



The Florida State University: Identity Management & NMI-Component Integration

NSF Middleware Initiative (NMI) Integration Testbed Case Study Series

Series contact: Mary Fran Yafchak, Southeastern Universities Research Association,
maryfran@sura.org.

The NMI Integration Testbed Program provided practical evaluation of NMI components within the context of real projects and application scenarios from June 2002 through November 2004. During that time, NMI Testbed sites collectively submitted over 220 evaluation reports to middleware component developers as direct feedback into the NMI development cycle. Site representatives also actively inspired, promoted and facilitated the integration of middleware throughout their institutions.

The NMI Integration Testbed Case Study Series documents the most significant influences and outcomes of NMI Testbed sites' middleware integration efforts, highlighting intersections with established projects, application contexts and influences, drivers for innovation, decision points and challenges. Through this documentation, the work of these pioneering institutions is captured to provide a breadth of insight and approaches for others to use towards successful middleware development and deployment.

This NMI Integration Testbed Case Study Series is sponsored by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium of EDUCAUSE, Internet2, and SURA. Additional support was provided by the National Science Foundation Cooperative Agreement NSF 02-028, ANI-0123937.

Copyright © 2005 The Florida State University. The Florida State University permits use of this content for noncommercial purposes with proper attribution. All rights reserved.



Executive Summary

FSU's need for a comprehensive, standards-based identity management solution evolved over time, driven by the increasingly robust and complex IT services FSU offered to its students, faculty and staff. By 1997, Florida State University (FSU) IT leaders were searching for a comprehensive identity management solution to implement a secure, single sign-on (SSO) capable, centralized authentication service on a campus-wide basis.

IT management and technical staff were acutely aware not only of the need for SSO, but to discontinue the use of social security numbers (SSNs) as primary student identifiers. Organizational and policy changes on campus also created the need for a centralized directory solution that put its two Lightweight Directory Access Protocol (LDAP) directories on a consolidation course as part of the new, single campus directory solution.

The path FSU took in evaluating and determining what their identity management solution should look like was influenced by information from Internet 2 and from FSU's participation in the National Science Foundation (NSF) NMI (NSF Middleware Initiative) Integration Testbed. Together, these groups made clear to FSU the advantages they would gain from implementing an NMI-compliant solution. Initially, FSU focused their resources on

deploying a new solution on their own. However, when campus resources were redirected due to the university's reprioritization of IT initiatives, FSU's IT leaders then decided they must retain an outside vendor that could provide a comprehensive solution that included consulting, software and maintenance support services. The solution's design needed to provide for an enterprise-level metadirectory that would provision data from the metadirectory to other services and applications. Through a thorough RFQ process, FSU selected Novell's eDirectory product, as only Novell's solution could integrate with FSU's ERP/People soft implementation.

As of Fall 2004, the Novell eDirectory software had been deployed. FSU deployed an adaptation of NMI-EDIT's standard enterprise directory design to fit with their Novell eDirectory solution and PeopleSoft deployment. This solution has allowed FSU to merge their LDAP directories and discontinue the inappropriate use of SSNs. Also, since Novell's eDirectory is NMI-compliant, the solution provides FSU the option of implementing other NMI technologies in the future.

For more information about FSU's identity management solution, contact Joe Lazor at JLazor@admin.fsu.edu.



NMI Components Highlighted in this Case Study

The NMI components discussed in this case study series encompass NMI Releases 1 through 4. Information about NMI Releases can be found at <http://nsf-middleware.org/>.

eduPerson Directory Schema

eduPerson contains identity-related attributes for higher-education institutions to deploy for enabling inter-institutional collaborations.

Home site: <http://www.educause.edu/eduperson>

Conventions and Best Practices

These NMI-EDIT documents reflect current NMI research in campus core middleware. The architecture approaches and policies promulgated here are in use at several leading campuses and institutions. Discussion includes “A Recipe for Configuring and Operating LDAP Directories,” “Practices in Directory Groups”, “Metadirectories Best Practices”, and “Enterprise Directory Implementation Roadmap” documents.

Home site: <http://middleware.internet2.edu/dir/>

Shibboleth Software

The Shibboleth technology supports inter-institutional sharing of web-based resources subject to access controls.

Home site: <http://shibboleth.internet2.edu>



The Florida State University: Identity Management & NMI-Component Integration

The Florida State University, a Carnegie I, public University located in the State capital of Tallahassee, Florida enrolls over 67,000 students, with 39,000 in residence, 28,000 on-line with an additional 11,000 faculty and staff. Other resident campuses are located in Panama City Beach Florida, London, England, Panama and Puerto Rico. Organizationally, FSU has 17 colleges and schools responsible for administering undergraduate and graduate degree programs. Centralized organizations provide financial and administrative support services, student services and, to a degree, information technology (IT) services.

As they moved into the new millennium, FSU IT leaders and staff were developing a comprehensive identity management solution that would address several major issues inherent in their then current infrastructure. Having concluded their solution should be based on NMI compliant standards, FSU has since selected and successfully implemented Novell's eDirectory solution. FSU now provides a centralized authentication service that offers campus computer users a single sign-on (SSO) and person identifiers no longer based on their Social Security Numbers (SSNs).

This article looks at the research and evaluation process that served as the foundation for the decisions that FSU's IT leaders made as they created their new eDirectory solution. Attention will be given to the understanding the value of basing such a campus solution on NMI compliant software, as well as how FSU's participation in the National Science Foundation (NSF) NMI (NSF Middleware Initiative) Integration Testbed¹ helped them better understand this value.

Need for an Identity Management Solution

FSU's need for a comprehensive, standards-based identity management solution evolved over time, driven by the increasingly robust and complex IT services FSU offered to its students, faculty and staff. By the late 1990's, FSU had been providing centralized academic computing and network access to e-mail services and an on-line public directory for many years. By 1997, FSU IT leaders were already searching for a solution to implement a secure, single sign-on (SSO) capable, centralized authentication service on a

¹ As part of its overall effort to develop and disseminate software that lets scientists and educators share resources across the Internet, NMI began a practical deployment and evaluation effort called the NMI Integration Testbed. <http://www1.sura.org/3000/NMI-Testbed.html>



campus-wide basis. Unfortunately, the enabling technology was not yet widely available or understood. Yet the need for such a solution became all the more important when, in 1998 and 1999, FSU broadened its web-based service offerings by deploying Blackboard for centralized content management of its online course development and delivery.

FSU's search for a secure identity management solution was also driven by the need to move away from the use of SSNs as the primary student identifier. In the early days of the Internet, there was far less concern about identity theft and individual privacy than in recent years. Thus FSU, like so many universities across the United States, had developed many of its university business processes around students' SSNs as identifiers (e.g., for tasks such as registration, grading, financial aid). As these business processes continued to evolve, especially towards web-based access, they offered many enhancements to the end-user. However, the need to insure the privacy and security of users that were accessing applications that contained confidential financial or personally identifying information was becoming more critical. IT management and technical staff became acutely aware not only of the need for SSO, but to provide a new mechanism to authoritatively determine identity.

Concurrent with these challenges of the late 1990s, FSU was also analyzing and testing two Lightweight Directory Access Protocol

(LDAP) directory services - one for accessing the FSU public directory and centralized e-mail services (the academic LDAP directory, or "LDAP1"), the other for securely accessing on-line administrative, business support applications and services (the business and service LDAP directory, or "LDAP2"). These two LDAP directories were on a course that would ultimately lead to their consolidation into a new, single campus directory solution. One factor driving this consolidation was the mandate by a Provost e-mail committee that established a standardized naming convention and set policy that e-mail would be an official means of communication between faculty and students.

A second driving factor for the consolidation of the directories was FSU's creation of a university-wide CIO position. At the time the CIO position was created, the two LDAP directories mirrored the duality in FSU's IT support structure. One LDAP directory and organizational IT entity supported academic computing, while the other directory and IT entity supported administrative and business computing. When the two IT support groups were placed under the purview of the new CIO, their separate LDAP directory projects were tagged for integration as well. However, that merger would be preceded by a best of breed enterprise directory "competition" between the LDAP1 and the LDAP2 project developers and managers that continued until the 2000 to 2001 timeframe.



Influence of Internet2 and the NMI Integration Testbed

By the spring term 2002, FSU had fully deployed the academic LDAP1 with Blackboard. Following this deployment, the central IT organization established a joint Directory Services Team (DST) whose primary focus was to bridge or integrate both LDAP directories, thus providing a centralized authentication service for the campus.

When the DST set about planning for integration of the LDAP directories, they used the information provided by Ken Klingenstein, Director of the Middleware Initiative for Internet 2, who had visited the university in the fall of 2001. During his visit, Klingenstein presented FSU staff with valuable information about identity management and a variety of other technology issues common to the higher arena. Klingenstein's visit helped jumpstart FSU's concerted efforts to deploy a new, consolidated LDAP architecture on campus.

FSU also took advantage of a unique opportunity that allowed them to reduce the developmental and research time needed to deploy their directory service. In June 2002, FSU began participating in the National Science Foundation (NSF) NMI (NSF Middleware Initiative) Integration Testbed. Managed by the Southeastern Universities Research Association (SURA) on behalf of

the NMI-EDIT² Consortium, the Testbed consists of eight universities that participate in a closely coordinated effort to deploy and evaluate NMI technologies. Participation as an NMI Testbed site enabled FSU to continue to build upon its body of knowledge in middleware through the systematic evaluation and review of NMI Releases and policies.

Working in the NMI Integration Testbed with NMI tools not only helped FSU build their institutional knowledge more quickly than they likely would've by working alone, it also provided FSU with significant information on where they stood in the deployment of an Enterprise directory service. In addition, the collaborations and communications between all members of the NMI Integration Testbed contributed to FSU's decision to integrate the directory architecture with FSU's ERP/PeopleSoft implementation that replaces their previous HR and Financial "home grown" systems.

NMI Components

FSU found various NMI-EDIT tools reviewed in the Testbed project particularly relevant to their identity management and directory services project:

- NMI-EDIT's [eduPerson](#)³ directory schema
- NMI-EDIT's middleware [Conventions and Best Practices](#)⁴, [LDAP Recipe](#)⁵ and

² NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT): <http://www.nmi-edit.org/>

³ eduPerson information:

<http://www.educause.edu/eduperson>

⁴ Conventions and Best Practices:

<http://middleware.internet2.edu/dir/>



Metadirectory Best Practices⁶

The [eduPerson](#) directory schema was a key enabler for FSU in their implementation process. They found that the [eduPerson](#) schema provides a strong standard and base that any organization can use to populate their metadirectory. This is true whether the institution is just starting a metadirectory, or already has a mature metadirectory. FSU extended the [eduPerson](#) schema by creating the “FSUperson”. Additionally, right “out of the box”, FSU found [eduPerson](#) enabled them to do inter-institutional authentication.

The [Metadirectory Best Practices](#) document, one in the series of NMI-EDIT’s [Conventions and Best Practices](#) documents, provided FSU with validation of the path they had already undertaken for the use of groups and group roles. This document includes discussion of the how to use groups and group roles in a directory structure. Another key factor in the metadirectory structure is to keep the naming conventions within the OU (Organizational Unit) flat, that is, not to create a deeply tiered hierarchy.

Finally, since the merging of their two FSU LDAP directories was a key step in their total solution, FSU also used the [LDAP Recipe](#) as a tool in their identity management and metadirectory deployment. While FSU would’ve liked more

“real world” examples of metadirectories integrated with Microsoft’s Active Directory to draw from, FSU found the practical recommendations and discussion of groups and metadirectories in the [LDAP Recipe](#) to be very helpful.

Need for a Vendor Solution

As noted, FSU had been providing centralized academic computing and network access to an on-line public directory and e-mail services for many years. Their deployment of Blackboard and other web-based applications added to the complexity of their authentication and authorization environment, as did concerns about the use of SSNs as identifiers. Over a two-year timeframe, they had also deployed a directory service layer comprised of LDAP directories 1 and 2 (primarily done using iPlanet’s Netscape directory service product and Microsoft’s Active Directory services). The directory service layer was a critical component for integrating the two previously standalone directory services as it provided the “authoritative source” directory required for an identity management solution. The layer enabled campus-wide connectivity to a new secure, centralized directory service that provided enterprise-wide authentication and authorization.

The Directory Services Team (DST) worked for at least seven months to create a bridge in the campus directory service layer between the academic and administrative services LDAP directories that comprised

⁵ “A Recipe for Configuring and Operating LDAP Directories” available at:

<http://www.duke.edu/~gettes/gjia/ldap-recipe/>

⁶Metadirectories Best Practices information:

<http://middleware.internet2.edu/dir/metadirectories/internet2-mace-dir-metadirectories-practices-200210.htm>



the campus's directory service layer. However, the DST team didn't have sufficient resources to complete their work "in-house". The dedicated internal resources the integration required were simply not available, due to the university's reprioritization of IT initiatives. Resources had been shifted away from the DST's centralized authentication initiative and redirected to a new campus initiative for the selection and implementation of (by July 2004) an Enterprise Resource Project.

Thus mid-year 2003, FSU's IT leaders reached a conclusion that it would take years and significant recurring funding to achieve full deployment, unless at least seven or more full- or three-quarter- time technical personnel were dedicated to the integration endeavor. At this critical juncture, the decision was made to retain an outside vendor that would provide consulting, software and maintenance support services as a key part of FSU's campus-wide deployment of an integrated, secure directory service and identity management protocol.

Complex Needs

IT leaders analyzed their options for an enterprise-level metadirectory solution that would provide the provisioning of data from the metadirectory to other services and applications. They developed an inventoryⁱ of the major enterprise-wide applications within the University that would need to connect to the new FSU metadirectory solution:

- *FSUcard*- Each on-campus faculty, student and staff is issued a "smart card". Both the LDAP1 and the LDAP2 use the FSUcard number as an identifier for authenticationⁱⁱ.
- *Computer Account Registration System (CARS)*- This "home grown" authentication domain system handles some 50,000 accounts for students, faculty and staff. The source for accounts includes data from Human Resources and the FSUcard system. The information is reflected in the LDAP1 server.
- *On-line Personal Services/Secure Login*- This "home grown" system handles some 100,000 accounts for students, faculty and staff. The source for accounts includes the HR and the FSUcard system, as well as legacy databases. The information is reflected in the LDAP2 server. Users authenticate into Secure Login by using their FSUcard, self-selected "Webname" or SSN.
- *Northwest Regional Data Center (NWRDC) login IDs*- The NWRDC houses most of the FSU enterprise administrative information. The SSN/PIN system table is used as an older-style of web authorization. Many Java-based applications use NWRDC accounts as well.
- *FSU Active Directory tree*- A cluster of Windows 2000 machines provide Microsoft Exchange, authentication and file service to approximately 4,000 administrative users on campus. A number of mail domains are serviced within this tree.



- *Novell Netware/eDirectory*- A number of Novell servers provide network drive space for approximately 4,000 administrative users on campus.
- *Emerging PeopleSoft ERP system* - FSU is replacing its HR and Financial “home grown” systems with PeopleSoft. Authentication for the PeopleSoft system is expected to leverage the existing LDAP directories or perhaps create another LDAP directory that contains a populated schema.
- *Prototype Portal*- This test portal manages the illusion of merging authentication requests from the LDAP1 or the LDAP2 using an instance of Yale’s CAS (Central Authentication Service) server.
- *Additional “pockets” of enterprise authentication*- Smaller systems relying on local authentication include Remedy, SEVIS, Business Objects and C.O.L.D.ⁱⁱⁱ
- *FSU Departmental servers*- A number of FSU departments have large enough populations and expertise that they have their own authentication domains. Some are connected to the FSU Active Directory forest, while others run a variety of heterogeneous environments.

- LDAP directories
- Active Directory clusters
- Self-service academic and business applications and their related databases
- ERP/PeopleSoft software
- Data warehouse

Furthermore, the vendor-provided solution needed to satisfy the following functional requirements:

- The identity management schema had to be extensible and expressed as an extension to the **eduPerson** schema, with **eduPerson** fields populated.
- Identity management tools had to be scriptable, and provide an API (application program interface).
- Code and examples for password synchronization needed to be included.
- Single sign-on (SSO)/initial sign-on (ISO) needed to be included.
- The solution needed to support the move away from using SSN as an identifier within the various systems and be able to handle visitor accounts with limited access and/or duration.
- The solution needed to support the integration of two iPlanet 5.1 directories (LDAP1 and LDAP2), Active Directory, PeopleSoft, Kerberos 5, NDS, and Blackboard.
- The solution needed to provide a standards-based tool for writing bridge/interface APIs to handle fits/gaps identified within the existing and future enterprise metadirectory service architecture (including connectivity to existing e-mail applications and non-

The Vendor Solution

RFQ Specifications

The vendor selected through FSU’s RFQ process had to provide an open-standards, secure services-/application-provisioning solution that enabled the enterprise integration of the following:



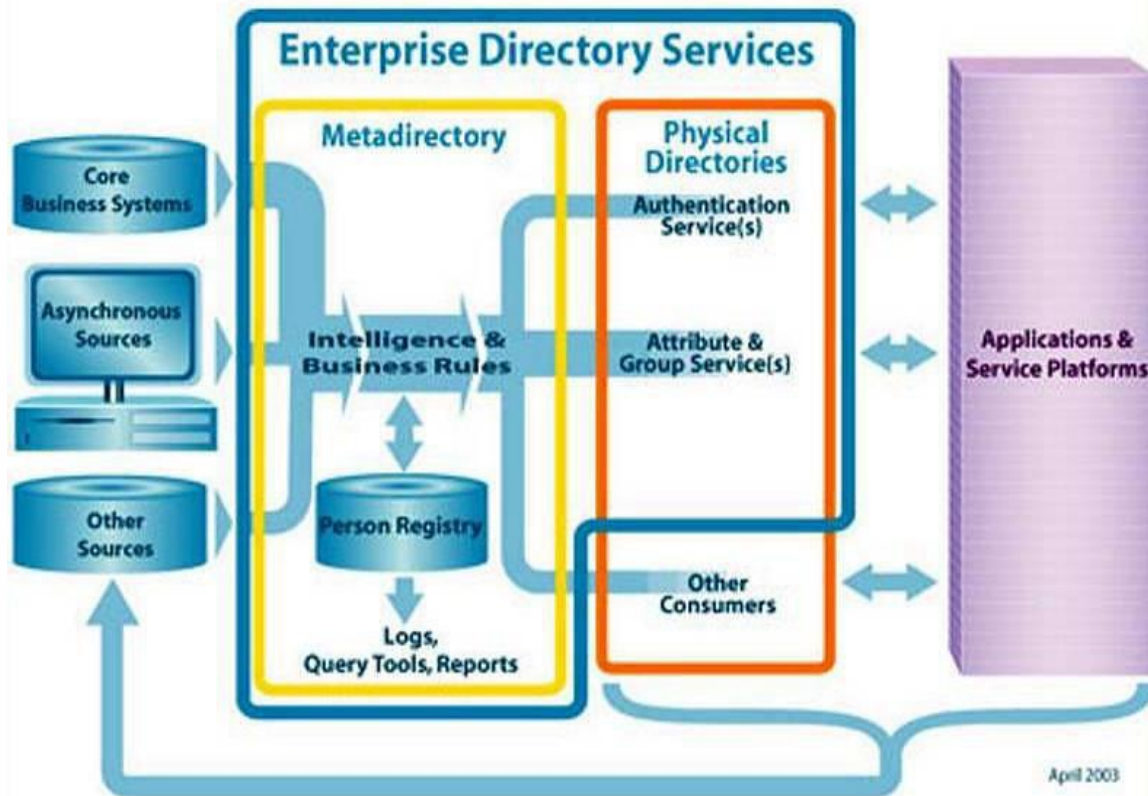
LDAP directory services, as well as standards-based portal solutions.)

- The solution needed to include a web ISO system with ability to authenticate IIS and Apache, and provide an API for at least the Java and Mod-perl programming

languages (PHP, PAM, and C desirable). Applications that were anticipated to use Web ISO from the metadirectory included CARS, Secure Login, Blackboard, PeopleSoft, Portal solution, NDS and Active Directory.

Fig. 1

Core Middleware for an Integrated Architecture



Vendor Selection

Using these specifications to evaluate vendor proposals, FSU selected Novell's eDirectory product. Novell was the clear choice, as only Novell met FSU's specific RFQ criterion for a solution that would also integrate with FSU's ERP/People soft implementation. The NMI-EDIT standard

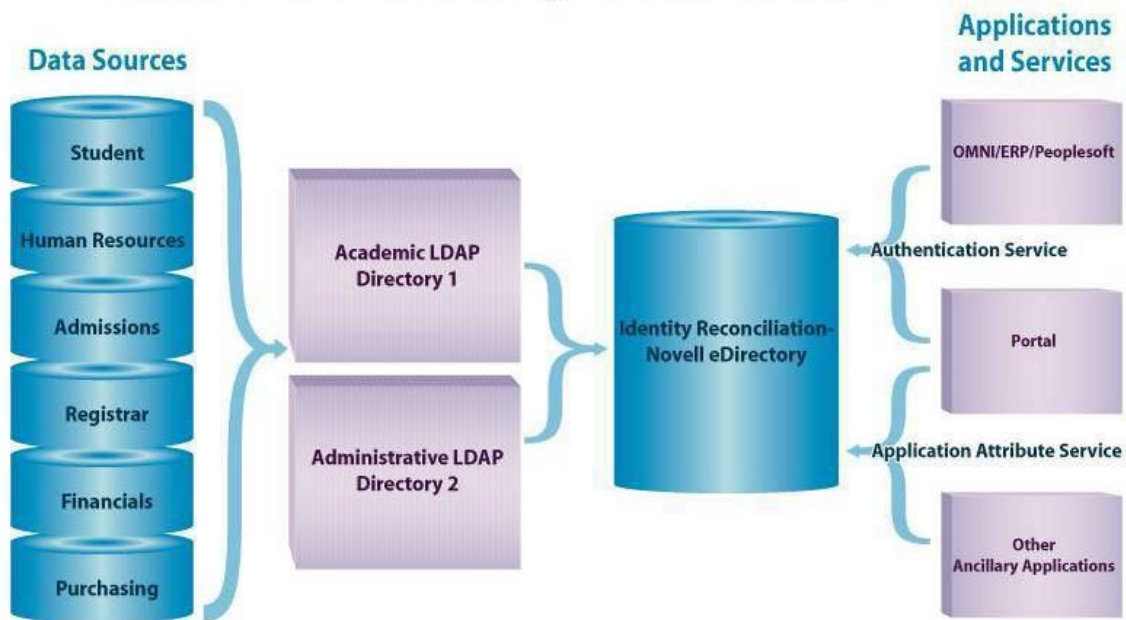
enterprise directory design⁷ (Fig. 1) is reflected in FSU's design architecture, which is customized to fit the FSU environment and includes the NMI-compliant Novell eDirectory solution and FSU's PeopleSoft deployment (Fig. 2).

⁷ http://www.nmi-edit.org/roadmap/dir-roadmap_200505/design/design-set.html



Fig. 2

Florida State University Solution Architecture



Implementation Chronology

Novell's consultants worked in partnership with FSU's metadirectory team to bring up the metadirectory in a lab environment. The entire project timeline was delineated in FSU's identity management RFQ as well as in the ERP/PeopleSoft project management plan. The projects proceeded as follows:

- Analysis and Design – November 2003 through March 2004.
- Laboratory testing – March through mid-June 2004.
- Production w/ERP – June 18, 2004.
- ERP financials, purchasing – July 1, 2004.

Project Integration of Person Identifiers

Concurrent with the rollout of the eDirectory, FSU IT leaders have implemented an active project to migrate FSU's departmental business processes and software away from the use of SSNs wherever possible. The development of two new person identities for use in the new eDirectory infrastructure provides the means by which this migration is being conducted.

The "private" use of SSNs will be replaced by new "FSU Security Numbers" (FSUSNs)^{iv}. Private use situations occur when an individual (student, employee, etc.) must prove their identity to an agent of the university (HR person, student service



employee, etc.). The second situation where SSNs have historically been used at FSU is termed "public" or "semi-public" use to uniquely identify individuals in a list. For example, a typical list of students by SSN might have been used for various reports in FSU's Housing, Registrar, and academic departments. As part of the SSN migration project, the public/semi-public use of SSNs will be replaced by individual FSUIDs. The FSUID is "public" in the sense that it can be used on reports to uniquely identify one person from another.

These situational usage guidelines are assisting FSU departments in making correct choices about how and when to use person identifiers. The ability for any particular department to implement their new person identifier business process with their business application software has been made possible by the thoughtful design decisions FSU's IT leaders made during the rollout of the new eDirectory. The eDirectory/FSUID application has been designed to be the key delivery method for FSUSNs to individuals. The FSUID login name and password will be used to authenticate people to the ERP/PeopleSoft system and ties together the major enterprise-wide existing identities (e.g., CARS/ACNS/Blackboard, Secure Login, Outlook, PeopleSoft) into a new SSO name and password.

Challenges Met

As of Fall 2004, the Novell eDirectory software had been deployed on five production servers located strategically across campus, providing redundancy and fault tolerance. The schema for this directory service^v includes key fields from the original two competing LDAP directories and a variety of additional attributes that serve new functions. The eDirectory now provides the following services for basic authentication and authorization:

- Password synchronization for a growing list of FSU identities, including ACNS (Academic Computing and Network Services) /garnet/mailler accounts, Secure Login/OPS accounts, Outlook Exchange accounts within two Active Directory trees, and the newly minted "FSUID" account.
- Centralized, coherent identity management tied to a single web location⁸ for all electronic identities at FSU.
- Extensive background of automated "feeder scripts" that keep the attribute values up to date. The schema currently stores the typical directory information as well as current data skimmed from the appropriate locations in the Student Information System (SIS) and HRMS systems. This includes, for example, current semester class schedules.
- Integration with key departments interested in having their local department identities merged into the eDirectory in an

⁸ <http://fsuid.fsu.edu/>



- appropriate fashion that allows retaining of autonomy.
 - PeopleSoft production and test instances of Financials, Portal, and HR.
 - A number of RADIUS servers used for VPN authentication.
 - New eDirectory-based public search engine⁹
 - Subsuming of "legacy" LDAP servers by converting the systems that use them to use the eDirectory in a native fashion.
- Secure Login was implemented in October 2004 and phasing out of the Human Resources Management System (HRMS) will take place on July 1, 2005.
- Implementing a new computer Helpdesk application that allows authorized Helpdesk staff to look up and assist users with account management.

FSU Identity Management and the Future

The FSU identity management project now has a life of it's own, with the equivalent of two full-time employees dedicated to continued support and development. Future efforts will concentrate on:

- Removing the legacy LDAP directories.
- Inviting more departments to connect their identities to the enterprise directory.
- Web SSO through the Yale-developed CAS server with FSUID, Blackboard, Secure Login and ACNS/CARS.
- Merging in the enterprise Novell Netware identities.

- Rollout of the FSUSN (SSN replacement private identity).
- Continual upgrades/upkeep of the hardware and software environments.

Novell's NMI-compliant eDirectory provides FSU option of implementing other NMI technologies in the future. FSU will investigate NMI-EDIT's *Shibboleth*^{® 10} software, an open-source, standards-based tool that provides mechanisms for controlling access to web based resources (particularly in inter-institutional environments) while offering options for protecting personal privacy. A related technology, "PKI" or Public Key Infrastructure, will also be investigated (PKI provides standards and services that facilitate the use of public-key cryptography). Additionally, the FSUID directory readies FSU to reach out beyond the institution through the population of NMI-EDIT's *eduPerson* fields.

More Information

For more information about FSU's identity management solution, contact Joe Lazor at JLazor@admin.fsu.edu.

References:

- (1) "SSN Replacement Principles- A Strawman Proposal".

<http://fsuid.fsu.edu/admin/ssn.html>

⁹ <http://fsuid.fsu.edu/search>

¹⁰ Shibboleth information:
<http://shibboleth.internet2.edu/>



Links of Interest

Florida State University (FSU) www.fsu.edu

FSU authentication domain <http://campus.fsu.edu>

FSUcard <http://fsucard.fsu.edu>

FSU Computer Account Registration System (CARS) <https://cars.acns.fsu.edu/>

FSU eDirectory http://fsuid.fsu.edu/admin/metadir_project.html

FSU PeopleSoft ERP system <http://www.aim.fsu.edu>

FSU Prototype Portal <http://uportal.fsu.edu>

GRIDS Center <http://www.grids-center.org/>

NMI-EDIT <http://www.nmi-edit.org/>

NMI Integration Testbed Program <http://www1.sura.org/3000/NMI-Testbed.html>

Novell eDirectory <http://www.novell.com/products/edirectory/>

NSF Middleware Initiative <http://www.nsf-middleware.org/>

NWRDC login IDs <http://nwrdc.fsu.edu>

On-line Personal Services/Secure Login <https://apps.oti.fsu.edu/servlet/login>

Yale's CAS Server <http://tp.its.yale.edu/tiki/tiki-index.php?page=CentralAuthenticationService>

ⁱ More technical detail about these applications is available at:

fsuid.fsu.edu/admin/metadir/FSUMetaDirRFQ.doc

ⁱⁱ The schemas used on LDAP1 and LDAP2 were not the same, nor was the information stored in the schemas (they use different domain names, for example). Most people have an LDAP1 and an LDAP2 entry that are, for the most part, equivalent. Some name collisions and omissions exist.

ⁱⁱⁱ *Remedy* – Remedy Ticketing system (Remedy accounts and a local Oracle server). *SEVIS* – a student tracking system. *Business Objects* – an on-line report generating tool that uses its own proprietary authentication system. (<http://buso.oti.fsu.edu/>). *C.O.L.D.* – store print files onto disk, own proprietary authentication scheme (replicates NWR “fs” accounts). (<http://www.docfinity.com/>).

^{iv} Project principles for FSU's migration away from the inappropriate use of SSNs to new FSUSNs are detailed at <http://fsuid.fsu.edu/admin/ssn.html>

^v The schema for FSU's Novell eDirectory service is documented at <http://fsuid.fsu.edu/cgi-bin/attributes/fsuid-schema.cgi>