

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 CM'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 'Submit' 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:

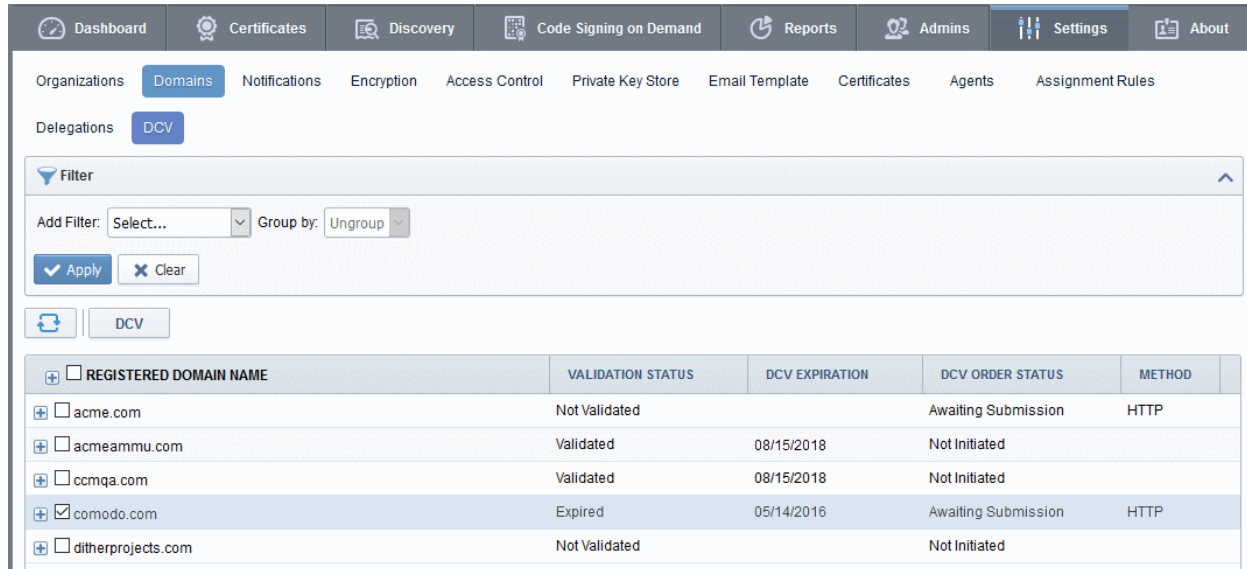
```
<MD5 hash>.yourdomain.com CNAME <SHA-1 hash>.comodoca.com
```

[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'



The screenshot shows the 'Domains' tab in the Certificate Manager. It includes a filter section with 'Add Filter' and 'Group by' dropdowns, and an 'Apply' button. Below the filter is a table with the following data:

REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV EXPIRATION	DCV ORDER STATUS	METHOD
<input type="checkbox"/> acme.com	Not Validated		Awaiting Submission	HTTP
<input type="checkbox"/> acmeammu.com	Validated	08/15/2018	Not Initiated	
<input type="checkbox"/> ccmqa.com	Validated	08/15/2018	Not Initiated	
<input checked="" type="checkbox"/> comodo.com	Expired	05/14/2016	Awaiting Submission	HTTP
<input type="checkbox"/> ditherprojects.com	Not Validated		Not Initiated	

Column Header	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.
Validation Status	Whether the domain has passed DCV or not. Status can be one of the following: <ul style="list-style-type: none"> Not Validated - DCV has not been initiated or is in-progress for the registered high level domain (HLD). Validated - The registered high level domain has passed DCV Expired - DCV on the domain has expired and has to be renewed. The DCV process has to be restarted for the domain
DCV Expiration	Indicates the date when Domain Control Validation for the domain expires. The DCV has to be done again after the expiry period.
DCV Order Status	Progress of validation on the domain. Status can be one of the following: <ul style="list-style-type: none"> Not Initiated - DCV has not been started for the registered high level domain (HLD). Awaiting Submittal - DCV has been initiated but the request has not yet been sent to the domain administrator (the admin who has control of the web server on which the domain is hosted). The 'Awaiting...' status is only available for the following DCV methods: <ul style="list-style-type: none"> HTTP / HTTPS CNAME Submitted - The DCV request has been sent to the domain administrator for implementation. Validated - The registered high level domain (HLD) has passed DCV.

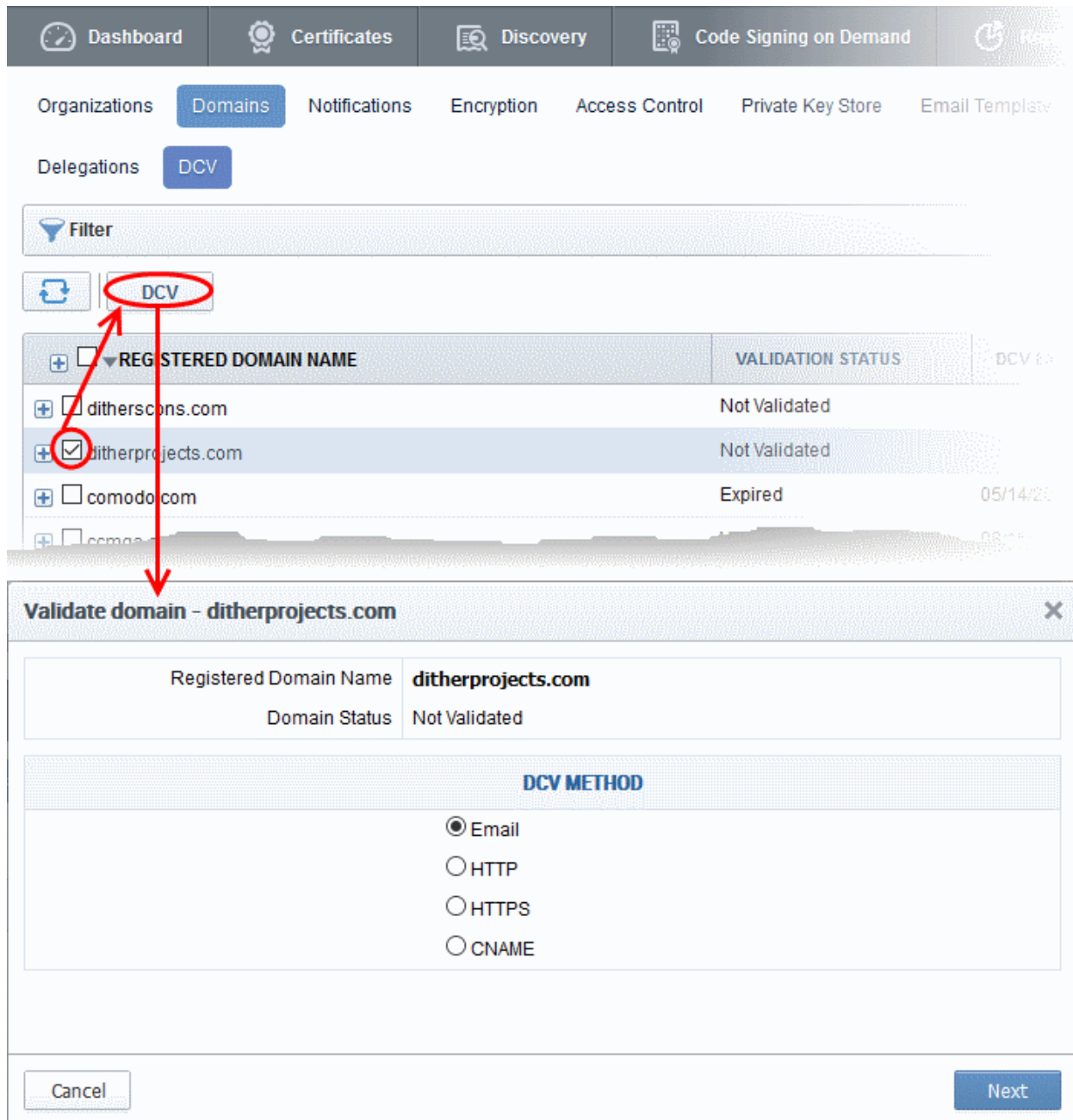
Column Header	Description
	<ul style="list-style-type: none"> Expired - DCV has expired on the domain. The DCV process has to be restarted for the domain .
Method	Indicates the DCV method chosen by the administrator for validating the domain.
DCV Control Button Note: The DCV Control button appears only on selecting a domain.	Enables the MRAO and RAO/DRAO SSL Administrators to initiate or restart the DCV process for the selected Domain.

The following sections explain on:

- [Validating a single domain](#)
- [Validating multiple domains at a time](#)

Validating a Single Domain

- 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 InCommon Certificate Manager interface. The top navigation bar includes Dashboard, Certificates, Discovery, Code Signing on Demand, and Renew. Below this, there are tabs for Organizations, Domains, Notifications, Encryption, Access Control, Private Key Store, and Email Templates. Under Domains, there are tabs for Delegations and DCV. A Filter section is visible above a table of registered domain names. The table has columns for Registered Domain Name, Validation Status, and DCV ID. The row for ditherprojects.com is selected, and its DCV ID is circled in red. A red arrow points from this DCV ID to a 'Validate domain - ditherprojects.com' dialog box. The dialog box shows the Registered Domain Name as ditherprojects.com and the Domain Status as Not Validated. Under the DCV METHOD section, there are four radio button options: Email (selected), HTTP, HTTPS, and CNAME. At the bottom of the dialog box, there are 'Cancel' and 'Next' buttons.

REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV ID
ditherscons.com	Not Validated	
ditherprojects.com	Not Validated	
comodo.com	Expired	05/14/23
ccmg.com		08/11/23

Validate domain - ditherprojects.com

Registered Domain Name: **ditherprojects.com**
Domain Status: Not Validated

DCV METHOD

Email
 HTTP
 HTTPS
 CNAME

Cancel Next

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

Email

On selection of EMAIL method, the next step allows you to select the email address of the Domain Administrator for sending the validation email.

Validate domain - ditherprojects.com

1 Email Selection ————— 2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	Email

Email Address

Select an email address:*

...
admin@ditherprojects.com
administrator@ditherprojects.com
hostmaster@ditherprojects.com
postmaster@ditherprojects.com
webmaster@ditherprojects.com

Save & Close Back Submit

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'.

Validate domain - ditherprojects.com

1 Email Selection ————— 2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	Email

A validation letter was sent to **admin@ditherprojects.com**.
Please, follow the instructions it contains.

Reset OK

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 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.

Validate domain - ditherprojects.com
✕

1 Get Validation Info
2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	HTTPS_CSR_Hash

SHA256 Hash	d79b9ba1f019f9a8858d41d319a9f5d7e13f893542b97b1a9ca9eb7bcfe04a62
MD5 Hash	52c5eb5a3d95e4fcd4b39de20c3c442b

Instructions for HTTPS DCV

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

```
d79b9ba1f019f9a8858d41d319a9f5d7e13f893542b97b1a9ca9eb7bcfe04a62
comodoca.com
```

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

```
52C5EB5A3D95E4FCD4B39DE20C3C442B.txt
```
3. Place the file in the /.well-known/pki-validation directory of the HTTPS server, so that it is accessible via the following link:

```
https://ditherprojects.com/.well-known/pki-validation/52C5EB5A3D95E4FCD4B39DE20C3C442B.txt
```
4. After you have placed the file on the server, click **Submit** button below.

Save & Close
Back
Submit

- Click the 'here' link in item 1 and save the .txt file or create a new notepad file, copy and paste the string given in item 1 and save the file with the name given in item 2.
- Click 'Save & Close'. InCommon CM will save the hash value generated for future comparison.
- Send the .txt file to the Domain Administrator through any out-of-band communication method like email and request the domain administrator to place the file in the root of the HTTP/HTTPS server, so that the file is accessible by one of the paths specified in item 3.
- Once the Domain Administrator has placed the .txt file on the HTTP HTTPS server, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab
- Resume the DCV process by selecting the domain and clicking the 'DCV' button
- Click 'Submit'. The DCV Order status of the domain will change to 'Submitted'.

Validate domain - ditherprojects.com
✕

1 Get Validation Info
2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	HTTPS_CSR_Hash

A request for HTTPS validation of **ditherprojects.com** has been successfully submitted.

Awaiting the validation result...

Reset
OK

- InCommon CM will check whether the file has been placed in the web server root and validate the domain. On successful validation, the DCV Order status of the domain will change to 'Validated'.

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

Validate domain - ditherprojects.com
✕

1 Get Validation Info
2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Awaiting Submission
DCV method	CNAME_CSR_Hash

SHA256 Hash **5452a0a15d3a9b3d51765a1f68b6d440c80f517eed1eac31bd9cbcd8cd86900b**

MD5 Hash **546f0fd9977f2339752e6ac5d6fd09f2**

Instructions for CNAME DCV

1. Create a CNAME DNS record for **ditherprojects.com** as shown below:

`_546f0fd9977f2339752e6ac5d6fd09f2.ditherprojects.com. CNAME
5452a0a15d3a9b3d51765a1f68b6d440.c80f517eed1eac31bd9cbcd8cd86900b.comodoca.com.`

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

Save & Close
Back

Submit

- Copy the CNAME DNS record given in item no. 1 and pass it to the domain administrator through any out-of-band communication method like email and request the domain administrator to create the record for the domain.
- Click 'Save & Close'. InCommon CM will save the hash value generated for future comparison.
- After the Domain Administrator has created the record, open the DCV interface by clicking 'Settings' > 'Domains' > 'DCV' tab
- Resume the DCV process by selecting the domain and clicking the 'DCV' button.
- Click 'Submit'. The DCV Order status of the domain will change to 'Submitted'.

Validate domain - ditherprojects.com

1 Get Validation Info ————— 2 Order Submission

Registered Domain Name	ditherprojects.com
Domain Status	Not Validated
DCV Order Status	Submitted
DCV method	CNAME_CSR_Hash

SHA256 Hash	5452a0a15d3a9b3d51765a1f68b6d440c80f517eed1eac31bd9cbcd8cd86900b
MD5 Hash	546f0fd9977f2339752e6ac5d6fd09f2

A request for CNAME validation of **ditherprojects.com** has been successfully submitted.

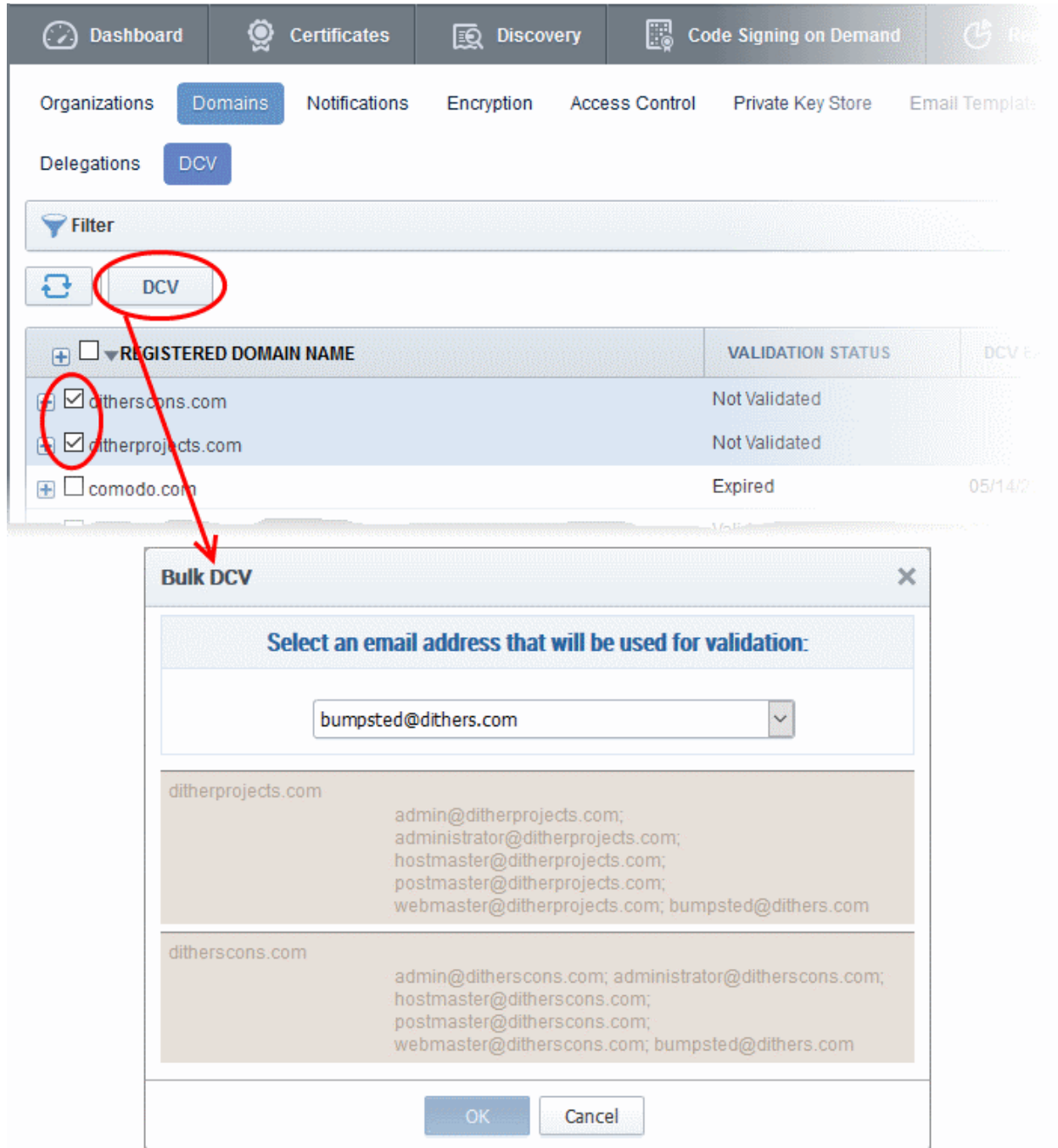
Awaiting the validation result...

Reset OK

- InCommon CM will check whether the record has been created. If it is found created, the DCV Order status of the domain will change to 'Validated'.

Validating Multiple Domains at a time

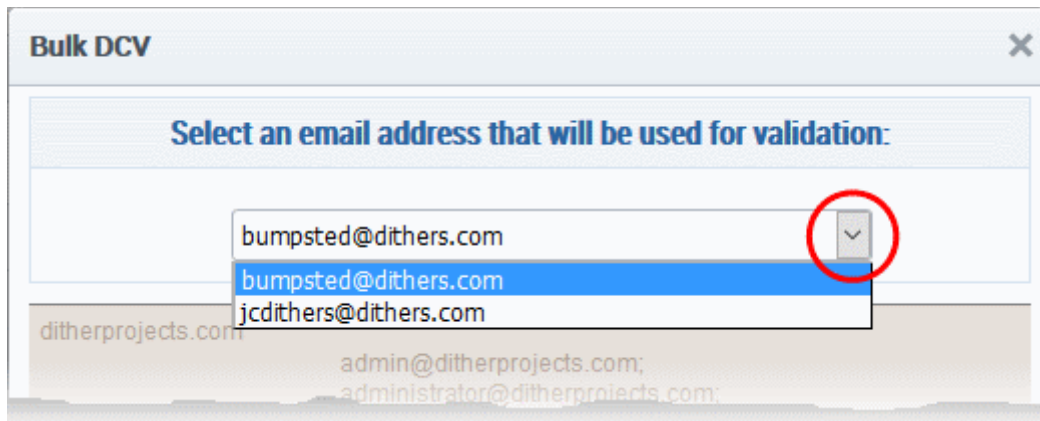
1. Initiate DCV by selecting the domains that share common domain administrator email address
2. Click the 'DCV' button



The screenshot shows the InCommon Certificate Manager interface. The top navigation bar includes Dashboard, Certificates, Discovery, Code Signing on Demand, and Reports. Below this, there are tabs for Organizations, Domains, Notifications, Encryption, Access Control, Private Key Store, and Email Templates. Under Domains, there are tabs for Delegations and DCV. A Filter section is visible, followed by a refresh icon and a DCV button circled in red. Below this is a table with columns for REGISTERED DOMAIN NAME, VALIDATION STATUS, and DCV EXPIRES. The table lists domains: ditherscons.com (Not Validated), ditherprojects.com (Not Validated), and comodo.com (Expired). A red arrow points from the DCV button to a 'Bulk DCV' dialog box. The dialog box has a title bar 'Bulk DCV' and a close button. It contains a section titled 'Select an email address that will be used for validation:' with a dropdown menu showing 'bumpsted@dithers.com'. Below this are two lists of email addresses for 'ditherprojects.com' and 'ditherscons.com'. The 'ditherscons.com' list includes 'bumpsted@dithers.com'. At the bottom are 'OK' and 'Cancel' buttons.

REGISTERED DOMAIN NAME	VALIDATION STATUS	DCV EXPIRES
<input checked="" type="checkbox"/> ditherscons.com	Not Validated	
<input checked="" type="checkbox"/> ditherprojects.com	Not Validated	
<input type="checkbox"/> comodo.com	Expired	05/14/2012

The Bulk DCV dialog will open. The dialog contains lists of possible domain administrator email addresses and the email addresses fetched from the Whois database for each domain. Common email addresses identified from the lists are displayed in the drop-down at the top.



3. Select the email address of the administrator who can receive and respond to the validation mail from the drop-down and click 'OK'.

An automated email will be sent to the selected Domain Administrator email address. The DCV status of the Domain will change to 'Submitted'.

On receiving the email, the domain administrator should click the validation link in it to open the validation form and enter the validation code contained in the email, in order to complete the validation process. Once completed, the DCV status of the Domains will change to 'Validated'.

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