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

Project Charter

Executive Summary

The Centralized Authentication Resiliency Enhancement (CARE) project will improve the resiliency of the UTLogin, Shibboleth, and Active Directory authentication services by implementing off-campus instances of those services and implementing the required connectivity to enable their use by both on-campus and hosted/cloud systems.

This project is part of the Identity and Access Management Roadmap.

Business Need and Background

The university's current central authentication systems provide varying levels of resiliency in the event of a loss of the primary university data center (UDC-C), as described in the Appendix. Although some resiliency is available through system components hosted in the secondary university data center (UDC-B), central authentication services cannot currently be maintained if both on-campus data centers are unavailable. In addition, in the event of a loss of connectivity between the campus network and the Internet, centralized authentication services for hosted/cloud applications (for example, Canvas and Workday) would not be available until connectivity was restored. Depending on the cause of the data center outage or loss of connectivity with the Internet, restoration of authentication services could take days or weeks.

By hosting authentication services off-campus, the resiliency of those authentication services can be enhanced and the impact of a data center outage or loss of campus Internet connectivity can be mitigated.

Description and Scope

The scope of this project will include the design and implementation of a production environment for the UTLogin, Shibboleth, and Active Directory authentication services in an off-campus location and the connectivity required to allow both on-campus and remotely hosted services to use them.

In Scope

- Implementation of UTLogin, Shibboleth, and Active Directory in an off-campus, virtualized environment with an appropriate backing user store, e.g. TED or a subset of TED data.
- Implementation of a synchronization process for the off-campus instances of UTLogin, Shibboleth, and Active Directory configuration data and backing user store data.

- Configuration and implementation of required networking/traffic management infrastructure.
- Training and documentation for parties involved when the off-campus environment is used in a disaster recovery or failover scenario.

Out of Scope

- Implementation of an off-campus version of TED for use by systems other than UTLogin, Shibboleth, or Active Directory.
- Implementation of two-factor authentication in an off-campus environment. This will be handled in a separate project.

Goals

The goal of this project is to deploy a resilient, off-campus authentication infrastructure so that the UTLogin, Shibboleth, and Active Directory centralized authentication services remain available if on-campus authentication services become unavailable or the campus network becomes unavailable.

Schedule

This project is scheduled to begin in Q2 FY2014-2015 and continue through the fiscal year. Further schedule milestones will be determined at the end of the design phase.

Milestone/Deliverable	Target Date
Plan Project	December 2014 - February 2015
Requirements Development	January – March 2015
Solution Analysis and Selection (including high-level plan for implementation)	TBD
Design	TBD
Build	TBD
Test	TBD
Deploy	TBD
Close Project	TBD

Project Management and Governance

Role	Names

Executive Sponsor(s)	Julienne VanDerZiel, Trice Humpert
Governance Oversight	IAM Committee
Customer Steering Committee	Recommended CSC membership: • Dave Pavkovic, ITS Systems • Cam Beasley, ISO • CW Belcher, ITS Applications • Tim Fackler, College of Liberal Arts • Elyes Benhamou, McCombs School of Business • Fred Gilmore, UT Libraries • Mario Guerra, CTL • Ed Horowitz, Cockrell School of Engineering • Mic Kaczmarczik or Scott Doane, UT Web • Darin Mattke, Project IQ • Juan Ortiz, ASMP • Alison Lee, ITS Networking
Project Oversight	CW Belcher
Project Manager	Justin Czimskey
Technical Lead	George Peek
Business Analyst	Rosa Harris
Information Security Officer	Cam Beasley or designee
Systems Point of Contact	Greg Baker or designee
Networking Point of Contact	William Green or designee
Customer Support Services Point of Contact	Sandra Germenis or designee

The IAM Committee will:

- Establish project goals and scope via this project charter
- Review and approve any changes to the project scope
- Review project progress at end-of-phase review checkpoints

Project progress will be reviewed as appropriate at scheduled IAM Committee meetings or via email.

The Customer Steering Committee will:

- Represent the university community in project decision-making and issue resolution
- Establish business and technical requirements
- Review and approve project deliverables
- Review project progress
- Provide guidance as needed to assist the project team in adhering to the goals and recommendations of the project

The CSC will meet as needed throughout the project and at the conclusion of each project. In-person meetings as well as email will be utilized.

Assumptions

- The components of the UTLogin, Shibboleth, and Active Directory authentication stacks can be built using a virtual machine environment that can be hosted remotely.

Constraints

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

Risks

Project risks include:

- The challenges of operating the authentication services stack in a remotely hosted virtual environment are largely unknown.
- Resource contention may delay project progress.

Appendix

Current Recovery Time Objectives (RTO) for Central Authentication Services

	Scenario A Loss of Primary UT Datacenter (UDC-C) Only	Scenario B Loss of Primary (UDC-C) and Secondary (UDC-B) UT Datacenters	Scenario C Loss of connectivity between Internet and campus network
UTLogin	Restoration of service in two (2) hours.	No service until at least one data center is restored	No service for hosted/cloud-based applications until connectivity is restored
SAML Identity Provider (Shibboleth)	Restoration of service in twenty-four (24) hours.	No service until at least one data center is restored	No service for hosted/cloud-based applications until connectivity is restored
TED	Restoration of service in two (2) hours.	No service until at least one data center is restored	No service for hosted/cloud-based applications until connectivity is restored
Austin Active Directory	No impact to service.	No service until at least one data center is restored	No service for hosted/cloud-based applications until connectivity is restored
Toopher (for UT Direct)	Restoration of service in three (3) days	No service until at least one data center is restored	n/a (Toopher for UT Direct is not available for hosted/cloud-based applications)