Notes from 2014 Quilt InCommon Federation Workshop

Introduction

Welcome from George Laskaris, NJEdge.net:

Working on federation pilots for K12 and community colleges has been a highly collaborative effort. The agenda for this workshop includes hearing from the current pilots, discussing partnership and business models, hearing about interfederation, and talking about getting started with a new pilot

Comments from Shel Waggener, Internet2 Senior Vice President, Net+ Services: The Quilt InCommon Pilots have been doing important work. Looking ahead, we will want to transition from pilots to wider production. Many educational institutions lack the resources/depth of staff to handle identity infrastructure. Should we should be thinking about architecting “identity as a service,” particularly for small colleges, community colleges and K12? It would be good to develop a more turnkey approach to identity management and federation. Does it make sense to develop a service that the regionals can offer? Or is it better to work on hardening standards and providing guidance and then have everyone offer their own unique service ?

Two paths:

1. We establish best practices
2. We offer a service

Please share your thoughts with John Krienke, Chief Operating Officer of InCommon and Steve Zoppi Associate Vice President, Services Integration and Architecture, both of whom are here at the workshop. Another challenge for our community is doing a better job of working with commercial providers and together defining standards that are effective for the education environment.

=======

Presentations from the Pilots

Merit Network

Slides (David Dennis)

- Merit has its own federation: Merit Michigan ID
- Had hoped to do Interfederation with InCommon, but it has not happened yet
- Pilot never fully materialized, but learned a lot along the way and collaboration has been fantastic
- At the Merit Member Conference in May 2013 there were sessions to highlight federation
- Don Welch talked about federation and Shel conducted a session
- Did email and outreach campaigns; Did a series on the benefits of federation
- Trained the member relations and sales team to talk to K12 and community colleges and to seek pilot candidates
- Good discussions, but interest tapered off after the conference
- What is the carrot at end of stick? The districts have limited resources
- Looking to do a K12 pilot with NJVID or Canvas
- Worked with a college that uses Canvas and want to do it in a federated fashion
- It did not become a high enough priority for them during this timeframe
- Talked with Canvas staff and they see the advantage to federating with Merit
- However, Canvas has other things on their priority list, so they put this off
- It will happen in the future, but not within the timeframe
- Lessons Learned:
- Need to recruit members, ensure as many members as possible are joining the federation
- Need one or two influencers in the community to help us build the case studies
- Continue looking for a K12 pilot interested in Cloud Media (NJVID)
- Overall, great learning experience
- Want to hear about how to do better outreach and education

MCNC

slides presented by Mark Scheible

- Small and focused pilot
- Worked with Davie County schools, already an InCommon member and Davidson County Community College (DCCC)
- Goal was to get Davidson County Community College federated so the K12 federation could be used to access resources
- Moodlerooms was the target application, the goal was to get an SP in front of that service
- Challenges: they key players already had busy schedules; hard to coordinate them
- Successes: got DCCC through process of joining InCommon; their metadata is in InCommon
- Accepting SAML assertions in the test environment
- Don't have students using it yet
- MCNC tried to get Moodlerooms into InCommon Metadata, but that does not work
- Trying to get Moodlerooms to submit the metadata
- They have only one endpoint, and we wanted something separate for this pilot
- Hope to get that resolved by end of month
- Currently doing testing and waiting for the SP to get into metadata

OARnet

slides presented by Paul Schopis

- Mark Beadles has been active in this effort but could not be here at the workshop
- For this pilot wanted to get 3-5 Ohio community colleges to federate
- Hybrid federation model
- Target Apps: Library system, State Board of Regents apps, and roaming wireless (eduroam)
- Partnering with Fischer International on this work
- Goal is to enhance teaching experience at community colleges
- Longer term goal is to extend federation beyond the community colleges to K12
- And provide easy transition for students who go to public universities
- Adoption is slow and steady; Underwhelming but picking up
- Is there a low demand for federation?
- Large universities can do their own thing
- Do the smaller schools not see the value? Is the cost prohibitive?
- Fischer International houses their cloud solutions in Rackspace
- OARnet was spinning up and hoping to use that cloud
- Fischer's technical people are apt and can communicate requirements
- But working with Rackspace was challenging
- OARnet is also developing capability to do hosting internally
- Trying to understand how many schools must adopt to have this as a sustainable business model
- The schools participating in the pilot are satisfied
- Plans for scaling via increased outreach and education

Q: Radius is a requirement for eduroam . Are the schools already running Radius?

A: No OARNet must stand up Radius for the schools.

=======

MDREN

slides Presented by Guy Jones

- Original pilot proposal was to work with Fischer International to set up central service and use contracts for individual schools
- Worked with Fischer to develop IDP contacts
- The planned approach was to get schools into InCommon
- But none of the members wanted to use the Fischer contracts.
- The focus shifted in early fall 2013; we moved forward with Coursera
- Tagged onto a different program that was rolling out an environment for MOOCs with Coursera
- It covered small and medium sized schools and was funded by the Gates Foundation
- Each school had a variable level of capability of establishing an internal IDP
- Each school accomplished this in its own way
- They wanted to do it because their was paid for and there was statewide interest
- Ended up with bilateral exchange of data with Coursera, where each school exchanges data with the SP
- It's not scalable but it worked
- Coursera and the schools were not excited about Shibboleth, even though Coursera is an InCommon member, they did not have Shibboleth set up
- At the schools, the simpler exchange of metadata is easier to implement initially
- MDREN worked with schools and with Coursera to provide interconnection; got the process up and going
- This is one-off, but we hope to bring on new services in the future
- We built a community of common shared interest in getting this done
- Coursera was NOT pushing for this; they would have wanted us to send them a list
- Took several conference calls to convince them; they did not have the expertise
- Even though Coursera is an InCommon member
- Looking ahead, there are some political hurdles; Setting up meeting with MD Dept of Education
- Re-look at InCommon and how to extend it out
- Data crossing the border is frowned upon
- Must have the interest and the interest is only there when you have the services/apps (chicken and egg)
- Hope to have a service that starts small and then has big growth

==

Comment: You covered a lot of ground. Why didn't districts sign contracts w Fischer International?

A: Some districts hired Fischer International on their own without the contract. Some schools hired other vendors. Some schools did it themselves.

====

Q:: Did the schools find Shibboleth easy to install?

A: In some cases they found it easy, in others they got local help.

Q: Is there interest from K12?

A: Yes, there is some interest from K12 in a common authentication structure. K12 in Maryland is limited in using cloud services. Must go through Annapolis. InCommon does a vetting process and the small schools may not be ready for vetting and controls. We are missing attractive applications, but we are close to working with NJVID

Illinois

slides

Presented by Bernie A'cs from University of Illinois and Jim Petersen from Illini Cloud

- NCSA and IlliniCloud are participants in the ISLE project with objective to develop and IdM solution that can be adopted by K12
- Establishing three foundational service dimensions for K12: 1) data services, 2) identity services, 3) presentation services
- Initial Goal: establish an IdM infrastructure for K12 districts that will allow them to manage relationships with SP's.
- Project space is to help them do metrics and visualizations of students progress
- Identity is critical and is connected with data
- Want to provide a single sign-on service for critical applications
- Used Aegis Identity for integration with legacy systems and provisioning and deprovisioning
- Unicon focused on how to do a presentation to create a solution that made sense for K12
- Districts want to do what they are doing now, with heavy lifting being done by a central service
- We need to create a low threshold adoption
- K12 teachers want real time info; They don't want to sort through a lot of stuff
- Did not want school services to have to make modifications
- Jim Petersen: We want to reduce the burden on school districts
- We have moved many services to the cloud (internal and external)
- Developed IlliniCloud Portal, which can be customized by the "tenants" (districts)
- As the districts move towards cloud-based services this is an interim step
- To avoid the political fallout, these are local school districts working together
- The university is not telling K12 how to do this

Questions:

Q: You use the portal to tie in the identity? For the school districts it's a hybrid ?

A: The portal is a conceptual space, This is an excuse to say we can make web based SSO work . We say look it's a cake, take a bite. Keep a low threshold for adoption. We tell the school district, you don't have to change what you are doing. Just play in this sandbox. We don't store anything locally. We don't house or cache or persist. We depend on their system to be the authoritative source.

============

Q: What will you do with the product? Roll it out to Illinois? Other states?

A: Pleased to have collaborations across state lines. But generally if you cross the border it’s an issue We must say this is bound by the state boundaries

it's open source though some of the affiliate work is not open source

Nebraska

slides presented by Mike Danahy and Scott Isaacson

- Stakeholders include Univ. of Nebraska and Nebraska Information Technology Commission
- Brought Shib Training to OHMHA in Oct 2013
- Eight K12 educational service unit reps participated in the Shib training
- Universities were also represented at the Shib training as well
- The Identity Systems are important for the seamless learning environment
- Formed a group that meets monthly to work across all systems and to move the concepts forward
- The effort really started 10 years ago and it has been quite a journey
- Started w a directory system statewide; meetings got hung up on the attributes
- Single sign on was identified as having strong value
- Explaining InCommon to the community is important
- Need to paint the picture and to connect the dots
- Need to get everybody on board
- SETDA website is helpful
- Repurposing an article from the SETDA website so the vision is clear (Jack's story)
- COSN has done good work and prepared a good primer on IDM http://www.cosn.org/sites/default/files/pdf/Single%20Sign%20On%20Primer.pdf

- Technical Challenge: we have wide variety of directory systems
- More and more privacy issues come up

Q: Shel: regarding engaging the state who are working on federation for their own agencies, should the Pilots send a letter to the states saying that federation is underway?

Comment: Could be a good strategic move, the message must be thoughtful and must explain what EDU brings to the table re schema definition and how is that applicable to the broader audience. What the pilots are doing is good press and is advantageous to anyone. working at the states

We don't way we will solve this problem for the state. Just to explain what we are doing for EDU

Utah

presentation by Jim Stewart

- **Status as of Feb. 2014**:
- A Service Center in SW Utah is committed to putting up an IDP and UEN is working with them to bring that online.
- Then UEN will work with them to be sure they have credentials into the UEN SP. That should happen by end of March 2014.
- The initial pilot will be finished at that point. Then UEN will look to go beyond the initial pilot.
- **Challenges as of Feb. 2014**:
- 1) Some of our services are not SAML2 complaint, and we must determine how to update or migrate to a SAML2 compliant service.
- 2) We want to get to where federated Identity is an official recognized service of UEN. We are working to get the board, the regional service centers and districts to understand the value proposition and the trust fabric. Need to them to commit to putting up IDPs. Cost can be a barrier. Some do not have the inclination given competing priorities.

- **Additional Comments from Jim Stewart**:
- Utah has had Single Sign-on conversations for many years
- Sent people to Shib training in June 2014
- MYUEN service will allow access to the Pioneer library, for services such as streaming video, etc
- http://www.uen.org/my.uen/help/faq.shtml
- Working to bring up the regional service center and ensure that there is federated access to the UEN services

Comments:

- Illinois and Utah and others have talked about the challenges of policy changes.
- It can be useful to work with local educational associations.
- Many unique trust issues in K12, for example issues around attributes for age cutoff for certain services
- We want to use the same architecture across the board for such attributes
- For example, Instead of sending an age attribute you send the permission.

Partnership Business Models

slides

presented by Mark Scheible, MCNC and Mark Johnson, MCNC

- A group of MCNC staff and InCommon staff met in Chicago in Sept. 2013 to start to develop proposed federation partnership business models
- See the resulting document at http://tinyurl.com/ky2r5wl

- A next step is to work on the financial terms associated with the proposed federation partnership business models
- MCNC will put model #4 (Full Service Steward) in place as a pilot effort

- Q: How do libraries fit into the business models?
- A: That is an issue for InCommon Steering. InCommon Steering committee governs the classes that can join InCommon. InCommon does not currently support libraries as a class, but libraries can be sponsored partners

- Mark Johnson: The categories of other (including heathcare) is an area where the regionals can potentially apply some leverage

- comment: NIST is working on other authentication models
- Shel: Ken Klingenstein has a grant from NIST to look at authenticated anonymous credentials, work is progressing on that.
- See http://www.internet2.edu/vision-initiatives/initiatives/trusted-identity-education/scalable-privacy/

- Q: How would the Regional Federation Operator interact w InCommon?
- A: Paul Caskey will discuss this in his talk on interfederation

- Comment: Could there be a representative of a regional serving on the board of InCommon? This is a governance issue that should be examined in the future.

- Question: Concerning a regional submitting metadata from a variety of institutions into inCommon's metadata aggregate, what about RA Validation? For example, if MCNC acts as that validator, will MCNC comply with the same level of trust that is used in InCommon?
- Answer: That will be part of a legal agreement re eligibility and classification.

- Some of the organizations represented at this workshop are not exactly regionals, but they are aggregators of IDPs and SP's
- Another type of class of InCommon participant
- Can libraries be a part of that model?
- We don't want to force a region into a representation model they are not ready for
- We want to honor a state's ability to organize itself
- Some states are organized differently at the identity layer versus the network layer

- This needs to work in a financial ecosystem

- Transaction models have not been tried in this space
- So unit of price could be based on number of IDPs
- For example, should two different states pay InCommon the same amount if they both have one IDP ?
- But what if the size the IDP is vastly different?
- We want to be clear and fair about how we approach our pricing models

- There is much interest in a lump sum pricing model to federate with InCommon, to simplify the accounting process

- InCommon is offering a **scholarship** for the Pilots. MCNC is one of the pilots taking advantage of this. See details at https://spaces.at.internet2.edu/display/InCQuiltFed/InCommon+K12+or+Community+College+Grant+for+Quilt+Pilots

- Mark Johnson: Thanks to the InCommon team for this work on the Federation Partnership Business Models.

Interfederation

presented by Paul Caskey

- Since 2004, the University of Texas System has been running a federation, including publishing a metadata aggregate
- See https://idm.utsystem.edu/utfed/index.html
- Started in policy space with the desire to raise bar for IDM, and this was before InCommon existed
- A lot of the work that the UT system does has now been superseded by the InCommon assurance program.
- http://www.incommon.org/assurance/
- UT system wanted flexibility to include entities in the trust circle without going through InCommon
- For example, UT System could bring in SPs that did not want to join InCommon
- Had visions for Texas government embracing a similar federated approach
- Wanted to be able to include govt , or corporate in the UT System Federation; that has not happened to date

- UT System want to publish metadata when we want to publish (example, Sunday at 4am)
- This is not a closed circle; we interoperate with rest of world through interfederation and InCommon
- The UT System pushes metadata up to InCommon and extracts from the InCommon metadata
- It's seamless and provides flexibility
- For example, the Texas Dept of Transportation has a SAML IDP and they are included in the UT System Metadata
- Currently setting up a federation (using Shibboleth) for Law Enforcement in TX
- For officers submitting accident reports from their car
- They have a federation of Law Enforcement and there is law enforcement on the UT System campuses
- That required crossing federation boundaries
- New features with metadata aggregation will make it even better
- InCommon can figure out the path forward concerning policy decisions
- UT System does not need to write our own policies; happy to be subordinate policy and governance to InCommon
- Federation governance board meets infrequently
- However there is a meeting scheduled to discuss the R&S policy;to automatically release attributes to research and scholarship
- TX has hybrid between models 4 and 5; This is model 4 with the customer metadata aggregate added

- The InCommon TAC interfederation working group meets biweekly
- https://spaces.at.internet2.edu/display/incinterfed/Interfederation+TAC+Subgroup
- All are welcome to participate; Warren Anderson of LIGO is the chair
- Have been focused on International Interfederation
- More difficult legal issues when data must cross the international boundaries
- Looked at eduGAIN, the European Federation of Federations,
- Federations can register metadata with eduGAIN
- John Krienke: InCommon is doing a legal review concerning participating in eduGAIN
- Looking at International law and Contractual law; there are privacy issues
- InCommon both imports and exports metadata
- If InCommon is to participate in eduGAIN, we may have to change the InCommon policies to explicitly state that we will export metadata

- Concerning interfederation within the USA, how high should we set the trust bar?
- The trust community understands and cares about assurance, but others don't care as much
- If the bar is too high then people won't participate and Google will take over
- University of California system took the approach of creating their own policies on top of InCommon

- Should we follow the eduGAIN model in the USA? http://www.geant.net/service/eduGAIN/Pages/home.aspx
- What does domestic interfederation look like?
- Why not have per entity metadata , have a RESTful based service
- Use a query and do it dynamic and real time, like DNS works
- Issue: DNS does not do trust, and trust is needed in this space

- John Krienke: a metadata distribution subcommittee has looked into having a pilot for single entity metadata
- A set of recommendations has been sent to InCommon TAC
- https://spaces.at.internet2.edu/display/InCCollaborate/Metadata+Distribution+WG
- In short term, we will have more metadata aggregates
- There is a campus for which InCommon handles their metaddata
- InCommon performs no registration or validation for the local metadata, and InCommon publishes it only to them

- comment: some community anchors don't fit the educational models
- Museums, libraries, healthcare, that becomes part of the question as far as aggregates
- For a metadata aggregate, it is important to know if everything complies with the same federation policies or not
- For interfederation with eduGAIN, the risk is that we import metadata and we don't know the processes used to get the data in there

- Comment: It is a problem when a Service Provider is in 25 local aggregates but not in the main InCommon aggregate
- Response: I'd like all the vendors to be in InCommon, but there are time constraints
- UT System has some vendors not in InCommon that we federatate with using SAML; some of these vendors don't do much business with HE and don't want to join InCommon
- If you see a vendor in 25 local aggregates, you should talk to that vendor and encourage InCommon membership
- Max at Penn State is a leader in working with Service Providers on the importance of joining InCommon

- Custom aggregate mixed with model #4 (Full Service Steward) is a good topic to discuss moving forward

Applications

slides

Presented by Bernie A'cs from University of Illinois and Jim Petersen from Illini Cloud

- ISLE - Illinois Shared Learninng Environment - has a lot of players and partners
- InBloom https://www.inbloom.org/about-inbloom is doing something important and influential
- They have recognize that data, identity and learning content must be woven together in an effective way
- Using a Data model to describe the educational process and how to implement that with an API
- Says put all this data in this pot and give people the ability to query against that based on their role
- Allows a community of vendors the ability to participate in the education space
- The learning registry is like a metadata registry for learning content
- There's a need for a consistent language
- LRMI - Learning Registry Metadata Initiative
- Virtualized infrastructure is what InBloom wants to do
- InBloom as the custodian of that data -- This is s a political nightmare for the districts
- Parents ask "Where Is my kids' data going?" and these concerns have contributed to a slow uptake
- To handle issue of concerns with putting data in the cloud, Illinois decided to host the data locally
- Need to rebrand, since InBloom is a valuable thing we want to take advantage of
- Create a standardized data model
- The data store is not running on a traditional database
- THE ED-FI model uses an MS SQL server (http://www.ed-fi.org/) which is in every school district today, so can be adopted more easily
- Comment: one of the concerns: a lot of the teachers are already buried in what they already have to do
- Younger teachers can generally deal with this; but older teachers sometimes struggle
- Need to show teachers how to use it and how it can save them time
- Not looking to change the practice in the classroom
- Professional development … the learning map
- This is an enhancement of the tools available to a teacher
- Good applications that provide value

Discussion of partnership business models and Next Steps

Summary of Questions and Issues from the Workshop so far

- Building your way up to model 4 (Full Service Steward)
- What about modified Version 4
- The ability to publish a subset of all your metadata, including from non-education community anchor institutions
- Is InCommon willing to handle non-education metadata?
- Will InCommon publish it, or is a private aggregate that is maintained separately ?
- Pricing issues?
- What about a transaction-based fee when you submit metadata? Not sure how realistic that is. Flat fees may make more sense if they are affordable

Discussion

- Governance: how to include the regionals or other constituents as part of the governance community?
- JohnK: InCommon Steering Committee governs InCommon
- http://www.incommonfederation.org/about.html
- There are 3 year terms, and every year some people complete their terms and others roll on
- In the InCommon Steering charter there is nothing specific about constituencies to be represented
- Every year in the conversation, before Steering solicits who they'd like to recruit as new members, Steering discusses what will be important in the next 3 years
- Such as is there representation from a university with a medical center
    - Public and private, small and large, geographic distribution
- It is up to Steering to be sure it balances out
- Steering is now reviewing the governing documents
- suggestion: InCommon Steering may want a regional representative
- comment: it's often better not to have explicit representation, just you have the right points of view in the room

- Wisconsin: what is appealing about Model 2 (Business Steward Role) is that you can start without being a member of InCommon, and you can grow into it
- KINBER agrees that Model 2 might be a good place to start
- comment: it depends on the expertise of the organization. If an organization does not have an identity person, then it can be easier to start with the business side

- In the next draft of the Models document, it would be good to discuss outsourcing with an affiliate or with InCommon

- As MCNC pilots Model 4 (Full Service Steward), we will know more about using the registration authority, and then MCNC can report back on how it worked
- Ann: the current identity related services that the InCommon affiliates offer is to help with IDM and connecting in with the Federation and with IDP and SP integration
- Its' not necessarily in metadata aggregates, but there is a baby step towards that
- comment: would like a generic metadata engine
- A vettted set of practiced is being developed by REFEDS.org. See https://refeds.terena.org/index.php/REFEDS_Planning_Documents_2013#REF13-4:_Understanding_and_improving_metadata_flow_across_federations

- UT System sometimes needs new metadata within a few minutes
- InCommon metadata is signed every day at 3pm
- InCommon might also look at generating a DIF file that just has the local changes, with the schedule for the DIF flexible to accommodate needs for metadata updates beyond omce per business day

- Shaun: a fair number of regionals are the domain registrars in their state for K12
- Part of the duty of business steward is to match domains to claims
- Given the antiquate nature of DNS management systems, they are not designed to be aware of InCommon; Is there work to bring together DNS management ?
- We need to replace our DNS management system with something newer
- John: there have been discussions about similarities about DNS and Host file
- DNS Management system is important
- [AI] (Shaun Abshere, WiscNet and David Dennis, Merit) look at how to map domain management systems to metadata verification

- InCommon may also want to provide training to the regionals to do the RA function

- How do IPD proxies work on the state level and what if scopes are used instead of IDP?
- Looking for volunteers to continue to work on these federation partnership business models
- [AI] (Jim Stewart) join the work on the federation business model definition effort.

- K12 Schema has come up, It would be good to make progress on eduperson enhancements for K12 federation.
- [AI] (Mark Sheible and Mike Danahy) will work with the MACE-Directories WG on extensions to eduperson. (MarkS will get MikeD involved in the MACE-Directories WG)

- [AI] (Ann) will set up an upcoming time on the All Pilots call to talk about schema (possible extensions to eduPerson for K12 /CC federation). Invite Ketih Hazelton to a call. (UPDATE:Keith will join the All Pilots call on Thurs. Feb 27, 2014 at 4pm ET)

Next Steps

[AI] (Pilot-Def Working Group) reach out to organizations that want to participate in new pilots (KINBER, MOREnet, LONI, WiscNet)

[AI] (Pilot-Def Working Group) look at which regionals, in addition to MCNC, MOREnet, and NJEDge are interesting in working through Model 4 issues.

[AI] (Pilot-Def Working Group -> Federation Partnership Models sub-group) Develop training requirements for regionals interested in Model 4 (Full Service Steward). The aim of the training would be to provide guidance on issues such as RA processes and metadata handling. Note: this action item will be done in conjunction with the Model development and implementation.

Link to Getting Started With Your Pilot: http://bit.ly/1jt2rXd

Action Items

see https://spaces.at.internet2.edu/display/InCQuiltFed/Action+Items+from+2014+Workshop