Requesting InCommon Certificates

S&T Information Security is providing trusted and managed certificates for various uses to Faculty, Staff, student employees as well as for web site usage. All certificates are signed by Comodo and are trusted by most web browsers and operating systems.

Types of Certs available to campus:

- SSL for web sites to ensure proper encryption. This is available for any *.mst.edu website. We cannot issue to any other domains.
- Personal certificates for file encryption and signing. This typically is used for email to ensure that:
  - Mail definitely came from you
  - Encryption when you have sensitive information to send or receive

Process for requesting:

- Be sure to read: https://wiki.mst.edu/security/public/incommonclient, especially the best practices.
- Make a ticket with the helpdesk: https://help.mst.edu
  - For SSL (web site) certificates, state the full web site name of the web page as it appears to the customer, not the server. In other words, if you want your site to appear as: JoeMiner.mst.edu, which is housed on another server, websites.srv.mst.edu, use that virtual host of JoeMiner.mst.edu and not the name of the server. Also state why you are needing the certificate. Are you requiring logins, sending of sensitive data and the type of data, etc.
  - For personal certificates, you must be a faculty (emeritus is considered faculty), staff or student employee, and state that you have read, or will read https://wiki.mst.edu/security/public/incommonclient

Tier-1:

Assign ticket to the Security Queue.

- Summary: Requesting Personal Certificate

or for Web Sites:

- Summary: Requesting Web SSL Certificate

SSL: Ensure that the web page looks like a virtual host name. In other words shouldn't be *.srv.mst.edu unless being requested by an IT staff member.

Personal Certificate: Make sure the customer reads/has read: https://wiki.mst.edu/security/public/incommonclient