

# Carleton College

## **Carleton College: Identity Management and Enterprise Directories at a Smaller Institution**



### **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 authors Joel Cooper, Richard Goerwitz, and Todd Piket.

Ann West, editor.

Copyright © 2004 by Carleton College. Carleton College permits use of the content for noncommercial purposes with attribution. All rights reserved.



# Executive Summary

In an effort to better serve its constituencies, Carleton College, a small liberal arts college of 600 faculty/staff, 1800 students, and 24,000 alumni, set out in 2002 to design an initial Identity Management System (IdMS) and accompanying Enterprise Directory Service (EDS) that would allow its information systems staff to track identities and provision services for anyone connected with the College.

Carleton needed an EDS capable of maintaining information about an individual's electronic access and still be simple enough to be deployable and supportable by a small IT staff. For this reason, the College needed to implement a "lean" or minimal enterprise directory service.

Project leadership determined that the best way to get campus by-in across the campus was to use the EDS to implement systems

that various groups had been requesting. As the IT department deployed the EDS, it worked with these various groups to determine data-access policy within the EDS. Based on research of best practices (including NMI-EDIT and EDUCAUSE sources), Carleton developed a system that met institutional needs and conformed to best practices in higher education.

After two years, the College is now rethinking their "lean" EDS and is considering the need for additional functionality in their IdMS. However, Carleton learned a number of useful lessons along the way and was satisfied with the decisions it made, understanding that the systems would need to grow in the future.

For more information about this Carleton College Case Study, contact Joel Cooper at [jcooper@carleton.edu](mailto:jcooper@carleton.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 to foster inter-institutional collaborations.

### **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.



# Carleton College: Identity Management and Enterprise Directories at a Smaller Institution

Higher education has come under steadily increasing pressure to provide online services to people with affiliations other than student, faculty, and staff. Although they will always be a primary focus for online services, we now understand the need to serve a broader range of constituencies like parents, prospective students, alumni, and other unaffiliated donors, all of whom can have enormous impact on the life and well-being of a college or university community.

In efforts to serve this full range of constituencies better, Carleton College, a small liberal arts college of 600 faculty/staff and 1800 students, set out in 2002 to design an initial Identity Management System (IdMS) and accompanying Enterprise Directory Service (EDS) that would allow its information systems staff to track identities and provision services for anyone connected with the College. The new target constituent groups included the 24,000 active alumni and 140,000 high school students who each year receive mailings or brochures from Carleton's Department of Admissions.

This case study presents how Carleton is supporting, despite its relatively small size, a viable IdMS and EDS to meet this need. The authors will also discuss how Carleton's approach has stood up over time and what the future might hold for e-provisioning and identity management at Carleton College.

## Problem Discovery

In 2002, while doing background research on a portal project, several Carleton IT staff members went to the Virginia headquarters of Zope, Inc. to attend content management system training and spoke with executives there about possibly helping jumpstart a portal project at Carleton. In the course of those discussions, it became clear that much of what Carleton wanted to do (web personalization and single sign-on.) was simply not possible because the College had minimal infrastructure in place to track the identities of the online constituencies.

Rather than jumpstart a portal project at that time, Carleton needed instead to develop a service that would keep track of people,



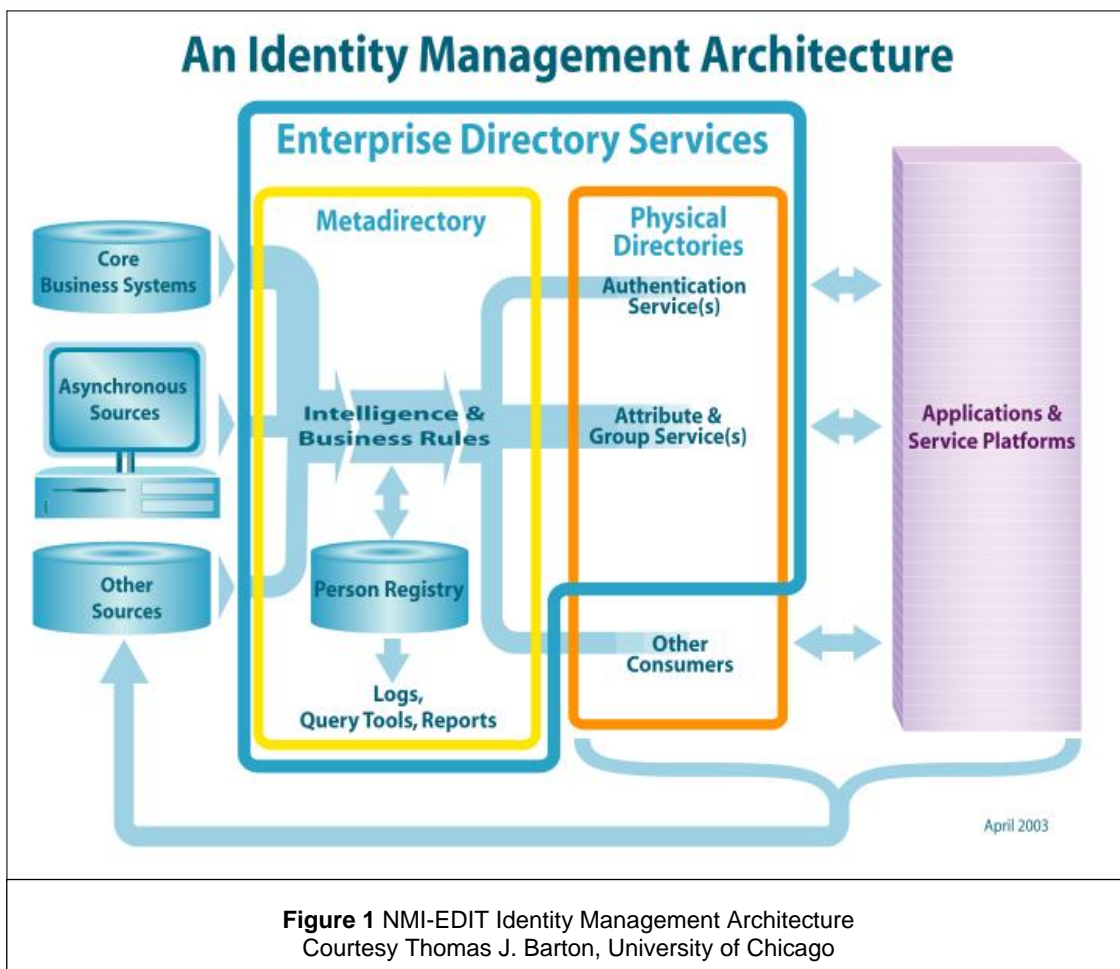
authenticate them, and help manage their online privileges and identity information. What Carleton needed, in fact, was an identity management system and, more specifically, an enterprise directory service.

## The Solution

After going through NMI-EDIT documentation as it existed in the late spring of 2002 Carleton IT staff came to the realization if an EDS was to be constructed at Carleton, it would have to be different. Most deployment scenarios outlined in NMI-EDIT doc-

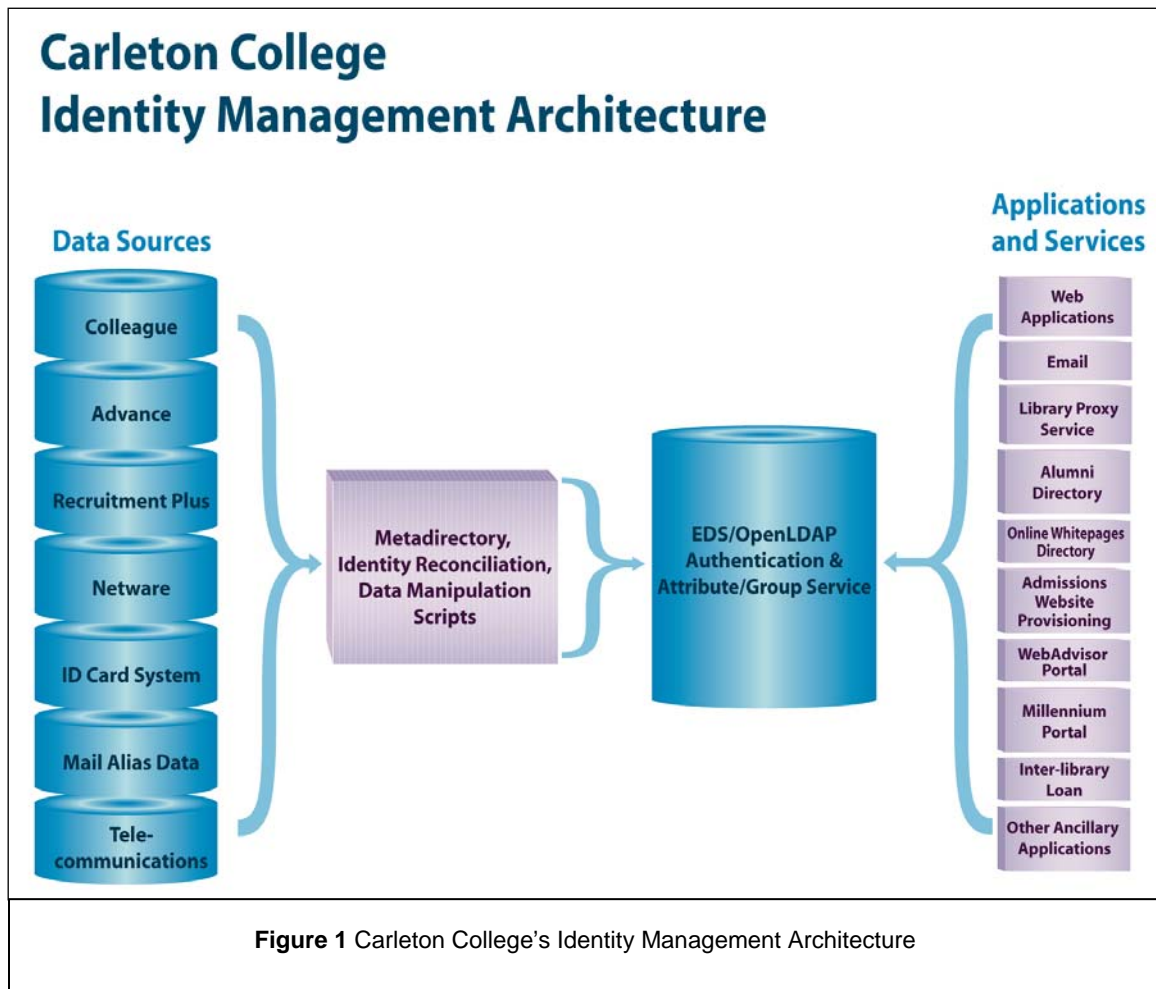
uments (See Figure 1) were done by institutions that had more staff resources than Carleton. In order to establish an EDS capable of maintaining the high quantity of attributes about people and still be simple enough to be deployable and supportable by a small IT staff, Carleton decided to implement what has since come to be known as its “lean” Enterprise Directory Service.

Carleton’s “lean” EDS was to draw data from the systems of record (e.g., ERP,



Admissions, Security, Alumni Relations and Development) and merge the most commonly used data elements into person entries resident on a central Lightweight Directory Access Protocol (LDAP) directory service. There would be no relational database component, or person registry, to store the intermediary data as recommended by most best-practice implementations, and the system would be used as a repository rather than a provisioning source. Creating a “heavyweight”, database-driven, writable provisioning nexus would have required infrastructure changes that the College simply didn’t have the resources to support.

In addition, the EDS itself would function from the standpoint of most client software as a read-only service. (See Figure 2 above.) The primary political challenge facing the EDS involved the possibility of users updating their data in the directory and the resulting ramifications for the source systems. Since the EDS was not the system of record for the data it served, the changed information (an address, for example) would have been pushed back to the appropriate system of record and used to update the corresponding fields there. At this time, the campus data stewards were not accustomed to having other people, or



especially other software, update the source data. To bring about the cultural changes needed to accommodate this feature would have required an unrealistic amount of time and resources and was not pursued.

Political forces, of course, were not the only ones at work. On the technical level, creating a heavyweight EDS with a person registry and a relational database back-end represented an impractical task for a staff that lacked true full-time programmers and database administrators for this project.

As a result, Carleton was faced with a very simple choice: Make the EDS lean, or don't make it at all.

### **Project Resources**

#### **Staff**

The EDS greatly affected the IT staff at Carleton, and although almost all of them had influence on how the EDS was deployed, certain positions within Carleton's IT organization became key players in the project:

- Richard Goerwitz, Web Technical Administrator, came to Carleton with substantial directory service experience. He worked half-time for three calendar months on the deployment.
- Mark Heiman, Web Applications Programmer, also worked approximately half-time on the project for about three months and implemented the first user-visible EDS-driven applications.
- Joel Cooper, IT director, was the project champion and made it a departmental and institutional priority for groups that

had historically operated separately to work together to develop the EDS.

#### **Funding**

Carleton College is a national liberal arts college and receives its funding from student tuition and fees, endowment revenue, and gifts. (The College ranks first among all national liberal arts colleges in alumni giving.) Infrastructure improvements have traditionally been funded out of one-time capital funds or by leveraging existing funding. The EDS project had no specific resources allocated to it at the start of the project and was simply added to the project lists of the two main staff charged with its deployment and the initial applications it supported. The funding model has not changed as a result of deploying the EDS, but it was implemented to support the requested applications.

Maintenance of the EDS itself requires about a fifth of one FTE. This does not account for new applications deployment, integration, and ongoing EDS-related collaboration inside and outside Carleton's IT department.

Open source software, OpenLDAP,<sup>1</sup> was chosen to be the enterprise directory because of its standards support and no cost. The hardware required to support the EDS cost under \$3000.

---

<sup>1</sup> <http://www.openldap.org/>



### Practices in Higher Education

Carleton made heavy use of the research and tools already provided by the NMI-EDIT Consortium at project initiation time. Such research included the eduPerson<sup>2</sup> directory schema documentation, and the Enterprise Directory Implementation Roadmap.<sup>3</sup>

Discussions with colleagues at EDUCAUSE also proved valuable, although ultimately Carleton chose to take what was, at the time, a streamlined deployment approach.

### The Project Timeline

Carleton's EDS deployment project began in June of 2002. Although technical hurdles were certainly a factor, the most difficult ones to jump were political.

#### Political Factors

At Carleton, no customer was actually asking for an EDS. The service, however, was presented by IT as being a necessary prerequisite for other work of great importance to the Registrar's Office, Business Office, Admissions, Alumni Relations, and the Dean of Student's Office. As a result, these latter constituencies became supporting stakeholders, though often indirect ones, of the EDS project.

Part of the reason for their trust in the project was also due to the care with which

---

<sup>2</sup> The NMI-EDIT eduPerson directory schema is located at <http://www.educause.edu/eduPersonObjectClass/949>.

<sup>3</sup> The NMI-EDIT Enterprise Directory Implementation Roadmap is located at <http://www.nmi-edit.org/roadmap/directories.html>.

Both are also available from the NMI-EDIT webpage at [www.nmi-edit.org](http://www.nmi-edit.org).

IT handled the institutional data and the corresponding stewards' needs. Before bringing the EDS online, the deployment team worked with representatives from many of the Carleton administrative and academic units listed above. Great effort was made to work with the data stewards to determine appropriate the data exposure and access-control policies. The Registrar and the Dean of Students, for example, developed the policies relating to student data access and ensured they conformed to FERPA legislation. The Development and Alumni Relations staff developed policies for the alumni information. And the Human Resources department and the Dean of the College determined the employee information policies, along with Administrative Computing staff and campus IT advisory committees.

#### Technical Factors

Technically speaking, the main obstacle that the EDS deployment team overcame was writing the code that extracted data from all the source systems and merging them into a common set of LDAP person objects. The reason this was an obstacle is that the systems of record for these constituencies did not offer easy-to-use applications interfaces. This meant writing a substantial amount of code to gather all of the necessary data with sparse vendor support.

Despite these challenges, the basic EDS was necessarily simple. Data flowed from feeder systems into metadirectory scripts which merged and/or reconciled it and



exported it to a read-only OpenLDAP server.

The feeder systems including the following:

- The ERP system, Datatel Colleague (UniData back end).
- The Advancement system, Advance/CS (Oracle back end).
- The Admissions system, Recruitment Plus (SQL Server back end).
- The photo ID component of Carleton's card access system, Picture Perfect (Informix back end).
- Novell's eDirectory (LDAP API).

Data in the EDS is accessed using well-known LDAP APIs available in most programming languages and systems in use at Carleton, such as Java JNDI, Perl Net::LDAP, and so on.

### **Deploying the EDS and EDS Applications**

In Mid-August of 2002, two and a half months after project kickoff, the EDS was deployed. The next task was to deploy the target applications. To educate people about the EDS and justify spending further time and resources on it, these needed to be highly visible.

### **The Online Directory**

In September of 2002, an online, white-pages directory was deployed--the first user-visible EDS-driven application. The rollout came at a time when College executives were struggling to find ways to reduce the need for printed material, such as phonebooks and departmental directories. The new white pages application included photos from Carleton's card-access system, a big hit with the faculty, staff, and the students. However, due to privacy

restrictions, pictures were accessible by authenticated viewers only, per the policies written by the data stewards. In addition, the information included in an individual's entry reflected an integrated view of his or her relationship(s) with the institution. For example, if a staff member is an alumna, teaches classes part-time, and is a parent of a Carleton student, these relationships are all reflected in their white pages entry.

Prior to this time, Carleton did not permit unaffiliated individuals to view any white pages/phonebook information. Now with the EDS, they have allowed anyone to view a subset of individual's entry. This was a great stride forward in both addressing a business challenge and enabling friends and associates of the College to lookup their colleagues' contact information.

The white pages application was very well received. As a result, at the start of the 2002/2003 academic year nearly everyone was using the EDS, knowingly or not.

### **Provisioning**

The Dean of Admissions wanted to provide each prospective student with a personalized view of Carleton's web site. Using this service, the student, depending on their class year and application status, would be asked to provide or update their personal information in one place and the data would update the source systems.

To implement the Dean's vision Carleton's IT staff created a system for generating usernames and passwords for all prospects



automatically, added them to the EDS, and passed them on to Admissions for inclusion in mailings. A special website was also created for prospective students to distribute their new credentials needed for admission.

Additional provisioning scripts were written to convert prospects into admitted students to set up Netware/Novell Directory Service (NDS) and email accounts automatically, and provide for the transfer of prospect information from the Recruitment Plus recruitment system to Colleague, the ERP system. Scripts were also written to convert the status of a graduated student to that of an alumnus/a, deleting their information from NDS groups and readying their information for the changeover from our ERP system (authoritative for students, staff, and faculty) to our Alumni Relations and Development system, Advance.

### ***Other Applications***

In addition to Carleton's online directory, prospect websites, and provisioning scripts, Carleton's EDS is also used in key applications like web authentication and authorization, authentication to our Library catalog (provided by Innovative Interfaces), and authentication to the Datatel WebAdvisor portal. Departmental web pages at Carleton also have faculty rosters driven by the EDS. Course folders in NDS are provisioned using the EDS. Mail routing, alias resolution, course mailing lists, and a growing number of ancillary applications also use the EDS. As of March 2003, our online alumni white-pages directory went into production. This project, which makes some use of the EDS,

was undertaken after vendor software purporting to support online communities never worked as advertised.

## **What the Future Holds**

The scope of Carleton's EDS has evolved to the point where it supports applications that serve a full range of constituencies, including prospects, accepted students, students, faculty, staff, and alumni. The EDS, however, has become a victim of its own success. In fact the breadth of its scope and its importance for the overall infrastructure has led the original deployment team to question whether the initial "lean" EDS deployment can meet Carleton's needs for much longer.

This is not to say that the deployment team regards the initial deployment as a mistake. At original deployment time the EDS had no real support outside the IT staff and it was, at best, a peripheral system used just for the online white-pages directory. Politically and technically speaking, it would have been impractical to deploy anything more complex or resource intensive than what was deployed.

It has only been with the growth of knowledge about identity management needs, the EDS role, and the broadening of its support base, both inside and outside the IT department, that Carleton has reached the point where it can even consider a "heavyweight" EDS implementation as a means of supporting further growth.



## Identity Management

Despite the success of our EDS, true identity management is still in its infancy at Carleton. IT management and technical staff have engaged departments like Human Resources and the Dean of Students Office in conversations about regularizing business processes (hiring and termination) so that we can automate and e-provision them.

## Authentication and Authorization

Carleton has only rudimentary single sign-on in place, and has instead implemented a single-*credential* setup in which everything authenticates, directly or indirectly, using Novell eDirectory. The EDS is a client of eDirectory so anything that can authenticate an entity by doing an LDAP bind can implicitly become part of the single-credential environment.

NMI-EDIT provides an open source software package called Shibboleth<sup>4</sup>, a standards-based tool that provides mechanisms for controlling access to web based resources (particularly in inter-institutional use), while offering options for protecting personal privacy. While Carleton isn't ready to implement Shibboleth on campus yet, it will be considered as the basis for web-based single sign-on.

Currently, authorization is addressed using dynamic as well as static course groups in the EDS. All too often vendors supply applications that do not leverage an LDAP directory to provide authorization informa-

tion, and the College ends up supporting another silo-like data store to support this function. We need to find a more efficient way to integrate the authorization functions of our applications with our IdMS infrastructure, so that individuals' roles at the College can drive their access to services.

## Lessons Learned

When implementing this new infrastructure, the following lessons were learned:

- Make sure your technical people are informed about the business needs and why the project is important. Make sure they are accessible; they have to work actively with constituencies that understand FERPA, HIPAA, etc.
- Don't underestimate the political issues you will face.
- Create applications that will win hearts and minds.
- Don't just implement LDAP roadmaps and best-practice documents cookie-cutter style; be prepared to adjust to local needs
- Understand that the infrastructure will evolve.
- Implement according to political realities and design with the future in mind.

## In Conclusion

Smaller schools have similar pressures to address technological-savvy students, parents, alumni, and other constituents as a growing electronic community. The issues, however, of resources and priority can become much more acute.

---

<sup>4</sup> The NMI-EDIT Consortium's Shibboleth software is available at [shibboleth.internet2.edu](http://shibboleth.internet2.edu) or from [www.nmi-edit.org](http://www.nmi-edit.org).

Carleton College has taken the large school approach and scaled it down to an architecture that can be supported and that can grow as the needs of the campus and constituents grow.

## More Information

For more information on Carleton College's identity management and directory infrastructure, contact Joel Cooper at [jcooper@ carleton.edu](mailto:jcooper@carleton.edu).

