

Changes in Domain Control Validation Procedure

On the 15th of November 2021, the DCV (Domain Control Validation) procedure will be adjusted to meet new requirements from CA.

What is Domain Control Validation?

Domain Control Validation (DCV) is the process by which a CA gains evidence that a particular domain is managed by the applicant for a certificate.

One of these options is file-based validation (also called; **HTTP/HTTPS, file authentication**), which requires the domain owner to upload to the domain a file containing a unique identifier given to the certificate applicant by the Certificate Authority (CA).

The CA can then locate and interrogate this file as proof that the requestor has control of this domain.

What will change exactly?

The new policy will be implemented on the 15th of November and will affect SSLs and orders in the following ways:

- 1.** It will be **no longer possible** to validate **Wildcard certificates** using file-based validation (all types of Wildcards are affected)
- 2.** When using file validation for **multi-domain certificates**, domain validation will be required for every FQDN/SAN (domain) individually.

Example:

Prior to the 15th of November - if you ordered a certificate for:

openprovider.nl

www.openprovider.nl

test.openprovider.nl

You would only need to place a file on *openprovider.nl/some-folder*

After the 15th of November - if you order a certificate for the above domains you will need to place the file on:

www.openprovider.nl/some-folder

test.openprovider.nl/.well-known/some-folder

openprovider.nl/.well-known/some-folder

3. When using file validation for **single domain certificates**, domain validation will be required for every FQDN/SAN (domain) individually.

Example:

Prior to the 15th of November - if you ordered a certificate for *test.openprovider.nl*, file could be placed either on test.openprovider.nl or openprovider.nl

After 15th of November - if you want to protect test.openprovider.nl, the file must be placed for test.openprovider.nl

4. For DV certificates (single domain) you can also receive the "www" as an additional name for free,

e.g. If you order a certificate for openprovider.nl you can receive www.openprovider.nl for free, and vice-versa

If you order for test.openprovider.nl you can receive www.test.openprovider.nl for free and vice-versa.

That also means files must be placed for both domains: with and without www.

Important: For Openprovider API users:

When requesting a certificate using our API, if you wish to request a certificate for a domain with WWW and without WWW, you have to specify host names and domain validation methods for both variants.

Certificate renewal: When processing a renewal request, we will first check which variants were initially issued for the particular domain; with WWW and without WWW variant or with just one. If you received first certificate with both, then the renewed certificate will include WWW and non-WWW domain.

If you received the certificate with just one variant but need both, you can always reissue it in SSL Panel with the above checkbox selected.

What is the impact?

1. The change will not affect certificate issues prior to the 15th of November.
2. It will affect all **new orders, renewals, and reissues** after November 15, when using file validation as a DCV method.
3. Other domain control validation methods are not impacted by this change, so this change **does not apply to Email- and DNS-based validation, which still are available for wildcard certificates.**
4. If you now use file validation for **wildcard certificates**, you will have to switch to email validation or CNAME validation.
5. **Wildcard** certificates which were previously issued with **file validation can not be directly renewed via the ssl panel (using the previous details). Please start a new order and select one of the supported validation methods.**
6. If you use file validation for single and multi-domain certificates and want to continue using it, you will need to prepare a separate file for each subdomain (SAN), or switch to another DCV method.

Openprovider strongly suggests choosing other methods of domain validation than HTTP / HTTPS validation:-

- **E-mail validation**
- **DNS / CNAME validation**

Both will make validation process quicker to complete.

Revision #2

Created 2026-08-07 14:24:16 UTC by Sarath

Updated 2026-08-07 15:43:26 UTC by Sarath