Single Sign-On, Multiple Benefits

A Primer on K–12 Federated Identity and Access Management

Single Sign-On, Multiple Benefits

A Primer on K–12 Federated Identity and Access Management

- What is identity and access management?
- What is federated identity and access management?
- How can federated identity and access management benefit K–12 schools?
- What unique challenges do K–12 schools face in managing user identities and access to online resources?

If you're a K–12 chief technology officer or educational technology professional, you might not even be asking these questions, let alone answering them. That's OK. You're in good company. This primer provides answers to these questions and highlights the work of a national K–12 Federated Identity and Access ManagementTask Force, which is focusing on the unique needs of K–12 schools. This task force includes leading organizations and initiatives that promote innovative use of technology in the K–12 and higher education communities:

- Consortium for School Networking (CoSN)
- EDUCAUSE
- InCommon Federation
- Internet2 K20 Initiative
- StateNets

The Growing Challenge of Managing Access to Online Resources

Anyone who uses the Internet has experienced both the wonder of its abundant content and the frustration of trying to get to the right stuff—quickly, and for the purpose at hand.

As the Internet increasingly becomes the repository for resources and the foundation for interaction and collaboration, finding and gaining ready access to appropriate resources is an emerging challenge. The more people rely on online resources, the more unwieldy it is to efficiently and effectively manage the gatekeeping mechanisms—different user names, passwords, e-mail addresses and, for some sites, security questions.

People cope by using idiosyncratic methods to manage their online entrances and access to resources, from the distinctly low-tech approach of littering computer monitors with sticky-note reminders of login information to the more sophisticated solution of password manager software, which stores and organizes an individual's many user names and passwords in one place. Some users resort to the "forgot user ID and password" option on the many sites they visit to reset their passwords and start fresh, with yet another password to manage. In a growing number of colleges and universities, however, students, professors and staff can use a single sign-on to access appropriate online educational resources within their institutions—as well as at external sites. Businesses, too, are setting up enterprise-wide, single sign-on access to enable their employees to be more productive.

In K–12 settings, it would work like this: Suppose a high school teacher wants to access an e-textbook that is licensed for use by educators and students in her school district and is stored in an online repository. She signs on to her school network using her school user name and password, and then visits the e-textbook site, which verifies that she is a teacher at the school and gives her immediate access to the teacher's edition of this resource. Alternatively, if she has not previously signed in to her school network, when she visits the e-textbook site it will redirect her to her school network to login with her school credentials before granting access. If she teaches the course that requires this e-textbook for two semesters, she would have a full year's access to it. Her students access the student edition of the e-textbook in the same way, using the same user names and passwords they use to access all school resources online. They would have access to this e-textbook for the semester in which they are enrolled in her class.

When new teachers join the staff, or new students transfer into the school or the class, they generally would have the same access privileges provided to everyone in their respective roles, unless there are extenuating circumstances requiring an exception. In fact, like every other member of the school community in the same role, they would be able to access a huge cache of resources from many organizations immediately, without waiting for days or weeks for someone to "set up their account." Likewise, anyone who changes their status or leaves the school would have their access privileges changed or revoked immediately, so that only legitimate users can access resources.

This scenario is made possible with a technology solution—federated identity and access management—that yields significant educational, economic, security and administrative benefits.

Starting Points: What Is Identity and Access Management—and What Are Its Benefits?

For many K–12 school districts, the starting point for understanding *federated* identity and access management is identity and access management (IAM) *within* a district.

IAM involves the business processes and supporting infrastructure needed for creating, maintaining and using digital identities to provide people with access to online resources, based on who they are and what roles they are in. An IAM system streamlines this process. For every user, an IAM system can enable a resource holder to answer these questions:

- Are you who you claim to be? (Authentication, asserted by IAM based on the users' login at their home institution)
- What is known about you? (IAM can provide to the resource holder the user's name, organizational role or other defining attributes, as negotiated by prior agreement)
- What are you allowed to access or do? (Authorization determined by the resource holder, based on some combination of attributes provided by IAM)

For example, a classroom teacher can access an online class gradebook, with all of her students' grades, and enter changes to it. Students can access only the portion of the gradebook with their records, in read-only mode, which means they cannot make any changes.

What are the benefits of IAM? According to information adapted for K–12 districts from *Identity and Access Management*, an infosheet from the Internet2 Middleware Initiative, IAM:

Simplifies and secures. IAM ensures that the right people access the right services. In many K–12 districts, this is implemented system by system, with duplicate identity data distributed across multiple systems. In other words, adding another service means adding the identity

infrastructure to go with it. Trying to manage the security issues associated with these duplicate identity stores keeps educational technology professionals' hands full.

The solution is to use the same identity information service for all district applications. By integrating district data about users (from the systems in which they reside) with the services the district uses into an IAM infrastructure, all the policies and procedures can be applied in one place, simplifying management considerably. This

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

The first steps in building an IAM infrastructure are to review the data distributed across the district about people, decide what's relevant from the source systems, and consolidate and update the information into one identity entry for each person in the district. So if "Bob," a student, has entries in the student information system, library system, and school database, the relevant identity data for Bob 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 district administrators can use tools to establish roles, grant access and add group membership as appropriate. 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 a group calendar, e-mail list, wiki space and so on, which individual teachers or administrators can request, and then control who can have access, all without Help Desk intervention. In many K–12 districts, these group memberships are not coordinated across services and have to be altered in each application when members change. Consolidating the groups and privileges allows groups to change once members are in the IAM system and for the change to be accessed by the services in the collaboration package.

Enables shared management. With the consolidation of identity information, the decision makers across the district can effect change much more quickly through interaction with the IAM system. The IAM infrastructure becomes a bridge from the institutional processes and resource owners to the technology operations. It also enables the scaling of information technology (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 authorization-related decisions as well as monitoring for security issues.

What Is Federated Identity and Access Management?

Federated identity and access management amplifies IAM with a sophisticated yet simple infrastructure for managing a person's multiple logons to access local and remote resources. The technology is sophisticated because it uses local credentials throughout the education lifecycles of students and educators, and because it assigns attributes that describe each person's identity or role and enables resource holders to permit them to access specific resources. The technology is simple because it permits a single sign-on, with a single authentication and authorization process.

As the Internet2 *Identity and Access Management i*nfosheet explains: Once the identity data has been enhanced with authority data, it is made available in a number of timely ways to the systems and services that use it. Not only is this applicable for controlling resources managed by a school or district, but the IAM infrastructure also can supply identity data to external service providers, such as external library consortia, course content partners or state departments of education, through the use of federated IAM software.

Federated IAM also streamlines the administration of online resources for authenticated, authorized users. The literal meaning of "federated" is "united in an alliance." This is exactly how federated IAM works. Multiple educational institutions agree to provide a trusted, managed means for accessing and using online resources efficiently in a secure environment. They "federate," or join together, and agree to recognize attributes used by other institutions. Each institution agrees to make its authentication policies publicly available for prospective resource and service providers (SPs) to use to determine whether they are sufficient for their needs. If they are not, the SPs can either refuse access to those users or work with the institution to negotiate a mutually agreeable solution.

Federated IAM provides users with portability and mobility of access to resources beyond their own institutions. For example, a school district might partner with a local community college or library to allow high school students to enroll in college classes or access materials using their school sign-on. Or a student working from home could access licensed resources simply by logging in to the school network to gain access.

How Does Federated Identity and Access Management Work?

- A collection of organizations forms or joins a **federation** and agrees to interoperate, using a common set of rules, particularly in the areas of privacy and security, and to post their authentication policies for prospective partners to evaluate. The federation agrees to use a standard set of attributes for each user, such as username, affiliation and role, as needed by resource providers to make an access control decision.
- One key feature is that **privacy** can be preserved where appropriate. That is, it may be sufficient to simply assert that a requesting user is an enrolled student in a particular class to access a resource, with no other identifying information provided. In other cases, it may be appropriate to release more detailed user information for a user to access sensitive data. There is a broad spectrum of privacy, all of which can be accommodated as needed.
- Federation is implemented using **open standards** such as OASIS SAML (Organization for the Advancement of Structured Information Standards; Security Assertion Markup Language) and OAuth. Both open source implementations (e.g., Shibboleth® software) and vendor implementations of SAML are available; many have tested successfully for **interoperability.**
- Federated identity allows a browser user to **authenticate** at their home organization (HO)—with which they already have a relationship—when accessing remote, licensed and cloud-based applications that provide access only to "authorized users." As part of creating the session with the service provider (SP), the home organization can assert attributes describing the user and the privileges the user has been granted at this SP. In an electronic library scenario, the HO would merely assert that this user is covered by the license; in a scenario involving a collaboration or business partner the HO also likely would assert name and other descriptive information. The SP would typically inspect the asserted attributes to determine whether the user is properly authorized to use the service.
- Federations work with **identity providers** (IdPs), such as educational institutions, which "own" user identities and maintain systems to authenticate users, and **service providers** (SPs), such as technical and content providers, which authorize users and provide access to protected online resources. These service provider partners support the **administration** of resources available for authenticated, authorized users. Essentially, service providers maintain full control of their resources to manage who can use them and how, based on negotiated agreements.

The InCommon Federation® is a U.S. higher education federation that now includes K–12 schools and other educational organizations on a limited basis. Internet2, an advanced networking consortium led by the research and education community, operates InCommon, which uses Shibboleth technology. InCommon serves more than 5 million end users, with more than 200 research and education participants.

> "Federated identity management made so much sense at the philosophical level and at the technical level."
>
> —Lee Cummings, director of technology services, Rockingham County Schools, NC

"Identity management is not very sexy, but it has the potential to enable huge benefits for education."

—Tim Poe, *senior collaborative technologist at MCNC, a member of the North Carolina Federated Trust*

How Can Identity Management Benefit K–12 Schools?

Higher education institutions that implement federated IAM cite a number of economic, administrative and educational benefits. K–12 districts could realize many of these same benefits, including:

- **Cost savings in managing identities and access to online content.** By creating or joining a federation, districts can reduce their administrative costs for setting up and managing multiple user names and passwords—and reduce requests for help when people forget their sign-on information. In addition, schools can achieve more granular control over their resources and, potentially, reduce the licensing fees for resources, by authorizing their distribution to appropriate users only and better tracking which resources are actually being used and by whom. These are particularly attractive benefits, given severe and widespread budget constraints.
- **Improving the effectiveness, efficiency and security of managing and accessing online learning content**. Administrators can integrate new users, services and resource providers faster and easier. Districts can provide greater security—driven by federation policies, standard technology and practices, and strong authorization controls over secure access channels—and secure mechanisms for ensuring privacy. Plus, time-consuming administrative duties, such as responding to calls to retrieve forgotten passwords, are dramatically reduced.
- **Increasing the quantity, quality and variety of educational resources available to support learning.** Districts can more easily and efficiently leverage the educational resources of many organizations, including other K–12 districts, higher education institutions, nonprofits (e.g., libraries, museums, science centers and public television) and commercial enterprises, such as publishers and educational technology companies. Educational resources accessed by means of federated IAM can be web-based, or can be in engaging digital formats, such as video and multimedia, which students enjoy using. And, to replace or supplement outdated print textbooks, schools can provide access to the latest e-textbooks, current information and new findings.
- **Enabling users to share and collaborate**. A federation is more than a mechanism for pulling resources from cyberspace. It also gives students, educators and administrators opportunities to connect, share resources and collaborate within their own organizations and with people in many other organizations—and reduce the friction and obstacles they encounter in the process.
- **Increasing instructional contact and time on task and reducing delays in access to online resources.** Single, secure sign-ons make it easier and faster for educators and students to connect online and to access resources quickly. Single sign-on also supports anytime, anywhere access and mobile learning.

- **Providing instruction with online resources targeted to the needs of specific populations.** Districts can more efficiently extend the depth and breadth of their in-house instructional resources with high-quality resources from other federation members. Educators can more easily track down appropriate resources for their students, and negotiate licenses only for users who will use particular resources, whatever their needs and wherever they are housed.
- **Supporting formative assessment.** Technology-enabled formative assessment lets teachers know immediately how well individual students are learning and helps them adjust their instructional strategies or provide differentiated support to students. Formative assessment also provides valuable, timely feedback to students, so they know what they need to work on.

Federated IAM enables students to sign on easily to a secure, web-based assessment application and take a test or quiz in a secure environment. The performance data can be tracked and analyzed according to state performance standards and expectations. Teachers and students have access to this information and use it to support student learning. Schools can provide parents with single sign-on access to formative assessment results as well, so they can stay abreast of their children's progress and offer support at home.

Using technology-based formative assessments within a federated IAM system improves security and reduces the need for students, teachers and system administrators to manage multiple login and password credentials.

NC Trust

A Statewide Federated Trust Model with a K–20 Vision

North Carolina's leadership in federated IAM, which culminated with the 2009 launch of the North Carolina Federated Trust, began with a vision of providing more efficient and effective access to statewide online resources. North Carolina is notable for bringing K–12 education into this collaboration from the outset.

With the state's broadband capacity and cloud computing services increasing, a task force spent two years exploring and implementing a K–20 federated IAM system to make better use of its technology infrastructure and online resources. The task force included:

K–20 education organizations at every level

- The Department of Public Instruction, which represents North Carolina's 115 school districts
- Higher education systems, which represent 16 public universities, 36 private colleges and universities, and 58 community colleges
- Two pilot K–12 school districts, Davie County Schools and Rockingham County Schools, which ultimately became the first K–12 districts in the nation to join InCommon

Three content and technology service providers

- NC Live, the state's online library service that provides free access to licensed e-books, audio books, videos, images, online magazines, newspapers, journals and more
- MCNC, an independent, non-profit organization that uses advanced networking technologies and systems to improve learning and collaboration in research and education
- Virtual Computing Lab, which provides remote access to high-end computers for researchers and students. While the state's university system had already developed its own, stand-alone federation, the task force decided to build the broader North Carolina Federated Trust on the foundation of the InCommon Federation. The choice mirrors the University of California's federated identification management system, which also uses InCommon as its foundation.

The North Carolina task force opted to use InCommon because of the policy, administrative and technical support provided by this established federation. The task force didn't want to reinvent the wheel, and knew it could benefit from the expertise of InCommon, according to Tim Poe of MCNC, who served as senior collaborative technologist for the initiative. Indeed, federation members faced a number of challenges with its pilot implementation—and in particular, overcoming the technology learning curve.

In response, the federation hosted "ShibFests"—Shibboleth software training workshops—to help technology professionals get up to speed on applications and network configurations.

The task force also faced administrative hurdles of "herculean proportions" in accomplishing "what appears to be a relatively simple task"—securing signed InCommon Participant Agreements from NC Live's collaboration of libraries in the state's university and community college systems and from public libraries serving all 100 counties in the state, as well as from independent colleges and universities.

Still, there is growing interest in the federation, including opportunities to expand licensing for a learning object repository to K–12 schools, integrate learning and content management systems and Google apps, and add museums, zoos and other educational organizations to the federation.

Moreover, future directions will be connected to North Carolina's Race to the Top implementation. In 2010, the state won second-round funding in this federal grant competition. One priority of Race to the Top is building next-generation, comprehensive data systems. Federated IAM could be an important piece of this work.

How Much Does It Cost?

Typically, a federation charges a one-time registration fee and then an annual fee. The fees are relatively modest, especially in relation to the benefits gained.

Two K–12 District Pioneers Glimpse the Potential of Federated IAM

When the chief technology officers in North Carolina's Davie County Schools and Rockingham County schools heard about North Carolina's federated IAM pilot initiative, they understood immediately that this could be a solution to a growing K–12 challenge—managing identities and access to resources.

Lee Cummings, director of technology services at Rockingham County Schools, describes the challenge as "CSV madness," referring to the comma-separated values file format in which the district's 13,500 student and 800 teacher names and associated data are stored in tabular form, which can be exported into a spreadsheet. Every SP with which the district does business requires its own fields of unique user names and passwords—and a new spreadsheet.

"Database management is a burden," he says. "The directory for vendor A does not talk to the directory for vendor B. There are completely different databases to maintain different user IDs and passwords. Everyone has two dozen user IDs and passwords. Different people maintain different databases for different vendors. If it begins to be too much, the product might be abandoned. There's a lot of redundancy, waste, inaccuracy and, perhaps, security risk. Or if the human being who knows the database walks out the door, there's a lapse of institutional memory. We'd have to start from scratch."

For Butch Rooney, director of technology, Davie County Schools, federated IAM seemed to be a logical extension of the Windows Active Directory the district already had in place for every school. "Federated identity works on a personal level. It allows us to serve the student, not the network," he says.

Federated IAM, Cummings adds, "made so much sense at the philosophical level and at the technical level."

Both districts made the transition to federated IAM easily. They credit the technical expertise and ShibFest workshops offered to them by MCNC. Already, the two districts have realized some benefits. In Davie County, immediate and ready access to NC LIVE, NC Wise Owl (a repository of K–12 resources) and N.C. Global Schools Network (an alliance of schools, organizations and businesses committed to innovative approaches to international education) was the most visible benefit, Rooney says.

Rockingham County is leveraging its federated IAM to reduce its database management burden. "It's my belief that really good technology falls silent," Cummings says. "It does what it says it's going to do and you don't care about it. The open source implementation—the SAML-based software concept as implemented by Shibboleth—worked from day one. We literally forgot what server it was on." Now, Rockingham County—a "poor and rural district," in Cummings' words—is pulling vendors along. The district recently put out an RFP for a learning management system and required vendors to support federated IAM system. "We found one that knew what we were talking about," he says.

Both Rooney and Cummings are impatiently awaiting North Carolina's plans for taking federated IAM to scale statewide. In the meantime, both of them are far ahead of their peers in imagining its educational potential. Rooney is a fan of onfizz (**www.onfizz.org**), a video sharing website hosted by the William & Ida Friday Institute for Educational Innovation in North Carolina. The site is free for teachers. "I want students to have their own onfizz library," Rooney says. "It would be like their own YouTube—in a safe, guarded, 'walled garden' environment. When you ask today's students to demonstrate what they know, they want to express themselves digitally."

Both Rooney and Cummings see that federated IAM will support access and safety in using cloud applications and servers and mobile learning. Cummings believes his district will save money on database management and storage servers.

Single Sign-On, Multiple Benefits

page 9

In Colorado

Tying Identity and Access Management to a Statewide Longitudinal Data System

The Colorado Department of Education has implemented a database-driven solution that authenticates authorized education officials to provide single sign-on access to school- and student-level data. The primary software is Oracle's identity management suite of tools.

To administer the access needs of 40,000+ educators in Colorado, the state uses Local Access Managers, or LAMs, a delegated person or persons at each school district who administers local IDs on the state system. The system captures student data from multiple sources, allows for data sharing across multiple agencies to inform policy, and will make data available to parents, students, educators, policymakers and researchers.

What Unique Challenges Do K–12 Schools Face in Federated Identity and Access Management?

There are special considerations for K–12 schools interested in federated IAM. They are not insurmountable, but they do require foresight and strategic planning:

- **Cultivating state, regional and organizational participation.** Very few K–12 school districts have the critical mass, in terms of community members, resources, and identity and content service providers, to realize the full benefits of federated IAM on their own. Economies of scale and depth and breadth of resources require collaborative participation. Securing adequate support, buy-in and participation, therefore, is essential.
- **Administering participation.** Adequate participation comes at a cost—the need for adequate administration to handle the details efficiently. It took North Carolina months to secure signatures of approval from scores of libraries. That state has 115 school districts—what happens with a statewide federation with hundreds of school districts?
- **Developing legal agreements and policies.** The "trust" in a federated trust is established with legal agreements that define roles, responsibilities and policies, particularly related to security and privacy.
- **Meeting compliance requirements.** K–12 school districts must comply with state and federal regulations that protect students' privacy, security and safety, such as the Family Educational Rights and Privacy Act (FERPA), which also applies to higher education, and Children's Internet Protection Act (CIPA).
- **Funding.** K–12 school districts face perennial funding challenges. Once the technical infrastructure is in place, participation in a federation does require modest upfront registration and annual fees. In the long run, however, federation actually could save districts money on managing and administering online access to resources.
- **Technology infrastructure and technical expertise.** A robust technology infrastructure supports federated IAM and, especially, reliable access to online resources that require sufficient bandwidth for multiple users. Technical expertise and training facilitate implementation. While it may be impractical for small school districts to deploy the required infrastructure, larger consortia or state or regional organizations might do this for multiple districts.

National K–12 Identity and Access Management Task Force

This primer is a joint production of CoSN, EDUCAUSE, Internet2 K20 Initiative, InCommon Federation and StateNets. This national task force is exploring the adoption of federated IAM technology beyond higher education and into K–12 schools.

The task force is focusing on answering several key questions:

- Why should school districts care about federated IAM?
- What does a district CTO need to know about the technology?
- What are the key technology challenges?
- How does K–12 involvement in federated IAM impact higher education, service providers and others?

Connecting with Interoperability

Federated IAM is part of a larger K–12 trend toward interoperability—the seamless sharing of data, content and services among systems or applications. A CoSN Technical Committee has produced a primer on this topic, *Interoperability Standards for K–12 Education: Working Together for a Compatible, Affordable IT Future.* The members-only primer is available at www.cosn.org.

Learn More

Additional information about federated IAM, including a PDF of this primer, is available at www.cosn.org/FederatedIdentity

Resources

Consortium for School Networking (CoSN)
www.cosn.org

EDUCAUSE
www.educause.edu

InCommon Federation
www.incommon.org

Internet2 K20 Initiative
www.internet2.edu/k20

StateNets
www.educause.edu/StateNets

References

Federated Identity Management Task Force Recommendations for Federated Identity in the State of North Carolina for 2010 and Beyond (January 2010).
https://edspace.mcnc.org/confluence/download/attachments/16613655/FIM+EOY+Report+-+NCTrust-20100308+-+Final.pdf

Internet2 Middleware Initiative. *Infosheet: Identity and Access Management.*
http://www.internet2.edu/pubs/IAM-infosheet.pdf

EDUCAUSE

InCommon®