IAM Committee
Meeting Notes
5/11/2015

Attendees: Greg Baker, Mark Barber, Cam Beasley, CW Belcher, Michael Bos, David Burns, John Chambers, Cesar de la Garza, Fred Gilmore, Alison Lee, Ty Lehman, Darin Mattke, Steve Rung, Charles Soto, Raul Villa

Absent: Ed Horowitz, Roy Ruiz, Kim Taylor

IAM Team Members: Josh Kinney, Marta Lang, Aaron Reiser, Autumn Shields, Dustin Slater

1. **Lightweight Authentication & BYOId – Update**

The project team has conducted a series of requirements-gathering workshops with the customer steering committee, as well as workshop open to campus. In the last CSC meeting, the team walked through the first draft of the project requirements and made some changes based on committee feedback. The CSC is currently reviewing the document, a copy has been sent out to the IAM Committee, and feedback is requested by Friday, May 15th.

Once the requirements have been approved, the team will begin reviewing solutions for BYOId and the local lightweight account component. The team will then review identity providers, develop guidelines for the appropriate use of lightweight authentication, and then work on a roadmap for guest EIDs.

Q: Have any recent events affected the project timeline?
A: No. The goal is to have the first project phase completed by the beginning of September. From there, the team can accurately baseline the actual development and release. The project is still on target.

Q: Have there been any surprises or issues?
A: The CSC has been weighing the relative benefits of limiting lightweight authentication to only the information needed for authentication as opposed to the creation of a minimal data store. There is also ongoing discussion regarding the potential campus customers, which of those customers might be early adopters of the service, and how to prioritize features and functions accordingly.

Q: Who is on the CSC?
A: The member list for the CSC is available at
http://www.utexas.edu/its/lightauthproj/governance/index.php .

Q: Would it be necessary to include representation from the research areas?
A: The research areas don't have use cases for lightweight authentication since the work requires that we have a high degree of confidence regarding their identities. As such, that becomes an issue of federated identities, not lightweight authentication.

2. **SailPoint Implementation Statement of Work – Update**

Work is still ongoing on the statement of work and additional resources have been leveraged to help complete it. The expected release date of the SOW is mid-June, 2015. The team would like to solicit the IAM Committee for volunteers to help review the SOW as well as participate in selection the vendor once responses have been received.

Q: What is the timeframe expected for volunteers?
A: The team would like volunteers to review the SOW over the next 2-4 weeks prior to release. After the release of the SOW, vendors will have 6-8 weeks to reply. Once those replies are received, a few weeks of engagement will be necessary to review responses and then participate in vendor presentations, ultimately in late July or early August.

Q: Is this a formal RFP?
A: Our intention is to procure these services through the Texas Department of Information Resources Deliverable-Based IT Services (DBITS) process.

Volunteers: Greg Baker (schedule permitting), Cam Beasley, CW Belcher, Ty Lehman, and Charles Soto.

3. **Two-Factor Authentication Initiatives – Update**

There is an overarching project to coordinate the UT Austin approach to meeting the requirements of the UT System mandate for two factor authentication. The project charter has been reviewed by the executive sponsors and will be sent out to the IAM Committee for further review once feedback has been incorporated. The IAM Committee will provide oversight for this project.

The goal of the initiative is to make available central solutions for two factor authentication to mitigate the need for departments to have to implement their own systems. Those efforts include incorporating two factor authentication capabilities in UTLogin and in Shibboleth. Some work including a proof of concept has already been completed.

Q: How would a system administrator or application developer enable two-factor on UTLogin?
A: During the first phase, the customer will need to contact the UTLogin stewards directly who will assist customers through the process.

Q: Does UTLogin support the option to only request two factor authentication if the user is connecting to a system from off campus?
A: The team does not currently believe that this feature is available, but they expect that it may be available in a future release of OpenAM.

It is important to note that the web applications for which two-factor authentication is mandated have already been addressed. Efforts on the part of ITS Networking will ensure that two-factor authentication is available via VPN prior to the mandated due date. System administrators who need two-factor authentication to connect to their systems can use VPN to remain in compliance with the mandate.

Some work is still needed regarding UNIX PAM modules and creating proofs of concept for server administrators who wish to incorporate two-factor authentication directly into their servers, however the we expect most systems administrators will use the VPN for off-campus access.

The team is also working to implement more robust two-factor support in Workday.

Lastly, work on hard token functionality is ongoing, but has been delayed as resources are deployed to meet UT System mandate requirements. The demand for hard tokens on campus is limited, but has been vocal.

Q: Has the team met yet with Salesforce (regarding their recent acquisition of Toopher)?
A: Yes, conversations have been held between Salesforce and the university. Some changes to the existing contract not involving functionality or scope may need to be made. Additionally, the university can expect some rebranding of the product as well as more support for features and functionality owing to the additional resources that Salesforce will be able to provide.

4. **Other Initiative Updates**
    a. **CARE Project**

Stakeholder meetings to gather requirements and considerations have been completed. A meeting on May 27th has been scheduled with the CSC to discuss and review those requirements. The requirements will be sent for review once they have been approved.

Q: Have there been any issues?
A: The current challenge is that there are many different opinions about how to achieve the project goals. These options have a variety of dependencies, costs, and the speed at which systems can return to operation. Additionally, considerations need to be made regarding global load balancing, which ITS Systems is projecting to have available in spring 2016.

Q: What's the next project milestone?
A: Project requirements are expected to be finalized in early June.

    b. **TADS / ASMP IAM Reviews**

An IAM questionnaire has been created for use with the purchase of new vendor products. Vendors are asked questions about authorization, identity provisioning, and other areas of concern so that the IAM Team can review their responses and work with the vendor and procurer to address problems, security issues, and other considerations.

The IAM team is currently working with the TADS initiative on new technical architecture components as well as Student Administration on the student portal. The Team is also working with Rich Janes in ASMP 2.0 to determine how many vendor applications are expected to be purchased as part of the Application Modernization component of ASMP 2.0. If any areas represented by the IAM Committee are considering purchasing vendor products, they are encouraged to contact the IAM Team.

Q: When looking at vendor products, are there particular questions we can ask?
A: Ideally before procurement, you can send the vendor the IAM questionnaire. This questionnaire includes all of the questions that the IAM Team would ask. This questionnaire is attached.