Information Security Office
Office of Information Technology

ISO Position Paper

Position Title	Self-Signed Web Server Certificates
Position Audience	Princeton IT Professionals
Contact	Information Security Office: InfoSec@princeton.edu
Position Release Date	August 10, 2017
Last Update	Initial posting

Problem Statement

Some web servers are configured to use “self-signed” certificates. However, these are not administered by any validating authority and are therefore not trustworthy. Self-signed certificates are commonly used by web servers that seek to distribute malicious data or imitate a legitimate site. In addition, users establish poor security habits when “accepting” the warning notice of a self-signed certificate.

When cost is an issue, it is also a common practice for self-signed certificates to be used in non-production environments, leading to certificate warning messages to the users.

ISO Position

It is the position of the ISO that all University servers, including development, QA, and production, utilize the OIT provided certificates.

Princeton University faculty, staff, and students should use only authorized certificates on University web servers. The University has a contract with InCommon as a legitimate certificate authority for an unlimited amount of certificates. These certificates are provided at no cost to the campus community through the Office of Information Technology.

Additional Information
Certificates: How to request a digital certificate for a web server at Princeton University

---