

Identity and Access Management

Critical for security and collaboration, the Internet2 Identity and Access Management model provides a framework for simplifying the management of access to services, implementing policy, increasing transparency, and enabling operations to scale by integrating an enterprise identity management infrastructure with services provided by both central and distributed IT.

What does Identity and Access Management do?

Simplifies and Secures

Identity and access management (IAM) ensures that the right people access the right services. In the past, this was implemented system by system with duplicate identity data distributed across campus. Add another service and you add the identity infrastructure to go with it. Now try to manage the distributed security issues associated with these duplicate identity stores and you have your hands full.

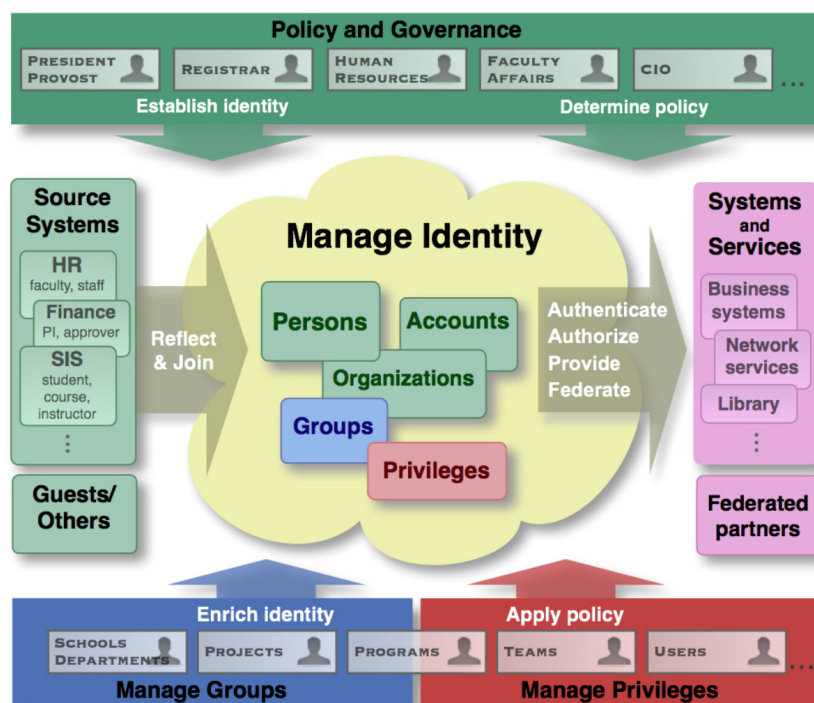
The solution is to use the same identity information service for all your applications. As exemplified in the diagram, if you integrate the data on the left and services on the right into the IAM infrastructure in the middle, then all the policies and procedures can be applied in that one spot in the center. This

- simplifies by leveraging one IAM infrastructure over and over.
- secures by consolidating your identity infrastructures from many to one and reducing the security headaches from overwhelming to manageable.

The first step in building an IAM infrastructure is to review the data distributed across the campus about people, decide what's relevant from the source systems (the light green box on the left in the diagram), and consolidate and update (or Join and Reflect) the information into one identity entry for each person in the community. So if Bob has entries in financial aid, student, and human resources systems, that relevant identity data would be extracted as needed and maintained in one digital identity record in the IAM system.

Helps Collaboration Happen

Once the identity information about a person is consolidated, appropriate campus constituents can use tools to establish roles, grant access, and add group membership as



Identity and Access Management (IAM) Model

represented in the blue Enrich Identity and red Apply Policy boxes on the bottom of the diagram. The resource owners can define the specific interactions (called privileges) with that resource, such as purchasing materials or updating grades for a homework assignment. Imagine setting up a standard “collaboration package” that includes group calendar, email list, wiki space, and so on, that campus individuals can request and then control who can have access to it, all without Help Desk intervention. In the past, these group memberships were not coordinated across services and had to be altered in each application when the members changed. Consolidating the groups and privileges allows groups to change once in the IAM system and be “pushed out” to or accessed by the services in the collaboration package.

Enables Shared Management

With the consolidation of identity information, the decision makers across campus can now also effect change much more quickly through interaction with the IAM system. This occurs because the IAM infrastructure becomes a bridge from the institutional processes and resource owners to the technology operations. It also enables the scaling of IT operations to meet the distributed needs and the mission of the institution; as the process and requirements evolve, the accompanying changes are made in just one place, the IAM system.

Makes Operations Transparent

Providing a single point of management enables consolidated logging and a consistent view of the access rights and requirements of the individuals and systems involved. This approach enables a transparent way of applying, viewing, and implementing policy decisions in the technology infrastructure. It also provides a history of who has granted access to what, and a single place for auditing and reporting of authority-related decisions as well as monitoring for security issues.

Federates Globally

Once the identity data has been enhanced with the authority data (as shown in the boxes on the bottom of the diagram on the previous page), it is made available in a number of timely ways to the systems and services (on the right of the diagram). Not only is this applicable for controlling resources managed by the institution, but the IAM infrastructure can also supply identity data to off-campus service providers, such as external library consortiums, course content partners, or discipline-specific Grids through the use of federated identity management software.

How does the work get done?

Partnering with the Internet2 Middleware Initiative since 1998, the Middleware Architecture Committee for Education (MACE) provides the primary direction and development guidance for the project. Consisting of a group of US and international higher-education IT architects, MACE was formed to investigate the creation of a national interoperable

identity and access management infrastructure for the US Research and Education community that would fit into a global context.

To do this, MACE developed an identity and access management architecture model and worked to address the missing functionality. These gaps are being addressed in five ways:

- Developing software and tools. An example includes the Shibboleth System.
- Gleaning the better community practices and developing roadmaps to help campuses deploy interoperable implementations. Examples include the directory practice papers and related Enterprise Directory Implementation Roadmap.
- Participating in standards-setting organizations to address interoperability. Examples include eduPerson schema and Security Assertion Markup Language (SAML).
- Partnering with others to promote their tools and software. Examples include the PERMIS Privilege Management Software and A-Select web single sign-on system.
- Providing educational opportunities to the broader community. Examples include the Campus Architecture and Middleware Planning (CAMP) workshops.

How can I get involved?

To learn more about the Internet2 Middleware Initiative and MACE, visit middleware.internet2.edu and join the community by participating on the email lists and attending the workshops and presentations offered around the country.

Acknowledgments

The Internet2 Middleware Initiative is supported in part by the NSF Middleware Initiative (Cooperative Agreements OCI-0330626 and OCI-0721896).