IAM Committee
Meeting Notes
4/11/2016

Attending: Thomas Beard, Cam Beasley, CW Belcher, Michael Bos, Bill Bova, John Chambers, Graham Chapman, Tim Fackler, Cesar de la Garza, Fred Gilmore, Alison Lee, Ty Lehman, Andy Loomis, Darin Mattke, Shelley Powers

Absent: Steve Rung, Charles Soto, Karen Weisbrodt

IAM: Pranaya Desireddy, Joel Guajardo, Rosa Harris, Justin Hill, Marta Lang, Mario Leal, Aaron Reiser

1. **IAM Identifier Support Recommendation – Discuss (CW Belcher)**

Reference handout.

There have been questions posed from the campus technical community about whether UINs are still the recommended identifier that should be used within systems (as opposed to the UT EID). To address these questions, the IAM Team is proposing that the support level for the centrally managed user identifiers (UT EID, UIN, Perm EID) be formally specified.

The distributed handout provides background information about the origins of UT EIDs and how UIN was envisioned to function and how those assumptions have not been realized in practice.

The proposal before the committee is that the UT EID (and the identifiers directly derived from UT EID, eduPersonPrincipalName and the Institutional Identifier) should be the recommended user identifier for both user-facing activities and internally within systems going forward. Second, the team proposes that the UIN be deprecated, but that support for the UIN should continue until the mainframe is retired. Third, the team proposes that the Permanent EID, which has been deprecated since 2006, be removed as an attribute from the uTexas Enterprise Directory (TED) effective 8/31/2016. Time-limited exceptions can be made for systems that continue to need access to Permanent EID in TED beyond that date as long as they have a plan for retiring their use of Permanent EID. The Permanent EID would continue to be maintained and supported on the mainframe until the mainframe is retired.

Q: With the mention of the Institutional Identifier, has any progress been made on requiring that members of the university community provide an email address as part of their records?
A: The Architecture and Infrastructure Committee (AIC) has been looking into this request and is the appropriate group to discuss university email policies. As an aside, the Information Security Office (ISO) has, through their initiative of certifying acknowledgement of the Acceptable Use Policy (AUP), reduced the number of staff members with active EIDs who do not have an email address on file.

2. **Identity Assurance Framework Questionnaire – Demonstration (Joel Guajardo)**

The Identity Assurance Framework (IAF) has been shared with the IAM Committee in the past and feedback has been incorporated. Discussions about incorporating the IAF into the IAM integration

process are ongoing, but as part of that initiative, a questionnaire has been created (which functions as a risk assessment survey) which will allow system administrators to provide information and receive a recommendation about which level of assurance is appropriate for their system.

IAF Questionnaire Demonstration.

The assessment is protected by UTLogin. Users are presented with a brief description of the IAF and prompted to provide information about their application.

Comment: It might make sense to integrate this assessment into the ISO application registry as well as the upcoming ESB application registry to prevent duplication of work.

Q: Is this questionnaire primarily for the benefit of the individual filling out the survey?
A: Yes, the goal is to get the application owner to go through the through process of risk assessment.

Q: Would it be helpful to incorporate this questionnaire into the ISO application registry?
A: Yes, the IAM team will look into that.

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

Reference handouts.

The first handout ("IAM Modernization Program, Phase 1 Progress") shows where the project stands compared with the initial project estimates. The project is under budget hours-wise.

The second handout details the list of deliverables and their current status. The project team is deeply engaged in Task 3 (Technical Architecture and System Environments). A prototype SailPoint IdentityIQ environment was demonstrated last week. Work on Task 4 (Interface and Data Transition Strategy) is ongoing and while that effort is currently on schedule, the project team believes that more time may be needed to be appropriately thorough with information gathering and analysis.

As soon as Task 4 has been completed (late May/early June) a scheduled re-assessment will take place to re-baseline the project. Additionally, work will begin drafting the Statement of Work for Phase 2.

4. **Other Initiative Updates**
    a. **IAM Team Staffing (Mario Leal)**

The IAM Team current has five positions open. Interviews are being conducted for the one software QA analyst position. One software engineer position has been posted and interviews are scheduled for another. Interviews are ongoing for a Senior Software Developer/Analyst. One Business Analyst position is in the process of being posted.

The team is starting to explore new strategies for finding good candidates. One strategy consists of going out in person to recruiting events. Another strategy involves building relationships with university departments to help the team understand the skillsets of the students graduating from these programs

and to communicate the skillsets that we are looking for. The team is also evaluating the use of an outside recruiting agency.

Q: Rich Janes is currently looking into drafting an RFP for recruiting. Is that effort on your radar and, perhaps, something you might want to be a part of?
A: UT System has signed contracts with four recruiting firms and those are the firms that the IAM Team is currently looking into. The team will reach out to Rich to share notes.

b. IAM Integrations (Mario Leal)

The project management component of the IAM Integrations effort is being shifted to Justin Hill. There are currently 20 outstanding requests with 3 in progress, 2 in verification, and 16 in the backlog. Verification means that the system engineer has reported that the integration work has been completed, but that the requester has not yet verified that it is working as expected.

The team is currently receiving 1-2 new requests for integrations per week which is straining the team's capacity. This issue will be addressed by filling the team's vacant positions and training existing system engineers on the integration process.

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

As of today there are 4300 users registered with Duo (comprising two-thirds of the potential VPN user base). The team's current focus is on the upcoming UTLogin release on May 8 which will integrate Duo, as well as the Shibboleth version 3 upgrade. The design for generating PDFs that require two-factor authentication via the PDF Generator has been developed. Toopher is on schedule to be retired in July.

d. Directory Services Roadmap (Justin Hill)

The Directory Services survey closed on April 1. There were 132 responses received and 115 of those responses were already using a directory of some kind. The next phase of the roadmap is a series of FYIs for campus and requirements gathering.

e. Lightweight Authentication (Rosa Harris)

The evaluation team is completing their review of the 6 received proposals and will be meeting with Purchasing on Thursday to narrow down the selection to 2-3 vendors who will be invited to campus for in-person presentations in May. The goal is to finalize the selection by mid-May and finalize the contract by mid-June.

f. Authorization Roadmap (Joel Guajardo)

Customer interviews for Apollo have been completed. The team is currently reassessing the schedule for removing position-based authorizations in Apollo.

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.

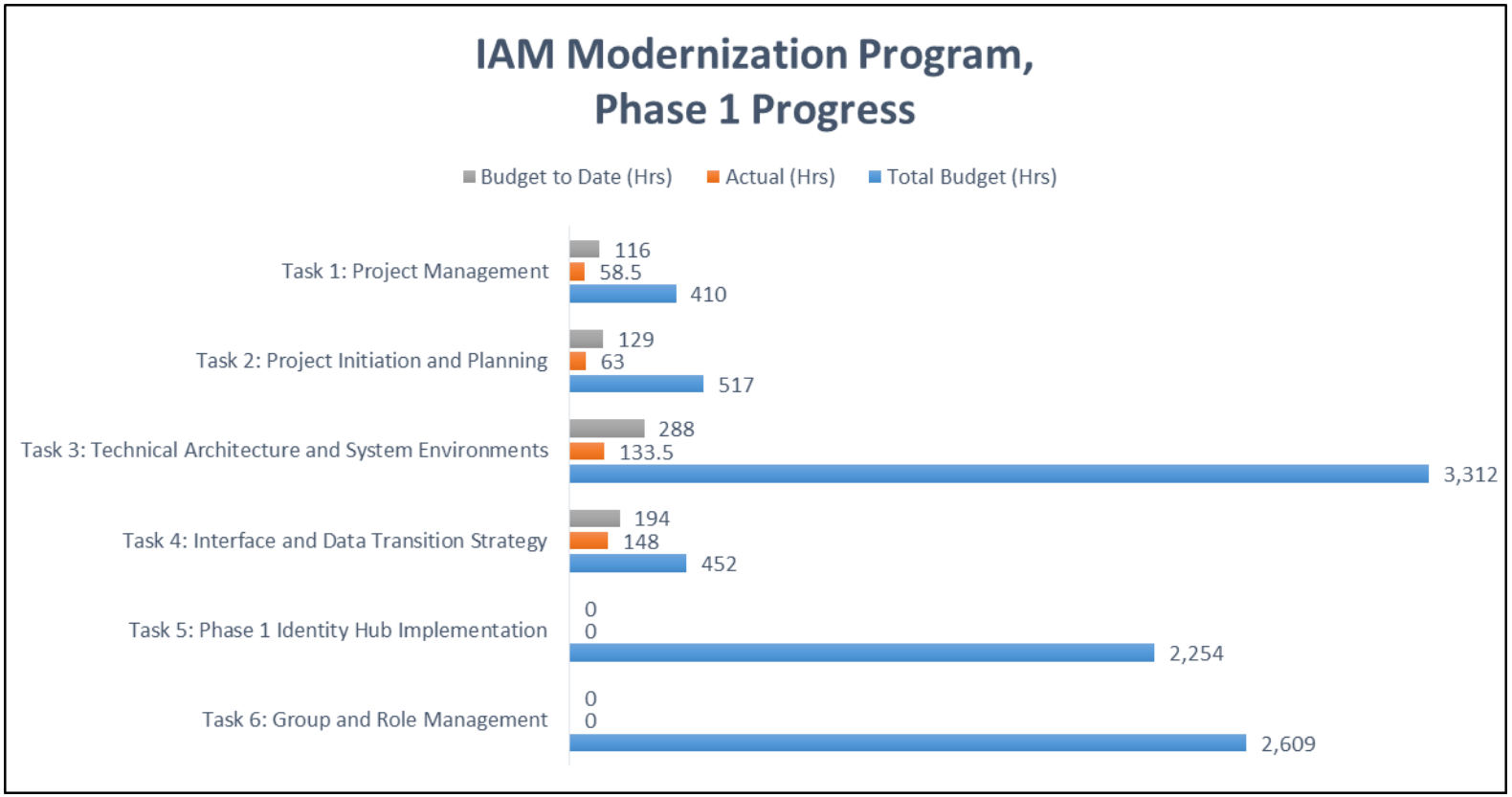
RECOMMENDATION

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.
- 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 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.


IAM Modernization Program,
Phase 1 Progress
Budget to Date (Hrs)
Actual (Hrs)
Total Budget (Hrs)
Task 1: Project Management
116
58.5
410
Task 2: Project Initiation and Planning
129
63
517
Task 3: Technical Architecture and System Environments
288
133.5
3,312
Task 4: Interface and Data Transition Strategy
194
148
452
Task 5: Phase 1 Identity Hub Implementation
0
0
2,254
Task 6: Group and Role Management
0
0
2,609

Project Task Area	Deliverable	Deliverable Name	Status	Baseline 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	In Progress	4/25/2016	EC: 4/25/2016
	D1.2.2	Q2 Quarterly Status Report	Not Started	7/25/2016	
	D1.2.3	Q3 Quarterly Status Report	Not Started	10/24/2016	
	D1.2.4	Q4 Quarterly Status Report	Not Started	1/30/2017	
	D1.3	Risk and Issue Register	Complete	3/21/2016	3/17/2016
	D1.4	Change Control Process	Behind	4/4/2016	EC: 4/11/2016
	D1.5	Communication Plan	Not Started	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	Not Started	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	In Progress	5/2/2016	EC: 5/2/2016
	D3.2	Prototype Environment(s)	In Progress	5/2/2016	EC: 4/18/2016
	D3.3	Technical Architecture Requirements	In Progress	5/16/2016	EC: 5/16/2016
	D3.4	Technical Architecture Design Blueprint	Not Started	6/20/2016	
	D3.5	Technical Architecture Build	Not Started	8/8/2016	
	D3.6	Technical Architecture Testing	Not Started	8/22/2016	
	D3.7	Technical Architecture Training	Not Started	8/29/2016	
	D3.8	Technical Architecture Deployment Playbook	Not Started	8/22/2016	
	D3.9	Technical Architecture Deployment	Not Started	9/12/2016	
	D3.10	Technical Architecture Operations and Maintenance Plan	Not Started	9/26/2016	
Task 4: Interface and Data Transition Strategy	D4.1	Interface and Data Transition Strategy Requirements	In Progress	5/9/2016	EC: 5/9/2016
	D4.2	Interface and Data Transition Strategy	In Progress	5/23/2016	EC: 5/23/2016
Task 5: Phase 1 Identity Hub Implementation	D5.1	Phase 1 Identity Hub Design Blueprint	Not Started	8/1/2016	
	D5.2	Phase 1 Identity Hub Build	Not Started	9/6/2016	
	D5.3	Phase 1 Identity Hub Test	Not Started	10/24/2016	
	D5.4	Phase 1 Identity Hub Training	Not Started	10/31/2016	
	D5.5	Phase 1 Identity Hub Deployment Playbook	Not Started	10/10/2016	
	D5.6	Phase 1 Identity Hub Deployment	Not Started	10/31/2016	
	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan	Not Started	11/14/2016	
Task 6: Group and Role Management	D6.1	Group and Role Management Use Cases	Not Started	8/22/2016	
	D6.2	Group and Role Management Requirements	Not Started	9/6/2016	
	D6.3	Group and Role Management Design Blueprint	Not Started	9/26/2016	
	D6.4	Group and Role Management Adoption Plan	Not Started	11/7/2016	
	D6.5	Group and Role Management Build	Not Started	10/24/2016	
	D6.6	Group and Role Management Testing	Not Started	11/21/2016	
	D6.7	Group and Role Management Training	Not Started	12/12/2016	
	D6.8	Group and Role Management Deployment Playbook	Not Started	10/24/2016	
	D6.9	Group and Role Management Deployment	Not Started	12/12/2016	
	D6.10	Group and Role Management Operations and Maintenance Plan	Not Started	12/19/2016	