How to validate a SSL order

Question

How to validate a SSL order once the request has been made?

Answer

In order for Sectigo to issue the SSL Certificate, one or multiple validation steps have to be taken to ensure that the company who requested the SSL, is also actually the owner. Which steps have to be taken all depends on the "Type of certificate" you have selected.

DV Certificates

- DCV Validation

OV Certificates

- DCV Validation
- Company validation
- Phone Validation

EV Certificates

- DCV Validation
- Company validation
- Phone Validation
- Signed Documents

DCV validation (Domain Control

Validation)

This is a check to confirm that you have ownership over the domain for which you are requesting the SSL Certificate.
This can be done by 1 of 3 options; via email confirmation, via a record in the DNS or file a file on the server.

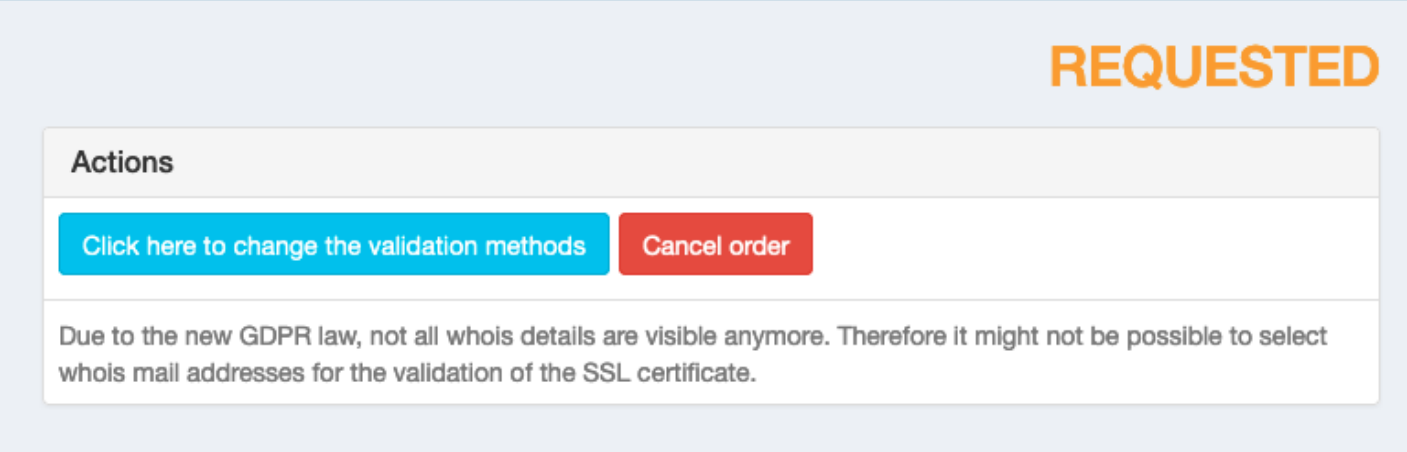
Email validation

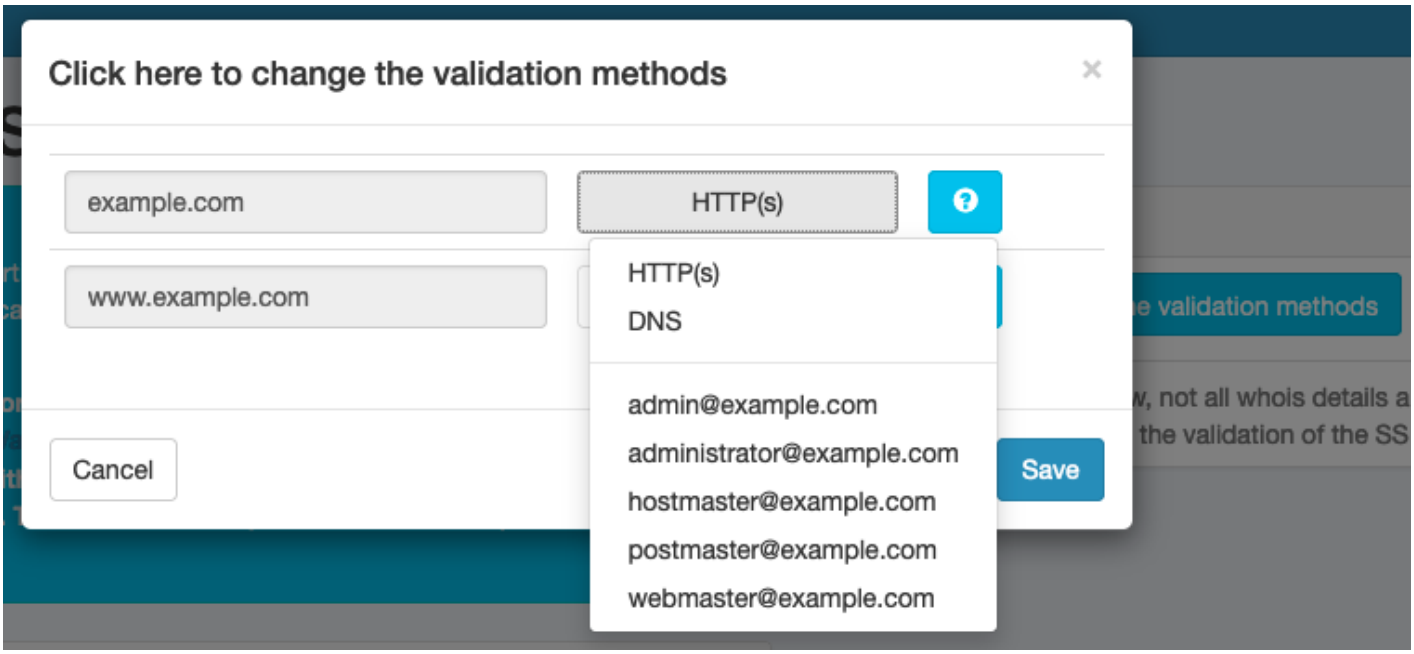
Confirming an email that is linked to the domain name is one of the options to proof that you own the domain. Therefore is not not possible to sent this email to any random email address, but it has to be connected to the domain.

The following so-called "approver email addresses" are provided as options:

- **admin**@..., followed by the (sub) domain of the certificate ;
- **administrator**@..., followed by the (sub) domain of the certificate ;
- **postmaster**@..., followed by the (sub) domain of the certificate ;
- **hostmaster**@..., followed by the (sub) domain of the certificate ;
- **webmaster**@..., followed by the (sub) domain of the certificate ;
- WHOIS-visible email [**Deprecated** - ***public Certificate Authorities will no longer allow WHOIS-based email addresses for domain validation. You can read more information about this here***]

Via the SSL panel, you can review all available options and make changes if required.





The email itself will be sent from noreply_support@trust-provider.com, with the subject Comodo Domain Validation for [domainname] (reference #number)

Sectigo Certification Authority
Comodo Domain Validation for [redacted] (reference #22[redacted])
To: [redacted]

Inbox - Google 15:06

Dear [redacted]

Comodo has received a request to issue an SSL certificate for [redacted]

If you want to have this certificate issued, please browse to https://secure.trust-provider.com/products/EnterDCVCode?orderNumber=1638[redacted]96 and enter the following validation code:

cihDyIbdXbX*R2ZA[redacted]

Please ignore this email if neither you nor a trusted colleague made a request for a certificate. If you have any questions about this order, please contact the party where you have placed your order. Do not reply to this e-mail as it is not monitored.

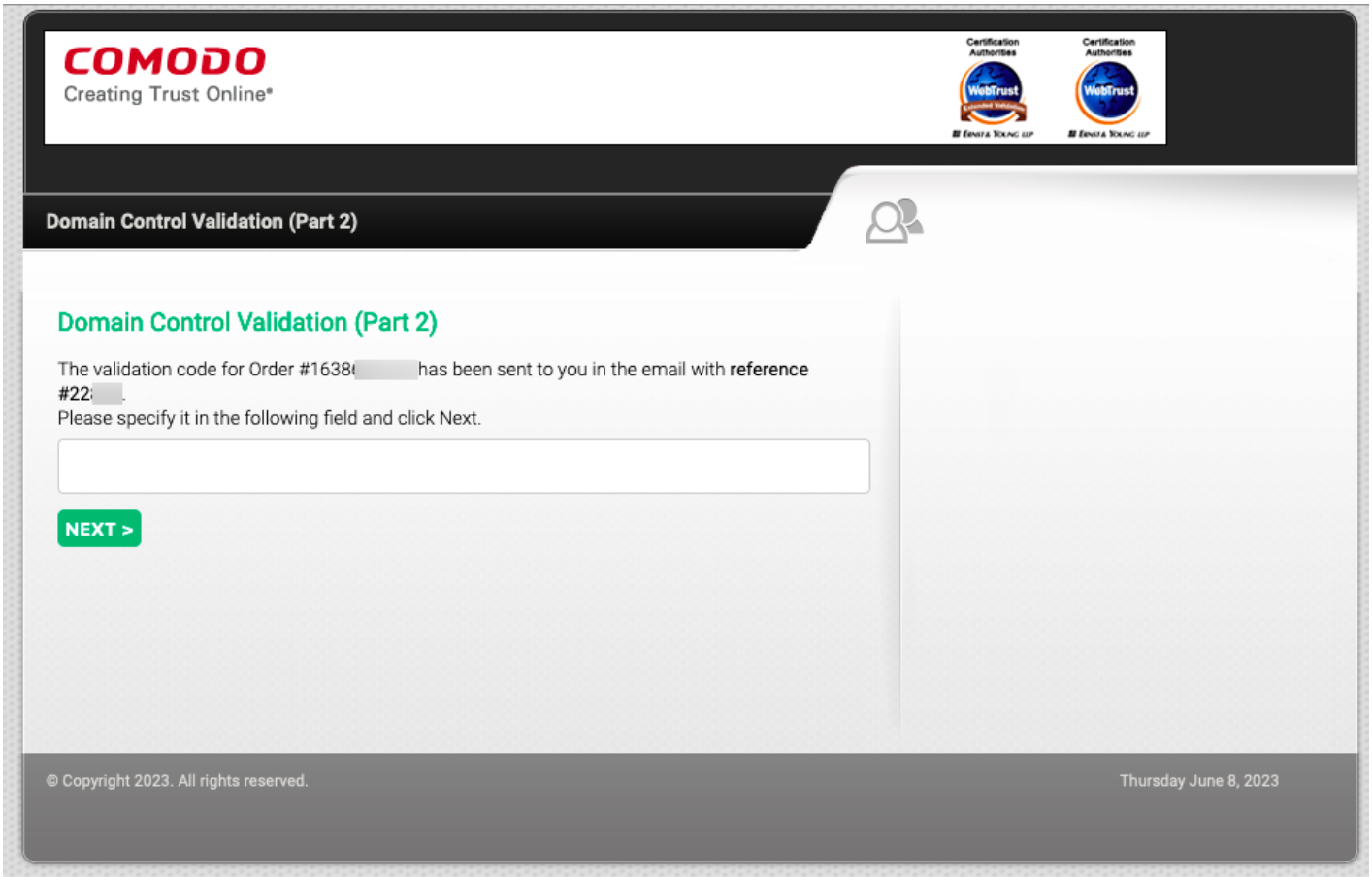
Kind Regards,

Comodo Security Services

Comodo CA Limited - US Office
525 Washington Blvd.
Jersey City, NJ 07310-1600

Comodo CA Limited - European Office
26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom

Please follow steps as described in the email to validate the request.

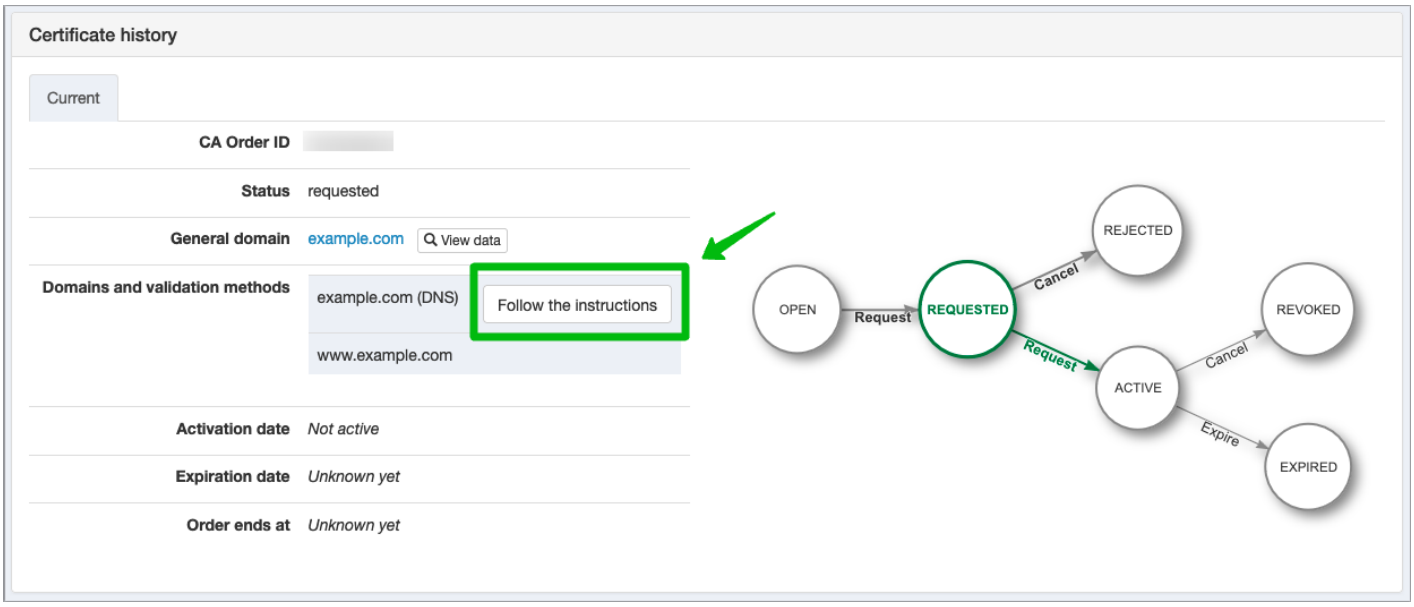


DNS validation

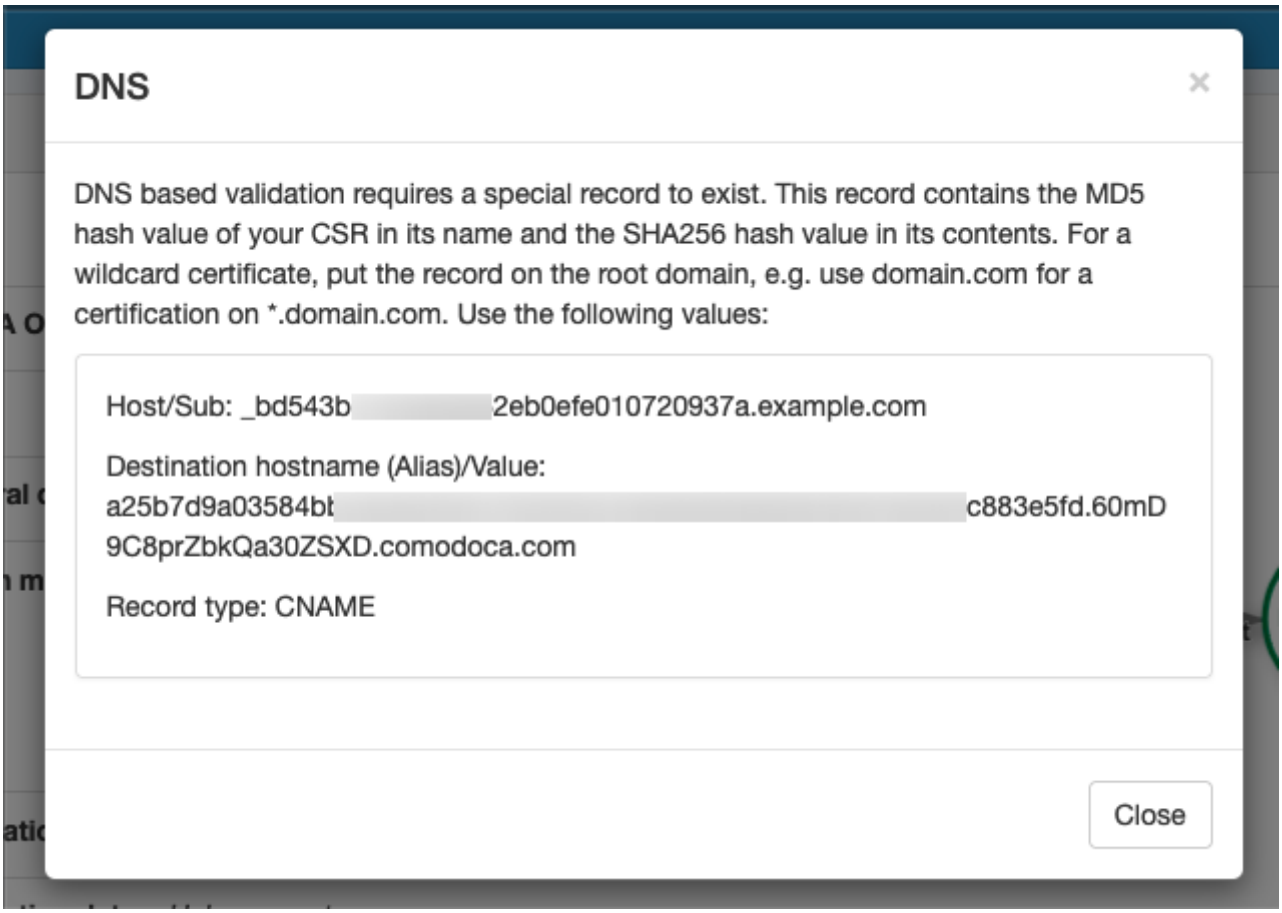
Another option to proof that you have control over the DNS, is by adding a record in the DNS zone of the domain. This option is especially interesting for resellers who control the DNS zone of the domain and prefer not to ask the registrant to go look for an email from Sectigo.

In case you select the DNS validation, you will need to add a CNAME in the zone of the domain. Please make sure to check where the zone is managed. If you manage the zone via Openprovider, you can add the record directly in the zone (or use the automated option during the SSL request) and in case you use a third party nameserver, you will need to add the record in the zone there.

The value which needs to be added will be unique and can be found in the SSL panel (or requested via API) via the button "Follow the instructions".



A pop-up will appear where you can find the details:

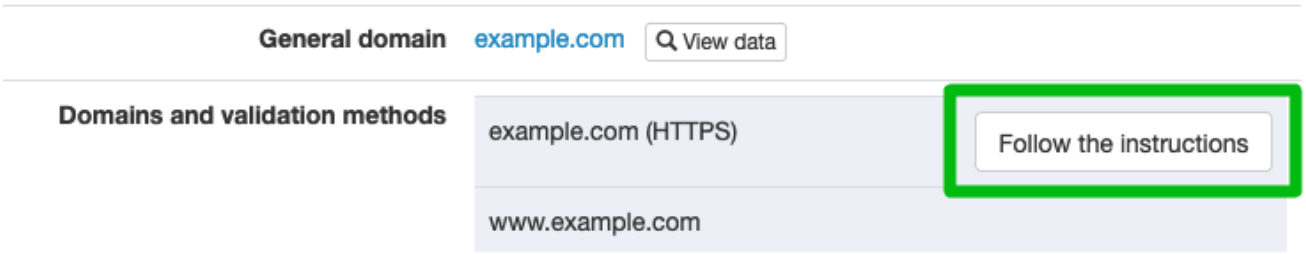


File validation (HTTP(s)

File validation (also referred to as HTTPs) validation works a bit similar.

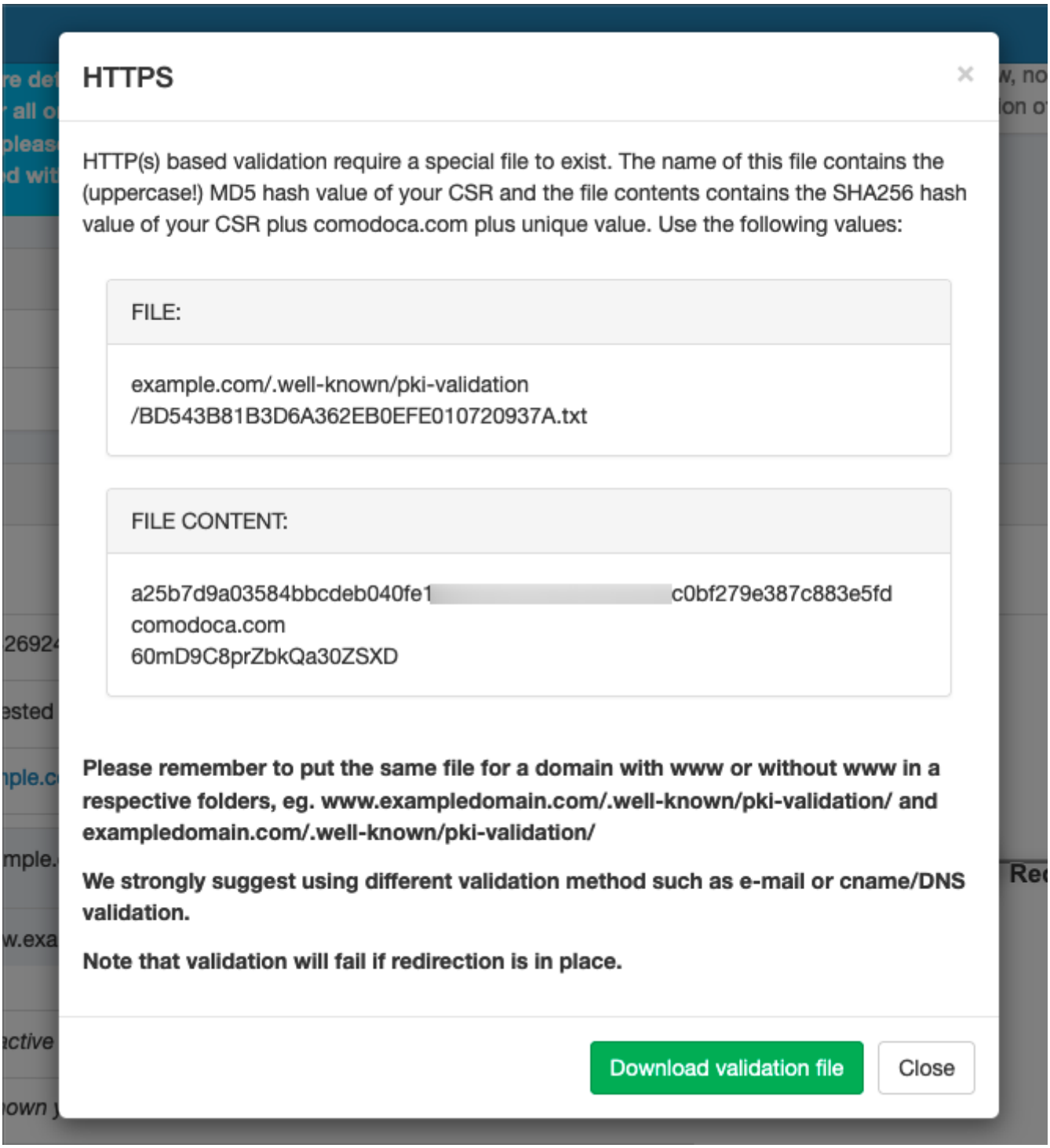
Hash values are provided to you to create a simple plain-text file and place this in a specific host directory on the server. Sectigo will check the location and when the file is visible, the validation is approved.

Please note: this method can not be used for validating certificates with **Wildcard** names. When using file validation for **multi-domain certificates**, domain validation will be required for every FQDN/SAN (domain) individually.
Note that validation will fail if redirection is in place.



The "hash: (the plain text value) which needs to be uploaded can be found in the ssl panel (Button "*Follow the instructions*" once the order is submitted or can be retrieved via API.

Please put the same file for a domain with www or without www in a respective folders, eg. www.exampledomain.com/.well-known/pki-validation/ and exampledomain.com/.well-known/pki-validation/



Company validation

Sectigo will verify that your organization is legally registered on the address that you have entered in the handle which you used to submit the request. This will typically be verify through a government database or online directories, like Dun & Bradstreet (https://www.dnb.com/), the Chamber of Commerce (for example; kvk.nl), etc.
Therefore it is very important that the information in the online directory is matching the information in the handle!

Phone Validation

In order to receive an OV and EV certificate, you must have a registered active telephone listing that is verifiable by an online telephone directory. It is important that your listing matches the exact business name and physical address that have been provided and verified.
In most cases the phone number is found in the company registration database when the company validation step is preformed.
During this call, Sectigo will ask to speak to the contact person which is mentioned in the handle

Note: It is **not** possible to ask Sectigo to call an unlisted phone number. It will only be possible to use phone numbers which are listed in a public directory. Your own website is not a public source, so phone numbers from your own website can not be used.

Signed Documents

In order to validate an EV certificate, a "subscriber agreement" document must be signed. This document will be sent to the email address mentioned in the handle.

Revision #2
Created 2026-08-07 14:38:01 UTC by Sarath
Updated 2026-08-07 15:52:30 UTC by Sarath