

# Federating the University of North Carolina: Origins and Benefits

Judith A. Pirani, ECAR  
Bob Albrecht, ECAR

**ECAR Case Study 2, 2011**

**EDUCAUSE**

4772 Walnut Street, Suite 206  
Boulder, Colorado 80301  
[educause.edu/ecar](http://educause.edu/ecar)

# Federating the University of North Carolina: Origins and Benefits

**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.

Copyright 2011 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to [ecar@educause.edu](mailto:ecar@educause.edu).

# Federating the University of North Carolina: Origins and Benefits

## 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*,<sup>1</sup> by Mark C. Sheehan et al. In addition to updating the picture of identity management practice reported in a baseline ECAR study conducted during 2005–2006,<sup>2</sup> the 2011 study takes a deep look at institutional adoption of federated identity technology.

We undertook this case study of the University of North Carolina (UNC) Identity Federation to explore the benefits and impacts of federated identity on the university and its 17 constituent institutions. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings.

ECAR owes a debt of gratitude for their time and insights to Gwen Canady, Project Management Officer, UNC General Administration (UNC-GA); Marshall Clark, Business and Technology Applications Analyst, UNC-GA; Celeste Copeland, Identity Management Manager, UNC at Chapel Hill (UNC-CH); Joel Dunn, Associate Vice Chancellor, Information

Technology Services, Administrative Systems, UNC at Greensboro (UNCG); Rob Gorrell, Middleware Engineer, UNCG; Donna Heath, Associate Vice Chancellor, Information Technology Services, Systems and Networks, UNCG; Susan Hensley, Director of Systems, Information Technology Services, UNCG; Steven Hopper, Director of Online Services and CTO for UNC Online, UNC-GA; John Leydon, Vice President for Information Resources and CIO, UNC-GA; Alan Mabe, Senior Vice President for Academic Affairs, UNC-GA; Kelly Rowett-James, University Registrar, UNCG; Jim Sadler, Associate Vice President for Academic Planning, UNC; Mark Scheible, Security and Compliance Manager, North Carolina State University (NCSU); Jan Tax, Systems Specialist, UNC-CH; and Heather Thomas, NC FIT Business Systems Analyst, UNC-GA.

## Introduction

In ECAR's 2006 baseline study on identity management in higher education, study author Ronald Yanosky raised a simple yet imperative question: "Who's there? Today about a billion people are equipped to come knocking at the online resources that colleges and universities have spent so much effort building. Most who do will come with legitimate purposes; some with malicious ones. It's more important than ever to know: who is there?"<sup>3</sup>

Several years later, the answer to Yanosky's question is even more imperative and complex. More and more institutional resources continue to move online, bolstered by the adoption of cloud computing and mobile applications. Access is increasingly cross-departmental and cross-institutional as academic, administrative, and research activities span organizational borders. The number of people who use these resources is rising as online education programs, alumni resources, and K-12 initiatives foster new online constituencies. Such circumstances call for IT organizations' deployment of identity management (IdM) practices—and policies, processes, and technologies—to establish user identities and enforce rules about access to digital resources.<sup>4</sup>

One IdM practice is the institution's collection of identity information about its constituents, which IT organizations store and manage in an identity system. Credentials are then created—username and password, usually—so that individuals can access institutional online resources. For example, a new student presents proof of her identity before her college registrar issues her an identity (ID) card and credentials to access the institution's online business systems. These credentials will allow the student to make appropriate use of institutional IT systems. But pursuing a higher education—and conducting research—increasingly calls for access to resources outside institutional boundaries. What happens when our student tries to access technology resources at another university? In the absence of some cross-institutional solution, her "home" credentials are likely to be useless.

Federated identity is an IdM practice that streamlines interorganizational access to resources. With federated identity, organizations come together to create a federation within a state university system or among unrelated institutions where participants configure their IdM systems to a preapproved set of policies, processes, and technologies, creating a "trust framework" that enables members' constituents to access

resources at each other's organizations with their home institution credentials. If the student's home college and the university with the research data belong to the same identity federation and have implemented the appropriate solutions, she can use her home credentials to gain access. (See the sidebar "Identity Management and Federated Identity Overview" for more information.)

## Identity Management and Federated Identity Overview

This sidebar provides an introductory overview about identity management and federated identity for nontechnical readers, incorporating information from the following resources:

- "7 Things You Should Know about Federated Identity Management" (<http://net.educause.edu/ir/library/pdf/EST0903.pdf>).
- InCommon, "Slide Deck—Intro to Federated IdM and InCommon" (<https://spaces.internet2.edu/display/InCCollaborate/Information+from+InCommon>).
- About Shibboleth (<http://shibboleth.internet2.edu/about.html>).
- Those wishing more technical information can access online resources at EDUCAUSE (<http://www.educause.edu/Resources/Browse/FederatedIdentityManagement/31075>), InCommon (<http://www.incommonfederation.org/>), and at the UNC Identity Federation (<http://federation.northcarolina.edu/>).

Many institutional online information resources and services—such as course registration services, library databases, and grant management applications—restrict user access. Identity management (IdM) refers to the policies, processes, and technologies that establish user identities and enforce rules about access to these resources.<sup>1</sup> As part of IdM, a higher education institution verifies the identity of its students, faculty, and staff via a driver's license, passport, or other form of identification; issues electronic credentials to them (e.g., username and password); and stores their identity information attributes (e.g., name, address, phone number, role, group affiliation, and/or e-mail address) electronically in an identity system. When a student, faculty, or staff member attempts to access an institutional online resource, the resource requires the user to authenticate him/herself (typically with a username and password). This information is passed to the identity system, which then verifies the user's identity and, if successful, furnishes the resource with predefined attributes permitting access.

Interinstitutional access to resources adds another layer of IdM in order to authenticate and authorize users from different colleges and universities. Federated identity management simplifies this problem, creating a trust framework for digital identities across multiple organizations. In a federated system, participating institutions (in the role of identity providers, or IdPs) provide their users' identity attributes on the basis of agreed-upon standards, facilitating authentication among members of the federation

*Cont'd*

and granting users appropriate access to online resources (from institutions in the role of service providers, or SPs). When a user affiliated with a federated institution requests a protected resource from another institution in the federation, that request generates a WAYF (“where are you from”) request. This request is passed to the user’s “home” institution, which verifies the user’s credentials and asserts to the requesting resource that the user is authenticated there. Significantly, individual privacy is protected, since the online resource never collects the user’s credentials; all that passes between the two member institutions is a WAYF request and an assertion of authentication. Users need only one set of authentication credentials to access resources from other federation members, and these credentials need never be exposed to outside entities.

Many higher education federations authorize users via Shibboleth, a standards-based, open-source software package developed by the Internet2 Middleware Initiative. Shibboleth allows a user to utilize a single ID and password to access protected resources. It allows the identity management system and the user to release only the information necessary to gain access to an online resource. Shibboleth incorporates OASIS Security Assertion Markup Language (SAML) 2.0 to exchange identity data and attributes between federated members. SAML is very flexible, allowing federated members to select which identity attributes to share during the authentication process.

## Endnote

EDUCAUSE, “7 Things You Should Know about Federated Identity Management” (September 10, 2009) (Boulder, CO: EDUCAUSE, 2009), 1, <http://net.educause.edu/ir/library/pdf/EST0903.pdf>.

Besides streamlining access, federated identity offers other inherent benefits. There are fewer user credentials for each federation member to maintain, simplifying administration and reducing the threat of accidental identity information release. In fact, within a trust framework, institutions may rely simply on assertions from one another that the person requesting a resource has some required attribute—such as being a registered student—without exchanging personally identifying information. Federated identity provides a preconfigured means to evaluate an individual’s access requests; developers can leverage that tool to build authentication hooks into new applications. Ease of access facilitates collaboration; individuals have to employ only a single set of credentials to gain access to various member resources. Federated identity also has intrainstitutional value as a single sign-on technology, so that users log in once to access an institution’s internal academic, research, and administrative resources. Among ECAR’s 2011 survey respondents, internal single sign-on was the most frequently named motivation for evaluating or implementing federated identity solutions, though providing resource access within a system or consortium was a very close second.<sup>5</sup>

When compared with national or international federation systems, those based on university systems or consortia exhibit some special qualities. It’s easier to set up a trust framework among institutions that already exist within a collaborative

context. System federations often have shared applications that fuel federation activities, and location within a single state's borders makes it easier to federate, since there's a more uniform legal environment.

One of the pioneers in identity federation within a state system is the University of North Carolina (UNC). Its General Administration's Information Resources (IR) division created the UNC Identity Federation (UNC-IdF) in 2008 to serve the UNC institutions and their affiliates. The Inter-Institutional Course Registration application, designed to permit online course registration between UNC campuses, mobilized federated identity efforts. But after two years, federated identity has demonstrated many other positive impacts throughout UNC and its campuses, and that is the focus of this case study. First the case study describes the UNC-IdF's intercampus implementation and consequential benefits. The focus then shifts to the UNC campuses and the federation's impact on local IdM activities. The final section describes the relationship between the UNC-IdF and two other federations—NC Trust, a North Carolina K–20 identity federation, and InCommon, a nationwide identity federation. The case study presents an operational, not a highly technical, examination of the UNC-IdF.

## System Dynamics

Chartered in 1789 by the North Carolina General Assembly, UNC has expanded from its initial Chapel Hill campus into a diverse multicampus public university encompassing 16 higher education institutions (also referred to as *campuses* in this case study) and one high school. Constituent institutions are Appalachian State University; East Carolina University; Elizabeth City State University; Fayetteville State University; North Carolina Agricultural and Technical State University; North Carolina Central University; North Carolina State University (NCSU); UNC at Asheville; UNC at Chapel Hill (UNC-CH); UNC at Charlotte; UNC at Greensboro (UNCG); UNC at Pembroke; UNC Wilmington; UNC School of the Arts; Western Carolina University; Winston-Salem State University; and the North Carolina School of Science and Mathematics. In fall 2009, slightly fewer than 200,000 full-time students attended UNC. However, individual campus enrollments highlight UNC's varied nature, ranging from fewer than 900 students at UNC School of the Arts to more than 30,000 at NCSU.

A board of governors oversees UNC's constituent institutions, electing a president who administers the university. A chancellor autonomously manages each constituent institution, reporting directly to the UNC president. The Office of the President and other university departments, including IR, reside within the UNC General Administration (UNC-GA).

Led by John Leydon, vice president for information resources and CIO, IR provides IT services to UNC-GA, UNC constituent institutions, UNC Online (UNC's digitally delivered course offerings), and distance education students. IR's mission is to complement, not replace, the IT services already provided by constituent institutions. For example, IR brokers system-wide vendor contracts and fosters initiatives to deliver IT services more efficiently to all of the UNC campuses. Steven Hopper, director of online services and chief technology officer for UNC Online, UNC-GA, characterized the relationship by saying, "Each campus's IT leadership and staff is responsible for their institutional IT

services and systems. IR becomes involved when there are broader implications.” Guiding IR is the UNC CIO Council, a monthly forum attended by Leydon and CIO representatives from each UNC campus IT organization.

Though each campus’s IT organization is autonomous, case study participants from campus IT organizations described UNC as a very collaborative system IT culture. “We are a large, relatively integrated university system that has a good history of various kinds of interaction,” stated Joel Dunn, associate vice chancellor, IT services, administrative systems, UNCG. “Our academic and administrative communities are used to accessing other campus applications to fulfill their needs.”

A notable example is the UNC Shared Services Alliance, which explores collaborative technology opportunities, including sharing the state’s allotment for ERP support systems and fostering centrally hosted ERP services for several of the UNC institutions. Perhaps this contributes to the system’s rather homogenous ERP environment, a factor in the development of the UNC-IdF. Most of the UNC campuses use the same vendor ERP system, with the exception of NCSU and UNC-CH. Learning management systems are more heterogeneous, with campuses using a variety of systems.

The autonomy and collaboration within UNC’s IT organizations come into play with development of the UNC-IdF. The bulk of IdM practices happen at individual campus IT organizations, where each maintains its own policies, procedures, and technologies, but federated identity factors increasingly into UNC’s intercampus collaborative activities.

## Intercampus Federation

The UNC-IdF’s inception was spurred by the need to support a new application that required intercampus user authentication and authorization. Because the federation’s and the application’s development are intertwined, this section includes both.

### The Driving Application

Federated identity enables users to access federated web-based resources without multiple log-in credentials, but finding that initial application on which to federate can be a challenging proposition. “If there is an issue with federation, it is the use case,” explained Mark Scheible, security and compliance manager, NCSU. “You need something that will generate enough interest to warrant the initial effort’s time and money.” The driving application must appeal to a common interest or a broad need among federation members.

UNC’s driving application was a web-based interinstitutional course registration application designed to facilitate online course exchange among UNC campuses. The application supports a major institutional project, the University of North Carolina Tomorrow Initiative. In 2007, the UNC Board of Governors commissioned that initiative to determine how UNC can respond directly and proactively to challenges facing the state in the 21st century through the fulfillment of the university’s mission.<sup>6</sup> One of the major commission findings included recommendations that involve IT. It called on UNC to increase access to higher education for underserved

regions, underrepresented populations, and nontraditional students—in specific by increasing access to university education programs for traditional students, nontraditional students, and lifelong learners.<sup>7</sup>

The initiative's recommendations led to a university-wide approach to online education. For example, UNC Online, a public portal, aggregates course, application, admission, and tuition information for all of the online courses at UNC's 16 higher education institutions. Furthermore, the UNC president and board of governors approved online course exchange in 2008, allowing a degree-seeking student enrolled at any UNC institution to take online courses offered at sister UNC campuses. "We want to encourage students to take courses from another campus, but we knew for this initiative to work, the registration process must be easy while protecting students' information," stated Alan Mabe, senior vice president for academic affairs, UNC-GA. "We wanted to develop a system that displays online course offerings at all UNC campuses with a single query, and enables registration."

The board of governors charged IR to create a technical solution to facilitate interinstitutional registration in December 2007, with a completion deadline of August 1, 2008, in order to transact course registrations for the fall 2008 semester. The idea seemed easy, but implementation was not. A student's identity information already resided at her home campus, but registering online at a sister UNC campus was problematic because IdM is administered locally at each UNC constituent institution. As things stood, a student would have to create new credentials at each sister UNC campus to receive the proper authentication and authorization to access that campus's registration web page. "We did not want to get into the whole notion of having to re-credential everyone, because all the students already had accounts issued by their respective schools," explained UNC-GA's Hopper.

With the board of governors' mandate in hand, IR and the CIO Council discussed various options. One potential approach was a centralized IdM solution to store everyone's unique identity, but that ran counter to UNC campuses' decentralized IdM approach. Federated identity offered "a perfect solution because every campus can still pursue their own IdM strategy," Hopper said. "IR creates certain guidelines from which the campuses could operate, and then we manage the trust relationship amongst ourselves."

That initial application spawned an intercampus federation that today contains 19 identity providers (IdPs) and 17 logical service providers (SPs). Membership is free. "We were truly lucky that UNC had a 'build it and they will come' situation," stated UNC-GA's Leydon. "Once it was available, it was easy to justify all the other applications we brought into the federation because there was little or no additional associated overhead."

## The UNC Identity Federation's Design

In response to the UNC Tomorrow Initiative, IR began to build UNC's Inter-Institutional Course Registration application in early 2008, incorporating federated identity for authentication and authorization. When designing the system, IR evaluated a number of vendor solutions as well as OpenID, an open authentication standard, but decided to implement Shibboleth 2.0 because of its more secure architecture.

When planning the UNC-IdF, which would underlie the application, IR decided to create a multiple-federation platform consisting of the actual production federation, a development federation for testing and experimenting, and an affiliates federation for external vendors and other entities. The multiple-federation structure gives the UNC campuses greater flexibility in defining policies about the release of identity attributes. For example, UNC campuses can utilize more stringent attribute release policies to affiliate federation members than to member campuses in the production federation.

IR delineated baseline attributes for federation IdPs and SPs, purposely designed to be consistent with the attributes of the InCommon Federation, a nationwide research and higher education identity federation, to maintain consistency across higher education. “We made an up-front decision to use commonly defined identity attributes in our federation to avoid splintering off UNC versus non-UNC attributes,” stated Hopper. “We try to use standards where they exist, and where they don’t, we’ll create a UNC-wide attribute.” Federation attributes cover user domain (e.g., student, faculty, staff, alum); username; unique identifier descriptor; e-mail address; and campus permanent ID, an attribute UNC developed because no standard definition existed.

Identity federation solved only part of the Inter-Institutional Course Registration application’s information exchange requirements. The UNC-IdF enables a UNC student to use her home campus credentials to log in and access a sister campus registration system. But when she enrolls in an online course, the sister campus registration system requires additional information from the student—information that resides back on her home campus’s administrative system.

IR resolved this problem by designing a web services back-channel to exchange relevant information, built upon the same attribute-exchange concept used in federated authentication and authorization. “The IdM piece coupled with the back-channel web services gives us the ability to provide centralized application delivery while still getting custom data back at the local campus ERP system,” stated Marshall Clark, business and technology applications analyst, UNC-GA. The web services pieces incorporate the same basic architecture as the Shibboleth identity management pieces. In other words, the back-channel information exchange uses Shibboleth’s IdP/SP model in the web services’ client/server context to pass previously agreed-upon user information.

## Implementation and Maintenance

From a responsibility standpoint, IR manages the UNC-IdF’s technical and policy infrastructure. Each campus IT organization owns and maintains its individual IdP. Early on, IR recognized the varying ability of each campus IT organization to complete these tasks, because UNC’s campus diversity extends to its IT resources. The simple fact was that some campus central IT organizations could fulfill their roles in the identity federation better than others. To overcome this potential roadblock, IR devised an implementation strategy to level the playing field: build a virtual appliance for each campus to facilitate its undertaking the IdP role.

Since IR and all the campus IT organizations used VMware for machine virtualization, IR created and distributed a virtual appliance (web server) for each campus, preconfig-

ured with Shibboleth and other necessary software for the campus to take on the IdP role. At each campus, the appliance is tied to its network behind its firewall to its LDAP directory. Each campus IT organization owns, operates, and maintains the appliance, but IR monitors it remotely, pinging it regularly and e-mailing a campus IT organization if the appliance goes down or encounters problems. IR provides technical support as needed to the campus IT organizations.

“It is hard to underestimate the value of IR’s decision to create a virtual appliance that we can deploy,” stated UNCG’s Dunn. “It would be hard to find the time to get the expertise to stand up one of these devices by ourselves, especially within the Inter-Institutional Course Registration project’s time frame. Having one delivered in a box was an important part of the federation’s successful implementation.” Some campus IT departments voiced initial concerns about the appliances’ potential reliability and their own ability to support them. But thus far, these problems have never materialized, since the appliances exhibited very little downtime and could typically be fixed simply by rebooting the device.

Then it was on to testing. “In my experience with federated apps, testing can be difficult because you are trying to transmit other people’s credentials into accounts on other systems,” stated Hopper. IR worked with UNCG to pilot the federation identity and the Inter-Institutional Course Registration application. IR sent a virtual appliance to the UNCG team, which the team got up and running. The two teams tested and tweaked the federation and the application over the next several weeks. The only significant issues involved altering data formats in the attributes tables to meet federation definitions.

With the virtual IdP appliances, the federation, and the application ready to go in April 2008, the next challenge was to prepare the campuses. According to Hopper, all the UNC campus IT organizations started from scratch. No campus had installed Shibboleth previously, though UNC-CH had enabled some of its applications to use Shibboleth. To bring the campuses up to speed, IR hosted an “install-fest,” an intensive one-day course about federated identity, its architecture (including Shibboleth), and IdP and SP software configuration as well. The meeting, held on April 30, 2008, included technical representatives from every UNC campus IT organization. A representative from Internet2’s Shibboleth project taught the session.

From May through July came the campus implementations. After the install-fest, each campus’s central IT unit booted up its virtual appliance and configured it for the campus IT environment. IR held one-hour web conferences with each campus’s IT staff to help them set up their IdP appliance and configure it into their LDAP directory. As a final step, IR validated all the campus IdPs, helping individual campuses address any last-minute problems. By August 1, 2008, all the campuses’ IdP appliances were operational to support the Inter-Institutional Course Registration application.

To manage the federation, IR built a database-driven, web-based application to add new entities—an IdP or SP, or even new federations—with just a few clicks. The latter is an interesting twist, with IR using the UNC-wide federation model to implement intrainstitutional federations (aka single sign-on) for campuses that lacked the IT resources to do so. (For more about this, see the section titled “Single Sign-On or Intracampus Federation.”)

IR continues to support local campuses as needed. The UNC-IdF website contains policies and comprehensive technical information about operations and testing. Hopper and his team offer consultative support as needed, too. “Over time, the campuses have learned a lot; now they can manage their IdP appliances themselves,” UNC-GA’s Hopper stated. “The campuses have done a good job of taking ownership and going forward with it.” He noted that the volume of help requests had declined significantly over time as the campus IT staff gained knowledge and expertise.

## Policies and Practices

Technology runs an identity federation, but predetermined policies and practices direct its operation. So IR worked to have the federation charter, policies, and guidelines in place before the Inter-Institutional Course Registration’s launch on August 1. As with the federation’s technical design, IR opted to draw from standardized resources, using InCommon’s trust framework as a model for the UNC-IdF. Next, the UNC Legal Affairs Division approved the federation charter, followed by the CIO Council. One helpful circumstance is that all the campuses operate under the single legal entity of the University of North Carolina, eliminating any interinstitutional legal issues.

## Federated Identity in Action

In August 2008, IR launched the UNC-IdF and the Inter-Institutional Course Registration application. But this was just the beginning. The identity federation and the web services backchannel created a new platform for centralized delivery of a wide variety of inter-campus applications. “When you build a federation, you use those building blocks, avoiding reinvention of the wheel,” commented Jan Tax, systems specialist, UNC-CH. “It addresses the issues of privacy and unintentional information release because you control exactly what entities the service provider sees.”

In addition, the new platform created a different approach to application development for IR. “We did not set the strategy and then work towards it,” stated UNC-GA’s Leydon. “We backed into the strategy because the application [platform] existed to do it.” Now future collaborative efforts among UNC constituent institutions will utilize federated identification; future administrative and academic vendors—whether open source or proprietary—must Shibboleth-enable (“Shibbolize”) their applications. “The UNC community now expects to interact with their services or software through the authorization and authentication processes associated with federated ID. It has been established and we are following that particular perspective,” stated Leydon.

IR selects applications to federate in a variety of ways. It uses its gatekeeper role for UNC campuses to learn about new application initiatives and suggest federation identity as a solution whenever appropriate. Sometimes direction filters down from the top, as for example with UNC Online’s Inter-Institutional Course Registration and Electronic Proctoring applications. Other times, individual campuses develop applications locally that fulfill broader university needs; examples include NCSU’s Virtual Computing Lab or UNC-CH’s RAMSeS research administration management system.

Whether projects originate top down, bottom up, or somewhere in between, federated identity offers ease of user access and streamlined application administration, which facilitate collaboration and resource availability across the university. The following discussions illustrate federated identity's pragmatic benefits with four application profiles.

### ***Collaboration via activeCollab***

The vendor A51's activeCollab is an online project management tool used throughout UNC. Federating activeCollab improved collaboration in interinstitutional projects. IR and campus project members used activeCollab to manage the Inter-Institutional Course Registration/UNC-IdF project. Initially they set up activeCollab in its native state, provisioning separate accounts to all team members across the UNC campuses. But team members forgot passwords, requiring resets. "It was a recursive problem," recalled Hopper. "We needed federated identity to use activeCollab effectively, and we were using the tool to create our identity federation for the Inter-Institutional Course Registration app." When the federation went live, IR Shibbolized activeCollab, and now UNC-IdF team members use their campus credentials to access a central site containing online project management discussions, instructions, tips, and other resources.

Other intercampus projects have adopted activeCollab, too. A good example is the UNC Finance Improvement and Transformation (FIT) initiative, a program that standardizes business processes and implements better accountability across the general accounting, contracts and grants, and financial aid areas of all 17 UNC institutions (including the high school). FIT also improves efficiencies through the development of shared back-office financial services and enhanced data management and data integrity. The expansive project involves a team in excess of 1,100 people across UNC-GA and the 17 institutions. FIT uses activeCollab to centralize communications and to store performance metrics and indicators, reducing the volume of project-related e-mail. Before IR federated activeCollab, account provisioning and management for the FIT activeCollab site was a time-consuming task for FIT's UNC-GA and campus project managers, according to Gwen Canady, project management officer, UNC-GA. For example, the release of a new FIT business process prompted team members to overload their project managers' e-mail boxes with information and password reset requests, leading to frantic support calls to local IT organizations. Now all team members can access activeCollab directly with their campus credentials, reducing the workload for project managers and for the campuses' IT support staff.

### ***Grant Management via RAMSeS***

RAMSeS, a research administration management system developed by UNC-CH's Office of Research Information Systems (RIS), is an example of an application developed outside the UNC IT organizations that eventually became a federated application within the UNC-IdF. The tool includes modules for human subject compliance, animal care compliance, conflict of interest, and technology transfer. Eventually RIS added interfaces to locate collaborative research opportunities across the 16 UNC higher education institutions by searching for and finding faculty who have grants and/or are conducting research in a particular area.

As RAMSeS evolved, other UNC campuses expressed interest in its deployment. Initially, UNC-CH's Information Technology Services (ITS) and RIS handled this locally. ITS deployed the software, with sister campuses providing hooks into their local IdM systems for authentication and authorization. This solution became unwieldy after the third campus implementation, so RIS decided to simplify the process by federating the application.

### **Virtual Computing Lab**

NCSU's College of Engineering and the Office of Information Technology (OIT) developed the Virtual Computing Lab (VCL), which allows a student to reserve a computer with a desired set of applications in Windows, Linux, or Solaris environments and remotely access it over the Internet. Though it was developed at NCSU, other UNC campuses and the K-16 community across North Carolina began to use VCL, too. The diverse user population forced the VCL team to adopt multiple authentication methods, most frequently tying to the user's home campus's LDAP environment. Eventually the VCL team Shibbolized the service to support a wide range of users with diverse computing needs across the UNC system. Since NCSU belonged to both the UNC-IdF and InCommon, the VCL team created SPs for both federations, enabling individuals from both the UNC and K-16 communities to access the VCL with their current credentials. (See <http://vcl.ncsu.edu/> for more information.)

### **Electronic Proctoring**

East Carolina University (ECU) currently offers 73 online degrees and approximately 1,400 online courses. Obviously, some form of exam proctoring is essential in online programs to give students, faculty, and accreditation bodies confidence in the student evaluation process. Unfortunately, this is much easier to say than to do. For example, the faculty of ECU's College of Business, which enrolls approximately two-thirds of its 600-member student body online, found that proctoring exams for so many widely scattered students had become unmanageable. Their problem filtered up to Senior VP Alan Mabe, who then charged IR to find a technology-based solution.

IR responded with an electronic proctoring application, released in August 2010. The application incorporates the federated identity/web services back-channel platform to identify a course's instructor and students and enable them to exchange relevant course information for exam notification and to schedule exams online at an approved test proctoring site. Federating the application further supports the UNC Board of Governors' cross-institutional online education initiative as recommended by the UNC Tomorrow Initiative. (See <http://services.northcarolina.edu/> for more information.)

## **Single Sign-On or Intracampus Federation**

With the UNC-IdF in operation since 2008, campus IT organizations have gained expertise in Shibboleth-based federated identity management. Growing confidence and expertise now encourages the extension of the federation—and its benefits—to intracampus applications, creating a single sign-on environment for them. Indeed, that is what IR envisioned when it created UNC's interinstitutional federation. "I really see

federation as a longer-term effort, using the UNC-IdF as the means to start the campuses down the path to build their own single sign-on environments,” Hopper said.

Larger campuses such as NCSU and UNC-CH have the necessary resources to tackle intracampus federation on their own. (See sidebar “The University of North Carolina at Chapel Hill’s Intra-Institutional Federation Efforts” for one example.) But some medium to smaller UNC campuses use the UNC-IdF as a springboard for their internal efforts. At UNCG, Susan Hensley, director of systems, ITS, recalled that her IT organization was “interested in implementing Shibboleth, but we did not have a perfect project to make it happen. But the UNC-IdF project completed a lot of the Shibboleth backend work and helped us lay out a road map to expand this to our campus. It jump-started our initiative to implement IdM in a more standard way.” Now UNCG ITS plans to build a central portal for single sign-on, and it created middleware engineer and middleware administrator positions to build SP functionality into campus applications.

### **The University of North Carolina at Chapel Hill’s Intra-Institutional Federation Efforts**

UNC at Chapel Hill (known affectionately as Carolina, but abbreviated as UNC-CH here) consists of 14 schools, the College of Arts and Sciences, and the William and Ida Friday Center for Continuing Education. UNC-CH’s Information Technology Services (ITS) organization manages the university’s telecommunications and networking infrastructures as well as its academic and administrative applications and services. ITS maintains a five-person Identity Management department.

UNC-CH’s highly decentralized IT environment creates an organizational dynamic between ITS and the campus’s schools and colleges similar to that between the UNC General Administration and the UNC campuses. UNC-CH’s schools and colleges may create applications to meet their specialized requirements, as for example the Office of Research Information Systems’ RAMSeS research administration management system. This decentralized environment complicates ITS’s identity management efforts.

ITS has in-house technical expertise with Shibboleth—one of its Identity Management department staff members contributes source code to Internet2’s Shibboleth project. The technical advances associated with the release of Shibboleth 2.0 and SAML 2.0 “created the perfect storm to develop a web-based single sign-on environment at our campus,” recalled Jan Tax, systems specialist at UNC-CH. ITS developed an intracampus federation, using Shibboleth as its default sign-on mechanism. The Identity Management department is directly responsible for maintaining the intracampus federation; that means running the identity provider virtual appliances for UNC-CH’s central IT organization, maintaining those devices for local authentication purposes for certain applications such as Blackboard and consulting with campus areas to implement service provider functionality. The same identity can be federated on the campus and externally to the UNC Identity Federation as well.

*Cont’d*

Several major UNC-CH applications are federated, including the Connect Carolina PeopleSoft ERP system, Blackboard, Sakai, the MyUNC campus portal, several student affairs applications, and the libraries' electronic proxies. The ITS staff's expertise enables them to Shibbolize some commercial software applications that are not usually federated. They modified Blackboard's native Shibboleth capability to function within the UNC-CH IT environment, and they added their own source code to PeopleSoft to handle all the required authentication values and attributes. UNC-CH's intracampus federation is very active, with ITS reporting a backlog of departments wanting to Shibbolize their applications.

There is one caveat with UNC-CH's intrainstitution federation strategy: Shibboleth's web-based orientation. This presents a problem for UNC-CH's non-web legacy applications. There is no easy way to create the appropriate interface between the two environments because it "flies in the face of Shibboleth," stated Celeste Copeland, identity management manager, UNC-CH. "It is really apples and oranges." The Identity Management group is investigating solutions to this problem.

For those campus IT shops that desire more help, IR designed the intercampus federation in such a way that it can be applied to intracampus applications. "It is one of the design principles that we used when we built our federation manager software," Hopper said. "As other campuses move to single sign-on, there is no need for them to re-create a federation. We can provision a new federation, easily creating an intracampus federation for any one of our campuses with a click of a few buttons in our web-based management tool. We can maintain it centrally, too."

## External Federation

The UNC-IdF serves the campuses and entities of the University of North Carolina, but some UNC constituent institutions belong to two other federations—NC Trust and InCommon—to federate with entities external to UNC. Together with the UNC-IdF, these federations provide "new means to explore how far we can push the model for aggregating identity providers," stated UNC-CH's Tax. "It is an exciting time to explore the different possibilities." This section profiles NC Trust and InCommon, highlighting their interplay with the UNC-IdF.

### NC Trust

MCNC, an independent nonprofit networking technology and services organization serving North Carolina's K-20 education community, formed the Federated Identity Management Task Force (FIM TF) in fall 2007 to strategize about the sharing of web-based resources across the North Carolina education community. FIM TF eventually launched the NC Trust pilot, a statewide identity federation for universities, community colleges, K-12 schools, and government organizations. Nine members make up NC Trust, including NCSU and UNC-CH.

Like the UNC-IdF, NC Trust's technologies are based on the Shibboleth and SAML 2.0 platform. But unlike the UNC-IdF, NC Trust uses InCommon's predefined policies and practices framework because NC Trust participants represent many different types of legal entities. Thus, NC Trust members must also belong to InCommon.

Lacking the board of governors' mandate that spurred UNC's federated identity projects, "the identification of service providers for universities, community colleges, and school districts to authenticate against or to access resources from was an initial challenge for NC Trust," stated Mark Scheible, security and compliance manager, NCSU, and FIM TF co-chair. Eventually FIM TF chose NCLive, a library consortium consisting of UNC, community colleges, private universities, and public libraries, which provides free access to e-books, audiobooks, videos, online magazines, newspapers, and journals.

The UNC-IdF interoperates with NC Trust. For example, to provide access to its videoconferencing services, MCNC is part of the UNC-IdF's affiliates' federation. An individual UNC campus videoconference coordinator, using his or her UNC home campus credentials, can log in to the MCNC website to set up and schedule videoconferences.

## InCommon

The Internet2 Middleware Initiative has been highly involved in the development of federated identity's technical framework, including the Shibboleth and SAML components. Through its creation of the InCommon Federation, it took the next step by providing a policy and practice framework in the Shibboleth/SAML environment. InCommon 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 federate with its diverse membership base. (See <https://spaces.internet2.edu/display/InCCollaborate/Information+from+InCommon> for more information.)

The InCommon Federation encompasses more than 250 higher education institutions, government agencies, nonprofit research entities, and sponsored partners.<sup>8</sup> Currently four UNC campuses—ECU, NCSU, UNC-CH, and UNCG—belong to InCommon. InCommon membership gives researchers at these institutions easy access to NIH and NSF resources via their campus credentials. The growing vendor community in the UNC-IdF and InCommon offers opportunities to accelerate the federation of commercial applications. UNC-CH's Tax acknowledged InCommon's role in enabling him to meet a two-week deadline to roll out a course evaluation system, usually a six-week process. Because both UNC-CH and the vendor belonged to InCommon, his work was streamlined. "To make it work involved numerous phone calls to enable the release of a couple of attributes that we do not release by default," he recalled. "Normally, we'd create a custom authentication schema, but the solution was literally in place." Now he checks both federations' membership lists routinely for new application implementations. If a vendor belongs to neither federation, he approaches IR to discuss the feasibility of the vendor's joining the UNC-IdF.

A recent InCommon member, UNCG joined to facilitate access to library resources. Beyond that, UNCG's Hensley sees InCommon as "a next step [in our IdM strategy]. We

can reach beyond UNC schools to share resources, and we are still evaluating ways to use our membership most advantageously.” Interestingly, IR’s strategy to incorporate technical (Shibboleth and SAML) and trust (InCommon) standards in the UNC-IdF facilitated UNCG’s InCommon membership. “The UNC Identity Federation completed the groundwork, so joining InCommon wasn’t a large step,” explained Hensley.

## Next Steps

IR’s goal is continued support for identity federation’s seamless school-to-school integration. “People are starting to understand the benefits, especially when they see how IR can deliver centrally developed and deployed applications to the entire system ‘in one fell swoop,’” Hopper remarked. “They are starting to see the power. As we continue to Shibbolize more and more, it opens the door to do more efficient application implementation.”

User requirements will continue to guide the UNC-IdF, much like internal demand drove the federation of Inter-Institutional Course Registration, RAMSeS, and electronic proctoring. Future plans may include federating an electronic mentoring program developed in partnership with NCSU to connect people involved in industry with graduate and undergraduate students. The application’s first focal area will be the professional master’s programs, with the ultimate goal of offering it to all UNC campuses through the UNC-IdF. Student aid is another possible area to enable users and campuses to share information, especially to support cross-institution online course enrollments. “It will be driven by need or demand. The idea of online mentoring could take off in a lot of different ways,” stated Mabe.

Not all applications in the UNC-IdF are internally developed; two commercial entities, with another two on the horizon, belong to its affiliate federation. Two barriers exist to federating commercial applications in the UNC-IdF. The first is the vendor’s willingness to Shibbolize its product, since this a basic requirement for joining the UNC-IdF. A prime example is ERP systems. Most UNC constituent institutions use the same ERP vendor, but these applications cannot be federated until they are Shibbolized. IR is reluctant to tackle this task itself due to ongoing maintenance issues, knowing that a vendor-supported solution would be more viable in the long term. Vendors’ reluctance may correspond to the proportion of revenue generated from the higher education market; Shibboleth is currently deployed mainly in higher education environments, and higher education represents only a small portion of many vendors’ revenues.

The second barrier involves licensing agreements. Current vendor agreements may not consider federated identity’s interorganizational nature. For example, online library resources may restrict access to a specific institution’s identifiers, requiring users from other federation members to create a separate set of credentials to access those resources, despite the presence of the federation’s trust framework. “You can federate all you want, but there is a blockage if content is restricted to a specific subset of the federation,” stated Tax.

Working closely with vendors may encourage such action; IR continues to talk with ERP vendors about Shibboleth-enabling their applications. But market forces

may prove to be a forceful incentive. As more vendors affiliate with federations like UNC-IdF or InCommon, Shibbolizing applications or renegotiating licenses may become prerequisites to remaining competitive in the higher education marketplace. Such a transformation could be occurring already. When the UNC-IdF came online in 2008, IR had to coax vendors to Shibbolize their applications; today, UNC-GA's Hopper noted a growing inclination among some software vendors to accommodate the federation's requirements.

Leydon believes that greater vendor participation will encourage the formation of more federations by increasing the number of compelling user cases. "Systems and their institutions can evaluate different vendor software in a more specific way and determine whether it is beneficial for them to federate."

## Lessons Learned

IR's experiences with the UNC-IdF offer numerous lessons learned for other higher education entities to consider when planning their federated identity strategies.

### *Identify an application on which to federate.*

Federated identity facilitates resource sharing, but identifying a compelling application that justifies the start-up costs of federation may be a challenge. "You need the application to drive the federation because the reverse is not going to happen," stated Leydon. For example, NC Trust had a defined mission to federate K-20 schools but struggled initially to find that compelling application. At UNC, the Inter-Institutional Course Registration application mobilized the university into action. "Federated identity technology would be of great advantage to my IT organization, but my problem was determining with what application and with whom I would collaborate to get this started," stated Hensley. "An institution by itself may have a difficulty there; it needs another organization with which to federate. IR had a need that was central to all of our [UNC] institutions, and it was a perfect model to take advantage of federated identity."

### *Get buy-in.*

At UNC, the president and board of governors were involved at the outset, presenting IR with a mandate to implement the Inter-Institutional Course Registration application, which in turn spurred the decision to federate. This high-level mandate helped IR to keep the project moving at individual UNC campuses. Not every fledging federation will possess such a strong top-down mandate, so it will behoove the federated identity project manager(s) to gain that senior-level support to facilitate members' implementations. Creating the required trust framework will most likely require the participation of high-ranking institutional officers, such as the general counsel. This will most likely require educational efforts to introduce the concept of federated identity and its benefits to a nontechnical audience. In addition, IR worked closely with UNC's CIO Council throughout the project, especially with federation governance, to maintain involvement and buy-in at each UNC campus IT organization.

***Identify a project catalyst.***

Several case study participants described the importance of having UNC's IR organization serve as the project catalyst that drove the federation's technical and policy implementations and then extended these to the UNC campuses. IR filled this role naturally because of its mission to complement individual UNC campus IT activities. Other federation initiatives may not possess such an obvious focal point and should address this requirement up front.

***Consider federation members' varying IT resources.***

The virtual appliance IR developed to facilitate the IdP role turned out to be a huge win for the UNC-IdF. IR completed the arduous implementation task for several UNC IT campus organizations by configuring the "IdP in a box" up front. The IT campus organizations' main task was to connect it directly into their networks. This strategy enabled smaller IT shops that lacked the resources and/or IdM expertise to get their IdPs operational by the Inter-Institutional Course Registration project's deadline.

IR continues to assist smaller IT shops by monitoring the virtual appliances remotely and providing technical support as needed. As campus IT shops move to create intrainstitutional federations (in support of single sign-on), they can apply locally many of the scripts and tools IR developed for the UNC-IdF or rely directly upon IR to create an intrainstitutional federation for them.

***Focus on the nontechnical benefits.***

Identity management is by nature a rather technical endeavor, and it is very easy for IT organizations to become engrossed in IdM's technical "nuts and bolts" at the expense of communicating its benefits to the organization at large. To gain support for the UNC-IdF, IR positioned federated identity as part of a larger centralized web services development strategy that included the web services backchannel, a concept that a nontechnical person might grasp more easily. "The light bulbs went off depending upon their actual usage or direct benefits," stated Leydon.

***Develop a formal application selection process.***

A system-wide or consortial federation needs a driving application to impel it, but adding subsequent applications enhances its value further. At UNC, the Inter-Institutional Course Registration application propelled the UNC-IdF, but later apps became federated more or less randomly. UNC Online provided some further application opportunities, but other application initiatives came about more informally from personal interaction between IR and individual campuses and entities. The collaborative nature of UNC campus IT organizations fostered such an approach, but other federations might want to consider a more formalized strategy in accordance with their organizational cultures.

***Don't overlook policy.***

As with many IT projects, it is easy to focus on the technical implementation at the expense of policy and governance, but with federated identity, formal develop-

ment of the actual trust framework of policies and practices is just as important. As Hensley suggested, “A technical implementation like this is actually the simple part. There is a lot of process that needs to be defined before you move into actually doing it.” Indeed, in ECAR’s recent IdM survey, 47% of respondents who had implemented a federated identity solution described policy/process issues as more challenging than technical issues, and another 38% said that policy and technical issues were equally challenging.<sup>9</sup>

As a single legal university entity, IR opted to create its own framework for the UNC-IdF, adapting the InCommon policies. On the other hand, to accommodate its diverse constituency, NC Trust decided to require its members to join InCommon and use that federation’s trust framework. Policy work may extend to the review of vendor licensing agreements to ensure they consider federation’s interinstitutional nature when defining user access, as illustrated by UNC-CH’s issues with its library resources.

### *Work closely with vendors.*

Not all applications in the UNC-IdF are internally developed, and IR continues to reach out to vendors to educate them and persuade them to join its federation. As more vendors opt to Shibbolethize their applications, a more conducive environment for federated identity is created.

## **Conclusion**

In 2008, UNC’s Information Resources unit created the University of North Carolina Identity Federation in response to the UNC Board of Governors’ call to action to respond to challenges in the UNC Tomorrow Initiative. Specifically, IR’s identity federation had a clear and immediate purpose: to solve authentication issues related to UNC’s interinstitutional online course registration application. During the interviews for this case study, personnel from UNC repeatedly emphasized the significance of having a driving initial application for the federation. Without it, the project could have wandered in search of a task; with it, UNC campuses were able to work together to create the UNC-IdF and begin to plan for future federated identity activities.

Subsequently, both internal and external applications of federation have developed. UNC-CH, for example, has initiated an intracampus federation to facilitate single sign-on for many institutional applications. Externally, the UNC-IdF interoperates with other federations, including NC Trust and InCommon, to create bridges rather than barriers. Current outreach efforts aim to encourage vendors to participate in the UNC-IdF by building Shibboleth capabilities into their software offerings.

Development of the UNC-IdF has been accomplished in a relatively short time, and much of its success has been achieved through careful planning, responsive participants within the UNC and its campuses, and significant attention to external efforts such as InCommon. The effort has achieved shared purposes and brought together diverse communities while maintaining the independence of the UNC campuses.

## 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. *Ibid.*, 9.
4. EDUCAUSE, “7 Things You Should Know about Federated Identity Management” (September 10, 2009) (Boulder, CO: EDUCAUSE, 2009), 1, <http://net.educause.edu/ir/library/pdf/EST0903.pdf>.
5. Sheehan and Bennett, *Identity Management*.
6. University of North Carolina Tomorrow Commission, “Executive Summary,” December 2007, 2, available at <http://www.northcarolina.edu/nctomorrow/execsummary.pdf>.
7. *Ibid.*, 2.
8. InCommon, “InCommon Participants,” <http://www.incommon.org/participants/>.
9. Sheehan and Bennett, *Identity Management*.

## Citation for This Work

- Pirani, Judith A., and Bob Albrecht. “Federating the University of North Carolina: Origins and Benefits” (Case Study 2). Boulder, CO: EDUCAUSE Center for Applied Research, 2011, available from <http://www.educause.edu/ecar>.