Sectigo Domain Control Validation (DCV) Guide

Sectigo Domain Control Validation (DCV) Guide

---

1. Purpose

Domain Control Validation (DCV) is required by Sectigo and all publicly trusted Certificate Authorities (CAs) to verify that the requester has control over a domain before issuing SSL/TLS certificates.

2. Supported Validation Methods

Sectigo supports the following DCV methods:

- Email-Based Validation
- DNS CNAME Record Validation
- DNS TXT Record Validation
- HTTP/HTTPS File-Based Validation
- Automated DNS Validation via Sectigo DNS Connectors

Full reference: https://docs.sectigo.com/scm/scm-administrator/validating-domains.html

3. Email-Based Validation

Process:

- Sectigo sends a validation email to an administrative address.
- Recipient clicks a unique link and enters a provided code to validate.

Acceptable Email Addresses:

- admin@yourdomain.com
- administrator@yourdomain.com
- hostmaster@yourdomain.com
- postmaster@yourdomain.com
- webmaster@yourdomain.com
- Or a contact listed in _validation-contactemail.yourdomain.com

Sectigo Domain Control Validation (DCV) Guide

NOTE: WHOIS-based validation will be deprecated as of June 15, 2025, in accordance with Ballot SC-80v3.

4. DNS CNAME-Based Validation

Process:

1. Generate MD5 and SHA-256 hashes from the DER-encoded CSR.

2. Create the following CNAME record:

_<MD5 hash>.<domain> CNAME <SHA-256 hash>[.<uniqueValue>].sectigo.com.

Example:

_c7fbc2039e400c8ef74129ec7db1842c.example.com. CNAME c9c863405fe7675a3988b97664ea6baf.442019e4e52fa335f406f7c5f26cf14f.sectigo.com.

- SHA-256 should be split into two 32-character labels.

- Unique tokens can be included for one-time use.

5. DNS TXT-Based Validation

Process:

- Sectigo provides a `randomValue` token.

- You create a DNS TXT record:

_pki-validation.<domain>. TXT "<randomValue>"

- Token is valid for 30 days and may only be used once per certificate order.

6. HTTP/HTTPS File-Based Validation

Requirements:

- Web server must be accessible on HTTP (80) or HTTPS (443).

- Wildcard domains are NOT eligible for this method.

File Setup:

1. File name: <MD5 hash>.txt

2. Content:

<SHA-256 hash>

sectigo.com

[optional uniqueValue]

3. File path:

http[s]://<domain>/.well-known/pki-validation/<MD5>.txt

Notes:

- No BOM
- ASCII text only
- CRLF or LF line endings acceptable

7. Automated DNS Validation (Sectigo DNS Connectors)

- Sectigo SCM integrates with DNS providers (Cloudflare, Route 53, Azure DNS).
- DNS CNAME records are created and validated automatically.
- Setup: SCM Configuration DNS Connectors

Reference: https://docs.sectigo.com/scm/scm-administrator/understanding-dns-connectors.html

8. Request Tokens & Uniqueness

A Request Token includes:

1. SHA-256 hash (from DER-encoded CSR)
2. The string 'sectigo.com'
3. (Optional) uniqueValue (max 20 alphanumeric characters)

Note: Tokens must be unique. Reusing a CSR may fail unless a unique value or attribute is included.

9. Multi-Domain Certificate (MDC) Validation

- Each FQDN must be validated.
- Different DCV methods can be used per domain.

- Revalidation is required if a new key is used.

API Notes:

- Use dcvEmailAddresses[], HTTPCSRHASH, HTTPSCSRHASH, or CNAMECSRHASH.
- Use CollectSSL with showMDCDomainDetails=Y to track DCV status.

10. Managing and Revalidating Domains

- Use SCM Domains Page to validate, revalidate, or clear domains.
- Use ResendDCVEmail API for email-based DCV.

Reference: https://docs.sectigo.com/scm/scm-administrator/understanding-domains.html

11. Subdomain Validation (WWW Domains)

- Control of www.domain.com no longer implies control of domain.com.
- Each subdomain must be validated individually.

12. DCV Reporting

- Available in SCM Reports Domain Control Validation (DCV).
- View domain, method, status, and expiration.

Reference: https://docs.sectigo.com/scm-pro/scm-pro/understanding-reports.html

13. Best Practices

Action | Benefit

---|---

Use unique CSRs | Prevents token reuse

Enable CAA Records | Restricts issuance to trusted CAs

Automate via DNS Connectors | Enables faster validation

Validate early | Avoids delays

Sectigo Domain Control Validation (DCV) Guide

For comprehensive DCV process and integration, visit: https://docs.sectigo.com