

**AUGUST 2024**



# **IAM ROADMAP QUARTERLY REVIEW**

---

The review of the IAM Roadmap for Q1, 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 2023-2024	Q4	FY 2024-2025 Q1	Q2
<b>Initiative 1:</b> Improve password security with new hash	<i>(On hold due to resource constraints.)</i>	<i>(On hold due to resource constraints.)</i>	<i>(On hold due to resource constraints.)</i>
<b>Initiative 2:</b> Reduce technical debt by modernizing tools  (IGA Modernization Program)	<ul style="list-style-type: none"> <li>✓ Complete configuration of TAP solution to meet Phase 2 requirements.</li> <li>✓ Complete group build out for transitioning customers.</li> <li>✓ Complete initial TAP solution testing of configurations for Phase 2.</li> <li>✓ Plan midPoint and Grouper upgrades and testing.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Complete midPoint and Grouper upgrades.</li> <li>✓ Complete regression testing for upgrades.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Revisit project schedule for cutover from SailPoint IdentityIQ to midPoint.</li> <li><input type="checkbox"/> Plan and begin external communications about upcoming changes.</li> <li><input type="checkbox"/> Revisit security, functional, and non-functional testing and remediate issues for Phase 2.</li> </ul>
<b>Initiative 3:</b> Right size data retention with identity lifecycles	<ul style="list-style-type: none"> <li>✓ Monitor Youth Protection Program affiliations usage.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Monitor Youth Protection Program affiliations usage.</li> <li>✓ Process request for new affiliations for Mccomb's Texas Executive Education (TEE) program.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete internal development, testing, and release of the new affiliations for TEE program.</li> <li><input type="checkbox"/> Support TEE testing, as needed.</li> </ul>

# IGA Initiatives

FY 2024-2025	Q3	Q4	FY 2025-2026 Q1 and beyond
<b>Initiative 1:</b> Improve password security with new hash	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete analysis and determine approach for transition of TED &amp; FI/ST mainframe authentication to new hash.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Begin transition of TED &amp; FI/ST mainframe authentication to new hash.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete transition of TED &amp; FI/ST mainframe authentication to new hash.</li> <li><input type="checkbox"/> Retire old hashes and purge hash history.</li> </ul>
<b>Initiative 2:</b> Reduce technical debt by modernizing tools  (IGA Modernization Program)	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete security, functional, and non-functional testing and remediate issues for Phase 2.</li> <li><input type="checkbox"/> Complete testing with Workday and UT System teams.</li> <li><input type="checkbox"/> Complete external communications about upcoming changes.</li> <li><input type="checkbox"/> Plan and complete service planning for Enterprise Identity Manager (midPoint).</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete Phase 2 Go Live.</li> <li><input type="checkbox"/> Monitor systems after transition – hyper care.</li> <li><input type="checkbox"/> Retire SailPoint IdentityIQ service.</li> <li><input type="checkbox"/> Define and finalize Phase 3 scope, charter, and project schedule.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete Phase 3 requirements.</li> <li><input type="checkbox"/> Complete Phase 3 design(s).</li> <li><input type="checkbox"/> Complete configuration of TAP solution to meet Phase 3 requirements.</li> <li><input type="checkbox"/> Complete security, functional, and non-functional testing and remediate issues for Phase 3.</li> <li><input type="checkbox"/> Complete Phase 3 Go Live.</li> </ul>
<b>Initiative 3:</b> Right size data retention with identity lifecycles	<ul style="list-style-type: none"> <li><input type="checkbox"/> Support TEE testing, as needed.</li> <li><input type="checkbox"/> Monitor usage of affiliations for TEE program.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Monitor usage of affiliations for TEE program.</li> </ul>	<p><i>(Additional work to be determined based on requests.)</i></p>

# Authentication Initiatives

FY 2023-2024	Q4	FY 2024-2025 Q1	Q2
<b>Initiative 1:</b> Separate Guest and Enterprise SSO	<ul style="list-style-type: none"> <li>✓ Complete set up Guest Authentication service.</li> <li>✓ Onboard two early adopters.</li> <li>✓ Maintain service in hyper care.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Onboard other early adopters.</li> <li>✓ Maintain service in hyper care.</li> <li>✓ Plan upgrade of core software (SimpleSAMLphp).</li> </ul>	<ul style="list-style-type: none"> <li>❑ Complete upgrade of core software (SimpleSAMLphp).</li> <li>❑ Release Guest Authentication for general availability and onboard customers.</li> <li>❑ Plan build of Guest Authentication metadata manager.</li> </ul>
<b>Initiative 2:</b> Continuous improvement	<ul style="list-style-type: none"> <li>✓ Plan cloud native component of Enterprise Authentication for updated DR/BC.</li> <li>✓ Plan upgrade of Enterprise Authentication core software (Shibboleth v5).</li> <li>✓ Maintain OpenID Connect functionality for early adopters.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Complete implementation of cloud native component of Enterprise Authentication.</li> <li>✓ Complete upgrade of Enterprise Authentication core software.</li> <li>✓ Maintain OpenID Connect functionality for early adopters.</li> </ul>	<ul style="list-style-type: none"> <li>❑ Make OpenID Connect available to the university, as appropriate.</li> <li>❑ Continue cloud native refactor of authentication services.</li> </ul>
<b>Initiative 3:</b> Multi-factor authentication enhancements	<ul style="list-style-type: none"> <li>✓ Research impact of Duo expansion to Retirees to meet state mandate.</li> <li>✓ Plan Duo expansion to Retirees with HR, Service Desk, and Communications partners.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Coordinate preparation activities with HR, Service Desk, and Communication partners.</li> </ul>	<ul style="list-style-type: none"> <li>❑ Finalize communication plan.</li> <li>❑ Begin communication campaign.</li> </ul>

# Authentication Initiatives

FY 2024-2025	Q3	Q4	FY 2025-2026 Q1 and beyond
<b>Initiative 1:</b> Separate Guest and Enterprise SSO	<ul style="list-style-type: none"> <li><input type="checkbox"/> Build Guest Authentication metadata manager.</li> <li><input type="checkbox"/> Continue transitioning customers to Guest Authentication.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Deploy Guest Authentication metadata manager.</li> <li><input type="checkbox"/> Continue transitioning customers to Guest Authentication.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Continue transitioning customers to Guest Authentication.</li> </ul>
<b>Initiative 2:</b> Continuous improvement	<ul style="list-style-type: none"> <li><input type="checkbox"/> Continue cloud native refactor of authentication services.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Continue cloud native refactor of authentication services.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete cloud native refactor of authentication services.</li> </ul>
<b>Initiative 3:</b> Multi-factor authentication enhancements	<ul style="list-style-type: none"> <li><input type="checkbox"/> Continue communication campaign.</li> </ul> <p><i>(Additional work to be determined based on priorities and investigations.)</i></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Release Duo availability to Retirees.</li> <li><input type="checkbox"/> Plan implementation of Duo Central Device Management to retire Duo Device portal.</li> </ul> <p><i>(Additional work to be determined based on priorities and investigations.)</i></p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete implementation of Duo Central Device Management.</li> <li><input type="checkbox"/> Retire Duo Device portal.</li> </ul> <p><i>(Additional work to be determined based on priorities and investigations.)</i></p>

# Directory Services Initiatives

FY 2023-2024	Q4	FY 2024-2025 Q1	Q2
<b>Initiative 1:</b> Retire WHIPS	(Customer transition from WHIPS to uTexas Enterprise Directory (TED) is on hold due to resource constraints.)	✓ Begin removal of WHIPS dependency from directory.utexas.edu web application.	❑ Continue removal of WHIPS dependency from directory.utexas.edu web application.
<b>Initiative 2:</b> TED Cloud Resiliency	✓ Continue cloud native refactor of Directory Service services.	✓ Continue cloud native refactor of Directory Service services.	❑ Continue cloud native refactor of Directory Service services.

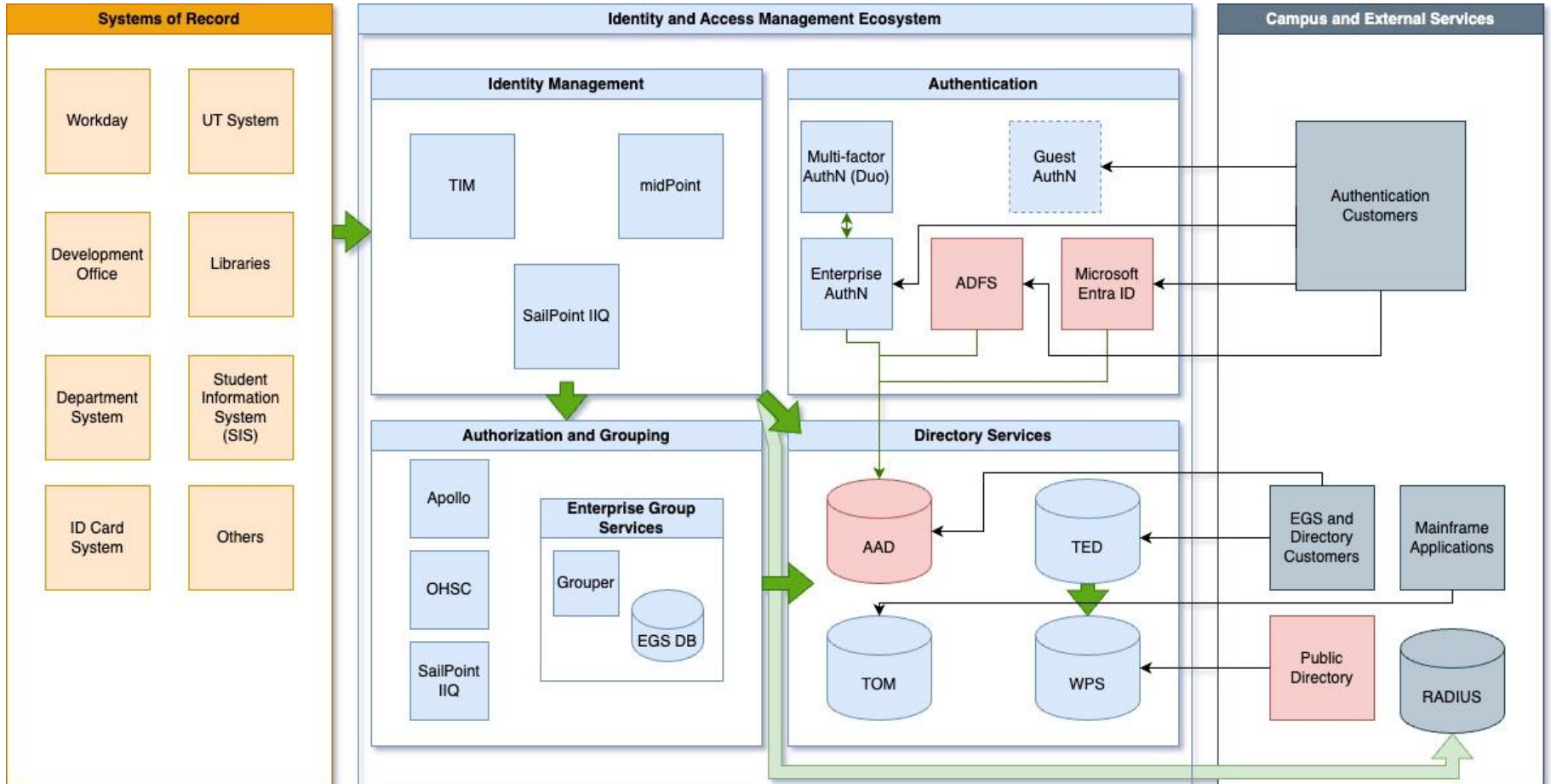
# Directory Services Initiatives

FY 2024-2025	Q3	Q4	FY 2025-2026 Q1 and beyond
<b>Initiative 1:</b> Retire WHIPS	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete removal of WHIPS dependency from directory.utexas.edu web application.</li> <li><input type="checkbox"/> Plan customer transition from WHIPS to uTexas Enterprise Directory (TED).</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Begin customer transition from WHIPS to uTexas Enterprise Directory (TED).</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete customer transition from WHIPS to uTexas Enterprise Directory (TED).</li> <li><input type="checkbox"/> Retire and decommission WHIPS.</li> </ul>
<b>Initiative 2:</b> TED Cloud Resiliency	<ul style="list-style-type: none"> <li><input type="checkbox"/> Determine and plan TED and WPS cloud migration timeline.</li> <li><input type="checkbox"/> Continue cloud native refactor of Directory Service services.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Communicate TED and WPS cloud migration timeline to stakeholders.</li> <li><input type="checkbox"/> Finalize cloud native refactor of Directory Service services.</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Complete cloud migration.</li> <li><input type="checkbox"/> Monitor performance and service usage on cloud architecture.</li> </ul>



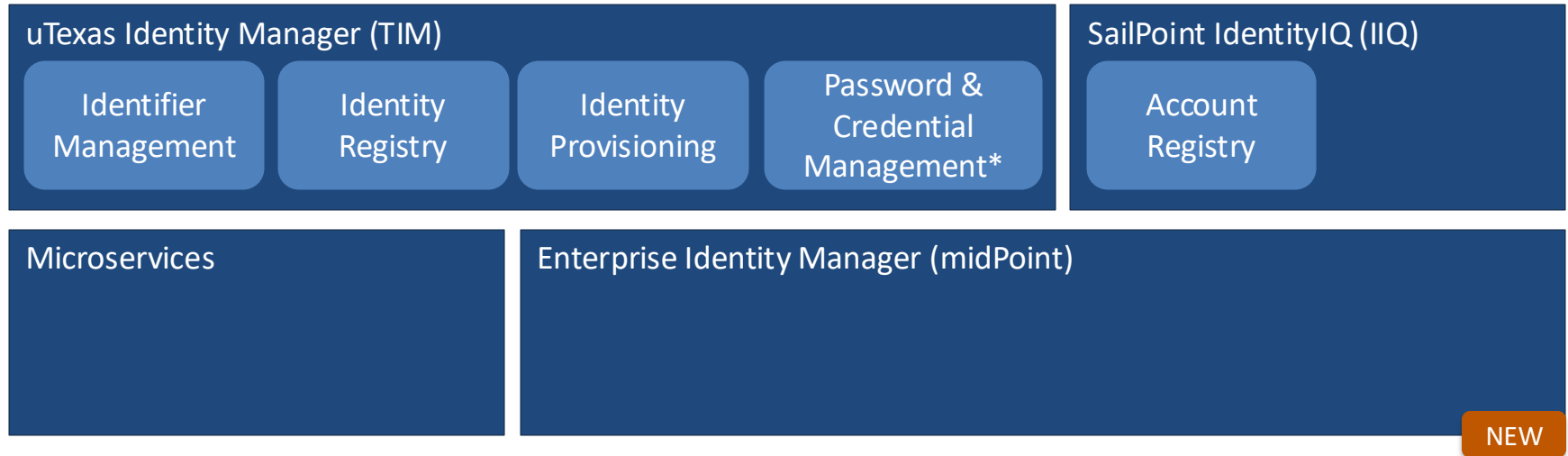
# Appendix

## Current State versus Planned Future State



# Identity Governance & Administration (IGA)

## Identity Management: Current State



\* TIM & Duo

# Identity Governance & Administration (IGA)

## Identity Management: Planned Future State

uTexas Identity Manager (TIM)

Retired

SailPoint IdentityIQ (IIQ)

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)

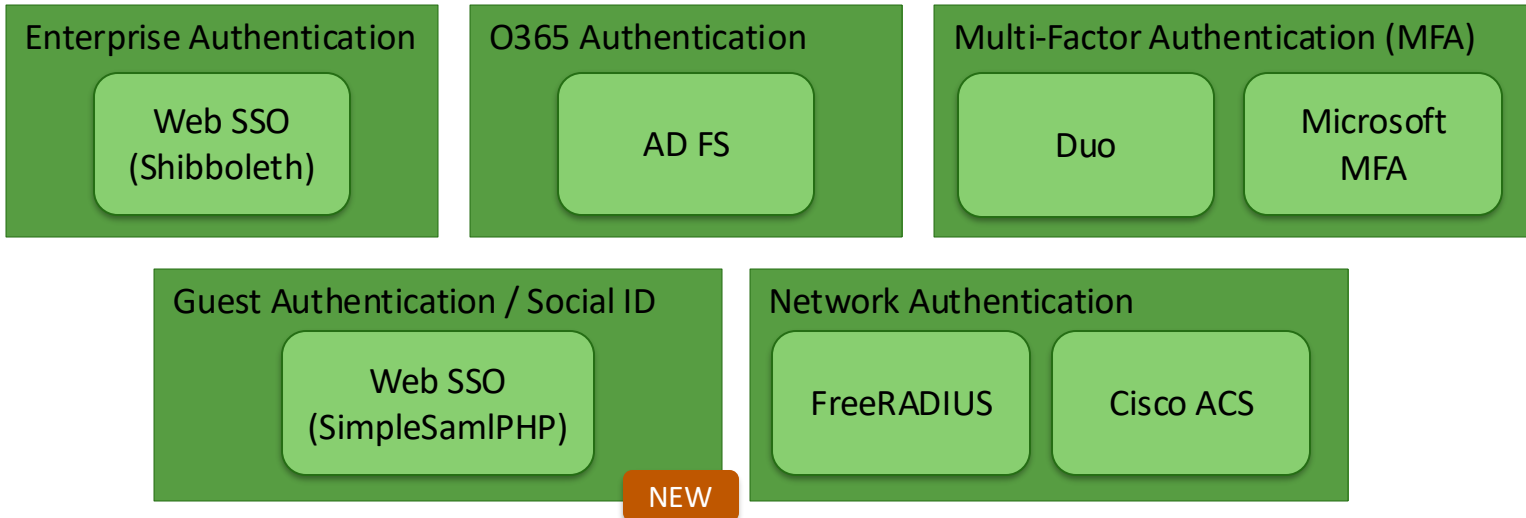
Group & Role  
Management

Authorization  
Reporting and Review

NEW

# Authentication

## Current State



\* Managed by ITS Networking

\*\* Managed by Collaborative Platform Services

# Directory Services

## Current State

Enterprise Directory - LDAP

TED (OpenLDAP)

Windows Management & AD Groups

(Active Directory)

Public Directory

WPS (OpenLDAP)

Enterprise Directory - Mainframe

TOM (Adabas)

\*\* Managed by Collaborative Platform Services



# Directory Services

## Planned Future State

Enterprise Directory - LDAP

TED (OpenLDAP)

Windows Management & AD Groups

(Active Directory)

Public Directory


Retired

Enterprise Directory - Mainframe


TOM (Adabas)

\*\* Managed by Collaborative Platform Services

# IAM AT-A-GLANCE 2023

 **57.48 MILLION**  
AUTHENTICATIONS


**3.54 BILLION**  
ENTERPRISE DIRECTORY  
SEARCHES 






 **318 PROTECTED**  
APPLICATIONS AND  
SERVICES

**22.1 MILLION**  
PUBLIC DIRECTORY  
SEARCHES 

**10.77 MILLION**  
UT EIDs MANAGED



 **192,005**  
PASSWORD CHANGES

-  15.12% via ASSISTED RESET
-  84.88% via SELF-SERVICE
-  51.44% via EMAIL TICKET
-  18.33% via RESET QUESTIONS
-  15.12% via KNOWN PASSWORD

**118 THOUSAND**  
UT EIDs PROTECTED BY  
MULTI-FACTOR AUTHENTICATION 

ACCOUNTING FOR  
**3 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.

<https://iamservices.utexas.edu/>