IAM Committee
Meeting Notes
5/9/2016

Attending: Thomas Beard, CW Belcher, Michael Bos, Bill Bova, John Chambers, Graham Chapman, Cesar de la Garza, Tim Fackler, Fred Gilmore, Ty Lehman, Darin Mattke, Steve Rung, Charles Soto, Karen Weisbrodt

Absent: Cam Beasley, Alison Lee, Andy Loomis, Shelley Powers

IAM: Rosa Harris, Justin Hill, Josh Kinney, Marta Lang, Mario Leal, Aaron Reiser

1. IAM Identifier Support Recommendation – Endorse (CW Belcher)

Reference handout.

Following up on this item from last week, the updated recommendation incorporates feedback from the committee. There was a question raised about the need to be able to map retired identifiers to EIDs on historical records kept for records retention purposes. This issue can probably be addressed by maintaining an identifier crosswalk for reference purposes. Future planning for identifier retirement will provide a resolution for this potential issue.

A concern has been raised on campus that the University Issue Number (UIN) would go away when Workday goes live, but this is not the case. While it is true that Workday will not store UINs, the UINs will continue to be generated and maintained at least through retirement of the mainframe environment. The IAM team will be working with the Administrative Systems Modernization Program (ASMP 2.0) team on communication on the topic of UINs.

Q: What options will be available to assist with the reconciliation of multiple identifiers belonging to a single identity?
A: The team recognizes that more work needs to be done in the realm of identity matching, but that is not a blocker to this particular recommendation. We will reassess how identity matching is performed as part of the implementation of Lightweight Authentication and the replacement of the TIM system.

Decision: The committee voted to endorse the recommendation.

2. IAM Modernization Program / SailPoint Implementation – Update (Marta Lang)

Reference handout.

The team is working on a set of investigation tasks that need to be completed as part of the Technical Architecture Design Blueprint. The team is also creating phased system and data diagrams for the Interface and Data Transition Strategy. The project is currently under budget with regard to hours worked.

Q: Is the project under budget due to resource constraints?
A: The original hour estimates were conservative and created using a top-down approach. Once the Phase 1 design deliverables are complete, the project will be re-baselined with the project team to develop better estimates for later activities.

As the team begins work on the design deliverables they are finding that more information gathering, analysis, and investigation is needed. This is resulting in some delays but getting these deliverables correct is critical to the success of the project.

The team will be bringing in experts from SailPoint professional services to provide an additional level of review on our requirements and designs for the system to ensure that they are consistent with best practices for SailPoint implementations.

Q: Within the context of other project roadmaps, dependencies on role management functionality in IAMMP have been identified. Are there any concerns there?
A: The IAMMP project team will begin creating role management use cases and engaging customers in June. Once that work is complete, the team will have a better idea of the customer base and which use cases should be prioritized for early adopter implementation.

Q: Have those customers been identified yet?
A: The early adopter customers have not been identified yet. However, through other work the IAM team is doing, such as discussing the roadmap for Apollo and Organizational Hierarchy System Contacts (OHSC) retirements with campus units, the team has already started gathering information that will help identify early adopter customers.

Q: Could you provide more information on the deployment playbooks? How detailed are they expected to be?
A: The Deployment Plan deliverable will be high level, whereas the Deployment Playbook deliverables will provide specific, itemized task lists for particular deployments of major system functionality.

3. Other Initiative Updates

a. IAM Team Staffing (Mario Leal)

The IAM Team currently has five open positions. A number of phone screens have been conducted, but unfortunately these have not been translating into many in-person interviews. The team has also maintained a presence at recruiting events, but that has also not yet translated into desirable candidates.

Q: In previous meetings there was talk of using an external recruiter. What came of that effort?
A: The use of an external recruiter has been put on hold due to budget issues, but is being included in the budget for the next fiscal year.

In addition to other efforts, the team will also be making adjustments to working titles to help attract better candidate matches.

b. IAM Integrations (Mario Leal)

Processing of IAM integration requests has been made more efficient with a revamped process and the addition of an extra project manager and extra software engineer helping with integrations. There are 21 outstanding requests: 17 in the backlog, 3 in progress, and 1 awaiting verification from the customer. The team looks forward to being able to further refine the process once ServiceNow is available.

c. Two-Factor Authentication / Duo Implementation (Justin Hill)

5000 users are currently registered with Duo out of 6500 potential VPN users, so customer adoption is proceeding well. Efforts are currently underway to integrate Duo with UTLogin and Shibboleth. The team ran into some technical roadblocks and have split the UTLogin release into two releases: Duo support via UTLogin WPA will be implemented in the first release, followed by Duo support via UTLogin SAML integrations.

The team will begin assisting Financial Information Systems (FIS) and Payroll Services in transitioning from Toopher to Duo this month.

Q: Could you go into more detail about the upcoming UTLogin release on May 15th?
A: This release includes Duo integration for UTLogin WPAs and changes to the logout flow, which was discussed by this group previously.

d. Directory Services Roadmap (Josh Kinney)

The directory services customer survey was completely recently with approximately 120 individual responses. Those responses are being incorporated into new use cases for directory services, centered on expanding support for added system integrations and adding user attributes not currently reflected in TED. The team will also be working with the Active Directory (AD) team to bring directory services and AD more closely in alignment with respect to the attributes available in each. This effort will be aided by SailPoint. The team is also experimenting with the different technical options available which will form that basis of directory services in the future.

Q: Our group has noticed issues whereby certain AD attributes aren't populated until a user claims an Exchange mailbox. Will this closer alignment address that issue?
A: In their current state, the uTexas Enterprise Directory (TED) and AD operate on different business rules regarding which attributes are written into each system, so the team is looking to unify those rules to ensure that the records align more closely. The team will work with the AD team to ensure that their specific needs are met.

e. Lightweight Authentication (Rosa Harris)

Six vendor responses were received to the Lightweight Authentication RFP. The evaluation team has narrowed the field to two vendors based on those responses. The first on-site presentation will take place this Thursday and the second presentation will take place on Tuesday of next week. The Customer Steering Committee and subject matter experts have been invited to these presentations.

f. Authorization Roadmap (Marta Lang)

Now that interviews with Apollo customers have been completed, the team has identified OHSC and DPUSER customers and will begin engaging with those customers.

Q: During the interviews, there was talk about building a utility to ease migration, but recently there has been word that the migration might need to be performed manually. What is the status of that effort?
A: There will be a new resource joining the project in the next few weeks who will be charged with working on a migration utility. More information will be shared as soon as it is available.

The University of Texas at Austin
Information Technology Services

IAM USER IDENTIFIER SUPPORT RECOMMENDATION

BACKGROUND

Originally, the EID System had two identifiers:

- Preferred EID – A user-facing identifier that was generally used by the EID holder to authenticate. Many business processes at the time used Social Security Number (SSN) or some other identifier for users – the EID System held a crosswalk between EIDs and SSNs.
- Permanent EID – A system identifier that was generally not known by the user. Preferred EIDs were user-selectable and user-changeable while Permanent EIDs were system-assigned and non-changeable. University Issue Numbers (UINs) were also associated with EIDs and functioned in much the same way as Permanent EIDs (system-assigned and non-changeable).

In 2002, the SSN Oversight Committee recommended that SSNs be replaced by the Preferred EID (renamed “UT EID”) as the primary means of identifying individuals, that UT EIDs be generated and only changeable through an administrative process, that Permanent EIDs be phased out, and that UINs be used as the identity key on system database files/tables.

The change to generated UT EIDs was implemented in the fall of 2002. The large-scale replacement of SSN with UT EID (or UIN) in campus systems occurred from roughly 2005 to 2007. Permanent EIDs were deprecated in 2006 but have continued to be generated and supported to maintain backward compatibility.

REASSESSING IDENTIFIERS

With the upcoming replacement of the core identity administration system (moving from uTexas Identity Manager – TIM to SailPoint IdentityIQ) and the modernization of administrative systems across campus, it is a good time to reassess the centrally maintained user identifiers and determine which should be recommended for use moving forward and which should be retired (and when).

One driver for the SSN Oversight Committee’s recommendation that UIN be used as the identity key within systems was that it anticipated that the UIN would be “immutable” and would be more stable than the UT EID. However, in practice the number of EID changes is very low compared to EID merges (20 EID changes occurred in 2015, compared to more than 16,000 merges). As a result, UIN is effectively no more stable than UT EID since an EID merge will often cause the UIN for a person to appear to change, requiring systems to update the UIN on their files/tables.

In addition, the recommendation to use UIN as a system identity key assumed that most systems would have ready access to and be able to use a UIN-to-EID crosswalk. However, this is not the case with many vendor package systems and most cloud-based applications (these systems generally use only UT EID as a user identifier).

Although Permanent EID was deprecated in 2006, it continues to be maintained to provide backwards compatibility for systems in the traditional administrative computing environment.

RECOMMENDATION

With the ultimate goal of reducing the number of user identifiers that must be supported in the long-term, the IAM team proposes the following:

- UT EID (and identifiers directly derived from UT EID: eduPersonPrincipalName and Institutional Identifier) will be the recommended user account identifier for campus systems, whether on-premise or remotely hosted.
- UIN will be deprecated but will continue to be generated and supported until the mainframe is retired. A UIN-to-EID mapping can be maintained for reference purposes beyond that date.
- Permanent EID will be retired from TED effective 8/31/2016 (an extension will be available for systems that still need access to Perm EID in TED beyond that date, as long as they have a plan for retiring their use of Perm EID). Permanent EID will continue to be available within the mainframe environment until the mainframe is retired.
- DPUSER Logon IDs will be retired when the mainframe is retired.
- UT ID Card number (ISO number) and Badge ID number will continue to be supported as-is.

USER IDENTIFIER OVERVIEW

Identifier	Description	Support Recommendation
UT EID-based Identifiers		
UT EID	2- to 8-character public user name. Designated as directory information for FERPA purposes.	Continue to support UT EID.
eduPersonPrincipalName (ePPN)	UT EID scoped to the utexas.edu domain (<eid>@utexas.edu). ePPN is defined in the eduPerson specification and is NOT an email address. Used by many remotely hosted systems.	Continue to support ePPN.
Institutional Identifier (IID)	UT EID in the form of an email address (<eid>@eid.utexas.edu). IID email routing is only available for person EIDs that are Member or Affiliate class, or Guest class with a specific entitlement. Used by remotely hosted systems that require the user account be in the form of an email address.	Continue to support IID.
Other EID-related Identifiers		
University Issue Number (UIN)	16-digit hexadecimal number that is attached to an EID identity record. UINs are commonly used within internal campus systems as the user identifier. Not generally used in external systems. UIN is designated as confidential data.	Deprecate the use of UIN but continue to generate and support UIN until the mainframe is retired.
Permanent EID (Perm EID)	Alphanumeric identifier attached to an EID identity record. Perm EID was deprecated in 2006 but is still maintained to support legacy systems.	Remove Perm EID from TED effective 8/31/2016 (with an extension possible for specific systems that need more time to transition). Continue to support Perm EID on the mainframe until the mainframe is retired.
UT ID Card Identifiers		
UT ID Card number (ISO number)	16-digit number printed on the UT ID card and encoded in the bar code and magnetic stripe on the card. Typically used in face-to-face transactions (e.g., Rec Sports sign-in, library check-out). Also used for Bevo Bucks and in other DHFS functions. ISO number is linked to EID identity by the ID Card System.	Continue to support ISO number.
Badge ID number	Proximity card identifier for use with BACS (Building Access Control System). Physically encoded within the UT ID card. Badge ID number is linked to EID identity by the ID Card System.	Continue to support Badge ID.
Mainframe Identifiers		
DPUSER Logon ID	Identifier used as the user name within the mainframe environment. DPUSER Logon ID is linked to EID-based identity by DPUSER.	Retire DPUSER Logon ID when the mainframe is retired.

Identity and Access Management Modernization Program (IAMMP)
Phase 1 Status

Monday, May 9, 2016

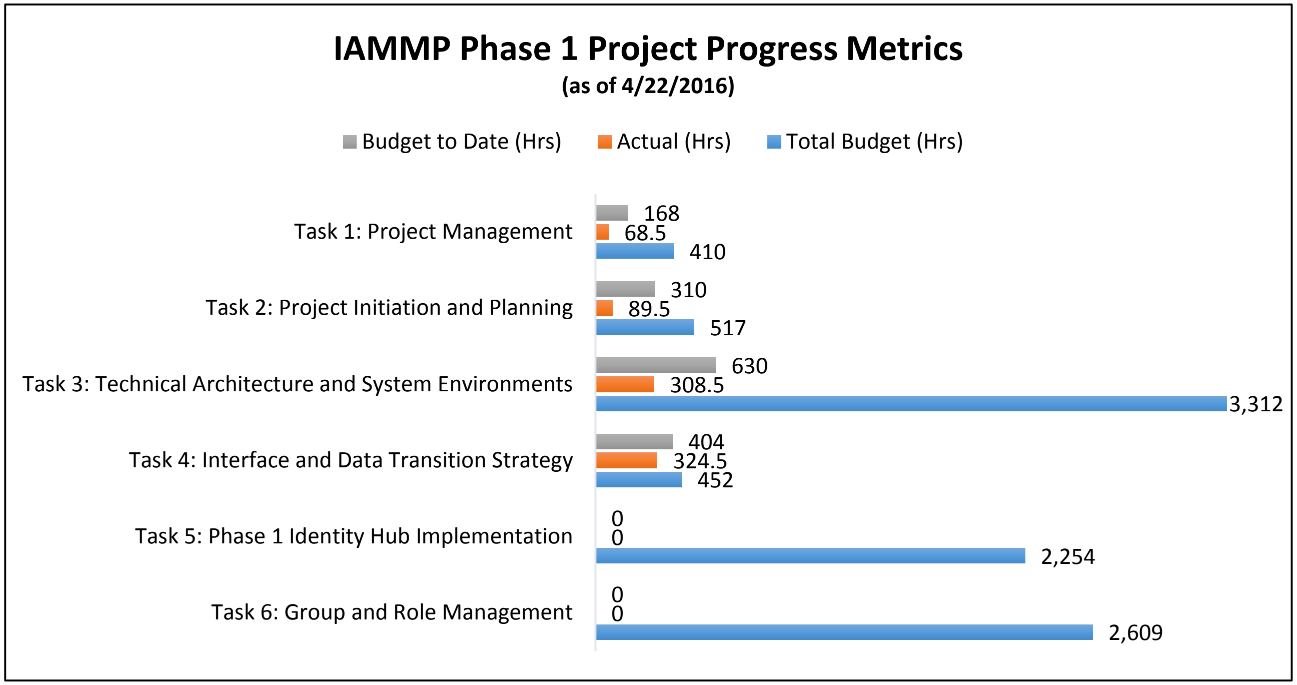
Program Overview

The Identity and Access Management Modernization Program (IAMMP) will guide a set of projects related to the implementation of SailPoint. The goal of IAMMP is to modernize the University's IAM systems, business processes, data management, and technical architecture, as envisioned in the IAM Roadmap.

Executive Summary

The following four tasks are in progress:

- Task 1: Project Management – Risks and issues continue to be documented. The Communication Plan will be drafted to reflect the Interface and Data Transition Strategy.
- Task 2: Project Initiation and Planning – The Deployment and Training Plans are under development as Task 3 and Task 4 progress.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Strategy and Requirements deliverables are under review for approval. Investigation tasks for the Technical Architecture Design Blueprint draft are underway. These tasks are necessary to write a detailed design document.
- Task 4: Interface and Data Transition Strategy – The Interface and Data Transition Requirements deliverable is under review for approval. The team is creating phased system and data driven diagrams to compose the Interface and Data Transition Strategy.


IAMMP Phase 1 Project Progress Metrics
(as of 4/22/2016)

Deliverable Status					
Project Task Area	Deliverable	Deliverable Name	Status	Planned Finish	Actual Finish
Task 1: Project Management	D1.1	Project Work Plan	Complete	3/21/2016	3/14/2016
	D1.2.1	Q1 Quarterly Status Report	Complete	4/25/2016	4/29/2016
	D1.2.2	Q2 Quarterly Status Report		7/25/2016	
	D1.2.3	Q3 Quarterly Status Report		10/24/2016	
	D1.2.4	Q4 Quarterly Status Report		1/30/2017	
	D1.3	Risk and Issue Register	Complete	3/21/2016	3/17/2016
	D1.4	Change Control Process	Complete	4/4/2016	4/11/2016
	D1.5	Communication Plan		7/18/2016	
Task 2: Project Initiation and Planning	D2.1	Application Development and Configuration Standards	Complete	4/18/2016	4/8/2016
	D2.2	Project Kick-off Meeting	Complete	2/29/2016	2/29/2016
	D2.3	Comprehensive Test Plan	In Progress	6/6/2016	
	D2.4	Deployment Plan	Behind	4/25/2016	EC: 5/16/2016
	D2.5	Training Plan	In Progress	5/23/2016	EC: 5/23/2016
Task 3:Technical Architecture and System Environments	D3.1	Technical Architecture Approach	Behind	5/2/2016	EC: 5/16/2016
	D3.2	Prototype Environment(s)	Complete	5/2/2016	4/18/2016
	D3.3	Technical Architecture Requirements	Behind	5/16/2016	EC: 5/27/2016
	D3.4	Technical Architecture Design Blueprint	In Progress	6/20/2016	EC: 6/20/2016
	D3.5	Technical Architecture Build		8/8/2016	
	D3.6	Technical Architecture Testing		8/22/2016	
	D3.7	Technical Architecture Training		8/29/2016	
	D3.8	Technical Architecture Deployment Playbook		8/22/2016	
	D3.9	Technical Architecture Deployment		9/12/2016	
	D3.10	Technical Architecture Operations and Maintenance Plan		9/26/2016	
Task 4: Interface and Data Transition Strategy	D4.1	Interface and Data Transition Strategy Requirements	Behind	5/9/2016	EC: 5/23/2016
	D4.2	Interface and Data Transition Strategy	Behind	5/23/2016	EC: 6/27/2016
Task 5: Phase 1 Identity Hub Implementation	D5.1	Phase 1 Identity Hub Design Blueprint		8/1/2016	
	D5.2	Phase 1 Identity Hub Build		9/6/2016	
	D5.3	Phase 1 Identity Hub Test		10/24/2016	
	D5.4	Phase 1 Identity Hub Training		10/31/2016	
	D5.5	Phase 1 Identity Hub Deployment Playbook		10/10/2016	
	D5.6	Phase 1 Identity Hub Deployment		10/31/2016	
	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		11/14/2016	
Task 6: Group and Role Management	D6.1	Group and Role Management Use Cases		8/22/2016	
	D6.2	Group and Role Management Requirements		9/6/2016	
	D6.3	Group and Role Management Design Blueprint		9/26/2016	
	D6.4	Group and Role Management Adoption Plan		11/7/2016	
	D6.5	Group and Role Management Build		10/24/2016	
	D6.6	Group and Role Management Testing		11/21/2016	
	D6.7	Group and Role Management Training		12/12/2016	
	D6.8	Group and Role Management Deployment Playbook		10/24/2016	
	D6.9	Group and Role Management Deployment		12/12/2016	
	D6.10	Group and Role Management Operations and Maintenance Plan		12/19/2016	