# Federated Identity

## Scenario

Gillian is a graduate student in oceanography, working on a large international, collaborative research project consisting of hundreds of researchers from dozens of institutions around the world. Gillian collects and analyzes data sets from laboratories and oceanographic facilities affiliated with other colleges and universities, government agencies, and some private organizations. The project participants provide facilities to support the exchange of data from their underwater instrumentation, as well as specialized applications they have developed. Gillian is both a consumer of and a contributor to those resources.

Enabling this level of collaboration to take place in a manageable way is a federated identity system that includes all of the organizations in the partnership as members. This system enables the project's administrators to grant access to project resources at many different organizations without tracking multiple identifiers for individual participants. It also facilitates collaboration with the project's far-flung participants by giving Gillian a common identifier across this and other projects. The project leverages Gillian's existing federated identity so that she is always identified as the same person across all of the resources.

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 in the collaboration, she logs in using her university credentials—the same credentials she uses to access university email, course management system, and other services—and her home institution confirms to the other organization that her credentials are legitimate. Gillian and the project administrators do not need to create dozens of user accounts and passwords for services at the many organizations. Indeed, the burden on their "guest" access systems is greatly reduced, as many of the users arrive with existing federated identities.

## 1 What is it?

Most organizations use digital identities to manage access to their resources by people associated with the organization. *Digital identity* refers to the information—the set of attributes—pertaining to an individual. Attributes can include identifiers, memberships, eligibilities, roles, and names. The reach of digital identities managed by an organization can be extended to resources operated by other organizations by means of *federation*. Federation is a service provided by a third party that enables participating organizations to leverage home organizations' digital identities to access partner resources by implementing a common standard for technical interoperation. In a federated identity model, a member institution's local identities become federated identities (that is, extended for use across multiple organizations) by using an Identity Provider application. That local identity can then be used across the entire federation to access resources and services. Organizations can choose which digital identities and resources to include in an identity federation. They can also choose which digital identity attributes to use in a federation, as long as those attributes adhere to a common standard published by the federation.

## 2 How does it work?

When a user affiliated with one member of a federation logs in to a protected service operated by another member, the login process includes a step for the user to identify the home organization. The federation technology that protects the service, called a Service Provider, redirects the user's browser to the home organization's Identity Provider, where the user enters the appropriate credentials. The Identity Provider verifies the user's credentials, asserts to the requesting Service Provider that the user has been properly authenticated, and provides attributes about the user. Service Providers and Identity Providers are embedded within a federation-assured trust fabric that provides them with cryptographic proof that a properly authenticated individual at one organization is interacting with the correct and bona fide service at the other organization. Beyond a secure technical infrastructure, trust in an identity federation is rooted in its members' mutually agreed-upon expectations for how home organizations (Identity Providers) and resource providers (Service Providers) manage and protect the identity information shared through federation. Service Providers rely on Identity Providers to maintain

# Federated Identity

the integrity, accuracy, and currency of the association of a digital identity with the person it describes, and Identity Providers rely on Service Providers to use attributes only as appropriate for the service, for no other purpose, and to use reasonable measures to limit their exposure.

## 3 Who's doing it?

Many higher education institutions use federated identity because it makes collaboration easier and fosters seamless access to research and other academic resources. Use of these types of federations is growing, particularly in the research and education (R&E) sector. Most countries operate a federation serving R&E-related organizations in that country (for example, InCommon in the United States), and the trust fabrics of these national R&E federations are integrated to create a global trust fabric called eduGAIN. Among numerous examples, the following indicate the range of activities and academic disciplines that rely on federated identity. The HathiTrust is a partnership of academic and research institutions offering a collection of millions of titles digitized from libraries around the world. The National Institute of Allergy and Infectious Diseases includes thousands of medical researchers and practitioners who collaborate in a global effort to better understand, treat, and eradicate infectious disease. In higher education, the Five College Consortium and its member campuses—Amherst College, Hampshire College, Mount Holyoke College, Smith College, and the University of Massachusetts Amherst—share a library catalog, their campus learning management systems, a universal directory, and an online schedule of classes, as well as the websites for the consortium and the campuses.

## 4 Why is it significant?

Digital systems have become integral parts of the higher education ecosystem, and identity and access management systems are critical components of that ecosystem. By using federation to extend the reach of local identities to community-wide resources, the value of local investment in identity and access management systems is multiplied. This maximizes the return on the identity management investments that most institutions and organizations already make as a matter of course. Federation also helps faculty, students, and staff do their work simply and effectively. Federation for the research and education sector has become a singular, global infrastructure. Thousands of identity providers and thousands of services are part of eduGAIN, and these numbers grow every day. Participation in global federation enables access to these services that is not practical by any other means, freeing resources that can then be used for the benefit of faculty, students, and staff everywhere.

## 5 What are the downsides?

Even though federated identity is growing in popularity, its use has not been adopted fully across all industry sectors, resulting in inefficient access practices. For example, some resource providers need to have a method (such as a separate user name) to allow individuals who are not affiliated with a federated institution to access resources. Inefficiencies can also exist within a federation. Some federated institutions have policies or procedures that impede federated uses of the digital identities of students, staff, and faculty in certain situations. Federation participation may also present a technology barrier for some organizations—most federation technologies currently available must be operated by each organization, requiring them to have someone on staff with enough time and skill to do so.

## 6 Where is it going?

Just as networking has become far more layered and extended over time, so has federation. Low-cost cloud service forms of Identity Providers and Service Providers are becoming available, and the growing integration of global federation with a broad range of commercial and other identity and service providers will deliver increasing value to R&E-related organizations. For example, hybrid identity systems that use external authentication services (e.g., Google) to unlock institutional identity attributes are starting to emerge. And on the resource side, new approaches are being layered on top of federation to enable federated access to specialized scientific instruments and high-performance computing infrastructures.

## 7 What are the implications for higher education?

Identity federations allow faculty, students, and staff at higher education institutions to interact quickly and seamlessly with colleagues, collaborators, services, and resources around the world. In addition to fostering ease of access and collaboration, participation in a federation allows service providers to focus more of their energy on managing and supporting resources rather than maintaining user credentials and access. Federated identity, as a single global infrastructure, is one of the simplest, most user-friendly and cost-effective ways to pursue the academic mission.