CoSN Compendium 2007

CoSN
ADVANCING K-12 TECHNOLOGY LEADERSHIP

Consortium for School Networking (CoSN)
1025 Vermont Avenue NW Suite 1010, Washington, DC 20005
Phone: 202.861.2676 ● Fax: 202.861.0888 ● E-mail: info@cosn.org ● Web: www.cosn.org

Digital Identity Management for K-20 Education

by Shaun Abshere, Ann West and Renee Shuey

Higher education leaders with expertise in this increasingly important field share suggestions, explanations and "lessons learned" with their K-12 colleagues.

Imagine for a moment that your superintendent has hired a consultant to create a "privacy spill prevention" report. Before delivering the consultant's report, the superintendent turns to you and other district leaders and says, "First, let's grade ourselves on how we're doing with identity management. Please take a look at the ten goals on the sheet that is being passed out and assign the district a grade on each one." You read:

1. Policies are in place, district-wide, that address data stewardship and access management.

2. Awareness is high about policies governing network access to services and information.

3. The cabinet is highly committed to our district's Digital Identity Management program.

4. Our district captures information about all people of interest to the district.

5. We have strong district practices that detect, avoid and resolve identity issues.

6. We can comply quickly with changes to legislation and evolving community requirements regarding the use and release of students' electronic identity information.

7. We can quickly determine or change all current access privileges for all users.

8. Our infrastructure supports the secure, legal exchange of identity data within the district, between districts, with our vendors, and with government agencies and post-secondary institutions.

9. We require our IT vendors, service providers and educational partners to support our digital identity standards and policies.

10. We audit and continuously improve our digital identity policies and practices.

If you find yourself giving your district failing grades on any or all of the goals above, you are not alone. Digital Identity Management (IdM) is a complex and rapidly evolving field and many K-12 districts have just begun to focus on it as an area of concern. However, with leadership from the top and a coordinated, district-wide effort to define and respond to the issues, your district can build an infrastructure that provides core IdM functions including:

- Unique digital identities whose attributes are maintained by, and securely released from, a trusted online enterprise directory.

- Secure, easy-to-use authentication process for users built on "Web Single Sign On" with multi-factor confirmation of identity across local and external services.

- Ability to release minimal identity information to licensed service providers for use in making access control decisions and customizing their interfaces and content.

- Authorization to use online resources from both internal and licensed external service providers, with access privileges and licensing compliance managed by institutional criteria.

- Procedures that preserve user privacy and intellectual property rights.

- Means to deliver "individualized" teaching, learning and accountability anytime and anywhere.

Learning from Higher Education

Concerns surrounding security and privacy issues have come to dominate the IT agenda in higher education in recent years. In interviews reported on by Dewey & DeBlois in EDUCAUSE *Review* in May/June 2006, college and university chief information officers (CIOs) ranked "Security and Identity Management" as their second highest priority in 2005 and their highest priority in 2006.

In addressing such concerns, 89 percent of U.S. colleges and universities engaged in IdM efforts or projects during 2006, according to *Identity Management in Higher Education: A Baseline Study* by Ronald Yanosky, which explains the challenge as follows:

> "At one time, institutions relied entirely on face-to-face relationships and familiar documentary credentials to identify people and authorize them to do things. But as colleges and universities have moved more and more of their operations online, they have also created a need for electronic mechanisms to perform these functions. It's not a trivial task. Among the billion people who have access to the Internet, Web-based systems must distinguish between those with legitimate purposes and those with malicious intentions. Even within the campus, good business practice and a growing body of regulations demand that online identity transactions be simple, fast, accurate and secure."

This increasing reliance on technology and data-intensive applications to manage aspects of the education enterprise is not unique to colleges and universities. A growing number of IT experts are calling on K-12 districts to join with higher education leaders to address the IdM challenge in a deliberate, policy-based manner. Chief technology officers in K-12 institutions may find much to learn and adapt from their post-secondary colleagues' experience as we all move education deeper into virtual terrain.

The Drivers for IdM

The drivers that are likely to force broader K-12 involvement in decisions on IdM policies and procedures include:

- **Regulatory Legislation:** In recent years, press coverage of identity theft problems prompted the U.S. Congress and state legislatures to tighten operating requirements for enterprises whose computing systems hold personal information. This growing body of legislation and regulation creates increased audit and compliance requirements for many enterprises (see **www.educause.edu/policy** for an overview of existing and pending legislation). Technologies and business processes related to identity management, credential distribution, authentication, and management of access control policies are now subjects for auditors – and current processes may be inadequate to meet the new audit criteria.

- **Public Pressure:** Press coverage about "privacy spills" increases public awareness and criticism of the risks posed when personal information that an enterprise ostensibly safeguards instead is viewed and retained by the unauthorized. K-20 enterprises are not immune to privacy spills. During 2006, at least 10 US universities reportedly "spilled" identity data, generating significant negative national press coverage and in several cases leading to resignations by the university IT executives responsible for securing the spilled data. In November 2006, for example, personal information on 100,000 students and 1,000 faculty of a South Carolina school district were found on computers sold at an auction. In the K-12 world, where the security of student information is a particularly sensitive issue, a privacy spill could have a disastrous effect on the public's trust.

- **Access for New User Communities:** Many K-12 districts now routinely provide login credentials to "extramural" groups of users, such as concerned citizens, parents, guardians, alumni, contractors, and benefactors. Many such users are not required to receive their credentials in person; often, the district will not know who actually is receiving and using these credentials or when to revoke them. For many applications (eg., viewing an events calendar) weak authentication is not an issue. However, there are other applications – such as online fee payments, access to student grades or IEPs, software maintenance by a consultant, or online surveys directed to particular groups – where strong or multi-factor authentication is a requirement that a district must address.

- **Scalable Services and User Experience:** K-20 institutions are gradually moving many learning and business services for students, teachers and other staff to an electronic self-service model. The model for user interaction now is online access, twenty-four hours a day, from any compatible networked device, instead of face-to-face only during school hours. How will a CTO manage access to this growing number of separate applications in a secure, reliable fashion? How will users manage – and securely remember – all the credentials needed?

The Benefits of IdM

When asked as part of the Yanosky baseline study about the benefits they expected to reap from a strategic commitment to develop IdM infrastructure, college-level CIOs indicated a variety of benefits ranging from the ability to track unauthorized activity to rapid deprovisioning or enablement of accounts as people leave or join the institution. (See "The Benefits Ranked" below.) While the largest group (81 percent) of higher education CIOs said that the concerns about security and privacy were driving their interest in IdM, a full 61 percent said they were also motivated by a desire to improve user services and satisfaction – for example, by reducing the number of accounts and passwords users must remember, provisioning accounts faster or improving self-service.

The following vignette describes the user experience in a hypothetical K-12 district that has addressed the need for IdM infrastructure:

"Time for homework," thinks Molly as she logs on to the district network with her username and password and draws her right index finger smoothly across the computer's swipe-scanner to confirm her identity to the portal. She views and sorts her personalized list of assignments, then clicks on an item at the top of the list, passing into the district's personalized learning management system where a history study session is already under way.

As the session winds down, Molly receives an instant message from Erik asking if she wants to study chemistry with him. They agree to try out the new chemistry courseware their district has invested in but Molly suggests that they first watch a recommended video on predicting chemical reactions from acid/base strength measurements. "Makes sense" replies Erik, and they each click on the link that takes them to the online digital media collection the district licenses through the state education network.

Their viewing done, the two return to their chemistry assignments list, select an exercise on acid and base and are passed into the National Science Digital Library portal and then on to the American Chemical Society's portal for chemical education. Practicing with the course-specific digi-demo and chatting to test each other's understanding, the two classmates prepare for the exam that they'll take online at the end of the week.

Erik signs off and Molly goes to check on her math assignment. Her teacher has posted the corrected math tests, along with grades for the quarter, and Molly is pleased to see that she did well at both. "I'll be emailing your parents to invite them to check out the grades as well," the teacher writes, "and I've submitted them to the front office."

Before beginning on tonight's math homework, Molly remembers that she had promised to reserve a room for next month's district-wide meeting for all the foreign language club presidents. She opens and passes into the facility-reservation service, where she selects an available room on a nearby campus and posts the meeting invitation to the online calendars of her fellow student presidents.

The Benefits Ranked

Asked to rank the importance to their institutions of 14 specific benefits of IdM, higher education CIOs replied:

High Importance

1. Track unauthorized activity
2. Immediate deprovisioning on user departure
3. Appropriate ID proofing confidence
4. Single sign-on
5. Single affiliations source
6. Self service

Medium Importance

7. Immediate new-user enablement
8. Scalable authentication and authorization
9. Immediate role change
10. User access to off-campus resources
11. Strong authentication
12. Appropriate guest access

Low Importance

13. Non-institutional user access to our resources
14. Decentralize account management

Source: *Identity Management in Higher Education: A Baseline Study*. Yanosky, Ronald. EDUCAUSE Center for Applied Research.

During the course of one evening, Molly benefits from a variety of compelling learning and support services, provided by trusted service providers, all of whom recognize her identity from her initial log-in. In accessing these resources, Molly, Erik, her teachers and her parents are using many of the core security, privacy and access functions that the district's digital identity management infrastructure can provide.

Building the Foundation

As K-12 technology leaders examine the inventory of technologies available for IdM, what does the current state-of-the-practice in K-20 reveal? The IdM references cited at the end of this article provide an overview of the wide range of digital identity management technologies that are fully or partially operational in higher education today.

To reap the benefits of IdM, however, a K-20 institution and its top technology leaders must overcome resource, organizational and technical challenges. When asked, as part of the Yanosky study, to name their top challenges to pursuing IdM, higher education CIOs replied in the following proportions:

54%: Other IT projects had higher priority

39%: Inadequate funding

30%: Difficulty developing campus policies and procedures

Noting a clear "capability gap" – in which the capability to deliver was rated lower than the importance of IdM to the institutions involved in the study – Yanosky suggests: "While critical to the success of an IdM initiative, documentation, policy and planning activities can be the most difficult parts of such an effort. ... The success of the ambitious IdM initiatives many respondents described may depend on the completion of these preparatory endeavors."

An infrastructure rests on its foundation. The fundamental insight that K-12 CTOs should take from their colleagues' experiences is: build a strong policy foundation for IdM.

The first step to accomplishing this involves developing a high-level plan that identifies functions, process, policies, and technologies needed to address your specific drivers. To orient your efforts, consider and discuss the illustration on the page that follows of a district's "ideal" IdM environment.

A plan in hand allows you to address the identified gaps as the opportunity arises, such as coupling a new "web single sign-on" service with an upgraded portal or establishing a higher level of assurance for higher-risk applications when implementing a new finance system.

For example, to develop a plan that puts the authentication challenges front and center, follow these steps:

1. Define your challenge for change, including drivers to help determine where you need to go.

2. Understand your district's service requirements and accompanying framework to manage authentication.

3. Develop a set of principles to guide decision-making.

4. Inventory how your district operates today.

5. Analyze your target online services, who is using them, what the risk issues are, and develop a list of technical architecture, business process, and policy gaps that need to be addressed to achieve 1 and 2 above.

Implementing Change

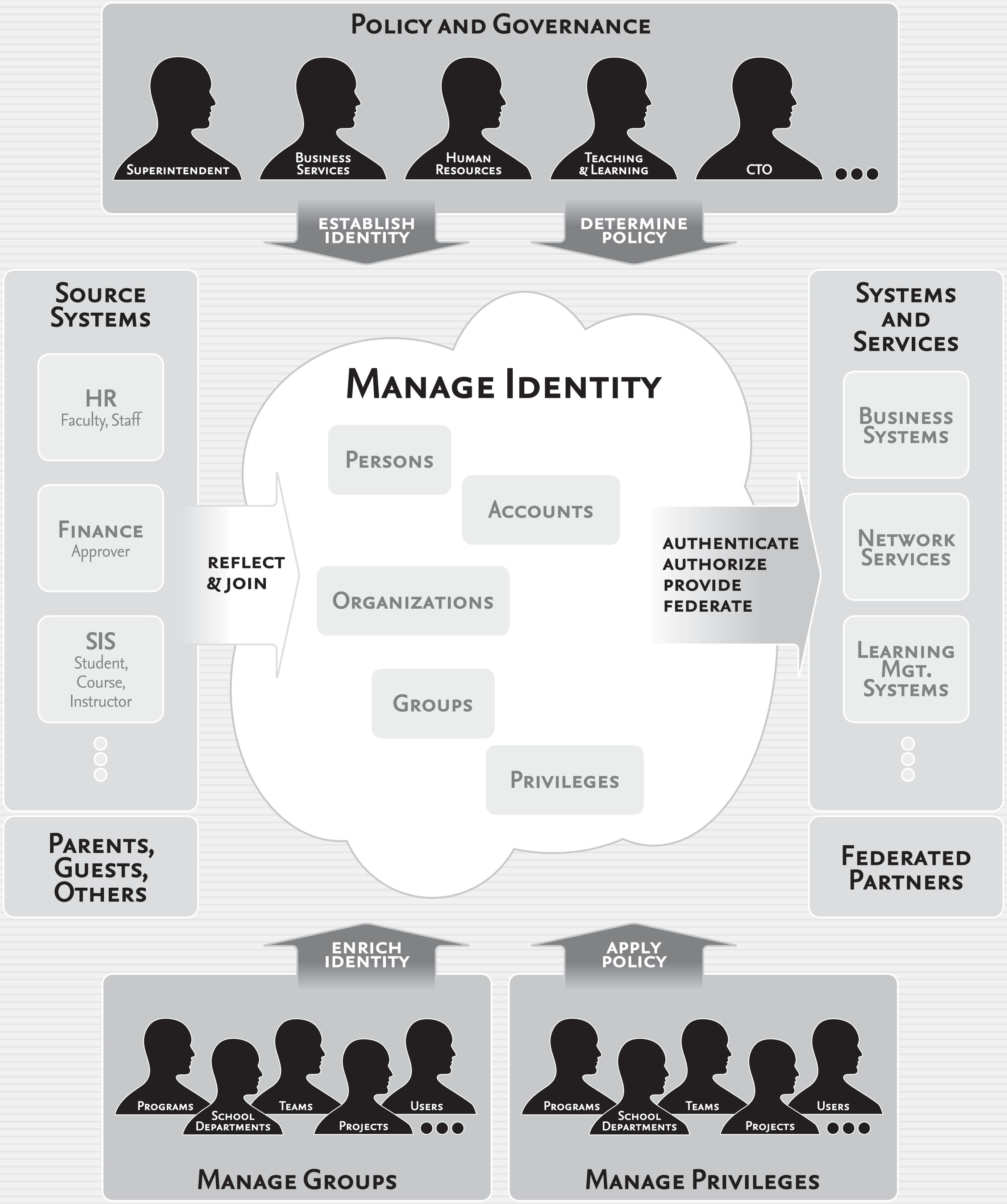
As your district begins implementing a new approach to digital identity management, it is important to work concurrently with constituencies across the district to ensure your *policy*, *business process*, and *technologies* are all "in synch."

Policy

Any district-wide approach to authentication services and identity management must include policies and processes consistent with the district's needs and community values. You should use your IT governance structure to develop the policy framework for the IdM project and incorporate it into your overall identity management and security policy framework. Policy states the "what" or "why"; it articulates the long-term institutional position, identifies mandates, scope, roles and responsibilities and requires a shared vision of the legal and regulatory landscape, business drivers of the institution, and the values and ethics of the institution. For example, authentication policy should address the following:

- **Identification:** What requirements will the district impose to ensure sufficient proof that the person is who they say they are? What credentials are required to confirm their employment, student status, or other affiliation

Digital Identity Management at a Glance



Source: Based on an illustration provided by Lynn McRae, Stanford University.

relationship to the institution? If identity data is derived from existing directory or user account databases, how will legacy information be verified?

- **Electronic Credentials:** What rules determine the form of the credential? How will the district identify the requirements or standards affecting this form? How will legacy architectures make use of the electronic credential? What encryption standard will we require? What is the anticipated lifecycle of our electronic credentials? Can they be changed, retired or reused?

- **Registration:** How do we obtain information about the individual? How are affiliates, such as parents, job applicants, alumni, and contractors added? What relationships or dependencies are required for our enterprise directory? Are appropriate protections in place to ensure the privacy of information about individuals? How will we link an electronic credential to information about the individual? In our vignette above, for example, Molly and Erik's school district licenses access to digital resources and has the responsibility to ensure that the individuals using these resources are authorized. The critical prerequisite step is to make sure the "physical" student or other authorized end-user is linked to the right electronic credential to ensure license compliance.

- **Service providers:** What requirements will we impose on service providers to ensure the privacy of identity information, whether on our premises or offsite? For example, in our earlier vignette, how long should the National Digital Science Library or the American Chemical Society retain the students' identity information sent originally to make a just-in-time authorization decision? Can these service providers use that data for another purpose? And who actually retains the data when one service provider acts as a proxy for another as in our example? What standards will we require to ensure protection of the credential during transmission? Will we need to support multi-factor authentication for some services that require higher security?

Business Processes

Key to business process change is the education of all the affected parties and an on-going review channel for reporting issues and problems with the new procedures. Continuing with the authentication example: educating managers and policy makers about the basics of authentication technology and implementation decision points ensures that a variety of viewpoints and sufficient data inform the decisions about authentication.

Below is a selection of the business processes that you should address:

- **Identification and Registration:** On- and off-campus identity vetting and other processes that may have to be considered if parts of the population cannot comply with vetting policies, such as exception procedures for dealing with constituencies who need access but fall outside the identified local populations (e.g., "guests" or remote users).

- **Electronic Credentials:** Creation of self-service or other password change mechanisms; password-reset exception processes; and procedures involving password sharing or compromise.

- **Account Management:** Status and affiliation change-management; Provisioning and de-provisioning accounts; how and when these are done

- **Support:** Help desk and related support personnel's responsibilities.

- **Security and Compliance:** Auditing and process debugging; security monitoring and compliance.

- **Staff Training:** Educating staff about new or changed processes and responsibilities.

- **Risk Assessment:** Evaluating the vulnerabilities, likelihood of damage, and cost to recover associated with data, transactions, and processes.

Technology

A critical goal when planning your IdM infrastructure is to ensure that it meets the agreed business and policy requirements. If unacceptable gaps exist, the district's technology leaders must work with their policy and process colleagues to achieve consensus on how to close the gaps.

Once you have identified existing constraints and mapped business requirements to technology requirements, you are ready to decide on your protocols and determine which products to support. Because institutional goals, drivers, skill sets, and resources vary widely across the K-20 community, there is no one technology that addresses all needs of all institutions.

As you decide, examine your choices in the light shed by the reported goals and experiences of higher education.

One recommendation is to consider open standards and architectures such as those being explored by the National Science Foundation's Middleware Initiative and its Enterprise and Desktop Integration Technologies Consortium (see resource directory at the end of this monograph). As Yanosky puts it, "It's hard to think of an area of IT that could benefit more from open standards and architectures than IdM. Though IdM standards remain immature, a solid core exists. Institutions that make the maximum possible use of standards and flexible architectures will be in the best position to exploit a maturing product marketplace and respond to emerging IdM demands."

Migrating to Production

To migrate the new infrastructure to production, pick a staging strategy. For example, you might begin by selecting relatively low-risk services for initial integration in order to test the functionality and the scalability of the new infrastructure. Consider integrating one or two district systems that are overseen by managers who are willing partners in piloting the new infrastructure. Here is one sequence of steps a district might follow:

- **Develop phased migration strategies** for moving from the existing infrastructure to the new one. This includes updating or creating the data feeds, implementing code changes, linking in the applications, and deciding the phases of the migration. Schedule the process of "going live" carefully, accounting for time-of-year or other anticipated factors affecting demand on the systems and staff resources. Remember to develop contingency plans for backing out of the new system if things prove problematic.

- **Start working through your communications and education plan**. Hold get-ready meetings with project members (including stakeholders, help desk staff, and so on) as developed by the business process team above. Be sure you discuss expectations with those involved in the project,

Digital Identity Management Glossary

Here are some terms that are relevant to IdM. See also the Johns Hopkins University Enterprise Services Glossary (**nts.jhmi.edu/es/glossary.cfm**)

Authentication is the process of validating the credentials presented in a particular security context. Proper authentication requires that the identification and registration processes that precede it are not compromised. Authentication should not imply access to resources, which is done with the Authorization step.

Authorization is the process of controlling, based on business rules, an individual's access to resources.

Credential is an object that is verified when presented to the verifier in an authentication transaction. Examples include user id and password pairs and digital certificates.

Identification is the process by which information about a person is gathered and used to provide some level of assurance that the person is who they claim to be. Generally, this identity verification takes place within the office (e.g. Human Resources or Student Services) that first encounters the individual and creates their record within the institutional system(s) of record. The next step is Registration (see below).

Identity Management is an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control their users' access to online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access, rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.

Identity Vetting is the process used to establish the identity of the individual to whom the credential was issued This is typically done at the Registration stage.

Multi-factor Authentication requires the use of two or more approaches from something you know, have, or are. Examples include using a password to unlock a digital certificate store. Typically, multi-factor authentication is associated with a more rigorous vetting process, providing a higher LoA, and therefore a higher security level for more sensitive services or systems.

Registration (also known as credentialing) is the process whereby users are given electronic credentials, leveraging the identification process above to ensure that they are coupled with the correct electronic identity information. For example, many institutions use a web-based mechanism to reset an initial password and establish a permanent one, ensuring a correct mapping by requiring the user to enter additional information validated against that which is contained in their record. It is important for institutions to establish rules that govern the processes used by the department or office that assigns and distributes credentials.

Single Sign-on Authentication, or SSO, allows users to login once and gain access to multiple applications for a defined time period without having to re-login each time: subsequent authentication takes place without further user interaction or interruption.

as well as critical district players, to avoid over-promising.

- **Migrate systems and users**

- **Institutionalize governance**. The district's authentication requirements will evolve as new end-user groups are identified, new compliance requirements are defined, and new technologies and services become available. Decide how best to migrate the project governance team to an on-going function. The creation of such a forum is critical: to preserve the commitment and risk-tolerance of your district, you must bring new issues to the attention of stakeholders.

In K-12 education, CTOs and other technology leaders have helped their enterprises move information and learning technology from the periphery to the core of their missions. Adapting and integrating a digital identity infrastructure into K-12 is but the next step and one with ample precedent – and colleagues – elsewhere in education.

This publication is one of six monographs that make up the 2007 CoSN Compendium, a collection of resources for members of the Consortium for School Networking (**www.cosn.org**), a national non-profit organization that promotes the use of information technologies in K-12 education to improve learning. Additional copies can be ordered onlne at **www.cosn.org/resources/compendium**.

Authors:

Shaun Abshere, Associate Director, WiscNet

Renee Shuey, Pennsylvania State University

Ann West, NMI-EDIT Outreach Lead for EDUCAUSE/Internet2, Michigan Tech

Additional Contributors:

The authors thank the following organizations and authors for their gracious permission to use their work:

Ronald Yanosky & **Richard Katz**, Educause Center for Applied Research

Steven Carmody, Brown University.

Lynn McRae, Stanford University.

NMI-EDIT Consortium of Internet2 and EDUCAUSE. Parts of this article are based on their work supported by the National Science Foundation Grant No. OCI-0330626.

Digital Identity Management for K-20 Education was edited by Judy Salpeter and produced by CoSN with art direction by Chris Leonard.

Sponsors

Thank you to the following companies for their support of the 2007 CoSN Compendium:

Platinum sponsors
- Dell
- IBM
- SAS inSchool

Gold Sponsors
- Apple
- Pearson Education

Silver Sponsors
- Gateway
- HP
- Mitel
- SchoolNet
- Texas Instruments
- Toshiba

IdM References

Publications referenced in this article:

McRae, Lynn. (2006) *Self-assessment Questionnaire: Building a Distributed Access Management Infrastructure*. NMI-EDIT.

Identity and Access Management Resources (2006). National Science Foundation Middleware Initiative - Enterprise and Desktop Integration Technologies Consortium (NMI-EDIT).

Dewey, Barbara I., DeBlois, Peter B., and 2006 EDUCAUSE Current Issues Committee. (2006) *Top-Ten IT Issues, 2006*. EDUCAUSE Review, vol. 41, no. 3 (May/June 2006): 58–79.

Yanosky, Ronald (with Salaway, Gail) (2006). *Identity Management in Higher Education: A Baseline Study*. (Key Findings). Boulder, CO: EDUCAUSE Center for Applied Research.

E-Authentication Password Credential Assessment Profile (Release 2.0.0). (2005). Washington, D.C.: Federal CIO Council. Available from www.cio.gov/eauthentication

Shuey, Renee and West, Ann. (2006) *Building a Balanced Identity Management Infrastructure*. EDUCAUSE Review, vol. 41, no. 5 (September/October 2006).

Carmody, Steven and West, Ann (editors). (2006). *The Need for Change – An excerpt from the Enterprise Authentication Implementation Roadmap*. NMI-EDIT.

To locate these and other relevant resources online, visit:

The NMI-EDIT Consortium Site
www.nmi-edit.org

EDUCAUSE Home Page
www.educause.edu

EDUCAUSE/Net@EDU Identity Management Working Group Site
www.educause.edu/idm

Internet2 Middleware Initiative Home Page
middleware.internet2.edu

Thank you to the following companies for their support of the 2007 CoSN Compendium:

Platinum sponsors

DELL

IBM®

SAS inSchool®

Gold sponsors

PEARSON
Education

Silver sponsors

Gateway®

hp®
invent

MITEL®

SAFARI
MONTAGE™
LIBRARY VIDEO COMPANY.

schoolnet®
The School Performance Network℠

TEXAS INSTRUMENTS

TOSHIBA
Leading Innovation >>>

Wimba
people teach people

CoSN
ADVANCING K-12
TECHNOLOGY
LEADERSHIP

Consortium for School Networking (CoSN)
1025 Vermont Avenue NW Suite 1010, Washington, DC 20005
Phone: 202.861.2676 ● Fax: 202.861.0888 ● E-mail: info@cosn.org ● Web: www.cosn.org