InCommon Domain Control Validation Options

Purpose

This document describes the options that InCommon supports for Domain Control Validatation (DCV). You must select one of the options, and the relevant procedures must be carried out before a new UW domain can be added to the InCommon Certificate service (this document also applies to annual renewal of DCV on existing domains).

Options

InCommon supports three methods for DCV: HTTP, CNAME, and Email. Email is not a good choice for most customers but is mentioned for the sake of completeness. Each of these options is described below.

HTTP

> **From InCommon documentation:**
>
> *InCommon generates a specific text (.txt) file which must be placed on the root directory of the domain undergoing DCV. InCommon's automated system will check for the presence and content of this file to complete the validation process. Administrators need to upload it only to the specified location.*

Steps:

1. The Identity and Access Management (IAM) team receives a request to use HTTP as the DCV option.
2. The Identity and Access Management (IAM) team requests the domain via InCommon Certificate Manager and waits for InCommon to verify UW domain ownership.
3. IAM selects "HTTP" as the DCV option.
4. Certificate Manager generates a text file and a specific filename to be used.
5. IAM communicates this information to the requestor.
6. The requestor must place this file in the root of a publicly-accessible web server at the domain name requested. For example, if the domain testing.com is requested, then the file must be available at http://testing.com/.well-known/pki-validation/filename.txt.
7. Once the file is in place, the requestor must notify IAM.
8. IAM returns to Certificate Manager, navigates to the domain, DCV, then clicks Test, then Submit.
9. Upon successful validation InCommon will notify IAM via email that DCV has been completed. **Note:** DCV expires after one year. This will not affect the validity of any certificates you have already obtained, but you will not be able to request new certificates in expired domains until you complete DCV again.
10. IAM will resolve your ticket, letting you know you can now remove the file and request certificates by submitting a CSR to Certificate Services.

CNAME

> **From InCommon documentation:**
>
> *InCommon CM will generate two specific hashes which must be entered as a CNAME DNS record. InCommon's automated system will check for the presence of the two hashes in your DNS records. DCV will be achieved after a successful CNAME check. Please use this format:*
>
> *<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com*

Steps:

1. The Identity and Access Management (IAM) team receives a request to use CNAME as the DCV option.
2. The Identity and Access Management (IAM) team requests the domain via InCommon Certificate Manager and waits for InCommon to verify UW domain ownership.
3. IAM selects "CNAME" as the DCV option.
4. Certificate Manager provides the text for a CNAME record that must be added to DNS for the requested domain.
5. IAM communicates this information to the DNS contact or requestor:
    a. If the domain is registered in UW DNS this information is provided to the UW NOC.
    b. If the domain is not registered in UW DNS this information is provided to the requestor. If the requestor is not the DNS contact for the domain they must coordinate with that person to add the CNAME record to DNS.
6. Once the CNAME record is added, the DNS contact or requestor must notify IAM.
7. IAM returns to Certificate Manager, navigates to the domain, DCV, then clicks Test, then Submit.
8. Upon successful validation InCommon will notify IAM via email that DCV has been completed. **Note:** DCV expires after one year. This will not affect the validity of any certificates you have already obtained, but you will not be able to request new certificates in expired domains until you complete DCV again.
9. IAM will resolve your ticket, letting you know you can now remove the CNAME record and request certificates by submitting a CSR to Certificate Services.

Email

Email DCV has changed significantly as of May 2018–please read the updated section carefully, especially the section on approved addresses.

Approved Addresses

To complete DCV via email, you must be able to receive messages sent to an address approved by InCommon. ***Following is the list of approved addresses--DCV emails cannot be sent to any other addresses. Note that emails listed in WHOIS contacts are no longer an option.***

- admin@domain.com (replace domain.com with your actual domain)
- administrator@domain.com
- hostmaster@domain.com
- postmaster@domain.com
- webmaster@domain.com

(While in the past DCV emails could also be sent to addresses listed in the WHOIS contacts, the European Union GDPR regulation has resulted in most registrars locking down their WHOIS databases. As a result, InCommon isn't able to get contact addresses from WHOIS and use them for DCV.)

The email will contain a unique validation code you will enter into a confirmation page to complete DCV.

Steps:

1. The Identity and Access Management (IAM) team receives a request to use Email as the DCV option.
2. The Identity and Access Management (IAM) team requests the domain via InCommon Certificate Manager and waits for InCommon to verify UW domain ownership.
3. IAM selects "E-mail" as the DCV option.
4. IAM selects the email address to send the DCV request to. Requests can be sent to email addresses pulled from the domain's whois record (even if those addresses aren't from the domain being validated) plus typical addresses listed above. The requestor needs to let IAM know which email address to use and they, or a person working on their behalf, must be able to receive email at that address. **IAM cannot send DCV requests to arbitrary email addresses–the *only* email addresses that can be used are the approved addresses listed above.**
5. InCommon will send an email to the selected address that contains a web link and a code.
6. The recipient must browse to the web link specified in the email and enter the code.
7. Upon successful validation InCommon will notify IAM via email that DCV has been completed. **Note:** DCV expires after one year. This will not affect the validity of any certificates you have already obtained, but you will not be able to request new certificates in expired domains until you complete DCV again.
8. IAM will resolve your ticket, letting you know you can now request certificates by submitting a CSR to Certificate Services.

See Also

- Obtain a Certificate from the InCommon CA
- Request a New Domain for InCommon CA Certificates