Electronic Identity: The Foundation for the Connected Age

Individuals in the higher education community, by their very nature, connect to each other and share information and resources. Faculty members connect to and share research with other faculty. Students desire to access institutional computing resources in order to share information with their faculty and other students. Librarians share resource materials with other librarians. This interaction with others and sharing of information presents higher education institutions with a number of responsibilities. Who is authorized to contribute information to be shared? Who is authorized to access such information and for how long? How do the individuals or institutions involved in the sharing transaction know that those who are authorized to engage in the sharing transaction are actually the ones doing so? Further, what methods are available to individuals and institutions to perform these authorizations and authentications in a manner that maximizes the privacy of the individuals involved in the sharing transaction?

In addition to the responsibilities enumerated above, higher education institutions find themselves in an environment in which the definition of who is considered a member of an institution’s community is becoming broader (e.g., related entities, alumni). Further, the information and resources expected to be provided by the institution are continuously expanded (e.g., cloud storage, financial aid services). Finally, institutions are often pressured by campus users, vendors, or other entities who want the institution to use—or facilitate the use of—external authentication systems established by the users individually (e.g., OpenID, login with Google or Facebook) when accessing institutional resources.

Trusted Identities
Many higher education institutions are utilizing the InCommon Federation (https://incommon.org/), a federated-identity and trust system operated by Internet2, as a means of addressing these challenges. This trust system establishes an agreement between the Identity Provider (the institution representing the user who is initiating the sharing relationship) and the Relying Party (the institution managing the service and granting access to the information or resource). InCommon participants— institutions representing higher education, government, research, and the commercial sector—agree to a set of standards for ensuring the electronic identities of their constituents, securing the privacy of their information, and performing private and secure online transactions. In the same way that individuals use ATM cards issued by their local banks to conduct transactions in other cities at other banks, a faculty member can use his/her home institution login credentials to access online and protected course content hosted by a vendor or a colleague at another institution. This federated authentication model, with its common set of standards and technologies, eliminates the need for the Relying Party to create and store credentials for each of its users and enables a high degree of collaboration and information sharing among members.

Authorization and Privacy
A service that is enabled for federated authentication may request certain information about the authenticating person. The information or attributes can be personally identifying (e.g., name and address) or may be more opaque (e.g., a student, faculty, or staff affiliation). The service may use these attributes to determine whether or not the person is authorized for a particular type of access. In most cases, minimal information is shared with the service, in order to maximize the privacy of the individual involved in the transaction. In some implementations, the individual attempting to access a service has the option to approve the release of his/her information to the service. This information release is decided on ahead of time and is coded into the software that manages the transaction.

Identity Assurance
Those Relying Parties, like the U.S. Department of Education’s Federal Student Aid services, that are “relying” on another organization to authenticate individuals accessing their service want to be very certain that the people are who they say they are. To ensure this, the federal government specified security requirements for the electronic credentials of individuals who will be accessing online government services. The InCommon Assurance Program (https://www.incommon.org/assurance/) provides such a framework of practices and a related compliance program tailored for higher education and approved by the federal government to access federal agency services. Many institutions are also finding that implementing these practices enhances their internal security and may contribute to their case for due diligence if they have a data breach.

Collaborating in the Cloud
The explosion of cloud services has opened up a broad range of information-sharing offerings at affordable prices, and faculty, staff, and students are already familiar with a wide array of cloud services available to the general public. E-mail, calendaring, and collaborative solutions are being outsourced, allowing...
educational institutions to devote their IT resources to other on-premise services. But what kinds of identities should be used to access cloud services? How can a faculty member be sure that “John.Doe@Google.com” is the same John Doe who is helping with his/her research project? For some services, formal identity confirmation may not be necessary. But in most cases, it is still important for faculty (or staff) to know which student or employee they are collaborating with. Fortunately, most cloud vendors’ authentication solutions can be integrated with the campus Identity Provider, allowing individuals to authenticate using the institution’s local credentials. Some cloud vendors are members of InCommon, which further helps to standardize authentication protocols, credential issuance, and identity management.

**Identities for Online Learning**

Whether hosted locally or in the cloud, online course offerings can provide large financial benefits to an institution by reducing the need to expand physical facilities. More students can enroll in an online course, whereas the same on-premise course might have a waiting list due to constraints of physical space. Courseware implementers have several options for online identities, depending on how important it is to know that the person who enrolled in the course is the same person who is submitting coursework and/or taking exams. For some courses, the institution’s credentials are the only ones that will be recognized, with the student agreeing not to share the credentials. Other courses may be designed to accept the credentials of another higher education institution. Some implementations of Massive Open Online Courses (MOOCs) are utilizing keystroke biometrics, photo IDs, and webcams to identify their users. Exams may need to be proctored at testing centers, where identities can be verified in person. Online courses may also be not-for-credit and may accept third-party credentials such as an OpenID supplied by Google, Yahoo, AOL, or MySpace.

**Policy Matters**

Institutions need to provide guidance to service implementers regarding the types of credentials that should be used to authenticate and authorize users of the service. During the early stages of development or procurement, each proposed service should undergo a risk assessment that includes determining the impact of authentication error (i.e., what happens if the wrong person gains access to the service or its data?). How important is it to know that the people accessing a set of information are who they say they are? Is the audience for the service primarily located elsewhere, and is the service-compromise risk low? If so, Google or Facebook logins may be acceptable to ease adoption. Some institutional information is highly sensitive; careful consideration of how to identify who has access to information will help ensure the security of the information and the privacy of the individuals who are sharing it.

**What’s in Our (Near) Future?**

As we have seen, there is much significance behind the notions of connections and electronic sharing, especially when the collaboration occurs outside and among our institutions and in the cloud. Intrinsic in these ideas is the further interdependence of the organizations that host not only a service but also the individuals who use the service.

Those of us in higher education have long depended on each other for good behavior in technology: think of the physical network that interconnects our campuses. Now we are connecting on another plane: shared service delivery. We feel the tug toward using more valuable, off-campus services—such as those that enable our faculty to use their campus electronic credentials to submit grant proposals to federal agencies. But for trust to happen in a federated identity context, the Relying Party must understand that the Identity Provider has adequate security, and the Identity Provider must be satisfied with the Relying Party’s policies and practices regarding the storage and use of the identity data sent during the transaction. This interdependence will ultimately drive identity practice standardization across higher education.

This situation will be felt most acutely in our academic medical centers: the higher education institutions that offer medical-related programs and degrees and that manage, or have a relationship with, a teaching hospital. Under the Patient Protection and Affordable Care Act, health information exchange points are being developed to reduce costs and increase the security and transportability of personal health care records. In keeping with federal requirements, policy governing these exchange points will require physicians to have highly secure, third-party (non-government) online credentials for viewing and updating a person’s record. Other staff with less sensitive access will need credentials that are less rigorous. Our institutions could be certified through InCommon to issue these credentials to medical staff, making it easier for staff to go about their work. Alternatively, institutions will have to purchase the credentials from companies such as Symantec or Verizon, putting the burden on the medical researchers and faculty to manage even more electronic credentials.

Higher education is again building a global network, just as we did in the 1980s and 1990s when we worked with partners to develop what eventually became the Internet. This time it’s an identity network designed to address challenges relating to electronic identities, but once again, higher education, through InCommon, is leading the way for other sectors.