

Building a Balanced Identity Management Infrastructure

The identity management function is a combination and interdependence of three areas: policy, business process, and technology. It consolidates the pertinent identity information about individuals from across campus and makes that information available, in appropriate and policy-guided ways, to services and applications. It also allows for the integration of services and authority management that can grant, change, or rescind access based on status or affiliation with the institution. Critical for security architectures, identity management provides the mechanism for appropriate, auditable access to online services.

Reasons to Build an Identity Management Infrastructure

The 2006 EDUCAUSE Current Issues Survey of higher education IT leaders ranked “security and identity management” as the number-one IT-related issue in terms of its strategic importance to the institution (<http://www.educause.edu/2006SurveyResources/10236>). Motivating forces for building an identity management infrastructure are both internal and external to the institution and include the following:

- *Legislation and Compliance.* The increase in regulatory legislation has created more audit and compliance requirements, particularly in the area of security management, for many campuses. Most recently, institutions are working to understand what burdens, if any, the Communication Assistance for Law Enforcement Act (CALEA) will place on the campus networking infrastructure and on resources related to tracking people and retaining data.
- *Publicity and Public Relations.* Publicity over incidents in which personal information has been stolen or lost has heightened public awareness of the risks posed when databases are used to hold large amounts of personal information. A growing number of publicized incidents have occurred on higher education campuses and have generated significant negative publicity for the institutions involved. Identity management can facilitate tighter controls of access to information, as well as consolidate logging, allowing campuses to more easily spot break-in attempts.
- *Growing Service Needs.* Generally, the most diverse set of requirements for identity management comes from internal pressures to offer more online services. These services can include providing accounts for distance-education students who will never be seen in person and also contracting with third-party hosted services, such as online music providers, external course management systems, and outsourced purchasing services.
- *Services Available from the Federal Government.* Federal agencies are also planning to offer services online, with access managed by credentials supplied by nongovernment identity providers. Higher education institutions will represent one class of customers for these services. To use the services, they will need to meet federal government requirements for practices related to identity proofing and distribution of credentials as well as for policies regarding, and documentation of, these practices.

Taken together, these motivators can provide compelling reasons for building an identity management infrastructure.

The Three-Legged Stool

The components of identity management can be thought of as a three-legged stool: (1) institutional policies, (2) business processes derived from those policies, and (3) the technology implementation that supports both the institutional policies and the business processes. Each leg must be built appropriately to provide the balance necessary for a well-established identity management system.

To illustrate this, we will consider some of the ramifications of the following institutional goal from Duke University: *Ensure that all faculty and staff can access the appropriate online services for their job within one hour of being hired.*

Institutional Policies

Policies state an organization's intent or decision on an issue and describe the “what” or “why.” In the goal cited above, a number of policy and institutional guiding principles come into play:

- *Data as a Strategic Resource.* Identity data stored in the systems of record, such as the Human Resources (HR) system, must be appropriately shared with the service providers, who typically are not in the HR department. These service providers can be the faculty member's academic department, the central IT department, the library, or an external provider such as the outsourced purchasing firm. Ensuring that access to these systems can be granted in the one-hour time frame requires appropriate sharing of the data across department boundaries. The basis of identity management policy is the institution's recognition of data as a strategic resource and the statement that data should be shared

outside the steward's department for appropriate institutional purposes.

- **Data and Service Definitions.** What does it mean for someone to become a new faculty or staff member? Who is responsible for this definition and its interpretation? Who are the stewards for the various data and service components? For instance, HR might be the steward for employee-related information, but IT might be the steward for the authentication and related identity-management infrastructure. Where does the boundary of one department end and the other begin?
- **Security and Privacy Balance.** What is the risk tolerance of the institution? If a person has signed an offer to become the new CFO but hasn't yet arrived on campus, should he or she be able to access the financial system? In addition, a balance must be struck in tracking activities for security purposes and in accessing those logs with personally identifiable information. What identity data does the institution keep directly in its source systems and indirectly in places such as network activity logs, and how does the institution protect that data?
- **Appropriate Use.** What are the responsibilities of the hired employee once he or she has access to the online campus services? Does the institution guide the employee in choosing an appropriate password and protecting it?
- **Compliance with Federal and State Regulations.** Are all these and related processes in compliance with federal and state regulations, such as the protection of identifiable and personal information?

Business Processes

Business processes describe the "how" of implementing a policy intent. In our example, once the employee has been hired and arrives on campus, a number of business processes are involved in the provisioning of services:

- **Identification.** In this process, information about a person is gathered and used to provide some level of assurance that the person is who he or she claims to be. Generally, this identity

verification takes place within the office (e.g., HR) that first encounters the individual and creates the employee record within the institutional system(s) of record.

- **Registration.** After the person has been identified, the registration process ensures that the physical person is coupled with the correct electronic identity information and then given electronic credentials. This links the physical person (who presented the ID to prove authenticity) with the login ID (who will present a password in the electronic world to do the same).
- **Service Provisioning.** After institutional policies provide overall guidance about who can assign authority for what resources and purposes, the employee should be granted a set of services based on his or her position and anticipated duties. Derived from the policy statements, a number of processes are associated with the assignment of institutional and departmental access rights and services.
- **Educating and Training.** The new employee should also be given information about the acceptable and appropriate use of electronic resources, as well as his or her responsibilities. This is especially critical for employees with access to sensitive information.

Technology Implementation

Supporting the business processes, technology describes the "how" of implementing the intent and expresses the institutional policy. Some of the technology pieces include the following:

- **Aggregation of Identity Information.** An individual may have identity-related information in several different locations: financial aid, student, HR, and athletics systems, for instance. Identity management reconciles the identity information and aggregates it to develop a consolidated view of the individual and enable access control based on his or her affiliation with or role at the institution. Business rules are then applied to assign credentials for authenticating and role or entitlement information for granting access to services.

- **Service Provisioning.** In our example, once the HR system indicates the person is approved to receive services, the identity management system reflects this change and makes the appropriate identity information about the individual available to the applications. This enables the new hires, for instance, to access the services required for their positions once they receive their credentials (e.g., userIDs and passwords.)
- **Authentication and Authorization.** After receiving these credentials, the new employee can then use them to verify his or her online identity and access the provisioned application. The authentication system and application both must be architected securely so as not to compromise the credentials and, consequently, the application or data the person is accessing.

Conclusion

These three components—policy, process, and technology—support each other to balance the stool of identity management. In particular, accommodating the above motivators requires a centralized approach to policy and management responsibilities for the identity-related services that underlie campus-wide and high-assurance-level (or high-security) services. This does not preclude organizational units from managing their own independent services for specific portions of the campus community; however, it does mean that the policy, business process, and technology architectures need to be defined at the institutional level. Only then can identity management offer the promise of secure collaboration and service opportunities and make a strategic contribution to the institution.

Note

This material is based in part on work supported by the National Science Foundation under the NSF Middleware Initiative, NSF Grant No. OCI-0330626. Special thanks go to Michael Gettes, Senior Technology Architect and Strategist at Duke University.

Renee Shuey is a Senior Systems Engineer and Team Leader in the ITS Emerging Technologies Group at Penn State. Ann West holds a joint appointment with EDUCAUSE and Internet2 to lead the identity management outreach activities for their NSF Middleware Initiative grant.