EDUCAUSE | CENTER FOR APPLIED RESEARCH

From Homegrown to the Cloud: Identity Management Evolution at Coppin State University

Judith A. Pirani, ECAR
Susan Foster, ECAR

ECAR Case Study 1, 2011

4772 Walnut Street, Suite 206 • Boulder, Colorado 80301 • educause.edu/ecar

EDUCAUSE

4772 Walnut Street, Suite 206
Boulder, Colorado 80301
educause.edu/ecar

From Homegrown to the Cloud: Identity Management Evolution at Coppin State University

EDUCAUSE
CENTER FOR APPLIED RESEARCH

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

From Homegrown to the Cloud: Identity Management Evolution at Coppin State University

Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes:

- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices;
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities;
- roadmaps—designed to help senior executives quickly grasp the core of important technology issues; and
- key findings—brief high-level summaries on the scope of an ECAR research study.

This case study accompanies the primary ECAR study *Identity Management in Higher Education, 2011*,[1] by Mark C. Sheehan et al. In addition to updating the picture of identity management (IdM) practice reported in a baseline ECAR study conducted in 2005–2006,[2] the 2011 study takes a deep look at institutional adoption of federated identity technology.

ECAR researchers conducted this in-depth case study to complement the core study. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings. We undertook this case study of Coppin State University to study its software-as-a-service identity management solution and its impact on the IT organization and relevant administrative departments. ECAR owes a debt of gratitude to the Coppin State University staff for their time and insights. Special thanks go to Habtu Braha, Dean, School of Management Science and Economics; Rene Brown, Computer Lab Manager; Prasad Doddana, Director, Information Systems; Ahmed El-Haggan, Vice President for Information Technology and CIO; Carol Miller, Technical Support Manager and Senior Database Administrator; Cindy Prevatte,

Human Resource Information Systems Manager; Robert Reddish, Network Administrator; Richard Siemer, Vice President, Administration and Finance; Thomas Smith, Director, Campus Network Services; Lisa Thuman, Senior Technical Analyst/Junior Data Base Administrator; and Margaret Turner, Registrar.

ECAR also wishes to thank the following for their insights about outsourcing IdM services: Joel Cooper, Director, Information Technology Services, Carleton College; Rodney Petersen, Senior Government Relations Officer and Managing Director of the Washington Office, EDUCAUSE; Donald Z. Spicer, Associate Vice Chancellor for IT and CIO, University System of Maryland; and Jack Suess, Vice President of Information Technology and CIO, University of Maryland, Baltimore County.

Introduction

In today's dangerous online environment of hacking, identity theft, and other cybercrimes, an institution's protection of its constituents' personal information and online resources remains a top priority. Effective identity management—the deployment of policies, procedures, processes, and technologies to establish and protect user identities and enforce rules about access to digital resources[3]—is an imperative and comprehensive endeavor. Institutions collect identity information about their constituents that their IT organizations store and manage in an identity database. Credentials are then created—typically username and password—so that individuals can access institutional online resources. For example, a new student presents proof of her identity before the college registrar issues her an identity (ID) card and credentials for access to certain institutional online systems. These credentials allow the student to make appropriate use of institutional IT systems.[4] Implementation of these complex systems involves considerable technical expertise as well as the intimate involvement of institutional entities—e.g., central IT, the human resources department, and the registrar—that manage personal information to create the identity information repository, the rules that guide resource access, and the processes that tie it all together. Implementation begets the daily maintenance tasks such as password resets, personal information updates, and system upgrades to ensure the correctness of personal information and the alignment of processes essential to an IdM system's smooth operation. Some institutions have begun to expand their IdM system's reach by streamlining access to the interinstitutional resources to facilitate collaborative and cross-institutional research; instruction and extramural administrative activities further add to the institution's IdM complexity and workload.

Such a system can tax the largest of institutions, but the impact can be even more profound for a small college or university with fewer than 4,000 full-time equivalent (FTE) students, where IT staffing tends to be smaller.[5] Under today's intense budget pressures, IT leaders at small institutions can't necessarily reallocate highly technical staff—something that already may be in short supply within their organization—to take on a comprehensive IdM project. ECAR's 2011 study on IdM practices in higher education shows clearly that, overall, smaller schools devote fewer resources to IdM

projects.[6] The investment of a robust IdM system can be a financial stretch as well, costing tens or hundreds of thousands of dollars, further straining tight IT budgets. ECAR's 2011 study notes that smaller institutions in general plan to spend significantly less on new IdM projects than their larger counterparts.[7]

Options exist to help small institutions build their IdM systems. Some may receive help if they belong to a university system or consortium; the University System of Maryland's larger institutional members created "cookbooks" to help their smaller counterparts build their underlying IdM infrastructures. Or instead of building an entire IdM system from scratch, a central IT organization may opt to integrate an IdM appliance with preconfigured software into the institution's IT infrastructure, or independent consultants can augment internal staff efforts to set up an IdM architecture. But these options do little to meet postimplementation maintenance requirements, which, if only because of constant turnover in student populations, can be considerable.

Another alternative is a software-as-a-service (SaaS) IdM solution. In this configuration, an external vendor provides IdM services over the Internet so that the central IT organization doesn't have to host and operate it on campus. This enables a smaller central IT organization to mitigate equipment and software costs for an entire IdM system, to purchase IdM capabilities as needed, and to offload some of the ongoing IdM system maintenance onto the SaaS IdM provider. Some obvious concerns immediately come to mind—for example, the security of personal information and network reliability. But as this case study will show, adequate planning can address these issues.

Coppin State University is a small institution with fewer than 4,000 FTE and a relatively small IT shop of 36 people. After supporting internally hosted IdM solutions for seven years, Coppin's IT Division had an opportunity to convert to a SaaS IdM solution in 2010. Rather than outsource its entire IdM implementation, now the IT Division offloads manual and time-consuming IdM functions—e.g., password reset and account provisioning—to the SaaS IdM provider. In this configuration, Coppin constituents' personal identity information is still maintained on campus, but when an individual requests access to campus IT resources or services, selected personal data—user ID, zip code, birth date, and campus ID number—are encrypted and transmitted over a secure Internet connection to the SaaS IdM provider. It is just enough personal information to complete the SaaS-based transactions without directly identifying the person.

Outsourcing these two functions has reaped significant benefits for Coppin. It accelerated the processing time for account provisioning and password reset from hours and days to just minutes. The IT Division estimates that delegating the actual password and provision processing as well as the backend server management, data backup and storage, and ongoing monitoring to the SaaS provider freed up approximately 1.5 FTE IT staff to pursue other strategic IT activities. "This solution is a good compromise for a smaller IT shop that may not have the expertise or resources to tackle IdM activities," stated Thomas Smith, director, campus network services support. "It is a win-win because it offloads IdM's manual and tedious practices, yet you still control the 'goods.'"

Some may consider Coppin's SaaS (or "cloud") IdM solution a novelty now, but a June 2010 article in *NetworkWorld* predicts more widespread use in the future:

> Cloud-based computing is a reality. Platform-as-a-service, application-as-a-service and, yes, identity-as-a-service will soon be as pervasive as client-server computing became in the last century. This will mean fundamental changes in the ways we think about identity and security. Get on that train, or be left at the station.[8]

This case study offers an introductory, not highly technical look at a SaaS IdM solution. It traces Coppin's evolution from manual processing of IdM functions to its current SaaS configuration, highlighting the SaaS IdM solution's technical operation, impact on relevant business processes, and future role in Coppin's IdM strategy.

Background

One of the historically black colleges and universities (HBCUs), Coppin State University was founded in 1900 in Baltimore, Maryland, as what was then called a Colored High School, a one-year training course for African American elementary school teachers. By 1902, the training program was expanded to a two-year Normal Department within the high school, and seven years later it was separated from the high school and given its own principal.

In 1926 the school was renamed the Fanny Jackson Coppin Normal School in honor of the outstanding African American education pioneer. Over the years, the school expanded to a four-year curriculum, was eventually renamed Coppin State College in 1967, joined the University System of Maryland in 1988, and became a university in 2004. Today Coppin State University offers 53 baccalaureate majors and nine graduate-degree programs, with 600 faculty and staff members serving a student population of nearly 4,000 students.

For over a decade, Ahmed El-Haggan, vice president for information technology and CIO, has led Coppin's Information Technology Division. The VP of IT reports directly to the university president. IT is a highly centralized function at Coppin, with the IT Division managing the university's network connectivity, Internet and intranet infrastructure, telecommunications, client computing support services, PC and computing labs operations, instructional technology, IT training, auxiliary systems IT support, web and multimedia development, digital AV systems, IT Students Help Desk and Support Center, and all academic and administrative computing needs. Staffing is lean—fewer than 40 staff members—and highly innovative. To stretch its resources, Coppin's IT Division frequently partners with vendors to develop leading-edge IT technology and applications for the higher education environment in exchange for free or highly discounted services and equipment. Over the years, the IT Division has collected numerous accolades, including the EDUCAUSE 2005 Award for Innovation in Network Technology. *The Daily Record* named El-Haggan one of Maryland's Innovators of the Year in 2010.

Because Coppin operates under the jurisdiction of the State of Maryland, the university's IdM practices must follow the state's Department of Information Technology's

Information Technology Security Policy and Standards guidelines, enacted in 2004. For example, all users who access online information must be uniquely identified; passwords must follow prescribed construction practices, be changed at regular intervals, and differ from the previously used 10 passwords; and authorization processes must be documented and users' access privileges verified annually.[9]

At Coppin, this translates into the expiration of each user's password every 120 days. Users receive a notification to change their password 14 days before it expires, upon logging on to their Coppin e-mail account or any campus computer. Passwords require eight or more characters, at least one lowercase letter, at least one uppercase letter, and at least one number. To conform to the University System of Maryland's policy, Coppin's system authentication policy requires any IdM solution to log users' previous 10 passwords. The commencement of a new semester typically brings a spike in IdM-related activity, as the university provisions and verifies access privileges as required for new or returning students and faculty to comply with state guidelines.

IdM Evolution

This section traces Coppin's IdM activities from 2003 to the present. During that period, IdM evolved dramatically at the university, from homegrown/manual practices, to internally hosted vendor solutions, to today's cloud-based, vendor-supported software-as-a-service IdM solution.

From Homegrown to Hosted IdM Solutions

Initially, Coppin's IdM strategy was straightforward. Its homegrown enterprise resource planning (ERP) system ran few online services. Student accounts were needed mainly to provide access to computers in the student lab. The IT Division created all student network accounts en masse each semester during a weeklong process for access to e-mail and other institutional services such as shared drives and the intranet, and the student computer lab manager distributed those accounts to students. The IT Division processed administrative accounts manually.

Over time, Coppin's technology environment evolved. The IT Division implemented Microsoft's Active Directory to enhance network management of user identities and resources. It replaced its homegrown ERP solution with PeopleSoft Human Resource (HR) and Campus Solution student administration system (SAS) implementations in 2003 and 2004, respectively. This enhanced the collection and storage of personal information, but more important, the new ERPs migrated Coppin's administrative services to an online environment. Now students, faculty, and staff required access to these online resources. A robust IdM strategy became imperative. "The move to PeopleSoft's web environment created a new set of IdM challenges," recalled El-Haggan. "How will people reset their passwords? How will we know who they are? We were very concerned about the staffing requirements to provision accounts in a timely fashion. That is why we were interested early on in managing identity and provisioning accounts automatically."

So the IT Division purchased an internally hosted IdM solution in 2003 to provision accounts. They introduced online self-service password management for students to be used only at an on-campus computer kiosk physically located outside the student computer lab, thereby offloading the 10–15 daily password reset requests from students. The IdM situation improved, but issues remained. The IT Division still created administrative accounts manually, and the hosted IdM vendor solution proved to be a suboptimal fit for Coppin's IT environment. The hosted solution, built with several vendor-licensed products, required considerable time for IT Division's staff to customize and integrate it into the university's central IT environment, straining its limited staff resources. Then the hosted solution's new ownership changed the relationship dynamics between school and vendor, and the IT Division chose to explore other IdM alternatives in 2004.

This exploration led the Coppin IT Division to Fischer International, a company that specializes in IdM solutions. Fischer wanted to enter the higher education market, and Coppin's IT Division agreed to work with the vendor on a significantly discounted implementation to adapt Fischer's Identity Suite solution for the higher education market. In addition to cost savings, two other factors influenced the decision. First, El-Haggan and the IT Division liked the product's single-vendor nature. Identity Suite is based on Fischer's Global Identity Architecture, an internally developed IdM platform based on industry standards, including Service Provisioning Markup Language (SPML), web services, Lightweight Directory Access Protocol (LDAP), Java Database Connectivity (JDBC), and Extensible Markup Language (XML).[10]

Second, the Identity Suite's modular configuration enabled Coppin's small IT shop to implement the solution in stages. The IT Division started in 2005 with identity management, as well as an online, self-service password reset utility, accessed through Coppin's EagleLINKS online self-service portal, where users could manage their passwords; it implemented a password management system to authenticate users via the answers to three personal questions. Automated provisioning went live in 2006 to process user access to Coppin's online resources for students, faculty, and staff. Over the years, Coppin and Fischer developed a productive relationship.

From Campus to Cloud

Further changes to Coppin's IdM solution were made in 2008. PeopleSoft's upgrade of Campus Solutions to version 9.0, announced in 2006, was significant, offering new features and processes, and significant data structure migration requirements from earlier versions. Oracle, which had completed its acquisition of PeopleSoft in 2005, planned to discontinue support for version 8 beginning in 2009. Correspondingly, version 9.0 required Fischer to modify its Identity Suite solution's interface with PeopleSoft Campus Solutions. Thus, Coppin completed extensive modifications to its PeopleSoft and Fischer implementations in fall 2008.

In fall 2009, Fischer approached the IT Division with a new proposal: to convert from an internally hosted IdM solution to one using SaaS. In the new scenario, Fischer would provide similar services—e.g., password management (including reset and synchroniza-

tion) and account provisioning—remotely over the Internet instead of through an on-site server-based implementation. Coppin would work with Fischer to develop a solution for the higher education market at no additional cost to the institution.

El-Haggan and his team were intrigued, but they were hesitant because there were so many unknowns. "We were comfortable with the solution that worked on campus," recalled El-Haggan. "But putting it in the cloud—that is another story." An obvious advantage was that a SaaS solution would reduce the IT Division's IdM maintenance commitment, as the vendor assumed more of this responsibility, potentially freeing up IT Division resources.

El-Haggan and his team raised several of their concerns with Fischer, and both parties worked to resolve them. The following sections detail the issues and subsequent actions. To illustrate their actions, Table 1 maps the IT Division's actions to the SaaS IdM evaluation recommendations presented in the Burton Group report *2010 Identity and Privacy Strategies Planning Guide: A Market in Transformation*.

Table 1. SaaS IdM Solution Evaluation Checklist

Burton Group SaaS IdM Evaluation Item	Coppin State University IT Division's Action
Consider the service provider's ability to support your organization's IdM information and workflow needs as well as its ability to adjust your costs to your consumption of services.	A proof of concept tested the solution's integration with Coppin's systems; automation of services reduced staffing costs to maintain IdM solution.
Evaluate the service provider's ability to meet your identity assurance requirements.	Consulted the Office of the Maryland Attorney General for state compliance; an outside consultant evaluated the vendor's solution; Coppin senior administration reviewed and approved Fischer's proposal.
Consider the service provider's ability to add new functionality quickly when required and to scale the solution to meet your requirements going forward.	Considered the impact on Coppin's plans for using federated identity to gain interinstitutional access to online resources.
Examine the service provider's contracts for business and legal issues.	Worked out service agreement with vendor, which the state attorney general reviewed for compliance with state standards.
Think about cost.	Though Coppin's implementation was gratis, the IT Division hoped to reduce staffing and equipment costs.
Thinking cost, be sure to consider the tax implications of contracting for a service versus purchasing equipment and software.	Not an issue because of the project's gratis nature and Coppin's not-for-profit status.
Involve legal, contracting, and line-of-business (LOB) personnel in the evaluation.	Coppin's general council as well as its IT governance structure, which encompasses faculty and administration leadership, reviewed Fischer's proposal.
Involve the privacy office and the security team in the evaluation.	Coppin's IT security officer reviewed Fischer's proposal, identifying potential issues for resolution.
Involve IT, HR, and the service provider from the beginning to ensure the necessary technical and process integration between on-premises infrastructure and service provider.	All were involved in the proof of concept to test the feasibility of Fischer's proposed SaaS IdM solution with Coppin's IT infrastructure.

Source: Burton Group, 2010 Identity and Privacy Strategies Planning Guide: A Market in Transformation.[11]

Technology

Perhaps the greatest concern for some IT Division staff members was the risk in delegating control of an integral IT service. Questions also emerged about the solution architecture and its impact on the IT Division's operations. After much debate among

staff members, the IT Division asked the vendor to conduct a proof of concept to help Coppin understand the risks and implications of migrating from an internally hosted to a SaaS IdM configuration.

The two parties worked over the winter of 2009–2010 on the proof of concept, replicating the administrative and student environments in a firewalled VMware test environment interfaced to the SaaS IdM solution. The IT Division, the Office of Records and Registration, the Office of Human Resources, and the vendor mapped out the user case scenarios to test. In addition, the IT Division and the vendor decided it was an optimal time to redesign the user interface of Coppin's online password-reset utility, reducing several user interface screens to one screen.

With everything in place, a team of IT Division staff, Fischer staff, and representatives from the Office of Records and Registration and the Office of Human Resources tested all user case scenarios. The password testing focused on the current set of services: password reset, logging users' 10 previously used passwords, and user identity verification questions. Students and the IT Division's student help desk staff tested the interface and validated various student user scenarios such as password reset. For the provisioning tests, the Office of Records and Registration and the Office of Human Resources focused on the events that trigger the automatic provisioning process and the workflows for student and administrative accounts, e.g., student matriculation and new hires, reactivating inactive users, and personal data corrections or changes. The proof of concept tested all password and provisioning scenarios for student, faculty, and staff users.

All tests were successful, alleviating staff members' concerns. The IT Division concluded that technologically, the SaaS IdM configuration was a viable solution for Coppin.

Security and Risk Assessment

The IT Division's IT security director developed a checklist of concerns: redundancy, disaster recovery, business continuity if Internet access should fail, and encryption and other security measures to prevent unauthorized access and release of personal information in transit and at rest at the SaaS IdM site.

Because Coppin State University is a state agency, the IT Division consulted with the state attorney general's office to learn about evaluation criteria to ensure the vendor's SaaS IdM solution met state-mandated requirements. (A source of evaluation criteria for other IT organizations is Shared Assessments, a member-driven organization that strives to standardize evaluations of service providers. Their website contains downloadable assessment tools. See http://www.sharedassessments.org for more information.)

In addition, due diligence required that the IT Division consider Fischer's long-term viability when contemplating the SaaS IdM implementation. The two parties negotiated a detailed service agreement that specifies confidentiality, disaster recovery, and legal obligations. The contract contains clauses that specify

- that Fischer will reinstall Coppin's internal IdM functionality if Coppin is not satisfied with the SaaS IdM solution,
- that Fischer has no direct access to Coppin's personal information (a FERPA clause),

- specific disaster recovery actions, and
- actions if Fischer goes out of business.

The Office of the Maryland Attorney General reviewed and approved the agreement. Additionally, Coppin engaged an outside consultant group to review Fischer's solution, including service level agreement, security policies and infrastructure, contract, and solution architecture.

Support

Support escalation concerned some IT staff members because Coppin users might perceive any SaaS-related problems as local IT problems. The IT Division wanted to delineate support provisioning roles and escalation triggers for both organizations to determine under what circumstances and at what point the IT Division would get involved in service problems. The two parties developed an agreement formalizing these issues.

Purchase Price

Purchase price did not factor into Coppin's implementation, due to the IT Division's agreement to co-develop a higher education SaaS IdM solution with Fischer. But it is likely to be of interest to those who may contemplate a similar solution. One point of reference for pricing information is an article published in 2010 by TechTarget that compares the cost to deploy or acquire the Fischer Identity Suite SaaS solution with a conventional hosted solution in a 1,000-user organization. In this example, the SaaS solution lists a one-time $50,000 implementation services fee and an annual $28 per-user service fee. The conventional solution lists initial costs of $100,000 for software license and connectors, $200,000 for implementation services (assuming that implementation cost is twice the cost of the software), and $10,000 infrastructure costs for servers and associated hardware as well as ongoing annual costs of $100,000; and administration costs of $90,000 for an administrator.[12] Note that the actual costs would vary by implementation; this example provides only a general cost comparison of SaaS and locally hosted IdM solutions.

Governance Review and Sign-Off

Coppin maintains a three-prong IT governance structure: the Faculty Information Technology Committee (FITC), chaired by a faculty member and composed of representatives from Coppin schools and departments nominated by the provost, as well as the CIO; the Information Resources Management (IRM) Committee, chaired by the CIO and consisting of the university vice presidents and directors of the major university divisions, as well as the FITC chair; and the IT Students Advisory Committee, co-chaired by the Student Government Association (SGA) president and the CIO and composed of other SGA officers. For action to occur, all three committees must first approve any IT-related proposal. It then goes to the university president for his final decision and signature. "Everything related to IT flows through these committees—policies, major projects, ideas, and planning—for feedback and approval," explained El-Haggan. "All these inputs feed into final decisions."

The proposed SaaS IdM solution followed this same governance path. The committees reviewed the proposal—and expressed some concerns. Richard Siemer, vice president, administration and finance and a member of the IRM Committee, described the proposal's pros and cons. "Outsourcing is a comfortable model in my world of finance. The university outsources many functions routinely, except those it wants to control. The idea of outsourcing some parts of IT as opposed to others hinges on the control issues. Initially, I felt the SaaS IdM solution fell into the latter category because of the control issues." Siemer and other IRM Committee members raised other concerns. "[Outsourcing IdM functions] was not commonly done. We were nervous about the proposal in terms of the transmission of data and its potential for interception, even when encrypted, and the reputational issues if it was hacked," continued Siemer.

Eventually, the committees approved the proposal for several reasons. First, the committees understood that the type of information transmitted off-site would not directly identify Coppin students, faculty, and staff. Second, Coppin had fostered a long-term and successful relationship with the vendor, which encouraged trust. Third, El-Haggan's personal backing persuaded them. Because of his personal reputation on campus and past successes with other IT projects, the committees trusted that his planning for the project and contingencies was thorough. The successful proof of concept validated El-Haggan's project assessment. "We approved the project because we felt the SaaS IdM solution's technology was sound as well as cost-effective and our information would be secure," stated Habtu Braha, dean, School of Management Science and Economics, and FITC chair. Coppin's president approved the project, too.

Migration to the SaaS Solution

With institutional approval in place, the IT Division and a Fischer representative completed the SaaS migration over a weekend in the spring of 2010. IT Division staff reported a very smooth transition, completing it earlier than planned. The IT Division staff members felt the technical and operational experience gained during the proof of concept contributed to the migration's success.

Since the migration, the IT Division reports smooth operations of the SaaS IdM solution, even during fall 2010 registration, a peak period for password management, identity management, and provisioning activities.

Operational Overview

Coppin manages its identity information internally, transmitting identity data elements to the SaaS IdM system. These data elements are carefully selected to include just enough personal information to complete the SaaS-based transactions without directly identifying the person. The SaaS IdM system then performs essential, routine IdM functions. Fischer hosts and operates Coppin's SaaS IdM system at its highly secured Tier III data center. The solution is based on the vendor's Global Identity Architecture, a standards-based, independent platform. This section presents an operational overview of Coppin's SaaS IdM solution.

Provisioning

The IT Division installed two proprietary IdM appliances, called Global Identity Gateways, which interface directly with Coppin's SAS and HR administration systems. When a Coppin user creates a new identity or when an account changes in either the HR or SAS ERP system, that event triggers a specific script. Depending on the person's job or student classification, the script instructs the Global Identity Gateway to query the ERP system for that individual's non–personally identifying information (e.g., user ID, security questions, zip code, birth date, and campus ID number) and then to hash it. The hashed information is forwarded to a discretely firewalled Coppin-based SaaS IdM web server, which transmits the secured information to Fischer's SaaS IdM site using Secure Sockets Layer (SSL) encryption over Coppin's 4-gigabyte network connection.

Once received at the SaaS IdM site, the information is decrypted and becomes the person's unique identifier. A user IdM record is built that does not contain any identifying information other than the hash code. The SaaS IdM system is set up to provision an employee's permissions automatically, on the basis of job classification. The Fischer Provisioning Server completes several functions in a proprietary fashion: It provisions accounts and e-mail access, adds users to correct PeopleSoft roles, sets/updates security questions and answers, creates home and web folders, and assigns permissions and sharing. The information is stored in a database at the SaaS IdM site and an acknowledgement is sent back to Coppin's ERP. New accounts and account changes are reflected automatically.

The appropriate Coppin office notifies users about their user ID and provides instructions on how to create their passwords using the online Account Manager Website. Coppin does not provide or distribute passwords to users; users create their own passwords. A person wanting to log in to a Coppin system enters his or her username and password into the system, which looks up the hash code that is on file for that person in Coppin's directory and sends that hash code to the SaaS IdM site, which then checks to see what systems the person with that hash code is authorized to use. If the person is authorized to access that system, the SaaS IdM system okays the log-in.

Self-Service Online Password Reset

Passwords for Coppin's network, EagleLINKS (Coppin's self-service portal), and Blackboard system are synchronized so that a single password provides access to all three accounts. Users must reset their password every 120 days, in accordance with the state's Information Technology Security Policy and Standards. They complete this task with the EagleLINKS online Password Kiosk. Users authenticate their identity by entering their username, home address zip code, birth date, and campus ID number and correctly answering a randomly selected user-defined security question. This information follows a similar hashing, encryption, and transmission path through the Global Identity Gateway, the firewalled SaaS IdM web server, and SSL transmission. Once received at the SaaS IdM site, the Identity Server updates the user's identity profile. The security questions are stored in a local Fischer database. The SaaS IdM service stores and maintains each user's previous 10 passwords in an encrypted database to prevent duplicate passwords, as required by the state. Acknowledgments are sent back to Coppin and reflected automatically in Coppin systems.

Maintenance and Monitoring

Because of the SaaS IdM system's integration with Coppin's ERP system, the Fischer and PeopleSoft maintenance upgrades must be synchronized. The vendor monitors the SaaS IdM solution 24/7, with the IT Division receiving scheduled log reports on IdM activities in accordance with Coppin's audit requirements.

Outages/Disaster Recovery

One concern frequently voiced about SaaS solutions is what happens if the Internet goes down. Coppin's SaaS IdM solution's main point of failure is Coppin's single external Internet connection. (The IT Division is procuring a second Internet connection.) If Coppin's Internet connection goes down, the IdM system collects and stores changes at Coppin, transmitting them to the SaaS IdM site when the connection is restored. In a worst-case scenario, new accounts could be processed manually on site, updating the SaaS IdM solution after the fact. El-Haggan explained his view: "We could still complete our provisioning processes manually, so nothing is affected if we should get a new hire or new student during an outage. Also, access to systems on campus is not affected. You have to weigh the pros and cons. Even if the solution is down for an hour, it is a lot faster than our previous week-long processing time."

In the event of longer-term outages, activities could continue, as both Coppin and Fischer have disaster recovery strategies in place. Coppin and Salisbury University have a joint-hosting agreement for each other's university systems. Fischer maintains multiple data centers.

Reversion to Campus-Hosted Solution

Coppin's contract with Fischer allows the university to revert to Fischer's on-campus hosted solution if unsatisfied with the SaaS IdM solution. In this event, the IT Division has the needed infrastructure in place to copy the data from the SaaS IdM servers back to servers located at Coppin—an inconvenient, though not inconceivable, proposition—and all IdM services would be delivered in-house again.

The IT Division estimates that the SaaS solution freed up 1.5 FTE IT staff from provisioning, server management, backup, storage, and monitoring requirements. The IT Division is using the recovered resources to tackle new projects, including refinement of current ERP business processes.

Business Process Integration

Some may consider IdM to be a technical issue, but when considering its entire scope, business processes become pertinent, too. As industry analyst Bob Blakely says, "In most mature organizations, an identity service provider will supplement, not replace, the existing enterprise IdM infrastructure. Thus the necessary technical and process integration between on-premises infrastructure and the SaaS IdM solution will require active collaboration between the IT department, relevant administrative offices, and the vendor staff."[13] This section details how the Coppin State University IT Division worked

with the institution's Office of Admissions, Office of Records and Registration, and Office of Human Resources to integrate the SaaS IdM solution's provisioning capabilities into their respective business processes.

Administrative Provisioning

When setting up the SaaS IdM solution, representatives of the IT Division, the Office of Human Resources, and the vendor delineated the major actions that would invoke the solution. For example, when a new hire's personal information is entered into the PeopleSoft ERP, it triggers an automated account-provisioning process. Termination and retirement are other examples of actions that trigger events in the SaaS IdM system.

Coppin maintains several employee classifications: federal work-study students and student contractual workers (i.e., nonfederal work-study students), temporary agency employees, contingent employees, regular nonacademic employees, adjunct faculty, and full-time instructors and faculty. The several employee classes associated with student workers, faculty, and staff members complicate the provisioning of administrative accounts. The SaaS IdM system team developed a schema to delineate resource access on the basis of the employee classes. "The employee's job classification dictates the level of access, so if your job is X, then you can access Y," stated Cindy Prevatte, human resource information systems manager. For example, a person's primary job entitles that person to permissions for various administrative, e-mail, and network services and certain EagleLINKS services. The SaaS IdM system is set up to provision an employee's permissions automatically, on the basis of her or his job classification. Individuals requiring additional access (e.g., deans or department chairs) must submit the appropriate form to the IT Division, though Prevatte stated that the system covers most employees without additional paperwork.

The SaaS IdM system team members meet to add to or modify the permission provisioning schema as necessary. For example, college work-study students used to fill out time sheets on paper. In spring 2010, their time sheet entry moved online, using PeopleSoft. In the past, these workers had no access to the online time sheet entry function, so the team had to reconfigure the SaaS IdM solution to accommodate this new requirement. In the end, they reconfigured the college work-study job classification and successfully worked through the provisioning process from start to finish for that classification. Subsequently, Coppin provisioned permissions for 200 college work-study students, which posed no problems for the SaaS IdM solution.

In cases such as this, the IT Division, the business process owner, and the SaaS IdM vendor all work together to ensure continued synchronization between the SaaS IdM solution, the network, and Coppin's administrative systems. "We learned a lot," stated Prevatte. "The IT Division needed to work with us so we could educate them about our changes and to ensure we followed the right rules. The IT Division and Fischer had to reconfigure the PeopleSoft system and IdM solutions respectively. We have to be cognizant that what we do will impact the IT Division as well as the SaaS IdM vendor to ensure that all elements remain integrated, so the process flows." Such a situation requires clear communication among all parties about the planned changes

and the different parties' time frames, deadlines, and lead times. Working together, the SaaS IdM team made appropriate changes in the previously described situation in a couple of days.

The automated provisioning process condensed new employee processing times from a week to a day. The new hire picks up her account in person at the IT Division. She verifies her ID number, her zip code, her user ID, and her date of birth; she creates a password; and she learns how to log on to the university systems. She leaves the IT Division with her account, enabling her to immediately begin working at her office. The SaaS IdM system is especially efficient at handling the complex account-provisioning needs of a changing faculty population. Each semester brings approximately 150 to 200 faculty and adjunct new hires or rehires to campus, and all must be efficiently outfitted with appropriate permissions. Prevatte noted no problems with the SaaS IdM solution during this peak time.

Student Provisioning

Student account provisioning is more straightforward than provisioning of employees' administrative accounts because far fewer categories of students exist. Student matriculation triggers a process for provisioning network and EagleLINKS access, a home directory, a web folder, and an e-mail account.

Coppin's Registrar Margaret Turner described two benefits of the SaaS IdM solution. First is significantly faster processing time for new student accounts and records corrections. In the past, students received their new accounts within 24 to 48 hours of matriculating. Today, the SaaS IdM solution creates a new student account within 10 to 15 minutes. "Now students take their placement test in one building," Turner says, "and upon test completion and matriculation, the new student can walk immediately over to the student help desk to pick up her account information." The second benefit is the 24/7 access for password resets. Instead of having staff process password resets manually, students can reset their passwords anytime by correctly validating their identity to the EagleLINKS portal's online password reset utility.

Next Steps

The IT Division continues to enhance the SaaS IdM solution's capabilities. Areas of focus include deprovisioning accounts, renaming accounts due to their owners' name changes, and creating accounts for non-Coppin entities.

But El-Haggan has a more strategic plan in mind, too. Coppin's SaaS IdM system manages access to the university's internal, "home" resources—e.g., the EagleLINKS portal and Blackboard learning management system. But the issue of interinstitutional access of resources grows imperative as academic, administrative, and research activities increasingly cross institutional borders. For example, Coppin's collaboration with the University of Baltimore enables students from either institution to take courses at the other for credit. But Coppin student, faculty, and staff "home" institution credentials may not work when accessing resources at other organizations. On a broader level, the University System of Maryland member institutions are actively talking about shared

services and broader interaction with the state's community colleges. Donald Z. Spicer, CIO and associate vice chancellor for IT for the University System of Maryland, stated that "a common IdM approach will be critical to us going forward. There is a general awareness that inward-looking solutions will not be adequate."

One such common IdM solution is federated identity, an IdM practice that streamlines interorganizational access to resources. With federated identity, organizations come together and create a partnership in which participants configure their IdM systems to a preapproved set of policies, processes, and technologies. This creates a "trust framework" that enables members' constituents to access resources at each other's organizations with their home institution credentials. If a student's home college and the university from which she accesses research data belong to the same identity federation, she can use her home credentials to log on at another institution because both parties comply with the same predefined trust framework.

One federated identity solution drawing attention is InCommon, a nationwide higher education partnership founded by the Internet2 Middleware Initiative. Participants pay a one-time registration fee and an annual fee to support the federation's operations. Members complete a rigorous series of policy, business practice, and technical steps to comply with the InCommon framework and then are allowed to federate with its diverse membership base.[14] The InCommon Federation encompasses almost 250 higher education institutions, government and nonprofit research entities, and sponsored partners.[15] Currently three campuses in the University System of Maryland—University of Maryland, Baltimore; University of Maryland, Baltimore County; and University of Maryland, College Park—belong to InCommon. The National Institutes of Health (NIH) and the National Science Foundation (NSF) are among the government and nonprofit entities. Sponsored InCommon members include Apple iTunes U, EDUCAUSE, Kuali, and Microsoft.

El-Haggan wants Coppin to join InCommon to provide access to resources located at other institutions. In preparation, IT Division staff members attended an InCommon boot camp as well as locally hosting training sessions to learn more about membership compliance. But fulfillment of El-Haggan's vision requires Fischer, a component of Coppin's current IdM infrastructure, to join InCommon or modify its products to comply with the federation's specifications. Fischer's support of Security Assurance Markup Language (SAML) and Shibboleth, which are integral parts of InCommon's technical framework, give the vendor a head start should it decide to seek InCommon membership.

The University System of Maryland has a goal to obtain robust internal and federated IdM solutions for all of its member institutions. Consequently, it is endorsing InCommon as its identity federation strategy, encouraging all member institutions, including Coppin, to join InCommon in order to offer system-wide federation services. An InCommon-compliant SaaS IdM solution would offer one way for member institutions that lack their own IdM expertise and resources to meet this goal.

To make InCommon membership affordable to all Maryland institutions—members of the University System or not—the Maryland Education and Enterprise Consortium

(MEEC), a statewide consortium that licenses the use of education hardware and software at competitive prices for K–16 private and public projects, is negotiating a MEEC-wide membership with the federation.[16] El-Haggan, a MEEC board member, is fostering this strategy. With MEEC as an InCommon member, any of the consortium's members, including Coppin, would be eligible to join the federation, too. If this plan comes to fruition, MEEC members could employ an InCommon-compliant SaaS IdM vendor to technically comply with the federation's guidelines. It is anticipated that Fischer's and MEEC's InCommon memberships will be finalized by the end of March 2011.

Lessons Learned

The IT Division's experiences with its SaaS IdM solution offer guidance and lessons for other IT organizations when considering outsourcing some IdM functions.

Perform a proof of concept.

Several case study participants emphasized the proof of concept's importance when evaluating the SaaS IdM solution. "It was really illuminating because it brought out a lot of issues," stated Coppin's Thomas Smith. It appeased fears about the security of personal information, facilitating the solution's endorsement from the IT Division and the IT Governance Committees. The experiences gained from the proof of concept enabled the IT Division, the Office of Records and Registration, the Office of Human Resources, and the vendor to address any technical or workflow kinks early on, smoothing the migration to a production service.

It takes a village.

A SaaS IdM solution involves more than just technology. There are security issues, legal issues, and administrative issues that involve non-IT departments and organizations. For example, Coppin had to confer with the state attorney general's office to ensure that the solution conformed to state IT security policies and practices. In some ways the SaaS IdM implementation resembles an ERP implementation because of the close interaction between the vendor, the IT organization, and the administration offices to configure the solution with the institution's network and administrative systems. Thus, an IT department must be prepared to educate and communicate clearly with nontechnical audiences throughout the project.

Proactively address stakeholders' concerns.

Any IdM solution is bound to be highly technical; security of personal information is a sensitive issue; and moving to a SaaS IdM solution is a relatively unconventional strategy. Any one of these circumstances might raise concerns from IT department staff members, business process owners, and/or senior administration; all three taken together are almost certain to heighten anxiety levels.

El-Haggan defused these fears by directly engaging the Coppin community. He facilitated discussions within the IT Division about the SaaS IdM solution, allowing staff to form a consensus around the proof of concept. He presented the solution to the

IT governance structure to address their security and risk concerns up front. And he engaged the Office of Records and Registration and the Office of Human Resources in the evaluation process to ensure a rich discussion of the SaaS IdM solution's impact on their business operations.

Choose a modular solution.

A key selling point of the SaaS IdM solution was its modular configuration, enabling the IT Division to take on only as much as it could effectively handle at a given time. With a modular solution, institutions with limited IT resources and staff can start small and scale their SaaS IdM solution accordingly.

Choose an empathic and flexible partner.

This may be obvious, but its importance cannot be overestimated. Several case study participants highlighted Fischer representatives' willingness to listen and their flexibility throughout the collaboration. These characteristics have contributed to the productive, multiyear relationship between the parties.

Cross the t's and dot the i's.

Make sure that as many contingencies are covered as possible and clearly assign responsibilities for their management and mitigation. For Coppin's SaaS IdM project, these included ensuring regulatory compliance, establishing steps to be taken in the event of failures, and formalizing an exit strategy with the vendor.

Reach out for help.

Coppin's IT Division is fortunate in that it collaborates strongly with its fellow members of the University System of Maryland. For institutions not part of a system, finding like-minded colleagues and institutions can bring wider experience and additional opportunities to the table. This is an invaluable asset to any institution embarking on a project like Coppin's, but it is especially valuable to one with constrained resources.

Conclusion

Managing IdM's many facets—hardware, software, business processes, and data—can be time-consuming and costly. Such an obligation can tax even the largest IT organization, and it can overwhelm a smaller one. Coppin State University's IT Division faced this situation. Managing user accounts and passwords—routine, somewhat time-consuming, but fundamental IdM functions—strained its limited IT resources, leading to lengthy processing times. So when the opportunity arose, Coppin's IT Division made a studied decision to outsource these functions to a SaaS IdM solution in 2010.

The decision enabled the IT Division to automate and streamline its IdM processes and to offload routine administrative functions, freeing up approximately 1.5 FTE IT staff for more strategic endeavors. It expedited password and account processing from days and hours to minutes. As Jack Suess, vice president of IT and CIO, University of Maryland, Baltimore County, observed, "The SaaS model is a real win for many

institutions. An IdM infrastructure tends to require highly technical people and a 24/7 IT infrastructure. Leveraging a company that has the system administration resources as well as the technical expertise to interface against the various institutional systems is a real win for a smaller school."

Endnotes

1. Mark C. Sheehan and Cedric Bennett, with Pam Arroway, Susan Grajek, Judith A. Pirani, and Ronald Yanosky, *Identity Management in Higher Education, 2011* (Research Study 1, 2011) (Boulder, CO: EDUCAUSE Center for Applied Research, 2011), available from http://educause.edu/ecar.
2. Ronald Yanosky and Gail Salaway, *Identity Management in Higher Education: A Baseline Study* (Research Study 2, 2006) (Boulder, CO: EDUCAUSE Center for Applied Research, 2006), available from http://educause.edu/ecar.
3. EDUCAUSE, "7 Things You Should Know about Federated Identity Management" (September 10, 2009) (Boulder, CO: EDUCAUSE, 2009), http://net.educause.edu/ir/library/pdf/EST0903.pdf.
4. For more technical information, see online resources at the EDUCAUSE Identity and Access Website, http://www.educause.edu/Resources/Browse/Identity%20and%20Access%20Management/17322.
5. In *Identity Management in Higher Education, 2011*, ECAR defines a small institution as one that has 1–4,000 FTE students.
6. Sheehan and Bennett, *Identity Management*.
7. Ibid.
8. David Kearns, "Cloud Computing Is Shifting the Way We View IdM," *NetworkWorld* (June 8, 2010), http://www.networkworld.com/newsletters/dir/2010/060710id2.html.
9. For more information about the Department of Information Technology's Information Technology Security Policy and Standards guidelines, see http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx.
10. For more information about Fischer International's Global Identity Architecture, see http://www.fischerinternational.com/competencies/global_identity_architecture.htm.
11. Bob Blakely, *2010 Identity and Privacy Strategies Planning Guide: A Market in Transformation* (Midvale, UT: Burton Group, September 30, 2009): 13, http://www.burtongroup.com/Client/Research/Document.aspx?cid=1827.
12. Laura Smith, "Identity Management in Cloud Computing Courts Enterprise Trust," *TechTarget* (April 13, 2010), http://searchcio.techtarget.com/news/1509770/Identity-management-in-cloud-computing-courts-enterprise-trust.
13. Blakely, *2010 Identity and Privacy.*
14. For more information about InCommon, see https://spaces.internet2.edu/display/InCCollaborate/Information+from+InCommon.
15. InCommon, "InCommon Participants," February 25, 2011, http://www.incommon.org/participants/.
16. For more information about the Maryland Education and Enterprise Consortium (MEEC), see http://www.meec-edu.org/index.html. See also Tamara Petronka and Donald Z. Spicer, "A Model for Highly Leveraged Procurements: The Maryland Education Enterprise Consortium" (Research Bulletin 7, 2010) (Boulder, CO: EDUCAUSE Center for Applied Research, 2010), available from http://www.educause.edu/ecar.

Citation for This Work

Pirani, Judith A., and Susan Foster. "From Homegrown to the Cloud: Identity Management Evolution at Coppin State University" (Case Study 1, 2011). Boulder, CO: EDUCAUSE Center for Applied Research, 2011, available from http://www.educause.edu/ecar.