IAM Committee
Meeting Notes
10/12/2015

Attendees: Tom Beard, Cam Beasley, CW Belcher, Michael Bos, David Burns, John Chambers, Graham Chapman, Tim Fackler, Cesar de la Garza, Fred Gilmore, Alison Lee, Ty Lehman, Andy Loomis, Darin Mattke, Michelle McKenzie, Steven Rung, Karen Weisbrodt

Absent: Shelley Powers, Charles Soto

IAM Team Members: Justin Czimskey, Rosa Harris, Josh Kinney, Marta Lang

1. IAM Roadmap – Review (CW Belcher)

See "IAM Roadmap Overview" handout.

- IAMMP (SailPoint implementation) and Duo Implementation are our largest projects this year.
- A significant amount of the team's time will be spent on IAM integrations for strategic projects (Workday, Application Modernization, TAI, etc.).

Q: What is TAI?
A: TAI (Technical Architecture Implementation) is part of ASMP and includes the implementation of the new administrative systems technical architecture for campus.

Q: When is Toopher being replaced?
A: We anticipate transitioning existing services using Toopher to Duo in late spring. Exact timing of the transition will be determined in coordination with the areas currently using Toopher two-factor authentication.

2. Lightweight Authentication Assessment Recommendation – Endorse (Marta Lang)

See "Lightweight Authentication" handout.

The team has completed an assessment of the lightweight authentication product landscape and recommends that an RFP be issued to procure a lightweight authentication solution.

Q: Which areas were consulted during the assessment?
A: The team has met with more than 13 campus units to elicit use cases and requirements related to lightweight authentication and the use of Guest EIDs.

Q: Why pursue an RFP versus an RFI?
A: During the assessment phase the team completed an informal RFI process, gathering information through written responses and oral presentations from vendors, so we are ready to proceed to the RFP stage.

Q: Do you think 6 months is adequate to complete the RFP process?

A: We will use the IAM software selection RFP as a template and the information from the lightweight authentication research summary to help accelerate the process of developing the RFP. The team is meeting with Purchasing this week to discuss the RFP schedule.

Decision: The committee endorsed proceeding with the RFP.

3. Other Initiative Updates

a. IAM Integrations (Justin Czimskey)

Since the last committee meeting, 4 IAM integrations were completed. 10 integrations are currently in flight. New requests continue to come in from TAI, AppMod, and campus in general.

b. Two Factor Authentication (Justin Czimskey)

An Exclusive Acquisition Justification (EAJ) for procuring Duo has been approved by Purchasing and contract review is in progress. Project planning for the Duo implementation is in progress.

Toopher will continue to provide two-factor authentication for W-2 downloads and other two-factor-protected applications on UT Direct through the Spring 2016 tax season.

c. CARE Project (Justin Czimskey)

As discussed at our last meeting, CARE will be placed on hold after the conclusion of the Architecture Assessment phase due to resource constraints. The CARE Customer Steering Committee (CSC) is scheduled to meet on October 16th to review the CARE Solution Architecture Summary and determine their preferred solution architecture(s). This architectural direction will be used when the CARE project is resumed or when other campus units investigate possible offsite hosting locations.

e. SailPoint Implementation (Marta Lang)

Four members of the IAM team completed a week-long SailPoint training course at the end of September and are now working on pre-implementation tasks in preparation for the implementation project.

KPMG has been notified of their selection for SailPoint implementation services, pending contract finalization. Contract discussions are beginning this week and we hope to begin the project in mid-November.

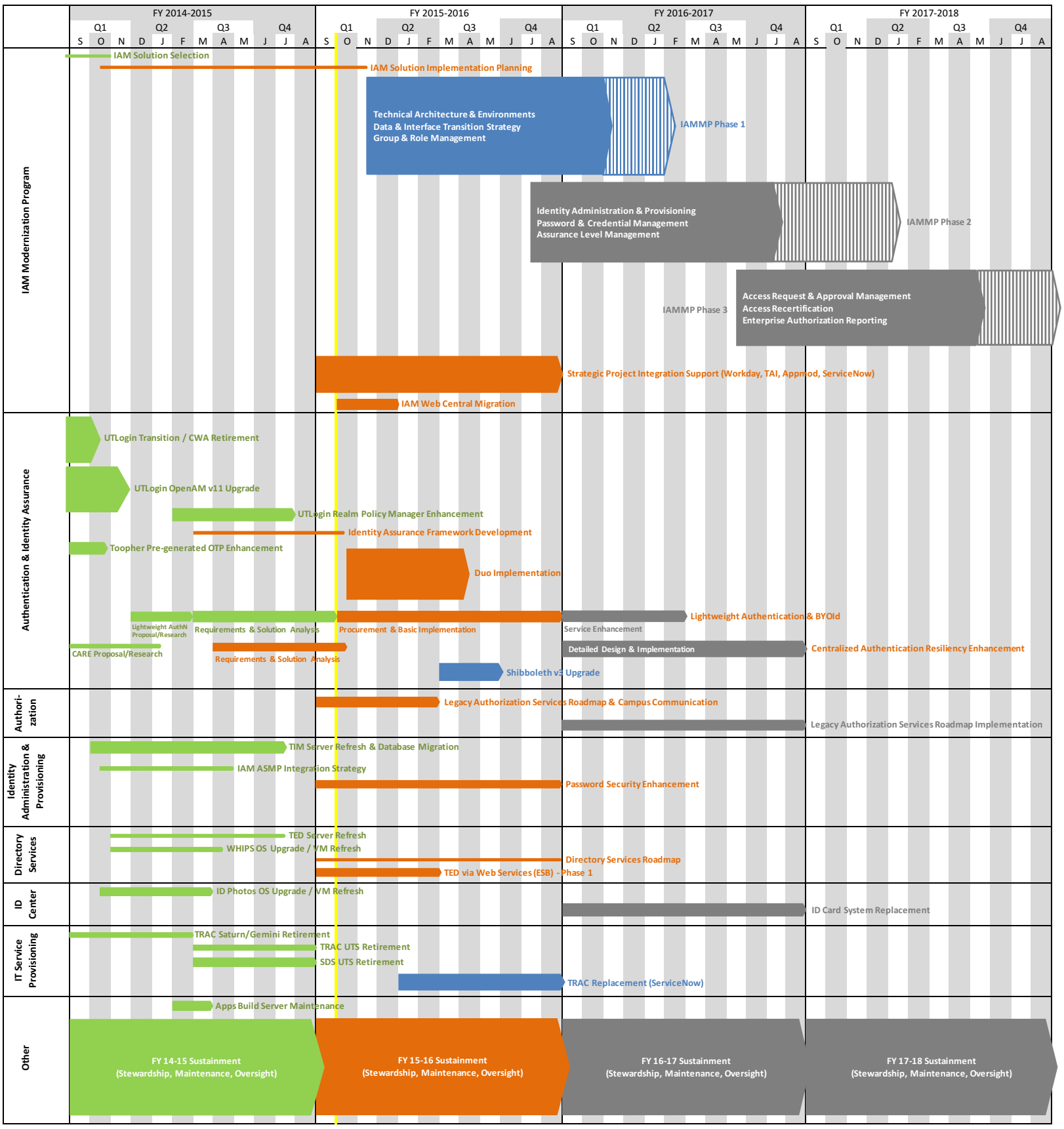
Q: At the oral presentation KPMG had indicated they may not be available to start until January. What is the status of this?
A: Resource availability and project start date will be discussed as part of the contract negotiations.

The University of Texas at Austin
Information Technology Services
Identity & Access Management

IAM Roadmap Overview

Status Key: Complete · In Progress · Planned · Future

Bar Height Indicates Level of Effort — 1 FTE



IAM Roadmap Initiative Descriptions

IAM Modernization Program

IAM Solution Selection (Complete): Select and procure new IAM software to support and enable the roadmap goals.
IAM Solution Implementation Planning: Complete high-level planning for the implementation of the software selected in the IAM Solution Selection project.
IAMMP Phase 1: Establish new technical architecture and environments for SailPoint; Develop data and interface transition strategy; Implement group and role management.
IAMMP Phase 2: Implement identity adminstration and provisioning, password and credential management, and assurance level management functionality.
IAMMP Phase 3: Implement access request and approval management, access recertification, and enterprise authorization reporting functionality.
Strategic Project Integration Support: Support authentication and identity data integration with University strategic projects, including Workday, TAI, ASMP application modernization, and ServiceNow.
IAM Web Central Migration: Migrate IAM web site content off of the end-of-life Web Central platform.

Identity Assurance and Authentication

UTLogin Transition / CWA Retirement (Complete): Transition Central Web Authentication & Fat Cookie customers to UTLogin and retire the CWA/FC authentication system.
UTLogin OpenAM v11 Upgrade (Complete): Upgrade UTLogin to the current version of OpenAM software to address bugs, implement session management enhancements, and stay current with vendor support.
UTLogin Realm Policy Manager Enhancement (Complete): Enhance the UTLogin RPM to allow delegated administration of sites on shared hosting environments like UT Web and Windows Web Hosting.
Identity Assurance Framework Development & Implementation: Implement a framework to assist campus departments in assessing risks and selecting an appropriate level of assurance to mitigate those risks.
Toopher Pre-generated OTP Enhancement (Complete): Add the ability to use pre-generated one-time-passwords (OTPs) with Toopher.
Duo Implementation: Implement two-factor authentication using the Duo Security solution.
Lightweight Authentication & BYOId: Implement a lightweight identifier and authentication service and integrate with external identity providers (Bring Your Own Identity).
Central Authentication Resiliency Enhancement: Improve the resiliency of central authentication services by leveraging off-campus hosting.
Shiboleth v3 Upgrade: Upgrade the Shibboleth federated authenication solution to the currently supported version.

Authori-zation

Legacy Authorization Services Roadmap & Campus Communication: Define the transition and retirement roadmaps for Apollo, OHS Contacts, and DPUSER Department Contacts systems and communicate with campus stakeholders.
Legacy Authorization Services Roadmap Implementation: Implement transition and retirement roadmaps for Apollo, OHS Contats, and DPUSER Department Contacts systems.

Identity Administration & Provisioning

TIM Server Refresh & Database Migration (Complete): Retire out-of-warranty servers and migrate to virtual server infrastructure and enterprise Oracle service.
IAM ASMP Integration Strategy (Complete): Define high-level plan for maintaing required integrations while source systems and IAM system are being replaced.
Password Security Enhancement: Improve the security of EID password storage infrastructure.

Directory Services

TED Server Refresh (Complete): Retire out-of-warranty servers.
WHIPS OS Upgrade / VM Refresh (Complete): Migrate to supported OS version and refresh virtual server infrastructure.
Directory Services Roadmap: Document new and evolving TED use cases and requirements and plan approach for addressing them.
TED via Web Services (ESB) - Phase 1: Implement an initial set of TED services on the ESB (public directory information lookup, group membership lookup, confidential directory information lookup).

ID Center

ID Photos OS Upgrade / VM Refresh (Complete): Migrate to supported OS version and refresh virtual server infrastructure.
ID Card System Replacement: Modernize ID Card System and remove mainframe dependency.

IT Service Provisioning

TRAC Saturn/Gemini Retirement (Complete): Retire use of out-of-warranty servers.
TRAC UTS Retirement (Complete): Migrate TRAC functions off end-of-life UTS service.
SDS UTS Retirement (Complete): Migrate SDS functions off end-of-life UTS service.
TRAC Replacement (ServiceNow): Replace TRAC functionality with ServiceNow.

Other

Apps Build Server Maintenance (Complete FY14-15): Maintenance and enhancements required to support ITS Applications software build and testing infrastructure.

10/12/2015

OVERVIEW

The first phase of the Lightweight Authentication Project explored the product landscape and performed a solution analysis against the University's lightweight authentication requirements and business needs. The project team engaged a Customer Steering Committee (CSC) including representatives of several campus business areas. The project team and CSC worked together to develop and approve detailed requirements, document use cases, complete interviews with peer institutions, and complete a comparative analysis of lightweight authentication products. The recommendation for the next phase of the project, endorsed by the CSC, is to proceed with a request for proposal (RFP) to receive detailed and formal responses from vendors on implementation approach and cost.

ACTION REQUIRED

The IAM Committee's endorsement is requested to move forward with the development and release of an RFP to procure a lightweight authentication solution.

IMPACT ANALYSIS

The CSC determined that the lightweight authentication solution for the University should provide the ability to create lightweight accounts using either an existing social identity or a local account that can easily be created by providing name, email address, and password. The solution should also provide a method to associate lightweight accounts with an EID and UIN.

Additionally, the project team has completed numerous interviews of Guest EID creators and users to better understand how Guest EIDs are used across campus. In many cases, the use of Guest EIDs could be replaced with a lightweight authentication identifier associated with a limited set of service entitlements, such as providing access to the network or library resources. A future service enhancement to the lightweight authentication service would explore how to meet these requirements.

PROJECT GOALS

Individuals that are loosely affiliated with the University need the ability to access university resources using an identity that is not burdensome to create, use, or remember. The Lightweight Authentication effort will provide a lightweight authentication option for external users. The Lightweight Authentication project will:

- Provide a basic lightweight authentication option for external users;
- Develop guidelines for the use of external identities in campus applications;
- Enhance the lightweight authentication to meet the additional requirements, such as linking to EIDs or to provide limited access to campus resources; and
- Complete Guest EID retirement planning.

SCHEDULE

- Complete solution procurement: March 2016
- Basic Lightweight Authentication Implementation: September 2016
- Enhanced Lightweight Authentication Implementation: March 2017

FOR MORE INFORMATION

For more information, please contact the project team: CW Belcher (cwbelcher@austin.utexas.edu), Marta Lang (mlang@austin.utexas.edu), or Rosa Harris (rharris@austin.utexas.edu).