Is your organization ready for high-frequency Domain Control Validation (DCV)?

The certificate lifecycle is accelerating. DCV timelines are tightening fast, and manual processes won't keep up. Organizations that fail to adapt will face a growing risk of outages, failed renewals, and non-compliance.

The shrinking timeline:
What you need to know

The CA/Browser Forum has committed to the following changes for certificate lifespans and the reuse period for domain validation:

Milestone	Today	By 2026	By 2027	By 2029
Certificate Lifespan	398 days	200 days	100 days	47 days
Max DCV Reuse Period	398 days	200 days	100 days	10 days

Bottom line: By 2029, organizations must revalidate their domains every 10 days. Without automation, this will create unmanageable operational overhead.

Assess your DCV automation readiness

Use this quick checklist to evaluate if you're ready:

- [ ] Can you track when each domain's validation expires?
- [ ] Are DCV workflows automated across DNS providers?
- [ ] Can you renew certificates every 47 days, or even 10, without manual steps?
- [ ] Do you have centralized visibility into domain and certificate status?
- [ ] Can you ensure consistent compliance across hybrid and multi-cloud environments?

If you answered "no" to any of these, it's time to revisit your automation strategy.

SECTIGO®

Next steps:
What you can do now

1. Review your domain validation and renewal process.
2. Identify any manual dependencies or compliance gaps.

Not sure where to begin?

You can reach out to Sectigo's industry experts for a readiness review.

Get in Touch

Key Certificate Lifecycle Management (CLM) capabilities to look for

To effectively manage upcoming DCV changes, consider CLM solutions that offer:

- ✔ Built-in DCV automation with DNS integration.
- ✔ Broad automation support for renewals and revalidation across environments, from DevOps pipelines to enterprise IT.
- ✔ Real-time visibility into validation and certificate status.
- ✔ Centralized management for both public and private PKI.

We're here to help

Sectigo Certificate Manager (SCM) includes built-in support for automated Domain Control Validation (DCV) as part of its broader CLM capabilities. By using DNS connectors, SCM integrates with supported DNS providers to automatically create and validate CNAME record challenges. This reduces reliance on manual processes and helps ensure ongoing domain validation continuity.

SCM continues to grow its list of supported DNS providers, now including:

Cloudflare | Amazon Route 53 | Azure DNS | GoDaddy DNS

Akamai Edge DNS | DNSimple | OVHcloud

View the full, up-to-date list of SCM supported DNS providers here.

SECTIGO®