

Signet™ Privilege Management

The Signet Privilege Management System enables consistent application of policy and business access rules across managed services. It places the control of a resource in the hands of its steward.

What's the Signet Advantage?

The Signet Privilege Management System was designed to address the challenges of managing what people can access and giving control of that process to those in the departments who make the decisions.

Because the implementation of access rules is typically scattered among many systems across an institution, coordinating policy and privileges campus-wide is difficult. This leads to individuals having levels of access that are inappropriate for their positions. And this contributes to loss in their productivity and increase in your security risks.

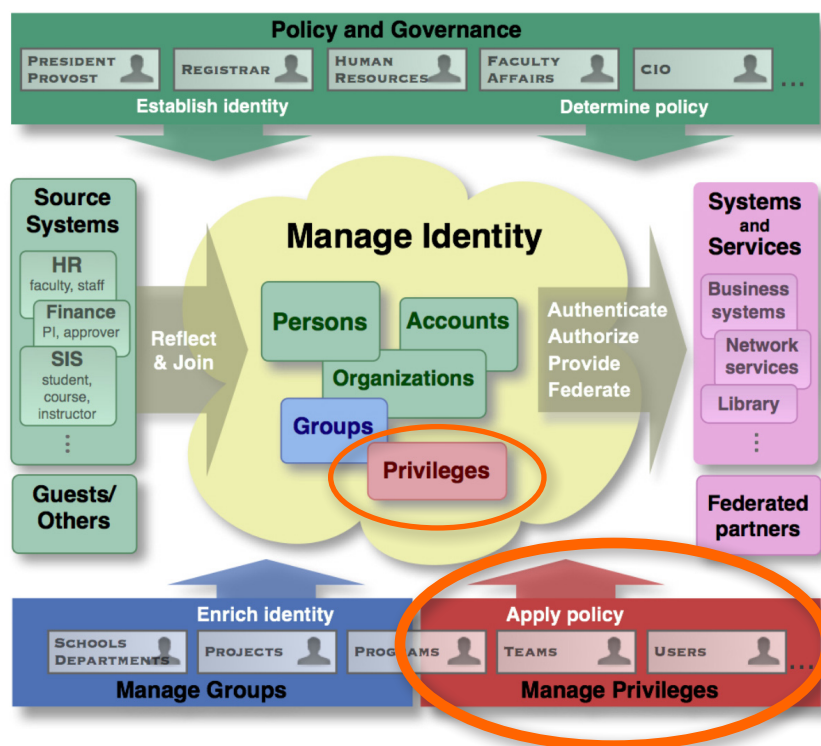
Provides a Single Point for Managing Authorization

Signet holds information about protected resources and services that someone might access or use, such as purchasing or learning management systems. It then enables the resource owner to define the specific interactions (called privileges) with that resource, such as purchasing materials or updating grades for a homework assignment. Appropriate campus decision-makers assign or delegate these privileges to individuals, guided by policy rules coded into the system.

In the diagram above, individuals across campus manage their users' privileges, which are then supplied to the identity management system and used by applications and services to make authorization decisions. Individuals can also use the system to review their own access privileges. Signet provides a consistent view and application of authority rules across all campus systems it serves.

Consolidates the Technology Infrastructure, not the Control

The decisions that determine who can access what should be distributed and maintained by the departments, schools, business offices, and others responsible for the use of resources. However, the infrastructure of electronic



Signet's Role in the Identity and Access Management (IAM) Model

identity should be stewarded centrally – departments should not have to run their own identity and access management databases to control access to their services.

Helps Business Happen

Signet keeps the business decisions in the hands of the business owners, access control in the hands of the application owners, and the technology management in the hands of the technologists. Schools, departments and even project leads can use your tailored Signet interface to manage access using plain language they understand. This removes IT from the middle of implementing the day to day access decisions and increases the overall integrity of the policy and technology interaction. If a department is host-

ing a meeting and wants the attendees to have access to the wireless network and local online collaboration space, the authorized meeting planner can just update Signet and access is granted according to institutional policy.

Keeps Track

Because Signet provides a consolidated point of policy enforcement and maintains a history of who has granted access to what, it provides a single point for auditing and reporting of authority-related decisions. This contributes to across-the-board compliance for the systems Signet supports.

Streamlines Operations

Signet separates the management of the policy and business rules from the technical system, so a change in system technology does not affect the access of those using it. And after integrating Signet with your identity management system, you'll have a way to manage the lifecycle of a person's access privileges, enabling automatic revocation of privileges based on status and affiliation changes. Removing IT from the middle of enabling or disabling a service for an individual and enabling distributed control will ease your helpdesk headache as well. And as you might imagine, the benefits of this software accrue as more and more systems use it.

The Combined Signet and Grouper Solution: Enabling Role-Based Authority

While Signet manages the information associated with what people can do and supports delegated administration of privileges, it doesn't manage groups or membership of groups such as the list of department chairs or business majors. Campuses can use the Grouper Group Toolkit (grouper.internet2.edu) to automate or enable a delegated management of groups and related memberships. Together, they provide a solution for role-based authority.

What Do I Need to Have in Place?

To implement Signet (or Grouper), you need to have

- An institutional identity management system and a model for how privilege management fits in.
- A good relationship with key stakeholders across campus to develop the policy and business rules associated with authority.
- A model for support to address problems associated with privilege management debugging and end-user questions.

How Do I Get Started?

To learn more about the Signet Privilege Management System visit signet.internet2.edu. Join the Signet community by participating on the email lists and attending the workshops and presentations offered around the country.

To get started with identity management infrastructures, refer to our NSF-funded project, NMI-EDIT, at www.nmi-edit.org, which offers roadmaps, practice papers, articles, and other tools to get you going.

About the Internet2 Middleware Initiative

Led by the Middleware Architecture Committee for Education (MACE), the Internet2 Middleware Initiative comprises a number of projects that address challenges in the middleware space, such as identity and access management. For more information, visit middleware.internet2.edu.

Acknowledgments

Development of the Signet Privilege Management System was supported with funding from Stanford University and Internet2 through their NSF Middleware Initiative (Cooperative Agreements OCI-0330626 and OCI-0721896).

Instead of having individuals share credentials, we'd like to have a person delegate their authority to someone else, sometimes for short periods, and do so in a way that's secure and hassle-free. Currently, we can do this on some systems, but not across the board. For example, researchers manage their collaborators' access to project-based systems, services, and data, but have no time to do it. Instead, they want to delegate these privileges to their trusted graduate student and free their own time to do research.

Tom Parker
Identity Management
Project Manager
Cornell University

SIGNET.INTERNET2.EDU