Domain Registration and Validation

Once your campus has subscribed to the Certificate Service and appointed Registration Authority Officer(s) (RAO), InCommon must validate each domain — that is, domain control must be demonstrated — before issuing certificates. This is called Domain Control Validation — please read the DCV documentation.

This process determines whether there is a reasonable ownership connection between the organization listed in WhoIs and the organization requesting the domain for certificate issuance. Because the Certificate Service is available only to U.S. higher education institutions, an insufficient connection will result in rejected domains. This determination is made at the sole discretion of InCommon. Here is a guide that InCommon uses for permitted non-Fully Qualified Domain Name (FQDN) entries.

Note about how to submit your base domains

IMPORTANT: You should be sure to not only submit your base domain (e.g. campus.edu), but you should also submit the wildcard of your base domain (e.g. *.campus.edu). This will enable you to do DCV once and have all of your sub-domains covered (sports.campus.edu, business.campus.edu, etc), rather than having to complete DCV separately for each sub-domain.

Steps for Domain Control Validation (DCV)

1. The RAO adds a domain name (or multiple domain names) in the the Certificate Manager (CM).
2. InCommon determines whether there is a reasonable ownership connection between the organization listed in WhoIs and the organization requesting the domain for certificate issuance.
3. InCommon will notify the submitter when the domain has been approved and it ready for DCV.
4. In the Certificate Manager, the RAO clicks the DCV button next to a domain. This opens the DCV wizard.
5. In the DCV wizard, the RAO chooses one of three methods for validating the domain:
    a. Email — This option sends an email to an address that would typically appear in the WhoIs listing (you will see a drop-down menu with several choices: admin@, administrator@, webmaster@, etc.). The email will include a validation code to paste into a confirmation web page.
    b. HTTP — The CM will generate a specific text (.txt) file which must be placed in the root directory of the domain. The automated system will check for the file.
    c. CNAME — The CM will generate two specific hashes which must be entered as a CNAME DNS record. The automated system will check for the hashes.
6. Once the DCV process is completed, the CM will show the domain as "approved" and will allow certificates to be issued.