Project Scope Statement

Duo Implementation

Executive Summary

In December 2014, the University of Texas System issued a memo mandating that certain sensitive data systems and financial applications require the use of two-factor authentication (2FA) for access. The Duo Implementation project will support a coordinated response to this mandate by allowing campus to enable 2FA using the Duo Security two-factor solution on applications where it is required.

Business Need and Background

In response to a previous UT System requirement that required access to sensitive financial applications be protected by 2FA, the university implemented and integrated the Toopher two-factor authentication solution with applications on UT Direct, including W-2 downloads, payroll bank routing information, non-payroll bank routing information, and student emergency loan applications. After UT System expanded this requirement to include new use cases, the Toopher infrastructure was evaluated for fit and was determined to be unsuitable to meet the new requirements.

In light of the need to replace the current Toopher two-factor authentication service, the IAM team completed a high-level product assessment of two-factor authentication solutions in early August 2015 to identify candidate solutions that would help the University meet its requirements for two-factor authentication, including those mandated by UT System policy. Based on this analysis, the Duo Security two-factor authentication product was identified as the strongest candidate solution.

To validate the compliance of Duo with the University's requirements, the IAM team partnered with other campus groups during August and September 2015 to complete a hands-on proof-of-concept using the Duo solution. Based on the results of the proof-of-concept, the university decided to proceed with the purchase and procurement of Duo.

Project Scope and Deliverables

The scope of the UT System mandate specifically includes:

- "When an employee or individual… logs on to a University network using an enterprise remote access gateway." This case includes the widely used campus Cisco VPN provided by ITS Networking.

- "When an individual working from a remote location uses an online function… to modify employee banking, tax, or financial information." This case includes (and expands an existing mandate) the protection of W-2, bank routing, emergency loan, and other sensitive financial applications.
- "When a server administrator or other individual working from a remote location uses administrator credentials to access a server that contains or has access to confidential University data." This is a wide-ranging case that includes a number of systems that store or use Confidential (formerly Category I) data.

The Duo Implementation project will coordinate the implementation effort of the Duo Security 2FA platform across all the above use cases, including the technical aspects, the introduction of new 2FA methods, operational readiness, and campus communication. Specifically, this includes:

- UTLogin SAML and WPA integration
- Shibboleth SAML integration
- Cisco VPN (web and native desktop client) integration
- Documentation to support PAM/RDP implementations

Additionally the project scope includes the transition of existing Toopher-protected applications to Duo.

Out of Scope

The following items will not be included in this project:

- Direct support for any of the Duo-provided integrations outside of UTLogin, Shibboleth, Cisco VPN, and PAM/RDP methods.

Project Schedule

The project is date-constrained by the UT System mandate deadline, which has been extended to March 18th, 2016, to accommodate the changes that must be made to the existing 2FA architecture. The project is split into two major phases, including:

- Technical Implementation – includes UTLogin, Shibboleth, VPN, PAM/RDP, operational readiness, training, and communication. This will be complete by March 18, 2016
- Application Transition – includes FIS and Payroll applications on UT Direct protected by Toopher. This phase will proceed beyond the stated UT System mandate deadline as they are currently and will continue to be in compliance using the Toopher solution. These transitions are planned to be complete by the middle of June 2016.

The full project schedule is available as a Microsoft Project file separate from this document.

Project Oversight

The Duo Implementation project will focus on providing the capabilities to campus to implement 2FA as needed with their applications. While this will involve other ITS resources such as ITS Networking for the VPN, CSS for product support, etc., the technical work will be performed primarily by the IAM team. The project executive sponsor will be the Associate Director of ITS Applications, CW Belcher. The IAM Committee will provide overall governance for this project. Regular updates on the status of the project will be provided to the project executive sponsor, the IAM Committee, the ITS directors, and the Chief Information Security Officer.

Impact Analysis

At the end of this project:

- Internal customers who rely on the central authentication infrastructure including UTLogin and Shibboleth will be able to implement 2FA with their applications.
- VPN end users will be required to use 2FA when accessing the VPN.
- System administrators will be able to leverage PAM/RDP modules to protect Linux and Windows machines with 2FA using Duo.

Assumptions

- Due to time and resource constraints, the project team will strive to use as much out-of-the-box functionality provided by Duo as possible. Customizations to the Duo product will be avoided.
- Application owners will be responsible for communicating directly with customers when enabling 2FA capabilities on their applications.

Constraints

- The UT System mandate has been extended to March 18, 2016. The capability for 2FA on the authentication systems and the VPN must be in place prior to this date. This has been noted in the schedule section of this document.

Risks

A detailed risks and issues log is available as a separate document.

Revision History

Version	Date	Updater Name	Description
0.5	11/10/15	Justin Czimskey	Created initial draft.