
Middleware Business Case

Alpha University

A sample Middleware Business Case
developed by the Internet2 Middleware Early Adopters Team

Discussion DRAFT

Send comments to:
mw-buscase-comments@internet2.edu

26 October 2001



Executive Summary

The global adoption of the Internet is driving changes in all organizations, including Higher Education. Electronic interactions with students, faculty, alumni, staff, other educational institutions, businesses, and government are increasingly an integral part of the daily functioning of the enterprise and its members. Middleware, a layer of shared network software and information systems, is an integral part of managing access to and use of these critical networked services.

The deployment of middleware will allow Alpha University to increase the number of business transactions conducted on the network in a secure, cost-effective manner. We can reduce the time for action completion and the need for additional personnel, while we increase service availability and offerings. A shared campus-wide, middleware infrastructure will simplify application development and avoid duplicating the costs of information management, authentication, and authorization services in applications.

Consolidation of authentication and authorization services also benefits users of networked resources. Improved network-based, administrative services meet our constituents' expectations for the availability of self-service applications and offer location-independent access to on-campus electronic resources. Middleware will also reduce the deployment time for new network applications by providing standard, compatible interfaces to authentication and authorization services.

Middleware is as much about policy and procedure as it is technology. To receive the maximum advantage from a shared middleware infrastructure, an institution-wide commitment is needed. All directory-enabled application development and deployment should be coordinated to realize the potential. The process of implementing new applications changes in this environment.

An enterprise directory is the essential starting point in a middleware deployment. The enterprise directory supports applications as simple as online white pages to those as complex as a Public Key Infrastructure (PKI). A middleware infrastructure, like the network itself, is a strategic resource that can be leveraged into multiple services across the institution.

The benefits of a middleware deployment are enhanced security through better control of accounts and authorization, improved productivity of both users and service providers and larger operational economies of scale. It is important to consider the capital and operational costs to fully understand the impact this type of project can have within an enterprise network. Studies indicate that there is a short-run return on investment in addition to the foundation provided for long-term, strategic initiatives.

Table of Contents

EXECUTIVE SUMMARY	2
I. INTRODUCTION	4
II. STATEMENT OF OPPORTUNITY	6
III. BUSINESS CASE FOR MIDDLEWARE	8
Benefits	8
Specific Uses/Applications	10
Impacts	13
IV. PROJECT AND FINANCIAL OVERVIEW	15
Funding sources	15
Phase 1 – Enterprise Directory Deployment	16
Phase 1 – Project Costs	16
Phase 2 – Leveraging the Directory	18
Phase 2 – Sample ROI for a Leveraged Directory Application	18
V. RECOMMENDATION	20
GLOSSARY	21

Draft Contributors

Tom Barton, University of Memphis
Robert Brentrup, Dartmouth College
Louise Miller Finn, Johns Hopkins University
Jack Seuss, University of Maryland, Baltimore County
Lesley Tolman, Tufts University
Ann West, Michigan Technological University/Internet2
Renee Woodten Frost, Internet2/University of Michigan

I. Introduction

In their book, *"The E is For Everything,"* Richard Katz and Diana Oblinger discuss IT leadership strategies for universities in the areas of e-commerce, e-business, and e-learning. They note that institutions must identify the technical building blocks necessary to move forward without constraining future options and opportunities. To accomplish this within higher education, we have begun to deploy integrated administrative systems. To pursue this further, however, we need to consider how we integrate these systems into our academic and research enterprise. How do we share this critical data to run our course management systems or grant access to research labs? Katz and Oblinger highlight the need to view our IT infrastructure as a strategic resource and present the case for middleware, identifying the requirements for intra- and inter-campus solutions that provide identity, authorization, and authentication services across applications.

But what is middleware? Sometimes referred to as "software glue," middleware is a layer of software services that exists between the network and the applications and manages security, access, and information exchange. In today's Internet, each application provides these services, using vendor-specific technologies, leading to incompatibility and duplication of effort. Our Information Technology department maintains many repositories containing access information for the applications that we support. Well-designed applications, however, use vendor-neutral standards to access one *enterprise* service for each function — information access, authentication, and authorization — or middleware.

By its nature, middleware aspires to be vendor neutral and requires institutional tailoring—there are no vendors providing out-of-the-box, end-to-end solutions. Consequently, we have delayed planning and deployment of these critical services. However, the time is right to begin our implementation, because we can leverage experiences from other institutions to inform our own planning. In addition, middleware can address the institutional goals of

- offering on- and off-campus students, faculty, and staff around-the-clock access to administrative and academic resources
- enhancing distance-education students experiences
- streamlining our research administration and proposal management process
- reducing the need to hire additional technology staff to manage new applications

This document focuses on the importance of middleware in developing our campus IT infrastructure and the role of middleware services in IT strategic planning. It is organized five sections in sections, including this introduction:

- Section II frames middleware services in a broader institutional context by identifying several fundamental drivers impacting higher education and briefly discussing how middleware services can be used to support activities addressing these drivers.

- Section III offers the business case for middleware by addressing twenty-four applications that use middleware services at their core. This section offers the reader key internal drivers, coupled with the broader potential benefit of middleware services.
- Section IV outlines Alpha University's project overview and financial implications in deploying initial middleware services, including information about one-time and recurring costs.
- Section V offers our recommendation.
- Appendix A offers the reader a glossary to augment definitions included in the text.

II. Statement of Opportunity

As noted earlier, access to information and the information economy are driving higher education to change. Legislation passed in the last decade to reduce government administrative costs further pressure academe to re-think and re-architect our own institutional processes. In addition, our students, faculty, and staff have increasing expectations of electronic access, while our campuses would like to offer more online services to their constituents.

The Higher Education sector is poised to benefit from the appropriate deployment and use of middleware. A number of drivers both inside and outside our institutions are moving our campuses toward implementing this infrastructure. They include:

Accommodating government legislation to reduce paperwork, ensure privacy of information, and mandate the use of electronic services wherever possible. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the guaranteed access to, portability of, and renewability of health insurance. It requires the creation of electronic identifiers and standards for electronic access and privacy of health care records. The government and health care industry are using middleware to facilitate the security stipulations of this Act.

Subsequent legislation, such as the Electronic Signature in Global and National Commerce Act, effective October of 2000, defines the legal status of electronic signatures in business transactions. A number of initiatives to implement secure electronic transactions for public services offered by the Federal Government are in progress. Higher Education is researching inter-operable solutions, which would be used in grant submission, financial aid reporting, and, in short, any financial or information interaction with the State or Federal Government.

Increasing requirements for interdisciplinary and inter-institutional research and collaboration. Academic collaboration requires appropriate sharing of data and resources among institutions. Scientific communities need to provide common access to discipline-specific resources such as telescopes and microscopes at distant locations. Licensing of and access to scholarly materials must accommodate students and faculty at remote locations for distance-learning initiatives, shared research, and collaborative publication and presentation development. All of these applications require management of personal profiles, identity, and security/access controls using standards-based technologies and information exchange, inter-operating among institutions.

Fund raising. Linking alumni and friends back to the institution through a campus portal is a high priority among many campuses. The benefit is higher satisfaction among those connected with the institution, resulting in higher contributions. Managing the security, privacy, and access controls associated with a portal requires yet another authentication/data management system, unless deployed using middleware.

Changing needs of teaching and learning. Instructional Management Systems that allow faculty to exchange course materials and set up online teaching environments need mechanisms for managing student and collegial use. In addition, the electronic experience of distance-learning students becomes a critical success factor in their overall perception

of the institution. Schools must be able to grant almost instant access to electronic services once a person has entered the institution, enabling use of e-mail, library resources, and online course work.

Digital libraries are also facing similar access issues: how do we allow the appropriate use of online materials and maintain the privacy of the person using them? Libraries need scalable, interoperable authentication and authorization with particular needs.

Escalating expectations for the pervasive access to, and use of, technology.

Expectations for individualized service are changing with the advent of secure, mass customization of online applications available today. Communities within our institutions, such as undergraduates, alumni, corporate partners, want access to information and services they understand and need. In the research realm, electronic personal security services are now an impediment to the next-generation computing grids. Our outreach to all our communities must be both tailored to the audience and able to be customized by the individual.

Increasing budgetary pressures. Online procurement accelerates the transaction time and more importantly can organize the buying power of the organization through a single delivery medium that can be monitored. This translates into volume discounts and savings for the organization. Middleware services can enable online purchasing by providing buyer authentication and authorization information to each online vendor.

But how do we address these drivers? Middleware can enable these new services. Explicit in the architecture is the concept of security and flexibility, creating an environment that is both mindful of and tailored to the needs of those using the applications. Deploying standard, accessible, and secure technologies will enable institutions to interact effortlessly without the traditional constraints of location, time, and platform.

III. Business Case for Middleware

The deployment of core middleware (directory, authentication, and authorization services) produces seven major outcomes that affect the institution:

- 1) Reduces the number of credentials constituents must know to perform actions for which they are authorized.
- 2) Reduces the implicit denial of service experienced by new members of an organization. New staff, for example, must give information to multiple people before they can use online resources to which they should have access. Before and during this process, the person cannot perform the functions for which they were hired.
- 3) Reduces the operational and management overhead of enabling our constituents to perform actions for which they are authorized. In particular, it reduces the incremental cost to implement a new online service.
- 4) Reduces the operational and management overhead of disabling authorization for clients who should no longer have access to online resources.
- 5) Enables the organization to quickly modify a client's access permissions as the client's role, and so their set of authorizations, changes.
- 6) Improves the quality of auditing of authorized actions across the organization by using permanent identifiers common to all applications.
- 7) Increases the institution's confidence that the credential presented by someone to perform an authorized action is presented by the person to whom the credential was issued. This can be accomplished by reducing the number of people and offices involved in issuing credentials and focusing on improving the procedures followed by those few offices which do issue credentials.

Benefits

The implementation of these seven items improve the organization's operational efficiency and security posture. Their benefits include enhanced security, simplified network and online service access, and economies of scale.

Enhanced Security

Many types of online services, including host operating systems, web services, remote access, and vertical applications, can be integrated with an enterprise directory. Once integrated, the task of managing user access to all of those services is reduced to just one place — in the middleware. And because the enterprise directory is integrated with our key administrative systems, there is no need to do *ad hoc* research on the list of users to determine who is an active student and who graduated last spring, for example. Their status is reflected in the directory. Hence, the amount of work to disable old accounts is small. Alpha University can largely eliminate the security risk presented by the existence of many active accounts no longer used. An additional benefit to our distributed environment

is that our identity management will be administered by a smaller group of staff and held in one protected data repository (enterprise directory), using single sign-on capability and data encryption.

By providing a way to express our access control policy, the same infrastructure can also provide authorization services to applications, extending our current security practices. Examples include differential access to dialup ports and wireless access points, restricted access to web content, restricted email relay services for members of the campus community, and controlled access to central email distribution lists. A sample list of applications follows this section.

Because the same user credential is presented to all integrated services, all system and application log files reference the same identifier. This greatly enhances after-the-fact auditing of online activity, allowing for more complete investigations of alleged cases of abuse and increasing institutional due diligence, thereby reducing our liability.

Simplified network and online service access

Middleware enables unified access to many online services (see examples below), resulting our constituents needing only one username and password. Because of the integration with web based applications, solutions to common service issues like remote access to library databases, unified and personalized email addressing, and self-service account management are enabled using a common infrastructure.

Middleware can also provide customization (tailoring to one's organizational role) and personalization (storage of personal preferences), critical elements for creating a campus portal strategy. The campus portal, coupled with web-based single sign-on provides the ideal way of deploying application services to our constituents.

Economies for Central and Distributed IT

IT routinely maintains a number of separate, user-identity repositories for maintaining University applications. We categorize these systems into two groups:

- primary sources —systems into which people are added when they first arrive at Alpha University (i.e.: Payroll, Student Registration)
- secondary sources — systems providing additional services such as the badging systems, library patrons, mainframe security, email systems and Alumni

Middleware provides a unified means of enabling and disabling access to a wide range of online services. The alternative is to manage access to each service separately, requiring more staff per service. However, the same number of staff can manage a larger suite of services if integrated using middleware as the common. And, since the same provisioning services are used for each application, the staff-training burden is reduced. Outsourcing applications using the same credential stored for other campus services also becomes possible and enables quicker application deployments. However, this provides economies of scale that can be difficult to quantify, since it involves the reallocation of efforts from the departments' technical staff to a central group.

Having consolidated systems and business processes for identity and account management and authentication and authorization services also reduces the cost and time to deploy new applications. Since these services do not need to be created for each

new application, the cost and time of doing so, and the recurring cost of independently maintaining those services are avoided.

Additionally, Alpha University will be able to provision network traffic according to policy and financial decisions using middleware. This infrastructure is needed to work in conjunction with the physical network to enable policy-based routing and switching.

Other opportunities

Middleware, especially enterprise Lightweight Directory Access Protocol or LDAP-accessible directories, is on its way to becoming a standard element of an enterprise's IT infrastructure, just as TCP/IP has become. Increasing numbers of off-the-shelf applications are designed to integrate with standard middleware, making its implementation a valuable investment for the organization in traditional return-on-investment (ROI) terms. In addition, several new types of inter-institutional applications using middleware are being developed and tested, chiefly under the auspices of the Internet2 Middleware Initiative.

Specific Uses/Applications

Following is a list and related descriptions of types of specific middleware-integrated applications known to be in production at other schools at the time of writing this document. These range from uses as simple as white pages to those as complicated as PKI. The several technical terms employed in their descriptions are explained more fully in the Glossary. Application descriptions have been grouped into broad application categories to help the reader understand their role in an overall IT infrastructure.

Some use is made of two special terms in the descriptions below. The first, customization, refers to run-time modification of capabilities presented to users based on their role in the organization or other administratively-determined per-user capabilities. Personalization refers to user-selected modifications to the options presented to them. As examples, customization enables an instructor to post grades for her classes only, and personalization permits her to specify her vacation message after she has posted the grades.

Resource Discovery and Scheduling

- 1) *White pages*. A service that offers searching capability for discovering contact information for people in the organization.
- 2) *Yellow pages*. A service that offers searching capability for discovering contact information for departments in the organization.
- 3) *Enterprise-calendar authentication, customization, and personalization*. Several calendar products integrate with LDAP for authentication allowing the publishing groups available for group scheduling, storing information about schedulable resources, and storing individual application preferences.

Messaging

- 4) *Mail box access, customization, and personalization*. Specific LDAP-integrated mail systems offer a number of features. For example, constituents can pick their preferred access methods. They can also specify a vacation message and subsequent forwarding, and folder sharing. Additionally, technical administrators can set characteristics such as mailbox quotas for users.

- 5) *Authenticated email relaying.* The University email relays must be restricted to prevent abuse by spammers. However, with an LDAP-integrated mail system, relays can be used by authenticated members of the campus community, regardless of their location on the Internet.
- 6) *Email routing.* Some email transport systems can use LDAP to lookup per-recipient attributes to determine precisely how an email is to be processed, effectively making the enterprise directory into an organization-wide “aliases” file. This allows email addresses to reflect how recipients (or the organization) would prefer their address to be published, rather than being limited to containing specific email routing information.
- 7) *Institutional, email-distribution lists.* Institutional groups, such as all faculty in a given college, all students in a given course section, or all staff in a given department, can be automatically maintained in the directory and used to facilitate email messaging.
- 8) *Authorized access to institutional email distribution lists.* At least one email-transport product authenticates the sender of a group message and determines if a user is permitted to send to that group. This permits the deployment of a mass-email service that does not rely on central IT staff to be involved in the actual transmission of mass email.
- 9) *Secure discussion groups.* Some groupware products can integrate with an LDAP directory for authentication and determination of roles for interacting with closed discussion groups. These roles include who can read, post to, and administrate a given group.

Web Applications

- 10) *Web authentication.* Some web servers can use LDAP directly for simple authentication. Alternatively, authentication may be indirectly referred to an LDAP directory or other authentication service by means of a web Integrated Sign On system.
- 11) *Web authorization.* To make access control decisions, some web servers can obtain attributes and group memberships from an LDAP directory, enabling the organization to selectively restrict access to web content.
- 12) *Web publishing.* Some web servers enable authorized users to configure authentication and authorization for their published content, permitting the web administrator to delegate responsibility for those tasks.

LAN Management

- 13) *Desktop and computer cluster authentication, authorization, customization, and personalization.* Numerous desktop/LAN management products are enabled most notably by either Microsoft’s Active Directory (AD) or Novell Directory Service (NDS) directories.
- 14) *Synchronization of disparate directories.* NDS and AD are the most prevalent directory technologies used by LAN management applications, and iPlanet and openLDAP are most often used for enterprise directory services. In many organizations, it may be beneficial to operate at least one directory for LAN management and another for enterprise directory services, and to maintain them in

appropriate synchrony automatically. Several examples now exist of processes that synchronize selected attributes in NDS and AD directories from iPlanet and openLDAP directories, and for maintaining all in synchrony using metadirectory technologies.

- 15) *Self-serve network registration.* Many residence-hall networks and some campus networks implement a scheme in which computers with an unregistered network adapter are dynamically placed in a severely limited “DMZ” network. In this situation, the computer’s network adapter is registered to an LDAP authenticated user and assigned a real, non-DMZ, IP address. This facilitates the process of installing new or replacement computers on the network, restricting access of a network port to authorized persons, and tracking which user was using a dynamically-assigned IP address at a given time.

Remote Access Services

- 16) *Remote and wireless access authentication, authorization, and customization.* Many network access servers, including most dialup servers and some wireless access points, can offload authentication and authorization functions to a central service. Some products, in turn, can rely on an enterprise directory to provide them with an authentication service and authorization data. As a result, we can limit access to a given dialup pool or wireless access server to those users in a given group in our enterprise directory. We can also customize the user’s “access profile”, enabling different characteristics such as maximum session length or special security filters to be applied to a given user’s dialup or wireless session.
- 17) *Authenticated, proxy access to remote licensed databases.* Proxy web servers and URL redirection systems can restrict the use of specified resources to authenticated persons. This enables remote access to licensed databases.

Account Management

- 18) *Automated and self-serve account management.* Identifiers and accounts can be created, enabled, disabled, and deleted automatically. The process is driven by changes in administrative systems coupled with business logic for this purpose. Card-swipe systems or web sites mediate self-serve maintenance of passwords, PINs, optional accounts, and other self-maintainable directory data.
- 19) *Storage and distribution of digital certificates, public keys, and certificate management information.* An enterprise directory is an essential part of a Public Key Infrastructure (PKI) deployment.
- 20) *Distributed administration of ad hoc groups for messaging and authorization.* Several applications mentioned elsewhere in this list can take advantage of directory resident groups, and so it is important to manage their memberships well. Some groups are best managed by programs embodying business logic, but others are by nature *ad hoc*. Maintenance of their membership can be delegated to appropriate users or groups of users, enabling applications of *ad hoc* groups to be facilitated by enterprise middleware.

Application Servers

- 21) *Portal authentication, customization, and personalization.* Many portal products support LDAP authentication, and some also enable either live or batch provisioning of customization information from a central directory service. However, there is significant movement by both vendors and in-house developers to directly integrate portals with administrative systems, rather than going through an enterprise middleware infrastructure.
- 22) *Course management system authentication, customization, and personalization.* The situation is similar to that for portal systems.
- 23) *Shell account authentication and authorization.* Several flavors of the UNIX operating system use LDAP for authentication and naming services, enabling LDAP-facilitated single sign-on to extend to shell accounts.
- 24) *Application server authentication and authorization.* Some applications servers can refer authentication to LDAP, some can also refer group tables to LDAP, and some can have proprietary group tables updated from an enterprise directory service.

Impacts

While implementing middleware, a number of issues may affect our deployment.

Considerable time and effort to conduct campus-wide planning, review, and negotiation processes. Educating the campus and stakeholders on the benefits and implications of middleware is necessary for a long-term, viable implementation. Outcomes of this deployment include developing new administrative policies and processes to enable accessing and using institutional data by online applications and security systems. After implementation, this education and negotiation should continue to accommodate on-going change in staff resources and computer, data, and institutional systems and processes.

Political impact from establishing or revising data stewardship and policies. Potential enduring challenges can arise when negotiating processes, data use, data ownership, and application use with stakeholders across campus. Who determines how a software developer can use (or display) a social security number, for example?

Modest increases or reallocation in capital equipment and staffing requirements for central IT. Depending on the size and scope of middleware project and relevance of existing infrastructure, we will need to plan for increased or re-purposed staff time, new server and software resources, and possible network upgrades. Additional resources and guidelines will be needed as more applications use this new infrastructure. For example, policies and requirements for identifying what applications can use the campus directory, how they use it, and how it is funded to accommodate the increased load are important considerations in its ongoing maintenance.

One-time costs to retrofit targeted applications to new central infrastructure. In addition to implementing new applications, institutions will want to alter appropriate existing services to use middleware data and security systems to reduce the number of data and access repositories they need to manage. This will take staff resources to complete, but should save time in the future.

Modest costs to build and maintain feeds from systems of record to central directory services. To deploy middleware, information on people, such as status, access, and contact data, will be needed by the enterprise directory. By querying existing student and HR systems, we can populate or update appropriate directory attributes. This feed process may change as the institution considers where best to store new and existing enterprise data elements. Initial setup and on-going maintenance and alteration will take additional staff resources.

Legal impact from new legislation and possible risk of litigation. Institutions interested in sharing applications and related data with the public (such as white page information) and with other schools risk sharing protected personal data. We must be aware of existing and pending legislation regarding privacy of data, the impact it may make on their directory services implementations, and the potential for litigation.

IV. Project and Financial Overview

A middleware deployment on our campus will provide a financial benefit for existing and future network initiatives. In phase one of the project, we will build the enterprise directory. Once this is complete, we can proceed with phase two and leverage the directory to deploy applications. It should be noted that phase two will require additional capital and ongoing operating funds as new applications are deployed or existing ones are retrofitted to use the directory. Moving campus services to using middleware is an evolutionary process and will continue into the future.

Also important to remember is that the bulk of phase one of the project costs will be incurred across the University, comprising staff time spent by IT technical personnel and data custodians.

Funding sources

There are a number of methods of securing funds for both phases of this project and our final decision will depend largely on the interests of the existing staff and their expertise and level of commitment to other production systems. It is possible to absorb the cost of the staffing into existing initiatives or ongoing operational budgets, or it may be submitted to management for funding as a new initiative. This decision will depend largely on funding availability and our willingness to take on new initiatives.

Scenario 1 – Absorbing the staffing cost

Middleware is a very technical subject whose value is difficult to convey to persons not knowledgeable about it. However, we can pursue the planning and information gathering stages in parallel with identifying the funding sources.

Using existing staff, allows us to start phase one earlier and has a number of effects:

- The project will not pose as much risk when mingled with other ongoing initiatives.
- The project will begin sooner, but require a longer project cycle than if funded on its own.
- The expertise of in-house staff will be leveraged, a valuable asset as we begin to form alliances with data owners, application developers, and end users. There may be more acceptance of middleware among the existing staff, as well. Furthermore, participation on the directory implementation team will provide interesting challenges to senior staff and development opportunities for junior staff. Such a project could be considered as a part of a staff-retention package.
- The need for an enterprise directory can be demonstrated without substantial out-of-pocket, capital costs.

Scenario2 – Requesting new funds for staff

The second scenario entails seeking funding for additional staff to work on or release existing personnel to design and deploy the enterprise directory. While the cost is considerable (See table below), it is very difficult to implement new services while supporting existing production ones. We estimate phase one will require an additional year to complete if not augmented with additional staff.

Phase 1 – Enterprise Directory Deployment

As noted earlier, the initial planning and tasks can be accomplished without incurring capital costs. Once software and hardware platforms are identified, however, we will review current inventory and order those pieces necessary to complete the directory implementation. Phase one of the project entails

- assembling the Directory Services team including new or existing staff. We will decide how to include University data custodians in this process as well.
- surveying our campus environment and identifying all systems that maintain directory data about people.
- surveying what common identifiers are used on campus.
- deciding how to leverage existing identifiers or create new.
- developing the directory service architecture and identifying the required data flow in and out of the directory. Will the directory be authoritative for any of its data? Will it update the systems of record?
- meeting with the data owners to obtain permission for the inclusion of their data in the directory and if possible establish an ongoing forum for directory information exchange.
- ordering and deploying new equipment and software
- selecting a targeted application for the new directory, such as online white pages, and prototyping the entire process of publishing this information from the directory. This process will provide a proof of concept for our architecture and highlight issues that need further development
- developing an on-going budget to continue the operation and development work needed to integrate applications into the directory. This budget will include the maintenance contracts for the servers and software, as well as an expansion capability for future capacity requirements

Phase 1 – Project Costs

The anticipated cost of the deployment of an enterprise directory service is provided below. We have sized the architecture to handle 10,000 entries, including faculty, staff and students.

Phase one of the project will take approximately one year to complete for scenario two and two years for scenario one.

Hardware Costs	Year 1 (FY01)		Year 2 (FY02)	
	Capital	Operating	Capital	Operating
Directory Server (1)	\$34,000			\$3,400
Database Server (1)	\$31,500			\$3,150
LDAP/Policy Servers (2)	\$10,000			\$1,000
HARDWARE TOTAL	\$75,500			\$7,550

Software Costs

Directory and mail services bundle	\$25,000			\$10,500
Database Package	\$32,300			\$7,500
Development Tools	\$4,500			\$450
Data Modeling Software	\$6,450			\$645
SOFTWARE TOTAL	\$68,250			\$19,095
HARDWARE/SOFTWARE TOTAL	\$143,750			\$26,645

Staff Salaries with Benefits Outlined in Option 2

Sr. Software Analyst/ Project Lead (1 FTE)	\$85,000			
Database Developer /DBA (1 FTE)	\$95,000			\$104,500
Web Developer (1 FTE)	\$70,000			\$77,000
Directory Engineer/Architect ¹ (1 FTE)	\$40,000			\$88,000
Equipment/Training/supplies	\$10,000			\$5,000
STAFFING TOTAL	\$300,000			\$274,500
GRAND TOTAL INCLUDING STAFFING	\$443,750			\$301,145

¹ The Directory Engineer/Architect is needed in second half of project. The first half is dedicated to front-end development work, working with data owners and setting up the metadirectory/registry.

Phase 2 – Leveraging the Directory

In the short term, industry analysts such as The Burton Group maintain that investment dollars spent on an enterprise directory service will produce a return of five times the investment. The final savings will depend on the number of users, the size of the network and the number of directories integrated into the enterprise directory. In the long term, strategic initiatives such as stronger security and ubiquitous access to applications and resources across the network will be realized. There are several components to consider when building the return on investment model.

Cost savings are realized through the reduction in IT resources required when account management is centralized. In a decentralized environment, this is not always quantifiable in dollars, but is realized in the amount of time freed up for IT personnel to spend on higher-level tasks. Economies of scale then emerge as the task of account management is centralized.

Lost productivity is traditionally not measured in an academic environment, however in today's competitive economy, it should be considered. Account and resource provisioning, as a middleware process, can enable new users to become productive faster than ever before. The wait time for access to networked resources can be trimmed from days to hours.

Increased opportunity is available to the University because we can deploy applications faster by tying new services to our existing middleware.

Increased security is achieved when account management for networked resources is centralized and automated. The change in user accounts as people flow in and out of the institution serves to minimize access to critical resources, which protects these resources from unauthorized access and usage.

Phase 2 – Sample ROI for a Leveraged Directory Application

To estimate the potential return on investment (ROI) that such a deployment could offer, we have used a model (<http://www.businesslayers.com/roi.asp>) designed to calculate an approximate payback scenario for this type of application in a corporate environment. We recognize there are many differences between a higher educational institution and a company; For example, many of our users are students instead of employees and should be considered differently in the productivity metrics. However, the exercise is a good one and worth considering as an illustration for the deployment of a directory-enabled application.

Within the next two years, we plan to proceed with phase two and leverage our directory for the e-provisioning of IT services across our organization. Eprovisioning is the automatic setup and removal of user accounts and services as people enter and leave our institution. Today this is handled by hundreds of IT people, at a cost that is ever increasing.

- When we consider the number of accounts we maintain for faculty/students/staff and how frequently they are created, modified or deleted, we pay an annual cost of \$756,000.

- Lost productivity costs to Alpha University mount to \$2,062,500, based on a two-day waiting period for each new employee/student. This dollar figure represents the total amount of work not done by new constituents unable to access their new accounts.
- Opportunity costs, those costs associated with the productive tasks a person could have accomplished had they been provisioned faster and/or more accurately, tally to \$7.8 million.

The total cost to Alpha University for the manual provisioning of IT services, lost productivity, corrected mistakes and use of services by past employees/students is \$10.7 million per year. Of course, these are not costs that can be recouped, but should be considered as potential savings in the future.

The cost to deploy an E-Provisioning application that would leverage the enterprise directory and automatically create/modify/delete accounts based on a person's role within Alpha University would cost approximately \$607,000. The application would provide a fifteen percent savings by streamlining and automating our IT provisioning services, for a savings of \$1.6 million per year. Therefore the payback time for this type of application, which would fully leverage the enterprise directory would be just under five months.

V. Recommendation

As noted earlier, IT infrastructures, such as our network and administrative systems, are strategic resources that once built, can be leveraged to service needs across the institution. Deploying a middleware infrastructure is no exception. In fact it allows us to further use our data and network to offer tailored, secure, and interactive services in areas of teaching, research, and recruitment that we cannot afford to offer now. Middleware allows us to move forward by broadening our future service possibilities through the centralization of provisioning information and systems—identity, authorization, and authentication—and assignment of access based on a person's role within the institution. Once these information, process, and technical systems are in place, the effort to quickly add new services or people to our service mix is minimal compared with today.

Furthermore, the deployment of middleware supports our institutional goals of

- offering on and off-campus students, faculty, and staff 24 hours access to administrative and academic resources
- enhancing distance-education students experiences
- streamlining our research administration and proposal management process
- reducing the need to hire additional technology staff to manage new applications.

Therefore, based on the short payback period, the relatively low risk, and the direct contribution to our institution's goals, we recommend approval for following:

- deployment of an enterprise directory and related identity services, as outlined in phase one of the project.
- implementation beginning next first quarter

Glossary

Authentication – The process of establishing whether or not a real-world subject is who or what its identifier says it is. Identity can be proven by

- Something you know, like a password;
- Something you have, as with smart cards, challenge-response mechanisms, or public-key certificates; or
- Something you are, as with positive photo identification, fingerprints, or biometrics.

Authorization – The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

Core middleware – The suite of services consisting of institutional identifiers, and enterprise directory, authentication, and authorization services.

Directory – The operational linchpin of almost all middleware services. It can contain critical customization information for people, processes, resources and groups. There are a number of different types of directories: NOS-administration directories, application-specific directories, enterprise directories, purpose-specific directories, and general-purpose, standards-based directories.

Directory-Enabled Networking (DEN) – A specification for how to construct and store information about a network's users, applications, and data in a central directory. This can enable applications to be developed that will automatically learn of user access privileges, bandwidth assignments, and resource policies, and provide services accordingly.

Early Adopters – The campus test-bed phase of Early Harvest, deploying core middleware at thirteen US campuses. Based on this experience, Early Adopters are developing roadmaps for other campuses to follow in their own deployments. Both Early Harvest and Early Adopters are sponsored by Internet2 and received some funding from the NSF.

Enterprise directory – The central University look-up repository that holds data regarding University people and services. The information held in an enterprise directory can be consolidated from a number of other data sources or be the primary source.

Identifiers – A function that maps real-world subjects into name or character strings, so that distinct subjects have distinct strings. A real-world subject may be a person, an object (i.e.: a printer or a file), a group, or a department. A real-world subject can have multiple identifiers. When campuses seek to interoperate, issues arise on the type of identifier that needs to be exchanged, and the forms and policies for that identifier. Moreover, to the degree that identifiers enable users to access other forms of electronic credentials, there may need to be agreements and consistency between campuses about the policies associated with classes of identifiers.

Internet Message Access Protocol (IMAP) – A method used by many email-client programs to interact with a mail server to enable a user to receive messages and manage their email folders. IMAP's chief distinction is that users may keep all of their mail folders on a central server and so have location independent access to their email.

Internet2 – A national project to research and develop advanced Internet technology and applications vital to the research and education missions of higher education. Over 170 U.S. universities, working together with partners in industry and government, are leading the Internet2 project. Internet2 is working to enable applications, such as telemedicine, digital libraries and virtual laboratories that are not possible with the technology underlying today's Internet. As a project of the University Corporation for Advanced Internet Development (UCAID), the Internet2 project is not a single separate network, but rather joins member network application and engineering development efforts together with many advanced campus, regional, and national networks. <http://www.internet2.edu>

Integrated Sign On (ISO) – A type of credential forwarding mechanism used to forward authentication credentials to participating servers, usually used in reference to the web. Generally, upon first encountering a server participating in a web ISO system, a user's browser is redirected to an ISO server to authenticate. A special cookie containing a resultant credential is cached for a limited time in the user's browser, which is then redirected back to the original server. Participating servers are configured to first check for this cookie to obtain the user's credentials, effecting a single sign-on system.

Lightweight Directory Access Protocol (LDAP) – A protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 compatible directories.

Metadirectory – An information-flow process that synchronizes data repositories based on business rules. For example, the metadirectory detects a new employee has been added to the HR system and updates the enterprise and departmental NOS directory accordingly.

Middleware – A layer of software deployed between the network and applications. This software provides services such as identification, authentication, authorization, directories, and security. In today's Internet, applications usually have to provide these services themselves, which leads to competing and incompatible standards. By promoting standardization and interoperability, middleware will make advanced network applications much easier to use.

NOS-administration directories– A directory deployed to serve the needs of a network operating systems. This includes directories such as Novell's NDS (Netware Directory Services) or Microsoft's ADS (Active Directory Services).

Public Key Infrastructure (PKI) – The software, protocols and legal agreements that are necessary to effectively use digital certificates combine to form a Public Key Infrastructure (PKI):

- A Certificate Authority (CA), that manages and signs digital certificates for an institution
- Registration Authorities, operating under the auspices of the CA, that validate users as having been issued certificates

- PKI management tools, including software to manage revocations, validations and renewals
- Directories to store certificates, public keys, and certificate management information
- Databases and key-management software to store escrowed and archived keys
- Applications that can use certificates and can seek validation of others' certificates
- Trust models that extend the realm of secure communications beyond the original CA
- Policies that identify how an institution manages certificates, including legal liabilities and limitations, standards on contents of certificates, and actual campus practices

Post Office Protocol (POP) – An old and simple method used by many email client programs to enable new mail to be retrieved from a central mail server and stored on the user's computer.

Quality of Service (QoS) – A measure of performance for a transmission system that reflects its transmission quality and service availability.

Remote Authentication Dial In User Service (RADIUS) – A protocol for carrying authentication, authorization, and configuration information between a network access server (e.g., dialup server or wireless access point) which desires to authenticate its links and a shared authentication server.

Single sign-on – A method of authentication that allows a user to log into a network, and, for a period of time, have his or her credentials passed to the requested applications, enabling the use of the resource without requiring separate authentication for each one.

Simple Mail Transfer Protocol (SMTP) – The Internet standard means of transporting email from a sender to a recipient.

SMTP AUTH – A means of authenticating the originator (a user as they initially send an email) or relay (an email transport system along the route to the recipient) of an email message, so that the sender of the email can be identified. Some email client programs will automatically and silently supply authentication credentials to an SMTP AUTH configured outgoing mail relay, easing the deployment of applications requiring authenticated email. For definition of SMTP, see above.

Virtual LAN (VLAN) – A group of devices on one or more LANs configured (using management software) to communicate as if they were attached to the same wire, when in fact, they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

Virtual Private Network (VPN) – A virtual network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

X.509 – A specification that describes the format and semantics of certificates and certificate revocation lists for PKI.