7 things you should know about...

Federated Identity Management

Scenario

Gillian's graduate work in oceanography involves enormous amounts of water-quality data from many sources along the Atlantic seaboard as well as the West Coast. From her institution in Florida, she collects and analyzes data sets from laboratories and oceanographic facilities affiliated with other colleges and universities, government agencies, and even some private organizations. Not only do these entities share data with Gillian from their underwater instrumentation, but some also allow her to remotely access specialized applications they have developed.

Enabling this level of collaboration to take place in a manageable way is a federated identity system that includes all of the organizations in Gillian's research as members. Under the system, Gillian maintains a single digital identity with the university where she is enrolled. When she goes online to access data or services from any of the other organizations, she logs in using her university username and password, and her home institution confirms to the other organization that her credentials are legitimate. Gillian does not need to create dozens of user accounts and passwords for the many organizations or for individual applications at particular organizations. Her university credential also provides access to a website where she can apply for and track state and federal research grants; the site uses authentication details from her university to provide information filtered for her research. The members of the federation do not need to maintain separate accounts for Gillian. Indeed, some of the facilities do not offer "guest" access to their computer systems, and the only way nonaffiliated individuals can log in is through a federation partner.

When her research begins to produce results, Gillian takes advantage of the federated identity system to share data sets and preliminary conclusions with other researchers—an update to authorization protocols allows authenticated researchers at federation partners to access Gillian's data. In the same way, other researchers open their research notes to this virtual community of oceanographers, resulting in new levels and kinds of collaboration around water quality and the many factors affecting it. And because commercial providers that Gillian uses for e-mail and document sharing are also members of the federation, she can access those services as well while maintaining a single digital identity.

1 What is it?

Identity management refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources. In a campus setting, many information systems—such as e-mail, learning management systems, library databases, and grid computing applications—require users to authenticate themselves (typically with a username and password). An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled. Federated identity management permits extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations. In a federated system, participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources. This approach streamlines access to digital assets while protecting restricted resources.

2 Who's doing it?

Most colleges and universities use some form of identity management to control access to institutional assets—including online educational resources, administrative information systems, emergency notification systems, and research tools—based on a user's identity and role, such as student, faculty (which could include TAs), staff, alumni, and so forth. The Indiana University Pervasive Technology Institute, the IU School of Medicine, Purdue University, and the University of Notre Dame have developed the Indiana Clinical Translational Sciences Institute HUB, which uses federated identity to provide access to medical databases, high-performance computers, and life science visualization tools. Several states have created identity federations, as have some system campuses, such as the University of Texas. One of the larger federations, the InCommon Federation, has more than 150 participating organizations—most of them colleges and universities—currently covering more than three million end users.

3 How does it work?

When a user affiliated with a member of a federation requests a protected resource from another member organization, the user is prompted for identifying information including his "home" organization. This request is passed to the home organization, which verifies the user's credentials and asserts to the requesting organization that the user has been authenticated. Federation members determine individually which attributes about users will

more ⇨

Federated Identity Management

be shared, such as name, title, or role. Based on this information and their respective policies, member organizations then grant or deny access to particular resources. Users need only one set of authentication credentials—which could be a name and password or some other identity token—to access resources from other federation members. As a result, federated identity management separates access from the establishment of identity and authorization. Institutions no longer have to create and maintain large numbers of user credentials, instead managing identities only for their own users and accepting credentials from other federation members. Attributes about users are verified by the home institution, which is most likely to have current, accurate information about the user, so there is no need to propagate status changes across multiple institutional identity systems. As student users graduate and assume new relationships with organizations, identity management systems in some cases can follow these changes and continue to provide appropriate access.

Why is it significant?

Because identity management eliminates the need to maintain distinct user credentials for separate applications, it results in greatly simplified administration and streamlined access to resources. By using a common framework to share information between trusted partners, federated identity frees institutions from having to establish separate relationships and procedures with one another to conduct transactions. Deploying new IT capabilities is easier because the authentication mechanism is already in place, and, as such, federated identity can play a key role in using cloud computing to provision IT functions and services. Federated identity management puts the focus on users of information and services rather than on entities that house those resources. By ensuring reliable access from multiple locations, federated identity systems provide a measure of mobility—for students who take courses at multiple institutions, for instance, or instructors who serve as visiting faculty. By eliminating the need to replicate databases of user credentials for separate applications and systems—each of which represents a potential point of weakness—identity management can offer improved security, both for digital resources and for users' personal information. This increased security facilitates compliance with federal and state regulations covering personal data, including HIPAA, FERPA, and others.

What are the downsides?

Despite the benefits of federated identity, the up-front costs to modify existing applications and systems can be an obstacle for some institutions. Federation membership might require different or more stringent identity protocols than an institution currently observes, and an institution might participate in multiple federations, each with unique requirements. Participating in a federation requires developing thorough institutional policies concerning access rights and compliance with the complex landscape of regulations. Although such policies and the work involved in writing them are beneficial, some institutions might not be ready to undertake such an effort. The risks associated with unauthorized access to certain services are sufficiently high that provider organizations sometimes demand additional assurance from federation members. In these cases, a federation member might follow guidelines that set a higher bar for ensuring that credentialed users are legitimate. Over time, these kinds of measures are likely to deepen the trust in federated identity systems, but the process of getting there will require the often difficult work of developing new protocols and revising expectations. In the meantime, a conservative approach to risk on the part of some institutions will slow adoption of federated identity practices. This contributes to a chicken-and-egg conundrum: lack of federation-ready institutions reduces the incentive to open applications to federated access, while a paucity of federation-ready applications makes the investment in a federated identity infrastructure less compelling to institutions.

Where is it going?

As federated identity practices and systems mature, best practices and shared understanding will likely emerge, resulting in more consistent operational patterns for users and participating institutions. Colleges and universities might not be the providers of "baseline" identities for students. Rather, another entity would supply students with credentials, and institutions might simply confirm that individuals are matriculated students, for instance, resulting in a distributed system of identity management that accommodates increased use of cloud-based services. If identity management indeed becomes user-centric rather than institution-centric, the issue of what entity serves as the originating and ultimate authority for digital identities will need to be resolved and agreed upon by participating organizations. Similarly, concerns about user privacy will need to be worked out to reassure users and ensure compliance with applicable regulations.

What are the implications for higher education?

A growing number of educational resources and services are offered online, and users—students, faculty, researchers, staff, alumni, or others—increasingly expect access to these resources from various locations, including mobile devices. Identity management allows institutions to provide this access in a reliable, secure manner without a proliferation of credentials. To the extent that federated identity allows institutions or even individual faculty to easily offer controlled access to research data or other resources, it has the potential to enable new levels of academic collaboration. Identity management can support institutional policies for extending access to valuable resources to certain groups of users, and the integration of identity management systems across academic, governmental, and commercial spheres further broadens the horizon for interdisciplinary, interinstitutional scholarship.