OSIdM4HE Meeting

January 5

2012

Attendees

- Hampton Sublett
- Chris Mackie
- Bill Thompson
- Bob Morgan
- Bill Yock
- Keith Hazelton
- Dedra Chamberlin
- Tom Barton
- Eric Westfall
- Misagh Moayyed
- Ben Oshrin

Introduction & Agenda

Keith - Understand the market and client environment mostly from a global perspective and not from the institution's POV.

Bill Y – need to recap strategy and organize work to date and make sure everyone's on the same page. Focus is on affordable and comprehensive IAM for institutions. The problem landscape is very well understood by all. The solution at hand is to form a joined venture. Benefits and key differentiations are outlines as well as organizational strategies and roadmaps.

Bob – Question came up about what can user do with this and users can't currently do with what they have? Need to highlight the benefits more and how that affects users in different and beneficial ways. Cloud-enabling may be the way to go here. Comparison should be made with legacy systems and how offerings are made better. Key benefit outlined here is no-binding contracts with vendors and try to avoid the vendor lock-in problem.

Bill – With a limited number of resources, you are forced to spend your resources more wisely. Open-source is not necessarily cheaper, but it does also relate to how upgrades and updates are done and how users are forced to carry out the burden of that in a vendor-lock situation.

Bill Y – In terms of strategies, templates (coordination, MOU and Reference architecture) are currently available out there as well as market diagrams but there are not enough detail to explain what it is and how the investment decision making process is carried out, and that is how this meeting was organized. To get to that level of detail, need to break down the work and proceed with a roadmap. The intent here is not to invent something new, but encourage community and use the same tools to promote. Vision is accepted by everyone, but the sense is the implementation and execution of the plan...and those details need to be well articulated. This also was discussed EduCause, small chunks of contributions are more encouraged.

Hampton – Key questions are, what are the offerings and when are they delivered? Interest may also be in the internal structure of the marketing.

Eric – Interest is out there to get material lead out there and contribute resources, but need the info to do that as well.

Bill – Has there been a pull of interest? What is the client demand and level of impact? What does the other side think about this set of offerings?

Bob – Discussions are made at group sessions to address the oracle problem. Vendor products are still surrounded by homegrown products.

Tom - For those who have bought the vendor product, i.e. oracle, users are helping each other out and they may be an area of interest so each individual doesn't have to carry on support at that level. Ease the individual burden for users.

Chris – Less than 1/3rd of projects deployed were not in open source. If a credible project proposal is delivered, demand will automatically generate. Design of that has a real impact on client demand and interest. Don't know how much demand is out there yet in detail, but we might have to go back to this topic again. We are not trying to finalize answers, but need to think about channels of execution for the overall vision for how to manage, package and distribute it.

Bill Y – Doing a Gap Analysis and requesting feedback from teams; Keith discusses provisioning and Tom addresses Identity Management. Start/End state viewpoints are very important; discuss existing APIs and products, integration options, modular suite of products and standards need to be considered.

Bob – Talking about product strategy is slightly unnerving, in that the product should focus on creating a community around the vision that is going to be sustainable. This is not just about maintenance, and will never have a product that addresses the problem state 100%.

Bill Y – Maybe we need to put some boundaries around what needs to be defined and we could talk about deliverable and steps that are taken to address the vision. The definition of product, compared to commercial vendors is rather loose and may have to focus on what can be delivered within our timelines.

Dedra – Benefit of this proposal is flexibility that we can add features over time. This requires creating an environment at low cost so that changes can happen with community help incrementally. Highlight who the buyer is and understand what matters from their POV. This impacts marketing heavily in that the central value proposition is an ongoing community practice around vision and services, but it always starts off with a product.

Chris - The looseness of a community is not what build s a practice, but the ownership aspect and the space around is super important. For instance, the IAM exists to serve other services and is built around a bunch of other products. On the one extreme, we have the community and practices and on the other, we have the product-driven strategy and design. If the packaging is done in a way that is relevant to big IT institutions, may not be adequate for folks that have limited resources. Smaller schools don't have the human resources to engage at that level.

Keith – The grouper evolution is evolving in a way that tends to address a broader set of audience.

Tom – We don't always just share solutions, but we are able to develop solutions. They build products, in the academic world. A lot of the value looked for, may be called more professional services with people who have the tips and tricks to carry out the service. In terms of addressing the need for CIOs, etc I am not sure we should tackle all that, but just wanted to reflect. We could create something that adapts better for higher ED and is adequate for institutions that have limited resources and the IT staff.

Bill Y – Going over work break downs, chunks are broken down to work streams. For each stream, phases are identified and tasks are outlined. Work Planning estimates excel sheet is available for participants. Each task also identified the estimated level of effort and the resources/skills required for each task, such as Identity Management. Assumptions are also made, and this is where the detail is required to understand the cost within the budget.

Dedra – Try to identify the basic uniform cycle across work streams and the resources/skills needed. This would be the place to generalize the template for each stream. Need to discuss how much detail is actually required so as to not get distracted.

Hampton – Evaluation and Planning seems to be missing. Assessment of different options available for implementation, and this impacts the development phase.

Chris – May have to do a one-to-one mapping of deliverables vs. expectations. A roadmap here comes to play and this is something that SOW and consultants can help.

Bill Y – Assumptions and level of effort can come from teams. Also need to identify a set of people that provide high level support for services and work streams. This includes QA, SCM, etc. Kuali Rice follows a model for this particular need, we could identify the common resources for each of the work steams and then move forward.

Chris – Discussing governance models and vision roadmap. Deadline is set to be March 31st

Dedra – Would like to identify the resources upfront right now, the concern is if we wait until March the same skill set may not be available. Need to set timelines to evaluation different options and can do a formal review of solutions. Need to discuss initial estimate of the requests and the timelines for all expectations.

Bill Y – Next steps, how to communicate the results of the meeting to the team? We currently have 4 work streams, but may need to readjust the concept here again. The idea is not about components or plug-ins, etc but have to organize the set of elements around the objective. Will have a caretaker for each component and work stream.

Hampton – In the Chicago meeting, we had identified 10 gaps and then prioritized action items. This was both based on IT demand and product services out there.

Dedra – May have to create separate work streams as we develop our assumptions about each solution (Registry & Matching). In terms of caretakers, there was no agreed upon role assignment but they should be used broadly across higher ED.

Ben – Leaning more towards separate streams, allows better prototyping, smaller, not a lot of moving parts, and the technical component still needs be done anyway. The current 4 streams are adequate, but a web directory work stream would be relevant to add. Could be made part of the Registry piece but doesn't seem to be a good fit.

Chris – Arrived at an elegant architectural overview, but proliferating projects and caretakers without supporting processes is dangerous. 4 work streams allow for a lightweight governance model. Web directory may not fit with the streams we have, but could be added as an exception as it represents a large class of components. This also needs to be part of the marketing strategy.

Team discusses technical reference architecture diagrams and Next Gen components...

Bill – Looking at the IAM Console, the diagram started to show the use cases and addressed user needs. This is the set of functionality that campuses need: acct management, user management, authentication, etc. The diagram brings out the functionality that outlines the offerings.

Ben – There are other things that are not a good fit for this particular list, but there are additional things like single sign out that could be added and looked at.

Break

Chris – Discussing value proposition, the first question stated here is: who is the customer?

1. Tier 1:
    a. Colleges and universities. (2/4 year lifecycle PSE)
2. Tier 2:
    a. Research organizations,
    b. Collaborative groups
    c. National labs
3. Tier 3:
    a. Campus organizations
    b. Non-profit organizations namely Campus Crusade for Christ. Bamboo could be also there
    c. Other public sector organizations (arts, municipalities, etc which may not be autonomous entities depending on the campus type).
    d. Learned Societies are also interested and attempt to join through InCommon.
    e. Hospitals could also be included.
    f. Governments. (More part of the international landscape)
4. Tier 4:
    a. Resellers and professional service providers.

b. Corporate Philanthropy

Campuses outside US tend to follow decisions made by a central body. Governments can be part of the international sector and may be addressed through public announcements and international partners. (Shibb work for Japan could be one example)

Having a finite amount of effort available, for 2/4 year lifecycle PSE, what kind of subcategories could be out there? 1% of the market has significant resources and IT support for architects and engineers. 99% don't have that to that level of availability and flexibility. From the tech POV, there's tremendous diversity. System Ministries may be included here too.

Tom – CIOs could be considered buyers here. Talking about vertical apps and the possible integration points and the effort required to do so need to be considered.

Hampton – Is there a difference of needs between 2 year and 4 year PSE? Does it change the marketing approach?

Eric – 2 years generally have a much higher turnover.

Chris – Turn over could be student population, and possibly staff in community colleges. Students that radically drop in and out of programs are not much of a case with 4 year institutes. Marketing needs to address needs of such clients. Average community college has 3 IT folks, one for each shift. Resource-starved environments, etc...

Bill Y – Government investment could be a different contribution in terms of funding and long-term scale.

Chris – Election year and with the budget crises, the cultivation process is rather difficult. At a minimum, the 1% institutions are part of our bulls-eye constituency, meaning investment plan and marketing. This related to committed interest. System Ministries could also be part of that focus, **systems that have procurement responsibilities are the focus here.** What about the 99%? There are significantly less resources available, marketing and strategies are different. Total profit in this section is high compared to the money-per-institution in the 1% sector.

Hampton – If we were to get 100 99% institutes, our focus would definitely shift.

Tom – Modest packages geared towards toward the 99% would perform better, given that they cant accommodate the big ask with their resources and budget.

Chris – www.kickstarter.org for instance, allows donations and contributions for new ideas. This is a basic example of how to get a lot out of a little! Now, let's talk about international. Taking Canada as an example, priorities change potentially and the scattered projects should have internationalization and localizations.

Bob – This should be a choice made before writing code.

Keith – This makes governance slightly more difficult, governance being related to the work done and taking contributions from various groups, say, Bristol.

Ben – Privacy issues also come into play, when it comes to various languages. Most of the issues come in Identity/Registry reg. SSO and attribute release, etc.

Tom – Would be a good idea to bring an international partner to help with that.

Chris – It is more beneficial to bring a partner from current affiliates and contributors. Northern University of South Africa could be one. Networking out through Kuali, I2, CFOs and etc could help identify potential support.

How likely is it to receive a substantial investment from the clients/customers listed above?

Dedra – If you have developer resources, you can actually get something done. You can produce/consume at the same time as part of a joint effort. In terms of that %1, this is not just about investment money but actual true partners. The model where you hand over money to developer resources outside, that has not worked so well. We are mostly looking for committed partnership. Some campuses in the target Tier 1 may not have dollars, but they have resources that could donate. Different kinds of investment can be expected from institutes.

More developers vs. More money. Kuali model is discussed and the management aspect of it.

Bill Y – Having strong project management is key across inter-institutional projects and we require models that can accommodate and address flaws in the PM work.

Tom - Bob Brammer industry consultant for I2 – Big in the commercial sector and understands the value proposition.

Chris – Corporate philanthropy could also be included, institutes that may not have budget but they act as consultants and volunteer. Now, to identify the buyers and those who make decisions and may have to be in contact.

CIOs report to CFO (control) and COO (planning budget, making strategic investments) All report to CEO. CISO, Architects and CTOs, DR also report CIO. Registrar Community and VPHR positions could be named here as well. In the long term, what firms are doing is disintermediation. These folks need to know why the things the care about are positively affected by modern IAM.

Dedra – Central service desks would want to make investments to allow for features like password reset, and not necessarily require IAM frameworks.

Tom – What does the package content sent to the CIO look like? The strategist should be identified for contact.

Chris – Who is the sweet spot here to contact for a sale? That would be powerful insight. Separating CIO, DR, Architects and CTI when we talk to these folks, what are they buying? Comprehensive IAM ? It looks like outside this triangle, it’s very hard to get any attraction. To get investment, product-based offering is much easier, however projects at their initial phase with only a diagram of details are very hard to sell.

Tom – Need to convince these folks to understand the real value. Education starts there.

Bob – Joined ventures, identify people who have some appreciation for the project and understanding the offering to a degree or have used/collaborated with the teams.

Dedra – The burden of proof is always on us, as there’s a lot of pressure on institutes to move towards vendor products like Oracle.

Bill Y – From the overall development perspective, the overall vision must be in sync with the timing. Can’t deliver separate components in very different timelines, regardless of the proposition value. For different components of the IAM offering, different people need to be contacted.

Chris – Is there a potential to get some of our CISOs to go to national institutes and participate in the marketing aspect? Different venues such as EduCause and their endorsement at events could be very valuable. The idea is to have a trophy wall of all the supporting sponsors.

Keith – CSG and CIC are possible candidates. I2 and Kuali are organizations that look forward to sponsoring partners.

Chris – Another aspect of community sourcing could be risk management. The notion of doing this together with partners and for these institutions has favorable outcomes on risk management. The trophy wall can be a tool of influence for the CIOs and COOs.

Launch

Bill Y – Breaking down tasks based on the 4 work streams identified in the diagram:

Shared services/tasks

1. Audit reporting
2. UI management console
3. Standards/API
4. Policy Management/lifecycle
5. Training material and events
6. Overall documentation
7. XACML: OASIS eXtensible Access Control Markup Language (No driving need exists for it at this point)
8. Workflow engines
   a. Kuali enterprise engine (no evaluation done yet for a possible wholesome open-source replacement)

Registry tasks

1. Identity Match, **person specific**. Does include reconciliation. Need to seriously consider internationalization as this would be a high effort area. Challenge is how and when to do and use the features (before/after the fact)
2. (Core) Identity SOR, golden record central repository SOR feeds into and back out, and the interfaces in-between. Need to support extensibility (attributing of persons, etc) and will include account management. **People/service specific.**
3. Self Service – User interface for managing person identities, delegated management, assignment and management of IDs, password/credential management (...which could be seen as a parallel task entirely, but may still be part of the IAM console. This is so it can be tailed to standalone installations for people that may not want the entire suite, but just the PM module)
4. Audit Reporting
5. Policy Management – Lifecycle (role changes)
6. Group/Organizational Identity (organizational management, central registry).

Chris – Cross suite integrations may require a separate work stream?

Eric – What about organizational registries and other types? #6 above.

Registry Assumptions & Starting Points

- Identity Match
  - Identity Management is currently unavailable or incomplete. Does not have to be open-source, could be a home-grown product. Solutions like that do save a bit of development time. Currently have an ID match StrawMan to indicate possible solutions that might be a front-runner (link is

    available on the I2 wiki site). NextGame is the name of the company active in the area, Open Registry is another candidate.
    - Data Integration; ETL falls elsewhere.
- Identity Registry
    - Distributed vs. Unified? Invest in one solution
    - Standards/API <=> Reference Implementations, development/resources
- Self Service
    - Integration to other registries/directories; extension points

Keith – The group has traditionally tried to define capabilities and functionality and has attempted to break them apart into separate work streams.

Dedra – What we build should support both functionality; Existing processes are instantaneous in some schools that feed other processes. Other schools require a separate process. Process management needs to be uniform for schools.

A representative group of people may be chosen to evaluate possible options available for Identity Registry (Open Registry, COmanage Registry (includes UI), KIM, Penn State Registry, etc). Are there any other schools we know that would want to invest in registry solutions and help with evaluations, documentation of pros/cons and recommend options? It does seem to be too soon to identify the strategy at this point, because we don't know a lot about individual solutions. We need committed people to do the homework and background work and that's the level of detail desired at this point.

Ben – There is a lot of overlap between options, however, looking at business assumptions is where they are mostly differentiated. In a rough look, open registry seems to have been designed for a distribute model whereas Penn state uses the unified approach.

Chris – At the end, one option needs to act as the reference implementation, some development work may be required.

Tom – As for the smallest first step, can we pick one solution at this point and evaluate features?

Bill Y – Lets all agree that the end state is one unified/core product experience, and based on that we could evolve to existing solutions that are out there, for institutes that require and have a need. Joined ventures can be utilized. **The solution we eventually might work on would have to clarify API, standards, reference implementation and documentation.** This removes the possible chance of duplicate effort.

Hampton – From a timeline perspective, whichever one is picked, that is up to the Registry team between now and March?

Ben – For the purposes of joined ventures, it'd be better to take a look at standards in general and not pick one solution. We don't have to say we have picked Product X, but make more generic statements that for instance, discuss building a Registry option just in terms of funding.

Chris – Might even be better to take this from a worst-case approach. Endorsements really focus on standards.

Tom – Are we asking for funding to pull all solutions along? That'd be the wrong approach. Reference implementation to standards is an iterative process and goes to a long process. Initially, there may not be a full complete set of API and it's something projects work toward. So, that does not necessarily exclude other projects since that is not going to get done in step 1.

Eric – KIM in terms of registry solution probably has the largest install base. If we're looking at funding the development of standards and API for these solutions and putting resources in charge, then solutions can be phases out. The challenge with KIM is that it was not designed to be a registry solution initially, but later evolved into one.

Ben – Something we could start very quickly, work on these standards can be a joined effort across all solutions. That is something we can get started with today. This could be useful a precursor to indicate where the final investment should go.

Dedra – Consensus is to evaluate options, but invest in only one and meanwhile, we will build our knowledge base and improve our understanding of how each solution works out.

Bill Y – 3 basic efforts: evaluation of the existing codebase **(current interface, what kind of work needs to be done, compare and state motivations)**, standards/API reference implementation that needs to happen to ensure viable continuation of the effort and of course, there needs to be development with resources to start writing the blocks moving forward.

Bill – Does Self Service refer to admin type of capabilities that employs registry features or does it only come from the user's POV? **Self Service is a broader UI component that is an add-on to the Core Identity SOR.** The UI provides management capabilities and uses registry features to the admin folks.

Provisioning tasks

1. Identity information schemas
    a. Schemas and Mapping: include mappings to/from canonical data models such as LDAP and RDBMS.
    b. To/From – ETL: policies are built based on such rules
2. Connectors: requires building of additional connectors for use and download. Much of this work has already been done, solutions need to be identified and evaluated for institutions.
    a. Provisioning is keeping the state of identity consistent across institutions, so that changes are propagates throughout all involved parties.
    b. Connectors are components that cascade the information down the line and act as the means to get info out of the system and influence other systems. Deliver as a set of design patterns, identify common provisioning tasks and connect to other systems such as PeopleSoft, SAP, ActiveDirectory, LMS, etc.
    c. Standards around service endpoints?
3. Recommended solutions
    a. Rule engine (policies) required to execute the mapping
    b. RESTful service as an enterprise integration pattern
4. Reference implementations and lifecycle models: ServiceMix, Kuali RICE

Chris – Would really want to deliver this piece as a set of design patterns, but with a reference implementation. Realistically, we are going to get investment from folks that end up using actual implementations of the pattern.

Keith – Recommended reference implementations could be Kuali RICE and Apache ServiceMix. In Kuali RICE, we are specifically talking about the workflow, the rule engine and the service bus. (We can't really implement to all possible environments) ServiceMix includes messaging, BPEL, rules using a number of other apache projects (Camcel, ODE, Karaf, etc)

Chris – The task breakdown as it's currently brown can really be executed with a rather small resource pool which does impact marketing and sales in a positive way. Can we save time/effort by using these tools/frameworks to delivery first deliverables?

Tom – Looking at commercial solutions to address identity provisioning needs, we should also address not only connectors but elements that get connected. Need to support lifecycle implementations, with the corresponding support for the standards; requirements that deliver service endpoints for connectors.

Access Management tasks

1. Standards/API and the effort required to maintain and integrate with solutions.
    a. KIM/Grouper and integration effort
    b. Grouper may require additional iterations on roles/permissions and the new UI stuff.
2. Access Certification
    a. Request, Review and Approval application (Currently no app exists, only the core functionality)
    b. Audit capabilities
3. Improved UI
    a. Grouper 2.0 will have a better UI, for users managing access
    b. Kuali RICE? may already be working on this functionality to a certain extent
4. Platform integration clients for Spring Security, PHP, .NET, Apache Shiro

Tom – Grouper is a tool for access management for groups, delegation and name management as well as roles and permissions. There is a provisioning component to the toolkit that is currently being taken out of the code base and released independently. Additionally, it has tools to pull pieces out of different systems, and there are about 10-11 components at this point where most deployments use a smaller subset. Current client exists for Atlassian, Oracle security, a partially complete one for uPortal, etc.

Dedra – Development work includes looking at workflow tools, building proof of concepts and sharing them with the community.

Eric – Not a lot of development effort is done yet on Standards/API. This requires substantial work to align with implementations. This isn't something new, but it's not all that usual either. This will be the task of ongoing management of standards and keeping up with their evolution. Additionally, workflow process generally depends on identity management.

Bill – In-house applications that want to make use of the Grouper API, support for various clients/plugin/connectors for various languages, Apache Shiro, Spring Security, PHP/.NET connectors? Require additional integration effort to map with Grouper.

Bill Y – What kind of assumptions can we make about workflow engines? Kuali RICE's engine a possible candidate? Need to evaluate possible UI options with workflows and how good they are.

Keith – This is also a question of tool used to build the UI + development environment and community (Spring Webflow, for instance). Lots of folks are out there with ideas to draw on and this builds again back to the joined venture with added marketing value. If accomplishments can be marketed more in light of coordination between parties, it would greatly help marketing factors.

In terms of development environments, however, we don't currently have all of the requirements to continue with the conversation. Question is, should we have to have the same dev environment for all components?

Chris – There are obvious advantages to that approach, however, in terms of funding, realistically that is not possible. The general pattern with Kuali is based on J2EE, Eclipse, jQuery and Spring Framework but not an all-inclusive IDE. Need to identify perhaps a common development environment toolkit?

Hampton – Would be more beneficial to identify needs in apps, like Bamboo, first in order to ask for funding from the parent organization. However, projects like Bamboo are not yet mature enough to provide endorsements.

Chris – For tomorrow, outlining volunteers for major work streams, we are trying to get people with the most interest in each of buckets. **Keith/Tom is formally responsible for provisioning. Bob is responsible for Authentication. Dedra is responsible for registry and Tom/Eric is responsible for access management. Bill is responsible for Shared Services. First category is "Gimme"s, stuff that we are going to get without any additional effort. Other bins are timelines that identify things that are realistically deliverable within 6-8-12-18-24 months**

Authentication tasks

1. Current solutions include CAS, Kerberos, Shibb, LDAP/SAML
2. Password management is something totally homegrown right now, includes password reset, policy and strength checking.
   a. **CASPM is an existing solution for password management contributed by Unicon.**
   b. The only campus using a password management module is Chicago
   c. **<u>Doable within a 2 year roadmap</u>**
3. Risk based authentication, verification and monitoring (CAPTCHA, etc); relies on tools that are not part of the IAM space.
4. Strong 2-factor authentication
   a. Focus on client certification, PKI
   b. Shibb-SMS based integration?
   c. InCommon Toolkit?
   d. **<u>Doable within a 2 year roadmap</u>**
5. EduRoam / RADIUS
   a. Could be considered a "Gimme". **<u>Doable within a 2 year roadmap</u>**
   b. Federated identity is done using RADIUS
   c. The eduroam initiative started in 2003 within TERENA's Task Force on Mobility, TF-Mobility. The task force created a test bed to demonstrate the feasibility of combining a RADIUS-based infrastructure with 802.1X standard technology to provide roaming network access across research and education networks. The initial test was conducted among five institutions located in the Netherlands, Finland, Portugal, Croatia and the UK. Later, other national research and education networking organizations in Europe embraced the idea and gradually started joining the infrastructure, which was then named eduroam.
   d. Passwords often need to be synced within different systems.
6. Non-web federated authentication
   a. Maybe already solved?
7. Social Identity & authentication
   a. Need to consider high-risk patterns for authentication; using school accounts to authenticate against other systems.
8. OAuth
   a. OAuth (Open Authorization) is an open standard for authorization. It allows users to share their private resources (e.g., photos, videos, contact lists) stored on one site with another site without having to hand out their credentials, typically username and password.

b. Provisioning implications to consider. Cloud and mobile-device auth?
c. Exploration work and research?

Chris – Is there a reference implementation work for any of the solutions? Federated capabilities are pretty much covered by Shibb. Do we also, have a sense for better homegrown technologies in this space? Considering all discussions, within a 2 year time period, what can realistically be delivered?

One think to keep in mind about the blueprint, is not the solution itself per se. The deliverables should be used to evaluate if there's any attraction when CISO/CIOs are contacted and that is the determining factor on what actually goes on the deliverables list.

Tom – Social identity is where users are allowed access to resources without an account with the system, but an external identity like a Facebook, Twitter and Gmail account.