

NMI-EDIT Extending the Reach Program: Final Report

The NMI-EDIT Consortium of Internet2 and EDUCAUSE was funded in 2001 by the National Science Foundation Middleware Initiative (NMI) to develop tools, software, and practices to support interoperable identity and access management infrastructures. The Consortium released the Extending the Reach (ETR) Call for Proposal in April of 2004 with the overall vision of exploring possible models to scale the outreach work and inform their development efforts through collaboration with a wider, more diverse group of institutions. This document summarizes the ETR activities, milestones, and approaches from the Call for Proposal in April 2004 to the submission of the individual project reports in January 2006.

Background

The primary goal of the NMI - Enterprise and Desktop Integration Technologies (EDIT) Consortium was to build an interoperable identity and access management infrastructure across research and education community. For the purposes of the grant, identity and access management (IdM) was considered a combination and interdependence of three areas: policy, business process, and technology. It consolidates the pertinent identity information about individuals from across an organization and makes that information available, in appropriate and policy-guided ways, to services and applications. Critical for security architectures, identity management provides the mechanism for appropriate, auditable access to online services.

Campus implementations of identity management can take several years, however, and clear directions for deployment had not been developed. Institutions either deployed through experimentation (which takes time) or by networking with others to learn what works and what doesn't. As a result, the outreach and education activities were not only critical to providing information about common practice and developed tools, but also to shortening the time to production. However, the demand for information and, in particular, peer networking exceeded the availability and NMI-EDIT decided to experiment with scaling the activities to reach more schools.

Extending the Reach Program

To prototype scaling the outreach efforts, NMI-EDIT developed a program for higher-education related communities that might also be interested in the benefits that identity management could provide. State higher-education systems and state education networks were chosen as logical audiences, since they both had established working relationships, existing member education and communication channels, and, in many cases, similar drivers among the multiple institutions.

The Extending the Reach (ETR) Call for Proposal was released in May of 2004 with overall vision of exploring possible models to scale the outreach work and inform the NMI-EDIT development efforts through collaboration with this wider, more diverse group of institutions.

ETR Program proposals required:

- Enabling deployments of core middleware (IdM) that conform to higher-ed practices.
- Developing and piloting diverse business models, services, and products for middleware training, consulting, and deployment.

- Disseminating information about the project to other organizations and communities to spur other similar activities.
- Contributing to NMI-EDIT outreach and technology-related work, where appropriate.

As a result of the Call, the NMI-EDIT partnered with and offered modest funding to the state systems of the University of Alaska, [University of Texas](#), and [California State University](#), as well as the [Great Plains Network Consortium](#) to support identity and access management education and deployment assistance to their member campuses. Not surprisingly, these project teams were requesting this additional funding to enhance a project that was already underway.

Summary of the Participants' Projects and ETR Milestones

Though the goals of the four participant consortia shared many commonalities, the individual projects addressed very different challenges. Results of the ETR Program can be further explored by viewing the individual case studies submitted by each of the participant institutions:

- **University of Alaska** focused on the development and printing of phone books based on a common electronic directory service in order to drive the acceptance of it across their system. The project was funded several months later to support an University of Alaska Identity Management Summit to increase the awareness and understanding of IdM-related issues across the UA system. For a detailed project report, refer to [Identity Management and Enterprise Directories in a University System](#).
- **University of Texas** pursued four projects associated with 1) building a [Shibboleth](#)® and related IdM infrastructures at member campuses, 2) deploying Shibboleth-enabled services with partners, 3) piloting the sourcing of IdM services for small campuses. The project manager also leveraged the ETR mini-grant to build a UT Federation, which was not a part of the original proposal. The project was funded again several months later to support the building and piloting a Shibboleth-enabled version of the UT system benefits annual enrollment application. For a detailed project report, refer to ["Extending the Reach" Case Studies](#).
- **California State University** leveraged their ETR mini-grant to support their on-going IdM project of facilitating the building of interoperable identity management implementations at their member campuses. To address the diversity of needs, resources, and staff expertise, the system piloted a project where one campus hosted the IdM back-end technical systems (person registry, enterprise directory, and authentication) for another. For a detail project report, refer to [The Identity Management Collaborative: Remote Middleware Support](#).
- **Great Plains Network Consortium** was a loosely-affiliated group of campuses spread across seven states in the central part of the country. These schools had a good track record of working together on previous projects and decided to launch an initiative to build an IdM middleware infrastructure across the region. Sharing research resources was identified as a priority and Shibboleth was deployed at a number of the sites. Two additional side projects were funded several months after the start of the project: The first entailed deploying the Shibboleth system to facilitate access to a bioinformatics application; and the second extended the [Subversion](#) code revision system to support Shibboleth for access control. For detail project reports, refer to [Building the Regional Middleware Infrastructure](#) and [Integrating Shibboleth, Grid and Bioinformatics](#).

Major milestones of the ETR Project centered on the dissemination of not only the materials developed through the efforts of the individual project teams, but also on the work that the project leads did to collaboratively prepare for their presentations. To convey a generalized view of their experiences, two tools were jointly developed: the Collaborative Identity Management Life Cycle (Appendix A) and the Identity Management Matrix (Appendix B). For a list of the major milestones, see the following table:

Major Milestones	Date
ETR Project Call for Proposals Released	April 2004
Kick-off Meeting for the ETR Project PIs	June 2004
Internet2 Fall Member Meeting Birds-of-a Feather on the ETR Project	September 2004
University of Texas System Workshop for Identity Providers: Shibboleth InstallFest	September 2004
Shibboleth InstallFest at the Oklahoma Supercomputing Center	October 2004
University of Alaska's Enterprise Directory goes into production	November 2004
University of Texas System's installation of Shibboleth in the Texas Medical Center Library goes into production. Includes a Shibboleth-enabled EZ Proxy Service which handles traditional IP-based and federated access methods.	April 2005
Internet2 Spring Member Meeting Track Presentation on the Collaborative Identity Management Life Cycle	May 2005
GPN-MidNet Conference on Campus IdM, Grids, and Networking	June 2005
California State University pilot goes into production	June 2005
University of Texas System Workshop for Service Providers: Shibboleth InstallFest	June 2005
California State University Identity Management Workshop	July 2005
Internet2 Fall Member Meeting Track Presentation	September 2005
University of Alaska Identity Management Summit	September 2005
EDUCAUSE Annual Meeting Preconference Seminar on Identity Management for the Rest of Us	October 2005
ETR Project Ends	December 2005
Case Studies made available	January 2006

Program Management Overview

Since the ETR Program was experimental and time to implement was relatively short, the program manager worked to design an environment which would provide a high probability of the success of the four projects. This included:

- expectation of individual project progress,
- opportunities for education and information sharing with national leaders in the IdM field,

- opportunities for project participants to help each other, and
- expectation of presenting on project findings at nation and regional R&E community meetings.

Primary methodologies used to encourage the above activities were bi-weekly phone calls, an email list, and collaborative presentations. A team collaboration website was set up, but not used very heavily; just-in-time exchange of documents seems to suit the participants better.

The calls for the first six months focused on getting to know the other members, sharing their project start-up challenges, and providing a consistent expectation of reporting. Several guest speakers were asked to join the calls to address questions posed by the project leads about the NMI-EDIT technologies and implementations. Tom Barton from the University of Chicago and Renee Frost from Internet2, among others, helped in this regard.

Presentation opportunities were identified early on in the project. Collaborating on developing these shared talks helped the participants to understand each other's project challenges, provided hard dates which influenced internal project milestones, and disseminated interim (and final) findings to the wider community. In addition, developing these presentations resulted in a Collaborative Identity Management Life Cycle and an Identity Management Matrix as mentioned earlier.

Lessons Learned

During the course of the 18-month initiative, several key successes became apparent:

- Progressing with the technology was not the most difficult part. Coordinating with member campuses, encouraging them to join the effort, and developing shared goals (or accepting them in some cases) and definitions of responsibilities were far more challenging.
- Starting small and finding an application that appeals to a key community was very successful in both the more structured and unstructured collaboration environments. Sharing an application or resources across many campuses resulted in improved service at reduced development costs.
- Moving beyond a proof of concept model and into the strategic realm requires stakeholder involvement and the establishment of a governance model. This can be very informal or formal, but involves setting direction and priorities and resolving issues that develop as the project progresses.
- Educating and dialogue is critical, especially early on and at critical decision points.
- Establishing guiding principles was helpful for curbing scope creep or project diversion later on. Maintaining progress depended on clearly defined priorities and strong project coordination and management in some cases and opportunities to collaborate in others.
- Staying current with practices, changes, and events of the broader middleware community was vital.
- Securing a solid IdM infrastructure was considered a continual effort and constant change aspect was reflect in the Collaborative Identity Management Life Cycle.

Outcomes

As a result of the collaborations, participants reported valuable outcomes stemming from the collaborations:

- Directly affected over 332,000 faculty, staff, students across 43 campuses, health centers, and state network providers. Also supported three master's theses.

- Published article in Scalable Computing Volume 7, Number 3, pp. 95–108 by Amy Apon, Greg Monaco, and Gordon Springer entitled “[The Great Plains Network \(GPN\) Middleware Test Bed](#)” describing their ETR work.
- Inter-institutional authentication via Shibboleth and authorization to central resources, scalable and manageable mechanism defining access to library resources and services across a consortium of more than 40 institutions,
- Better understanding of the shared management responsibilities between identity provider (typically the campus) and the service provider (could be another campus or the system/central office). This includes the pull and tug of individual campus autonomy and preservation of branding and student data stewardship with the seamless integration of services across the member schools in a consortium.
- Provision of remotely supported identity management services to isolated campuses with limited resources.
- Secured access to multiple applications (Oracle, Banner, Blackboard, Library Systems, and PeopleSoft) via common interfaces eliminates duplication of identity data and authentication systems.
- Shared virtual organization that offered common bioinformatics tools to support research across the regional membership.
- Collaborative models for developing and supporting a Identity Management Infrastructure on another campus that can be exported to other schools with similar resource constraints.

Future Work and Conclusions

Future work that would benefit the community and leverage the ETR findings includes:

- Extending these models and outcomes to develop a set of best practices and guidance for other higher-education systems.
- Leveraging the new interest in identity management in the state networks community and work with them to outreach to their constituents, an even broader community typically comprising higher education, K12, libraries, and local and state government entities. An initial step would include working with network providers to develop business case for providing education and support for IdM.
- Consolidating and packaging the work done by the ETR participants and developing a toolkit that is useable by a wider range of organizations.
- Exploring existing state-based and national research and education federations for the purposes of making recommendations on pros and cons of each. This might include investigating the business case, implementation considerations, and longer term operational ramifications of the two (or more) models.

Identity and Access Management lies at the core of building a diverse and flexible environment that invites collaboration and research, while mitigating financial and management burdens often associated with an ever extending list of service providers and collaborators. Providing opportunities for institutions to help each other and learn from the experiences of others are critical to secure and appropriate deployments.

The ETR Program was significant in that it explored a number of ways to help campuses plan and develop an interoperable identity management infrastructure to support both security and collaborative services. The program also investigated the outsourcing of IdM infrastructure which was successful and still operable in both instances. Unexpected results included the establishment of a federation in Texas.

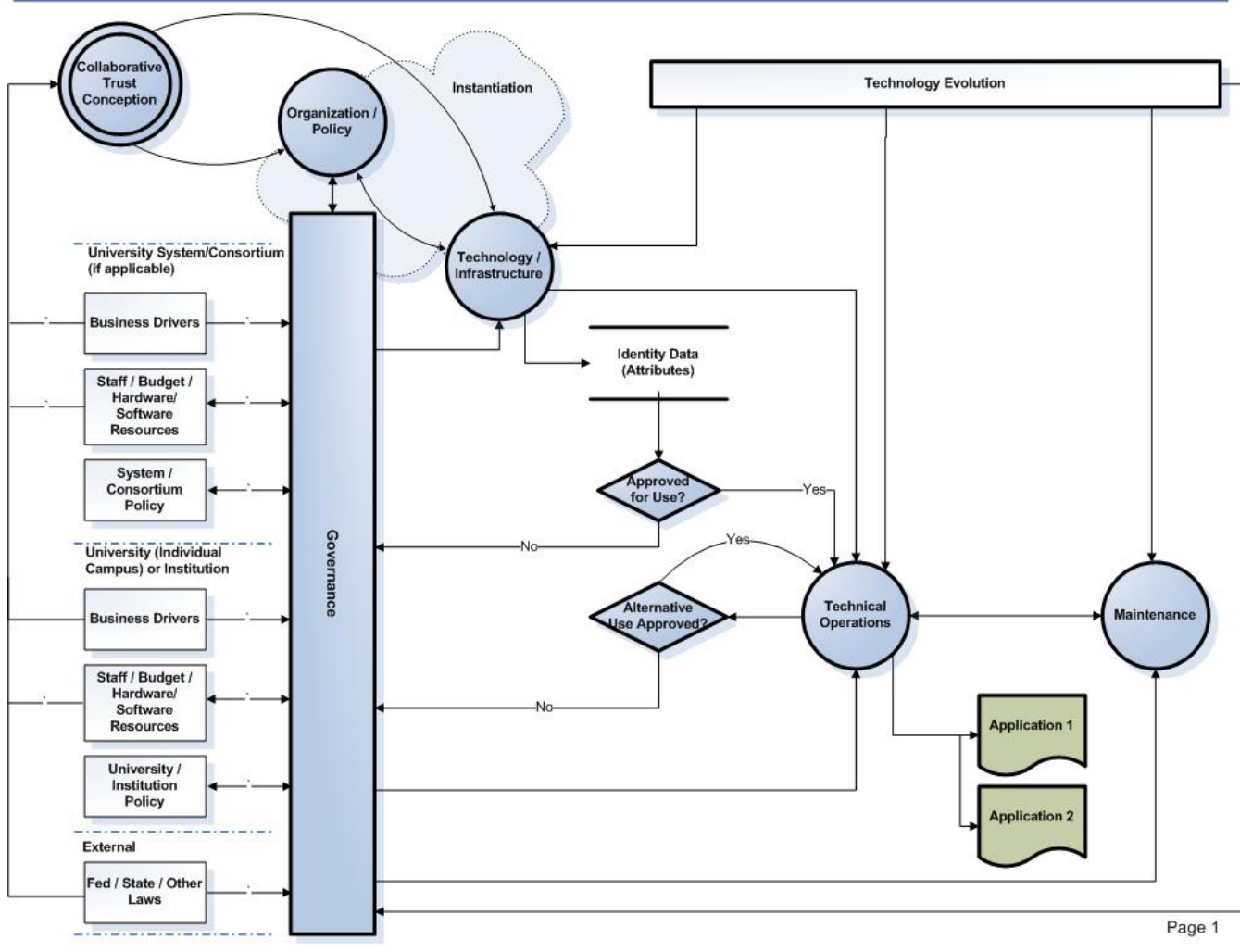
Aside from the specific projects, the program in a very short time, nurtured a number of individuals who are still involved today in the development and management of this infrastructure through helping their colleagues in other states. It is clear that state systems and regional network providers can have a large impact in enabling this not only for their member institutions and but also for other campuses across the nation.

For more information, contact Ann West at awest@educause.edu or awest@internet2.edu.

Appendix A: Collaborative Identity Management Life Cycle

As part of the Internet2 Track sessions, the ETR project leads developed a life-cycle that represented their common experience with implementing identity management across their member campuses.

Collaborative Identity Management Life-Cycle



Appendix B: Identity Management Matrix

This matrix was developed as a part of the EDUCAUSE Preconference Seminar: Identity Management for the Rest of Us and provided an at-a-glance view of the project management aspects and technology components involved in implementing identity management.

↑ Identity management components ↓	Federation <i>(Federate)</i>							
	AuthZ <i>(Provision)</i>							
	AuthN <i>(Relay)</i>							
	Web Gateway <i>(Privilege)</i>							
	Directory <i>(Reflect)</i> <i>(Credential)</i>							
	Registry <i>(Join)</i> <i>(Affiliations)</i>							
	Business	Policies & Stakeholders	Security	Technologies	Deployment	Integration	Resources	

← Aspects of identity management success / project mgmt →