FAQ - Certificate Service SSO and MFA

- Who can use single sign-on?
- I'm already an RAO and my organization uses SSO and MFA. How do I start using SSO?
- We don't use SSO now, but it sure sounds like a good idea. How do I do that?
- Does InCommon recommend a specific Multifactor Authentication method for use with the Certificate Service?
- We use MFA locally, but I'm not sure about this REFEDS profile. What's that about?

Who can use single sign-on?

Both RAOs and DRAOs at campuses that used federated identity (e.g. have an identity provider in the InCommon Federatoin) and support MFA locally can use the SSO/MFA feature.

I'm already an RAO and my organization uses SSO and MFA. How do I start using SSO?

Review this wiki page for the process.

We don't use SSO now, but it sure sounds like a good idea. How do I do that?

If you subscribe to the Certificate Service, your organization is an InCommon participant and you have access to the InCommon Federation. In order to use SSO, you would need to have an identity provider in the federation (which means your campus would need the proper identity management infrastructure). You can find out if your campus already has an identity provider by searching on this page. You may also be interested in reviewing this basic information on the InCommon Federation.

Does InCommon recommend a specific Multifactor Authentication method for use with the Certificate Service?

We do not have a specific recommendation. However, your MFA solution must support the REFEDS MFA Profile.

We use MFA locally, but I'm not sure about this REFEDS profile. What's that about?

The REFEDS profile ensures interoperability by specifying requirements that allows the service provider (in this case the Comodo Certificate Manager) to communicate its need for MFA and for the identity provider to communicate that it has successfully used MFA to authenticate the user.