THE UNIVERSITY OF TEXAS AT AUSTIN
ITS· Information Technology Services

Lightweight Authentication
Document Version 3.0
Prepared by *Autumn Shields, ITS*
Last Edited January 15, 2016

PLAN ❯ REQUIREMENTS ❯ SOLUTION ANALYSIS ❯ DESIGN ❯ BUILD ❯ TEST ❯ TRAIN/DEPLOY ❯ MAINTENANCE

Lightweight Authentication Project Charter

Lightweight Authentication

Executive Summary

The Lightweight Authentication Project will provide an alternate method of authentication for external users who need to access online university resources. The recommended solution is to make external identities consumable by campus applications using a centrally provided gateway.

Business Need and Background

One goal of the IAM Strategy Roadmap is to develop authentication tools that create a better balance between usability and security. The University benefits from online collaboration with a variety of external users, from prospective students, alumni, and job applicants to international visitors and research collaborators. While the UT EID was designed for members of the UT community, it is also widely used by external users. However, the process of creating a UT EID and remembering a UT EID and password can be problematic for users who only have an occasional need to access campus resources. Requiring UT EID authentication for these users delivers a poor user experience and also leads to calls to the Help Desk for password resets. Many of these external users already have accounts with other identity providers such as Google and LinkedIn.

Project Description and Scope

The Lightweight Authentication Project will be completed in four phases and will address the following:

Phase 1 – Requirements, Solution Assessment, and Guest EID Roadmap

- Gather requirements for lightweight authentication solution.
- Identify identity providers to be included in the implementation.
- Identify a lightweight authentication solution for users who are not comfortable using a social account (e.g., Facebook, LinkedIn) to access UT resources. This could be be a third party identity provider that is not linked to a social account provider.
- Complete a solution assessment.
- Procure a solution.
- Develop roadmap for currently existing guest-class UT EIDs.

Phase 2 – Solution Procurement and Basic Implementation with Early Adopters

- Complete solution selection.
- Complete high level design of overall lightweight authentication solution.
- Develop guidelines for applications that grant access to external identities. Determine where external identities fit in the identity assurance framework.
- Identify and incorporate early adopter applications.
- Implement a lightweight authentication solution that allows a user to authenticate using a social account (e.g., Facebook, LinkedIn), a local account (an account managed by the solution itself, or a UT EID.
- Implement a solution for business processes that depend on the EID/UIN.
- Complete adoption planning.
- Complete Guest EID transition planning.

Phase 3 – Service Enhancement

- Implement the ability to assign entitlements to a lightweight identity.
- Design and implement an account – linking process to connect an external identity to a UT EID.

Phase 4 – Transition, Adoption, and Guest EID Retirement

- Complete transition and adoption of Guest EID consumers.
- Retire guest-class EIDs

Project Goals

When this project is complete, applications that serve external users should be able to transition to using external identities in lieu of guest class UT EIDs. The following goals will support this outcome:

- o Select external identity providers,
- o Provide application owners with clear guidelines for working with external identities,
- o Offer users an option to authenticate with an identity that is not connected to a social account,
- o Implement a method for Campus applications to consume external identities through a central authentication gateway that will translate and provide identity information in a standard format,
- o Provide users the ability to choose their preferred identity provider using a discovery service.

Project Schedule

Milestone/Deliverable	Target Date
Phase 1	February 2016
Phase 2	January 2017
Phase 3	March 2017
Phase 4	December 2017

Project Management and Governance

Role	Names
Executive Sponsor(s)	Julienne VanDerZiel
Governance Oversight	IAM Committee
Customer Steering Committee	Recommended CSC membership: • CW Belcher, ITS Applications • Cesar De La Garza, University Development Office • Michael Caldwell, Office of Admissions • Steve Rung, Office of Admissions • Samuel Westerfeld, Information Security Office • Alex Barth, ITS Systems • John Chambers, College of Natural Sciences • David Mok, International Office • Vadim Gorelik, McCombs School of Business
Project Manager	Marta Lang
Technical Solution Lead	Autumn Shields
Business Analyst	Rosa Harris
Information Security Officer	Cam Beasley or designee
Systems Point of Contact	Alex Barth
Networking Point of Contact	William Green or designee
Customer Support Services Point of Contact	Sandra Germenis or designee

Assumptions

- The protocols to be supported by the multiprotocol authentication gateway will depend on requirements gathered in Phase 1.
- Application owners may need to make changes to existing systems to transition to using external identities.
- Application owners may subscribe or choose not to subscribe to the lightweight authentication gateway.
- Application owners who choose to consume external identities will use the authentication gateway endorsed by campus.

Constraints

The project will use resources and budget as outlined in the IAM Roadmap and IAM fiscal year project planning.

Risks

Project risks include:

- Resource contention between multiple simultaneous projects may delay project progress.
- New technology components may introduce a need for training and education for project team members which may extend the project timeline.
- The need to coordinate with multiple groups within the University increases complexity of implementation.
- The need for high availability may add to project complexity.
- Relying on external identity providers introduces risks since their reliability and availability is beyond the University's control.
- Complex business requirements may make it difficult to understand the implications of design decisions.
- Working with third-party identity providers and vendor products may increase complexity and introduce constraints.
- The IAM Modernization Project schedule may affect integrations with IAM systems.

Revision History

Version	Date	Updater Name	Description
V 1	01/15/2015	A Shields	Initial draft completed.
V 2	02/12/2015	A Shields	Version 2.0 completed.
V 3	07/20/2015	A Shields	Updated phase deliverables.
V 4	09/25/2015	R Harris	Updated scope, project schedule, and project management and governance.
V 5	01/15/2015	R Harris	Updated Project Description and Scope.