

InCommon®



InCommon Certificate Manager

Initiating Domain Control Validation (DCV)

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Domain Control Validation in InCommon Certificate Manager

The purpose of this document is to explain the new domain control validation (DCV) processes for the InCommon Certificate Manager (CM).

DCV is an industry wide directive that requires all Certificate Authorities (CAs) to verify domain control prior to the issuance of a certificate to a domain. This affects all new certificate applications and certificate renewals. DCV requirements apply to all SSL web-server certificate types.

InCommon has simplified the DCV process by seamlessly integrating DCV fulfillment wizards into the InCommon CM interface. We are always looking for feedback: if you have any questions or comments, then please contact us at admin@incommon.org.

- [What is DCV?](#)
- [What implementation choices are available?](#)
- [How to initiate DCV in InCommon CM?](#)

What is DCV?

- Before any SSL certificate can be issued, the registrable domain name (e.g. domain.com, domain.edu, domain.net, etc.) must pass DCV. This confirms to InCommon that the applicant has control of the domain for which the certificate application is being made. Once passed, DCV will remain valid for domain names within InCommon CM for 1 year (meaning subsequent certificates can be issued to the same domain without requiring another round of DCV).
- You can complete DCV using any one of three supported methods - Email, CNAME or HTTP / HTTPS. You can use any combination of the three methods across your domains as per your business preference.
- If a wildcard domain is created and delegated to an Organization or a Department, InCommon CM will validate only the registered High Level Domain (HLD). If the HLD is successfully validated, all the sub domains within the name space of the HLD will be considered validated.
- For Multi-Domain Certificates and Unified Communications Certificates, all listed domains must pass DCV.
- Your existing domains will continue to work. DCV only comes into play when an existing domain is next up for renewal.

What implementation choices are available?

There are three supported methods of DCV: Email, HTTP / HTTPS and CNAME. All three methods are automated and will take just a few minutes to complete

Email

When using the email challenge-response system, the applicant must be able to receive an email sent to an address at the domain for which the application is being made.

The email will contain a unique validation code that the applicant has to paste into a confirmation web-page before the application can proceed. InCommon's automated system will retrieve addresses registered to the domain from the Whois database and present them to the application for selection. The system also presents a selection of 'typical' addresses, such as admin@domain.edu, webmaster@domain.edu, hostmaster@domain.edu, administrator@domain.edu and postmaster@domain.edu.

[How to initiate Email DCV](#)

HTTP/HTTPS

InCommon CM 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 location mentioned in the wizard before clicking the 'Test' button.

[How to initiate HTTP/HTTPS DCV](#)

CNAME

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
```

[How to initiate CNAME DCV](#)

How to initiate DCV in InCommon CM?

Note - Prior to initiating DCV, administrators (RAO or DRAO) should add domains to InCommon CM, delegate the domain to either an organization or a department and await approval by InCommon. Once the domain shows as "Approved" in the CM:

First open the DCV configuration screen by selecting 'Settings > Domains > DCV'

Certificates | Discovery | Reports | Admins | **Settings** | About

Organizations | Domains | Notifications | Encryption | Access Control | E-mail Template | Certificates

Delegations | DCV

Add Filter:

Group by:

|

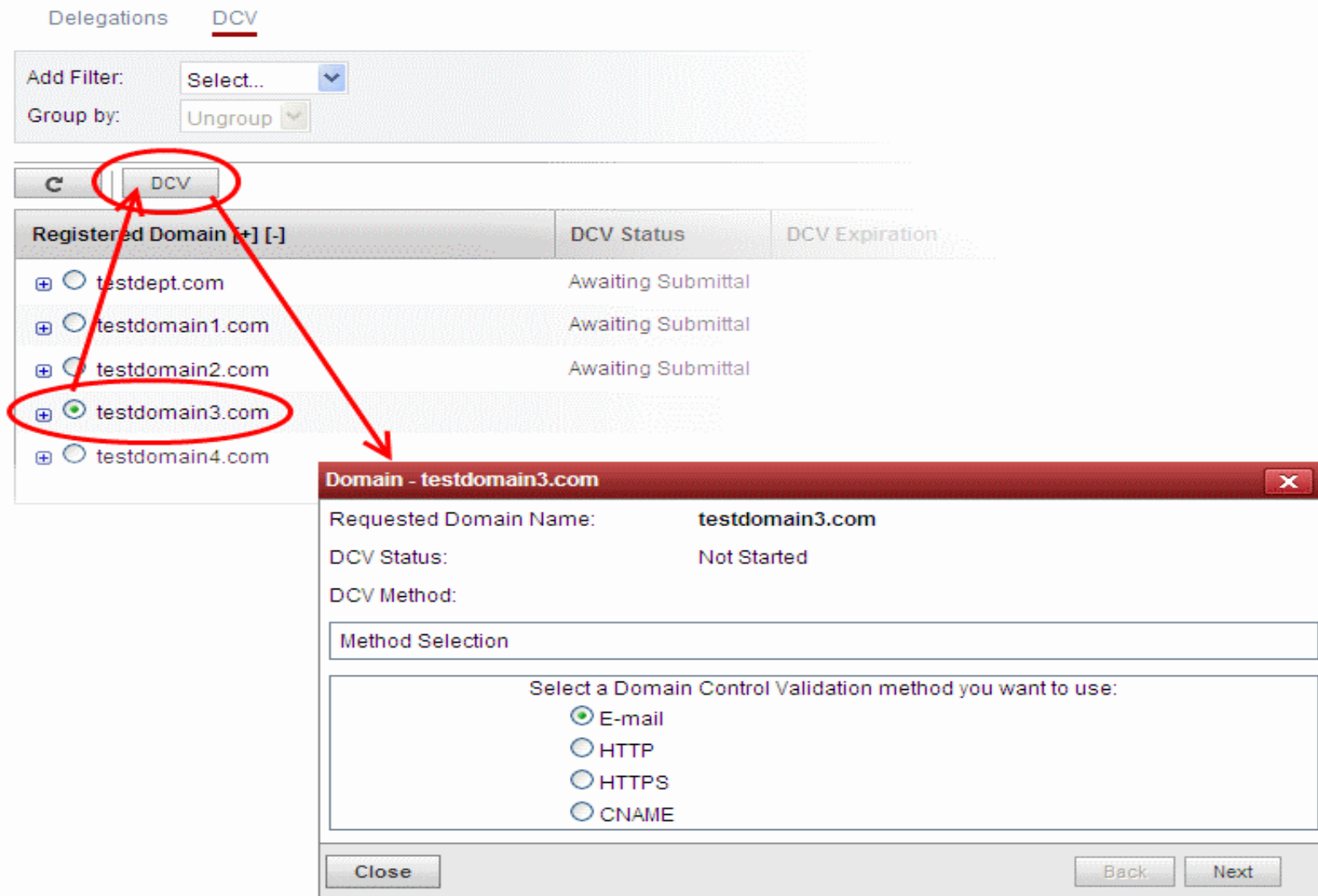
Registered Domain [+] [-]	DCV Status	DCV Expiration	Method
<input type="radio"/> testdept.com	Awaiting Submittal		HTTP
<input type="radio"/> testdomain1.com	Awaiting Submittal		EMAIL
<input type="radio"/> testdomain2.com	Awaiting Submittal		EMAIL
<input checked="" type="radio"/> testdomain3.com			
<input type="radio"/> testdomain4.com			

rows/page 26 - 30 out of 35

Column Display	Description
Registered Domain	A list of all available Domains created for this account. Clicking the '+' beside a domain name displays the sub-domains of the registered domain.
DCV Status	<p>Indicates the validation status of the domain. The status can be one of the following:</p> <ul style="list-style-type: none"> • Not Started - The DCV process has not been initiated for the registered high level domain (HLD). • Awaiting Submittal - The DCV process has been initiated but the request has not yet been submitted to the Domain Administrator. This status will be available only for the following DCV methods: <ul style="list-style-type: none"> • HTTP/HTTPS • CNAME • Submitted - The DCV request has been submitted to the domain administrator. • Validated - The registered high level domain (HLD) has been successfully validated • Expired - The DCV request has expired for the HLD.
DCV Expiration	Indicates the expiry date of the DCV request.
Method	Indicates the DCV method chosen by the administrator for validating the domain.
'DCV' Control Button	Enables the MRAO and RAO/DRAO SSL Administrators to initiate or restart the DCV

Column Display	Description
Note: The DCV Control button appears only on selecting a domain.	process for the selected Domain.

- Next, initiate DCV by selecting the domain and clicking the 'DCV' button that appears at the top. This will open the DCV wizard:



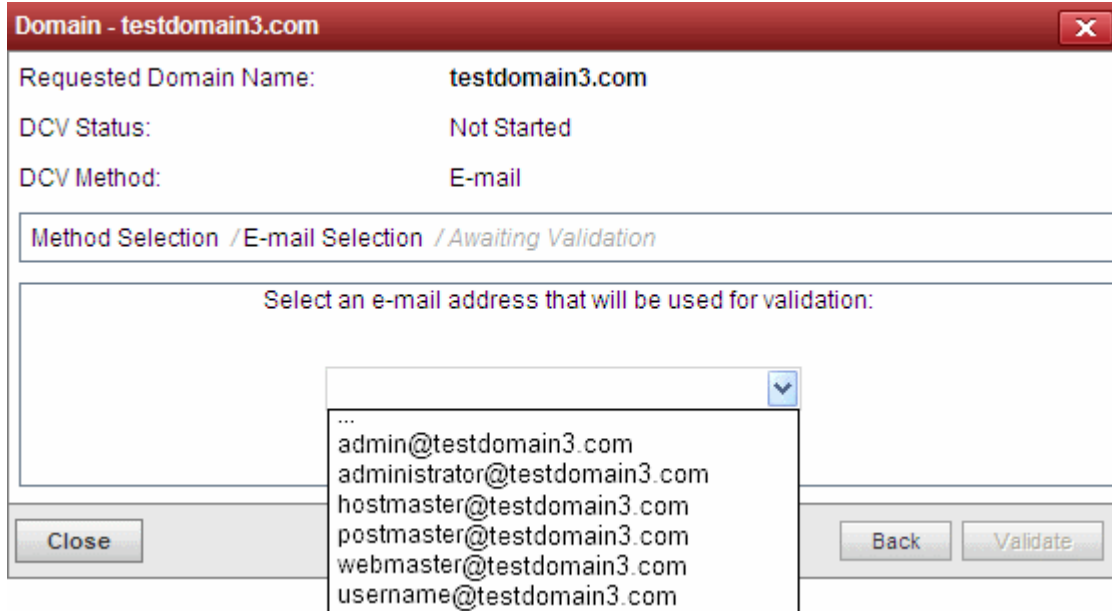
The screenshot shows the 'Delegations' tab with the 'DCV' sub-tab selected. A table lists registered domains with their DCV status. The 'testdomain3.com' row is selected, and the 'DCV' button above it is highlighted with a red circle. A red arrow points from this button to a modal window titled 'Domain - testdomain3.com'. The modal window displays the requested domain name, DCV status, and a 'Method Selection' section with radio buttons for E-mail, HTTP, HTTPS, and CNAME. The 'E-mail' option is selected.

Registered Domain [+]	DCV Status	DCV Expiration
<input type="radio"/> testdept.com	Awaiting Submittal	
<input type="radio"/> testdomain1.com	Awaiting Submittal	
<input type="radio"/> testdomain2.com	Awaiting Submittal	
<input checked="" type="radio"/> testdomain3.com		
<input type="radio"/> testdomain4.com		

- Select one of these DCV methods:
 - [Email](#)
 - [HTTP/HTTPS](#)
 - [CNAME](#)

Email

After choosing 'Email', the next step is to choose the address to which the DCV challenge-response email will be sent. The applicant must, of course, be able to receive emails at this address. DCV will be completed when the applicant verifies domain control by clicking a link in the email.



The screenshot shows a web application window titled "Domain - testdomain3.com". The window displays the following information:

- Requested Domain Name: testdomain3.com
- DCV Status: Not Started
- DCV Method: E-mail

Below this information is a breadcrumb trail: "Method Selection / E-mail Selection / Awaiting Validation". The main content area contains the instruction: "Select an e-mail address that will be used for validation:". A drop-down menu is open, showing a list of email addresses for the domain testdomain3.com:

- ...
- admin@testdomain3.com
- administrator@testdomain3.com
- hostmaster@testdomain3.com
- postmaster@testdomain3.com
- webmaster@testdomain3.com
- username@testdomain3.com

At the bottom of the window, there are three buttons: "Close", "Back", and "Validate".

The drop-down menu contains a list of registered email addresses for this domain that have been dynamically drawn from Whois. It also contains 'typical' email addresses such as:

- admin@domain.com
- administrator@domain.com
- hostmaster@domain.com
- postmaster@domain.com
- webmaster@domain.com

Click the 'Validate' button after making your selection. A challenge-response email will be sent to the selected email address. The DCV status of the domain will change to 'Submitted'.

Domain - testdomain3.com ✕

Requested Domain Name:	testdomain3.com
DCV Status:	Submitted
DCV Method:	E-mail

Method Selection / E-mail Selection / Awaiting Validation

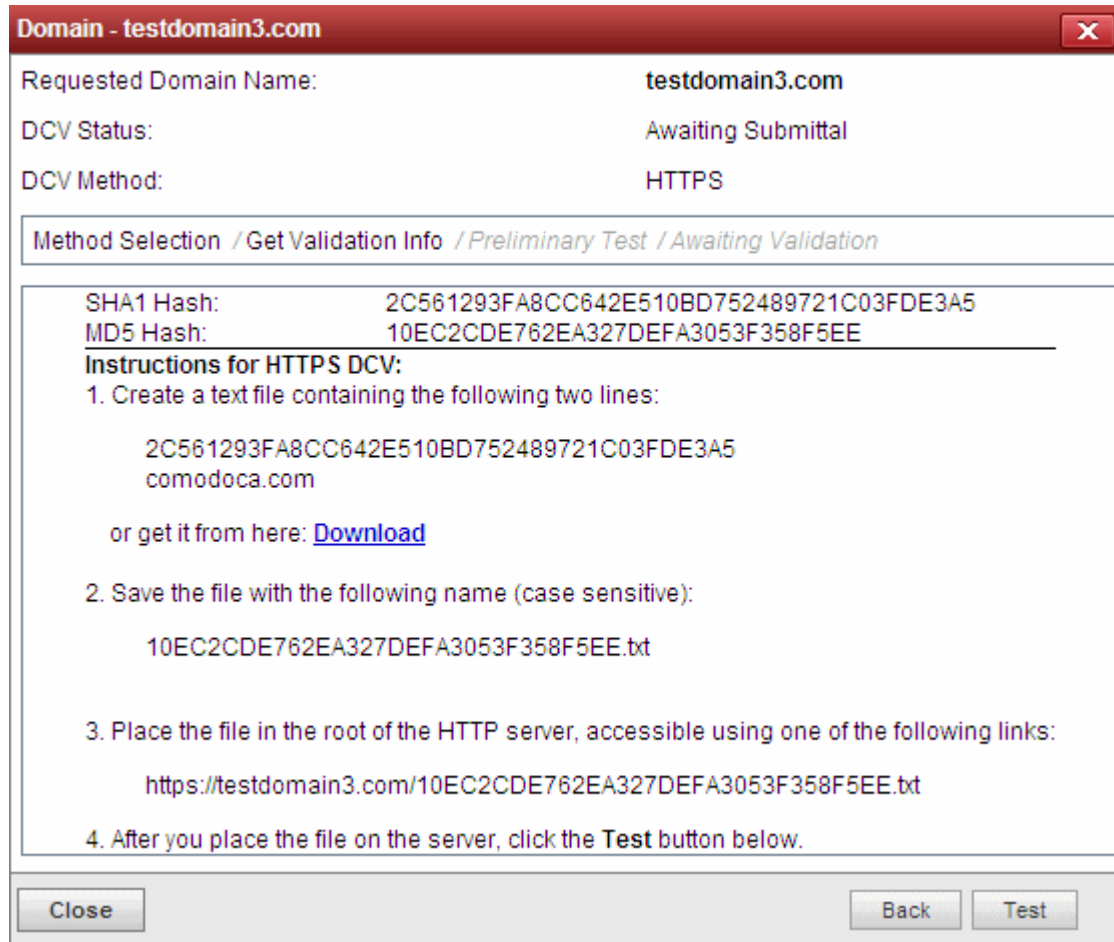
A validation letter was sent to **administrator@testdomain3.com**
Please follow the instructions it contains.

Close Reset

Upon receiving the email, the applicant should click the link in the email and enter the unique code into a validation web-form. If DCV is successful, the status of the domain will change to 'Validated'.

HTTP/HTTPS

InCommon CM generates a specific text (.txt) file which must be placed on the root directory of the domain undergoing DCV. InCommon systems will check for the presence and content of this file and if verified as correct, the domain will pass DCV.



Requested Domain Name:	testdomain3.com
DCV Status:	Awaiting Submittal
DCV Method:	HTTPS

Method Selection / Get Validation Info / Preliminary Test / Awaiting Validation

SHA1 Hash:	2C561293FA8CC642E510BD752489721C03FDE3A5
MD5 Hash:	10EC2CDE762EA327DEFA3053F358F5EE

Instructions for HTTPS DCV:

1. Create a text file containing the following two lines:

```
2C561293FA8CC642E510BD752489721C03FDE3A5  
comodoca.com
```


or get it from here: [Download](#)
2. Save the file with the following name (case sensitive):

```
10EC2CDE762EA327DEFA3053F358F5EE.txt
```
3. Place the file in the root of the HTTP server, accessible using one of the following links:

```
https://testdomain3.com/10EC2CDE762EA327DEFA3053F358F5EE.txt
```
4. After you place the file on the server, click the **Test** button below.

Close Back Test

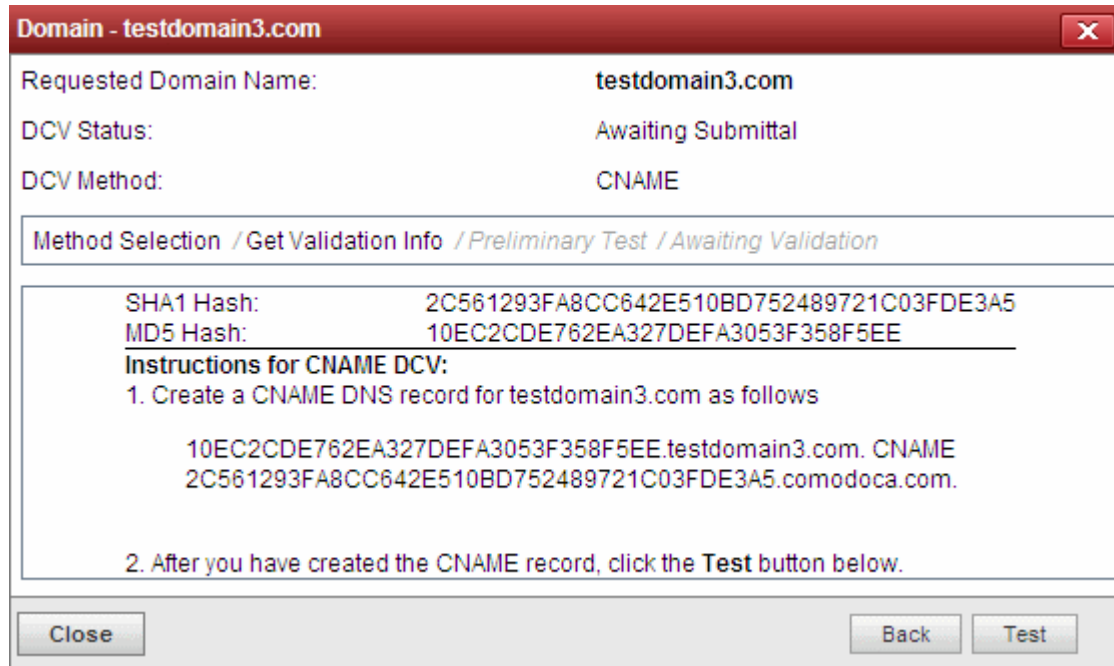
Place the file in the root directory of the domain in question so that it is publicly accessible at one of the paths specified in step number three (see image above). Click 'Test' to check that the file has been uploaded correctly. If correct, the 'Submit' dialog will appear and the DCV status of the domain will change to 'Submitted'. InCommon systems will now attempt to perform DCV by checking for this file. If successful, the DCV status of the domain will change to 'Validated'.

If you need time to get the file uploaded to your server, you can close this wizard and submit later. This can be done by returning to the main DCV interface (Settings > Domains > DCV) then clicking the DCV button alongside the appropriate domain. Again, you need to click 'Test' then 'Submit'.

CNAME

The CNAME method allows you to complete DCV by creating a CNAME DNS record which includes two unique hash values (MD5 & SHA1) generated for you by InCommon CM. The CNAME record should be passed to your domain administrator for implementation, if necessary. The format we look for:

<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com



Requested Domain Name:	testdomain3.com
DCV Status:	Awaiting Submittal
DCV Method:	CNAME

Method Selection / Get Validation Info / Preliminary Test / Awaiting Validation

SHA1 Hash: 2C561293FA8CC642E510BD752489721C03FDE3A5
MD5 Hash: 10EC2CDE762EA327DEFA3053F358F5EE

Instructions for CNAME DCV:

1. Create a CNAME DNS record for testdomain3.com as follows

10EC2CDE762EA327DEFA3053F358F5EE.testdomain3.com. CNAME
2C561293FA8CC642E510BD752489721C03FDE3A5.comodoca.com.

2. After you have created the CNAME record, click the **Test** button below.

Close Back Test

Copy the CNAME DNS record provided and pass it to your domain administrator. Click 'Test' to check the record is correct. If correct, the 'Submit' dialog will appear. The DCV status of the domain will change to 'Submitted'. InCommon systems will now attempt to perform DCV by checking for this record. If successful, the DCV status of the domain will change to 'Validated'.

If you need time to get the record created, you can close this wizard and submit later. This can be done by returning to the main DCV interface (Settings > Domains > DCV) then clicking the DCV button alongside the appropriate domain. Again, you need to click 'Test' then 'Submit'.

Additional Resources

- [InCommon Certificate Manager RAO Admin Guide](#) - Section 4.4.2.1.2 DCV
- Comodo Support Knowledge Base (Comodo is an InCommon partner) - <https://support.com/index.php?m=knowledgebase&a=viewarticle&kbarticleid=1367>