Internet2

TIER Workshops - Participant User Stories

Catalog Document (All Workshops)

TIER Project Team

4-11-2015

Table of Contents

Arizona State University (001.asu.1.20150412)

Modified: 4/12/2015 1:46:20 PM

Participants

CIO or CIO Delegate

Workshop 2	*Gordon Wishon*
Workshop 3	*Gordon Wishon*

Senior Identity Architect

Workshop 2	*Vince Boragina*
Workshop 3	*Vince Boragina*
Workshop 3	*Vince Boragina*

Other Institutional Identity Needs

Workshop 3	*Jack Hsu*
Workshop 3	*Jay Steed*
Workshop 3	*Nate Wilken*
Workshop 2	*Tina Thorstenson*
Workshop 3	*Tina Thorstenson*

Continuing Research with a PhD Candidate

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
External collaborator or contractor
Alumni

Story Narrative:

Alumni do have access to certain ASU systems and information, but it mainly pertains to their educational history and related resources. In this particular case, an ASU alumni obtains his/her PhD and graduates from ASU but is still working with his former faculty research advisor.

The recent alumni needs more access than the normal Alumni affiliation system rules provide. The ASU faculty member and his former student, now at UGA, need to share files and collaborate to continue their research. For this case, due to the systems being accessed, we added an additional “Courtesy Affiliation” to the PhD/alumni’s account. This creates, or re-activates, a second digital ID (account) that can be used to access the needed information. We can then deactivate this account later when the collaboration ends, and the alumni can continue to access their information with their “alumni” account.

Arizona State University (002.asu.2.20150412)

Modified: 4/12/2015 1:44:25 PM

Participants

CIO or CIO Delegate

Workshop 2	*Gordon Wishon*
Workshop 3	*Gordon Wishon*

Senior Identity Architect

Workshop 2	*Vince Boragina*
Workshop 3	*Vince Boragina*
Workshop 3	*Vince Boragina*

Other Institutional Identity Needs

Workshop 3	*Jack Hsu*
Workshop 3	*Jay Steed*
Workshop 3	*Nate Wilken*
Workshop 2	*Tina Thorstenson*
Workshop 3	*Tina Thorstenson*

Parent-Guest Account Access

Actors

Home Organization
Parent/Guest

Stakeholder Groups

Learner/Student
Parents/Guests

Story Narrative:

Parents frequently need a level of access to their child's information to pay bills, assist with basic housing and campus life issues. We needed a way to grant parents access to parents and make sure we allowed the students to have control of their FERPA information.

Due to the systems being accessed for grading, bills and housing, we needed to grant the parents a PeopleSoft ID (EMPLID) and subsequent electronic persona in an on-demand, self-service fashion. We did not have a mechanism for this at the time. Up to this point, ASU only created accounts through employment, student application/admittance, or manually.

A mechanism was developed that allowed students to send an authentication code to a parent's email address. The parents would use the code to create, or re-enable an existing account if one existed, so that they had access to the student's portal pages (called MyASU). The student maintains the authorization control to give access to basic functions, bill payment, housing, grades, etc…. The system has been a success. Its only downside is that it is very conservative when search-matching existing electronic identities and will create duplicate accounts in PeopleSoft and thus duplicate electronic personas. These duplicate IDs have to be manually cleared up later.

Arizona State University (003.asu.3.20150412)

Modified: 4/12/2015 1:45:36 PM

Participants

CIO or CIO Delegate

Workshop 2	*Gordon Wishon*
Workshop 3	*Gordon Wishon*

Senior Identity Architect

Workshop 2	*Vince Boragina*
Workshop 3	*Vince Boragina*
Workshop 3	*Vince Boragina*

Other Institutional Identity Needs

Workshop 3	*Jack Hsu*
Workshop 3	*Jay Steed*
Workshop 3	*Nate Wilken*
Workshop 2	*Tina Thorstenson*
Workshop 3	*Tina Thorstenson*

Application ID to ASU ID

Actors

Individual User
Home Organization

Stakeholder Groups

Learner/Student

Story Narrative:

A student applicants first fill out an application with ASU using an ID that is not held within the normal ASU IDM system. An account notification email is sent to the student. The student can use their “application account” (persona) to edit the application until it is complete. Once complete, the application is submitted and a record is created in suspense tables within PeopleSoft. A search-match runs systematically to see if an ID for the person exists in the system. If not a new ID is created.

The student is then sent another account activation email, to the email address used in the application process, for the main ASU account they will use for their application review process and through their entire ASU lifecycle. When the student generates an ASU account they receive the @asu.edu email address and it is placed on their bio-demo record in PeopleSoft. Students may choose to automatically have email forwarded to another non-ASU email address. Ultimately, one account for the entire process would be less confusing to constituents.

Baylor University (004.baylor.1.20141205)

Modified: 12/5/2014 9:33:19 AM

Participants

CIO or CIO Delegate

Workshop 1	*Pattie Orr*

Senior Identity Architect

Workshop 1	*Jon Allen*

Struggles with Service Providers and Federation

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Vendor who recently joined InCommon

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
ITS and department licensing service

Story Narrative:

Baylor University contracts with a service provider to use a new cloud application. As part of the agreement, Baylor sponsors the service provider into the InCommon federation. Generally the service provider has knowledge of SAML federated authentication. Sadly more often than not Baylor ITS staff spends a significant amount of time getting the service provider up to speed on how to implement Shibboleth with the InCommon federation. Even worse some service providers insist on using assertions outside of the InCommon metadata to complete the federated authentication implementation.

Baylor University (005.baylor.2.20141205)

Modified: 12/5/2014 9:33:37 AM

Participants

CIO or CIO Delegate
Workshop 1   *Pattie Orr*

Senior Identity Architect
Workshop 1   *Jon Allen*

Two Factor with Shibboleth

Actors

Individual User
Home Organization – Campus Departments and ITS
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Baylor University has a moderate number of federated service providers authenticating via InCommon. We have reached the point from a risk perspective that we want to implement two factor authentication using DUO for some of the service providers that contain more sensitive information. Sadly, the current state of Shibboleth requires two additional open source modules separately maintained to complete this desired level or authentication. While possible this becomes risky for a high utilization and uptime systems. This is even more of a concern as we do not have a dedicated identity management staff. The desire would be to have Shibboleth include these functionalities as a base supported service. Ideally a Net+ authentication vendor should easily integrate with Internet2 InCommon authentication services.

Boston University (006.bu.1.20150412)

Modified: 4/12/2015 2:01:40 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Schroeder*

Senior Identity Architect

Workshop 3 *Vlad Grinman*

Two factor authentication with Duo

Actors

Individual User
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Information Security

Story Narrative:

Professor Johnson is ….. doing research in the area of …..

He wishes to check the status of his research grants.

Professor Johnson accesses Boston University BUworks SAP Portal using his browser.

He provides his Boston University Kerberos username and password and then gets prompted for second factor authentication, which is a mandatory requirement for access to the BUworks Portal.

Professor Johnson selects “push notification” as an option for second factor authentication and opens his Duo Security app on his mobile phone. He presses the green button when prompted and gets access to BUworks SAP Portal.

After finishing his grant work, Professor Johnson decides to check his students’ progress on a homework assignment for the class he is teaching at Boston University. He accesses Boston University Blackboard web-site and gets access without providing any credentials, since Boston University Blackboard web-site is protected by Federated authentication that uses the same Shibboleth IdP as BUworks Portal.

Professor Johnson identifies several students who are having difficulty with the homework and decides to approach their Faculty advisers. To find out who these advisers are, Professor Johnson accesses Boston University Faculty Link web Portal. He gets prompted for his Boston University Kerberos username and password again because the Faculty Link Portal is protected by institutional custom WebLogin application that is not federated.

Professor Johnson approaches IS&T and asks if his access to the Faculty Link could be made as seamless as his access to Blackboard. He also points out that when he first accesses Blackboard and authenticates using his Boston University Kerberos username and password only (second factor authentication is not required to access Blackboard), and then switches to BUworks Portal, he gets prompted for his Boston Kerberos username and password again.

To simplify Professor Johnson's work Boston University IS&T plans to convert the Faculty Link to use Shibboleth Federated authentication. This project requires replacement of Boston University's custom web session management system, which is integrated with WebLogin and has provisioning for capturing Kerberos Ticket Granting Ticket (TGT), which will be necessary to access Mainframe based APIs. Current Shibboleth implementation has "out of the box" integration with Kerberos authentication, but doesn't have a configurable option to return TGT.

IS&T also plans to upgrade Shibboleth implementation at Boston University to version 3.x which has provisioning for Multi-Context Broker (MCB). After the upgrade Professor Johnson will be able to skip the Kerberos prompt in the case when he accesses BUworks after already being authenticated through Blackboard. Professor Johnson will be asked to provide only second factor authentication through Duo Security.

Boston University (007.bu.2.20150403)

Modified: 4/3/2015 8:13:48 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Schroeder*

Senior Identity Architect

Workshop 3 *Vlad Grinman*

Office 365 Authentication

Actors

Individual User
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Information Security

Story Narrative:

Professor Richards is ….. doing research in the area of …..

As a member of one of the IS&T Governance committees he wishes to prepare for the upcoming meeting by reading some documents that were published on the committee's SharePoint web-site.

Professor Richards accesses Boston University Office 365 SharePoint web-site using Firefox browser on Windows PC computer in his office. He gets access without providing any credentials, since Boston University Office 365 SharePoint web-site is protected by Federated authentication that uses the ADFS server, which runs on the BU Network and is capable of picking up credentials from any computer that joins the Boston University Active Directory (AD) domain.

After he finishes reading the governance committee documents, Professor Richards decides to post a new homework assignment for the class he is teaching. He accesses Boston University Blackboard web-site and gets prompted for his Boston University Kerberos username and password because the Blackboard web-site is protected by Federated authentication that uses the Shibboleth IdP, which is not integrated with ADFS.

Professor Richards approaches IS&T and asks if his access to the Blackboard web-site could be made as seamless as his access to SharePoint. He also points out that when he uses the Chrome browser on his office Windows PC, or on his MacBook, to access the SharePoint web-site, he actually gets prompted to identify himself as a Boston University affiliated person by providing his institutional email address. He then gets prompted for his Boston University Kerberos username and password and this prompt looks different from the Blackboard prompt for authentication.

To simplify Professor Richards's work, Boston University IS&T plans to re-configure our ADFS server so it will use Shibboleth IdP for authentication. The Professor's challenges with the Chrome browser and with his MacBook will be quickly addressed by the Help Center by adding necessary settings and offering to add his MacBook to the Boston University AD domain.

Boston University (008.bu.3.20150412)

Modified: 4/12/2015 2:02:16 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Schroeder*

Senior Identity Architect

Workshop 3 *Vlad Grinman*

Access to High Performance Computing Resources in the MGHPCC

Actors

Individual User
Service Provider

Stakeholder Groups

Researcher/Scholar
Information Security

Story Narrative:

Professor Peterson is doing research at Northeastern University in the area of …. He wants to use high performance computing resources in the Massachusetts Green High Performance Computing Center (MGHPCC) that are hosted by Boston University. Professor Peterson opens the Boston University TechWeb quick start guide for Shared Computing Cluster (SCC) and finds that he needs to establish an account with Boston University and then use this account to authenticate to SCC.

Professor Peterson approaches Boston University IS&T and asks if he can use his Northeastern University credentials to authenticate to SCC. He also mentions that he would currently need to establish one more account and password to access regional computing resources like Massachusetts Life Sciences Center (MLSC) cluster on MGHPCC. The same is true for national computing resources like the NSF Extreme Science and Engineering Discovery Environment (XSEDE) cluster. He describes a scenario when someone is computing on a couple of different platforms and then wants to move data between the systems using Globus Online, which requires yet another identity.

Boston University IS&T already did set up our Globus Online endpoint so that it uses Shibboleth for the authentication, but at this moment we can't address Professor's Peterson requirements and is interested if TIER can provide a solution for his case.

Carnegie Mellon University (009.cmu.1.20150412)

Modified: 4/12/2015 2:03:09 PM

Participants

CIO or CIO Delegate
Workshop 3 *Steve Huth*

Senior Identity Architect
Workshop 3 *Michael Gettes*

Modifying Duke's Extended Identity Lifecyle

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Alumni/Exceptional Donors/Friends of

Story Narrative:

CMU should follow Duke for the short presentations.

CMU agrees with the overall Duke Extended Identity Lifecycle with some questions and concerns added on top. Duke's premise is that social identities should be linked to the institutional identity and that social identities will be stable and live as long as our institutions. Predicting the future is always hard and we are not going to say whether or not this is going to happen. But, what if it doesn't? Many companies have come and gone (or are going) with large communities that can play into this concern. Myspace came and went, AOL is going and we can all names dozens where the concerns exist.

We would modify the Duke Lifecycle story to give John a real CMU identity as soon as is practical and note his Facebook or other identity to be used in providing self-service password resets. Of course, with some vetting of external identities, these externals can come and go and the real identity survives – which also provides a level of stability in the technology used by the hundreds or thousands of applications viable for use by the institution. We would also have the CMU identity live beyond the primary years at CMU and be sure to provide services of interest to keep the eyeballs coming back so the identity is useful and limit the need for password resets. The lifelong relationship is fundamental to the giving process and desirable by Alumni relations at CMU and every other institution of Higher Education.

Furthermore, this notion of extending the lifecycle goes beyond the academic affiliation.   We believe it applies to anyone issued an identity. They should have, with no other formal affiliation, a basic authentication account used for web based services (SSO), for those non-enterprise based uses like wiki collaborations and interim cases like staff needing access to tax data, students wanting access to transcripts, and so on.

Carnegie Mellon University (010.cmu.2.20150406)

Modified: 4/6/2015 1:00:35 PM

Participants

CIO or CIO Delegate

Workshop 3 *Steve Huth*

Senior Identity Architect

Workshop 3 *Michael Gettes*

Synergies – AKA Conservation of Writing

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Having read through the remaining Duke stories, all 9 (extending identity lifecycle excluded), CMU is in favor of Duke's perspective. As we understand, the key product out of the TIER workshops is alignment of desires for future Identity related activities. This also has the interesting by-product of conserving the amount of writing by CMU. While CMU doesn't have the medical based needs of Duke, those medical needs translate to a variety of other common activities. The ideas are right from an Identity perspective.

Our deepest appreciation and thanks to Duke for the well thought out use cases.

Carnegie Mellon University (011.cmu.3.20150406)

Modified: 4/6/2015 1:00:49 PM

Participants

CIO or CIO Delegate

Workshop 3 *Steve Huth*

Senior Identity Architect

Workshop 3 *Michael Gettes*

Credential Management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

This isn't so much a story, but the initial definition of a need. CMU has developed a credential management system. Why? We had SIM and we have moved to OIM. As part of the transition, we have come to realize most, if not all, Identity Management systems supporting a password management (or Cred Mgmt) function manage the passwords in a reversible fashion. This means should an attacker gain access to the Identity Management product – then they will be able to find the keys and reverse ALL passwords for the institution. With this in mind, and recognizing there were a variety of other custom (but common) needs, we embarked on developing our own Cred Mgmt System (yes, yet another CMS) whereby passwords would only be maintained using a one-way hash.

The reason why products store reversible passwords is for when you want to bring on a new system where password sync is needed (no SSO, Kerberos or other capability exists for the app) then the Identity manager system only need propagate the passwords it knows on to the new system. Given how often this event happens, we decided it was needed and should it be needed, asking the community to perform a password change wouldn't be so hard – politically, annoying, yes. CMU does password sync to Kerberos (Heimdal) and to AD.

Among the above mentioned features, other features we have added are:

Password changes (doh!)

Provisioning passwords using SIM or OIM to handle provisioning to the target system where needed and then removing the password from the provisioning system.

Password history

Passwords are stored as one-way hash

Google: for IMAP and other clients, a password needs to be assigned to the google account. We support this for multiple google domains. The user logs in using SSO and can manage their “other” passwords.

Supports multiple AD domains.

First Pass Coupon – for initial credential distribution, we use a coupon mechanism to allow people to establish their initial password.

Administrative password resets. Communities of people are in grouper and those who can perform resets are also in grouper. An “admin” group can reset a constituency group.

Eventually, token management will be part of our cred mgmt system.

Password Expiry and notifications. We have a modification on Heimdal Kerberos to detect an expired password and via Shib, force the user over to credMgmt.

Password strength requirements. Can apply different requirements for different communities of people (group driven).

Security Questions for self-service password reset

Support for forced password changes on communities of users (such as 90 day regular password changes – communications/reminders by email).

Password strength feedback on web UI for password changes

Administrative UI

Integrates with ActiveMQ

There are probably other features we have implemented but failed to recall.

Case Western Reserve University (012.case.1.20150127)

Modified: 1/27/2015 8:24:41 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Can We Get Rid of Passwords?

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Today we have many problems related to the use of passwords. Passwords are often chosen poorly. Passwords are sometimes shared with others. Passwords are sometimes phished. Passwords are sometimes stolen. Passwords are sometimes forgotten. The business processes associated with password management are sometimes complex. A large percentage of our Help Desk tickets still revolve around problems with passwords. Can we get rid of or at least reduce the use of passwords?

Case Western Reserve University (013.case.2.20150127)

Modified: 1/27/2015 8:24:14 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Identity Management as a Service

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

We no longer want to operate, maintain, or update the software and infrastructure required to support the local identity management system and would rather use identity management as a service.

As the central information technology service provider for our university, our role and responsibility is to support the primary mission of the University, which is research and education. Today we devote considerable resources and expertise to operate and maintain a local identity management system. We would rather reduce the amount of resources devoted to supporting the local identity management software and infrastructure and repurpose those resources towards more direct support of the University's mission.

Our experience with other critical central systems which have been moved to software as a service has shown us that there are many tangible benefits to moving a service system to a software as a service model, including but not limited to better reliability, better performance, quicker paths to improved features and capabilities, less risk for disasters, and more satisfied customers.

Case Western Reserve University (014.case.3.20150127)

Modified: 1/27/2015 8:24:05 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Certificate Management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

The management of digital certificates is still difficult, particularly for personal use. We need to develop a set of best practices and tools to help us successfully use and manage personal digital certificates. There are a variety of applications where being able to utilize digital certificates would improve functionality, ease of use, and security.

Case Western Reserve University (015.case.4.20150127)

Modified: 1/27/2015 8:23:37 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Are You Who You Say You Are?

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Today we have a complex web of practices for people to provide evidence that they are who they say they are. As identity providers at our university, we don't have visibility into the specific mechanism that individuals use to prove identity. That makes it difficult to assure others that a person is who they say they are when they use a University identity.

For identity assurance purposes, it would be helpful to have a set of best practices and standards to follow. It would be helpful for users and identity providers if there were an identity assurance broker where the user could prove their identity once to the broker and then the broker could provide future assurances that the individual is who they say they are.

Case Western Reserve University (016.case.5.20150127)

Modified: 1/27/2015 8:23:57 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Best Practices

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

There are many complex aspects of identity management. It would be very helpful to have a comprehensive identity management best practices document for higher education. This will help save time and resources that we would spend reinventing solutions that others have discovered and found effective.

Case Western Reserve University (017.case.6.20150127)

Modified: 1/27/2015 8:24:22 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Can I Use My Preferred Identity Instead Of Getting a New One?

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Some number of users have raised the question of whether they can use a preferred identity they already possess from another service or institution rather than getting a new one from us. Can we support the use of identities other than the one we provide? (eg, Facebook, Google, Twitter, Microsoft, etc).

Case Western Reserve University (018.case.7.20150127)

Modified: 1/27/2015 8:24:32 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Support Additional Federation Protocols

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Support additional widely used standard authentication and authorization protocols for federation. For example, support OAuth in addition to SAML (Shibboleth).

Case Western Reserve University (019.case.8.20150127)

Modified: 1/27/2015 8:24:48 AM

Participants

CIO or CIO Delegate

Workshop 2 *Sue Workman*

Senior Identity Architect

Workshop 2 *Jeff Gumpf*

Support Transactional Integration with ERP

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Our current IdM system generally receives/sends batch files when interacting with the ERP systems. Service would be more timely if the interactions occurred on a transactional basis rather than a batch basis.

Case Western Reserve University (020.case.9.20150127)

Modified: 1/27/2015 8:24:54 AM

Participants

CIO or CIO Delegate
Workshop 2 *Sue Workman*

Senior Identity Architect
Workshop 2 *Jeff Gumpf*

User IDs

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Today we regularly have people question us about the assignment of userIDs. For our institution, it is an 8 character id which conforms to a specific set of rules. Users have indicated that they would like other choices such as longer IDs, the ability to choose their own IDs, the ability of their IDs to be in their own character set (eg, Chinese, Korean, Japanese, Arabic, etc and not just ASCII).

Clemson University (021.clemson.1.20150412)

Modified: 4/12/2015 5:59:07 PM

Participants

CIO or CIO Delegate
Workshop 2 *Jill Gemmill*

Senior Identity Architect
Workshop 2 *Billy Cook*

Shared Use of University Managed Resources Across Institutional Boundaries

---

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Professor X has a project that requires use of a Hadoop cluster at Clemson, a high performance computing cluster at University of Utah; moving data between those two locations; and using the Science DMZ to assure fast and reliable transfer. He has collaborators at institutions in addition to the two named here; they and their students will also be participating in this project.

Clemson University (022.clemson.2.20150412)

Modified: 4/12/2015 6:00:05 PM

Participants

CIO or CIO Delegate

Workshop 2   *Jill Gemmill*

Senior Identity Architect

Workshop 2   *Billy Cook*

Better Management of Guest Accounts through Federation, credential vetting, and other means

---

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
External collaborator or contractor

Story Narrative:

Examples of persons who are provided Clemson Guest accounts today include:

- Professors who need to collaborate in an online course
- Summer camp students
- Alumni
- Fans of Clemson, Donors, etc.
- Parents (easier because we can have them verify their identity based on info about their child)

Biggest problem is how to handle mixing in these identities with lower levels of assurance with the identities that originate from the student and HR systems. These are people who need or want to have some kind of access into Clemson systems but have been traditionally given access to everything via a generic guest account. Some kind of identity vetting process is needed for people who we will never see in person--maybe something like banks use that asks questions about cars and property you owned previously.

I think we have the tools needed to build the system except for a service like banks use for questions about property. Going in another direction, Facebook makes sure you can identify people from pictures shared with you by friends.

Clemson University (023.clemson.3.20150412)

Modified: 4/12/2015 6:00:19 PM

Participants

CIO or CIO Delegate

Workshop 2 *Jill Gemmill*

Senior Identity Architect

Workshop 2 *Billy Cook*

We already do not own identities we've issued

Actors

Individual User

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student

Story Narrative:

Unfortunately, email address has become your identity in most cloud services. Many people use their institutional email address. So, when we cut off email access when a person leaves the institution, we are cutting them off from cloud services they own.

Cornell University (024.cornell.1.20150309)

Modified: 3/9/2015 1:59:18 PM

Participants

CIO or CIO Delegate

Workshop 3 *Dan Hawryschuk*

Story 1: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Cornell University (025.cornell.2.20150309)

Modified: 3/9/2015 1:59:20 PM

Participants

CIO or CIO Delegate

Workshop 3 *Dan Hawryschuk*

Story 2: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Duke University (026.duke.1.20150412)

Modified: 4/12/2015 2:37:34 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Extending the Identity Lifecycle Bi-directionally

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Alumni, Retirees, Applicants, Prospects, pre-college students

Stakeholder Groups

Researcher/Scholar
Learner/Student
Faculty/Instructor
External Collaborator / Contractor
Staff

Story Narrative:

The boundaries of electronic institutional identities continue to expand as institutions implement more proactive recruitment and development processes. IDM facilities must adapt to the wider identity lifecycle in order to provide a seamless user experience over a much broader lifecycle.

John is a high-school math prodigy living in Kansas when his parents enroll him in a Duke TIP program for gifted pre-college math students. TIP (the Talent Identification Program) is a Duke-affiliated pre-college program that enjoys the use of University computing resources for its summer programs.

As part of his enrollment, his parents provide some basic identifying information on his behalf. The TIP program's enrollment system uses a RESTful API to inform the institutional IDM about him, and the IDM in turn assigns a lightweight identity to him. He receives an email invitation to join the University's social-to-saml gateway, and chooses to register his Facebook account. His lightweight identity is automatically provisioned with access to the web-based, virtualized console interface used by his TIP class.

In mid-August, when his TIP program ends, his authorization to access the virtualized console system is automatically revoked, but his identity, along with his Facebook registration, remains on file.

Two years later, John visits the Admissions web site for information about applying to Duke. He opts to start an application directly from the Admissions web site, and enters some information to identify himself. The Admissions system uses the same RESTful API to determine that John's identity is already on record in the IDM system, and creates and associates an account at a cloud-based application management service for him, directing him to the social-to-saml registration site, where he's reminded that his Facebook account is already registered. He uses his Facebook account to log in and complete his undergraduate application.

John is accepted the following year, and matriculates in the Engineering School in the Fall. At matriculation, the IDM system automatically detects his status change, assigning him an affiliation of "student" and provisioning him with access to various Engineering School systems, as well as generic student systems throughout campus.

Just prior to his early graduation three years later, John receives a reminder that although his NetID will be deactivated following his graduation, his Facebook registration will remain active, and he'll continue to have access to various alumni systems, as well as to the Registrar's and Bursar's systems (for accessing transcripts, etc.). John uses his Facebook ID 18 months after graduation to log into the Registrar's system and request a transcript, which he shares with a prospective employer.

Three years later, John is a well-established PE at a major civil engineering firm in Texas. He logs into the alumni system to check in with some ex-classmates (again, using his Facebook account) and sees that he has a payment due on his annual pledge. He clicks the "make a pledge payment" link on his profile page, and is able to complete his donation without entering anything but particular payment information.

Duke University (027.duke.2.20150412)

Modified: 4/12/2015 2:37:52 PM

Participants

CIO or CIO Delegate

Workshop 3	*Tracy Futhey*

Senior Identity Architect

Workshop 3	*Rob Carter*

Other Institutional Identity Needs

Workshop 3	*Richard Biever*

Lightweight identities and bring-your-own-credential

Actors

Individual User
Service Provider
Non-SAML identity provider
Cooperating Organization

Stakeholder Groups

Learner/Student
Staff
External collaborator / Contractor

Story Narrative:

The risk and cost associated with establishing and maintaining institutional credentials for potentially large numbers of external and non-affiliated users with limited access campus resources and no LoA drive the need to support lighter-weight, low-LoA identities linked to externally-managed credentials.

Dr. Mangrove is an ophthalmologist practicing in rural North Carolina. A graduate of Johns Hopkins Medical School, she completed her residency in Florida and has no prior relationship with Duke.

In an effort to foster better healthcare in rural areas, the Duke Eye Center, in conjunction with Duke Continuing Education, offers a six-week, online continuing education series on strategies for long-term management of industrial and agricultural ocular injuries. The course offers six CE credit hours toward enrollees' annual board certification requirements upon successful completion.

Dr. Mangrove visits the Duke Continuing Education web site to sign up for the course. She's directed to an online registration form where she enters her name, her email and postal addresses, and her board certification number. Identity matching through the IDM facility determines that she is not yet known to Duke and a special, lightweight identity is created for her in Duke's IDM. Minutes later, she receives an email containing instructions and an activation code for associating an existing social provider credential with her new Duke identity. Following the instructions, she successfully authenticates using her existing Google+ account and authorizes Google to release an identifier to Duke. Meanwhile, Duke's IDM system adds her unique Duke identifier to the cloud LMS' user database as an enrollee in the selected course. Asynchronously, a workflow is initiated that verifies the board certification number Dr. Mangrove provided and marks her as eligible for CE credit.

When the CE course begins, she visits the cloud provider's web site and follows a link to the Duke CE course. The cloud LMS redirects her to Duke's Shibboleth IDP, where she selects Google as her preferred provider. She's redirected to Google's authentication service, where she successfully authenticates and is immediately recognized by the cloud-based LMS. Three days later, when she visits the course site using her iPad to complete an assignment, she happens to already be in an authenticated session with Google+, and is recognized by the Duke IDP, and ultimately the cloud LMS, without being challenged to enter credentials.

Upon her successful completion of the CE course, Duke Continuing Education reports her verified board certification number to the AMA along with her continuing education credits.

Six months later, Dr. Mangrove sees a patient who needs ophthalmic surgery and decides to refer him to the Duke Eye Center. She visits the Eye Center web site and finds that she needs to establish authentication credentials in order to access Duke's new Epic EHR system to order the referral. Remembering her prior CE interaction, she clicks the "login" button in the web interface and is taken to the social provider selection page so familiar during her six weeks of course work. She selects Google as her login provider and is immediately recognized by the Duke EHR system. Since she's not previously acted as a referring physician, she's required to enter additional information to further establish her credentials before completing the referral.

Duke University (028.duke.3.20150412)

Modified: 4/12/2015 2:38:42 PM

Participants

CIO or CIO Delegate
Workshop 3 *Tracy Futhey*

Senior Identity Architect
Workshop 3 *Rob Carter*

Other Institutional Identity Needs
Workshop 3 *Richard Biever*

Dynamic and Context Sensitive Privilege Management

Actors

Individual User
Home Organization

Stakeholder Groups

Learner/Student
Staff

Story Narrative:

Traditional role-based privileging solutions fail to address the complexities of higher education environments, where individuals may hold multiple roles, and where roles may be applied by multiple authorities. In academic medical centers, the issue may be compounded by context dependencies. IDM systems need to provide mechanisms for expressing and evaluating authorization rules that go beyond simple roles to address complex authorization scenarios.

Kelly McHugh is a practicing RN at Duke Raleigh hospital, specializing in pediatric critical care nursing. She works the second shift at the hospital four days a week. She is also an accomplished folk singer, and she volunteers on weekends at the Children's Hospital's pediatric oncology clinic, holding sing-alongs for pediatric inpatients.

On a normal Tuesday evening, Kelly would report for work at Duke Raleigh hospital just before 7:00 pm and use her ID badge to activate the door to the pediatric CCU, clock in for her shift, and then begin her shift. This evening, however, Kelly neglects to clock in at the time and attendance kiosk. Starting her shift, she uses her NetID to authenticate to a web-based pharmacy order for additional supplies of an anti-seizure medication for the unit. The Pharmacy system checks the assertions provided by the institutional IDP, which indicate Kelly is a member of the CCU nursing staff group, authorizing her to place the Pharmacy request. Soon after, Kelly attempts unsuccessfully to use her badge to open the scheduled drug cabinet in the unit. Surprised, she remembers that she neglected to clock in for her shift, and realizes that the cabinet will not open until she does. The card system is integrated with the institutional IDM, which implements a rule that limits physical access to authorized individuals whose time and attendance status is “on shift”. Kelly stops at the time and attendance kiosk and clocks in late for her shift, and is then able to open the cabinet.

Saturday morning, the Health System nursing coordinator calls Kelly to ask if she can fill in for an injured CCU nurse’s evening shift at the main hospital. Kelly agrees, planning to stay at the hospital after her volunteer event. When she arrives at the main hospital Saturday afternoon, she stops by the pediatric nursing station and attempts unsuccessfully to log in to check her shift schedule – the workstation denies her login based on her location in the main hospital not matching her medical role as reported to the IDM system by the Epic EHR. She returns to the pediatric nursing station just before 7pm. The nursing coordinator entered her into the main hospital nursing schedule for second shift as contract nursing staff, and since her shift is nearly begun, she is now able to log in. After the shift ends, her access rights are automatically revoked.

Later in the year, Kelly enrolls in a nurse management course in the Nursing School. She logs into the EHR system with her NetID and is offered a choice of roles (“student” or “CCU Nurse”). She chooses “student” in order to access some case study materials authorized to students in her management course. While she’s logged in, she attempts to check the status of one of her CCU patients from the night before and is denied access, since her session is bound to her “student” role. She logs out and back in, this time specifying her CCU Nurse role, and is able to access the information.

Two years later, Kelly applies and is selected to replace the first shift nursing supervisor in Pediatric CCU at the Raleigh hospital.   Changes are entered into the EHR system to reflect her supervisory role and are imported at the next batch update into the IDM system. When the SAP HR system indicates that her new position is effective, the IDM system updates her group memberships and role information, and at 7:00 AM on her first day in the new position, she notices that she has supervisory access to information about all patients in the unit, not just her own.

Duke University (029.duke.4.20150412)

Modified: 4/12/2015 2:39:05 PM

Participants

CIO or CIO Delegate
Workshop 3 *Tracy Futhey*

Senior Identity Architect
Workshop 3 *Rob Carter*

Other Institutional Identity Needs
Workshop 3 *Richard Biever*

Federated InterInstitutional Access to Research Computing Resources

Actors

Individual User
Home Organization
Virtual Organization
Federated Computing Resource

Stakeholder Groups

Researcher/Scholar
Learner/Student

Story Narrative:

Compute- and data-intensive, inter-institutional research efforts drive the need to extend federated identity beyond inter-institutional authentication to federated authorization, and to extend federated identity into non-web-based environments.

Prof. Alexis Pavlov, from Duke University, and Prof. Reginald Keynes, from the University of Virginia, are co-awardees on a multi-year USDA grant focusing on the application of statistical data depersonalization to the analysis of large social data collections. As part of the grant, they have access to roughly 200 GB of personally-identifiable purchasing, medical and socio-economic data.

Alexis' research entails developing statistical data models based on social data, and she and her four graduate assistants develop Linux-based model generation code in C++. Reginald's primary interest is the effect of socio-economic factors on the effectiveness of outreach programs, and he and his graduate assistants use custom Windows-based tools to perform their statistical analyses.

Alexis and Reginald agree to house the USDA data inside Duke's protected data network. Alexis creates a research project framework using a web-based self-service tool at Duke, identifying herself and Reginald as co-PIs for the effort, and adding her graduate students as collaborators. Reginald logs into the same self-service interface with his UVA credentials and enrolls his four graduate assistants as collaborators in the same project, contingent upon their being identified by UVA's IDP as part of Reginald's research group. It falls to one of the UVA graduate assistants to transfer the dataset from UVA to Duke's protected data network, which she does using a Duke-hosted federated data transfer tool over a pre-reserved network channel between the two sites. Due to the sensitive nature of access into the Duke private network, each authentication requires the use of MFA.

Alexis and her students develop their model-generating tools using virtualized Linux workstations hosted within Duke's protected data network, and periodically perform model runs to generate depersonalized datasets, which are written to CIFS shares outside the protected network, in Duke's research DMZ. Reginald and his students, in turn, use their UVA credentials to initiate interactive sessions on virtualized windows desktops in the research DMZ, where their roles in the collaboration grant them read-only access to the depersonalized datasets Alexis' group have generated. Halfway through the grant period, one of Reginald's graduate assistants leaves his research and although John remains an active student at UVA, his access to the collaboration ceases when he leaves Reginald's research group.

On a periodic basis throughout the project, Reginald uses his UVA credentials through a SAML-enabled VPN and federated remote desktop mechanism to access a dedicated Windows machine inside the protected data network and run his team's analysis against the original USDA dataset to validate that the modeled data and the non-depersonalized data produce consistent statistical results.

Alexis later invites one of her CS colleagues at UNC-CH into the collaboration with read-only access to the depersonalized data and a restricted Gitorious repository, where her team's modeling code is housed. Her UNC colleague uses his UNC credentials to access the Gitorious repository and fork the modeling code, ultimately applying it to a similar dataset involving driving records and insurance claims in North Carolina, validating the modeling mechanisms employed.

Duke University (030.duke.5.20150412)

Modified: 4/12/2015 2:39:24 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Hybridizing on-prem and cloud IDM services

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Learner/Student
Faculty/Instructor
Staff

Story Narrative:

Address latency-related performance issues and disaster resilience requirements through extending IdM services to the cloud, resulting in a hybrid environment for authentication services on-prem and in the cloud.

Lisa Simpson is a student in the School of the Environment working on a degree in Earth and Ocean Science. She's taking Professor Saffer's EOS513 course on atmospheric dynamics to fulfill her final requirement before graduation.

Professor Saffer has chosen to use a cloud-hosted, private instance of Sakai to manage his course materials. The Sakai service is hosted by a third party operating out of two data centers in the Midwest. Early in the semester, Lisa complains that logging into the Sakai service, which relies on Duke's on-prem Shibboleth IDPs for basic authentication and integrates directly via LDAP with the institutional directory service for real-time access to certain user information, is undesirably slow. Central IT staff discover that the cloud-based Sakai service is performing multiple LDAP queries back to the institutional LDAP service for each user login. With a 120 ms network round-trip time through the commodity network between the hosting site and Duke, cumulative latency issues are making access to the service unpalatably slow. Fortunately, Duke's LDAP service is being provided with containerized directory servers, and IT staff arrange to co-locate container instances at the hosting site where Sakai is running, and to make the

Sakai service preferentially use the co-located LDAP instances. They take advantage of recently-added asynchronous replication support in their LDAP software link the on-prem directory instances to the cloud-based instances, trading a small delay in updates for better wide-area replication reliability. Four weeks into the semester, Lisa finds that her Sakai sessions are as crisp as her logins to the on-premise graduate student wiki.

In late April, an unusually early-season tropical storm comes ashore off the coast of North Carolina, and while Duke's local network is unaffected, connectivity to the rest of the Internet through both of its wide-area providers is interrupted. Just weeks before, IT staff had completed stationing a pair of Shibboleth IDPs and read-only KDCs in the Microsoft Azure cloud. After the storm subsides, both Lisa and Professor Saffer find that power is still on at their homes and that they're both able to connect to the Internet via local LTE services. Lisa is able to log into Sakai via the Azure-based Shibboleth IDPs and schedules a phone call with Professor Saffer to discuss her thesis via Exchange using Office 365 with its existing Azure AD and using the Azure-hosted IDPs and KDCs for authentication. Professor Saffer is able to grade her work from home in time to report her grade in Sakai before the semester ends, but has to wait a week, until campus connectivity is restored, to grant her the access they discuss to his research data on tropical systems, since the on-premise Grouper instance is not available.

Hearing of his Grouper issue, IT staff make plans to take advantage of a new SaaS Grouper offering provided by I2 that will allow selective, bi-directional replication of group information between an on-premise Grouper instance and the cloud, realizing that in so doing, they can make their IDM infrastructure more resilient before the next major disaster strikes. Seven months later, during an outage caused by a major ice storm, Professor Saffer is unaware that his access to an online journal from his vacation home in Florida is actually being authenticated and authorized through cloud-based instances of institutional IDM services.

Duke University (031.duke.6.20150412)

Modified: 4/12/2015 2:39:52 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Faceted Identities and Delegated Management

Actors

Individual User
Home Organization
Subordinate Organization

Stakeholder Groups

Researcher/Scholar
External Collaborator / Contractor
Staff

Story Narrative:

The IDM needs of sub-organizations may vary significantly from those of the institution as a whole. Central IDM systems need to provide flexible delegation mechanisms to allow sub-organizations appropriate control over their unique data, and flexible mechanisms for integrating external attributes and credentials with central services in order to avoid complete IDM service fragmentation.

Dr. Jay Hyde is clinical faculty in Endocrinology at Duke Hospital, specializing in the treatment of pancreatic disorders. In addition to an MD, he holds a PhD in Pharmacology. Tammi Houston is a senior IT analyst at the Duke Clinical Research Institute (DCRI), a subsidiary of the Duke School of Medicine founded to host clinical trials and touted as the largest academic research organization in the world.

GlaxoSmithKline (GSK) contracts with DCRI to host a Phase I clinical trial of a new synthetic insulin analog. Dr. Hyde accepts DCRI's invitation to become the clinical PI for the trial, and Tammi is directed to establish access to the electronic resources necessary for him and Jack Elsworth, GSK's project manager for the trial. She establishes a database instance in an MS-SQL environment joined to DCRI's local Active Directory domain and a collection of web-based tools protected by the University's Shibboleth environment for the trial. As part of the set-up process, Tammi creates a collection of groups in the DCRI Active Directory associated with the clinical trial.

Tammi logs into the University IDM portal with her NetID and searches for Dr. Hyde's entry. As IT staff in DCRI, she is authorized by the portal to initiate provisioning of an account in the DCRI AD, and within seconds, a DCRI AD account is created for Dr. Hyde. Dr. Hyde receives an email informing him of the account, and instructing him how to activate the DCRI account.

Tammi next logs into the Institute's AD and uses her local administrative credentials to create an AD account for Jack Elsworth. She uses a local DCRI tool to assign both Jack and Dr. Hyde 16-digit trial user identifiers, which are recorded in their AD entries, and add them to groups associated with the clinical trial.

After discussing the trial with Dr. Hyde during a routine visit, Janet O. agrees to participate. Dr. Hyde is already logged into the hospital EHR reviewing Janet's history, and clicks a link to the DCRI trial portal to log into the DCRI portal and enroll her. His existing SSO session authenticates him automatically, and the Shibboleth IDP retrieves attributes from both the University IDM and the DCRI AD in order to fulfill the attribute release requirements of the DCRI portal. Based on the assertions it receives, the portal authorizes Dr. Hyde to enroll Janet in the GSK trial, and the system creates a DCRI AD account for Janet and emails her instructions for activating it and using it to make weekly reports thorugh the DCRI portal during the trial.

One week later, Janet visits the trial portal and is directed to the University Shibboleth IDP to log in. As instructed, she does so using a scoped identifier (janeto@dcri.duke.edu) and her DCRI password. Based on the scoped ID, the Shibboleth IDP authenticates her against the DCRI AD rather than the institutional Kerberos environment, and retrieves her attributes from the DCRI system. She is recognized as a participant in the trial and authorized to enter her weekly report.

Later that week, Jack Elsworth logs into the DCRI portal using a similar mechanism (with the id jelsworth@dcri.duke.edu) and is able to produce a report listing data about all the trial participants. The report identifies the patients solely by their 16-digit participant identifiers, preventing Jack from gaining insight into their actual identities.

Duke University (032.duke.7.20150412)

Modified: 4/12/2015 2:40:11 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Internationalization and Effective ID Matching

Actors

Individual User
Home Organization
International Affiliate

Stakeholder Groups

Learner/Student
External Collaborator / Contractor
Staff

Story Narrative:

As our institutions expand internationally and as our student and employee populations become increasingly diverse (culturally and geographically), IDM systems will have to address new challenges posed by integrating with internationally-provided software as well as culturally-diverse identities and identity data.

Li Lee is a Shanghai native and recent graduate of the undergraduate Psychology program at Duke. Her student visa having expired, she's moved back to her native China, only to find that opportunities for recent Psychology graduates are not as common as she'd hoped. She hears about the new DKU (Duke-Kunshan University) and its MBA program, and decides to investigate enrolling.

After achieving high marks on the US version of the GMAT before returning to China, Li is hopeful about her prospects for admission, and visits the Chinese-language version of the DKU web site to begin the online application process. She enters her personal information and provides a signed electronic copy of her GMAT scores along with her application. One week later, she receives a phone call from a DKU admissions officer who informs her that her GMAT scores could not be verified, and asks her to double-check her submitted application. On review, she notices that while she entered her name as "Lee Li" (the ordering to which she is accustomed when working in a Chinese language context) she had reported her name as "Li

Lee" when taking the GMAT in the US two years before. The admissions officer is able to adjust her online application during the conversation, and three months later, Li is accepted to DKU as an MBA student.

Upon her matriculation, the DKU Registrar's office submits her information into the Duke SIS system (since DKU share an SIS system and DKU students are considered "students" by Duke). Because her application had been updated to reflect her name as "Li Lee", the SIS system is able to properly match her with her undergraduate records. Consequently, her entry in Duke's IDM system is also matched, resulting in her existing NetID being re-enabled. On her first day at DKU, she's issued a new RFID badge that she uses to access academic buildings as well as to access the dormitory where she lives during her 18-month MBA program.

Two years later, Li applies for a Manager position in the DKU Office of Student Affairs, and she is hired as a DKU employee. Unlike students, DKU employees are not considered Duke employees – DKU operates its own separate payroll and HR ERP developed and sold by a Chinese corporation (as mandated by Chinese regulations). Duke does provide certain DKU employees with electronic access as sponsored guests and the International Office at Duke chooses to grant Li that level of access. Because the DKU ERP, however, identifies Li using UTF-16 and a Mandarin code page, and having no US tax identifier or other shared unique key to use for verification, the automated ID matching logic is unable to arrive at a definitive match for her identity, and International Office staff inadvertently establish an entirely new identity for Li, rather than associating her new guest role with her existing Duke identity.

Li notices the discrepancy months later, when she moves into a new apartment and changes her address in the DKU payroll system but finds that her DKU alumni information continues to reflect her old address. IT staff investigate the situation and, realizing the error, perform an identity consolidation using an administrative web interface in the IDM to merge Li's identity records. They make a note to retrofit the code ingesting DKU HR data into the IDM to look for potential name ordering confusion and provide enhanced UTF-8 and UTF-16 support in future.

Duke University (033.duke.8.20150412)

Modified: 4/12/2015 2:40:29 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Lifecycle-driven Provisioning/Deprovisioning

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Learner/Student
Faculty/Instructor
Staff

Story Narrative:

Individuals in higher education frequently pass through myriad roles and relationships with the institution, often exhibiting multiple roles across multiple institutional contexts simultaneously. Institutional provisioning tools need to driven by the IDM lifecycle, and flexibly implement both simple automated provisioning and deprovisioning policies and more complex schedule- and workflow-driven (de)provisioning policies across a range of both on-premise and cloud-based services.

Nils Petersen has just been selected for a PA position in an outlying clinic owned by Duke Medicine. The clinic's HR representative begins the online hiring process, entering information from Nils' application into the corporate HR system (SAP), which in turn calls a web service API provided by the institutional IDM system to initiate the creation of an electronic identity.

The IDM system performs an identity match and determines that Nils is a new community member, so a new unique identifier is automatically assigned and returned to SAP. Subsequent calls to the web service reference the assigned unique identifier and add initial ERP data to his IDM record resulting in the IDM assigning him "pre-hire affiliate" status. His transition to pre-hire affiliate causes a message to be queued to the provisioning system, where an adapter creates a new NetID and records its value in the person registry. That update in turn sends messages to multiple provisioning queues, where other provisioning adapters provision access to the Duke Medicine AD, the medical LMS environment, and Office 365 (where his outbound mail is flagged with a “require DLP” policy). A Service Now workflow is also initiated to establish an unprivileged Epic (EHR) account for Nils. As the clinic HR staff add roles to his Epic account following his completion of HIPAA training, an hourly import process triggers his addition to Grouper groups based on his role assignments in Epic. Membership in those groups, in turn, triggers the addition of physical access to specific parts of the medical center and the clinic to the security profile of his employee ID badge.

When his hire is completed, another web service call from SAP triggers messaging and workflow initiation that causes his IDM affiliation to be updated to “staff” and his NetID to be provisioned with a Box account flagged with BAA requirements, a Service Now account, and an SAP (medical requisition) account. On his first day, he is issued an ID badge, which he uses at a local kiosk to activate his NetID, enabling all of his provisioned access.

When Nils enrolls in a class in the Medical School, the PeopleSoft student system triggers further calls to the IDM API. Upon his matriculation, these calls cause the IDM to add a “student” affiliation to his identity and assign him membership in a collection of course-related groups that convey access to instructional resources on campus, as well as the cloud-hosted Sakai system and the PeopleSoft student registration system. When the semester ends, PeopleSoft calls the IDM API again, triggering the removal of Nils’ “student” affiliation and automatic deprovisioning his PeopleSoft and Sakai access.

Five years later, when he leaves the clinic, an SAP call to the IDM API triggered by his transition to an “inactive” state causes his staff affiliation to be removed. A provisioning message queued by that transition causes all the IDM connectors which have his identity in a provisioned state to deprovision him. Each connector implements its own separate deprovisioning policy, some of which involve immediate removal of access (eg., from Epic and its related Grouper groups, and from the Duke Medicine AD) while others may implement workflow-driven or time-driven deprovisioning (to, eg., permit outstanding ServiceNow tickets to be reassigned or allow shared data in Box to be assigned to a new owner).

Duke University (034.duke.9.20150412)

Modified: 4/12/2015 2:40:50 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Facilitating Mandatory Authorization

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Learner/Student
Researcher/Scholar
Staff

Story Narrative:

Adoption of best practices in authorization by service providers and applications has traditionally been as weak as adoption of centralized and federated authentication services has been strong. Many applications continue to support only ad hoc, individual delegation as an authorization model or, worse, support no real authorization model, conflating authenticating and authorization. To facilitate better practices among service providers and application developers, IDM systems must provide more flexible and approachable authorization services.

Bob Newman is a senior IT analyst in the Office of the Provost. His primary responsibility is the Office's web presence, but he dabbles in programming, building the occasional web application for the Office.

The Provost's office maintains bulk licenses for a number of commercial scholarly and administrative applications, which it offers free of charge to faculty and students in academic departments on campus. The Provost's licenses typically permit academic use of the software by any employee or student, but a few limit use to the College of Arts and Sciences. Bob is tasked by the Provost with automating the delivery of licensed applications through the Office's web site. Keen to exercise his development skills, Bob decides to design a simple PHP-based software download service he can host on the Office's web servers.

Bob is very aware of the institutional Shibboleth infrastructure – his web servers already run Shibboleth SPs, so he quite easily arranges to require NetID authentication for all downloads through his tool. Satisfied he's met the Provost's requirements, he moves on.

A few months later, Internal Audits begins a routine audit of licensed software on campus, starting with the Office of the Provost. Bob's new application is targeted as a point of control for licensed software, and Bob is asked to provide records of software downloads from his web servers. Bob gladly complies, confident that his use of Shibboleth will make passing the audit easy.

A month after the audit begins, Bob is shocked when the Provost reports that his application has been cited for multiple licensing violations due to downloads by contractors, collaborators and unauthorized students outside Arts and Sciences. Bob reads the details cited in the Audit report, and sure enough, multiple individuals with "affiliate" affiliations successfully downloaded licensed software from his server. Looking further, he finds that a number of recent alumni have also availed themselves of the service (but he chooses not to volunteer that information).

Worried, Bob contacts the central IDM group for assistance. He learns that OIT has recently upgraded its Grouper infrastructure to the latest I2 release and gets pointers to online documentation for a simple self-service process to request specific group membership information from the campus Shibboleth IDPs. He uses a user-friendly Grouper interface to scan the hundreds of thousands of available Grouper groups. Reviewing his software licenses, he determines that he can make proper authorization decisions based on membership in less than a dozen affiliation- and school-based groups, and he uses an online self-service tool to request IDP release of the relevant group membership information to his application. He also finds example code on the campus IDM web site to help him design better authorization into his application. With surprisingly little effort, Bob retrofits his licensed software site with explicit authorization, and after follow-up review, IA removes the finding from their final report a week later.

Duke University (035.duke.10.20150412)

Modified: 4/12/2015 2:41:08 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tracy Futhey*

Senior Identity Architect

Workshop 3 *Rob Carter*

Other Institutional Identity Needs

Workshop 3 *Richard Biever*

Federating Attributes from Multiple Authorities

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
External Collaborator / Contractor
Staff

Story Narrative:

Inter-institutional research and other collaborations increasingly demand rich sets of attributes, both to provide highly customized user experiences and to make complex authorization decisions. Many attributes may be asserted by one's home institution, but increasingly, service providers have to aggregate attributes from multiple authorities. IDM systems need to embrace this burgeoning federated attribute ecosystem by providing flexible mechanisms for attribute release and providing more powerful mechanisms for attribute aggregation.

Professor Gary Ross is research faculty in the Sanford Institute of Public Policy. His research interest is the relationship between municipal government policies and individual housing decisions. He has been working closely with the US Conference of Mayors for years to accumulate a database combining municipal zoning information with property tax and real estate records.

Professor Ross recognizes that his data lend themselves geospacial analysis, and acting on a tip from a colleague in the Library makes an inquiry of the Ball State University Library, where he's been told there's a significant GIS research facility. Ball State is an InCommon participant, as is Duke, so the Librarian at Ball State recommends that Professor Ross use his Duke account to access the Library's collection of online GIS mapping and analysis resources. He forwards Professor Ross a URL to use to access the Ball State resource.

Ball State's GIS resource has recently been added to the InCommon R&S category, and during a recent upgrade to the v3.1 IDP, Duke's IDP has been configured to automatically release the R&S attribute bundle to federated SPs in the R&S category. When Professor Ross visits the Ball State URL, the Duke IDP automatically releases his name, email address, and eduPersonPrincipalName, allowing Ball State to build a profile for him.

Professor Ross finds a geospacial visualization tool perfectly suited to probing his data that provides a simple interface for importing data from remote object stores, but when he attempts to import data from his Conference of Mayors object store, his request is denied by the Ball State system with an error message referencing something called an ORCID.

He contacts Rich, an IT staffer at the Institute, and after a bit of research, Rich determines that the Ball State SP requires an ORCID in order to effectively track and report on the use of its resources by outside researchers. Rich helps him first establish an ORCID ID and password, then use Duke's self-service ORCID interface to link his new ORCID with his Duke identity. Duke's IDP is configured to release the attribute to R&S SPs, but only if the user authorizes it through the IDP's informed consent mechanism. When Professor Ross next visits the Ball State resource, the Duke IDP requests his approval for releasing his ORCID to Ball State. Once he approves the release, Ball State adds his Duke-asserted ORCID to his profile, and authorizes him to use the data import mechanism.

Later, when Professor Ross submits a paper to *Public Policy Review*, he receives a request to grant access to his research data to peer reviewers from UNC, Princeton, and UC Davis. The *Review* notes that its IT staff have recently established a standalone attribute authority to release peer reviewer information. Using recent extensions to the Duke object store to support SAML-based attribute requests, Rich is able to help Professor Ross authorize his peer reviewers to access his data. When the reviewers from the other three schools log into the Duke object store using their federated identities, the object store requests and receives SAML assertions from the AA operated by the *Review* verifying their status as peer reviewers and authorizes them to read Professor Ross's data.

Emory University (036.emory.1.20150412)

Modified: 4/12/2015 2:42:32 PM

Participants

CIO or CIO Delegate

Workshop 3 *Sriram Chari*

Senior Identity Architect

Workshop 3 *Anne Marie Alexander*

Person Data Persona/Role Management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

In institutions that have heavy research and health care affiliations, one of the challenges involves representing the persona of individuals and the roles they play across various business units. One of the typical use case involves a practicing physician also being a professor. In addition the professor could be adjunct or tenured etc. The individual requires various representations of their roles when accessing specific application. This lends itself into a need for role and group authorization for context specific data management, need to manage this data and governance around this persona data management.

Emory University (037.emory.2.20150412)

Modified: 4/12/2015 2:42:53 PM

Participants

CIO or CIO Delegate

Workshop 3	*Sriram Chari*

Senior Identity Architect

Workshop 3	*Anne Marie Alexander*

Single Sign out

Actors All

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups All

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Single sign on provides users the benefit of a common authentication mechanism into multiple applications. This is hugely beneficial in environments where users typically use many applications to perform various functions throughout the day. One of the common use cases is the ability to logout of individual applications that contain business critical data or PCI data to ensure user session does not continue. This is usually handled by redirecting the user individual application logout to the single sign on logout, which logs the user out of all applications. This is less than desirable when modern day browsers support multiple tab and users are akin to opening applications on several tabs. A standardized approach to logout of individual applications would benefit many critical applications.

Harvard University (038.harvard.1.20150412)

Modified: 4/12/2015 2:44:59 PM

Participants

CIO or CIO Delegate

Workshop 3 *Jane Hill*

Senior Identity Architect

Workshop 3 *Tim Gleason*

External Self Registered

Actors

Individual User
Home Organization
Vendor Service Provider
Program Administrator

Stakeholder Groups

Learner/Student
University Program
Security/Audit

Story Narrative:

As a graduate school offering courses to external non-degree participants, the university would like to offer the ability for the registrant to create an identity to enable immediate course enrollment. During the sign-up process, which includes paying by credit card, the program's administrative system will capture data about the individual registrant. This administrative system is currently an on-premise system, but the team is expecting to migrate to a vendor product. The Program wants to ensure that the registrant is able to access online resources that will be secured using the University's enterprise IAM system. The Program expects the new registrant to either be associated with an existing campus identity or issued a new identity as a part of this onboarding transaction. There is an expectation that the IAM system will subsequently interact with the registrant via email, enabling that user to set up a credential that will work for accessing the program resources, or be advised how to recover a password if a previously issued credential no longer works. The IAM system is concerned that the identity is tagged with the appropriate level of assurance and that an internal persona/role is captured that can be used by the IAM system to support authorization for online (and perhaps even physical) resources. It is necessary to capture information about which University department and program was responsible for issuing the identity and assigning a new persona/role to the registrant. The Program has asked whether it is possible for their registrants to use a commercial identity (like LinkedIn, or Google+) or in the case of a medical context, an existing Hospital identity instead of having to get a new credential.

Nearly immediate access upon registration (e.g. register a few minutes before the course is scheduled to start)

Online learning model

Level of assurance for self registration influenced by financial transaction

Association and matching to campus identity

Avoiding duplicate identity issuance, if possible

Use of social or campus provider

Ability for registrant to access University wireless for basic services

Harvard University (039.harvard.2.20150412)

Modified: 4/12/2015 2:44:33 PM

Participants

CIO or CIO Delegate

Workshop 3 *Jane Hill*

Senior Identity Architect

Workshop 3 *Tim Gleason*

Only return a SAML Authentication Response when a user meets application-specific eligibility requirements

---

Actors

Individual User
External Service Provider (Vendor)
SAML identity provider
Authentication Service Administrator
Vendor Representative

Stakeholder Groups

Vendor
University Department who contracted with Service Provider
Legal / Audit

Story Narrative:

Problem Description:

A third-party provider (non-InCommon) that is being integrated with the University Shibboleth IDP to provide a service to the University community as an agent of the University is unwilling or unable to base the authorization of an authenticated user on standard attributes. The vendor expects the authorization response to be based on an authorization filter in addition to the credentials so that the University has the full responsibility for enforcement of the terms of usage (license.)

Alice has received a request from the CIO's Office to integrate a research service vendor's site with the University enterprise credential using SAML. Although the vendor can work with SAML, they request that Harvard enforce the recently update license agreement terms by adding an authorization step to the authentication flow that only returns an authentication assertion if the authenticated user is a full-time, paid faculty or staff member, or a degree candidate student. They are particularly concerned that Continuing Education students who are registered but are not pursuing a degree are not authorized to use the service. Further, the vendor wants Harvard to display a web page to an individual who tries to access the service, but is not eligible, outlining why the user was denied access so that these users do not call the service provider and complain.

Indiana University (040.iu.1.20141205)

Modified: 12/5/2014 9:34:53 AM

Participants

CIO or CIO Delegate	
Workshop 1	*Brad Wheeler*
Workshop 1	*Rob Lowden*
Senior Identity Architect	
Workshop 1	*Jacob Farmer*
Other Institutional Identity Needs	
Workshop 1	*David Bickel*

A doctor's tale of multiple logins

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Staff

Story Narrative:

Doctor Mustard begins each day by logging into the patient tracking application on his tablet using his credential issued to him by his university medical center. He uses the patient tracking application for all daily activities around his medical office.

After a busy morning of seeing patients, Doctor Mustard grabs some lunch and heads onto campus to teach a course at the University. Once on campus, he uses his university credentials to access the LMS and assign course work to his students.

Doctor Mustard then leaves campus and goes to the University Medical Center to check on some of his patients. While he is there he once again has to log in to the medical center database and patient tracking application using the credentials issued by the medical center. Noticing that he has some extra time, he decides to evaluate a few of the medical students there and must log those observations into the university system, once again using his university credentials.

Once he is home for the evening, Doctor Mustard must log in to his laptop as he works on the research grant he is proposing with collaboration from some of his peers at various other educational institutions.   He performs this work using his university credentials presented out through SAML assertion to a cloud application.

The next morning, Doctor Mustard travels to a university-run hospital facility in the northern part of the state. Before he travels, Doctor Mustard takes a few moments to recall which of the 3 proximity based key cards are used for that facility.   Once in the facility he plans on performing some evaluations on the medical staff.   While Doctor Mustard is there they ask him to consult with them on a patient. In order to perform that task, Doctor Mustard is required to obtain yet another set of medical center credentials.

Often, Doctor Mustard mixes up which password to use in which system.   This frequently results in him getting locked out and having to contact support at his medical center or the university.   This is not only frustrating, but also time consuming, resulting in disruptions to patient care and student education. Doctor Mustard would be very grateful if he only had a single credential to use across the university and its affiliated medical centers.

Indiana University (041.iu.2.20141205)

Modified: 12/5/2014 9:35:13 AM

Participants

CIO or CIO Delegate

Workshop 1	*Brad Wheeler*
Workshop 1	*Rob Lowden*

Senior Identity Architect

Workshop 1	*Jacob Farmer*

Other Institutional Identity Needs

Workshop 1	*David Bickel*

Accounts lifecycle management, delayed action

Actors

Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

The identity management team needs to be able to properly apply changes to accounts when a person separates from the university. This system needs to take into consideration all of the roles the person had and make adjustments to all connected systems. These changes also need to be performed on a set delay so that the person has advanced warning.

The current system we have in place does meet most of these requirements. However, as some time has gone by it is evident that a redesign would help us address many processes that are currently lacking.

The first issue we would like to address can be found in the delayed action mechanism. The system works by writing out effective dated records to handle a “disable” and a “deletion” operation. One core issue we have run across with this process occurs when a user returns to the university. The process worked well when all accounts were removed after leaving the University. However, now many former students maintain their active directory and student email. If they return later as an active student, the system may handle them improperly and need manual intervention.

The existing system was also designed before those former users existed in the system. A user's status is represented by a single role, (student, alumni, employee, former employee, faculty, etc.). Thus a user who is both a former employee and a current student, may inadvertently have her Former Employee status trump her Active Student status. This again requires manual intervention by the identity management team.

To address these issues, we need to move to a redesigned system that is more flexible and able to adjust to growing complexities. Some examples of those on the horizon would be managing cloud services as well as extended complexity of roles.

Iowa State University (042.iastate.1.20150406)

Modified: 4/6/2015 1:35:58 PM

Participants

CIO or CIO Delegate
Workshop 3 *Angela Bradley*

Multiple AuthN and AuthZ Entities / Birthright Services

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Students, faculty, and staff at ISU use different UserIDs and passwords to authenticate and gain authorization to different required central systems and applications. The Student Information System and campus HR system use the University ID (nine digits) and a RACF eight-character password for authentication. Email, Box, SharePoint, printing, … use Active Directory-based NetIDs and a separate password. A "people file" is created each night to share information between the systems.

Jane Student applies to Iowa State and is offered undergraduate admission. Jane is given a University ID and password to access the central portal, Access Plus, when she is offered admission. She is only authorized to accept the offer in AccessPlus, then she is allowed to register for a NetID once she has a UID. The NetID/password combination allows access to email (Google Apps for Education), storage services, Box, Lynda.com, etc. Joe Student is loaded as a prospect in the Admissions system after attending a university event. He is given a UID at that point. When he applies for undergraduate admission, his UID already exists and he could potentially apply for a NetID before accepting admission, allowing access to the birthright services provided by the NetID.

Joan Faculty/Staff applies for employment through a cloud service, PeopleAdmin. Some of the information is transferred to the central HR system, but not all. Officially, Joan Faculty/Staff is assigned a UID when the personnel action takes place. However, a new employee can request an early UID and a provisional NetID early in the process. The NetID again gives access to email (Office365), storage, Box, Lynda.com, etc.

Jack Visiting Professor is added to the payroll / HR system as a different employee type that does not allow a NetID to be created. The department requests a “sponsored” account to have access to email.

Goals for ISU:

One system for authentication.

One system for authorization.

No services based on authentication, only.

Multi-factor authentication depending on data classification access.

One portal?

Questions:

What is the best way to integrate with cloud providers? Federation for both authentication and authorization or shared attributes?

How do we move forward changing our authN and authZ models, use federation for the cloud, and keep current processes working?

Iowa State University (043.iastate.2.20150412)

Modified: 4/12/2015 3:11:45 PM

Participants

CIO or CIO Delegate

Workshop 3 *Angela Bradley*

Management of Person Data

Actors

Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

ISU has separate data stores for HR, Admissions, and Registrar with constant updates required between the systems. Students, faculty, and staff are generally well-defined and managed, but affiliates and third-party users are not. Some services require university UIDs and NetIDs for people who are not employees and not students. For example, spouses and dependents need a UID to use campus recreation facilities. Visitors attending sports/academic camps need a UID for dining services. Visitors using the campus library are given a local account on the system while students, faculty, and staff use NetIDs. Consortiums with other universities require Blackboard access for people not enrolled at ISU.

Because of all the crossover between users and systems, it is very difficult to match data sources and define a person authoritatively in one place. File transfers are much too common, allowing local applications to use their own authentication and authorization systems. For example, the Facilities, Planning, and Management department uses a project system that allows users to login with their official NetID, but a different password.

Cloud providers are asking for attributes that require more disbursement of data. ISU recently contracted with the Blackboard help desk service. Blackboard can see the information stored in our campus system, but they insisted on getting birthdate information for users. This necessitated a feed from the central databases.

Goals for ISU:

Eliminate or significantly reduce file transfers and multiple master repositories

Increased governance and analysis of requests for information access

Decrease local application authN/authZ services. Promote federation as a best practice.

Questions:

How are affiliates and third-parties included but separated?

What matching algorithms are being used?

What process is used in deciding to share information with cloud providers?

How are campus units encouraged to use central authN and authZ services?

Lafayette College (044.lafayette.1.20150412)

Modified: 4/12/2015 3:12:15 PM

Participants

CIO or CIO Delegate

Workshop 1	*John O'Keefe*

Senior Identity Architect

Workshop 1	*Bill Thompson*

Account Activation/Self-service

Actors

Individual User (Students only)
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Student account activation used to be time and resource intensive as initial credentials (i.e. passwords) were sent via U.S. Postal to home address, with the assumption that users would change them was activated. The system in place now requires in-coming students to have an “alt email” address on record, which is used to send a NetId and a one time use activation code that can be used to set the password. The same mechanism is used for password reset for students and other constituents.

For account other than Students, user services communicates the netid/password to the hiring manager or responsible person, with instructions to reset the password using self-service web site, as well as encouragement to set an AltEmail address.

Alumni can have altEmail set by Office of Alumni after identity proofing occurs. HR or Provost vet identities and can update altEmail in cases where users need to reset or activate an account.

Lafayette College (045.lafayette.2.20141205)

Modified: 12/5/2014 9:23:28 AM

Participants

CIO or CIO Delegate

Workshop 1 *John O'Keefe*

Senior Identity Architect

Workshop 1 *Bill Thompson*

Portal Access / Identity Lifecycle

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

There is a gap in our ability to provided access to classes of users (e.g. “admit-coming”) due to delays or gaps in data and/or business processing. Banner doesn’t mark admit-coming as “students” until they are enrolled in a course. Portal student access is keyed on banner notion of “student”. Often unclear how to close that gap and which data/process would be appropriate to use (leading to deep dark dependencies). Generally struggling with complicated identity lifecycle, overlap of roles, transient users, etc. Lacking process/system for managing identity lifecyle independent of business specific systems.

Michigan State University (046.msu.1.20141201)

Modified: 12/1/2014 11:36:04 AM

Participants

CIO or CIO Delegate

Workshop 1 *Joanna Young*

Story 1: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Michigan State University (047.msu.2.20141201)

Modified: 12/1/2014 11:36:36 AM

Participants

CIO or CIO Delegate

Workshop 1 *Joanna Young*

Story 2: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

MIT (Massachusetts Institute of Technology) (048.mit.1.20150412)

Modified: 4/12/2015 3:13:42 PM

Participants

CIO or CIO Delegate

Workshop 1 *John Charles*

Senior Identity Architect

Workshop 1 *Thomas Hardjono*

Cross-Institution Big Data Sharing

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator

Story Narrative:

Dr Simpson is an epidemiologist conducting research at the Harvard Medical School into the spread of diseases in the world. She is named principal investigator in a grant under which the analysis of tens of thousands of blood samples coming from a certain country in Africa is made available through the Centers of Disease Control and Prevention (CDC). However, Dr. Simpson realizes that in order to gain a deeper understanding of the spread of diseases in that African nation, she would need access to “movement data” of the people in the nation.

Dr Simpson connects to the TIER Big Data Federation service, and learns that some researchers at the MIT Media Lab possess a large repository of mobile phone data (GPS data) from that African nation. This data was bequeathed to MIT by a European mobile carrier that provides mobile telephone services throughout Africa. This data was given to MIT under the legal condition that the raw-data is never made available outside MIT. As such, the MIT researchers have stood-up a RESTful API that provides access to an abstracted data-set where the PII information have been removed.

From the TIER Big Data Federation service Dr Simpson also learns that some geo-sciences researchers at Cambridge University in the UK have created a mapping service that can read this

GPS data from MIT and overlay it onto a detailed Google map and geographic terrains map of the African nation. This service is also accessible via RESTful APIs.

Dr Simpson then creates an Application that reads data from both the MIT APIs and the Cambridge University APIs. Through this application Dr Simpson authenticates herself via InCommon Federation to MIT and Cambridge University. She waits until the OpenID-Connect Servers at both MIT and Cambridge University grants her application with the appropriate access tokens. Upon receiving these authorization tokens, she runs her application that accesses the various data-sets are three distinct entities (CDC, MIT and Cambridge University).

Dr Simpson's application is able to successfully correlate the diseases data from the CDC, the GPS data from MIT and the Geo-mapping data from Cambridge University. Dr Simpson and her team is able to gain new insight about the patterns of spread of the disease, the velocity of spread and other aspects regarding the disease.

Dr Simpson then contributes back her research data-sets to the global community by publishing the information regarding her available data-sets and the APIs to the local BDPaaS service at her campus. Overnight the local BDPaaS service advertises this new information to the TIER Big Data Federation service.

NOTE: In the above use-case, fictitious names of institutions have been used to maintain privacy of actual institutions involved.

MIT (Massachusetts Institute of Technology) (049.mit.2.20150412)

Modified: 4/12/2015 3:14:13 PM

Participants

CIO or CIO Delegate
Workshop 1 *John Charles*

Senior Identity Architect
Workshop 1 *Thomas Hardjono*

Sharing of Personal Data via MIT OpenPDS

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Students today increasingly use social media as a means of interacting with peers and other members of the MIT community. The day-to-day life of a typical student on campus generates a surprisingly large amount of personal data – both consciously-generated data and data generated subconsciously as a by-product of conducting a task. For example, when a student posts a Tweet, Facebook entry or photos online he or she is consciously and voluntarily generating personal data. When a student runs from one lecture to another on campus, he or she generates GPS location data by virtue of the devices they carry.

The personal data generated by members of the MIT community represents a new asset class to both them and potentially to MIT. The leadership at MIT understands the importance of this new asset class, and a new initiative called the *MIT Living Lab* has been established on campus which seeks to facilitate the creation of trusted repositories of personal data called *personal data stores*. MIT's own implementation is called MIT OpenPDS. In this vision, each of the community members would each own a repository of personal data (an OpenPDS instance), which they could share with other members of the MIT community, including social scientist, data scientists and other researchers. This personal data could be used to help MIT improve itself, better facilities, classrooms, public health, etc., making MIT a true living laboratory for its students, faculty and staff.

Additionally, an MIT community member may choose to share personal data in their repository with researchers from outside MIT. When a researcher outside MIT seeks to access a personal data store within MIT OpenPDS, the researchers must not only authenticate himself/herself to MIT infrastructure (e.g. via InCommon), but also obtain explicit consent from the owner of the OpenPDS instance. OpenPDS allows its owner to set the “degree” of sharing as a way to preserve privacy of the owner. For example, the owner may allow GPS data-sets to be accessed but with the mobile phone number automatically removed upon access. A personal data store is a useful method to store *attributes* regarding the person (e.g. student, faculty), and giving each community member an OpenPDS instance empowers that person to share these attributes – which is in-line with the aims of *attribute-sharing* in TIER.

There a number of identity and privacy requirements for the campus infrastructure implementing personal data stores. Some of these are as follows:

Strong authentication and authorization: Authentication of MIT community member when accessing the personal data store of another community member. Authentication of a Non-MIT entity federation member (e.g. InCommon member) seeking access to the personal data store at MIT.

Delegated authorization: Owners of personal data stores must grant access to not only the requesting party (e.g. another person), but also to the Application software being used by the requesting party.

Logging and audit of requests and data access: If the data stores are hosted at an institution, then it its hosting infrastructure must provide built-in accountability features that log/audit access history information and make these transparent to the data store owners.

Data confidentiality and privacy: Confidentiality and privacy-preserving technologies must be used for personal data residing in these repositories.

New York University (050.nyu.1.20150412)

Modified: 4/12/2015 3:15:11 PM

Participants

CIO or CIO Delegate
Workshop 3 *David Ackerman*

Senior Identity Architect
Workshop 3 *Gary Chapman*

Data Issues Are Killing Us

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Background

NYU is large in size, very diverse, very complex. Innumerable constituencies and silos remain (or are newly created!). We've been working on central identity management with a "Registry" and its data as a foundation element for 2 decades. NYU has been aggressively evolving, expanding, intensifying in just about every dimension, including everything to do with IT services, over this period. Is its possible that we spend so much effort adding floors to our building that strengthening its foundation never receives proper attention?

Problem Description

Version 1: GIGO

Version 2:

Our core identity management approach can be described as follows:

1) Track the affiliations of members of the community

e.g. who is a current degree student? who is a current adjunct faculty member?

who is a current contractor?

2) Assign a set of privileges based on current affiliation(s); de-assign privileges when enabling affiliations end.

This strategy depends fundamentally on data management, which centers for us around a "person registry" that obtains source data from authoritative systems of record SORs). "Bad source data" then risks "bad privilege management". Not to mention the overhead that comes from service problems, client support, troubleshooting, manual fixes, etc etc when members of the community are unable to readily access the services or data to which they are entitled.

Unfortunately data management and quality is less than perfect.

- Across SORs, consistency is weak (and unmeasured); integration between SORs is spotty.
- Overall data governance/stewardship is only now in the early data of serious coordination; a common data dictionary is not in place.
- Much data management is highly distributed, even discretionary (e.g. student employment de-activation).
- Even touchstone concepts are subject to change! (e.g. we used to have "departments" at NYU!).
- Data elements captured or retained (and associated business processes) don't necessarily match identity management needs (e.g. proofing).
- The only system of record for affiliates (e.g. contractors, visiting scholars, etc etc etc) is the identity registry itself – there is no associated business office with a responsibility for data management and a stake in its accuracy.
- Some of our tools (our Registry itself!) is largely locally developed code.

A different statement of the source problem: the many, specific purposes for which data is maintained in source systems do not magically align with or directly support IdM purposes. We are trying, for example, to know who is a "current adjunct employee" (or even a "recent adjunct employee"), but such designations are not core to the system from which we obtain employee information. So we have to compute this affiliation (so its definition is not something necessarily commonly agreed upon) or we have to customize the HR system to make this calculation for us (and the proprietors of that system tend to perceive little ongoing importance of that calculation).

Examples

• multiple NetIDs are assigned to the same person

• our fancy new SIS system has a 30 character field to describe foreign study of a student, with no data input requirement that the actual global location of the "program" be mentioned!

• typos! typos! typos!

• we hope to federate with our business school - but even if we used a common identifier for all members of the affected school population, we have completely disjunct processes for maintaining affiliation records: our list of business school community members overlaps 80% with their list!

• we find student employees with anywhere from 1 - 10 "active" jobs, which means "active job" just isn't a reliable indicate of precise current employment!

• we implement (over-complicated) privilege “grace periods” so as not to cut off access prematurely and allow time for source records to be updated indicating continued affiliation with the institution – which means we provide privileges in fact for “too long” for some people.

What to do? What to do?

Option A. Continue to bumble along

Option B. An organized, multi-front attack on the problem

Option C. Option A + at least a bit of Option B!

New York University (051.nyu.2.20150403)

Modified: 4/3/2015 8:20:09 PM

Participants

CIO or CIO Delegate

Workshop 3 *David Ackerman*

Senior Identity Architect

Workshop 3 *Gary Chapman*

Challenges of a Global University

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Over the past 5 years, NYU has conducted a *massive* expansion in the global dimension, highlighted by:

- expansion/improvements to 14 study-away sites around the globe
- creation of major new campuses in Abu Dhabi and Shanghai

A whole new IT organization (Global Technology Services) was actually created in order to provide sufficient focus and resources to support technology services in and to these evolving locations.

In this context, every IT-related conversation, project, plan over recent years has now come to include serious consideration of "global" impact and viability. Our "degree of difficulty" has certainly gone up as a result of the global dimension, all the new employees and consultants, all the new needs and desires centered around the global locations.

These kind of questions arise:

• What will end-user performance in Abu Dhabi be like? In Shanghai? In Ghana? Can we test here in New York by rigging up a network segment with increased latency?

• How can they be allowed to put up Exchange when nobody else at NYU uses it?

• How come the data feed (!) we get of HR data from NYU Shanghai contains Chinese versions of names in parentheses despite our understanding all business would be conducted in English?

• How can we provide unfettered access to the Internet from Shanghai?

• Should our enterprise service bus (or other middleware infrastructure) have instances in multiple global geographical locations? If we put stuff in Amazon, does that help or hurt with respect to global access?

• Is it okay to put a Radius server with local password stores in every global site we have so that if long-haul Internet connectivity is disrupted, local wireless access will still be possible?

• Can we synchronize multiple instances of a database not just across data centers in NYC or in the US, but between here and China or here and Abu Dhabi?

• Will Duo 2-Factor authentication work everywhere? Better test!

So, the various dimensions that now color every discussion and plan include:

• Policy – NYU and regional

• Provision of application services: New? Different ones? Special? Tuned-up?

• Support – Must provide 24x7x365 worldwide support now (and watch out for holidays!)

• Network infrastructure and application/database performance over great distances

Impact has not been negative in any significant sense on central identity-related services, and in fact global initiatives have provided in some cases strong motivation and even resources to enable improvements that benefit the entire institution.

Issues with something like in-person identity proofing (not something we much require) have not yet come squarely into focus, but the fact the we have staff in so many locations of the world would potentially help us significantly for those not in New York City.

Northwestern University (052.northwestern.1.20150412)

Modified: 4/12/2015 3:15:49 PM

Participants

CIO or CIO Delegate

Workshop 1	*Sean Reynolds*

Senior Identity Architect

Workshop 1	*Philip Tracy*

Onboarding is Hard

Actors

Individual User

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Dr. Kay Ahern has been hired into the School of Medicine as a post-doctoral research fellow. She will be working on an active human-subject research protocol (clinical trial), as well as performing related laboratory research using radioisotope labeling. As part of the onboarding process, Dr. Ahern is automatically issued a netid/password and an Exchange account, along with a small bundle of services given to all faculty and staff (wireless/physical network access and so forth).

Dr. Ahern’s local department IT staff request access to the SSLVPN infrastructure for remote access, and add her to several AD groups for departmental file/print sharing. A recently-hired colleague helps Dr. Ahern by showing her how to download and submit the forms required to gain access to the radioactive materials storage facility and the online IRB system. A department assistant reminds her to login to the LMS to sign up for two different types of required lab safety training.

A month after starting, Dr. Ahern discovers she must also request access to the online effort reporting system for one of her grants, and take additional training in order to use the medical school’s shared equipment facility. Three weeks later she also discovers that she needs to fill out yet another form to request access to research project data that is stored on a system administered by the teaching hospital involved in the research protocol.

Northwestern University (053.northwestern.2.20150412)

Modified: 4/12/2015 3:16:09 PM

Participants

CIO or CIO Delegate

Workshop 1 *Sean Reynolds*

Senior Identity Architect

Workshop 1 *Philip Tracy*

I just need to share some stuff with a few people…

Actors

Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Tom the IT Guy works for the Department of History. Tom has been directed by his department chair to set up a website/application that will:

Highlight the department’s current research and areas of faculty expertise

Serve as a recruiting tool for faculty and graduate students, providing a way to interact with prospective faculty and students

Host the department’s calendar of seminars, receptions and outside talks

Provide an informal “chat” space for faculty and graduate students to discuss miscellaneous administrative and academic matters

Provide a way to share documents among faculty and graduate students

Tom talks with central IT, who offer him a Sharepoint site, access to the centrally-funded Box site, or an applet inside the University portal. These have most of the features Tom wants, but all are limited to users that already have campus-issued netids, which makes the recruiting features difficult or impossible to implement.

Tom decides to stick with Sharepoint for now since it’s easy to set up. Central IT creates an automatically-updated Active Directory group for “history department” based on data coming from HR and the student information system. This works reasonably well, except that it turns out the department wants to exclude faculty with joint appointments in the English department. Eventually IT helps Tom by adjusting the rules populating the “history department” group.

A few weeks later, Tom’s boss asks for a portion of the site to be restricted to tenured faculty only. Tenure status exists only in the HR system, so Tom again asks IT for help. IT suggests that Tom make a web service call into the HR system to check for this in real time. Tom asks why he can’t just use the existing web access management system he has recently learned about. IT tells him that (a) the WAM system doesn’t currently work with Sharepoint but might someday, and regardless of that, (b) WAM doesn’t have direct access to the tenure data either (HR only). In the end, Tom settles for a manually-administered AD group which he will have to update periodically based on department records and HR system queries.

After 6 months, the need to extend the system to users without University netids becomes more pressing, and Tom again approaches IT for help. He is told his options are to wait for IT to put up a Shibboleth SP or get ADFS working, issue all users a new account. It may also be possible to accept logins from social web sites. Tom thinks this over and then becomes concerned that at some point he will want to know with more certainty what actual person the social identities belong to, and wonders how to record, store and reference that information.

Oregon State University (054.oregonstate.1.20141205)

Modified: 12/5/2014 9:31:53 AM

Participants

CIO or CIO Delegate

Workshop 1 *Lois Brooks*

Senior Identity Architect

Workshop 1 *Erica Lomax*

Managing external community identity/accounts

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Our IAM solutions are based on our institutionally issued ID which is sourced from our SOR (Banner HR and Student). We currently have very limited ways to issue accounts to the greater OSU community that needs access to campus resources. This population is large and includes diverse groups employees of external companies housed on OSU campus, co-located state & federal employees, non-degree students, visiting researchers, and our Extension community volunteers.

There are several challenges presented in issuing accounts to these groups. First, most lack an existing SOR to allow automation of account provisioning and deprovisioning. The responsibility for manually creating and managing accounts needs to be distributed throughout the entire university.

Second, people in these groups often have affiliations with one or more groups and/or are also members of our internal (student/employee) community.

We need a solution that will allow searching and creation of identities along with person matching to existing identities that can integrate with existing account provisioning technologies. There need to be APIs into it to allow automation of identity creation for those that have SORs.

Oregon State University (055.oregonstate.2.20141205)

Modified: 12/5/2014 9:32:07 AM

Participants

CIO or CIO Delegate

Workshop 1 *Lois Brooks*

Senior Identity Architect

Workshop 1 *Erica Lomax*

Central Authorization Toolkits

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

We are now implementing broader tools (Grouper) for support of centralized authorization. The next step is to bring existing and new campus software solutions online with supporting the centralized information. Tools and/or documentation for integration to commonly used commercial and open source products as well as toolkits for custom software development in commonly used languages.

Oregon State University (056.oregonstate.3.20141205)

Modified: 12/5/2014 9:32:38 AM

Participants

CIO or CIO Delegate

Workshop 1 *Lois Brooks*

Senior Identity Architect

Workshop 1 *Erica Lomax*

Local SAML metadata management/aggregation

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

We currently have a limited number of campus systems using our Shibboleth IDP. As that number continues to grow, there are significant benefits for the aggregation and publishing of SAML metadata. We would like to have a method similar to InCommon's process to allow registering/updating of metadata by the IDPs and SPs.

Oregon State University (057.oregonstate.4.20141205)

Modified: 12/5/2014 9:32:51 AM

Participants

CIO or CIO Delegate

Workshop 1 *Lois Brooks*

Senior Identity Architect

Workshop 1 *Erica Lomax*

Multiple account to individual identity mapping

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

As we mature in our identity processes, we're dealing with a legacy of manual accounts for individuals with limited and inconsistent attributes. Our users have multiple user accounts in our Active Directory forest. We have tens of thousands of these accounts with attributes that need to be matched to individual identities.

Even without a full-fledged person registry, there is a need for a person matching algorithm/code/tool that could be plugged into account management processes. This may be something that is run administratively against a data source (e.g. Active Directory or export of data) or may be an interactive user process (e.g. account claiming web interface).

Penn State (Pennsylvania State University, The) (058.psu.1.20150412)

Modified: 4/12/2015 3:17:35 PM

Participants

CIO or CIO Delegate

Workshop 1 *Kevin Morooney*

Senior Identity Architect

Workshop 1 *Nick Roy*

Multiple Competing ERPs

Actors

Service Provider ← this is the main actor in this story

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Note: all stakeholder groups are important in this story, but the typical/traditional ones affected by big ERP changes are students and employees.

As a large and extremely distributed research university, Penn State has several different, frequently siloed and competing sources of authority for the same type of information for a single individual. Multiple ERPs for HR – one for most university employees, one for medical center staff and one for medical center faculty. There are also new student ERP (PeopleSoft), new HR ERP (WorkDay) and legacy ERPs (built on the mainframe by EDS in the 80s) all working toward either implementation or close-down, at the same time. Some systems are capable of transactional commits of identity data to our central person registry. Some are batch-only. Meanwhile, we are working toward implementation of a unified person record in our person registry. We need to support both batch and real-time or near-real-time transactional parity across all these systems, and implement policies and processes in the systems that result in a predictable and unified end result for the user. Support for both off-the-shelf and custom registry connectors are important, as is a rules engine and visibility for the rules into data from all contributors to be able to make decisions about what data to update when.

Penn State (Pennsylvania State University, The) (059.psu.2.20150412)

Modified: 4/12/2015 3:18:21 PM

Participants

CIO or CIO Delegate

Workshop 1 *Kevin Morooney*

Senior Identity Architect

Workshop 1 *Nick Roy*

Replacement of Legacy Systems

Actors

Service Provider ← This is the main actor in this story

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Parents, Bill Payers, etc.

Story Narrative:

Note: all stakeholder groups are relevant for this story

Penn State has many mature but long-in-the-tooth as-built systems related to IAM. We are in the process of replacing these with new custom systems (the Penn State Central Person Registry) and many off-the-shelf systems (OpenLDAP, Active Directory Domain Services, Shibboleth, Grouper, etc.). While we do this, we need to improve our levels of support for customer integrations. Thus we are adopting systems that more stock software can work with. We need the ability to rapidly deploy new IAM systems via rapid bulk provisioning from our person registry, realtime updates via message-based provisioning and support for downstream customers via identity data warehouse functions (both LDAP and SQL for querying and bulk synchronization/"sanity checks"). Validation of data against legacy systems and bulk "shipping around"/"data plumbing" tasks are important in our current work of replacing the as-built with standard solutions. They will continue to be important as we work toward cloud-based solutions such as Office365.

Purdue University - Main Campus (060.purdue.1.20150412)

Modified: 4/12/2015 3:19:31 PM

Participants

CIO or CIO Delegate

Workshop 1 Gerry McCartney

Senior Identity Architect

Workshop 1 Robert Stanfield

Maintain Unique Identity Across Systems

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

To uniquely identify its faculty, students, staff, and affiliates, Purdue University has taken the approach of assigning an identifier to its constituents. This identifier is used to maintain a single identity across multiple identity sources (HR, Student, guest, etc), and to replace existing SSN use across campus. Purdue maintains this identity service as a locally developed application to minimize and eliminate duplicate identities from being created.

Previous investigation into alternatives in this “de-duplicate” space found no strong alternatives. This service is our basis for building identity.

Purdue University - Main Campus (061.purdue.2.20150412)

Modified: 4/12/2015 3:19:38 PM

Participants

CIO or CIO Delegate

Workshop 1	*Gerry McCartney*

Senior Identity Architect

Workshop 1	*Robert Stanfield*

Authorization Management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

A professor is co-teaching a course within the campus learning management system. To give access to a non-Purdue student, each external student must be given a local credential, provide the credential information back to each student, and then add that student login to the particular section within the LMS for the course they are co-teaching.

Purdue hires a consulting company to assist with an HR project. A local credential is created for the consultant, but then the appropriate access is granted within the ERP system.

In both cases, authorization management is done locally at the application level, in addition to the need for a local account. While centralized authentication and authorization are available, granting external (and internal) constituents authorization to resources is challenging due to the lack of application support for centralized authorization management.

Rice University (062.rice.1.20150412)

Modified: 4/12/2015 3:21:11 PM

Participants

CIO or CIO Delegate

Workshop 1 *Klara Jelinkova*

Senior Identity Architect

Workshop 1 *Barry Ribbeck*

IAM and Research

Actors

Individual User
Home Organization
Virtual Organization
Collaborating parties and vendors

Stakeholder Groups

Researcher/Scholar
Learner/Student
External collaborator or contractor

Story Narrative:

(HPC ACCESS EXAMPLE)

Actors: Individual User, Virtual Organization, Home Organization | Stakeholders: Researchers, External collaborator 12/18/2014

Rice HPC plays host to and shares HPC resources with many external parties including actors in the Texas Medical Center and international communities such as the University of Sau Paulo. There are no difficulties in providing access through our visitor processes. The challenges are with managing credentials and access controls based on non-standardized processes and policies. The challenges do not lie in credentialing or vetting but in ensuring appropriate access to external identities in a more automated manner. With large numbers of institutions involved and constant change in the players there are difficulties that occur when a collaborator who breaks ties with an institution where credentials are issued but remains active in the Virtual Organization. We need better processes for ensuring the credentials for identities are persistent and access controls are well managed. Credentials should be persistent for as long as the participant is alive, only access should be changed as may be appropriate.

(Making it easier for Medical Research players)

Actors: Individual User, Virtual Organization, Home Organization, Collaborating Parties | Stakeholders: Researchers, External collaborators and contractors 12/18/2014

Lowering the barriers for non or semi academic institutions with HIPPA requirements to participate in InCommon IAM services and resources is a step in the right direction. When we can define a goal of allowing all players to be able to identify themselves ubiquitously this will aid in lowering those barriers. Proprietary systems meant to server single entities will either need to expand their reach or we will need to ensure that our inter-institutional credentials can be appropriately mapped to intra-institutional identities that will allow access.

(Data Sharing)

Actors: Individual User, Virtual Organization, Home Organization | Stakeholders: Researchers, External collaborator 12/18/2014

Another area of prospective need include collaboratively shared documents for publication or grant management. Much work and data are stored and collaboratively developed externally and then brought into the institutional perview only after the work is near completion. If this is an issue as seen by the institution, then we need to address it appropriately by providing well managed data sharing from within the institution or by ensuring that data owned by the institution is identifiable in external resources. Efforts like those of I2 Net+ Box are making data exchange collaboration across all aspects of Higher Education real with low I.T. barriers and high functionality. I would caution that while these collaboration supporting applications are good much of the work has been focused on access and sharing and little has been focused on long term data management.

Rice University (063.rice.2.20150412)

Modified: 4/12/2015 3:22:05 PM

Participants

CIO or CIO Delegate
Workshop 1 *Klara Jelinkova*

Senior Identity Architect
Workshop 1 *Barry Ribbeck*

In support of non-premise based services

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Any or All - ALL Actors APPLY in this scenario – Vetted 12/18/2014

Any or All - All Stakeholders APPLY in this scenario – Vetted 12/18/2014

“Cloud” SaaS applications are growing at a fast pace as premise based installations of applications which require higher vendor overhead drives businesses to re-assess their support models and become more competitive. We are experiencing a very fast adoption rate of these services which may have been premise based in prior years but are only available “in the cloud” today or in near term release options from the vendors. Some of the challenges include having to assist vendors in the implementation of SAML and especially those who need to understand leveraging external RBAC services. Providing functional standards for interoperability and service bus access for data exchange is needed. Standards for vendors are poorly followed and we have experienced multiple levels of interoperability with vendor software under “integrates with LDAP or AD” statements even within those applications provided under Net+.

Changes in Browser default configuration by the browser manufacturers have also had a negative effect in the SAML space. SAML is somewhat difficult to support for users who need multiple profiles. A professor trying to access a MOOC using SAML based access as a student has to use 2 different browsers or clear cookies and this makes the workflow difficult. The ability to escalate and de-escalate privileges on the fly, multifactor authentication or client log off are areas of development that may be useful. Many of these type of changes need to be funded in support for SAML installations in the future to make the protocol useful for adoption by vendors.

Adoptions of external authentication providers is challenging without well-established standards for LOA. Self-asserted credentials trust mapping and user pairing is an identified challenge when looking to adopt external credentials that have the potential for allowing low initial barrier access to extra-institutional collaborations.

Rutgers University (064.rutgers.1.20141126)

Modified: 11/26/2014 12:57:05 PM

Participants

CIO or CIO Delegate

Workshop 1 *Don Smith*

Story 1: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Rutgers University (065.rutgers.2.20141126)

Modified: 11/26/2014 12:57:06 PM

Participants

CIO or CIO Delegate

Workshop 1 *Don Smith*

Story 2: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

The Ohio State University (065.rutgers.2.20141126)

Modified: 4/12/2015 3:22:49 PM

Participants

Applicant Access and Matriculation

Actors

Individual User
Service Provider

Stakeholder Groups

Learner/Student

Story Narrative:

(Technical Title: Federated Access to University Data and Initial Account Provisioning by Applicants)

John Doe is a high school student applying for admission to the university. As part of the application process, he identifies an account with a social identity provider, an ISP, or possibly a national testing service. The university, as part of the application process and initial identity creation, registers an identifier associated with this account. He uses this account to authenticate to university resources available to applicants, such as early access materials or to check the status of his application.

Upon admission to the university, the applicant again authenticates with the registered account in order to perform initial activation of his university account and set an initial password.

University of Arizona (067.arizona.1.20141205)

Modified: 12/5/2014 9:35:59 AM

Participants

CIO or CIO Delegate

Workshop 1	*Michele Norin*

Senior Identity Architect

Workshop 1	*Gary Windham*

External Access for Humanities Seminar Programs

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student

Story Narrative:

The Humanities Department conducts short-term seminars where instructors put resources, occasionally copyrighted, online and make them available for download. Due to copyright terms, users must authenticate to access these resources. The participants in these seminars are largely non-tech-savvy, so creating a new account (e.g., in Drupal) is a cumbersome and mistake-laden process. Likewise, going through the UA's official "affiliate" registration process (which we call "designated campus colleagues"), is too time-consuming and complex (due to the workflow and approvals involved).

University of Arizona (068.arizona.2.20141205)

Modified: 12/5/2014 9:36:11 AM

Participants

CIO or CIO Delegate

Workshop 1 *Michele Norin*

Senior Identity Architect

Workshop 1 *Gary Windham*

Short-Term Access for Outside Reviewers on Promotion/Tenure or Academic Program Reviews (APR) committees

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
External collaborator or contractor

Story Narrative:

Departments are reviewed every 7 years by an outside committee; currently boxes of paper files are stored in a common location for them to review. Tenure track faculty are reviewed during the first 3-5 years of their contract, and tenured faculty at regular intervals for promotion. Currently, files are emailed, or shared via Dropbox/Google Drive to external reviewers.

As we move to electronic document storage, we will need to provide access to our repositories instead of hard copies or using third party providers. Reviews are typically completed within 6 weeks, start-to-finish.

University of Arizona (069.arizona.3.20141205)

Modified: 12/5/2014 9:36:22 AM

Participants

CIO or CIO Delegate

Workshop 1	*Michele Norin*

Senior Identity Architect

Workshop 1	*Gary Windham*

Access to Online Resources for Foreign Participants in COPH Summer Research Training Program

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student

Story Narrative:

Foreign (not US citizen or Perm. Resident) students in College of Public Health’s Undergraduate Summer Research Education Program in Phoenix, AZ need access to online resources required for the program. The “affiliate” registration process (DCC), used for US participants, becomes very time-consuming and laborious for these foreign participants due to requirements around identity-proofing (visa documentation, résumé/CV, etc).

University of Arizona (070.arizona.4.20150412)

Modified: 4/12/2015 3:23:47 PM

Participants

CIO or CIO Delegate

Workshop 1	*Michele Norin*

Senior Identity Architect

Workshop 1	*Gary Windham*

Access to AZ TRAIN (online learning resource for public healthcare professionals)

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

External collaborator or contractor
Public Health Workers

Story Narrative:

The Arizona Public Health Training Center (AzPHTC) is part of a network of 38 Public Health Training Centers nationwide, funded by Health and Human Resources and Services Administration (HRSA), and operated by UA's College of Public Health. This service has a very diverse user base, most of whom are not affiliated with the University of Arizona at the time they use AZ TRAIN, but may be at a later date. The use of site-specific credentials with AZ TRAIN, and similar services, leads to forfeiture of any opportunity to track and leverage the user's interaction with the UA in a broader context.

University of Arizona (071.arizona.5.20141205)

Modified: 12/5/2014 9:37:12 AM

Participants

CIO or CIO Delegate

Workshop 1 *Michele Norin*

Senior Identity Architect

Workshop 1 *Gary Windham*

Extending the "reach" of central person registry

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Staff

Story Narrative:

Certain campus units (e.g., College of Engineering, Residence Life) have expressed the desire to reflect "local/contextual" attributes in the central person registry. Certain of these attributes (e.g., roles, workgroups, etc) can be expressed via Grouper groups, but others (e.g., location/time-based attributes, unofficial organizational relationships) cannot. Hence, there is a desire to "mash-up" locally-sourced/managed attributes with the standard "institutional" attributes reflected in the person registry, but using a common service/protocol. From the central IT perspective, we wish to provide this capability, but in a "decentralized/federated" way where organizational units can manage their own attributes, schema, and relate them to institutional person entities in a scalable, extensible manner.

University of Arizona (072.arizona.6.20141205)

Modified: 12/5/2014 9:37:25 AM

Participants

CIO or CIO Delegate

Workshop 1 *Michele Norin*

Senior Identity Architect

Workshop 1 *Gary Windham*

Event-based provisioning/de-provisioning

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

A confluence of factors (the explosion in cloud services, an ever-increasing set of “institutional affiliation” vectors, etc) has resulted in a “hue and cry” in recent years for real-time provisioning/de-provisioning of access and entitlements, based on identity life-cycle events. The status quo (overnight batch processing of changes to person data) has become woefully inadequate. While we have certain point-to-point integrations that facilitate a more “real-time” approach for certain, key applications (e.g., the ability to generate your NetID, get your email account, and login to ERP applications), there is a need for more a pervasive notification/messaging model, that allows any service provider (central IT, or departmental) to consume identity lifecycle “events” proactively. The portfolio of services required by various constituents at the University is complex, varied, and dynamic enough that a batch-oriented, or even a centralized “push-based” real-time model, is insufficient.

University of Arizona (073.arizona.7.20141205)

Modified: 12/5/2014 9:37:49 AM

Participants

CIO or CIO Delegate

Workshop 1	*Michele Norin*

Senior Identity Architect

Workshop 1	*Gary Windham*

Identity continuity

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Many departments and programs engage with prospective students via “ancillary” vectors--outreach programs, seminars, etc., many of which have an online component requiring some form of identity/authentication. Several departments have expressed the desire to be able to track identity continuity across time and multiple “engagements” with the University. This “identity metadata” should bridge gaps between University engagements/encounters, as well as “pre-“ and “post-“ University life.

University of California - Berkeley (074.berkeley.1.20150412)

Modified: 4/12/2015 5:59:40 PM

Participants

CIO or CIO Delegate

Workshop 2 *Lyle Nevels*

Senior Identity Architect

Workshop 2 *Jeremy Rosenberg*

Sharing an email account

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

A program in a department is implementing a by-appointment tutoring system and needs the ability to track and field all requests for by-appointment tutoring. A student coordinator will assist the program coordinator in administering the program, and thus, will need admin privileges to the email account. The email service providers used to issue departmental email accounts for this purpose. But this required users to share a common password to access the departmental account. When a student coordinator was replaced, someone would need to remember to change the password and tell the new password to the new user. It was also not possible to determine who was acting on behalf of the departmental account at any given time.

To solve this problem, the central Identity Management team developed a Special Purpose Account which is a computing account which is tied to a Grouper group. Any member of the group can login to any CAS protected system with their own credentials and impersonate the departmental account. Now the student coordinators can be managed through group membership, using their own computing accounts to access the departmental email and shared file spaces. All access is logged through the CAS logs and the department is able to share coordination responsibilities without sharing passwords.

University of California - Berkeley (075.berkeley.2.20150412)

Modified: 4/12/2015 6:00:48 PM

Participants

CIO or CIO Delegate

Workshop 2 *Lyle Nevels*

Senior Identity Architect

Workshop 2 *Jeremy Rosenberg*

Professors need to email all students in a section

Actors

Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff

Story Narrative:

A professor is teaching a course. She needs to send emails to all students in the various sections. She tries to get her teaching assistants to maintain accurate lists of students in her courses, but she finds she gets inconsistent lists. Some keep up with changes to course rosters really well, others set up the list once and forget about it. As a result some students are left without important information.

The professor brought this to the attention of her departmental administrator who followed up with the central identity team. Because the Identity management team had automated the population of Grouper groups based on enrollment information pulled from the Student Information System, they were able to automatically populate and update Mailman mail groups each night with current enrollment information. Now the professor can email her various course sections knowing that the list membership is automatically kept current.

University of California - Merced (076.ucmerced.1.20150412)

Modified: 4/12/2015 3:25:45 PM

Participants

CIO or CIO Delegate

Workshop 3 *Ann Kovalchick*

Senior Identity Architect

Workshop 3 *John Kamminga*

Other Institutional Identity Needs

Workshop 3 *Nick Dugan*

User Name Change

Actors

Individual User

Stakeholder Groups

Staff

Story Narrative:

Recently, the IDM team was notified that a student, Yaqueline Airam Parra (UCMNetId: “yparra2”), had completed a new legal name change to Yaqueline Airam Parra Aragon (UCMNetId: “yparraaragon”).

Contact was made with the student, and IDM renamed the UCMNetId successfully. Additional checks were requested from the UCMCROPS (UCM’s learning management system) support staff to reassign access to that service, swapping the old UCMNetId with the new account, as well as the Office 365 team to verify that the account was correctly reflected as the newly renamed UCMNetId, licensing was appropriately assigned, and email access was active.

There has been a pattern of errors related to DirSync, the application required for synchronization between Active directory and O365 as attribute modifications being applied locally are not reliably relayed. These errors result in a disassociation between the local domain user account and its related cloud user account, essentially disabling the service for the user until adjustments are manually performed.

Additional services such as access to CatCard (UCM’s ID Card and Access System) are handled by our many data feeds, and take affect once the data is entered into IDM and fed to those downstream systems automatically.

These changes and checks must occur in a particular order, and can take anywhere from as little as 60 minutes, up to the following morning, depending on the status of a user. In this case, all went smoothly and the user was operational with their new UCMNetId with no issue.

Issues arise in downstream systems not setup to handle userId changes. For example, the CatCard system receives a feed file from the Identity management system and sometimes will create a new Identity (e.g. yparraaragon) in their system instead of matching it to the existing account “yparra2”. Then, access will be given to the wrong account and the user will complain because they do not have access to a building. This can be very time consuming to track down as well.

University of California - Merced (077.ucmerced.2.20150412)

Modified: 4/12/2015 3:26:42 PM

Participants

CIO or CIO Delegate

Workshop 3 *Ann Kovalchick*

Senior Identity Architect

Workshop 3 *John Kamminga*

Other Institutional Identity Needs

Workshop 3 *Nick Dugan*

Duplicate Identities

Actors

Individual User

Stakeholder Groups

Staff

Story Narrative:

On 04/25/13, the UCMNetId: “traczkowski” (**Thad Traczkowski**) was provisioned by a departmental MSO. On 5/13/2013, UCMNetId: “traczkowski2” was provisioned, by the same MSO (**UCLA Staff, Departmental MSO)**, and for the same individual. After confirming with the departmental MSO, the two accounts were merged, keeping “traczkowski” for use by Thad going forward.

On 3/12/2015, IT staff were contacted about a problem with Thad’s ability to print, as well as access to the BruinBuy (Electronic procurement system) service housed out of the UCLA campus.

Troubleshooting via the Identity Management system indicated that only UCMNetId: “traczkowski” existed for this user, the duplicate account did not exist in IDM anymore. However, UCLA staff reported that they had two accounts, “traczkowski” and “traczkowski2”, still in their records. Confirmation that there should only be the single account for Thad clarified the issue and Thad reports successful access to the BruinBuy service.

In this situation, it appears that the local merger of the two accounts may have occurred after the information was fed to UCLA for use by BruinBuy. We were notified of it only after the user contacted us, in this case two years later. There is no reason for them to have known, but is an indicator of the weaknesses in our Identity Management system that potentially occur from duplicate accounts.

University of Chicago (078.uchicago.1.20150412)

Modified: 4/12/2015 3:27:34 PM

Participants

CIO or CIO Delegate

Workshop 1 *Klara Jelinkova*

Senior Identity Architect

Workshop 1 *Tom Barton*

Shibboleth Authentication, password management, and session management, step-up interaction

Actors

Individual User

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

User is logging into an application where authentication is centralized by Shibboleth. User logs in via Shib credentials.

Password Self-Service - User wants to update his/her Shib password during the login process or after the login process (independent of application), setup their challenge response question, setup email, phone, and/or text contact information.

There are sensitive applications protected by Shibboleth the user is accessing. These applications do not have 2fa enforced by default. User logs into Shib user self-service screen and selects the application(s) he/she wants to enforce 2FA to.

Likewise, user logs into an application to process sensitive transactions. As the user clicks to process a sensitive transaction (e.g. e-prescription of controlled substances), user is prompted for an additional validation (e.g. 2FA) to confirm and secure transaction.

User forgets password, clicks on the ‘forgot password’ link. Shib will email the user, or text the user a new password reset link. User can also choose to answer challenge & response questions.

University of Chicago (079.uchicago.2.20150412)

Modified: 4/12/2015 3:27:46 PM

Participants

CIO or CIO Delegate

Workshop 1 *Klara Jelinkova*

Senior Identity Architect

Workshop 1 *Tom Barton*

Shibboleth Service Provider Integration

Actors

Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Web application owners often default to LDAP as the user store repository because it is easier to integrate than Shibboleth.

A Service Provider administrator who wants to use Shibboleth should be able to use an easy to navigate configuration page to allow for: self-service enrollment of the application, allow for application specific configuration (session time out, 2fa enforcement, step-up auth, etc), and attribute management.

Once configured, if part of inCommon, Service Provider administrator wants to connect to a non-prod environment to test the integration without developer interaction unless there are issues.

University of Florida (080.ufl.1.20150412)

Modified: 4/12/2015 3:28:16 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Weak Person identity

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
External collaborator or contractor

Story Narrative:

There are two major cases of weak identity: The invited person and the self-asserted. These encompass about 100,000 distinct user accounts at UF.

The invited persons can be collaborating researchers, consultants, and/or Parents/Guardians of students. These identities are brought into UF by the invitation of the person whom controls the data they would like to access. Most identities receive a UF account and credentials. UF has a strong desire for social identities and federated identity usage in this situation. UF wants to limit the creation of local credentials to a much smaller number of these individuals, base it on the risk of permission granted and the ability to federate from their institution.

The self-asserted cases are used largely for educational outreach programs in extension and other areas, such as K-12 educators and a few others. Activities exist that they, as the Public, can consume for free or fee based. They need a credential to access the material. We create a registry entry, assure the email is unique, and grant a small set of permissions to the self-asserted user. Ideally, these would be supported by social ids that are bound to a registry entry.

We have uses of this from the extension service, College of Law, College of Education and others who desire to provide outreach.

University of Florida (081.ufl.10.20150412)

Modified: 4/12/2015 3:30:42 PM

Participants

CIO or CIO Delegate	
Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*
Senior Identity Architect	
Workshop 2	*Dave Gruber*
Other Institutional Identity Needs	
Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Use of Non-Institutional Identities

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

The College of Engineering is partnering with a large number of other institutions to develop a graduate recruiting portal. Students will be able to login to the portal and enter demographic and academic data, and upload example coursework. Recruiters from partnering schools can login and screen applicants based on the submitted information.

Students and recruiters from InCommon federated institutions can use Shibboleth to authenticate to the portal. Since only a small subset of the 100-odd participating institutions support InCommon, a large number of students and recruiters will have to use alternate credentials. The effort required for UF to manage these credentials could be overwhelming, and jeopardize security if users select poor passwords because they cannot remember yet another.

University of Florida (082.ufl.2.20150412)

Modified: 4/12/2015 3:28:31 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Account Management

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

We have many needs regarding issues of account management:

Online students and other remote users may never be physically on the campus to enable in-person identity proofing. We need methods to support identity verification for both present and non-present users.

Users increasingly are working during non-business hours and from remote (often very remote) locations that prevent them from presenting at the Help Desk to reset a forgotten password. Existing approaches use trivial 'reset questions' that are too easily guessed by those other than the user, leading to compromised accounts.

An improved experience for maintaining passwords would benefit users and improve security. Possible features include indications of password strength and alerts to the user upon account changes – such as notification to alternate email addresses or via text message of password expiration, change events, and maybe failed attempts that indicate an attack.

IT staff can manually create arbitrary ‘service’ accounts in Active Directory and local systems. These accounts enforce no password controls, following no naming convention or check for duplicates or restricted names, and have no automated lifecycle management.

Attribute-based logic that defines which entities in the Registry are eligible for different account types, Levels of Assurance and credential strength requirements.

Account creation processes need to support both self-service and proxy creation. UF is so large and distributed that proxy functions are highly distributed. Software needs to guide self-service and proxy functions, minimizing errors.

University of Florida (083.ufl.3.20150412)

Modified: 4/12/2015 3:28:55 PM

Participants

CIO or CIO Delegate	
Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*
Senior Identity Architect	
Workshop 2	*Dave Gruber*
Other Institutional Identity Needs	
Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Assurance Features

Actors

Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Embed assurance related features to support concepts like: Level of Assurance, Assurance Vectors, Proofing on site, Remote Proofing of user not physically present at a "convenient site", and Risk level of Credentials based on permissions granted to the holder of the credentials (p1 – p5 at UF). These may need to consider multiple federation standards (Bronze, Silver for Incommon) (Orange and Apple for somewhere else or UF local LOA for internal federation).

Currently at UF, the LOA and credential strength are controlled by the manner in which a credential is created, proofed, is the data in registry, and the role permissions assigned.

MFA is a desire as UF moves forward, but it's currently not implemented.

UF has completed self-service setup credentials to a monitored level 5 credential.

University of Florida (084.ufl.4.20150412)

Modified: 4/12/2015 3:29:11 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Automatic Entitlement provisioning/de-provisioning for services based on select person and source system attributes.

Actors

Home Organization
Virtual Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Goal is to take action within 15 minutes or less on an individual based on attributes such as affiliation, EduPerson affiliation, assurance level, etc. and provide automatic provisioning and de-provisioning capabilities when trigger events happen. Affiliations are created and/or changed. UF has a lifecycle for affiliation and the accompanying rules for a certain small set of allowed permissions like: Student Lifecycle, Employee Lifecycle, Cont. Education Lifecycle, and other actions such as employee termination, retirement, elapsed time since last certification, and edits for training and segregation of duties.

A more robust implementation of these capabilities would be a very useful tool.

The feature here is event recognition and then the desired effect. Override capabilities of this are required at times due to special circumstances.

University of Florida (085.ufl.5.20150412)

Modified: 4/12/2015 3:29:24 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Event Driven messaging for ingest from sources and provisioning/deprovisioning to services and related system components

Actors

Home Organization
Virtual Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Goal is a maximum 15 minute delay in data propagation/replication. Provide event triggered ingestion from sources of record, such as HR, SIS, Researcher, other Related Organization sources. Same is true for provisioning to services or related system components that receive data from the IAM system. A data centric messaging approach should be considered. Recognizing that at certain times mass term changes in student status, it may be better to call a batch interface. In all cases, the same API/web service logic and edits should be applied.

IAM staff and any dashboards interfaced to the Registry need distributed intake. Depending on the person and his/her attributes, changes can be requested, approved or implemented. The source of record information cannot be changed, except by special administrator access. UF currently supports a network of about 500 locations that provide input to the IAM registry and access privileges via an online interface. Each location has at least two workers in the area.

Since the registry functions as a person data hub, the systems of record must first interact with the person Registry to locate or create a person. This means HR, SIS and others do not control the basic Person master data.   The registry owns Person Master Data. As the Person Master Data owner, the registry must be able to quickly and accurately forward information to dependent applications.

University of Florida (086.ufl.6.20150412)

Modified: 4/12/2015 3:29:43 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

IAM Logging & Monitoring

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Currently, UF monitors for expiring permissions, certain data quality, and revocation of certain access automatically. This is currently not granular nor proactive enough. Goal is to provide both proactive and reactive reports and analytics against data content, logs and audit trails recorded during the management of user and permissions as well as the use of those activities. The result would be the capability to perform the following: Threat Recognition, Audit Compliance, Data Quality, Permissions vs Risk vs Assurance Level of accessing person organization or thing. etc.

Need to provide a way to manage risk and detect possible threats in a better manner given the issues faced each day.

University of Florida (087.ufl.7.20150412)

Modified: 4/12/2015 3:29:59 PM

Participants

CIO or CIO Delegate

Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*

Senior Identity Architect

Workshop 2	*Dave Gruber*

Other Institutional Identity Needs

Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Registry allows for multiple Identifiers for an object of the registry.

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Since the registry should consider People, Organizations, and “things” on the internet, accurate Identifiers become important for these objects.

A primary Identifier (UFID in UFs case) should be associated with an object instance. However, persons may need to be known via multiple identifiers: Shands Badge number, orcid id, State of Florida Library ID, Gator One Id Card, Prox Device, COMITT ID, Board of Governors ID, National Identifier are a few examples. Need the ability to add and associate these identifiers together onto a particular person.

University of Florida (088.ufl.8.20150412)

Modified: 4/12/2015 3:30:21 PM

Participants

CIO or CIO Delegate	
Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*
Senior Identity Architect	
Workshop 2	*Dave Gruber*
Other Institutional Identity Needs	
Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

Identity Resolution and Matching

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

The goal of the Registry at UF is to create a single instance of the “person”. It is the authentic master data source for base person data. With that said and based on current matching algorithms and searches we see a small percentage of cases with multiple/duplicate person records. These occur normally at the intake of a person as a student applicant or in some cases when an HR entry is made with full employable identifiers for the person.

A matching algorithm needs to be strong and customizable.

However, the Identity resolution process needs to account for the merging of primary identifiers into a single authentic person record. The process should allow for a state to be recorded in the registry and associated account credentials so that the person is “frozen” until administrators collectively work to resolve. The multiple identifier occurrence. System that may have consumed the person master data info are coordinated while the person is frozen to adjust their respective applications as needed.

UFID, GatorLink Account Credentials, SIS, HR, Active Directory etc. all need to be adjusted to the resolution and part of the process. Some parts of the process are manual some are automated.

In the end a user is resolved to a single person record with a single credential, email, etc..

What are primary cases? A) Eastern Culture foreign nationals often complete info especially names in reverse order, do not have National IDs and other data to easily match. Discovered by Admissions, International Center, and employment procedures. B) Parents who enter incorrect info usually an identifier for their applicant.

This has occurred on about .01 percent of the registry entries. However, the roughly 1500 cases per year over the past 11 years can create a good deal of effort. Early detection and prevention is the key to the work load involved.

If a person is found after significant entries are made in SIS and the HR / Payroll both then the cure is much more difficult. Thankfully the current cases of these most problematic cases are very low in number. Say less than 50 per year.

The registry, IAM as a whole and consuming Services of Person data needs to have a process supported by enough automation to keep this effort low.

University of Florida (089.ufl.9.20150127)

Modified: 1/27/2015 10:59:19 AM

Participants

CIO or CIO Delegate	
Workshop 2	*Elias Eldayrie*
Workshop 2	*Rob Adams*
Senior Identity Architect	
Workshop 2	*Dave Gruber*
Other Institutional Identity Needs	
Workshop 2	*Erik Deumens*
Workshop 2	*Warren Curry*

MFA Desire

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

Phishing attacks are constant and increasingly sophisticated, outpacing the ability for users to discern the malicious impact. At the same time, brute force attacks against user passwords have forced institutions to implement higher complexity requirements for passwords. This creates passwords that are harder for users to remember, which has required mechanisms for users to deal with forgotten passwords. These forgotten password mechanisms then become another avenue for attack.

Multi-factor authentication can provide relief for all of these problems by creating brute-force resistant passwords that constantly change (limiting the effectiveness of phishing) and allow the password that must be remembered by the user to be simpler and longer lasting.

University of Illinois - Urbana-Champaign (090.illinois.1.20141205)

Modified: 12/5/2014 9:24:08 AM

Participants

CIO or CIO Delegate

Workshop 1	*Mark Henderson*

Senior Identity Architect

Workshop 1	*Tracy Tolliver*

Affiliation Service

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Affiliates

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

We are a large research university with a diverse group of affiliates needing access to a variety of resources, electronic and otherwise. We have legacy identity and access management systems in place that were quite good at the time they were built, but unfortunately, the identity management portion of the system has been neglected for a number of years and does not support the wide range of affiliates needing support and does not support the entire life cycle of the mainstream affiliates such as students and employees that it does handle. This has resulted in service providers all over campus creating their own processes and systems for handling these users and their credentials. Any identity system being created for a university environment needs to recognize the diversity in affiliations and the need to delegate management of many of these affiliations.

We are in the midst of a large scale university-wide (3 campuses and university administration) identity and access management project in which we have an opportunity to re-architect our entire system. We are proposing an affiliation service that would allow for sponsored affiliations that could be initiated by the affiliate, the sponsor, or batch created. This service will utilize the central matching process, update/create identity records in the identity registry, and supply the affiliate with a “tokenized link” in email or a “registration token” to facilitate password setting/management. The service will also include administrative functions for the sponsor such as managing affiliate start and end dates for the term of the affiliation, expiration reminders, and possibly password registrar functions. The plan is to make this modular so that it can interface with other components of the central identity and access management system or it can be integrated by service providers where appropriate. It also needs to be a service that is very responsive, user friendly, and timely because many of these shadow systems were not only created because the central service did not handle the affiliate, but also because the central processes that do exist to handle “guests” are very manual, cumbersome, and slow.

Any identity management system in a box needs to provide for the affiliates who may not be handled by mainstream processes that are in place.

University of Illinois - Urbana-Champaign (091.illinois.2.20141205)

Modified: 12/5/2014 9:24:21 AM

Participants

CIO or CIO Delegate

Workshop 1 *Mark Henderson*

Senior Identity Architect

Workshop 1 *Tracy Tolliver*

Matching and International Students

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

We are a large research university and have a growing population of international students; in fact, we had the third largest international student population for 2013-2014, behind New York University and University of Southern California. Historically, we have had a high percentage matching process, primarily using first name, last name, date of birth, gender, and SSN (optional). With the influx of international students, we are experiencing difficulties with matching in some cases. The cultural differences in name conventions are posing issues. A shared matching algorithm that can support a global user base and a minimum data schema needed to support the process would be a necessary component in an identity management system in a box solution.

University of Iowa (092.uiowa.1.20150412)

Modified: 4/12/2015 3:31:27 PM

Participants

CIO or CIO Delegate
Workshop 2 *Steve Fleagle*

Senior Identity Architect
Workshop 2 *Chris Pruess*

Ubiquitous SSO: Reduce Login Requirement

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Suzy Student would benefit from a ubiquitous single-sign-on environment. Today, she must login multiple times with the same ID and password, sometimes with a domain qualifier, sometimes not.

The University's enterprise authentication engine is based on a campus-wide, shared Active Directory forest. The netID is named "HawkID." Multiple authentication solutions for web apps are supported in this environment. Campus administrators may also implement solutions utilizing Active Directory functionality, as they wish.

Shibboleth

Active Directory Federation Services (ADFS)

HawkID Login Tools (homegrown, CAS-based)

LDAP (F5 abstraction of the domain controllers presented as "dc" service)

The major student systems all go against the same password store, and there is some SSO within selected sets of services.

A day in Suzy's life might include logins such as:

Purpose	**Service Name**	**AuthN**
Access Wireless in residence hall	Eduroam	Radius (RADIATOR)
Check email or retrieve files	Office 365	ADFS

Login at computer lab	Instructional Technology Center	Windows authentication
Turn in homework in learning management system	ICON	HawkID Login Tools
Watch Online learning vignette	Lynda	Shibboleth
Check U-bill in Student portal	ISIS	HawkID Login Tools
Work on student collaboration project outside of defined class	Sharestream (video platform)	LDAP auth (dc service)
Find Student organization information	Orgsync	Shibboleth

A similar story can be told around the faculty and staff experience with services using enterprise authentication.

We would like to find a solution that integrates the various protocols for continuous SSO integration. We need to maintain single-logout functionality.

University of Iowa (093.uiowa.2.20150412)

Modified: 4/12/2015 3:31:40 PM

Participants

CIO or CIO Delegate
Workshop 2 *Steve Fleagle*

Senior Identity Architect
Workshop 2 *Chris Pruess*

Checking for Duplicates

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

As the university and testing organizations have moved away from SSN as a primary key and even a stored attribute, and as recruiting efforts have ramped up, the number of duplicate entries created from test score files and prospecting lists has grown. The first challenge is to prevent duplicate identities from being created. We have developed a significant dupe-check process within our SIS processing but a more sophisticated duplicate matching method using heuristics and fuzzy searching is needed.

The number of dupes generated out of test score files and prospecting lists is huge and growing especially as we extend the prospecting effort to high school freshman and sophomores and junior high students.

Iowa assigns a University ID (UnivID) to its faculty, staff, students, and others with a recurring institutional business relationship. For a student, this assignment happens when he/she applies for admission. The UnivID assignment process provides the second check for duplicate identities.

The number of dupes generated out of the UnivID process is relatively small. The UnivID system is the gateway into our IAM processes for campus services. Duplicates that surface after services are deployed multiple times for the same person can cause confusion and service disruptions for the individual.

University of Iowa (094.uiowa.3.20150412)

Modified: 4/12/2015 3:31:58 PM

Participants

CIO or CIO Delegate

Workshop 2 *Steve Fleagle*

Senior Identity Architect

Workshop 2 *Chris Pruess*

Password Resets and DIY Tools

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Herky Hawk, UI student, reads his email in an off-campus mail system so when he wasn't enrolled for the summer session, he wasn't regularly logging in. When he returned to campus in the fall and needed to retrieve his class schedule late one night, he had forgotten his HawkID password. Herky, and many like him, had never set up password hints. Herky was unable to login until he could visit the Help Desk to have his password reset.

We ask our faculty, staff, and students to access various tools for setting up service information. It's easy for something to be missed. Password reset requests are always in the top-5 most frequent Help Desk requests for help.

We are envisioning a do-it-yourself tool that would support a security profile workflow. We want to leverage the identity vetting that occurs when the University ID card is issued. Individuals must make payment elections at the first issuance. Our vision includes collection of the following person registry information at that first encounter.

ID card charging and payment elections

Emergency contact information for campus emergency alerts

Emergency contact information: who to contact if you have an emergency

Permission to text to mobile phone for use in password resets, emergency alerts, class waiting lists, etc.

White pages directory restrictions, preferences

Password hints for self-service resets

DUO 2-factor signup (faculty/staff)

Preferred name

An IAM DIY tool framework that campuses could adapt to local use could be helpful.

University of Iowa (095.uiowa.4.20150412)

Modified: 4/12/2015 3:32:10 PM

Participants

CIO or CIO Delegate

Workshop 2 *Steve Fleagle*

Senior Identity Architect

Workshop 2 *Chris Pruess*

Credentials for Special Populations ("Guest" Accounts)

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

We have good Systems of Record for employee and student identities. There are several additional, special populations that need credentials. Multiple solutions are in place across campus, depending on what is available to the particular service. Standardized processes and tools for providing support are needed. Examples of populations include:

Parent accounts – controlled by their student

Guests

Accrediting bodies

Search committees (non-university members)

State employees housed on campus (e.g., auditors, historical society)

Library patrons

Local law enforcement (campus emergency alerts)

External Workflow routing

Applications that are available to external persons

Campus workshops (batch input needed)

Developing a standard framework for managing non-institutional people that included systems of record attributes and tools for approvers to create identities would be useful.

It would be useful to bring in ForgeRock or other vendor in as a Net+ service partner to get an OpenID connector for social networking IDs.

University of Iowa (096.uiowa.5.20150412)

Modified: 4/12/2015 3:32:22 PM

Participants

CIO or CIO Delegate

Workshop 2 *Steve Fleagle*

Senior Identity Architect

Workshop 2 *Chris Pruess*

Event-Driven Provisioning/Deprovisioning

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Learner/Student
Staff
Help Desk

Story Narrative:

Adam Applicant and his parents were confused about why his HawkID (netID) worked in some services, but not all. Adam was able to login to the Admissions portal, but he could not login to the housing application to apply for a place to live.

Applicant HawkIDs (netIDs) are assigned in real-time. Following submission of his/her application for admittance, an email message with a link to generate the HawkID is sent. The HawkID is generated real-time, based on choices the student makes. The Active Directory credential is created immediately and is available for authentication to the student portal. However, there is a gap before for other campus services, such as the portal for housing applications, have the related identity information.

University of Maryland - College Park (097.umd.1.20141205)

Modified: 12/5/2014 9:30:32 AM

Participants

CIO or CIO Delegate

Workshop 1 *Eric Denna*

Senior Identity Architect

Workshop 1 *Tripti Sinha*

Other Institutional Identity Needs

Workshop 1 *John Pfeifer*

Multiple Authoritative Systems of Record

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Sven comes in contact with the university first as an applicant for student admissions. He is admitted and becomes a student. While a student he takes a part-time job at the university helpdesk. Upon graduation, Sven leaves the university for a period of time eventually returning as a faculty member who also has a staff appointment to an interdisciplinary research institute. Over the years he also pursues occasional course work in interpretive dance. Eventually, he retires with emeritus status.

Over his lifetime, Sven’s identity information will reside in various systems of record (admissions, student, payroll, alumni, etc.) with potential inconsistencies between them such as different email addresses in student system as compared to the payroll system. This makes it difficult to resolve these various relationships into a single institutional identity and difficult for Sven to know where to go to update his information. Also, as Sven’s relationship to the university changes, his roles and consequently authorizations need to change fluidly rather than be dependent upon various one-off or manual processes.

University of Maryland - College Park (098.umd.2.20141205)

Modified: 12/5/2014 9:30:48 AM

Participants

CIO or CIO Delegate

Workshop 1 *Eric Denna*

Senior Identity Architect

Workshop 1 *Tripti Sinha*

Other Institutional Identity Needs

Workshop 1 *John Pfeifer*

Multi-institutional High Performance Computing Collaboration

Actors

Individual User
Home Organization
Virtual Organization

Stakeholder Groups

Researcher/Scholar
External collaborator or contractor

Story Narrative:

Svenja, a faculty member whose research requires computationally intense data analysis, wishes to access high performance computing (HPC) assets held by a consortium of local institutions. Shell/ssh command-line access is required for these HCP systems and so federated authentication is not available. Svenja must be registered with the IDM at the collaborating institution and issued and id & password that is specific to each HPC resource. This leads to a proliferation of credentials as well as confusion on the part of Svenja.

University of Maryland Baltimore County (099.umbc.1.20150412)

Modified: 4/12/2015 3:33:38 PM

Participants

CIO or CIO Delegate
Workshop 3 *Jack Suess*

Senior Identity Architect
Workshop 3 *Todd Haddaway*

Managing Identity Services Over A Lifetime

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

I want to break the chains between account credentials, passwords, and services and recognize that almost everyone connected to the university will move between having an institutional role (student, staff, faculty, collaborator) and being an interested party in the university (friend, prospective student, patron, spectator, alumnae, etc.).

Jane applies to campus by sending us her application through the CommonApp. She is interested in applying for scholarships and financial aid so goes to our portal and signs in using the social identity she listed as her personal email address on her application. She is immediately connected to her application and can see the admissions checklist of items to complete and the associated due dates. She comes back often to complete items, always using her social identity to log in.

Jane is accepted but decides to attend a community college for the first two years to save money, she defers her admittance and attends the community college. Since we know that Jane plans to finish her studies at UMBC she can continue to log in through her social identity and get resources tailored for her to successfully transition to UMBC and make her transfer as easy as possible. As Jane gets her AA degree she notifies admission via the deferred admittance that she will be attending next semester. As she logs into our portal with her social account she has a pop-up window congratulating her and asking her to create a username at UMBC so she goes in and quickly sets up a username. This is linked back to her social identity and cell phone number so if she ever forgets her password she can get it easily get it fixed.

The next time Jane logs in with her social account she is reminded that she has a UMBC username and that she needs to use that for some specific campus services, such as course registration. She quickly enters those and now has full access to all services.

Jane is very motivated and goes to the career services group. As part of creating her resume she is instructed on how to create a LinkedIn account. As she does that, her new LinkedIn profile is captured by our career services software and propagated to the IDMS. Jane is really motivated and decides to do a number of special activities we have on financial literacy, leadership, and community service. As she does these activities she finds she is earning achievement badges. These badges show up in her campus advising profile and are automatically propagated to her LinkedIn account as endorsements from the university.

Jane does so well she graduates in two years and lands a great job. As she is graduating she receives an email congratulating her and telling her we want her to remain connected to the university. She goes to her account management page and sets up how she wants to be connected – does she want to keep her UMBC account active, transition over to personal social account, or use her LinkedIn account? Jane never liked email, she thought that was too old-school, and selects LinkedIn. Once she does all her resources are saved; however, she will now log into our portal as an alumni through her linkedIn account. Jane can still earn achievements by completing some of our MOOC courses we offer alumni as part of our commitment to lifelong learning. A few years later, Jane decides she wants to finish her Master's degree. She logs into the portal through her linkedIn account and selects the apply to graduate school link. Jane fills out her materials, is accepted, and as she goes to attend classes she logs in with her LinkedIn account and is reminded that for some academic functions she needs to re-enable her university account. She clicks the button to re-enable her university account, since Jane still has her same cell phone number, she gets a code texted to her phone and she is asked to enter that code to re-enable her account. She does this and sets up her UMBC account.

As Jane completes her Master's courses she finds she is earning endorsements for the new skills she is learning, these are automatically propagated to her linkedIn profile. Once she completes her Masters, Jane is given the option to transition her account as she did when she was an undergraduate and resumes following her alma mata through her LinkedIn account.

University of Maryland Baltimore County (100.umbc.2.20150412)

Modified: 4/12/2015 3:33:17 PM

Participants

CIO or CIO Delegate	
Workshop 3	*Jack Suess*
Senior Identity Architect	
Workshop 3	*Todd Haddaway*

Provisioning Campus Services During the Onboarding Process

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

While some of the faculty / staff / student onboarding process is automated, a number of computing resources are manually provisioned. Sometimes the automation process provides access to resources that aren't needed, sometimes not enough. A new IAM system should provide a good level of granularity and automation in regards to provisioning computing resources.

Scenario: Cal, a new admissions counselor, is hired in the Undergraduate Admissions office. Before he arrives, Cal's new Campus ID is sent to his personal email address and he is given the opportunity to create his computing account. Upon creation Cal is given access to email, calendar and other Google apps. Cal is also able to log into a general login unix shell, which he finds quite exciting, yet useless for his job. Cal's new supervisor Brooks asks Cal to review a list of prospective students on the department's Active Directory shared drive.

Fast forward an hour – Cal has just entered his first helpdesk ticket asking for access to the department's AD drive and asking what he is supposed to be doing with this unix login shell.

Ideally, the onboarding process would have granted Cal email and the rest of the Google apps suite as well as access to the departments AD drive and perhaps the department's Box folders. Since Cal has access to sensitive information, Cal should have been enrolled into Duo, our second-factor solution. Finally, unix shell access would not have been granted.

University of Miami (101.miami.1.20150412)

Modified: 4/12/2015 3:34:09 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tim Ramsay*

Master Data Management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Standardization of Person Data model for central Identity repository or Master data tailored to support identity lifecycle in Academic environments. We consolidate the person bio-demo and academic affiliation specific data between multiple sources of identities or system of records. Having this consolidated master data could allow us to streamline integrations with access management tools and thereby enhancing the chances of achieving higher identity assurance levels and also alleviating duplicate identity problem to certain extent.

University of Miami (102.miami.2.20150412)

Modified: 4/12/2015 3:34:30 PM

Participants

CIO or CIO Delegate

Workshop 3 *Tim Ramsay*

Social-External Identities

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Social/external identities: We have applications that are required to be exposed to non-university affiliated persons. We often end up creating a guest identity and controlling their access through shibboleth. In most of these situations we may not necessarily need to manage their identities. We are interested in a tool which addresses the use cases from the Social/External Identities Working Group.(https://spaces.internet2.edu/display/EXTID/Home)

University of Michigan - Ann Arbor (103.umich.1.20141218)

Modified: 12/18/2014 10:42:50 AM

Participants

CIO or CIO Delegate

Workshop 1 *Laura Patterson*

Senior Identity Architect

Workshop 1 *Holly Nielsen*

Other Institutional Identity Needs

Workshop 1 *Luke Tracy*

A Tale of Two Devices - Visiting faculty accesses a patient's medical device.

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Staff
External collaborator or contractor

Story Narrative:

A security professional at the University of Michigan is asked by the Medical Center's Compliance Officer to review the activity logs for *a medical device* and validate all access was properly authorized according to *compliance policy*. The Compliance Officer has provided the MAC address of the medical device.

The security professional begins reviewing access logs in the log aggregation system and discovers traffic between this medical device and multiple networked entities and records all of the IP and MAC Addresses involved. Additional log mining for all of these IP and MAC Addresses reveals the identities that each of these devices/entities is known by and she correlates this with login information for some of these entities and identifies on-duty medical staff monitoring the *medical device* from hospital floor workstations through applications that are using the University's Roles System for authorization.

However, two devices that have accessed the medical device are unaccounted for in this correlation. The security professional determines these two devices are mobile devices, a tablet and a smartphone, based on MAC address. She needs to work with the IAM team to discover which people have an established relationship with these two mobile devices. The IAM team reveals that the tablet is a hospital-managed tablet assigned to a visiting member of the medical Faculty, Dr. Chen, and the smartphone is a personally owned device owned by Dr. Chen.

The security professional reviews the patient information for the *medical device* and discovers that Dr. Chen is not one of the patient's physicians.

The security professional again works with the IAM team to access the OAuth2 authorization server records and determines the following authorization flow that took place to provide Dr. Chen access to the *medical device*.

Dr. Chen is listed in the University's Roles database as having access to active patient records.

Dr. Chen uses her mobile app for monitoring this type of *medical device* and looks up the patient whose device she is interested in and chooses to request access to the *medical device*.

Dr. Chen's mobile app queries active patient records on Dr. Chen's behalf to determine the attending physician for the patient. The mobile app then initiates an OAuth2 request to ask for permission from the attending physician to access the patient's medical device for monitoring purposes.

The OAuth2 authorization server is integrated with the University's Roles System and verifies the attending physician is authorized to grant access to a patient's device.

The attending physician receives the request and approves the access for a period of one week.

Dr. Chen's mobile app receives notification that the access has been granted, and connects to the *medical device*.

She has done this on her issued tablet initially. When she attempts to also do this from her personal smartphone, the previous authorization is not adequate from that device and an additional authorization request is sent to the attending physician to authorize this access from an unmanaged device.

The attending physician receives the request and approves the access for a period of one day.

Having now accounted for all access to the *medical device* and determining that all access was authorized through established processes, the security professional reports back to the Medical Center's Compliance Officer that all access was properly authorized.

University of Michigan - Ann Arbor (104.umich.2.20141218)

Modified: 12/18/2014 10:42:23 AM

Participants

CIO or CIO Delegate

Workshop 1	*Laura Patterson*

Senior Identity Architect

Workshop 1	*Holly Nielsen*

Other Institutional Identity Needs

Workshop 1	*Luke Tracy*

Rock Solid On-boarding

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Staff
External collaborator or contractor

Story Narrative:

Two professors of Geology at the University of Michigan have been studying the tectonic structural differences that support the tallest mountains in the world. Their work frequently takes them to China and Tibet and requires that they collaborate with geologists, guides, suppliers, and government officials from those regions.

These two professors need to share information and instrumentation access with these colleagues. Some of them are able to access the University's collaboration services and have either federated, or direct accounts within the collaboration system that can be granted access to the research data. Others do not and will require the University create an account for them. In some cases, the collaboration system the University uses is simply not available to the collaborators due to government Internet filtering.

The instrumentation these collaborators require access to is secured with University accounts, federated accounts from InCommon and other Research and Scholarly federations, and other standards based federated identity systems such as OpenID.

The professors contact the IAM team to initiate the creation of University accounts for some of their collaborators.

The IAM team works with a vendor that performs identity vetting and proofing globally, including in-person vetting through a network of agencies worldwide. The vendor supplies accurate identity data for the collaborators and the University generates an invitation to the collaborators to establish a digital credential with the University.

The collaborators follow the link from the invitation to a University web application, validate their identity information against data gathered by the identity vetting and proofing vendor, and are granted the ability to choose a login name and establish a password.

Once the account is established, the professors are notified and they can begin to establish the appropriate access to the research data and instrumentation by accessing the service request system online and ‘shopping’ for the access the collaborators require, including the alternate collaboration platform that is required due to government Internet filtering.

Access workflows are immediately initiated and soon approved, automated account provisioning and access permission occurs, and the professors and collaborators are informed that they are ready to work together.

University of Michigan - Ann Arbor (105.umich.3.20141218)

Modified: 12/18/2014 10:42:02 AM

Participants

CIO or CIO Delegate

Workshop 1 *Laura Patterson*

Senior Identity Architect

Workshop 1 *Holly Nielsen*

Other Institutional Identity Needs

Workshop 1 *Luke Tracy*

The API Transit Authority

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

The IT Service Providers throughout our University's three campuses and Medical Center would like a common web services platform to integrate with, and publish services and APIs to, when developing new applications and services. They would like this common platform to be well integrated with IAM and security services and meet the availability and fault tolerance needs of our most demanding use cases.

When developing new applications and services, developers would like to interact with IAM and security services in the same way they would interact with any other service on the common platform. This common platform would meet the identity and access needs of the underlying services, including auditing, monitoring, and compliance, without overly complicating the platform. In fact, the IAM and security services would be partners with the platform and enable seamless integrations involving multiple service providers and resource providers.

Using this web services platform, staff, faculty, and students would develop modern and innovative applications that scale and are appropriately well secured. The cost to support these applications would be decreased due the economies of scale that would be achieved through reuse of existing APIs and services, as well as faster time to delivery for developers when using familiar integration patterns and designs.

University of Minnesota - Twin Cities (106.umn.1.20141126)

Modified: 11/26/2014 12:57:17 PM

Participants

CIO or CIO Delegate

Workshop 1 *Scott Studham*

Story 1: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

University of Minnesota - Twin Cities (107.umn.2.20141126)

Modified: 11/26/2014 12:57:18 PM

Participants

CIO or CIO Delegate

Workshop 1 *Scott Studham*

Story 2: ***[Story Not Available Yet]***

Actors

Individual User
Home Organization
Virtual Organization
Service Provider
Other (Please Specify)

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
Other (Please Specify)

Story Narrative:

University of Missouri (108.missouri.1.20150412)

Modified: 4/12/2015 3:35:51 PM

Participants

CIO or CIO Delegate
Workshop 2 *Beth Chancellor*

Senior Identity Architect
Workshop 2 *Joanne Boomer*

Application Integration Issues with an integrated University System identity environment

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff

Story Narrative:

The University of Missouri identity system supports 4 campuses, a hospital and system offices (6 business units). A centralized identity store ensures each individual has one unique electronic identifier across the entire system. The primary authentication source is Active Directory (AD) and the individuals' account lives in one of 9 domains within a single AD forest.

While the centralized identity store is a strong advantage for UM, ensuring users don't have to keep track of multiple identities and passwords, we continue to have occasional issues with applications and resources integrating with our environment both internally and externally.

Because integration with Active Directory/LDAP is 'easier' and, if done properly can leverage the entire forest, there has not been a strong desire to utilize Shibboleth/SAML for internal application integration, as it is viewed as 'harder to implement'. We also have issues with applications (especially in healthcare) that can only be aware of one domain, which results in request for duplicate accounts for an individual or requests to move an individual to a domain within which they do not belong (i.e. students).

For externally hosted applications, integration with Shibboleth/SAML is not always easy. Vendors who claim they can handle Shib/SAML are frequently not proficient in the solution and require a lot of hand holding. Those that refuse to integrate with Shib/SAML require either a separate solution which must be developed and/or a request for an exception which includes separately managed accounts and passwords (prohibited via policy). Many applications are given an exception because of the 'required business need.'

University of Missouri (109.missouri.2.20150412)

Modified: 4/12/2015 3:36:12 PM

Participants

CIO or CIO Delegate

Workshop 2 *Beth Chancellor*

Senior Identity Architect

Workshop 2 *Joanne Boomer*

Integrated and Federated login to shared Unix Research Cluster (non-web resources)

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
External collaborator or contractor

Story Narrative:

The Research Computing team runs a High Performance Computing cluster (but is applicable for most researchers that use a Linux centralized resource) on the RNet network which allows researchers to utilize its resources. Currently local credentials are individually provisioned on the system for the campus and external individuals and SSH Keys are frequently used. These credentials are not in sync with the University identity systems. The Research group must maintain and administer these accounts. They would like to utilize a federation solution that would allow both MU credentials and other institution credentials would allow researchers easy access to resources across the world and enhance collaboration.

University of Missouri (110.missouri.3.20150412)

Modified: 4/12/2015 3:36:31 PM

Participants

CIO or CIO Delegate

Workshop 2 *Beth Chancellor*

Senior Identity Architect

Workshop 2 *Joanne Boomer*

Centralized Provisioning/Deprovisioning System

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff

Story Narrative:

The University of Missouri currently runs a legacy provisioning system that needs replaced. The home-grown system was not well documented and none of the original developers work for the University, so it is difficult to continue to support. The University had a failed attempt at replacing this system with a vended product that turned out not to meet the institutional needs. A second vended system was considered but the license and implementation cost were too expensive.

A new system must be developed and we would like it not only to be supportable without being reliant on one or two individuals but for it to be extensible as well. In addition to handling the provisioning and deprovisioning for the current centralized systems, it needs to ensure additional services can be added without major effort. This includes a growing list of vended/hosted solutions that require custom development to integrate with an API or some other manual provisioning method to ensure it is supportable for a large number of University users.

University of Missouri (111.missouri.4.20150412)

Modified: 4/12/2015 3:36:51 PM

Participants

CIO or CIO Delegate

Workshop 2 *Beth Chancellor*

Senior Identity Architect

Workshop 2 *Joanne Boomer*

Password Tools

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff
External Visitor/Guest account

Story Narrative:

While the University of Missouri as a single identity for each user within the System, many different password tools have been developed and are in use across the System. We would like to have a single, integrated toolset for every type of user. The toolset should include identity registration (i.e. claiming an account/identity proofing), self-service reset, password change and administrative reset options. Long-term, ideally the solution could also integrate multi-factor authentication in the self-service or MFA management options.

University of Missouri (112.missouri.5.20150412)

Modified: 4/12/2015 3:37:14 PM

Participants

CIO or CIO Delegate

Workshop 2 *Beth Chancellor*

Senior Identity Architect

Workshop 2 *Joanne Boomer*

Retaining accounts 'for life'

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff

Story Narrative:

UM currently retains the Active Directory account for all former employees and students of the University. The primary purpose of retaining the accounts is for continued use within the appropriate ERP system. The primary uses for HR include access to paystubs, electronic W-2's, and retirement calculations. Primary uses for Student include access grades, transcripts, and paying bills.

The retention of these accounts introduces problems related to deprovisioning. Many resource owners tend to rely on a 'deletion' process to clean-up authorization to their services. Central IT cannot identify all the resources an individual has access to in order to ensure authorization is properly removed. While currently the AD account is locked for a short-time after separation, the account will be unlocked to allow access to ERP systems and there is no way to ensure an individual does not still have access to systems he/she should not. HR is pushing to reduce this timeframe so an employee can still access the necessary documents. In addition, these account introduce long-term password support issues. Should the passwords remain static and available for years even with non-use? Users who forget their password also continue to need help.

University of Nebraska - Lincoln (113.unl.1.20150412)

Modified: 4/12/2015 3:37:57 PM

Participants

CIO or CIO Delegate

Workshop 1	*Mark Askren*

Senior Identity Architect

Workshop 1	*Brett Bieber*

Vendor Support & The Black Box Identity Registry

Actors

Home Organization

Stakeholder Groups

Home Organization
IDP Operators
Central IT Group

Story Narrative:

The University of Nebraska-Lincoln engaged an external support vendor to implement a name-brand identity registry (Sun Waveset) in 2011. The Waveset application was declared end-of-life by Oracle, and the external support vendor evaporated into thin air, leaving us with an under-supported product and little-to-no on-campus expertise for configuring it.

The Identity Registry has become a black box, containing all of our business logic, without any portability to another solution. Ideally, the identity registry should allow configuration that is visible to inspection, can be tracked via version control, and is portable when replacement needs arise.

University of Nebraska - Lincoln (114.unl.2.20141205)

Modified: 12/5/2014 9:28:32 AM

Participants

CIO or CIO Delegate

Workshop 1 *Mark Askren*

Senior Identity Architect

Workshop 1 *Brett Bieber*

Barriers to Implementation & Adoption of SP Technology

Actors

Service Provider

Stakeholder Groups

Staff

Story Narrative:

Vendor-supplied applications, as well as in-house applications haven't moved quickly enough to support federated authentication methods. We've encountered vendors and colleagues that are unsure of the technology, developers that find the concepts difficult to understand, and poorly written & organized documentation on how to implement a Service Provider.

The documentation needs to be re-organized to be more effective and clear, with the creation of a repository of solutions for bolting-on federation for common products.

Specific products we're interested in, or have attempted bolting-on federated authentication:

Blackboard (implemented)

GitLab (attempted)

GoSignMeUp (implemented)

PeopleSoft (not attempted)

SAP (not attempted)

Drupal (attempted)

University of Nebraska - Lincoln (115.unl.3.20141205)

Modified: 12/5/2014 9:28:42 AM

Participants

CIO or CIO Delegate

Workshop 1 *Mark Askren*

Senior Identity Architect

Workshop 1 *Brett Bieber*

High Performance Computing & Code Collaboration

Actors

Virtual Organization

Stakeholder Groups

Researcher/Scholar

Story Narrative:

Researchers create virtual organizations to utilize shared computing services and collaborate on research projects. Unfortunately many of the individuals do not come from institutions with InCommon representation. We also need to simplify command-line access, and facilitate collaborative development environments.

Once the virtual organization has been set up, they would like to collaborate on the code they develop. Integration with a source control repository, e.g. GitLab, would allow all these users to quickly collaborate on both the code they develop and the computing resources they need access to.

University of Nebraska - Lincoln (116.unl.4.20141205)

Modified: 12/5/2014 9:28:57 AM

Participants

CIO or CIO Delegate

Workshop 1	*Mark Askren*

Senior Identity Architect

Workshop 1	*Brett Bieber*

Preservation of an Endangered Language

Actors

Virtual Organization

Stakeholder Groups

Researcher/Scholar
Learner/Student
External collaborator
Faculty/Teacher
Students at K-12 Public School

Story Narrative:

The language of the Native American Tribes of the Omaha and Ponca people of Nebraska and Oklahoma is studied by a limited set of researchers at various institutions, and is still spoken by some older members of the Omaha Nation. Preservation of this endangered language could be aided by setting up a virtual organization, to facilitate study of its historical documents and collaboration in translation, recording and teaching efforts.

Researchers working with the language are scattered across various institutions, and speakers from the Omaha Nation are often scattered as well. Some researchers are at institutions with InCommon IdP Infrastructure, while others are not. What technical infrastructure is available to the individuals from the Omaha Nation is limited to that provided at the public school on the reservation.

Select schools in Nebraska participate in a pilot project to access a longitudinal data dashboard sponsored by the Nebraska Department of Education. The participants in this pilot are larger schools that can accommodate the extra burden of running an IdP, and have existing IdM infrastructure for authentication.

Schools that do not have such infrastructure are left out, until specific needs arise, or until they are required to participate via mandate by the Department of Education.

An IdP sponsored through the Omaha Nation Public School could act as a catalyst to expand the available services to one of the poverty stricken schools within the state. If the technology was simple enough to allow operators to establish an Identity Registry and Identity Provider, this will simplify the collaboration needed for this project, and many others.

The ability to create a virtual organization and a common workspace shared by researchers and community participants would empower teachers, linguists and native speakers to more easily collaborate to preserve the Omaha language and provide students at the Omaha Nation Public School access to the stories that describe their heritage.

University of North Carolina - Chapel Hill (117.unc.1.20150412)

Modified: 4/12/2015 3:39:25 PM

Participants

CIO or CIO Delegate

Workshop 2 *Ethan Kromhout*

Senior Identity Architect

Workshop 2 *Celeste Copeland*

Provisioning/Deprovisioning

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Staff
External collaborator or contractor

Story Narrative:

Amy starts a new job at UNC-Chapel Hill. She has been asked to choose her Onyen (Net ID) prior to arriving so that her workstation will be prepared for her in advance. On her first day, Amy's supervisor Sharon has already arranged for her email and to have access to AFS space including the group's shared AFS directories, three of her group's databases, and administrative access to their group's web site. Sharon was able to do this easily by clicking on a few available options in a central location, so that these things would be available for Amy to begin work immediately.

Two years later, Amy transfers to a different group within UNC-Chapel Hill. Her new supervisor, Mark, would like for some access to be retained. As part of the transfer process, Sharon elects to remove access to her group's databases, web site, and AFS directories, but does not choose to remove her overall AFS access. Mark in turn elects for Amy to have access to his group's AFS space, as well as administrative rights with their Sakai implementation. This transition happens seamlessly, with no loss of general AFS access or Amy's AFS home directory, email account, etc.

Five years later, Amy is terminated from UNC-Chapel Hill as she moves on to a different institution. Mark is able to deprovision all access from the central location that he has visited before. The deprovisioning of these services is achieved in an automated fashion. Amy's Onyen is automatically deprovisioned a few days later according to university Onyen policy.

University of North Carolina - Chapel Hill (118.unc.2.20150412)

Modified: 4/12/2015 3:39:38 PM

Participants

CIO or CIO Delegate
Workshop 2 *Ethan Kromhout*

Senior Identity Architect
Workshop 2 *Celeste Copeland*

Two-Factor Authentication

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Mary has a user's level of access to the campus PeopleSoft implementation. Bob has an HR Administrator's level of access to this program, which allows him to do certain privileged data changes. Beth has a System Administrator's level of access to this program, which allows her to change most everything within the application.

Mary authenticates using Web SSO to the PeopleSoft application, which verifies who she is and allows her to change certain elements of her own data. Bob authenticates using Web SSO, but is also prompted for a second factor. He has elected to be sent a PIN through his cell phone to provide the second factor. He authenticates and then is allowed to change certain data for people who are members of his department. Beth authenticates using Web SSO, but is also prompted for a second factor. Beth has elected to be called on her desk phone to be given the second factor. She authenticates and then is allowed to change data for any person, and other administrative functions to which other users do not have access.

University of North Carolina - Chapel Hill (119.unc.3.20150412)

Modified: 4/12/2015 3:39:51 PM

Participants

CIO or CIO Delegate

Workshop 2 *Ethan Kromhout*

Senior Identity Architect

Workshop 2 *Celeste Copeland*

Guest Authentication/Authorization

Actors

Individual User
Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Non-affiliated person

Story Narrative:

Brad is a professor in the Romance Studies department. His new student Janet is an intermediate French student and needs to have experience conversing with a francophone in order to progress with her studies. Brad knows Babette, who is a native French speaker, and who would be glad to donate some spare time to instant messaging with Janet in order to improve her conversation skills. Babette is not affiliated with the university.

Brad provides information for Babette to go to a guest registration site, where she is able to create a guest account. Once she's done that, she provides Brad with a unique identifier that he can then use to grant permission for her and Janet to chat using their departmental IM utility. Once the class is over, Brad is able to remove this access for both Babette and Janet.

University of Notre Dame (120.nd.1.20150412)

Modified: 4/12/2015 3:40:12 PM

Participants

CIO or CIO Delegate

Workshop 2 *Ron Kraemer*

Senior Identity Architect

Workshop 2 *Michele Decker*

Other Institutional Identity Needs

Workshop 2 *David Seidl*

Group Management at Notre Dame

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor
3rd party software vendors
compliance organizations

Story Narrative:

The University of Notre Dame has a broad range of systems that currently rely on a combination of Banner security groups and an internally built group management capability based on LDAP groups which requires a relatively high level of knowledge of our identity management environment. In addition, group membership management is delegated, but creation is not. As we add additional enterprise and departmental software, the need for a group management solution that is both user friendly and capable of being integrated easily with a variety of third party solutions has become evident.

Our current major projects include integration with bulk email capabilities to replace an existing large-scale Listserv implementation. We currently populate and manage 44,000 academic listservs during a typical semester. The process to do this relies on a tangled set of scripts and legacy code built years ago by Banner developers and Listserv adins. In order to move away from Listserv to a Google Groups based environment we need a group management system that can feed Google Groups and allow nimble updates of our group memberships to handle class adds, drops, and other changes.

Our campus is in the process of adopting a compliance and training solution which needs our organization to be mapped to groups in a variety of ways depending on the training or compliance objectives that individuals, departments, and work groups must meet. This can be quite complex, as a given individual might be a former or current student, a faculty member, a staff member, a member of multiple research labs, a trained operator of specific equipment, and they might also have a role as a faculty advisor for a club or organization. These mappings don’t exist in a single system, and group management is needed to track each membership while allowing additional arbitrary roles and groups to be managed over time, while still tracking that person’s training or compliance status throughout their career, and despite position and affiliation changes inside the University. This system expects LDAP data as well as flat files, meaning that a capable system must be able to output organizational information in multiple formats that we can provide as a vendor spec.

A second concurrent major initiative is “All Resource Planning” or “ARP”. This is an API-centric resource planning tool that combines financial data with a range of institutional data from both our ERP and other central systems. Much like our training and inspection system, ARP needs to have updated and historic tracking of group membership across complex organizational structures that may contain the same individual in multiple groups that shift in complex ways over a career spanning decades. Unlike our training and inspection system, ARP is designed from the ground up to consume data via APIs, meaning that a well-documented API with example code would be ideal

Our ideal solution will be a common solution with strong support including documentation and sample code demonstrating how to access or consume data, a VERY user-friendly interface with an approachable learning curve for non-technologically adept customers, as well as a strong, API-centric design that allows us to provide well written, understandable, and approachable documentation and interfaces to third parties.

It must be capable of being deployed in both a traditional datacenter environment and a Infrastructure-as-a-Service or a Platform-as-a-Service mode. Importantly, tools should be developed to use standard protocols, LDAP, SAML, message queueing, with common syntax so you don't need specialized knowledge (of a product) for integration.

University of Oklahoma (121.ou.1.20150403)

Modified: 4/3/2015 8:23:47 PM

Participants

CIO or CIO Delegate

Workshop 3	*Anna Biggers*

Senior Identity Architect

Workshop 3	*Dave Shields*

Other Institutional Identity Needs

Workshop 3	*Jeff Wall*

Who's Really Who? IDM Confusion

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Staff

Story Narrative:

A new faculty or staff member is hired by the University of Oklahoma at any of our three campuses (OU Norman, OU Health and Sciences Center, or OU Tulsa). Parts of the user's identity come from many different streams of data including our HR system (PeopleSoft), our ePAF program, or by manual entry into our Oracle DB Vault. If any piece of the user's information is not a 100% match (maybe the information was hand keyed directly into the system but spelled incorrectly), our system may create multiple users and there is currently no simple way to reconcile this information. If the error is not caught early on, the user may have incomplete access or incorrect access that isn't detected until someone on the backend happens to catch it. Once it is caught, the process of unifying the account can be particularly challenging. The current state of IdM at OU is such that there is very little way of knowing who really is who and what they have access to, a functional IdM solution would have to address those needs.

University of Oklahoma (122.ou.2.20150406)

Modified: 4/6/2015 12:58:23 PM

Participants

CIO or CIO Delegate
Workshop 3 *Anna Biggers*

Senior Identity Architect
Workshop 3 *Dave Shields*

Other Institutional Identity Needs
Workshop 3 *Jeff Wall*

Library Software Needs Universal Login Source

Actors

Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Our Library Information System team, through a partnership with our VPR office, is embarking on a digital initiative that includes long-term archive, data curation, and indexing. The data repositories could reside across multiple locations throughout the globe, but a common user interface provides seamless interaction with the entire collection.

The challenge to the assignment is that users of the system are diverse, and reside within multiple disciplines, organizations and departments. As such, each of the customers of the system are expected to have allocated access rights based upon several factors; including organization, location, name, and role as producer or consumer of the archived data.

The Library Information System team has an expectation of pointing their system to a single, authoritative source for authentication and role determination. This leaves the IT organization in a position to provide a system service that both federates login traffic with several sources, and also leverages the federated data to determine the access rules for the user. Such authentication and role-based access controls require that the IT department generate both the relationships and the connections required to federate with peer higher-ed institutions, research collaborators, scholars in relevant fields, and guests. This allows users of the system to leverage preexisting credentials to access the system.

University of Oklahoma (123.ou.3.20150406)

Modified: 4/6/2015 12:58:12 PM

Participants

CIO or CIO Delegate

Workshop 3	*Anna Biggers*

Senior Identity Architect

Workshop 3	*Dave Shields*

Other Institutional Identity Needs

Workshop 3	*Jeff Wall*

Career Continuity – Where Are My Papers?

Actors

Individual User

Stakeholder Groups

Learner/Student
Faculty/Teacher
Staff

Story Narrative:

A student enrolls in a graduate or doctoral program at the University of Oklahoma. During the course of this program, the user contributes to (and receives authorship credit for) several papers, a few of which are published. The student successfully graduates, and obtains a research position at Baylor, contributing to a number of research papers. During this period, the student marries, and experiences a change in surname. Some years later, the student decides to return to the University of Oklahoma as a faculty member, and continues to publish.

Across this scenario, the user has possessed more than one role, more than one institution, and more than one name. Further, unless the user remembers his or her network ID when returning to OU, the user might end up with more than one account. The likelihood of easily being able to find everything published by this user is small, at best. A few recent initiatives, such as ORCID, are attempting to bridge this gap by maintaining a registry for researchers; however, the resulting ID would need to be connected to the user, across institutions and roles, in order to be effective.

University of Oregon (124.uoregon.1.20150406)

Modified: 4/6/2015 1:04:24 PM

Participants

CIO or CIO Delegate

Workshop 3 *Melissa Woo*

Senior Identity Architect

Workshop 3 *Kevin Foote*

Unified Group Management - at scale

Actors
Individual User
Home Organization
Virtual Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

Problem Description:

At various time in the past multiple groups on campus within Information Services and other

patron groups have requested a way to organize users into groups. The various use cases for groups have been across the board in terms of downstream systems some digital others list or report based.

Internal IS group, network services has wanted to use some sort of group access to provide detailed network utilization information to various patron groups that utilize our network for some time now. These groups would be ad-hoc in nature with the ability to manage a groups contents at any point.

The added ability to use external identities within a group context is also desired. This would provide the ability to mimmic VO use locally and create access structures that patrons desire. As an additional gain, unified group management would allow us the ability to streamline many of the “bolt on” processes and back channel mechanisms we have in place to handle this today.

University of Oregon (125.uoregon.2.20150412)

Modified: 4/12/2015 3:41:12 PM

Participants

CIO or CIO Delegate

Workshop 3 *Melissa Woo*

Senior Identity Architect

Workshop 3 *Kevin Foote*

Painted into a corner with provisioning

Actors
Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Staff

Story Narrative:

Problem Description:

During the early stages of the original IDM system at the UO it was decided to base the provisioning logic around very granular affiliation data. This data is in constant flux as Faculty and Staff tend to move between and within the differing org units that the UO encompasses.

Susie a new hire in the zebra fish research group on campus has a start date of June 2014 she is anxious to get working on here data analysis and assigned first quarter research goals. Since the biology department has also hired Susie on to a non tenure faculty role she will eventually hold two affiliations within the IDM system.

The biology department is anxious to get their Summer 2 schedule lined out and quickly assigns Susie as instructor on two courses which begin Aug 4. The biology academic staff and local HR representative, who have been around The UO for quite some time, know that Susie has to be initially assigned a non-tenure roll within the EIS to obtain the affiliation record that is needed to assign her as instructor of record on these courses. The biology HR rep. begins the paperwork and additionally works with HR to fill in the remaining job description and appointment record. Meanwhile, the HR representative for the research arm of biology has decided that when Susie arrives they will start working on getting her the access and account information she will need (no communication).

The “paperwork” process involved with each phase of hiring Susie is moving through the EIS and IDM system(s) at a differing speed. Susie arrives on day one of her research job and does not have the means to obtain her account through the claiming process limiting the effectiveness of her start date. The net result of this paperwork & EIS IDM breakdown is lost access during critical day one activities.

Other related scenarios are during the de-provisioning actions taken on accounts. Making use of the fine graned affiliation status to drive end services can leave people in limbo cases where access to resources is mistakenly removed.

University of Pittsburgh (126.pitt.1.20150403)

Modified: 4/3/2015 9:56:37 PM

Participants

CIO or CIO Delegate
Workshop 3 *Jay Graham*

Senior Identity Architect
Workshop 3 *Chris Keslar*

Implementing Single Sign On for TIAA/CREF and UPMC Health Benefits

Actors

Individual User (Faculty)
Home Organization
Service Provider

Stakeholder Groups

Faculty/Teacher
Staff
External collaborator or contractor

Story Narrative:

The story started last summer (2014) when Human Resources approach CSSD (The Central IT organization) with a request to implement SSO through our Portal. (My.pitt.edu) Up to this point we successfully implemented many single sign on pass through authentication via the portal. They include, the Student System, Blackboard, Student ID Card Management, and other. They were all well received by the students and the portal gained in popularity and now receives more than 27 million logins per year. Over the past 5 years we implemented SSO for our financial system (Oracle's E-business suite) to allow employees to submit their time sheets online, online pay statements, change deductions for tax purposes, and complete the annual open enrollment process. Another service added about 2 years ago was the UPMC Health Benefits system that allows users to manage their flexible spending account and health benefits. Both of these went out with the usual marketing and information dissemination that typically happens with such services. That is, it goes to the various committees and working groups for approval and is finally announced and advertised through all applicable means. CSSD fully expected "blowback" from faculty and staff when these were implemented, but we received very little feedback and staff seemed to like the idea of not having to remember different passwords for each of the services.

Fast forwarding to the beginning of this semester, we worked with HR to implement the TIAA/CREF single sign on and released it earlier this year. Well, the "blowback" we suspected would happen when the time sheets, online pay statements and the health benefits happened with TIAA/CREF. An email from a concerned faculty member in Psychology was sent to the University Senate President and and it ballooned from there. We are still in the middle of this at the time of the writing and will share updates at the tier conference.

What this illustrates is not technical gaps, but a political gap that nobody on campus foresaw. The faculty are complaining that we shouldn't make these types of services available via single sign on because they share their username and password with their administrative staff and graduate students and CSSD has been preaching for years that this account grants access to restricted resources and passwords should not be shared. The faculty are also lobbying for "opt out" on these services and that is something the vendor has to apply and not all of them have this capability built in. So there are some major questions that need answered.

Should these types of services be available via SSO?

Should some type of re-authentication or MFA be implemented for these types of services?

What are the security risks of using SSO vs using separate accounts for each service?

Who in the University should decide this?

University of Southern California (127.usc.1.20150412)

Modified: 4/12/2015 3:42:03 PM

Participants

CIO or CIO Delegate

Workshop 1 *Pete Siegel*

Senior Identity Architect

Workshop 1 *Asbed Bedrossian*

USC's iVIP – System of Record for Affiliates.

Actors

Individual User
Service Provider
Data Stewards
Systems of Record
Affiliates
Guests

Stakeholder Groups

Researcher/Scholar
Learner/Student
External collaborator or contractor
Emeriti
Retirees
Medical Interns & Residents

Story Narrative:

When USC's homegrown IAM platform was deployed, it took care of faculty, staff and students because they were mastered by the payroll and student information systems. We identified the need to master "guests and affiliates," in a new system of record (SOR). Soon we discovered that there were large populations affiliated with USC who fell through the cracks between Payroll and SIS: emeriti, retirees, ROTC instructors, and medical interns, etc.

We developed iVIP, ca 2007. In the initial years it took many hits because it simply didn't do enough to fill the great need, but we developed robust processes around it. For example, schools and departments have their local iVIP admin who creates new affiliates, and sponsors services for them. Most departments assign their home department HR coordinator to also be their iVIP admin.

iVIP admins meet regularly to discuss operational issues, learn, and communicate new features and developments.

Biweekly meetings are held by the “iVIP working group”, to manage new requirements. There are also biweekly “tech team” meetings.

iVIP now masters over 4,500 affiliate records. They can be sponsored to tens of services, with a specific “affiliation” (e.g.: “visiting scholar”, or “retiree”). Sponsored services are managed with explicit start and end dates.

Areas of improvement: When affiliates become faculty, staff or student, or vice versa, there are frequent “duplicate record” issues generated in our Person Registry. Also, brand new incoming records take overnight to generate NetID’s to be used for online services. Some schools hire 1-day temps, - e.g. temp nurses, - and iVIP is not real-time enough to help.

Suggestion: many institutions have a need for an affiliate SOR. There could also be an InCommon-wide Affiliate SOR. USC’s experience can be written up as a detailed use case, with lessons learned and best practice recommendations.

University of Southern California (128.usc.2.20150412)

Modified: 4/12/2015 3:42:24 PM

Participants

CIO or CIO Delegate

Workshop 1 *Pete Siegel*

Senior Identity Architect

Workshop 1 *Asbed Bedrossian*

Operational issue: duplicate PR records

Actors

Home Organization
Data Stewards

Stakeholder Groups

Staff
IAM group
Data Stewards
Service Providers
Individual Users

Story Narrative:

The greatest operational challenge the IAM team faces, is in dealing with the creation of duplicate PR records for people, most often in their transition between iVIP, and Payroll/SIS. E.g. a temp who is later hired as an employee; or an employee who leaves, but is hired as a consultant. To a slightly lesser degree we have issues with hard affiliation shifts between payroll and SIS as well. E.g. an employee who leaves to become a student; or a student who graduates and is hired as an employee.

In the above cases, if the target SOR is not provided with the USC university ID (10-digit "USCID"), then a duplicate PR record is created, causing considerable challenges.

From the early days of developing our IAM platform, the various SOR populations did not have the same "golden record" rule matching criteria, and cross-SOR population matching was problematic. E.g. employee and student records are considered to be "the same person" if they match on first name, last name, SSN, and DOB. We never collect SSN for affiliates, so there can theoretically never be an automatic match.

Modern matching technologies can vastly improve record matching.

University of Southern California (129.usc.3.20150412)

Modified: 4/12/2015 3:42:42 PM

Participants

CIO or CIO Delegate

Workshop 1 *Pete Siegel*

Senior Identity Architect

Workshop 1 *Asbed Bedrossian*

Support for the Lifestyles of the Attribute Rich and Privacy Preserved (LARPP)

Actors

Data Stewards

IAM Governance Bodies

InfoSec

Stakeholder Groups

Researcher/Scholar

External collaborator or contractor

Cross-federation researchers

Collaborators

Scholars

InfoSec

Story Narrative:

As a second step, USC’s vision of supporting federation-wide collaboration while preserving the user’s privacy is by supporting LARPP. LARPP allows for a scoped end user control over which person attributes may be released and to which services. This is a federation’s implementation of “informed consent”.

University of Southern California (130.usc.4.20150412)

Modified: 4/12/2015 3:43:25 PM

Participants

CIO or CIO Delegate

Workshop 1 *Pete Siegel*

Senior Identity Architect

Workshop 1 *Asbed Bedrossian*

InCommon R&S Category support

Actors

Data Stewards
IAM Governance Bodies
InfoSec

Stakeholder Groups

Researcher/Scholar
External collaborator or contractor
Cross-federation researchers
Collaborators
Scholars
InfoSec

Story Narrative:

USC has an IAM governance committee called IAMSC, which reviews attribute access requests (AAR) for person related data. When the committee endorses an AAR, the data stewards of relevant SOR's review the request to authorize access, and enable the service.

USC plans to implement the InCommon R&S category support through an AAR request. When implemented, USC accounts will be able to visit R&S category services at any participating institutions, without any additional configuration at either USC, or the other institution. This will greatly improve the user experience of cross-site collaboration.

University of Utah (131.utah.1.20141209)

Modified: 12/9/2014 8:20:28 AM

Participants

CIO or CIO Delegate

Workshop 1 *Steve Corbato*

Senior Identity Architect

Workshop 1 *Subhasish Mitra*

Account Registration/Self-service

Actors

Individual User (All Users)

Home Organization

Stakeholder Groups

Researcher/Scholar

Faculty/Teacher

Learner/Student

Staff

External collaborator or contractor

Story Narrative:

Account activation at the U is basically a simple process of Customer Service Advocate contacting the individual user to inform him/her his unique uNID and first-time default password with instructions to do so via https://somelink.utah.edu (home grown portal).

First-time the user is forced to change/reset his password to his own like.

Upon authentication to the portal, the optional steps related to account activation processes that he/she can perform (self-service) are –

Publish emergency notification service information

Assign Security Questions for Password Self-Service

Change Email Address / Assign Alias

Provisioning to down-stream application is dependent on this step, IAM Program prespective, The first-time password is too ease to guess, the security question is an optional step in the process, the account acceptance policy is missing.

We need account registration process and system which follows more industry standard and can be coupled with either Password Management Solution or Long-term Identity-Lifecycle Management System.

University of Utah (132.utah.2.20141209)

Modified: 12/9/2014 8:20:47 AM

Participants

CIO or CIO Delegate
Workshop 1 *Steve Corbato*

Senior Identity Architect
Workshop 1 *Subhasish Mitra*

Two Factor with CAS and Shibboleth

Actors

Individual User
Home Organization – Campus Departments and ITS
Virtual Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff
External collaborator or contractor

Story Narrative:

University of Utah has a moderate number of federated service providers authenticating via InCommon and uses CAS for internal applications (200+).

We have reached the point from a risk perspective that we want to implement two factor authentication-using DUO for some of the service providers that contain more sensitive information.

We have narrowed two primary use case for MFA –

User Opt-In to MFA for all CAS & Shibboleth enabled applications. (High Priority, where in we under planning of releasing for smaller internal communities with Campus and Hospital).

Application due its nature/purpose, Security Office would like to make that application MFA enabled for any/all users accessing the application.

In collaboration with Incommon, Unicon developed CAS overlay to integrate with DUO, which we need to maintain locally for future.

Sadly, the current state of Shibboleth requires two additional open source modules separately maintained to complete this desired level or authentication. While possible this becomes risky for a high utilization and uptime systems.

The desire would be to have CAS and Shibboleth include these functionalities as a base supported service.

University of Virginia (133.virginia.1.20150412)

Modified: 4/12/2015 3:44:27 PM

Participants

CIO or CIO Delegate

Workshop 1 *Virginia Evans*

Senior Identity Architect

Workshop 1 *Jim Jokl*

Improved Identity Life-cycle Management

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

A new user becomes affiliated with the university via one of many sources, has an identity created, and is able to use this identity throughout their lifelong engagement with the university. Identity deduplication is not a burden on central staff. Data sources can leverage real-time central identity creation via appropriate APIs. End users have access to an Identity Console to update key central attributes and be assured that these updates will be properly propagated to all university systems.

University of Virginia (134.virginia.2.20150412)

Modified: 4/12/2015 3:44:39 PM

Participants

CIO or CIO Delegate

Workshop 1 *Virginia Evans*

Senior Identity Architect

Workshop 1 *Jim Jokl*

Improved Provisioning Services

Actors

Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

A person affiliated with the university often transitions through many different phases from applicant, to student, to employee type a, to employee type b, to alumni, etc. Within each of these phases, a person may assume various roles depending on function, classification, training, research, and other factors. A flexible, reliable provisioning solution with standard interface APIs and pre-built interfaces (as appropriate) automatically provisions appropriate services, facilitates authorization for self-provisioned services, and ensures that an accurate record exists for all of the services provisioned to a user at any point in time.

University of Washington (135.uw.1.20150412)

Modified: 4/12/2015 3:45:39 PM

Participants

CIO or CIO Delegate

Workshop 2 *Kelli Trosvig*

Senior Identity Architect

Workshop 2 *Nathan Dors*

Other Institutional Identity Needs

Workshop 2 *Brad Greer*

Inter-Institutional Research

Actors

Virtual Organization

Stakeholder Groups

Researcher/Scholar

Faculty/Teacher

External collaborator or contractor

Story Narrative:

As a clinical researcher and faculty member in medical education, I interact with a wide variety of individuals affiliated with different institutions – researchers and students at other schools, doctors at regional medical centers, folks at funding agencies, external advisory committees, etc. To achieve our goals around research, education, and patient care, we often form virtual organizations (VOs). These VOs depend on access to collaboration tools, research instruments, large and small data sets, electronic medical records, and other resources. Some of the resources, like email and calendaring, are more commonplace, while others, like some of the instruments and data sets, might be created during our collaboration. Much of our work involves highly sensitive PHI, so we take HIPPA compliance very seriously. We need IAM solutions for dealing with these complex inter-institutional research activities, particularly solutions for the access issues that arise at the start of our VOs and continue until they end.

University of Washington (136.uw.2.20150412)

Modified: 4/12/2015 3:47:28 PM

Participants

CIO or CIO Delegate
Workshop 2 *Kelli Trosvig*

Senior Identity Architect
Workshop 2 *Nathan Dors*

Other Institutional Identity Needs
Workshop 2 *Brad Greer*

Mixing MFA into Microsoft Infrastructure

Actors

Identity Infrastructure Operator
Service Provider
Individual User

Stakeholder Groups

Governance Stakeholder
Help Desk
3rd Party Software Vendor

Story Narrative:

This story involves an institution that uses Microsoft technologies (Windows desktops, Windows servers, SQL servers, Exchange, SharePoint, Office 365, etc.). These technologies require the identity infrastructure operator to provide infrastructure components such as Active Directory, Active Directory Federation Services (ADFS), and/or Azure Active Directory. Because these components provide some of the same IAM capabilities as other infrastructure components, the identity infrastructure operator must coordinate strategy and design across components to meet the needs of Service Providers and Individual Users, as well as others stakeholders. This is particularly true for the coordinated delivery of multi-factor authentication (MFA) as described by these related user stories:

As an **identity infrastructure operator**, I want to enable service providers to select cost-effective solutions for MFA without negatively impacting the experience of individual users. For more discretionary cases, also want individual users to be able to opt in to MFA, so that they have some choice in the strength of authentication they use. If I can also factor in other potential risk indicators (e.g. unusual geographic locations, unrecognized devices, unusual network addresses, uncharacteristic patterns of use), it would help me serve my customers better. My challenge is figuring out how to deploy MFA solutions across my Microsoft and non-Microsoft infrastructure components to reduce duplication and provide a consistent, usable experience to individual users.

As a **service provider**, I know that threats like phishing and password reuse are problems I need to confront head-on with my identity infrastructure operator. I want to protect information through appropriate safeguards for risks such as unauthorized access and other unintended or inappropriate disclosures. I know that MFA is an effective security control I can use to manage these risks. However, for more discretionary cases, I'd like to allow my individual users to opt in to using MFA. I can accept some additional risk, but I'd like my identity provider operator to factor in other risk indicators and adjust user interactions to balance risk and convenience. I think this is friendlier and makes more sense to my individual users. I need my identity infrastructure operator to provide solutions for Microsoft and non-Microsoft technologies.

As an **individual user**, I don't want more than one account and password to manage. If I'm required to use MFA, I don't want to be issued more than one other credential, and a fallback mechanism. I don't want to carry around an extra device. I also want self-service ways to opt in to MFA for access to my information. I may want to enroll my own device for this, and please, don't make me log in again just because it's after 5pm and I've reached some sort of timeout – that annoys me and sometimes even causes me to lose work. That's not fun.

University of Wisconsin - Madison (137.wisc.1.20141209)

Modified: 12/9/2014 7:13:20 AM

Participants

CIO or CIO Delegate

Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*

Senior Identity Architect

Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Simplified Service Federation

Actors

Individual User
Home Organization
Federation Service Provider

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

A faculty member on a UW campus is engaged in teaching a cooperative course involving students from multiple institutions. The faculty member has created several electronic resources that are protected by the institutional authentication system used by her campus. She would like the remote students to be able to access these resources using their home institution’s credentials.

The campus IT organization providing authentication services does not have a high degree of technical expertise in supporting federated services, but is able to install and configure a federated authentication service easily based on simplified packaging and installation of TIER software. Default configurations for common service providers assist the campus IT organization in enabling the service for federation. Easy tools for federation endpoint configuration allow the campus IT organization to register their service endpoints in an identity federation without intimate knowledge of the finer points of federation metadata management.

University of Wisconsin - Madison (138.wisc.2.20141209)

Modified: 12/9/2014 7:21:56 AM

Participants

CIO or CIO Delegate

Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*

Senior Identity Architect

Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Community-supported Identity Registry

Actors

Individual User
Data Custodian
Identity Infrastructure Operator

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

An Identity Infrastructure operator requires the ability to consolidate person data into a central registry to create a single representation of an individual and their associated roles across multiple source systems for the purpose of providing a unified view of people to service providers.

The Identity Infrastructure operator participates in development of a TIER-sponsored, community-supported Identity Registry product that includes facilities for normalization of data from disparate source systems, identity linking and management and person data delivery services.

University of Wisconsin - Madison (139.wisc.3.20150125)

Modified: 1/25/2015 2:42:19 PM

Participants

CIO or CIO Delegate

Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*

Senior Identity Architect

Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Federated Access for Flexible Degree Students

Actors

Individual User
Data Custodian
Identity Infrastructure Operator

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

University of Wisconsin System students in the Flexible Degree Program are required to access resources from multiple campuses in order to complete self-paced courses and pass a competency-based exam. These courses do not follow the traditional boundaries of semester or term.

Flexible Degree students will be registered at one of 13 UW System campuses, but may be required to access course resources at other institutions. These resources could include access to electronic library resources, virtual computer labs, learning management systems or other electronic assets.

Many of these assets are licensed to a single campus or a subset of users on a campus studying a particular degree program, so the Flexible Degree students must not only authenticate, but be recognized as authorized to use the resources that are licensed for the degree programs being studied.

University of Wisconsin - Madison (140.wisc.4.20150125)

Modified: 1/25/2015 2:45:50 PM

Participants

CIO or CIO Delegate

Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*

Senior Identity Architect

Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Cross-Institutional Grouping and Group Management

Actors

Individual User
Data Custodian
Identity Infrastructure Operator

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

The University of Wisconsin System offers a number of applications to all 13 member campuses, usable by all (or a significant subset) of students, faculty and staff. Additionally, each campus may offer services that are needed by users on campuses other than the hosting institution.

The UW System manages a SAML-based identity federation, but requires a cross-institutional grouping system to support externalizing authorization from applications while allowing cross-institutional access. This grouping system must support data-driven grouping based on institutional data as well as ad-hoc grouping across institution that is expressed and maintained by non-technical users.

University of Wisconsin - Madison (141.wisc.5.20150125)

Modified: 1/25/2015 2:52:13 PM

Participants

CIO or CIO Delegate	
Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*
Senior Identity Architect	
Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Registration of Virtual Organizations

Actors

Individual User
Data Custodian
Identity Infrastructure Operator

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

The University of Wisconsin System has managed a system-wide identity federation for a number of years. This system allows service providers to serve users across multiple campuses while allowing users to use their home institution's credentials..

There is an increasing need to register additional partners into the Wisconsin Federation. Examples include hospitals and clinics that are affiliated with UW System institutions, K12 and technical college districts with resource sharing agreements and research organizations. These partners require access to services that are protected by the Wisconsin Identity Federation, and need to be registered as Identity or Service Providers.

UW System requires a simple method for managing registration of virtual organizations to the Wisconsin Identity Federation, and for managing and distributing metadata about virtual organizations to all federation participants.

University of Wisconsin - Madison (142.wisc.6.20150403)

Modified: 4/3/2015 1:29:25 PM

Participants

CIO or CIO Delegate

Workshop 1	*Bruce Maas*
Workshop 2	*Ty Letto*
Workshop 3	*Ty Letto*

Senior Identity Architect

Workshop 2	*Tom Jordan*
Workshop 3	*Tom Jordan*

Application Provisioning

Actors

Individual User
Data Custodian
Identity Infrastructure Operator

Stakeholder Groups

Student
Faculty/Teacher
Staff

Story Narrative:

The University of Wisconsin System has managed a system-wide identity federation for a number of years. This system allows service providers to serve users across multiple campuses while allowing users to use their home institution's credentials..

The Wisconsin Identity Federation requires an effective tool for dynamically provisioning application accounts, roles and permissions in applications that require user provisioning prior to first login. This tool should be able to provision using standards-based provisioning interfaces (SPML, SCIM) and should include the ability to develop or license connectors for common application endpoints (LDAP, Active Directory, relational databases, etc).

Virginia Polytechnic Institute and State University (143.vt.1.20150412)

Modified: 4/12/2015 3:50:17 PM

Participants

CIO or CIO Delegate

Workshop 1	*Scott Midkiff*

Senior Identity Architect

Workshop 2	*Karen Herrington*
Workshop 1	*Mary Dunker*
Workshop 2	*Mary Dunker*

Open ID for native and web-based mobile applications

Actors

Individual User
Home Organization

Stakeholder Groups

Faculty/Teacher
Learner/Student
Staff

Story Narrative:

Most Virginia Tech constituents carry mobile devices -- smart phones, tablets -- and they often need to access Virginia Tech applications while they are away from a desktop or laptop computer. Virginia Tech has developed a mobile application which consolidates access to those applications, but authentication is a major barrier to a fluid user experience across native and web-based mobile interfaces. Both native mobile apps and the web-based interfaces need support for SSO. If our IdP supported OpenID Connect we could provide a seamless SSO experience for our users on mobile devices. We believe that our IdP must support multiple authentication protocols in order to support a growing ecosystem of mobile applications.

Virginia Polytechnic Institute and State University (144.vt.2.20150412)

Modified: 4/12/2015 3:50:28 PM

Participants

CIO or CIO Delegate

Workshop 1	*Scott Midkiff*

Senior Identity Architect

Workshop 2	*Karen Herrington*
Workshop 1	*Mary Dunker*
Workshop 2	*Mary Dunker*

Tools for configuration and auditing

Actors

Home Organization

Stakeholder Groups

Staff

Story Narrative:

Virginia Tech’s identity management infrastructure includes a central person registry, OpenLDAP directories, Shibboleth IdP, group management, CAS, and appropriate middleware to connect the components and replicate information to other systems. A directory administration tool (DAT) was developed to perform functions such as viewing identity information, managing accounts, and resetting passwords. Connectors import identities from the ERP system into the registry, and identities that need not exist in the ERP system can be created individually using the DAT. Administrative tools are lacking for the following:

Shibboleth configuration and authorization maintenance

Importing ad-hoc groups of identities into the person registry

Audit reporting tools

The absence of administrative configuration and audit tools generates additional work for technical support staff and raises auditing questions. Including such tools in the core TIER products will benefit participants with identity management systems of all maturity levels.

Virginia Polytechnic Institute and State University (145.vt.3.20141205)

Modified: 12/5/2014 9:25:06 AM

Participants

CIO or CIO Delegate

Workshop 1	*Scott Midkiff*

Senior Identity Architect

Workshop 2	*Karen Herrington*
Workshop 1	*Mary Dunker*
Workshop 2	*Mary Dunker*

Discretionary attribute release and management

Actors

Individual User
Home Organization
Virtual Organization
Service Provider

Stakeholder Groups

Learner/Student

Story Narrative:

Due to concerns with FERPA compliance, Virginia Tech does not release personally identifying attributes for students unless a contract exists between the university and the specific service. For employees, we release the Research & Scholarship attributes to all InCommon service providers. For students, we only release the minimal attributes required for authentication. This inconsistency in attribute release policy can cause confusion for service providers and end users when a Virginia Tech graduate student or non-standard employee affiliate attempts to access a R&S service such as GENI. Additional attributes can be released with approval from the individual, but our current process requires a manual configuration change to the IdP.

As our user community becomes more aware of the collaborative research opportunities offered through InCommon, our case-by-case handling of student attribute release for individual services will not scale. If students and other affiliates were able to consent to releasing some of their personally identifying attributes to services, we believe FERPA concerns would be addressed while preserving student privacy. We need to include functionality in our IdP that enables discretionary release and management of attributes by the end user.

Virginia Polytechnic Institute and State University (146.vt.4.20150412)

Modified: 4/12/2015 3:50:49 PM

Participants

CIO or CIO Delegate

Workshop 1	*Scott Midkiff*

Senior Identity Architect

Workshop 2	*Karen Herrington*
Workshop 1	*Mary Dunker*
Workshop 2	*Mary Dunker*

Multi-factor Authentication

Actors

Home Organization

Stakeholder Groups

Researcher/Scholar
Staff

Story Narrative:

Virginia Tech was certificated to assert InCommon Silver assurance using a multi-factor alternative means. While Silver assurance does not require multi-factor authentication, institutions may look at implementing multi-factor as a best practice in order to meet the Silver criteria of the InCommon Identity Assurance Profiles Bronze and Silver. Since the SAML multi-context broker was developed for Shibboleth v2, that code base will be obsolete for institutions implementing Shibboleth v3. Virginia Tech’s multi-factor integration is implemented in CAS, but we would expect other institutions to benefit from porting the multi-context broker to Shibboleth v3.

Washington University - Saint Louis (147.wustl.1.20150412)

Modified: 4/12/2015 3:51:20 PM

Participants

CIO or CIO Delegate
Workshop 2 *John Gohsman*

Senior Identity Architect
Workshop 2 *Dan Zweifel*

Other Institutional Identity Needs
Workshop 2 *Kevin Hardcastle*

Shared Service SaaS app provisioning

Actors

Home Organization
Service Provider

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
Staff

Story Narrative:

The University decides to adapt a Net+ SaaS app that will be available to all current faculty, staff and students. The Service Provider offers SAML for authentication, Just-In-Time provisioning and API's for managing user attributes and account status. The IAM team is required to integrate the new service with existing IAM infrastructures to manage authN, entitlement and user attributes.

Given the lack of a standards-based integration services layer we are forced to roll our own solution. As we expand our adoption of cloud solutions significant resources will be needed to manage individualized integration points. Having a service that supports standards like SPML/SCIM, OAuth for SCIM, etc. and contains out of the box interfaces for Box.net, Google Apps, etc. would simplify adoption of SaaS offerings.

Washington University - Saint Louis (148.wustl.2.20150412)

Modified: 4/12/2015 3:51:54 PM

Participants

CIO or CIO Delegate

Workshop 2 *John Gohsman*

Senior Identity Architect

Workshop 2 *Dan Zweifel*

Other Institutional Identity Needs

Workshop 2 *Kevin Hardcastle*

Not Quite All

Actors

Service Provider

Other (Non-employed Resources e.g. Agency Staff, visiting faculty)

Stakeholder Groups

Researcher/Scholar

Staff

External collaborator or contractor

Story Narrative:

Collaborator Steve from a peer institution is participating in a WashU research project. Before Steve can begin work he must complete WashU's compliance requirements. The PI that Steve is working with doesn't know that Steve had a previous role at WashU and since little information about Steve is required to facilitate access to compliance systems a new record is created for him. Steve shows up at the lab ready to work; sits down to complete his compliance requirements; logs in with his known WashU credentials and finds that there are no compliance requirements assigned for him to complete! Frustration sets in for Steve and the PI because their work together is delayed by at least one day until Steve's identity crisis can be untangled and he meets his compliance requirements…

Having multiple entry points for person data with no central attribute search capability and limited Service Provider federation for external entities causes duplicate entities to be created leading to disruption in or incomplete access to resources, additional administrative overhead and an inability to address single end-point log and application access.

As we expand access to systems for agency staff (contractors, temps, consultants), partners and other outside entities there is no clear record of authority to assist in managing their person data or WashU roles.

There are other concerns around campus notification. How do we you inform "other" continuance that are on campus that there is a shooter on campus?

Yale University (149.yale.1.20150412)

Modified: 4/12/2015 3:54:44 PM

Participants

CIO or CIO Delegate

Workshop 3 *Susan Kelley*

Senior Identity Architect

Workshop 3 *Amit Poddar*

Expanded Authentication Service

Actors

Individual User
Home Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
Learner/Student
External contractors
Parents/Guardians

Story Narrative:

Stakeholders:

Researcher/Scholar -- collaborators

Faculty/Teacher -- guest lecturers

Learner/Student -- applicants

External contractors / parents-guardians

Yale currently assigns a username (netid) for authentication purposes to all active members of the community. This is possible because we institutionally curate accurate identity data for our community. Certain individuals, however, have a need to authenticate to Yale services but are otherwise unknown to us. This population includes guardians of existing undergraduates who may wish to cover certain student expenses, applicants to Yale for student admission and parties representing external vendors who do business with the university (and others). Sometimes it is necessary for us to record identity information for these folks but often it is sufficient to have someone vouch for the authenticity of the individual in order to perform a very specific task. A generalized framework is, therefore, desirable that would allow the bounded lifecycle of an identity external to the University to be managed along with specific subset access control to limit access to only appropriate services.

Yale University (150.yale.2.20150412)

Modified: 4/12/2015 3:54:51 PM

Participants

CIO or CIO Delegate
Workshop 3 *Susan Kelley*

Senior Identity Architect
Workshop 3 *Amit Poddar*

Library Special Collections

Actors

Individual User
Home Organization -- Library
Virtual Organization -- Special Collections
Service Provider
External collaborator

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
External collaborator or contractor

Story Narrative:

The University libraries maintain special collections in both physical and electronic form that are only accessible with approval by the library staff member who curates the collection (and potentially the collection donor). The requests frequently come from folks who are neither affiliated with Yale or another research institution (e.g. journalists). The criteria for access varies from collection to collection and access is often limited to a subset of the collection and time bounded. Other specific limitations are often noted on the access to a special collection including the ability to copy all or part of the content or even the ability to create annotations or detailed notes on the content. Providing support via a trust framework for this complex set of requirements is desirable.

Yale University (151.yale.3.20150412)

Modified: 4/12/2015 3:55:34 PM

Participants

CIO or CIO Delegate

Workshop 3 *Susan Kelley*

Senior Identity Architect

Workshop 3 *Amit Poddar*

Collaborating Researchers

Actors

Individual User
Home Organization
Virtual Organization

Stakeholder Groups

Researcher/Scholar
Faculty/Teacher
External collaborator or contractor

Story Narrative:

It is common for researchers at Yale to collaborate (often by way of a shared research grant) with peers outside of the university. Often there is a need for the collaborator to be granted authenticated access to Yale-owned resources. While traditional federation services via In-Common and eduGain address a large number of these needs, a comprehensive set of recommendations and technology would be desirable for circumstances where research partners lack federation affiliation and may not even have easy access to the most traditional OpenID Connect social/external authentication sources. An alternative that doesn't devolve to the assignment of Yale credentials would be desirable. This solution would ideally be extensible to test/research subjects and would not be encumbered by institution-level identity proofing.

Yale University (152.yale.4.20150412)

Modified: 4/12/2015 3:55:53 PM

Participants

CIO or CIO Delegate

Workshop 3 *Susan Kelley*

Senior Identity Architect

Workshop 3 *Amit Poddar*

Transparent and secure data access for application developers

Actors

Home Organization

Stakeholder Groups

Staff

External collaborator or contractor

Story Narrative:

Yale is in the process of building an API portal to provide access to data for application builders. Some of this data, like Laundry and Events, are public information and an API key identifying the application is sufficient for security but for other data such as Course Information we need to make sure that the end user has the appropriate affiliation to the University. Instead of delegating the task of authenticating and identifying the end user to the application, if would be preferable if it was done by a central authorization point that allows the application to access the data on behalf of the end user using an opaque token. This authentication and identification process needs to be not burdensome for application developers and also should have security and robustness of an Enterprise Single Sign On (SSO) solution.

Yale University (153.yale.5.20150412)

Modified: 4/12/2015 3:56:16 PM

Participants

CIO or CIO Delegate

Workshop 3 *Susan Kelley*

Senior Identity Architect

Workshop 3 *Amit Poddar*

Shibboleth Improvements

Actors

Home Organization
Service Provider

Stakeholder Groups

Staff
External collaborator or contractor
Federation partners

Story Narrative:

Yale has numerous federation partners both in enterprise and higher education and as we choose to move more applications to the cloud this number is increasing. Lot of these partners need access to specific attributes which are released just to them. It is desirable that we are able to manage, report on and configure this information in a comprehensive automated fashion of creating XML files and placing them in specific folders and writing custom tools.

We have also found cases where adding some attributes for one partner breaks the whole system and we end up implementing custom ways of segregating the providers to ameliorate the problem. It would be desirable that shibboleth was built in a way that changes for one partner do not affect the other partners and that we had a way to run a dry run of the assertion generation process to see what effect a change will have before enabling the change.