a result, an application silo is a microcosm of all facets of the University System Architecture – identity management, security, even hardware selection and operation. Service providers control who has an identity and password to their service, what hardware is used and even where it is housed.

The successful future business environment must deliver integrated service as transparently as possible. Identities must be managed centrally. Security must be overseen centrally and administered through reliable
services. The current means of passing data between silos\(^6\) cannot support real-time service models and must be replaced with standards-based messaging techniques. All of these requirements point to a removal of application silos in favor of University-wide structures and services within the University System Architecture.

The unification of identity management and user management is required to deploy the service portal, Web single sign-on, and to increase security across the University. A transaction bus between applications, based upon Web Services, unifies services and exposes administrative data through secure, standard interfaces. Processing and database hardware can be organized to share loads under “grid” or “network-based” computing models. The result is that the fundamental functions of user identity, security, processing, data storage, and infrastructure can be managed centrally while business units concentrate on service delivery from their specific application.

**Return on Investment**

The overall benefits of the University System Architecture will be effectiveness, speed, distributed management, and confidence in security.

- More effective user interactions. Users will know where to go to access services and can customize the portal to their work style. With intuitive designs and sufficient guidance, users will assist themselves. Immediate feedback assures the user that the transaction was completed.

- Reduction in errors and service times. Errors will be reduced since users will be the source of the information and consistency checks can give immediate feedback. Self-service will reduce service latency and many services will be completed immediately as simple database changes.

- Confident security. Rigorous identity management will ensure that all persons with access to enterprise applications are known and have been approved. Distributed management of entitlements will give controls to service administrators who need to grant individual access.

- Cost-effective transactions with major suppliers. Coupling University systems to external suppliers will allow customer-initiated purchasing with immediate updating of financial data. Electronic transactions avoid many costs associated with paper processing, to the point that vendors offer discounts for electronic purchasing.

- Rapid deployment of services. Open standards software for inter-application messaging will ease deployment of new systems and allow for distributed authoring of intra-institutional applications. Vendors will develop increasing functionality through these methods.

- Real-time awareness of the business situation. Coupled University systems can pass information more quickly and reliably, making possible aggregation of information

---

\(^6\) Inter-silo communication is always a custom software development project to create a pair of “connectors” to act as message senders and receivers in each silo. These connectors must be maintained and modified for every change in the silo application. The software industry coined the term “Enterprise Application Integration” for the offering of pre-packaged connector suites and toolkits for developing new connectors. This approach will be replaced by Web Services, the technology recommended in this paper.
University System Architecture for Integrated Enterprise Systems

across systems for business analysis. Up-to-the-moment status of resources and commitments can be delivered to users.

**Prerequisites for Success**

There are several conditions for success of the University System Architecture. Listed below are major categories with explanatory detail and some examples.

- **Deploy a unified identity management and authorization infrastructure.** Security of all systems will depend upon trust in universal electronic identities and associated entitlements. All users must be registered with this single service and creation of identities must be regulated to balance flexibility against security. Silo authorization databases must be eliminated.

- **There must be common data definitions and acknowledge authorities for data items.** A dictionary of data items, common to all enterprise applications, must be hammered out and adopted. For each data item, there must be an authority that manages its values. The most commonly used data items about persons should be stored in a central registry database and requested by each application when needed, not duplicated for convenience.\(^7\)

- **User management must be provided centrally with distributed ability to manage entitlements for rule-based authentications.** Once security is tied to digital identities, business processes must change. Default authorizations created with an identity may be well below those needed by an individual to carry out business functions until a service administrator grants access. Service administrators may have to perform other functions, such as password resets, to maintain a desired level of security for their applications. Stronger authentication may be desirable (second password, tokens, biometrics, etc.)

- **Role-based authentication must be defined.** Service administrators must agree what default entitlements will be assigned for each role (student, faculty, staff, etc.). Roles must be defined and business rules set out for defining assignment of roles to identities based upon authoritative information items.

- **A portal software solution must be deployed.** The current PeopleSoft Enterprise Portal could be suitable for this purpose; however, there may be better alternatives.

- **An inter-application messaging architecture must be deployed.** Open standards for loose coupling of applications through Web Services (XML, SOAP, WSDL, WS-*) are forming quickly. A small service infrastructure will be needed to handle message routing, logging, etc. Eventually, the University will create a catalog of service specifications for use by programmers (UDDI).

- **There must be capable staff sufficient to deploy and maintain the technologies.** Three primary technologies, portal, identity management, and Web Services, will be largely new to Northwestern. NUIT staff must deploy and maintain them. The conversion of

---

\(^7\) The importance of this issue cannot be understated. Reliable identity management and security, consistent inter-application communication, and low-cost maintenance are impossible without rigor in the definition and use of institutional data. The University must complete work on this concern as quickly as possible.
Enterprise applications to new services will require both development and support of legacy applications. New job roles and training paths must be defined to reach an endpoint with enough applicable resources.

- Service units must have incentives to change. Service administrators and system administrators both must appreciate the importance of self-service, of University-to-vendor linkages, and of reduced errors and service times. All staff must see new modes of work as improving institutional effectiveness.
# Appendix A – Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Silo</td>
<td>A vertically-integrated, isolated business application which is not designed for integration with other applications and stands alone in data definitions, identities, authentication, and other factors.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Validating that the principal producing an identification token is that exact principal to whom the token is assigned.</td>
</tr>
<tr>
<td>Authority</td>
<td>An individual or process which is trusted always to be correct and consistent concerning a defined set of governed principals and their assigned identities.</td>
</tr>
<tr>
<td>Authorization</td>
<td>The act of ensuring that an authenticated principal is given access to only the services and data required to support allowed tasks, either explicitly or implicitly through group or role memberships.</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Sensing and digitizing physical characteristics of a person (fingerprint, retinal pattern, etc.) for use in authentication.</td>
</tr>
<tr>
<td>Connector</td>
<td>A software module used in application silo architectures to send and receive messages from other applications. These are often packaged in larger Enterprise Application Integration software suites.</td>
</tr>
<tr>
<td>Coupling</td>
<td>The programming of application-to-application real-time communication. A “tightly-coupled” pair of applications has special knowledge of one another and may have special software installed to accomplish the communication. By comparison, “loosely-coupled” applications use standards-based means of exposing and using services without special knowledge of the application asking for or providing service.</td>
</tr>
<tr>
<td>Entitlement</td>
<td>An approval to access data or applications within the resources managed. An entitlement could be implied by membership in a group (“financial administrators”) or it may be an individual permission (“may change salary data”).</td>
</tr>
<tr>
<td>Group</td>
<td>A logical grouping of identities maintained manually or defined automatically within Identity Management software. Groups are one means to grant entitlements or define roles.</td>
</tr>
<tr>
<td>Identification</td>
<td>The act of assigning a unique marker or a token to a principal, such that principals can be distinguished from one another.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identity</td>
<td>Electronic records that represent network principals, including people, machines, devices, applications, and services. At a minimum, this will include a unique identification, one or more authorization methods, and assigned authorizations. Synonymous with “digital identity.”</td>
</tr>
<tr>
<td>Identity Management (IdM)</td>
<td>A set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities within a legal and policy context.</td>
</tr>
<tr>
<td>Integration</td>
<td>A perceived unity of service while delivery is accomplished through cooperation of systems.</td>
</tr>
<tr>
<td>Portal</td>
<td>A Web application designed to bring together many important and frequently used information sources and application access points. Portals can be tailored to the user based upon role, entitlements, or personal taste.</td>
</tr>
<tr>
<td>Portlet</td>
<td>An application running within a portal that brings a single information source or service to the portal user.</td>
</tr>
<tr>
<td>Principal</td>
<td>A unique person or entity, in fact.</td>
</tr>
<tr>
<td>Registry</td>
<td>A directory-like database of identities, constructed from authoritative sources, holding passwords, entitlements, and other attributes useful for security across the enterprise.</td>
</tr>
<tr>
<td>Role</td>
<td>A property assigned to an identity based upon attributes from authoritative sources. Roles are much like groups, but are usually fewer in number and express wider concepts, such as “faculty” or “student”. Roles are important for tailoring portals.</td>
</tr>
<tr>
<td>Role-based (access, etc.)</td>
<td>Describing application settings that control access to resources through identity role attributes. Due to the broad nature of roles, restricting access based upon roles may not be sufficient for many applications.</td>
</tr>
<tr>
<td>Rule</td>
<td>A logical process for managing access control to a resource. When an identity requests access to an application or information, systems can apply local, global, or network-based rules to determine if access should be granted. Rules are programmed into systems by administrators.</td>
</tr>
<tr>
<td>Rule-based (access, etc.)</td>
<td>In contrast to role-based logic, access control based upon rules gives finer granularity and thus more confidence in security. Rule-based access can rely upon group membership, single or multiple entitlements, or even a particular identity as the requirement.</td>
</tr>
</tbody>
</table>
Appendix A - Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-service</td>
<td>A Web-based service model where information and transaction forms are displayed to the user, who fills in the necessary information and submits it for processing. The after error checking, the submission carries out the request immediately without manual review.</td>
</tr>
<tr>
<td>Service Administrator</td>
<td>The person responsible for defining and delivering a given University service offered inside or outside the community.</td>
</tr>
<tr>
<td>Service Unit</td>
<td>The University administrative unit responsible for delivering a given service inside or outside the community.</td>
</tr>
<tr>
<td>Shadow System</td>
<td>A local software database application that models the state of central administrative data for more timely reporting. Information in the local database may come from central administrative data feeds or by double-entering transactions.</td>
</tr>
<tr>
<td>Silo</td>
<td>See “Application Silo”</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>See “Web Single Sign-On”</td>
</tr>
<tr>
<td>Strong Authentication</td>
<td>A level of authentication above normal identity and password methods, usually adding some physical device (swipe card, USB key, thumbprint, one-time password generator, etc.) to decrease the risk of a compromised identity.</td>
</tr>
<tr>
<td>System Architecture</td>
<td>A set of agreed-to methods, standards, and techniques that promote both efficient division of responsibility and increased functional reliability while building complex functions from simple components.</td>
</tr>
<tr>
<td>User Management</td>
<td>The set of administrative actions taken to modify the state or status of a given identity, such as password reset, assignment of entitlements, suspension of service at separation, etc.</td>
</tr>
<tr>
<td>Web</td>
<td>The World-Wide Web. A set of communication protocols and representation languages (“markup languages”) that are used to deliver services across the Internet.</td>
</tr>
<tr>
<td>Web Services</td>
<td>A software infrastructure operating between applications on the Web using XML messages. Those applications providing services accept request messages and return result messages. This allows deployment of standard services available to all applications within the enterprise and potentially to trading partners.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web Single Sign-On</td>
<td>A software infrastructure serving Web-based applications. The Web infrastructure in which the applications are embedded uses a common authentication method for the first access and thereafter uses a session key or cookie to hold the credential for additional authentications. The result is a single authentication challenge across many applications, unless stronger authentication is needed at some point.</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language. XML is the fundamental communication language for applications that are coupled over the Web.</td>
</tr>
</tbody>
</table>
The University System Architecture organizes components into Platforms, Delivery Systems, and Applications. Common to all these components is the need for system management, directories (identities, entitlements), and security. Rather than addressing these needs individually, common services and structures are present.

Platforms include all hardware present in the network, from the central server through the user desktop/laptop/mobile device. Management and security of each of these resources is vital.

Delivery Systems are the utility software services present to promote interoperability and integration. Data management includes database services, backup, etc. Integration middleware includes the portal, identity management and access control, and Web Services.

The Applications are those systems delivering services to the user. Core enterprise systems hold institutional assets for finance, student records, research grant administration, and human resources. Specialized applications are usually dependent upon some core data and have wide use across the University (course management, alumni, library). Schools, divisions and departments may have applications that also need central data, but have narrow purpose. All applications will rely upon integration middleware to deliver identity, authentication, and authorization information.