FEBRUARY 2025

IAM ROADMAP QUARTERLY REVIEW

The review of the IAM Roadmap for Q2, FY 2024-2025

MARTA LANG
Senior IT Manager, IAM Team Lead, The University of Texas at Austin

Key Roadmap Priorities

- Identity Governance & Administration (IGA): Modernize tools, reduce technical debt

- Authentication: Continuous improvement

- Directory Services: Unify platforms

- Knowledge building: AWS technologies

IGA Initiatives

FY 2024-2025	Q1	Q2	Q3
Initiative 1: Improve password security with new hash	*(On hold due to resource constraints.)*	*(On hold due to resource constraints.)*	*(On hold due to resource constraints.)*
Initiative 2: Reduce technical debt by modernizing tools (IGA Modernization Program)	✓ Complete midPoint and Grouper upgrades. ✓ Complete regression testing for upgrades.	✓ Monitor and debug performance issue(s) internally and with vendors, Unicon and Evolveum. ✓ Reassess and test architecture for midPoint to optimize performance and cost. ✓ Automate minimum testing checklists for midPoint and Grouper.	❑ Complete upgrade to midPoint 4.8.7, which contains performance defect fixes. ❑ Monitor midPoint performance. ❑ Implement architecture changes to optimize performance and cost. ❑ Revisit project schedule for cutover from SailPoint IdentityIQ to midPoint. ❑ Plan external communications about upcoming changes. ❑ Reassess and reconnect Phase 2 connectors (e.g. Workday, etc). ❑ Revisit security, functional, and non-functional testing and remediate issues for Phase 2.
Initiative 3: Right size data retention with identity lifecycles	✓ Monitor Youth Protection Program affiliations usage. ✓ Process request for new affiliations for Mccomb's Texas Executive Education (TEE) program.	✓ Complete internal development, testing, and release of the new affiliations for TEE program. ✓ Support TEE testing, as needed.	❑ Support TEE testing, as needed. ❑ Process request for new affiliations for Dell Medical Center.

IGA Initiatives

FY 2024-2025	Q4	FY 2025-2026 Q1	Q2 and beyond
Initiative 1: Improve password security with new hash	❑ Complete analysis and determine approach for transition of TED & FI/ST mainframe authentication to new hash.	❑ Begin transition of TED & FI/ST mainframe authentication to new hash.	❑ Complete transition of TED & FI/ST mainframe authentication to new hash. ❑ Retire old hashes and purge hash history.
Initiative 2: Reduce technical debt by modernizing tools (IGA Modernization Program)	❑ Complete Phase 2 connectors (e.g. Workday, etc). ❑ Begin security, functional, and non-functional testing, and remediate issues for Phase 2. ❑ Begin testing with Workday and UT System teams. ❑ Begin external communications about upcoming changes.	❑ Complete security, functional, and non-functional testing and remediate issues for Phase 2. ❑ Complete testing with Workday and UT System teams. ❑ Complete external communications about upcoming changes. ❑ Plan and complete service planning for Enterprise Identity Manager (midPoint). ❑ Complete Phase 2 Go Live. ❑ Monitor systems after transition – hyper care.	❑ Retire SailPoint IdentityIQ service. ❑ Define and finalize Phase 3 scope, charter, and project schedule. ❑ Complete Phase 3 requirements. ❑ Complete Phase 3 design(s). ❑ Complete configuration of TAP solution to meet Phase 3 requirements. ❑ Complete security, functional, and non-functional testing and remediate issues for Phase 3. ❑ Complete Phase 3 Go Live.
Initiative 3: Right size data retention with identity lifecycles	❑ Support TEE testing, as needed. ❑ Monitor usage of affiliations for TEE program.	*(Additional work to be determined based on requests.)*	*(Additional work to be determined based on requests.)*

Authentication Initiatives

FY 2024-2025	Q1	Q2	Q3
Initiative 1: Separate Guest and Enterprise SSO	✓ Onboard other early adopters. ✓ Maintain service in hyper care. ✓ Plan upgrade of core software (SimpleSAMLphp).	✓ Complete upgrade of core software (SimpleSAMLphp). ✓ Ongoing support for early adopters.	❑ Complete Service Planning. ❑ Plan build of Guest Authentication metadata manager. ❑ Ongoing support for early adopters.
Initiative 2: Continuous improvement	✓ Complete implementation of cloud native component of Enterprise Authentication. ✓ Complete upgrade of Enterprise Authentication core software. ✓ Maintain OpenID Connect functionality for early adopters.	✓ Refine OpenID Connect functionality for early adopters. ✓ Continue cloud native refactor of authentication services.	❑ Make OpenID Connect available to the university, as appropriate. ❑ Investigate OpenID Connect functionality in Entra ID. ❑ Perform Disaster Recovery test to confirm hybrid-cloud resiliency.
Initiative 3: Multi-factor authentication enhancements	✓ Coordinate preparation activities with HR, Service Desk, and Communication partners.	✓ Finalize communication plan. ✓ Begin communication campaign.	❑ Continue communication campaign. ❑ Prepare for Duo release. ❑ Release Duo availability to TEE on Tuesday, April 8, 2025. ❑ Release Duo availability to Retirees on Wednesday, April 23, 2025. ❑ Plan to enable Duo Verified Push for the Admin Panel, including communications.

Authentication Initiatives

FY 2024-2025	Q4	FY 2025-2026 Q1	Q2 and beyond
Initiative 1: Separate Guest and Enterprise SSO	❑ Release Guest Authentication for general availability and onboard customers. ❑ Build Guest Authentication metadata manager. ❑ Continue transitioning customers to Guest Authentication.	❑ Deploy Guest Authentication metadata manager. ❑ Continue transitioning customers to Guest Authentication.	❑ Continue transitioning customers to Guest Authentication.
Initiative 2: Continuous improvement	❑ Investigate strategic alignment of Shibboleth and Entra ID as identity provider(s).	❑ Assess the implementation timeframe of aligning Shibboleth and Entra ID as identity provider(s).	❑ Implement alignment plan Shibboleth and Entra ID as identity provider(s).
Initiative 3: Multi-factor authentication enhancements	❑ Monitor and support Duo for Retirees. ❑ Enable Duo Verified Push for the Admin Panel, including sending communications to impacted users. *(Additional work to be determined based on priorities and investigations.)*	❑ Investigate Duo Central Device Management transition options. *(Additional work to be determined based on priorities and investigations.)*	*(Additional work to be determined based on priorities and investigations.)*

◇ Quarterly progress check & course correction

Directory Services Initiatives

| FY 2024-2025	Q1	Q2	Q3
Initiative 1: Retire WHIPS	✓ Begin removal of WHIPS dependency from directory.utexas.edu web application.	✓ Continue removal of WHIPS dependency from directory.utexas.edu web application. ✓ Plan and start communications about implementation of new web application.	❑ Complete communications about implementation of new web application. ❑ Complete removal of WHIPS dependency from directory.utexas.edu web application.
Initiative 2: TED Cloud Resiliency	✓ Continue cloud native refactor of Directory Service services.	✓ Continue cloud native refactor of Directory Service services.	❑ Plan cloud native component of TED for updated DR/BC. ❑ Begin implementation of cloud native component of TED.

Directory Services Initiatives

FY 2024-2025	Q4	FY 2025-2026 Q1	Q2 and beyond
Initiative 1: Retire WHIPS	❑ Assess customer transition from WHIPS to uTexas Enterprise Directory (TED). ❑ Plan customer transition from WHIPS to uTexas Enterprise Directory (TED), including customer coordination.	❑ Begin customer transition from WHIPS to uTexas Enterprise Directory (TED).	❑ Complete customer transition from WHIPS to uTexas Enterprise Directory (TED). ❑ Retire and decommission WHIPS.
Initiative 2: TED Cloud Resiliency	❑ Complete implementation of cloud native component of TED. ❑ Plan perform Disaster Recovery test to confirm hybrid-cloud resiliency.	❑ Perform Disaster Recovery test to confirm hybrid-cloud resiliency. ❑ Monitor performance and service usage on cloud architecture.	❑ Monitor performance and service usage on cloud architecture.

◆ Quarterly progress check & course correction

Appendix

Current State versus Planned Future State
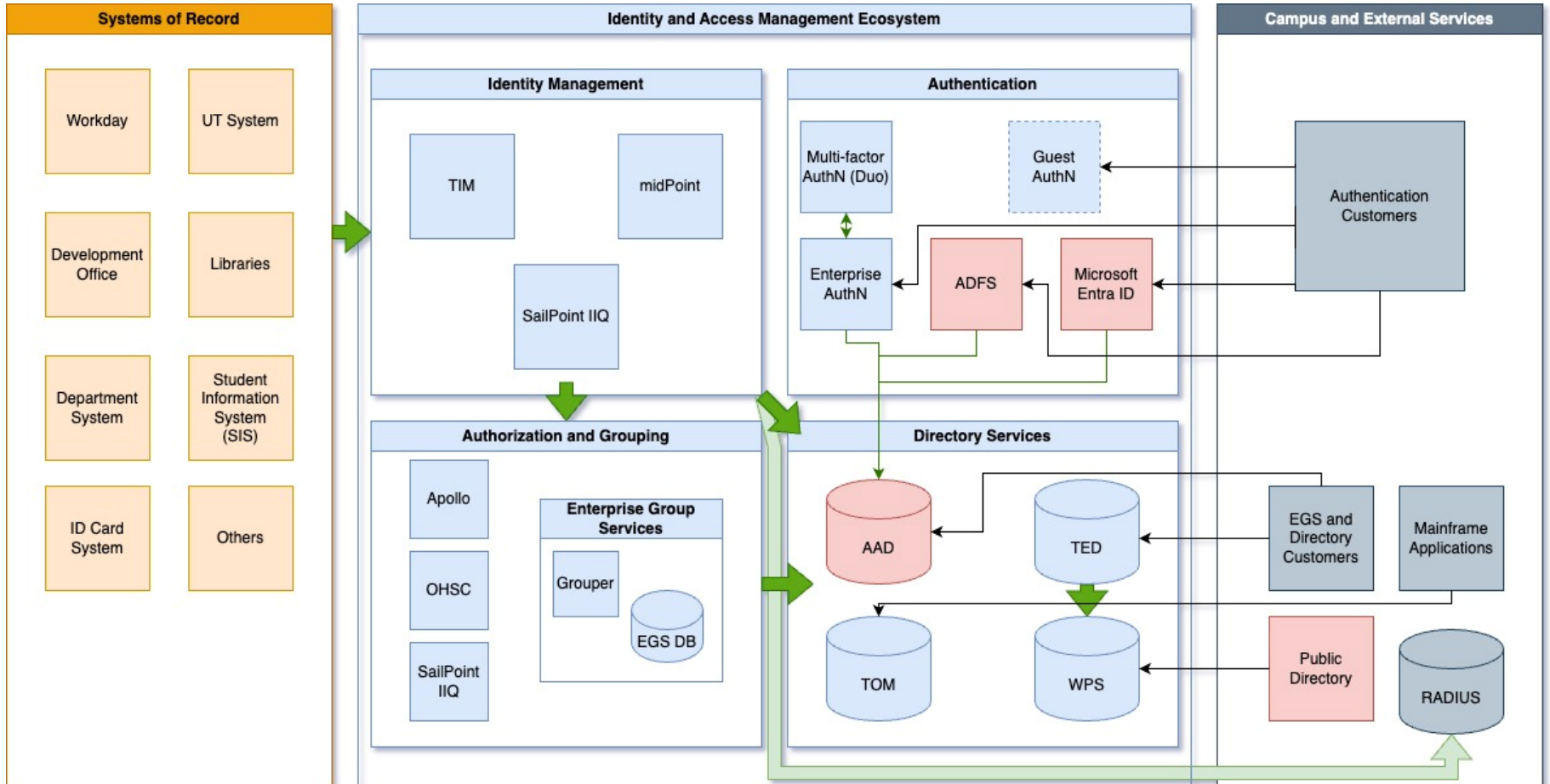
Identity Governance & Administration (IGA)

Identity Management: Current State

uTexas Identity Manager (TIM)

| Identifier Management | Identity Registry | Identity Provisioning | Password & Credential Management* |

SailPoint IdentityIQ (IIQ)

Account Registry

Microservices

Enterprise Identity Manager (midPoint)

NEW

* TIM & Duo

Identity Governance & Administration (IGA)

Identity Management: Planned Future State

uTexas Identity Manager (TIM)	SailPoint IdentityIQ (IIQ)
Retired	Retired

TIM Microservices

Identifier Management	Mainframe Broker

Enterprise Identity Manager (midPoint)

Identity Registry	Identity Provisioning	Account Registry	Password & Credential Management*

NEW

* will include Privileged Access Management

Identity Governance & Administration (IGA)

Authorization Services: Current State

SailPoint IdentityIQ (IIQ)

Group & Role Management

Authorization Reporting and Review

Legacy Authorization Management

Apollo

*DPUSER

OHSC

Custom

Identity Governance & Administration (IGA)

Authorization Services: Planned Future State

SailPoint IdentityIQ (IIQ)

Retired

Legacy Authorization Management

Apollo	*DPUSER	OHSC	Custom

Enterprise Group Services (Grouper)

Group & Role Management	Authorization Reporting and Review

NEW

Authentication

Current State

Enterprise Authentication

Web SSO
(Shibboleth)

Microsoft Authentication

AD FS**

Entra ID**

Multi-Factor Authentication (MFA)

Duo

Microsoft MFA**

Guest Authentication / Social ID

Web SSO
(SimpleSamlPHP)

NEW

Network Authentication

FreeRADIUS*

Cisco ACS*
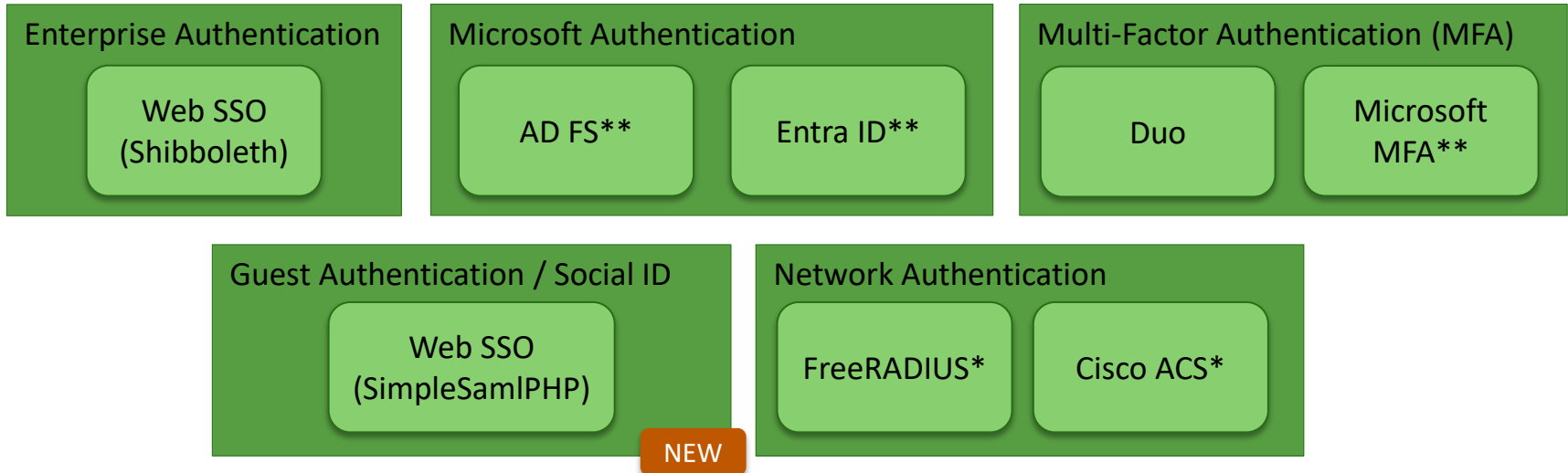
* Managed by ITS Networking
** Managed by Collaborative Platform Services

Directory Services

Current State

Enterprise Directory - LDAP	Windows Management & AD Groups
TED (OpenLDAP)	(Active Directory)**

Public Directory	Enterprise Directory - Mainframe
WPS (OpenLDAP)	TOM (Adabas)

** Managed by Collaborative Platform Services

Directory Services

Planned Future State

Enterprise Directory - LDAP	Windows Management & AD Groups
TED (OpenLDAP)	(Active Directory)**

Public Directory	Enterprise Directory - Mainframe
Retired	TOM (Adabas)
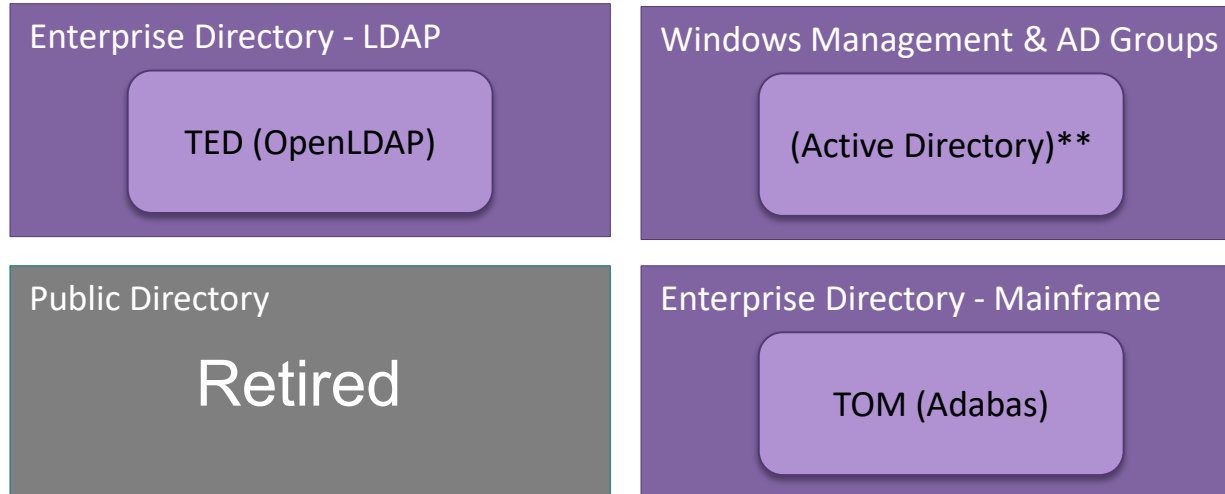
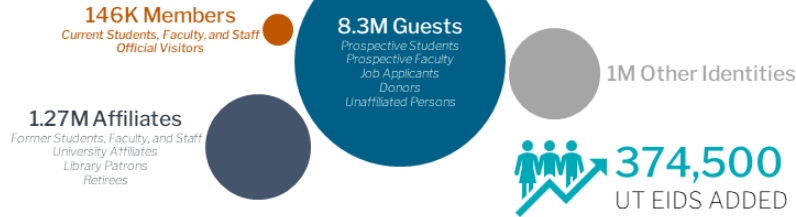** Managed by Collaborative Platform Services

IAM AT-A-GLANCE 2024

56 MILLION AUTHENTICATIONS

3.23 BILLION ENTERPRISE DIRECTORY SEARCHES

367 PROTECTED APPLICATIONS AND SERVICES

21.4 MILLION PUBLIC DIRECTORY SEARCHES

11.15 MILLION UT EIDs MANAGED

652K Businesses

146K Members
Current Students, Faculty, and Staff
Official Visitors

8.3M Guests
Prospective Students
Prospective Faculty
Job Applicants
Donors
Unaffiliated Persons

1M Other Identities

1.27M Affiliates
Former Students, Faculty, and Staff
University Affiliates
Library Patrons
Retirees

374,500 UT EIDS ADDED

413,800 PASSWORD CHANGES

33.03% via ASSISTED RESET

66.97% via SELF-SERVICE

25.96% via EMAIL TICKET

7.97% via RESET QUESTIONS

33.03% via KNOWN PASSWORD

124 THOUSAND UT EIDs PROTECTED BY MULTI-FACTOR AUTHENTICATION

ACCOUNTING FOR
3.28 MILLION AUTHENTICATIONS PER MONTH

The **Identity & Access Management (IAM) team** provides tools and services to make sure that the right people have access to the right resources at the right time.