



## **Georgia State University: Building an Identity Management Infrastructure for the eUniversity**

### **NMI-EDIT Case Study Series**

In response to calls from the higher-education community, the NMI-EDIT Consortium has developed a series of Identity Management Case Studies to explore the planning and implementation of this critical infrastructure at higher-education institutions around the country.

The Case Studies are drawn from schools/consortiums with varying sizes, populations, and missions in an effort to provide examples of the diverse technology, policy, and project management approaches.

This NMI-EDIT 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. Thanks are extended to the author Arthur Vandenberg.

Ann West, editor.

Copyright © 2004, Board of Regents of the University System of Georgia by and on behalf of Georgia State University. All rights reserved. Content may be used for non commercial purposes with attribution



# Executive Summary

Georgia State University is enabling the eUniversity – the system of basic communications and transactional services that characterize the electronic, next-generation institution of higher education. Enabling this identity management vision requires a complex architecture of inter-working technical and policy components to manage individuals' electronic identities, secure authentication processes, and access authorization to campus services. The research and education environment of the 21<sup>st</sup> century must provide the ability for on-campus and remote students to take courses, for faculty to collaborate with partners at distant sites, for researchers to conduct research with distributed investigator teams, and for administrative services to span the reaches of the global cyberspace.

In February of 2000, Georgia State began working on this eUniversity and the electronic infrastructure to support it. A new group, named Advanced Computing Services (ACS), was formed and charged to investigate, design and work collaboratively to implement this new infrastructure. ACS was mindful that the identity management infrastructure should conform to best practices and standards to ensure effective interoperation with the higher-education community. Their new identity management system soon reflected the model of the NMI-

EDIT Consortium recommendations, including the Internet2 Middleware Initiative directory schemas, software components, best practice papers, and policy recommendations. Georgia State's participation since May 2002 in the NMI Integration Testbed program served to further inform the process.

Georgia State's identity management solution is being achieved through working with the campus stakeholders to define requirements, data and business flow, synchronization procedures, and core applications supported by the identity management infrastructure. Along the way, they used a communications strategy for developing project acceptance and keeping the campus informed.

As this case study shows, a number of lessons were learned regarding the data and policy of identity management, the technical infrastructure solutions available, and also the institutional benefits in the establishment of new relationships and business processes of identity management to support the emerging eUniversity at Georgia State.

---

For more information about this Georgia State University Case Study, contact Art Vandenberg at [avandenberg@gsu.edu](mailto:avandenberg@gsu.edu).



---

## NMI-EDIT Components Highlighted in this Case Study

### **eduPerson Directory Schema**

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

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

### **A Recipe for Configuring and Operating LDAP Directories**

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

This document outlines practices of common directory deployments within the Higher Education community.

### **Metadirectory Practices for Enterprise Directories in Higher Education**

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

This document outlines a set of metadirectory issues that are commonly considered in the deployment of enterprise directories and offers accompanying practices for higher education.

### **Practices in Directory Groups**

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

This document offers recommendations to institutions embarking on the implementation of the use of groups to facilitate basic authorization.

### **Enterprise Directory Implementation Roadmap**

<http://www.nmi-edit.org/roadmap/directories.html>

The Enterprise Directory Implementation Roadmap is a web-based structure of resources that institutions can draw on to help deploy and use enterprise directories in higher education and research communities.

### **Shibboleth Software**

<http://shibboleth.internet2.edu>

The Shibboleth support inter-institutional sharing of resources that are subject to access controls.



# Georgia State University: Building an Identity Management Infrastructure for the eUniversity

A move from the traditional bricks and mortar institution to a virtual community is taking shape across the higher education landscape. Serving students, faculty, staff, and affiliates, this approach offers online services, portals tailored to customer profiles, and seamless integration of administrative, academic, and research applications. The result is enabling on-campus and remote constituents to take courses, collaborate with partners, conduct research, and provide administrative services that span the reaches of the global cyberspace.

Georgia State University, a public, Doctoral/Research Extensive University with 28,163 students (Fall 2003 enrollment), accepted this vision as a challenge. In February of 2000, the University's Information Systems & Technology (IS&T) began an initiative focusing on middleware infrastructure for the eUniversity.

Analogous to the commercial sector's engagement with e-Commerce, today's institutions of higher education are rapidly entering a system of basic communications and transactional services that could be called the "eUniversity," the electronic, next-generation institution of higher education.

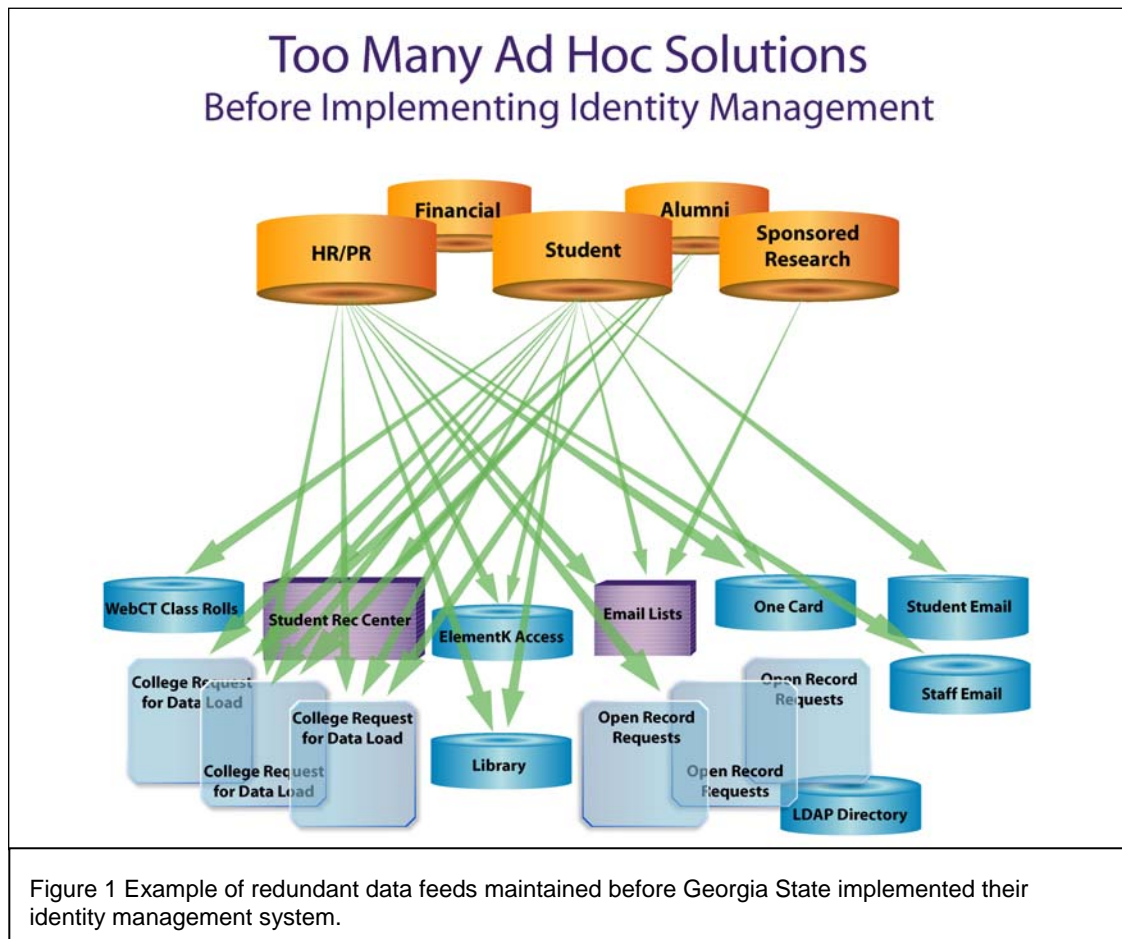
Requiring a complex architecture of inter-working parts to manage individuals' electronic identities and their access privileges, IS&T identified the following challenges:

- The integration and appropriate access of information and services in the e-University electronic campus requires a much broader paradigm of identity management than the traditional application-specific approaches.
- More thorough, comprehensive methodologies for validating the identity of an individual in the electronic environment are critical.
- The association of authenticated identities with pre-specified privileges allowing access to electronic functions in the e-University is expected.
- The seamless, comprehensive integration between all components of the e-University is an important outcome. This includes access to administrative application systems, library services, e-mail, calendaring, electronic course content, buildings or rooms, or technology resources like workstations or network ports.



In early 2000, IS&T also wanted to provide a public, globally available email address, but existing processes were not appropriately established. (There was no consistent, campus-wide convention for email names, no defined process for assigning email addresses, and no apparent solution to support the use of the various email packages individuals preferred.) In addition, the campus maintained redundant account/password models for accessing student-based applications (registration,

From a policy perspective, these problems extended beyond merely technical challenges and hypothetical scenarios into active concerns about network and data security. There was a need to provide reliable security for data by providing managed coordination of source-to-consumer data transfers without losing unit or departmental stewardship over it. The Data Stewardship & Access Policy (<http://www.gsu.edu/~wwwist/data.stewardship.html>) was already in place as a policy



WebCT, email, campus computer labs...), as well as redundant data feeds that inconsistently provisioned each application from the source systems. (See Figure 1.)

foundation, developed several years prior to the identity management initiative.



## The Solution

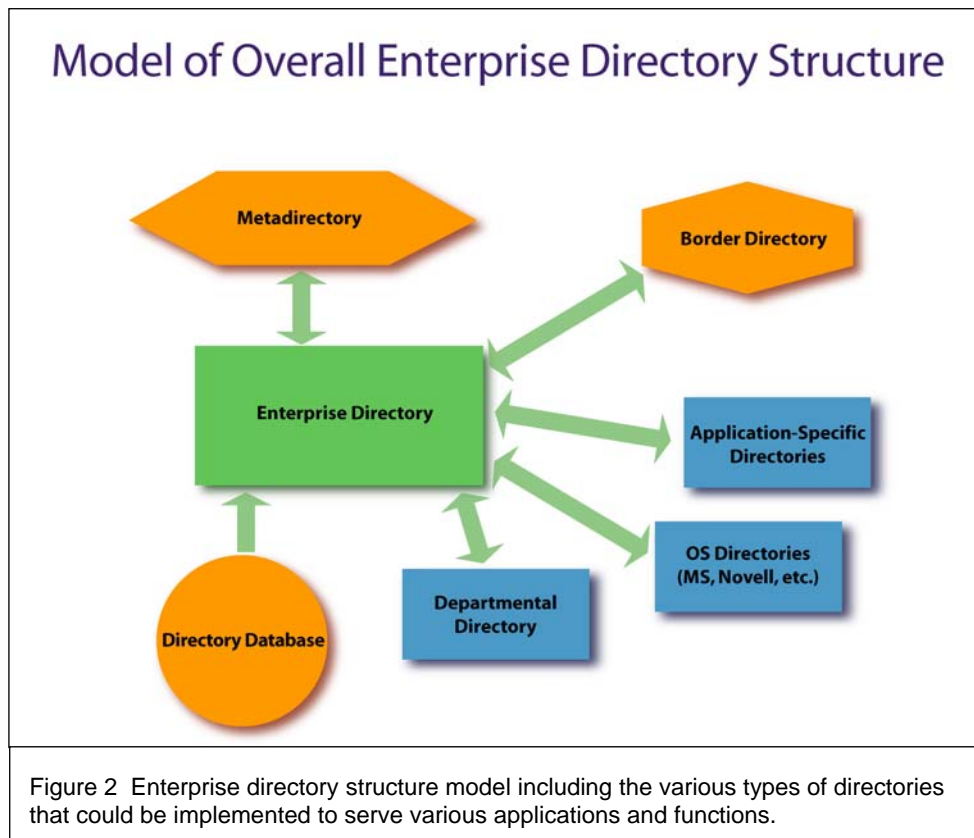
Because of the intra- and inter-institutional information requirements of their vision, Georgia State was concerned that their infrastructure supported standards required for interoperation with other institutions across higher education. They chose to model their identity management system after the NMI-EDIT directory schemas, software, and best practice papers to ensure this inter-operability. Key activities for identity management initiative included:

integrate the information about people present in these systems.

- Developing an enterprise directory architecture to house information used for authentication and authorization by applications. (See Figure 2.)

### Resources

In 2000, a new group within IS&T was charged to investigate, design and implement this new middleware infrastructure. Called Advanced Computing Services (ACS), the new group began



- Taking an inventory of major electronic identifiers in enterprise source systems.
- Developing a metadirectory architecture, a person registry, and related policies to

reviewing the eUniversity and eCommerce requirements and assembling an architecture. Initially, it was staffed with one director and one project manager, reallocated from Y2K project teams that were being returned to “regular” duty. The

primary staff resources would be drawn from across the IS&T directorates in a matrix management model as stages of the middleware architecture developed.

The institution receives most of its funding from the State with some supplemental funding coming from campus services such as printing. IS&T aligns its strategic plan with the campus strategic plan, and justifies its funding initiatives accordingly. The eUniversity model was an articulation of critical success factors for the overall University strategic plan. The internal re-alignment of IS&T funding to create the Advanced Campus Services unit was done to provide proper focus at an enterprise level and ensure an effective, coordinated team effort from resources across IS&T, and engagement with the wider campus community.

## The Project Chronology

As an Internet2 member, Georgia State became aware in Fall 1999 of Internet2's middleware initiatives related to identity management and Public-Key Infrastructure. While tracking their working groups, Georgia State also engaged other University System of Georgia research institutions in ongoing discussion concerning the Internet2 directory and PKI initiatives. The Burton Group also facilitated directory and PKI briefings for a group of University System of Georgia participants in September 1999 and March 2000. The Burton Group analysis confirmed that implementation of PKI or any centralized authentication service would be

well served by first addressing directory services. They also reiterated that a first step for the institution was to develop a logical and coherent identity namespace and related policies and management processes – a metadirectory architecture– also described by Internet2 Middleware working groups.

In May of 2000, IS&T established an Enterprise Directory Infrastructure Steering Group, made up of the CIO and IS&T Directors, charged to provide guidance and oversight of middleware deployment, as well as reach consensus on resource assignments needed to accomplish goals. The Steering Group developed an initial scope document with the objective “To establish an enterprise directory infrastructure for Georgia State University based on LDAP technology, with consideration of interoperation issues for the University System of Georgia community of interest.”

The newly formed ACS unit worked with the Steering Group to identify several concurrent activities:

- Assembling the data stewards group to discuss directory data and the policies and procedures governing directory data use.
- Inventorying the main source system identifiers and create an identifier strategy.



- Identifying an initial architecture and vendor for the enterprise directory.
- Developing data feed processes from source systems and implement a person registry model to join all identifier information about individuals into a single entry per person.
- Deploying an enterprise directory based on an identifier strategy and source data definitions.
- Discussing impact and benefits of the new infrastructure with campus units. Identifying initial applications to demonstrate the value.

As part of the project process, ACS developed a few project principles:

- Set the long-term direction for the architecture, but ensure flexibility in the short term by adjusting to accommodate applications opportunities that could demonstrate the early success of the infrastructure.
- At its core, identity management is a campus-wide data infrastructure and thus requires the support and participation of campus constituencies. Relationships and communication are extremely important, to ensure the infrastructure serves both campus and inter-institutional application needs.
- Don't try to do everything or solve all problems at once.

### **An Enterprise Directory Emerges**

After identifying the pieces of the architecture, data stewardship representatives were convened from Finance, Human Resources, Research, Student Services, Campus Card Office, and Alumni. The group consulted Campus Legal Counsel as needed during the project, especially when addressing legislation such as the Family Educational Rights and Privacy Act (FERPA), which governs how students' directory information can be released.

They also established a University System of Georgia (USG) Directory Services Working Group to address awareness, discuss directory activities, and collaborate where possible across the University System of Georgia. Concurrent with this, ACS drafted an internal whitepaper to articulate the direction, architecture, and business proposition for the identity management infrastructure. Entitled "Enterprise Directory Infrastructure for Community of Interest: A White Paper," the document provided a state and national context for the identity management project and linked the institution and the ACS project planning to external efforts such as Internet2. Leveraging the USG Directory Services Working Group ongoing discussions, ACS presented the perspectives in the document to the CIOs of the University System during their semi-annual Administrative Committee on Information Technology in 2000/2001.



### ***Technology Factors***

When IS&T staff first started talking about directory needs on campus in 2000, some presumed that there was no existing directory. On further scrutiny, however, it turned out that indeed for many years Novell had depended on directory services for NOS management, and further, IS&T was initiating a project to provide universal student email using Novell's LDAP-enabled Netmail. Certainly, this observation that a key vendor partner was taking a lead in directory services helped to clarify (and simplify) some internal technical decisions and, more importantly, created re-enforcement of the directory services effort for the campus stakeholders.

In late 2000, the technical team began planning and implementation of LDAP-directory enabled services deployment. After review of NMI-EDIT's *A Recipe for Configuring and Operating LDAP Directories* (or LDAP Recipe), the team was confident that that Novell was strategically aligned with directory services and supported the practices recommended by the LDAP Recipe.

### **Campus Input, Policy Document, Person Registry Success, and Student Resources**

In 2001, meetings continued with campus data stewards, representing the registrar, human resources, alumni, campus card, financial and legal to understand data

sources and data flows for directory services. Through CIO discussions with faculty and administration, and from customer input via the various IS&T directorates, the Enterprise Directory Infrastructure Steering Group began identifying possible synergistic projects, looking for the "killer app" that would demonstrate the benefit of directories. The Steering Group also developed a scope document and an Enterprise Directory Policy (See Appendix A.) to guide their work.

On the technical side, IS&T began deploying a person registry, following early versions of Internet2 Middleware best practices documents such as LDAP Recipe and NMI-EDIT's *Metadirectory Practices for Enterprise Directories in Higher Education* and personal recommendations from the NMI-EDIT developers. (See Figure 3.) The person registry became a natural and useful focal point to support universal student email, WebCT, and card access to the new Student Recreation Center – all strategic, highly visible initiatives for the campus. While still early in the overall deployment of directory services, the work in the person registry itself paid off in being able to support the provisioning needs of student email (Novell's LDAP based NetMail), WebCT class roles (student ID lists), and the PantherCard office (active PantherCard identifiers). The consolidation of identity records in the person registry was itself a



valuable resource in providing these data feeds.

To handle data flow, the ACS began investigating what is now called IBM Directory Integrator. The group also found a solution to technical staff resources that would later become a very successful model

these new computing technologies such as directories, metadirectory models and Java-based integration tools. Interestingly, the students were less skeptical of new solutions and were comfortable with “picking it up” and trying it.

#### Deploying LDAP-enabled Applications –

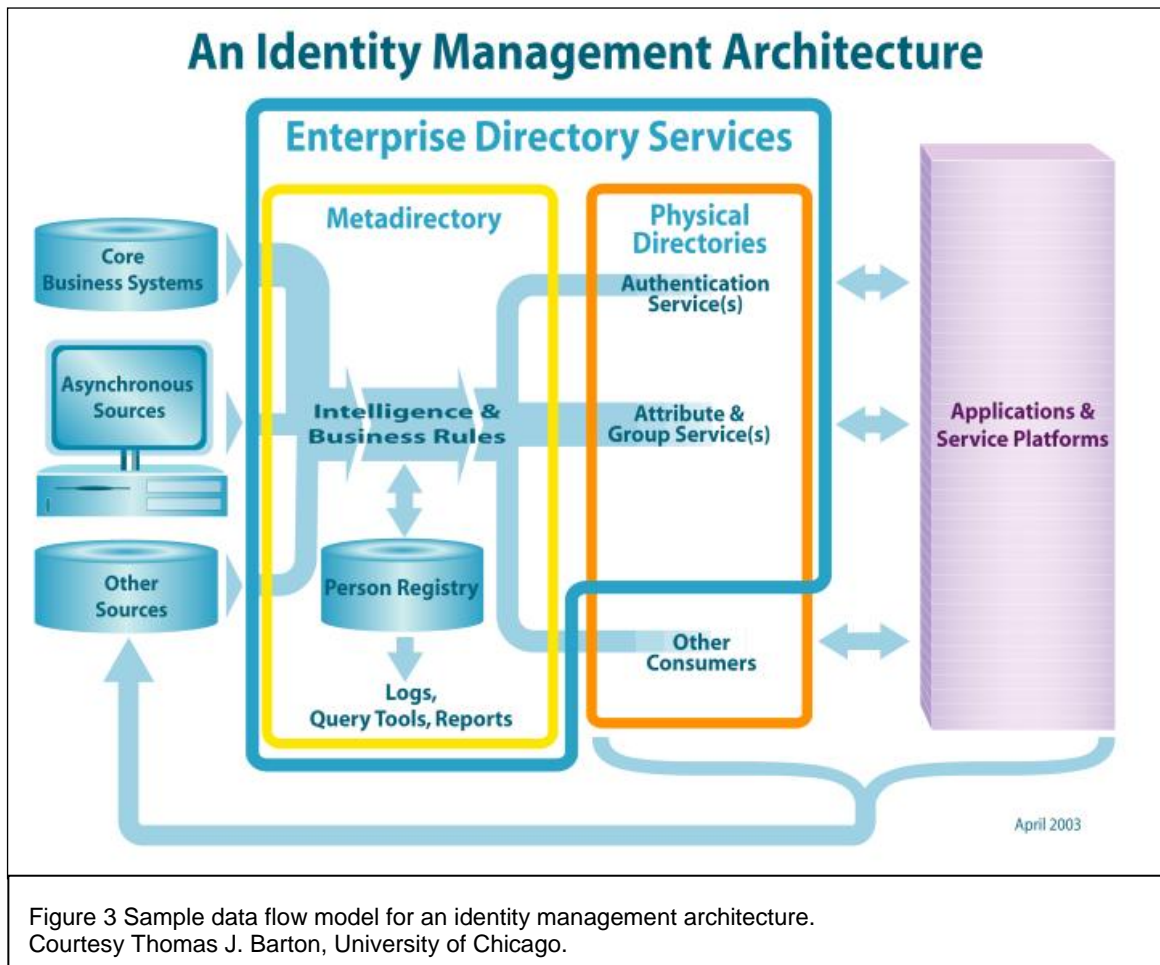


Figure 3 Sample data flow model for an identity management architecture. Courtesy Thomas J. Barton, University of Chicago.

for its middleware implementation – students. When ACS’s technical staff position became vacant, the position funds were redirected to supporting two students, a Masters student and an undergraduate, both in Computer Information Services. It was helpful to have “several minds” to discuss middleware solutions and the students were very open, and interested, in

#### Policy and Technical

In 2002, Directory White Pages and student email list groups were identified as two of the first LDAP-enabled applications. With the person registry in place, the goal of publishing a Directory White Pages service was nearer, but there were still major challenges. The first hurdle in this process was to standardize on a campus identifier as



the single, publicly visible enterprise id. A particularly challenging aspect of this was the fact that there were two name spaces in use, one for students and another for employees. IS&T technical and management staff had significant debates early on and decided that 1) a unique campus identifier and one name space was a best practice and 2) that the management of identities was critical in achieving the eUniversity vision. With good guidance from Internet2 Middleware activities, including LDAP Recipe and NMI-EDIT's [eduPerson](#) directory schema specifications, CampusID was established as a basis for identity management. The technical team began the process to decommission the legacy CSO PH directory and transition to the LDAP White Pages.

Email groups had always been a hot topic and the definition of a CampusID, and the discussions of Internet2 working groups and publication of NMI-EDIT's [Practices in Directory Groups](#) fueled the flame. The college administrative units wanted to send email to broad constituencies such as all\_students, all\_freshmen, all\_College\_of\_Arts\_&\_Sciences, etc. These groups were identified in collaboration with the data stewards group established earlier and a group of deans' representatives. Student attributes for college, major, and status were updated every night in the enterprise directory. By using dynamic

LDAP groups in conjunction with the Novell's LDAP NetMail (the solution for universal student email) an effective solution for student group email was delivered. Turn-around time for student group email postings went from days to hours.

In both provisioning the White Pages and the student group email directories, the IBM Directory Integrator was the metadirectory tool of choice. The policy-related business logic was implemented, tested, and reviewed with the appropriate data stewards to ensure expected behavior. Directory attributes were provisioned with individual information. And for the first time, an employee who was also a student was listed in one consolidated record with both their employee and student information. Appropriate logic was also in place to recognize which students elected to suppress or reveal their directory publication under FERPA and show their White Pages entry accordingly.

General project communication continued with articles in the IS&T FocusIT newsletter regarding the progress of the milestones, and with presentations to Deans Group, staff and departments. As a side note, at the end of 2002, staff in other departments were pleased with the imminent deployment of a LDAP Directory White Pages, because they could enable their various mail clients lookup services to use the LDAP Directory.



# Synchronized Data Flows After Implementing Identity Management

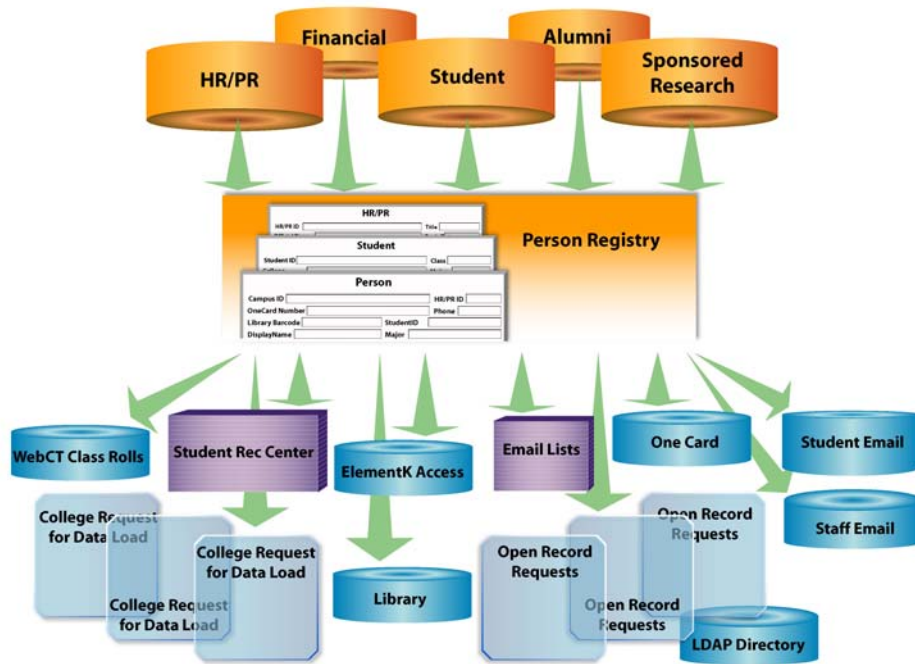


Figure 4 Georgia State's data flow after implementing their identity management infrastructure.

Additionally, in May 2002, IS&T's Advanced Campus Services became a participating site of the National Science Foundation Middleware Initiative (NMI) Integration Testbed Program (<http://www.nsf-middleware.org/testbed/>) The NMI Testbed Program was proposed as part of NMI to provide real-life feedback on the design, evolution, and deployment of NMI middleware components for directory and Grid technology services. Certainly, Georgia State University found that active participation in the NMI Testbed has been instrumental in advancing its adoption of directory middleware into its production infrastructure.

## E-mail Policies and Self-service... and Grids... and Staff Resources

In January 2003, the LDAP Campus Directory White Pages were officially deployed. Its impact continued in the adoption of email policy, requiring all employees, faculty, staff to use email as means of official communications. Simply put, with a unique CampusID being used for email (cf. [avandenberg@gsu.edu](mailto:avandenberg@gsu.edu) – the `eduPersonPrincipleName` attribute of `eduPerson` objectless), the new *profileManager* (see below) web application allowing one to set one's mail routing, and the Campus Directory being used for lookups, anyone could send email correctly and reliably to anyone else associated with the campus.



The *profileManager* was designed initially to enable users to authenticate against the Oracle database and change their password and set their email routing address stored in the Person Registry. However, the *profileManager* also became a standard interface for self-service management of identity. A long-standing holy grail of a paperless office became possible when the printing and hand distributing payroll check advices for the multiple payroll runs was phased out. Employees could authenticate using the *profileManager* and view online not only their current pay record, but also the history from the past six month. They could also view their up-to-date leave balances. The cost savings of not printing and issuing such pay advices was a significant bonus result.

Since the NMI Integration Testbed Program also included grid components evaluation, Advanced Campus Services expanded conversations with faculty and identified grids as a potentially critical component for research infrastructure. A *GRID Group @ GSU* workgroup began to meet to share information among faculty and technology staff on this topic.

From a human resources perspective in 2003, ACS continued to use students to work as an advance team to explore middleware, investigating grid technology. In addition, a former student graduated and was hired as staff, working half time in ACS on grid-related projects and half time with enterprise systems staff to support the

production person registry. This was a very positive outcome for ACS, since they were now benefiting from their investment.

### **On to LDAP Authentication, Account Provisioning, Completing the Identity Management Infrastructure**

In 2004, employee email groups were implemented by provisioning the appropriate attributes to the LDAP groups tree, similar to the student groups the previous year. Focus areas for 2004 became developing the LDAP authentication and identity management services to support account provisioning and password synchronization. (See Figure 4.)

To be added to the person-registry system, staff, faculty or students are first added to the Human Resources or Student Services ERP systems of record. The adds and changes are then picked up on automated data feed. An algorithm is then run to determine if matches currently exist in the person registry record. If not, the new person is added to the person registry and given a unique internal person-registry record key. Each person is also assigned additional appropriate enterprise identifiers and credentials, including a unique 16-digit identifier "PantherCard" number (which can only be activated upon producing photo identification), a unique Library barcode, a unique CampusID, and an initial encrypted password.

### **Identity Management Part Two**

With a new CIO in Spring 2004 came a rejuvenation of the complete identity management solution to integrate core



business systems and other authoritative sources with business intelligence, ensuring applications have appropriate authentication and authorization services.

At Georgia State, from the first day of a new hire or admitted student, to retirement or graduation, the complete life cycle of the eUniversity is important. Because of this vision, the Enterprise Directory Infrastructure Steering Group authorized an initiative to establish LDAP authentication to replace the current Oracle-based password as the official enterprise authentication mechanism.

Georgia State is now deploying an LDAP directory specifically for authentication and authorization. Novell provides an identity management solution for automatically provisioning network ids, email accounts, or other services and ensuring password synchronization among them, which could be a well suited for advancing the metadirectory architecture.

Future plans include expanding the existing Shibboleth® deployment to provide a transition from the Library EZProxy server and to enable access to web-based applications such as electronic theses and dissertations portfolio systems.

## Lessons Learned

During the implementation process for this new infrastructure, several lessons were either validated or emerged.

- Data are not owned, according to the stewardship approach. Rather, their use and care are the responsibility of students, departments, and units across campus. Because of FERPA, Georgia State's Data Stewardship & Access Policy ([www.gsu.edu/~wwwist/data.stewardship.html](http://www.gsu.edu/~wwwist/data.stewardship.html)), increased awareness of identity theft, and requirements for data retention, campus stakeholders are increasingly savvy about data use and abuse. For example, students tend to be aware of social security number issues and the business units are concerned about privacy issues surrounding data entry and retrieval activities.
- Problems and oversight contexts will sometimes arise that cross units, disciplinary boundaries, and responsibilities. For example, when the University created their "Campus Directory White Pages" in January of 2003, decisions had to be made about maintaining the *accuracy* of data, which is currently updated nightly directly from the person registry. Responsibility for the accuracy of that data resolves to 1) the authoritative source system (HR or Student Information Systems, for example) 2) the data steward for the person registry (ACS), and 3) the user of the person registry data (email group, Student Rec Center). This multi-pronged approach provides several levels of oversight and accuracy.



- Data stewardship is an ongoing and public educational effort at Georgia State, with the stewardship policies to be revisited annually.
- Some institutional projects have resulted in noticeable shifts between units and departments that have not historically collaborated together. For example, ACS actively seeks out undergraduate and graduate students across disciplines rather than solely depending on in-house planning and expertise. This approach to staffing benefits both the graduate students looking for research and applied practice *and* the IT departments in need of innovative energy. Interactions and collaborations between IT and university faculty are part of the university's mission and the directory and identity management projects bring that mission to the forefront of daily interactions.
- There is no “one solution,” but rather a collection of tools and components flexible enough to serve most situations. To choose the best for the purpose at hand, it helps to get guidance, validation, review, and practice recommendations from peers at other

institutions. Georgia State has only a few staff supporting their identity management infrastructure and the support and good ideas they receive from peers at other institutions with similar challenges are invaluable.

- Identity management and the related middleware services are a critical core of the university's enterprise infrastructure.

## In Conclusion

Georgia State's Vandenberg reports that the support of NMI-EDIT resources has significantly contributed to the identity management and directory work success. Beyond the immediate horizon – under the guise of identity management, directories, and middleware – is real institutional change. The eUniversity is taking shape through the appropriate use of resources and the ability to integrate data sources for the purposes of offering new applications to all the constituents of the institution.

## For More Information

For more information on Georgia State University's eUniversity: Contact Art Vandenberg – [avandenberg@gsu.edu](mailto:avandenberg@gsu.edu)



# Appendix A:

## Georgia State University

### Enterprise Directory Policy

The primary purpose of an Enterprise Directory at Georgia State University is to provide access to “Person” information that will enhance and support the academic, research, and administrative activities of students, faculty, staff, alumni, and affiliates. Generally, “Person” information may include name, title, contact information, office location, or other organizational data. Such data is commonly expected, for example, in a “white pages” lookup or other application.

Georgia State University is creating a technologically advanced information environment for which a key strategy is to provide improved access to administrative data. The University developed a formal *Data Stewardship and Access Policy for University Information* based upon the philosophy that University Information is a critical asset. The *Data Stewardship and Access Policy* is “To provide guidelines for management and access to data” comprised from various sources that “in aggregate may be thought of as forming a single, logical database.” Further,

“The scope of this [*Data Stewardship and Access*] policy is to have broad application, particularly with respect to data and

information resources which have impact for institutional operation. Data that may be managed locally may yet have significant impact if it is used in a manner that can impact University operations.”

<http://www.gsu.edu/~wwwist/data.stewardship.html>.

Such broad application applies to the Enterprise Directory that must provide integrated, timely, online access to “Person” data in support of critical operational services for the University community.

#### Guiding Principles

- The Georgia State University Enterprise Directory provides electronic information access to “persons” – students, faculty, staff, alumni, and affiliated individuals or organizations – or other objects associated with the official business of the university.
- The Enterprise Directory respects the privacy of “Person” data and follows applicable laws, regulations, and policies related to access, including the *Georgia State University Data Stewardship and Access Policy for University Information*, other institution



policies, and other mandated regulations such as FERPA.

- An Enterprise Directory in a higher education campus-wide environment will have several components whose integrated operation and timely provision of data can significantly enhance the overall value of the Enterprise Directory to the institution.
- Each individual in the Georgia State University community has responsibility for accuracy and currency of their data as it may impact University operations.

#### **Commitments**

- *Data Stewards for Georgia State University Person Data*, whose functional areas include “Person” data, work together to manage the Enterprise Directory. Functional areas are those as provided for in the *Data Stewardship and Access Policy* and may include additional areas deemed appropriate to the overall management and operation of the Enterprise Directory.
- *Data Stewards for Georgia State University Person Data* identify data sources for attributes and provide data mappings to an Enterprise Directory schema based on Lightweight Directory Access Protocol (LDAP) standard attributes and referencing schema models available from higher education and directory standards groups.

- *Data Stewards for Georgia State University Person Data* establish authoritative data sources for attributes. Authoritative sources are the primary arbiter of attribute characteristics after consideration of campus-wide issues. Authoritative sources may change as “Person” roles change.
- *Data Stewards for Georgia State University Person Data* address issues of identifiers, including appropriate selection of identifiers, consistent use of identifiers, and reconciliation of multiple or conflicting identifiers. The overall goal is to provide for effective integration of multiple roles under a uniquely identified “Person” record.
- *Data Stewards for Georgia State University Person Data* review processing schedules and timing issues related with “Person” data so that the Enterprise Directory has accurate and current information. The important consideration is the timely availability of “Person” data for campus services. An authoritative data source may be required to amend its processing to ensure its data is available to other campus services in a timely manner.
- *Data Stewards for Georgia State University Person Data* recommend mechanisms to ensure that updates or corrections to Enterprise Directory “Person” data are facilitated. In general, it is preferred that source data is corrected - ensuring that correct data flows into the Enterprise Directory.



- *Data Stewards for Georgia State University Person Data* regularly review the Enterprise Directory status and its overall operation.

#### **Policy Review Status**

September 12, 2000 – Initial draft by Data Stewards for Georgia State University Person Data Working Group.

October 12, 2000 – Revision #1 based on comments from Data Stewards for Georgia State University Person Data Working Group.

November 27, 2000 – Revision #2 based on additional comments from by *Data*

Stewards for Georgia State University Person Data Working Group.

December 11, 2000 – Revision #3 and “Final Draft” approved by the Data Stewards for Georgia State University Person Data Working Group.

January 22, 2001 – Reviewed by Enterprise Directory Infrastructure Steering Group. Consensus that document is appropriate. Next steps may include review by ISAT, Deans, and/or other groups.



# Appendix B: Scope Document

<b>Project Name:</b> Enterprise Directory Infrastructure	
Project Sponsor: <Chief Information Office>	Project Leader: <Director Advanced Campus Services>
Project Start Date: February 2000	Project End Date: [ongoing]
<p><b>Objective:</b> To establish an enterprise directory infrastructure for Georgia State University based on LDAP technology, with consideration of interoperation issues for the University System of Georgia “community of interest.”</p>	
<p><b>Narrative:</b> The Burton Group recognizes the potential for PKI solutions to authentication and authorization needs yet cautions that PKI is still on the horizon. The Burton Group recommends focusing first on the foundational enterprise directory infrastructure:</p> <p>“University System institutions must prepare for PKI by first planning and implementing the overall infrastructure that will support PKI... Simply put, each institution – and the University System as a whole – should be planning its PKI strategies and policies, viewing those efforts as an essential part of creating e-business infrastructure... The University System should strive to create general-purpose security infrastructure that many applications can leverage, integrating that infrastructure with directory and authorization services.”</p> <p>Georgia State University will establish a baseline directory infrastructure by following guidelines and “best practices” available from higher education, research, and Internet communities and coordinating with the other University System of Georgia institutions. The critical issues for the Fiscal Year 2001 are related to resolving enterprise identifier strategies, designing appropriate schemas, and addressing administrative processes and policy issues for directory information management. Additionally, the implementation of technology solutions integrated into GSU’s environment, the identification of resource requirements, and planning for FY 2002 activities are important.</p>	



Deliverables: (Tangible and intangible products, processes, results and services)

Establish a structure of "Steering Group" for overall direction with "working groups" for accomplishing tasks. A working group will focus on a specific deliverable and the Steering Group will be kept informed of progress.

Compile a GSU campus profile using survey models after Internet2 Middleware or CREN CA initiatives. The intent is to gather appropriate, relevant information about GSU identifiers, directories, authentication, and authorization infrastructure.

Define an LDAP directory schema for "GSU PERSON" - by working with data stewards for human resources, student, alumni, auxiliary, and other data. Consider EDUCAUSE "eduPerson" as reference model.

Document data flows relating functional applications data with the LDAP directory data. Include any processing steps, other databases, meta-directories or person "registries" that represent the logical LDAP directory.

Define a policy on data stewardship responsibilities related to GSU Person Directory.

Recommend strategy for and implementation of an integrated GSU identifier solution. Such a solution should accommodate GSU functional applications in a way that is consistent with the concept of a "single, logical" record for each person.

Implement an LDAP based GSU Person directory.

Enable improved account management procedures using the GSU Person directory per Recommendation 1 of *March 2000 Information Technology Internal Audit Follow-Up*.

Coordinate GSU activities with University System as recommended by The Burton Group report of March 2000 and the subsequent discussions.

Establish Fiscal Year 2002 objectives for enterprise directory infrastructure work.

Investigate opportunities for additional investigation, activity, or collaboration in enterprise directory infrastructure.



Boundaries: (Empowerment limits and project constraints)

Resources must be accounted for by coordinating activities with other priorities and/or acquiring any additional funding, staffing, or technology that may be required.

Address policy issues at an institutional level. These issues may be related to management of directory data, business process re-engineering related to timeliness of workflow, or coordination of identifiers.

The enterprise directory schema will focus initially on existing person data as found in student, human resources, alumni, and similar administrative systems.

The GSU Banner Student & Financial Aid project timeline must be accommodated - for instance as regards decisions on identifiers.

The target date for Recommendation 1 of the *March 2000 Information Technology Internal Audit Follow-Up* (improved account management) is June 2001.

Scope Document Review:(History of document)

**August 28, 2000** – Enterprise Directory Infrastructure Steering Group discussed issue of charter document. Consensus was to use model of Banner Project Scope document to set expectations and boundaries.

**September 14, 2000** – Enterprise Directory Infrastructure Steering Group reviewed draft SCOPE document. Discussion confirmed that issues were adequately set out. Recommendation that format be adjusted to list Boundaries below Deliverables so that readability was easier (the two-column format seemed to imply one-for-one association of a Deliverable and Boundary.) Also recommended that a Scope Document Review section be added.

**January 22, 2001** – Reviewed and approved by consensus.

