KSU Information Technology Services - Decision Memo
August 7, 2017

Issuance of Digital Certificates

Background: ITS has historically issued Secure Sockets Layer[1] (SSL) certificates for use in encrypting web traffic and signing code for organizations within the University. The Data Classification policy (PPM 3433) requires that confidential information be encrypted by SSL during transmission. In a few cases personal digital certificates have also been issued for individuals requiring the ability to digitally sign or encrypt email. Certificates are requested via a ServiceNow request form.

Issue: Management of digital certificates has become cumbersome. Efficiencies would be gained by consolidating certificate management operational functions including vetting, issuance, and revocation for SSL, code signing and personal certificates. Other considerations include 1) issuance of extended validation certificates, 2) selection of standards, and 3) auditing and enforcement of standards.

Assumptions:

- K-State will continue to require use of SSL certificates for encrypted transmission of confidential information.
- ITS will continue to be the enforcement body for PPM 3433 and the issuer of digital certificates for University use.
- Internet2 via InCommon or some similar organization will continue to provide K-State with access to a certificate authority (CA) and a means of issuing digital certificates.

Decision: Enterprise Server Technologies (EST) and the Network Operations Center (NOC) will manage the operational functions. Information Security and Compliance (ISC) will manage the standards, auditing, and enforcement of standards.

1. EST will be the operational owner of SSL Certificate Management and acting Registration Authority Operator (RAO)
   a. Director of EST will be the Master Registration Authority Officer (MRAO)
   b. Team lead of EST Platform team and one other designee will have RAO access.
   c. EST RAO's will manage Department Registration Authority Officer (DRAO) access.

[1] SSL is a computing protocol that ensures the security of data sent via the Internet by using encryption. Oxford Dictionary. https://en.oxforddictionaries.com/definition/ssl. Last accessed: August 5, 2017.

Approved by ITS Directors on October 2, 2017

2. NOC will remain as primary contact (tier 1 support) for basic operations for departments without DRAO access (or as a backup DRAO for those that do)
    a. EST will be tier 3 support for NOC

3. ISC designee will have RAO access for auditing/reporting functions.

4. EST will handle Domain Control Validation (DCV) to streamline the process (since it holds both RAO access and DNS management).

5. ISC will set standards for digital certifications.

6. EST develop Implementation Plan

Implementation Plan

Milestone 1 – Training and Documentation – 11/30/2017

- Develop and conduct training for EST Staff on SSL and DNS
- Develop documentation packet for Department Registration Authority Officers (DRAO)
- Assist NOC staff with training and support
- Transition Master Registration Authority Officer to EST Director
- Transition Registration Authority Officer (RAO) to EST Platform Team Lead, EST Associate Director, ISC Designate
- EST Staff Abilities
    - Edit SSL details after they are uploaded
    - Approve cert requests
    - DCV for domains
    - See every department for SSL certs (all certs in domain)

Milestone 2 – Delegation – 1/1/2018

- EST Director will identify additional DRAOs to reduce operations and approve access on a case by case basis.
    - The threshold for access will be 10 or more certs managed by the group.
- DRAOs will have access over their domains

Approved by ITS Directors on October 2, 2017