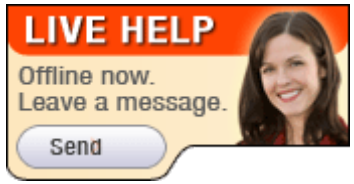
COMODO
Creating Trust Online™

Login

Your email address

Remember me

Lost password Login



Live Chat by LivePerson

NEWS

What can we help you with? SEARCH

Knowledgebase

Alternative Methods of Domain Control Validation (DCV)

All Comodo certificates **must** pass through DCV (Domain Control Validation) before they are issued. DCV is a mechanism used to prove ownership or control of a registered domain name.

There are 3 mechanisms for DCV:

1. **eMail-based DCV (Traditional)**
   You will be sent an email to an administrative contact for your domain. The email will contain a unique validation code and link. Clicking the link and entering the code will prove domain control.

   Valid email addresses are:
   Any email address which our system can scrape from a port 43 whois check;

   The following generic admin type email addresses @ the domain for which the certificate is being applied:

admin@
administrator@
postmaster@
hostmaster@
webmaster@

2. **DNS CNAME-based**

The CSR you submit to Comodo will be hashed. The hash values are provided to you and must be entered as a DNS CNAME record for your domain.

The hashes are to be entered as follows:

<Value of MD5 hash of CSR>.*yourdomain.com*. CNAME <value of SHA1 hash of CSR>.comodoca.com.

Note: Please take notice the trailing period/fullstop at the tail end of each of the TLDs as this is required to make the entry fully-qualified.

Note2: *yourdomain.com* in the example above (and below in the HTTP(S) method instructions) means the Fully Qualified Domain Name (FQDN) contained in the certificate. If you are ordering a MDC or UCC certificate, separate CNAME records must be created for EACH FQDN in your order.

Examples:

<Value of MD5 hash of CSR>.subdomain1.yourdomain.com. CNAME <value of SHA1 hash of CSR>.comodoca.com.

<Value of MD5 hash of CSR>.subdomain2.yourdomain.com. CNAME <value of SHA1 has of CSR>.comodoca.com.

3. **HTTP(S)-based DCV**

The CSR you submit to Comodo will be hashed. The hash values are provided to you and you must create a simple plain-text file and place this in the root of your webserver and served over HTTP-only!

The file and it's content should be as follows:

http://*yourdomain.com*/<Upper case value of MD5 hash of CSR>.txt

Content (as a plain text file):

<Value of SHA1 hash of CSR>
comodoca.com

Note: The DCV will fail if any redirection is in place.

Note 2: yourdomain.com in the example above (and in the CNAME method instructions; above) means the Fully Qualifed Domain Name (FQDN) contained in the certificate. If you are ordering a MDC or UCC, each FQDN in the certificate MUST have the TXT file in place in its root folder.

Examples:

subdomain1.yourdomain.com/<Value of MD5 hash of CSR>.txt
subdomain2.yourdomain.com/<Value of MD5 hash of CSR>.txt

Additional Information

In the event that you were not provided with your CSR hashes, then you may use our Online CSR Decoder.

We recommend using the follow settings before clicking the **Decode** button:

* Uncheck **Show Empty Fields**
* Check **Show CSR Hashes**

Notes

Re-issuing

Re-issues of the certificates will require re-validation *unless* the re-issue is within 7 days of the original validation and is for the same end-customer account.

We now allow the re-issue to *not* require revalidation of already-validated FQDNs *if the same private key is used to generate the CSR for re-issue*. If a new private key is used to generate the CSR, then the order must have DCV re-performed by one of the available methods for all FQDNs in the request before the certificate can be issued.

This will also apply to re-issues that facilitate the addition or removal of domains for multi-domain certificates.

www. sub-domains

For all of the above validation methods, we consider proof of control of 'www.DOMAIN' as also proving control of 'DOMAIN'.

This rule doesn't apply to any other sub-domain or sub-domains, but only to 'www'. It does not apply for 'www1.', or 'mail.', or 'ftp.', or any other sub-domain.

This behavior is to support the very common use-case where a customer applies for both 'www.DOMAIN' and 'DOMAIN' as FQDNs in a certificate, but has only so far configured his web server to serve the 'www.' sub-domain.

This only holds when DOMAIN is also an FQDN that we would issue a certificate for.

(1374 vote(s)) Helpful Not helpful

Comments (3)

GEPL Capital Pvt ltd
November 23 2016 07:49

Please reissue the SSL certificate for the new server i already the Key file

Jan Tongar
December 03 2016 22:13

I need re-issuing of Cert, since we loss the private key. Many tks

Tep Chanveasna
January 03 2017 10:10

I didn't have the certificate