

IAM Committee

Meeting Notes

6/13/2016

Attending: Thomas Beard, CW Belcher, Bill Bova, Tim Fackler, Fred Gilmore, Alison Lee, Ty Lehman, Andy Loomis, Darin Mattke, Charles Soto, Karen Weisbrodt, Tiffany Yanagawa

Absent: Cam Beasley, Michael Bos, John Chambers, Graham Chapman, Cesar de la Garza, Shelley Powers, Steve Rung

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

1. Two-Factor Authentication / Duo Implementation – Update (Justin Hill)

Reference hangout.

Q: Regarding the communication strategy for the migration from Toopher to Duo, will any action be needed in response to these communications, or is the communication informational only?

A: No user action will be required before applications are transitioned from Toopher to Duo (though customers will be provided a link to register their devices with Duo before the transition date). The IAM Team will also be working with Payroll to assist with customer communications as Payroll transitions their applications to Duo. Since our customers are already familiar with the two factor authentication at a conceptual level, and because Duo already has a sizeable user base on campus, we expect the transition to be smooth.

On July 12th the EID Administrative Services application will transition from protecting certain key functions with Toopher to placing the entire application behind Duo. Customer communications are forthcoming.

In order to comply with the UT System mandate, later this summer access to 3270 from off campus will start requiring VPN.

Q: Are there any concerns about scaling with the VPN with the addition of new customers?

A: ITS Networking is not currently concerned about scalability, particularly after recent upgrades.

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

Reference handout.

For Task 3 (Technical Architecture and System Environments) the project team plans to review the technical architecture design with the IAM Committee using a template used by the Technology Architecture Implementation (TAI) Architecture Review Board. The design will be available for review by the IAM Committee in July, and there may be a meeting scheduled in addition to the regular committee meeting to review and gather feedback.

Task 4 (Interface and Data Transition Strategy) looks at the interface and data transition needs for the entire project holistically over multiple phases of release. The team will provide the committee with an overview of Phase 1 transitions and interface approaches over the next few months.

For Task 6 (Group and Role Management), the team will document use cases based on stakeholder interviews and will bring those to the committee for feedback regarding prioritization for a phased release.

There are several deliverables that are running behind schedule because of the time needed to invest additional time and resources to get the deliverables right, since they will set the direction for the next three project phases. The team plans to re-baseline the project around mid-July.

Q: Could the team provide a copy of the strategy requirements that committee members can use as a model for their own projects?

A: Yes. A copy will be shared with the committee.

Q: For the Architecture Design Review meeting, how far in advance will meeting materials be sent out?

A: A pared down set of information will be sent out around a week in advance of the meeting. A full copy of the documentation (currently estimated at 60 pages) is available upon request.

3. Lightweight Authentication – Update (Rosa Harris)

Two vendor presentations were conducted and a solution was selected. The project team is currently performing vendor reference checks and will perform a cost analysis to determine how to move forward based on budget constraints. A meeting with the CSC is upcoming to discuss next steps and the output of that meeting will be shared with the IAM Committee.

4. Other Initiative Updates

a. IAM Team Staffing (Mario Leal)

At the last meeting the team had five vacant positions. One Business Analyst offer has been accepted and two Software Engineer offers are in progress. The vacant Senior Software Developer/Analyst and Senior QA Tester positions are being revised and will be reposted as a Software Developer/Analyst and Lead QA Tester.

b. IAM Integrations (Mario Leal)

There are currently 23 requests outstanding, three in progress, and 20 in the backlog. The team is currently reviewing how the IAM Operations team can assist with the integrations process.

Q: Have any issues been closed lately? It's unclear if the numbers presented have been static, or reflect work being completed and new requests coming in.

A: The team completed one request last week. In the future, we will include information about how many requests are being completed.

c. Directory Services Roadmap (Josh Kinney)

The project team has developed a new set of directory services use cases based on survey data. Work is in progress to align the new and old use cases. The team has identified several technology candidates to assess their match with the use cases. After that analysis is complete, the team will set up prototypes for more thorough testing.

Q: What's the mix of old/new use cases?

A: Roughly 80% old and 20% new. There are about 16 existing use cases and 3 new use cases.

Q: Would you be able to share these use cases with the committee?

A: Yes, they will be shared along with the meeting notes.

d. Authorization Roadmap (Joel Guajardo)

The project team is now focusing on the Organizational Hierarchy System Contacts application (OHSC). The team is creating a report to determine area owners and will communicate the position-based contact conversion strategy with those owners. The team is also working on creating implementation plans which will include detailed technical information.

Q: What is the project timeline after OHSC? Will you go back to Apollo?

A: The project will likely proceed with work on utilities for transitioning position-based authorizations/memberships/contacts all the systems in parallel after the OHSC assessment is complete. The goal is to send out communications for all systems by the end of July.

Q: With the OHSC there has been talk of IAM doing the conversion work. Will that happen with Apollo?

A: There will be an automated option for transitioning position-based authorizations and group memberships available for Apollo customers.

Duo Implementation Project - Status Update

Current Registered Users - 5500

UTLogin

2016.1.2 – Estimated Completion: Sunday, June 26

- Includes SAML and HardToken functionality

Shibboleth

v3 Upgrade – Estimated Completion: Thursday, July 14

- Currently testing in TEST
- Delayed due to resource constraints, competing priorities and technical roadblocks from deeper changes to upgrade than initially understood.

Integration – Estimated Completion: Early September

PDF Generator

- Currently testing in QUAL with Payroll and FIS
- Estimated Completion: Thursday, June 23

Migration from Toopher to Duo

- Estimated Completion: Monday, July 25
- Communication Strategy
 - 1st Email Notice – Monday, June 27
 - 2nd Email Notice – Wednesday, July 20
 - Final Email Notice – Monday, July 25

Toopher Retirement

- Estimated Completion: Late August

Identity and Access Management Modernization Program (IAMMP)

Phase 1 Status

Monday, June 13, 2016

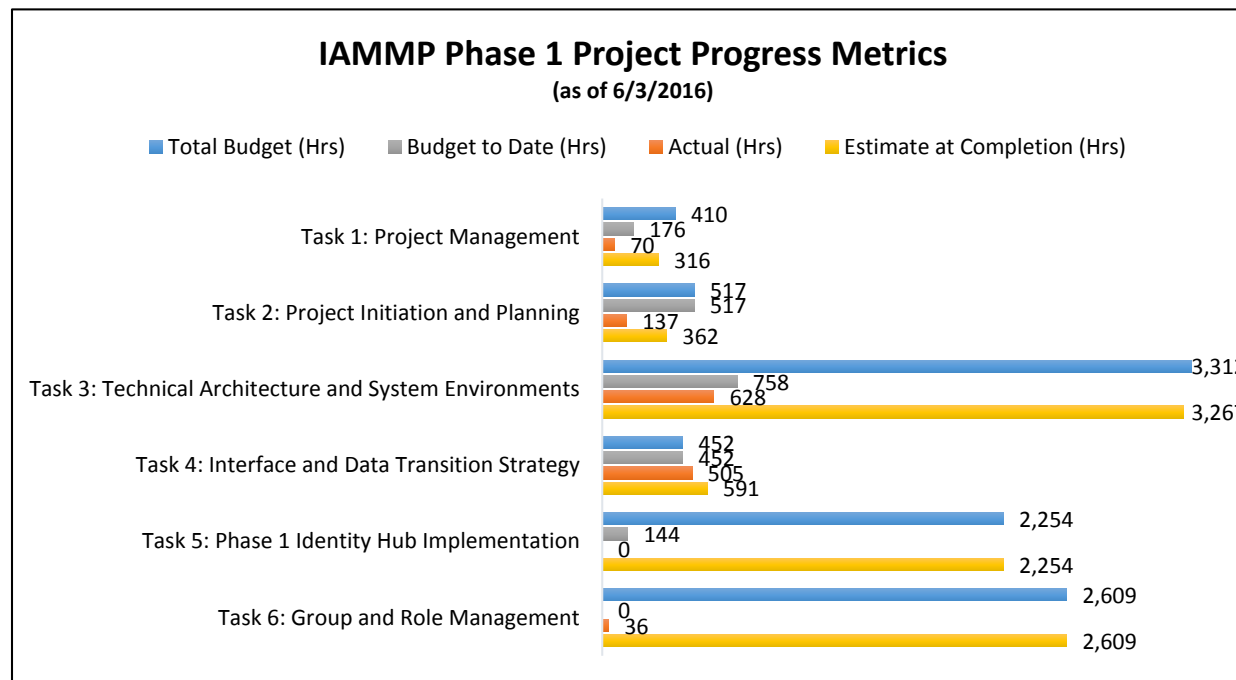
Program Overview

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 2: Project Initiation and Planning – The Deployment Plan and Training Plan are under review as Task 3 and Task 4 progress. The Comprehensive Test Plan was kicked and is underway.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Approach and Requirements deliverables were approved. The team has created detailed diagrams and is working on the technical architecture descriptions for the Technical Architecture Design Blueprint. The VM and server order was placed with ITS Systems and is in progress.
- Task 4: Interface and Data Transition Strategy – The Interface and Data Transition Requirements deliverable was approved. The team continues to develop the phased system and data transition diagrams and narratives as part of the Interface and Data Transition Strategy.
- Task 6: Group and Role Management – The team identified stakeholder groups and is scheduling interviews to draft use cases.



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
Task 2: Project Initiation and Planning	D1.5	Communication Plan		7/18/2016	
	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	Behind	6/6/2016	EC: 7/25/2016
	D2.4	Deployment Plan	Behind	4/25/2016	EC: 6/24/2016
Task 3: Technical Architecture and System Environments	D2.5	Training Plan	Behind	5/23/2016	EC: 6/24/2016
	D3.1	Technical Architecture Approach	Complete	5/2/2016	5/20/2016
	D3.2	Prototype Environment(s)	Complete	5/2/2016	4/18/2016
	D3.3	Technical Architecture Requirements	Complete	5/16/2016	6/10/2016
	D3.4	Technical Architecture Design Blueprint	Behind	6/20/2016	EC: 7/25/2016
	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	
Task 4: Interface and Data Transition Strategy	D3.10	Technical Architecture Operations and Maintenance Plan		9/26/2016	
	D4.1	Interface and Data Transition Strategy Requirements	Complete	5/9/2016	6/3/2016
Task 5: Phase 1 Identity Hub Implementation	D4.2	Interface and Data Transition Strategy	Behind	5/23/2016	EC: 7/25/2016
	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	
Task 6: Group and Role Management	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		11/14/2016	
	D6.1	Group and Role Management Use Cases	In Progress	8/22/2016	EC: 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		

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements

Interface and Data Transition Strategy Requirements Traceability Matrix Overview

The Requirements and Traceability Matrix documents the interface and data transition requirements captured from analyzing existing and new interfaces, current business processes, and identity management data collections and entities. These requirements will be used to define the strategy for all major phases of IAMMP and intermediate states of the Identity Management environment. It describes the integrations required as well as any constraints and service level agreements known to date at a level that is specific and verifiable to define the strategy. The requirements will be used by key stakeholders and project team as the checklist for verifying that the correct strategy is in place for each of the phases of IAMMP. The traceability matrix will be used to track the inclusion of each requirement throughout the project, from design through final testing.

Many of the Business Process Requirements in this document refer to an Identity Hub. The Identity Hub is a Service-Level abstraction and not a particular product or service. The composite of the University's legacy and future IAM systems provide services that together comprise the Identity Hub. The Identity Hub will change over the course of the project and the Interface and Data Transition Strategy will define the conceptual-level state of the Identity Hub in each of the phases, including the intermediate states between phases.

Business Process Requirements Tab

The Business Process Requirements tab contains a listing of requirements which need to be accounted for in the design of the Interface and Data Transition Strategy. Fields should be filled out as follows:

<u>ID</u>	Generally a number, sometimes with a project abbreviation, such as XYZ.001.
<u>Category</u>	A logical organizing structure for requirements, primarily applicable to functional requirements. For most products, the functionality can be sub-divided by business processes. See the "Categories" section below for example categories.
<u>Business Process</u>	A sub-division of the Category field. Business processes are generally divided into activities which occur as part of the process.
<u>Requirement Type</u>	Functional, Non-Functional, or Constraint. See below for definitions.
<u>Duration</u>	Integration or Bridge. See below for definitions.
<u>Priority</u>	Critical, Important, or Desired. See below for definitions.
<u>Source</u>	The department or group which proposed the requirement. This group may be contacted for clarifications regarding the requirement.
<u>Requirement Status</u>	Proposed, Approved, or Removed. See below for definitions.
<u>Creation Date</u>	The date on which the requirement was proposed / added to the requirements matrix.
<u>Notes</u>	Notes regarding the individual requirement.
<u>Rollout Phase</u>	Each requirement must be scheduled for a specific rollout phase.
Value Definitions	
The definitions for some of the field values are included below:	
Categories	
<u>Integration</u>	Ability to interface with other systems or processes -- List the ways that the system will need to integrate with other system and processes, including naming the applications or types of applications with which the system will integrate, the tools and/or protocols that will be used for integration and data exchange, and architectural considerations or consequences of integration.
<u>Performance</u>	Metrics for how the system should function under normal and peak loads -- Define measurable targets for normal and peak usage situations, such as response time in service level agreements, number of transactions processed in a period, number of concurrent users or sessions, accuracy of calculations, etc. Consider how these factors may influence the system architecture.
<u>Duration</u>	
<u>Integration</u>	A requirement is considered an "integration" requirement if it is expected to be a long-term integration that will last beyond the transition of IAM systems.
<u>Bridge</u>	A requirement is considered a "bridge" requirement if it is expected to be a temporary (i.e. short-term) bridge used during the transition of IAM systems.
Priority	
<u>Critical</u>	A requirement prioritized as "Critical" represents a product element which absolutely must be delivered and without which the product is considered not viable. This terminology replaces the "Must Have" priority in standard UT RTMs.

<u>Important</u>	A requirement prioritized as "Important" is highly desirable but could be waived for compelling reasons. This terminology replaces the "Should Have" priority in standard UT RTMs.
<u>Desired</u>	A requirement prioritized as "Desired" is considered optional for the project/product. This terminology replaces the "Nice to Have" priority in standard UT RTMs.
Requirement Status	
<u>Proposed</u>	A requirement is considered proposed if it has yet to be approved by the project governing body or if the requirement has been modified since approval and is awaiting review and re-approval.
<u>Approved</u>	A requirement is approved once the governing body, project team or primary customer has reviewed and agreed to the requirement.
<u>Removed</u>	A requirement is considered removed if the project the governing body, project team or primary customer has reviewed the requirement and agreed that it does not apply to the project/product. This may occur for both approved and proposed requirements.
Requirement Type	
<u>Functional</u>	Functional requirements describe what the product will do, such as allowing specific user actions, handling data, and managing access.
<u>Non-Functional</u>	Non-functional requirements describe the system architecture, availability parameters, and other technical details.
<u>Constraint</u>	Constraints describe limitations or restrictions on the choices available for designing or implementing the product. Examples include applicable laws and policies, go live dates and pre-existing architectural decisions.
Traceability Tab	
The traceability tab is used to link requirements with use cases and test cases. The fields should be filled out as follows:	
<u>ID</u>	Automatically filled from the Requirements ID field.
<u>Description</u>	Automatically filled from the Requirements Description field.
<u>Requirement Status</u>	Proposed, Approved, or Removed. See above for definitions.
<u>Use Case</u>	ID for use case(s) which apply to the requirement.
<u>Design</u>	Design document(s) or diagram(s) which apply to the requirement.
<u>Test Case</u>	Test case(s) which apply to the requirement. All requirements must be traced to a test case.
<u>Notes</u>	Notes regarding the traceability.
Revisions Tab	
The revisions tab defines major revisions. The field in this tab should be filled out as follows:	
<u>Version</u>	The version of the document in which changes occurred.
<u>Date</u>	The date that the new version of the document was submitted.
<u>Updater Name</u>	The individual who made the changes to the document.
<u>Description</u>	Description of the changes made during the revision.
Archive Tab	
This tab contains all requirements that were proposed and eventually removed from the Business Process Requirements tab.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
1.0 Active Directory										
1.1 Inbound Interfaces										
1.1.1	Integration	Read	Identity Hub shall read Active Directory Account information.	Functional	Desired	IAM Team	Approved	3/9/2016		
1.1.2	Integration	Read	Identity Hub shall read Active Directory Group Account information.	Functional	Desired	IAM Team	Approved	3/9/2016	Need to discuss if we want to mirror the AD tree in SailPoint by 11/01/2016.	
1.2 Outbound Interfaces										
1.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to Active Directory.	Functional	Critical	IAM Team	Approved	3/3/2016		
1.2.2	Integration	Create / Update	Identity Hub shall provide Group EID information to Active Directory.	Functional	Desired	IAM Team	Approved	3/3/2016		
FINAL	6/3/2016	Marta Lang	Executive Sponsor sign off of deliverable.	Functional	Critical	IAM Team	Approved	3/3/2016		
1.2.4	Integration	Create / Update	Identity Hub shall provide department information to Active Directory.	Functional	Critical	IAM Team	Approved	5/25/2016	In Phase 0, AD receives Org unit name. Department Information = Org unit information from Workday, and is distinctly separately from Department EIDs.	
1.2.5	Integration	Merge	Identity Hub shall support the TIM EID merge process in Active Directory until replaced by the 1.2.5 merge process.	Functional	Critical	IAM Team	Approved	3/22/2016	Current process: TIM sends 2 deletes and an add of the surviving record to AD.	
1.2.6	Integration	Merge	Identity Hub shall disable an EID account in Active directory when initiated by a merge.	Functional	Desired	AD Team	Approved	3/22/2016	Future process requested by AD team: Use the SailPoint IIQ integration to disable an EID directly within AD.	
1.2.7	Integration	Password Change	Identity Hub shall provide Active Directory with updates to password information.	Functional	Critical	IAM Team	Approved	3/22/2016		
1.2.8	Integration	Lock / Unlock	Identity Hub shall provide Active Directory with updates to account status (lock flag).	Functional	Critical	IAM Team	Approved	3/22/2016	This is a current state TIM process, which involves the IAM system notifying Active Directory to lock or unlock an account. For the future IIQ process see requirement 1.2.8.	
1.2.9	Integration	Disable	Identity Hub shall disable a Person EID account in Active Directory when an account is locked in the Identity Hub.	Functional	Desired	IAM Team	Approved	3/22/2016	This is a proposed future state IIQ process, which involves SailPoint IIQ disabling an account directly in AD with the SailPoint IIQ connector. For the current TIM process, see requirement 1.2.7.	
1.2.10	Integration	Termination	Identity Hub shall notify Active Directory of employment affiliation changes whenever a termination occurs.	Functional	Critical	IAM Team	Approved	3/22/2016		
1.2.11	Performance	SLA	Identity Hub shall send EID password changes to Active Directory in less than five (5) seconds.	Non-functional	Critical	AD Team	Approved	4/20/2016	Per Alex Barth on 04/20/2016.	
1.2.12	Performance	SLA	Identity Hub shall send EID attribute updates to Active Directory in less than ten (10) seconds.	Non-functional	Critical	AD Team	Approved	4/20/2016	Per Alex Barth on 04/20/2016.	
2.0 UTexas Enterprise Directory (TED)										
2.1 Inbound Interfaces										
2.1.1	Integration	Read	Identity Hub shall read Person EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016		
2.1.2	Integration	Read	Identity Hub shall read Group EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016		
2.1.3	Integration	Read	Identity Hub shall read Service EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016		
2.1.4	Integration	Read	Identity Hub shall read Business EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016	May be able to remove this functionality in Phase 2.	
2.1.5	Integration	Read	Identity Hub shall read Department EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016	May be able to remove this functionality in Phase 2.	
2.1.6	Integration	Read	Identity Hub shall read ID Only EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016	May be able to remove this functionality in Phase 2.	
2.1.7	Integration	Read	Identity Hub shall read Device EID information from TED.	Functional	Desired	IAM Team	Approved	3/9/2016		
2.2 Outbound Interfaces										
2.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016	This will include Person Employee department information.	
2.2.2	Integration	Create / Update	Identity Hub shall provide Group information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016		
2.2.3	Integration	Create / Update	Identity Hub shall provide Service EID information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016		
2.2.4	Integration	Create / Update	Identity Hub shall provide Business EID information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016	Required during Phase 1.	
2.2.5	Integration	Create / Update	Identity Hub shall provide Department EID information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016	Required during Phase 1. Department EIDs are a distinct object populated with departmental information (req. 2.2.8).	
2.2.6	Integration	Create / Update	Identity Hub shall provide ID Only EID information to TED.	Functional	Critical	IAM Team	Approved	3/3/2016	Required during Phase 1.	
2.2.7	Integration	Create / Update	Identity Hub shall provide Device EID information to TED.	Functional	Desired	IAM Team	Approved	3/22/2016		
2.2.8	Integration	Update	Identity Hub shall update department information attributes to TED.	Functional	Critical	IAM Team	Approved	5/25/2016	Department information is similar to Org unit information from Workday, and is distinctly separately from Department EIDs. Department information is being called out as a requirement, because the business processes and treatment of department information are potentially changing. The nature of this change will be investigated as part of Task 4.2.	
2.2.9	Integration	Merge	Identity Hub shall merge Person EIDs on TED.	Functional	Critical	IAM Team	Approved	3/22/2016		
2.2.10	Performance	SLA	Identity Hub shall send EID password changes to TED in less than five (5) seconds.	Non-functional	Critical	AD Team	Approved	4/1/2016	Per CW Belcher and Scott Doane on 04/13/2016.	
2.2.11	Performance	SLA	Identity Hub shall send EID attribute updates to TED in less than six (6) seconds.	Non-functional	Critical	AD Team	Approved	4/1/2016	Per CW Belcher and Scott Doane on 04/13/2016.	
3.0 Library										
3.1 Inbound Interfaces										
3.1.1	Integration	Update	Identity Hub shall receive requests to update Person EID information from Library.	Functional	Critical	IAM Team	Approved	3/21/2016	Mainframe requirement was T3NSIDMR (create non-member EID). In Phase 0, only receive updates on Entitlements and Affiliations from Mainframe.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
3.1.2	Integration	Prohibit Entitlement Provisioning	Identity Hub shall receive requests to restrict Library Access for specific EIDs.	Functional	Desired	Library Team	Approved	3/29/2016	Library currently maintains a hard coded lists of EIDs that are never allowed to use resources. We will need to determine a way to ensure the individuals on this list can never receive the appropriate entitlements which provide resource access.	
3.2	Outbound Interfaces									
3.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to Library.	Functional	Critical	IAM Team	Approved	3/21/2016	Borrowers, Other UT institutions, Public libraries - all lumped together under "courtesy borrower". Library systems receive primary role, email address if it exists, street address, etc.	
3.2.2	Integration	Merge	Identity Hub shall notify the Library of an EID merge.	Functional	Critical	IAM Team	Approved	3/21/2016	Use Case: Libraries receive an email notification of a merge.	
3.2.3	Performance	SLA	Identity Hub shall process Library transactions in less than five (5) minutes.	Non-functional	Critical	IAM Team	Approved	4/12/2016	Per Alison O'Balle: "1 minute or less would be ideal, 2 - 3 minutes would be better, 5 minutes is the max amount of time updates can take before patrons become vocally annoyed. Quicker the better."	
4.0	Public Network Authentication (PNA)									
4.1	Inbound Interfaces									
4.1.1	Integration	Read	Identity Hub shall read PNA account information.	Functional	Desired	IAM Team	Approved	3/9/2016		
4.2	Outbound Interfaces									
4.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to PNA.	Functional	Critical	IAM Team	Approved	3/4/2016		
4.2.2	Integration	Create / Update	Identity Hub shall provide Device EID information to PNA.	Functional	Desired	IT S Networking	Approved	3/18/2016		
4.2.3	Integration	Password Reset	Identity Hub shall provide password reset information to PNA.	Functional	Critical	IAM Team	Approved	3/18/2016	Per Alison Lee "There is not a currently defined SLA for password reset."	
4.2.4	Integration	Merge	Identity Hub shall delete a Person EID for PNA when initiated by a merge.	Functional	Critical	IT S Networking	Approved	3/18/2016	Need to determine Merge functionality in Design / Strategy Discussion (Task 4.2).	
4.2.5	Performance	SLA	Identity Hub shall transact EID creates and updates to the PNA system in less than six (6) minutes.	Non-functional	Critical	IAM Team	Approved	4/6/2016	Per Jason Wang on 4/6/16. " Includes both Create and Update."	
5.0	Workday									
5.1	Inbound Interfaces									
5.1.1	Integration	Read	Identity Hub shall read Workday identity record information for Employee Person EID information.	Functional	Critical	IAM Team	Approved	3/9/2016	including organizational hierarchy (supervisory org) and role (Workday calls these positions)	
5.1.2	Integration	Create	Identity Hub shall receive requests to create Employee Person EIDs from Workday.	Functional	Critical	CW Belcher	Approved	5/26/2016	This is to support an HR Admin user creating a Person Employee EID on behalf of that employee. CW comments: " IAM will need a way for Workday to request creation of a Person EID for a new employee if one does not already exist. This call would come from a bolt-on outside of Workday proper but part of the hire process."	
5.1.3	Integration	Create/ Update	Identity Hub shall receive requests to create Business EIDs from Workday.	Functional	Critical	Finance	Approved	4/25/2016	On 5/26/16, Don Simpson stated that Business EIDs will be created in Workday in a custom-built add-on similar to Person EIDs.	
5.1.4	Integration	Update	Identity Hub shall utilize Workday as the authoritative system for updating employee identity attributes.	Functional	Critical	IAM Team	Approved	3/16/2016	Precise Attributes (such as affiliation, entitlements, etc.) will be derived during detailed requirement gathering (Task 5.1). Updates certain fields of a user. Investigate Roles - what influence will Workday have on IIQ roles? (Task 5.1).	
5.1.5	Integration	Termination	Identity Hub shall update access after an Employee Person is terminated in Workday.	Functional	Critical	IAM Team	Approved	4/20/2016		
5.1.6	Performance	SLA	Identity Hub shall update access for Person Employee EIDs after a planned termination based on an update from Workday in less than 24 hours.	Non-functional	Critical	IAM Team	Approved	3/16/2016	Use Case: Planned termination scenario. Nightly batch job processing is acceptable.	
5.1.7	Performance	SLA	Identity Hub shall update access for Person Employee EIDs after an unplanned termination based on an update from Workday in less than 30 minutes.	Non-functional	Critical	Internal Audit	Approved	4/14/2016	Use Case: "Bad Actor" scenario, requiring immediate unplanned termination. From Internal Audit on 04/13/16: "30 minutes = worse case scenario, 15 minutes is better, 1 minute is ideal."	
5.1.8	Integration	Go-Live	Identity Hub shall support Workday at the time of Workday Go-live.	Constraint	Critical	IAM Team	Approved	3/16/2016	Go-Live is June 2017 (as of March 17, 2016). Workday testing commences end of May 2016, beginning of June 2016.	
5.1.9	Integration	Create	Identity Hub shall receive requests to create an electronic identifier for businesses and vendors from Workday.	Functional	Critical	Workday	Approved	3/17/2016		
5.1.10	Integration	Update	Identity Hub shall receive requests to update an electronic identifier for businesses and vendors from Workday.	Functional	Desired	Workday	Approved	3/17/2016	As of Phase 0, no departments update Business EIDs.	
5.1.11	Integration	Update	Identity Hub shall represent department information from Workday.	Functional	Critical	IAM Team	Approved	5/25/2016	Department information is similar to Org unit information from Workday, and is distinctly separately from Department EIDs. Department information is being called out as a requirement, because the business processes and treatment of department information are potentially changing. The nature of this change will be investigated as part of Task 4.2.	
5.1.12	Integration	Update	Identity Hub shall update department information received from Workday.	Functional	Critical	IAM Team	Approved	5/25/2016	Department information is similar to Org unit information from Workday, and is distinctly separately from Department EIDs. Department information is being called out as a requirement, because the business processes and treatment of department information are potentially changing. The nature of this change will be investigated as part of Task 4.2.	
5.1.13	Integration	Merge	Identity Hub shall process merge requests for Person EIDs from Workday.	Functional	Critical	Workday	Approved	3/17/2016		
5.1.14	Integration	Restrictions	Identity Hub shall process requests for restrictions placed on employee Person EIDs from Workday.	Functional	Critical	Workday	Proposed	3/17/2016	Workday is currently unsure of how to handle restrictions. Dependent upon Workday.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
5.1.15	Integration	Identity Association	Identity Hub shall associate Person EIDs to businesses or vendors.	Functional	Desired	IAM Team	Approved	4/15/2016	This is a request by the Finance department to associate one or more Person EIDs to a Business/Vendor EID and allow that Person EID to act on behalf of the Business/Vendor.	
5.1.16	Integration	Read	Identity Hub shall read organizational hierarchy information from Workday.	Functional	Critical	CW Belcher	Approved	5/19/2016	This information is based on Supervisory Org data from Workday and is intended to maintain the current department EID information published in TED, as well as for scoping roles with SailPoint that have an organizational scope component. This information may be a part of department information from 5.1.11 or it may be separate. Investigation during Task 4.2 will determine if these need to remain separate requirements.	
5.1.17	Integration	Update	Identity Hub shall represent access and entitlements based on job functions within Workday.	Functional	Critical	CW Belcher	Approved	5/19/2016		
5.1.18	Integration	Update	Identity Hub shall represent access and entitlements based on security roles within Workday.	Functional	Critical	CW Belcher	Approved	5/19/2016		
6.0 Administrative User Interface										
6.1 Inbound Interfaces										
6.1.1	Integration	Create	Identity Hub shall receive requests to create Group EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/3/2016		
6.1.2	Integration	Create	Identity Hub shall receive requests to create Service EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/3/2016		
6.1.3	Integration	Create	Identity Hub shall receive requests to create Business EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/3/2016		
6.1.4	Integration	Create	Identity Hub shall receive requests to create ID Only EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/3/2016		
6.1.5	Integration	Create	Identity Hub shall receive requests to create Device EIDs from an Administrative User Interface.	Functional	Important	IAM Team	Approved	4/22/2016		
6.1.6	Integration	Update	Identity Hub shall receive requests to update Person EID information from an Administrative User Interface.	Functional	Critical	CW Belcher	Approved	5/19/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.7	Integration	Update	Identity Hub shall receive requests to update Group EID information from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.8	Integration	Update	Identity Hub shall receive requests to update Service EID information from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.9	Integration	Update	Identity Hub shall receive requests to update Business EID information from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.10	Integration	Update	Identity Hub shall receive requests to update ID Only EID information from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.11	Integration	Update	Identity Hub shall receive requests to update Device EID information from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	4/22/2016	Which attributes can be updated (entitlements, personal information, EID information, etc.) will be defined in Task 5.1.	
6.1.12	Integration	Update	Identity Hub shall receive requests to generate a new EID value to replace an older EID value from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016	Determine design strategy in Task 5.1	
6.1.13	Integration	Lock	Identity Hub shall receive requests to lock EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016		
6.1.14	Integration	Unlock	Identity Hub shall receive requests to unlock EIDs from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016		
6.1.15	Integration	Password Reset	Identity Hub shall receive requests to reset passwords from an Administrative User Interface.	Functional	Critical	IAM Team	Approved	3/15/2016		
6.1.16	Integration	Merge	Identity Hub shall receive requests to merge EIDs from an Administrative User Interface.	Functional	Critical	RFP	Approved	3/15/2016	Taken from Non-functional RFP requirements.	
6.1.17	Performance	SLA	Identity Hub shall respond to simple transactions from an Administrative User Interface in less than one (1) second.	Non-functional	Critical	RFP	Approved	3/15/2016	Taken from Non-functional RFP requirements (Line 14).	
6.1.18	Performance	SLA	Identity Hub shall respond to complex transactions from an Administrative User Interface in less than five (5) seconds.	Non-functional	Critical	RFP	Approved	3/15/2016	Taken from Non-functional RFP requirements (Line 14).	
6.1.19	Integration	Create	Identity Hub shall create Sailpoint IIQ Roles from the Administrative User Interface.	Functional	Critical	IAM Team	Approved	5/25/2016		
6.1.20	Integration	Update	Identity Hub shall update Sailpoint IIQ Roles from the Administrative User Interface.	Functional	Critical	IAM Team	Approved	5/25/2016		
6.1.21	Integration	Delete	Identity Hub shall delete Sailpoint IIQ Roles from the Administrative User Interface.	Functional	Critical	IAM Team	Approved	5/25/2016		
6.1.22	Integration	Update	Identity Hub shall add Sailpoint IIQ Role assignment from the Administrative User Interface.	Functional	Critical	IAM Team	Approved	5/25/2016		
6.1.23	Integration	Update	Identity Hub shall remove Sailpoint IIQ Role assignment from the Administrative User Interface.	Functional	Critical	IAM Team	Approved	5/25/2016		
6.1.24	Integration	History	Identity Hub shall display EID history from an Administrative User Interface.	Functional	Critical	CW Belcher	Approved	5/19/2016	Allows a user with access to the Admin Application to view the history of an identity and identity attributes. Functionality provided during Phase 0 TIM Admin application - must have: Prior EIDs, Prior UINs, When & where the EID was created, name change history, birthday history, email address history, last valid login.	
6.1.25	Integration	History	Identity Hub shall display extended EID history from an Administrative User Interface.	Functional	Desired	Josh Kinney	Approved	5/26/2016	Allows a user with access to the Admin Application to view the history of an identity and identity attributes. Additional features not supported by the Phase 0 TIM Admin application, but desired by the IAM team and Helpdesk include: Lock history, Unified history in chronological order, history on specific EIDs (when dealing with merged EIDs), historical merges (prior to Sailpoint IIQ), actor who performed a merge.	
6.1.26	Integration	Update	Identity Hub shall create administrative notes on an EID record from an Administrative User Interface.	Functional	Critical	Josh Kinney	Approved	5/19/2016		
7.0 Self Service Portal										
7.1 Inbound Interfaces										
7.1.1	Integration	Create	Identity Hub shall receive requests to create Person EIDs from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/3/2016	Revisit once IAM Lightweight Authentication goes live.	
7.1.2	Integration	Change Password	Identity Hub shall receive requests to change password from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/15/2016	Use Case: Password is known.	
7.1.3	Integration	Change Password Reset Questions	Identity Hub shall receive requests to change password reset questions from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/15/2016	Use Case: I know my password and want to change my questions.	
7.1.4	Integration	Find my EID	Identity Hub shall receive requests to find a Person EID from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/15/2016	Actor is the actual EID owner in this scenario. Use Case: I do not know my EID and I'm trying to find it.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
7.1.5	Integration	Update	Identity Hub shall receive requests to update Guest-class Person EID attributes from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/15/2016	Self service has a MANAGE Functionality. We will define what specific attributes Self-Service portal can update during Task 5.1 requirement activities. Expect them to include password information, affiliations (maybe), password reset questions, and other info). This is a use case relevant to "Guest" EIDs i.e. non-student, non-staff. Revisit in Task 5.1 for what a student should be sent to and what a staff should be sent to. Also, Guest EIDs are called out here because Employee Person and Student Person EIDs will update information through other systems, but if you are neither of these two, you use the Self Service Portal.	
7.1.6	Integration	Merge	Identity Hub shall receive requests to merge Person EIDs from a Self Service Portal.	Functional	Critical	IAM Team	Approved	3/15/2016	Design discussion to be revisited during Task 5.1.	
7.1.7	Performance	SLA	Identity Hub shall respond to simple transactions from a Self Service Portal in less than one (1) second.	Non-functional	Critical	RFP	Approved	3/15/2016	Taken from Non-functional RFP requirements (Line 14).	
7.1.8	Performance	SLA	Identity Hub shall respond to complex transactions from a Self Service Portal in less than five (5) seconds.	Non-functional	Critical	RFP	Approved	3/15/2016	Taken from Non-functional RFP requirements (Line 14).	
7.1.9	Integration	Password Reset	Identity Hub shall receive requests to reset passwords via email from a Self Service Portal.	Functional	Critical	CW Belcher	Approved	5/19/2016	Use Case: I do not know my password and I do have access to my university granted email account. These individuals must have been issued UT email accounts or they will not receive this option.	
7.1.10	Integration	Password Reset	Identity Hub shall receive requests to reset passwords via password reset questions from a Self Service Portal.	Functional	Critical	CW Belcher	Approved	5/19/2016	Use Case: I do not know my password and I do not have access to my email. Password reset questions must include ID card number if a person has been issued an ID card.	
8.0 Mainframe Applications										
8.1 Inbound Interfaces										
8.1.1 Student Mainframe Applications										
8.1.1.1	Integration	Create	Identity Hub shall receive requests to create Person EIDs from Student Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016		
8.1.1.2	Integration	Update	Identity Hub shall receive requests to update Person EID attributes from Student Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	Which particular attributes MF apps can update (restrictions, affiliations, entitlements, password information) will be determined during Task 5.1.	
8.1.1.3	Integration	Merge	Identity Hub shall receive requests to merge Person EID accounts from Student Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016		
8.1.2 Human Resources Mainframe Applications										
8.1.2.1	Integration	Create	Identity Hub shall receive requests to create Person EIDs from HR Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	This functionality will be replaced by Workday.	
8.1.2.2	Integration	Update	Identity Hub shall receive requests to update Person EID attributes from HR Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	This functionality will be replaced by Workday. This needs to include restrictions, affiliations, entitlements, etc.	
8.1.2.3	Integration	Merge	Identity Hub shall receive requests to merge Person EID accounts from Payroll Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	Payroll initiates merges per Andrew Russell's research. This functionality will be replaced by Workday.	
8.1.3 Finance Mainframe Applications										
8.1.3.1	Integration	Create	Identity Hub shall receive requests to create Business EIDs from Finance Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	This functionality will be replaced by Workday.	
8.1.4 Organizational Hierarchy System (OHS)										
8.1.4.1	Integration	Create	Identity Hub shall initiate creation of Department EIDs from Organizational Hierarchy System (OHS) Mainframe Applications.	Functional	Critical	IAM Team	Approved	3/3/2016	Note that the integration with the current OHS/Department system is a pull process. OHS does not send create requests to TIM. There is an IAM Natural batch process that polls the OHS/Department system each night and if a new department is detected, that batch process sends the create request to TIM.	
8.1.4.2	Integration	Update	Identity Hub shall initiate updates to Department EID attributes from Organizational Hierarchy System (OHS) Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	Note that the integration with the current OHS/Department system is a pull process. OHS does not send update requests to TIM. There is an IAM Natural batch process that polls the OHS/Department system each night and changes in department data are detected (by comparing to what is on TOM) that Natural process sends an update request to TIM.	
8.1.5 Organizational Hierarchy System Contacts (OHSC)										
8.1.5.1	Integration	Create	Identity Hub shall receive requests to create Role EIDs from Organizational Hierarchy System Contacts (OHSC) Mainframe Applications.	Functional	Critical	IAM Team	Approved	3/3/2016	Role EIDs are conceptually separate from Group EIDs, although TIM sees them as groups.	
8.1.5.2	Integration	Update	Identity Hub shall receive requests to update Role EID attributes from Organizational Hierarchy System Contacts (OHSC) Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	Role EIDs are conceptually separate from Group EIDs, although TIM sees them as groups.	
8.1.5.3	Integration	Update Membership	Identity Hub shall receive requests to update Role EID membership from Organizational Hierarchy System Contacts (OHSC) Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/5/2016	Role EIDs are conceptually separate from Group EIDs, although TIM sees them as groups.	
8.1.6 Donor										
8.1.6.1	Integration	Create	Identity Hub shall receive requests to create ID Only EIDs from Donor Mainframe Applications.	Functional	Critical	IAM Team	Approved	3/3/2016		
8.1.6.2	Integration	Create	Identity Hub shall receive requests to create Business EIDs from Donor Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/5/2016	Donor system creates Business EIDs per Andrew Russell's research.	
8.1.6.3	Integration	Create	Identity Hub shall receive requests to create Person EIDs from Donor Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016		
8.1.6.4	Integration	Create	Identity Hub shall receive requests to update Business EIDs from Donor Mainframe Applications.	Functional	Desired	IAM Team	Approved	4/1/2016	Donor System would like to do this in the future.	
8.1.6.5	Integration	Update	Identity Hub shall receive requests to update Person EID attributes from Donor Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/1/2016	Donor system could push an update to affiliations, which would fall under this requirement. Revisit in Task 5.1.	
8.1.7 Miscellaneous										
8.1.7.1	Integration	Password Reset	Identity Hub shall receive requests to reset passwords initiated by Mainframe Applications.	Functional	Critical	RFP	Approved	3/15/2016	Taken from RFP.	
8.1.7.2	Integration	Password Update	Identity Hub shall receive requests to update passwords initiated by Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/5/2016		
8.1.7.3	Integration	EID Lookup	Identity Hub shall receive requests to lookup EID information from Mainframe Applications.	Functional	Critical	IAM Team	Approved	4/13/2016	Per CW Belcher on 04/13/2016.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
8.1.7.4	Integration	App Retirement	Identity Hub shall accommodate Mainframe Applications being removed upstream from IAM applications on the Mainframe.	Functional	Critical	IAM Team	Approved	4/20/2016		
8.2 Outbound Interfaces										
8.2.1 Merge										
8.2.1.1	Integration	Merge	Identity Hub shall provide EID merge/change information to the EID Merge Mainframe Notifier.	Functional	Critical	IAM Team	Approved	3/31/2016	Result of CW Belcher meeting on 3/31.	
8.2.2 TED on Mainframe (TOM)										
8.2.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016		
8.2.2.2	Integration	Create / Update	Identity Hub shall provide Group EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016		
8.2.2.3	Integration	Create / Update	Identity Hub shall provide Service EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016		
8.2.2.4	Integration	Create / Update	Identity Hub shall provide Business EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016	Required during Phase 1.	
8.2.2.5	Integration	Create / Update	Identity Hub shall provide Department EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016	Required during Phase 1.	
8.2.2.6	Integration	Create / Update	Identity Hub shall provide ID Only EID information to TOM.	Functional	Critical	IAM Team	Approved	3/31/2016	Required during Phase 1.	
8.2.2.7	Integration	Update	Identity Hub shall provide department information to TOM.	Functional	Critical	IAM Team	Approved	5/26/2015	Department information is presumed to be Org unit information from Workday, and distinctly separately from Department EIDs.	
8.2.3 Miscellaneous										
8.2.3.1	Performance	SLA	Identity Hub shall provide EID data requested from a mainframe application in less than one (1) second.	Non-functional	Critical	IAM Team	Approved	4/14/2015	Per CW Belcher on 04/13/2016.	
9.0 Lightweight Authentication (LWA)										
9.1 Inbound Interfaces										
9.1.1	Integration	Read	Identity Hub shall read Lightweight Authentication user account information.	Functional	Desired	LWA Project	Approved	3/9/2016	Updates to information of a user will be captured through the read.	
9.1.2	Integration	Go-Live	Identity Hub shall support the Lightweight Authentication system at the time of LWA Go-live.	Constraint	Critical	LWA Project	Approved	3/8/2016	Go-Live date TBD by IAM Lightweight Authentication Project.	
9.1.3	Integration	Association	Identity Hub shall associate an internal identity (Person EID) with an external identity from Lightweight Authentication consuming systems.	Functional	Important	LWA Project	Approved	5/25/2016	In some cases people with external identities will also have an internal (traditional Person EID) identity and we need some way to associate them.	
9.1.4	Integration	Create	Identity Hub shall receive requests from Lightweight Authentication consuming systems to create identities.	Functional	Desired	LWA Project	Approved	5/25/2016	Use Case: Consuming system initiate identity creation when a customer needs an identity.	
9.1.5	Integration	Update	Identity Hub shall receive requests from Lightweight Authentication consuming systems to update identities.	Functional	Desired	LWA Project	Proposed	5/25/2016	adding an entitlement, changing a name, etc. on a	
9.1.6	Integration	Disable	Identity Hub shall receive requests from Lightweight Authentication consuming systems to disable identities.	Functional	Desired	LWA Project	Proposed	5/25/2016		
9.2 Outbound Interfaces										
9.2.1	Integration	TBD	Identity Hub shall support the business cases that are identified as a part of the Lightweight Authentication Project.	Functional	Desired	LWA Project	Approved	3/25/2016	TBD by Lightweight Authentication Project.	
10.0 ServiceNow										
10.1 Inbound Interfaces										
10.1.1	Integration	Read	Identity Hub shall read ServiceNow user account information.	Functional	Desired	IAM Team	Approved	3/9/2016	SailPoint connector.	
10.1.2	Integration	Read	Identity Hub shall read ServiceNow group account information.	Functional	Desired	IAM Team	Approved	3/9/2016	SailPoint connector.	
10.1.3	Integration	Update Entitlement	Identity Hub shall receive requests to update Person EID entitlement information from ServiceNow.	Functional	Important	IAM Team	Approved	3/25/2016		
10.1.4	Integration	Update	Identity Hub shall receive requests to update role membership from ServiceNow.	Functional	Important	IAM Team	Approved	3/25/2016	Create / Update / Disable functionality. In Phase 0, this is Group access information, will determine how IIQ will handle in Task 5.1.	
10.1.5	Integration	Create	Identity Hub shall receive requests to create Groups from ServiceNow.	Functional	Desired	IAM Team	Approved	3/25/2016		
10.1.6	Integration	Create	Identity Hub shall receive requests to create Service EIDs from ServiceNow.	Functional	Desired	IAM Team	Approved	3/25/2016	Use Case: Service Now facilitates the request fulfillment process to create a new Service EID. This will be a 1 time process per EID created. This request process will include the responsible party, department information, and access required.	
10.1.7	Integration	Create	Identity Hub shall receive requests to create Device EIDs from ServiceNow.	Functional	Desired	IAM Team	Approved	3/25/2016	Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per EID created. This request process will include the responsible party, department information, MAC address and device serial number.	
10.1.8	Integration	Update	Identity Hub shall receive requests to add Sailpoint IIQ Role assignment from Service Now.	Functional	Desired	IAM Team	Approved	5/25/2016		
10.1.9	Integration	Update	Identity Hub shall receive requests to remove Sailpoint IIQ Role assignment from Service Now.	Functional	Desired	IAM Team	Approved	5/25/2016		
10.2 Outbound Interfaces										
10.2.1	Integration	Create / Update	Identity Hub shall provide Person EID information to ServiceNow.	Functional	Critical	IAM Team	Approved	3/25/2016	Source is TED in Phase 1, IIQ in future phases. Specific entitlements shall be investigated in Task 5.1 review.	
10.2.2	Integration	Create / Update	Identity Hub shall provide Group information to ServiceNow.	Functional	Critical	Service Now	Approved	3/25/2016	Future state requirement, SailPoint connector.	
10.2.3	Integration	Create / Update	Identity Hub shall provide business and vendor information to ServiceNow.	Functional	Desired	Service Now	Approved	3/25/2016		
10.2.4	Integration	Create / Update	Identity Hub shall return Device EID information to ServiceNow.	Functional	Desired	IAM Team	Approved	5/25/2016		
10.2.5	Integration	Update	Identity Hub shall grant permission to Person EIDs to access certain functions within ServiceNow.	Functional	Desired	IAM Team	Approved	3/25/2016	Role functionality.	
10.2.6	Integration	Go-Live	TIM / TED system shall support integration with ServiceNow at the time of ServiceNow Go-Live.	Constraint	Critical	IAM Team	Approved	3/25/2016	Service Now Go-Live date planned for 07/12/2016.	
10.2.7	Integration	Go-Live	Identity Hub shall integrate with ServiceNow.	Constraint	Critical	IAM Team	Approved	3/25/2016	The nature of this integration will be determined in Task 5.1.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
11.0 Future Student Information System										
11.1 Inbound Interfaces										
11.1.1	Integration	Update	Identity Hub shall utilize the future Student Information System as the authoritative system for updating student identity attributes.	Functional	Critical	IAM Team	Approved	3/16/2016	Precise Attributes (such as affiliation, entitlements, etc.) will be derived during detailed requirement gathering (Task 5.1). Dependent upon Student Information Systems replacement project.	
11.1.2	Integration	Go-Live	Identity Hub shall support the Go-live of the future Student Information System.	Constraint	Critical	LWA Project	Approved	3/8/2016	Go-Live date TBD dependent upon Student Information Systems replacement project.	
12.0 Identity Hub Internal Processes										
12.1 Processes										
12.1.1	Integration	Read	SailPoint IIQ shall read TIM data.	Functional	Important	IAM Team	Approved	3/9/2016	Additional requirements for Identity Hub Internal Processes 12.0 will be defined in Tasks 4.2, 5, 6 and Phase 2.	
12.1.2	Integration	Read	TIM shall read SailPoint IIQ data.	Functional	Critical	IAM Team	Approved	3/9/2016	Additional requirements for Identity Hub Processes 12.0 will be defined in Tasks 4.2, 5, 6 and Phase 2.	
12.1.3	Integration	Go-Live	SailPoint IIQ shall be capable of running concurrently with Legacy IAM systems.	Constraint	Critical	IAM Team	Approved	3/16/2016		
12.1.4	Integration	EID History	Identity Hub shall retain EID attribute history.	Functional	Critical	IAM Team	Approved	3/29/2016	Investigate how this will be handled in SailPoint IIQ as part of 4.2.	
12.1.5	Integration	EID History	Identity Hub shall retain actor history for the author of changes to EID attributes.	Functional	Critical	IAM Team	Approved	3/29/2016	Investigate how this will be handled in SailPoint IIQ as part of 4.2.	
12.1.6	Integration	Merge	Identity Hub shall be able to receive requests to merge Person EID accounts.	Functional	Critical	IAM Team	Approved	3/29/2016	Merge process must enforce business rules and be capable of interacting real-time with systems of record (SORs) to verify merge eligibility. The non-surviving identities must be maintained in an inactive state, but shall not be available for use (other than historical reporting).	
12.1.7	Integration	Unmerge	Identity Hub shall be able to receive requests to unmerge Person EID accounts.	Functional	Desired	IAM Team	Approved	3/29/2016		
13.0 Merge and Change Process										
13.1 Outbound Interfaces										
13.1.1	Integration	Merge	Identity Hub shall provide EID merge information to a non-mainframe EID Merge notification list.	Functional	Critical	CW Belcher	Approved	5/19/2016	Suggested destination: RabbitMQ operated by the MCA team.	
14.0 Information Security Office (ISO)										
14.1 Inbound Interfaces										
14.1.1	Integration	Lock	Identity Hub shall receive requests to lock EIDs from ISO.	Functional	Critical	IAM Team	Approved	3/28/2016		
14.1.2	Integration	Unlock	Identity Hub shall receive requests to unlock EIDs from ISO.	Functional	Critical	IAM Team	Approved	3/28/2016		
14.1.3	Integration	Disable	Identity Hub shall receive requests to disable EIDs from ISO.	Functional	Desired	IAM Team	Approved	3/28/2016	In Task 5.1, determine the implementation of lock / disabled types desired by ISO.	
14.1.4	Integration	Bulk Lock / Unlock	Identity Hub shall process bulk lock or unlock requests from ISO.	Functional	Critical	IAM Team	Approved	3/29/2016		
15.0 Data Model Modernization										
15.1 Person EIDs										
15.1.1 Student										
15.1.1.1	Integration	Data Model Modernization	Identity Hub shall be the source for Student Person EID identifier information.	Functional	Critical	IAM Team	Approved	4/6/2016	Identifier information as described in the TED schema.	
15.1.1.2	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID name information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Name information as described in the TED schema.	
15.1.1.3	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID association information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Association information as described in the TED schema.	
15.1.1.4	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID student information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Student information as described in the TED schema.	
15.1.1.5	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID address information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Address information as described in the TED schema.	
15.1.1.6	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID telephone information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Telephone information as described in the TED schema.	
15.1.1.7	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Student Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/6/2016	Credentials information as described in the TED schema.	
15.1.1.8	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Student Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/6/2016	Credentials information as described in the TED schema.	
15.1.1.9	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Student Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/6/2016	Credentials information as described in the TED schema.	
15.1.1.10	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Student Information System as a source for Student Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Name information as described in the TED schema. Credentials information as described in the TED schema.	
15.1.1.11	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Student Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/6/2016	Entitlement information as described in the TED schema.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
15.1.1.12	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Student Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/6/2016	Entitlement information as described in the TED schema.	
15.1.1.13	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Student Information System as a source for Student Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Entitlement information as described in the TED schema.	
15.1.1.14	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Student Information System as the source for Student Person EID restrictions information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. Restrictions information as described in the TED schema.	
15.1.1.15	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Student Information System as a source for Student Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. "Other" information as described in the TED schema.	
15.1.1.16	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Student Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/6/2016	Future Student Information System data attributes will be determined as part of the SIS vendor implementation. "Other" information as described in the TED schema.	
15.1.1.17	Integration	Data Model Modernization	Identity Hub shall associate a Student Person EID with an external identity from Lightweight Authentication consuming systems.	Functional	Desired	LWA Project	Approved	5/25/2016	In some cases people with external identities will also have an internal identity and we need some way to associate them.	
15.1.2 Employee										
15.1.2.1	Integration	Data Model Modernization	Identity Hub shall be the source for Employee Person EID identifier information.	Functional	Critical	IAM Team	Approved	4/7/2016	Identifier information as described in the TED schema.	
15.1.2.2	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID name information.	Functional	Critical	IAM Team	Approved	4/7/2016	Name information as described in the TED schema. Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.3	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID name information.	Functional	Critical	IAM Team	Approved	4/7/2016	Name information as described in the TED . Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.4	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID association information.	Functional	Critical	IAM Team	Approved	4/7/2016	Association information as described in the TED schema.	
15.1.2.5	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID association information.	Functional	Critical	IAM Team	Approved	4/7/2016	Association information as described in the TED schema. Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.6	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID employee information.	Functional	Critical	IAM Team	Approved	4/7/2016	Employee information as described in the TED schema.	
15.1.2.7	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID employee information.	Functional	Critical	IAM Team	Approved	4/7/2016	Employee information as described in the TED schema. Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.8	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID address information.	Functional	Critical	IAM Team	Approved	4/7/2016	Address information as described in the TED schema.	
15.1.2.9	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID address information.	Functional	Critical	IAM Team	Approved	4/7/2016	Address information as described in the TED . Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.10	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID telephone information.	Functional	Critical	IAM Team	Approved	4/7/2016	Telephone information as described in the TED schema.	
15.1.2.11	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID telephone information.	Functional	Critical	IAM Team	Approved	4/7/2016	Telephone information as described in the TED schema.	
15.1.2.12	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Employee Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/7/2016	Credentials information as described in the TED schema.	
15.1.2.13	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Employee Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/7/2016	Credentials information as described in the TED schema.	
15.1.2.14	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Employee Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/7/2016	Credentials information as described in the TED schema.	
15.1.2.15	Integration	Data Model Modernization	Identity Hub shall utilize Workday employee information as a source to determine Person EID authentication status.	Functional	Critical	IAM Team	Approved	4/7/2016	Use Case: When a termination is initiated in Workday, the terminated worker's authentication will be locked in some systems, such as Active Directory, but not all systems. Timing dependent on Workday Go-Live.	
15.1.2.16	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Employee Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/7/2016	Entitlement information as described in the TED schema.	
15.1.2.17	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Employee Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/7/2016	Entitlement information as described in the TED schema.	
15.1.2.18	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe HR system as a source for Employee Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/7/2016	Entitlement information as described in the TED. Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.19	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as the source for Employee Person EID restrictions information.	Functional	Critical	IAM Team	Approved	4/7/2016	Workday was evaluating how restrictions will be implemented as of 04/21/16. Transition of authoritative source dependent on Workday Go-Live. Restriction information as described in the TED schema.	
15.1.2.20	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe OHSC system as the source for Employee Person EID roles information.	Functional	Critical	IAM Team	Approved	4/7/2016	Roles information as described in the TED schema.	
15.1.2.21	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe HR system as a source for Employee Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/6/2016	"Other" information as described in the TED schema. Transition of authoritative source dependent on Workday Go-Live.	
15.1.2.22	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Employee Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/6/2016	"Other" information as described in the TED schema.	
15.1.2.23	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Person Employee department information.	Functional	Critical	IAM Team	Approved	5/25/2016	Department information is similar to Org unit information from Workday, and is distinctly separately from Department EIDs. Department information is being called out as a requirement, because the business processes and treatment of department information are potentially changing. The nature of this change will be investigated as part of Task 4.2	
15.1.2.24	Integration	Data Model Modernization	Identity Hub shall associate a Employee Person EID with an external identity from Lightweight Authentication consuming systems.	Functional	Desired	LWA Project	Approved	5/25/2016	In some cases people with external identities will also have an internal identity and we need some way to associate them.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
15.1.5 Guest (Unaffiliated)										
15.1.5.1	Integration	Data Model Modernization	Identity Hub shall be the source for Unaffiliated Guest Person EID identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema.	
15.1.5.2	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface and a Self Service portal as a source for Unaffiliated Guest Person EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	
15.1.5.3	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Unaffiliated Guest Person EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	
15.1.5.4	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Unaffiliated Guest Person EID address information.	Functional	Critical	IAM Team	Approved	4/11/2016	Address information as described in the TED schema.	
15.1.5.5	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Unaffiliated Guest Person EID address information.	Functional	Critical	IAM Team	Approved	4/11/2016	Address information as described in the TED schema.	
15.1.5.6	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Unaffiliated Guest Person EID telephone information.	Functional	Critical	IAM Team	Approved	4/11/2016	Telephone information as described in the TED schema.	
15.1.5.7	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Unaffiliated Guest Person EID telephone information.	Functional	Critical	IAM Team	Approved	4/11/2016	Telephone information as described in the TED schema.	
15.1.5.8	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Unaffiliated Guest Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/11/2016	Credentials information as described in the TED schema.	
15.1.5.9	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Unaffiliated Guest Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/11/2016	Credentials information as described in the TED schema.	
15.1.5.10	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Unaffiliated Guest Person EID credentials information.	Functional	Critical	IAM Team	Approved	4/11/2016	Credentials information as described in the TED schema.	
15.1.5.11	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Unaffiliated Guest Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/11/2016	Entitlement information as described in the TED schema.	
15.1.5.12	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Unaffiliated Guest Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/11/2016	Entitlement information as described in the TED schema.	
15.1.5.13	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Applications as a source for Unaffiliated Guest Person EID entitlement information.	Functional	Critical	IAM Team	Approved	4/11/2016	Entitlement information as described in the TED schema.	
15.1.5.14	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Unaffiliated Guest Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.1.5.15	Integration	Data Model Modernization	Identity Hub shall utilize a Self Service portal as a source for Unaffiliated Guest Person EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.1.6 External Identities										
15.1.6.1	Integration	Data Model Modernization	Identity Hub shall utilize the Lightweight Authentication System as the source for external identity identifier information.	Functional	Desired	IAM Team	Approved	5/25/2016	utexasEduPersonEid and utexasEduPersonUn and unique identifier from the Lightweight system. More information about this unique identifier or whether existing EID space will be used will be determined as part of Task 5.	
15.1.6.2	Integration	Data Model Modernization	Identity Hub shall utilize the Lightweight Authentication System as the source for external identity name information.	Functional	Desired	IAM Team	Approved	5/25/2016	all name attributes	
15.1.6.3	Integration	Data Model Modernization	Identity Hub shall utilize the Lightweight Authentication System as the source for external identity address information.	Functional	Desired	IAM Team	Approved	5/25/2016	Email Only	
15.1.6.4	Integration	Data Model Modernization	Identity Hub shall utilize the Lightweight Authentication System as the source for external identity other information.	Functional	Desired	IAM Team	Approved	5/25/2016	entitlement, birthdate, test record switch	
15.2 Non-Person EIDs										
15.2.1 Business EIDs										
Note:	As part of the Data Model modernization, deliverable 1.5 will define a communication plan that addresses changes to Business EIDs.									
15.2.1.1	Integration	Data Model Modernization	Identity Hub shall be the source for Business identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema.	
15.2.1.2	Integration	Data Model Modernization	Identity Hub shall utilize Finance Mainframe Applications as a source for Business EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	
15.2.1.3	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for business and vendor name information.	Functional	Critical	Finance	Approved	5/26/2016	Name information as described in the TED schema. Don Simpson of Finance says a Workday addon will be created to initiate the creation and update of Business EIDs.	
15.2.1.4	Integration	Data Model Modernization	Identity Hub shall utilize Finance Mainframe Applications as the source for Business EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Association information as described in the TED schema.	
15.2.1.5	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for business and vendor association information.	Functional	Critical	Finance	Approved	5/26/2016	Association information as described in the TED schema. Don Simpson of Finance says a Workday addon will be created to initiate the creation and update of Business EIDs.	
15.2.1.6	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for Business EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.1.7	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for business and vendor "other" information.	Functional	Critical	Finance	Approved	5/26/2016	"Other" information as described in the TED schema. Don Simpson of Finance says a Workday addon will be created to initiate the creation and update of Business EIDs.	
15.2.2 Groups EIDs										
Note:	As part of the Data Model modernization, deliverable 1.5 will define a communication plan that addresses changes to Group EIDs.									KPMG advises keeping the existing group structures, but divorcing it from the identity name-space.
15.2.2.1	Integration	Data Model Modernization	Identity Hub shall be the source for Group identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	An investigation is required as part of task 4.2 to determine if Groups can be represented without EIDs as a unique identifier. Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Identifier information as described in the TED schema.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
15.2.2.2	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Group EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Name information as described in the TED schema.	
15.2.2.3	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Applications as a source for Group EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Name information as described in the TED schema.	
15.2.2.4	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Group EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Association information as described in the TED schema.	
15.2.2.5	Integration	Data Model Modernization	Identity Hub shall utilize Mainframe Applications as a source for Group EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Association information as described in the TED schema.	
15.2.2.6	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as the source for Role information pertaining to Group EIDs.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. Roles information as described in the TED schema.	
15.2.2.7	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for Group EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	Phase 0 Group EID will be utilized by Sailpoint IIQ Roles. "Other" information as described in the TED schema.	
15.2.3 Service EIDs										
Note:	The desired creation process of a Service EID is related to requirement 10.1.6. Use Case: Service Now facilitates the request fulfillment process to create a new Service EID. This will be a 1 time process per Service EID created. This request process from Service Now will include the service name, owner, and owner's department.								Process agreed upon by Service Now represented Ruby Phillipose.	
15.2.3.1	Integration	Data Model Modernization	Identity Hub shall be the source for Service EID identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema.	
15.2.3.2	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for Service EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	
15.2.3.3	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a single use source for Service EID name information when creating a new Service EID.	Functional	Desired	IAM Team	Approved	6/2/2016	Related to requirement 10.1.6. Use Case: Service Now facilitates the request fulfillment process to create a new Service EID. This will be a 1 time process per EID created. This request process will include the service name represented as name information.	
15.2.3.4	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for Service EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Association information as described in the TED schema.	
15.2.3.5	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a single use source for Service EID association information when creating a new Service EID.	Functional	Desired	IAM Team	Approved	6/2/2016	Related to requirement 10.1.6. Use Case: Service Now facilitates the request fulfillment process to create a new Service EID. This will be a 1 time process per EID created. This request process will include the responsible party represented as association information.	
15.2.3.6	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for Service EID credentials information.	Functional	Critical	IAM Team	Approved	4/11/2016	Credentials information as described in the TED schema.	
15.2.3.7	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Service EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.3.8	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Acceptable Use Policy Application as a source for Service EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.4 Department EIDs										
Note:	As part of the Data Model modernization, deliverable 1.5 will define a communication plan that addresses changes to Department EIDs.								Information about Department EIDs will be sourced from Workday after the Workday go-live. The translation of the Department EID identifier from Supervisory Org information in Workday may have to be performed by the Identity Hub. The nature of this change will be investigated as part of Task 4.2.	
15.2.4.1	Integration	Data Model Modernization	Identity Hub shall be a source for Department identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema. Dependent upon Workday.	
15.2.4.2	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as a source for Department EID identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema. Dependent upon Workday.	
15.2.4.3	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as a source for Department EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	
15.2.4.4	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Department EID name information.	Functional	Critical	IAM Team	Approved	5/24/2016	Name information as described in the TED schema.	
15.2.4.5	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as the source for Department EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Association information as described in the TED schema.	
15.2.4.6	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Department EID association information.	Functional	Critical	IAM Team	Approved	5/24/2016	Association information as described in the TED schema.	
15.2.4.7	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as the source for Department EID address information.	Functional	Critical	IAM Team	Approved	4/11/2016	Address information as described in the TED schema.	
15.2.4.8	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Department EID address information.	Functional	Critical	IAM Team	Approved	5/24/2016	Address information as described in the TED schema.	
15.2.4.9	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as the source for Department EID telephone information.	Functional	Critical	IAM Team	Approved	4/11/2016	Telephone information as described in the TED schema.	
15.2.4.10	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Department EID telephone information.	Functional	Critical	IAM Team	Approved	5/24/2016	Telephone information as described in the TED schema.	
15.2.4.11	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Department EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.4.12	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System as a source for Department EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.4.13	Integration	Data Model Modernization	Identity Hub shall utilize Workday as a source for Department EID "other" information.	Functional	Critical	IAM Team	Approved	5/24/2016	"Other" information as described in the TED schema.	
15.2.5 ID Only EIDs										
15.2.5.1	Integration	Data Model Modernization	Identity Hub shall be the source for ID Only identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
15.2.5.2	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as the source for ID Only EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.6 Device EIDs										
Note:	As part of the Data Model Modernization, deliverable 1.5 will define a communication plan that addresses the creation of Device EIDs.									
Note:	The desired creation process of a Device EID is related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process from Service Now will include the device name, owner, owner's department, necessary entitlements, physical location, MAC address and serial number.								Process agreed upon by Service Now represented Ruby Phillipose.	
15.2.6.1	Integration	Data Model Modernization	Identity Hub shall be the source for Device EID identifier information.	Functional	Desired	IAM Team	Approved	5/24/2016	Identifier information as described in the TED schema.	
15.2.6.2	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID name information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the device name represented as name information.	
15.2.6.3	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative Interface as a source for Device EID name information.	Functional	Desired	IAM Team	Approved	5/24/2016	Name information as described in the TED schema.	
15.2.6.4	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID association information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the device owner represented as association information.	
15.2.6.5	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Device EID association information.	Functional	Desired	IAM Team	Approved	5/24/2016	Association information as described in the TED schema. Member and Owner specifically.	
15.2.6.6	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as the source for Device EID department information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the device owner's department represented as department information.	
15.2.6.7	Integration	Data Model Modernization	Identity Hub shall utilize Administrative interface as the source for Device EID credentials information.	Functional	Desired	IAM Team	Approved	5/24/2016	Credentials information as described in the TED schema.	
15.2.6.8	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Acceptable Use Policy Application as a source for Device EID "other" information.	Functional	Desired	IAM Team	Approved	5/24/2016	"Other" information as described in the TED schema.	
15.2.6.9	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID entitlement information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the wifi entitlement if necessary.	
15.2.6.10	Integration	Data Model Modernization	Identity Hub shall utilize a REST interface as a source for Device EID entitlement information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the wifi entitlement if necessary.	
15.2.6.11	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Device entitlement information.	Functional	Desired	IAM Team	Approved	5/24/2016	Entitlement information as described in the TED schema.	
15.2.6.12	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative Interface as a source for Device EID address information.	Functional	Desired	IAM Team	Approved	5/24/2016	Address information as described in the TED schema.	
15.2.6.13	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID address information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the physical location of the device represented as address information.	
15.2.6.14	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID MAC address attribute information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the MAC address. MAC address attribute is a new attribute that is unsupported by TIM or TED at the beginning of IAMMP. This new attribute will have to be added to support Device EIDs.	
15.2.6.15	Integration	Data Model Modernization	Identity Hub shall utilize Service Now as a source for Device EID Serial number attribute information.	Functional	Desired	IAM Team	Approved	5/24/2016	Related to requirement 10.1.7. Use Case: Service Now facilitates the request fulfillment process to create a new Device EID. This will be a 1 time process per Device EID created. This request process will include the device serial number. Serial number attribute is a new attribute that is unsupported by TIM or TED at the beginning of IAMMP. This new attribute will have to be added to support Device EIDs.	
15.2.7 Role EIDs										
Note:	As part of the Data Model Modernization, deliverable 1.5 will define a communication plan that addresses changes to Role EIDs. Whether or not Role EIDs will be deprecated and the timing will be addressed in Task 4.2.								Role EIDs are a subset of Group EIDs. For Group EIDs, KPMG advises keeping the existing group structures, but divorcing it from the identity name-space. For Role EIDs, Task 6 should define which existing Role EIDs should be modeled as Sailpoint IIQ Roles and which should be transitioned to Groups. The results of this investigation will have to be part of Task 6 implementation and communication.	
15.2.7.1	Integration	Data Model Modernization	Identity Hub shall be the source for Role EID identifier information.	Functional	Critical	IAM Team	Approved	4/11/2016	Identifier information as described in the TED schema.	
15.2.7.2	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System Contacts system as the source for Role EID name information.	Functional	Critical	IAM Team	Approved	4/11/2016	Name information as described in the TED schema.	

IAMMP Task 4.1 Interface and Data Transition Strategy Requirements										
ID	Category	Business Process	Requirement	Requirement Type	Priority	Source	Req. Status	Creation Date	Notes	Rollout Phase
15.2.7.3	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System Contacts system as the source for Role EID association information.	Functional	Critical	IAM Team	Approved	4/11/2016	Association information as described in the TED schema.	
15.2.7.4	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System Contacts system as the source for Role EID roles information.	Functional	Critical	IAM Team	Approved	4/11/2016	Roles information as described in the TED schema.	
15.2.7.5	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Role EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.2.7.6	Integration	Data Model Modernization	Identity Hub shall utilize the Mainframe Organizational Hierarchy System Contacts system as a source for Role EID "other" information.	Functional	Critical	IAM Team	Approved	4/11/2016	"Other" information as described in the TED schema.	
15.3	Sailpoint IIQ Roles									
15.3.1	Integration	Data Model Modernization	Identity Hub shall be the source for Sailpoint IIQ Role identifier information.	Functional	Desired	IAM Team	Approved	5/25/2016	A unique identifier is required. More information about this unique identifier or whether existing EID space will be used will be determined as part of Task 5.	
15.3.2	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Sailpoint IIQ Role name information.	Functional	Desired	IAM Team	Approved	5/25/2016	Name information as described in the TED schema. Specifically: CN, commonName.	
15.3.3	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Sailpoint IIQ Role description.	Functional	Desired	IAM Team	Approved	5/25/2016	Description information as described in the TED schema. Specifically: CN, commonName.	
15.3.4	Integration	Data Model Modernization	Identity Hub shall utilize an Administrative interface as a source for Sailpoint IIQ Role association information.	Functional	Desired	IAM Team	Approved	5/25/2016	Association information as described in the TED schema. Specifically: owner, member(s).	
15.4	Miscellaneous									
15.4.1	Integration	Data Model Modernization	Identity Hub shall represent lock types.	Functional	Critical	IAM Team	Approved	3/29/2016		
15.4.2	Integration	Data Model Modernization	Identity Hub shall account for current day "EID Contact" functionality.	Functional	Critical	IAM Team	Approved	3/29/2016		

IAMMP Interface and Data Transition Strategy Requirements Revision History

All changes to the requirements and traceability matrix should be documented.

As a general guideline, major versions should be used when requirements are added, removed, or significantly altered. Minor versions may be used for updates to the traceability matrix alone or minor changes to requirement wordings, etc.

Version	Date	Updater Name	Description
Template	3/8/2016	Greg Heidner	Initial approved template created.
V0.1	4/22/2016	Josh Kinney	Draft submission of deliverable.
V0.2	5/29/2016	Josh Kinney	Updated draft submitted for sponsor review.
V1	6/3/2016	Josh Kinney	Finalized draft submitted for sponsor review.
FINAL	6/3/2016	Marta Lang	Executive Sponsor sign off of deliverable.

PLAN

REQUIREMENTS

SOLUTION
ANALYSIS

DESIGN

BUILD

TEST

TRAIN/DEPLOY

MAINTENANCE

Use Case

1.0 Use Case Name

Allow directory services customers to connect via REST and SOAP.

2.0 Use Case ID

DSR-UC1

3.0 Objective

Currently, customers must connect to the uTexas Enterprise Directory (TED) using LDAP. Due to the mainframe retirement and the Administrative Systems Modernization Program (ASMP 2.0) a number of customers are transitioning to new products and services which prefer to make web services calls for their queries. Customers are specifically interested in REST (Representational State Transfer) and SOAP (Simple Object Access Protocol), with REST being in higher demand.

4.0 Scope

4.1 In scope

Customers should be able to make a query of directory services using REST and/or SOAP and receive the results and attributes to which they are entitled, as they current do with an LDAP Query to TED.

This use case has been developed as part of the Directory Services Roadmap effort and the adoption of a new directory services technology stack is considered in scope for this use case.

4.2 Out of Scope

Changes to access groups, the records and attributes available to those access groups, and the members of said access groups is out of scope of this use case.

5.0 Actors

5.1 Primary

Directory services customers

5.2 Secondary

Directory services administrators
Identity and Access Management Team

6.0 Pre-conditions

User must be authorized to query directory services, and must be authorized for the records and attributes which they are querying.

7.0 Post conditions

Authorized user is able to query directory services and receive the results of that query using REST and/or SOAP.

8.0 Triggers

User queries directory services using REST and/or SOAP.

9.0 Assumptions and Dependencies

Standard environmental assumptions apply – availability of server, service, network, power, etc.

10.0 Terms and Abbreviations

Term	Definition
REST	Representational State Transfer
SOAP	Simple Object Access Protocol

11.0 Process Diagrams and Steps

11.1 Normal

1. User submits a query to directory services using REST/SOAP.
2. Directory services confirms user’s authorization to make the query.
3. Directory services returns the results and attributes queried for which the user is authorized.

11.2 Exceptions

1. User submits a query to directory services using REST/SOAP.
2. Directory services notes that user is not authorized to make the query.
3. Directory services returns an appropriate error message.

11.3 Variations

Enter any data entry or technology variations e.g, different methods of data input, screen/module invocation, browser versions, etc.

12.0 Requirements

The table below should include the requirements that are addressed in this use case.

ID	Description

13.0 Operational Impact

Implementation of this use case should result in no impact to services upon which directory services depends (uTexas Identity Manager) or which are dependent on directory services.

14.0 Stakeholders

Identity and Access Management Committee (governance committee)

Mulesoft project team

IAM Sailpoint implementation team

15.0 Issues

List any issues associated with this use case. For example, a known defect in the selected software that is expected to be fixed by the vendor but not does not have a scheduled release.

Revision History

Version	Date	Updater Name	Description
V 0.1	5/10/2016	Aaron Reiser	Initial draft completed.

PLAN

REQUIREMENTS

SOLUTION
ANALYSIS

DESIGN

BUILD

TEST

TRAIN/DEPLOY

MAINTENANCE

Use Case

1.0 Use Case Name

Allow users to subscribe to attribute updates, such as through persistent searches.

2.0 Use Case ID

DSR-UC2

3.0 Objective

Customers wish to receive updates to values of attributes within directory services. This objective may be met in one or more ways. For real-time or near-real time updates, directory services should allow for persistent searches. For consumers which do not require near-real-time updates, they would like to be able to subscribe to update notifications.

4.0 Scope

4.1 In scope

Directory services customers may require updates about both person and non-person identities.

This use case has been developed as part of the Directory Services Roadmap effort and the adoption of a new directory services technology stack is considered in scope for this use case.

4.2 Out of Scope

Directory services will not gratuitously inform an ESB of record changes.

5.0 Actors

5.1 Primary

Directory services customers

5.2 Secondary

Directory services administrators
Identity and Access Management Team

6.0 Pre-conditions

User must be authorized to query directory services, and must be authorized for the records and attributes which they are querying.

User must have a client capable of performing persistent searches.

7.0 Post conditions

User establishes and maintains connection to directory services.

8.0 Triggers

User connects with the appropriate flag to indicate that they wish to establish a persistent search.

9.0 Assumptions and Dependencies

This use case assumes an updated directory services technology stack as part of the Directory Services Roadmap.

Standard environmental assumptions apply – availability of server, service, network, power, etc.

Upon the termination of a persistent directory services connection, it will be the client’s responsibility to re-establish the connection. This will also apply to maintenance events.

10.0 Terms and Abbreviations

Term	Definition
LDAP	Lightweight Directory Access Protocol
Non-persistent search	A one-time search operation in LDAP in which the client is disconnected from the server after receiving the results of their search operation.
Persistent search	A mechanism which extends the LDAP search operation with the ability to track changes in the directory. The client remains connected to the server after the “normal” search operation is finished and the server provides additional results as data in the directory changes.

11.0 Process Diagrams and Steps

11.1 Normal

1. User submits a query to directory services with a flag that indicates the query should be persistent.
2. Directory services confirms user’s authorization to make the query.
3. Directory services returns the results and attributes queries for which the user is authorized, while the connection persists.

11.2 Exceptions

1. User submits a query to directory services with a flag that indicates the query should be persistent.
2. Directory services notes that user is not authorized to make the query.
3. Directory services returns an appropriate error message.

11.3 Variations

Enter any data entry or technology variations e.g, different methods of data input, screen/module invocation, browser versions, etc.

12.0 Requirements

The table below should include the requirements that are addressed in this use case.

ID	Description

13.0 Operational Impact

Implementation of this use case should result in no impact to services upon which directory services depends (uTexas Identity Manager) or which are dependent on directory services.

Enabling persistent searching on directory services will increase the number of active network connections to directory services, and may also increase CPU load.

14.0 Stakeholders

Identity and Access Management Committee (governance committee)

ServiceNow

15.0 Issues

It is unclear how the system will handle a change in client authorization while a directory services connection persists.

We need to investigate provisioning of authorization to perform persistent searches due to potential service impact.

Revision History

Version	Date	Updater Name	Description
V 0.1	5/10/2016	Aaron Reiser	Initial draft completed.

PLAN

REQUIREMENTS

SOLUTION
ANALYSIS

DESIGN

BUILD

TEST

TRAIN/DEPLOY

MAINTENANCE

Use Case

1.0 Use Case Name

Allow directory services customers to append attributes to directory entries.

2.0 Use Case ID

DSR-UC3

3.0 Objective

Current customers of directory services have need of maintaining records which primarily consist of attributes available in the centralized enterprise directory, but also consist of attributes of value to their Customer Service Unit (CSU). Currently, this is accomplished by the customers maintaining their own “shadow database” within their own CSU.

4.0 Scope

4.1 In scope

Giving authorized directory services customers write access to aspects of directory records.

4.2 Out of Scope

Allowing customers to modify attributes for which they are not the official System of Record.

Customers will not be allowed to create arbitrary or new records.

5.0 Actors

5.1 Primary

Directory services customers

5.2 Secondary

Directory services administrators
Identity and Access Management Team

6.0 Pre-conditions

User must be authorized to query directory services, and must be authorized for the records and attributes which they are writing and querying.

7.0 Post conditions

User is able to write/modify attributes for existing records for which they are authorized.

8.0 Triggers

List the event(s) that start this Use Case, e.g., User accesses application.

9.0 Assumptions and Dependencies

This use case assumes an updated directory services technology stack as part of the Directory Services Roadmap.

Standard environmental assumptions apply – availability of server, service, network, power, etc.

10.0 Terms and Abbreviations

List common terms that will be used in this Use Case. If common terms are defined project-wide, provide a link to the appropriate documentation.

Term	Definition

11.0 Process Diagrams and Steps

11.1 Normal

List the main flow of events, step-by-step, i.e., describe the straight and simple path where everything goes as expected and enables the primary actor to accomplish his or her goal. Main flow/path should always end with a success end condition.

1. Precise methodology dependent upon technology selected and implemented by the Directory Services technology refresh.

11.2 Exceptions

List the exceptions of the main flow, step-by-step. These exceptions address deviations from the main path, such as errors.

1. Dependent upon technology selected and implemented by the Directory Services technology refresh and normal operating procedures.

11.3 Variations

Enter any data entry or technology variations e.g, different methods of data input, screen/module invocation, browser versions, etc.

12.0 Requirements

The table below should include the requirements that are addressed in this use case.

ID	Description

13.0 Operational Impact

Implementation of this use case should result in no impact to services upon which directory services depends (uTexas Identity Manager) or which are dependent on directory services.

Implementation of this use case requires a significant number of additional personnel to support the service (e.g. creating and maintaining attribute addition policies, fielding requests for additional attributes, maintaining ownership records for custom attributes, managing policies and procedures around decommissioning custom attributes, etc.).

Auditing of changes to directory records becomes significantly more complicated.

14.0 Stakeholders

Identity and Access Management Committee (governance committee)

15.0 Issues

There are multiple technological approaches to solutions for this use case, though their implementation vary dramatically.

Increased complexity of access controls increases the attack surface with regard to restricted data.

Need to determine scope of attribute access for customers to prevent write collisions (both from a technical and a policy perspective).

A significant increase in record attributes as well as a significant increase in write activity run the risk of significantly impacting directory services performance.

The potential extreme increase in record attributes presents a usability challenge for record consumers.

Revision History

Version	Date	Updater Name	Description
V 0.1	5/10/2016	Aaron Reiser	Initial draft completed.

