



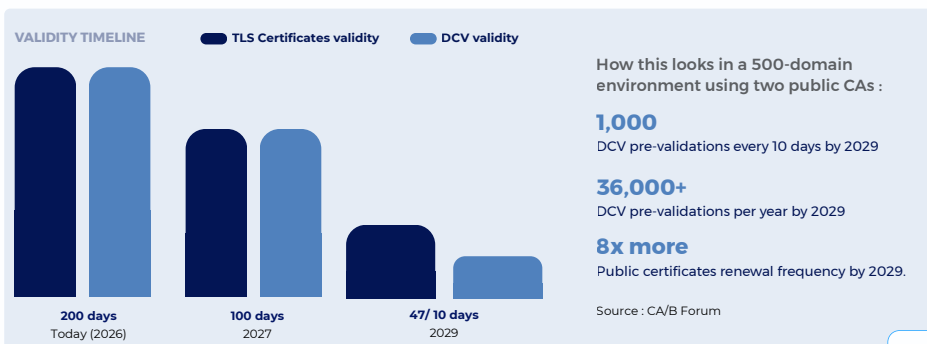
Automate public certificate renewals and DCV across multi-public CA environments

Evertrust DCV Automation centralizes domain validation and public certificate operations across CAs and DNS providers, so teams can scale without CA silos or manual DNS workflows.

The missing step in public certificate management

Public certificate automation extends beyond issuance and renewal. Evertrust's DCV Automation module helps organizations automate DCV centrally across all public CAs and DNS environments, so certificate operations stay fast, governed, and scalable.

Why this matters now



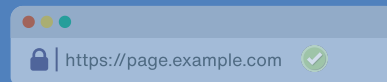
As public certificate validity drops to 47 days by 2029 and DCV pre-validation drops to 10 days, certificates teams are now responsible for revalidating domain control more often across every product that depends on DCV. That includes website certificates, regulated website authentication certificates, sector-specific public trust products, and secure email products. CLM without DCV automation leaves the most fragile part of the workflow untouched.



What is Domain Control Validation?

DCV is the process a public CA uses to verify that the requester controls the domain for which a certificate is being issued.

DCV is required for public certificates including DV, OV, and EV. Once a domain is pre-validated, certificates can be issued without repeating proof of control until the validation window expires.



Products impacted by this change

- Public OV & EV TLS
- X9 PKI for TLS
- PKIoverhead Private Services Server
- Secure email
- EU QWAC
- EU QWAC PSD2

What Evertrust DCV Automation delivers

Cross-public-CA certificate and DCV operations

Centralize DCV orchestration and lifecycle operations across public CAs from one control plane and avoid CA silos.

DNS challenge provisioning across heterogeneous environments

Automate DNS-based validation workflows across provisioners and webhook-based coverage for DNS platforms with APIs.

Faster validation cadence for shorter lifetimes

Support high-frequency validation operations as DCV windows shrink, with package concepts ranging from hourly checks to 5-minute intervals for advanced DCV automation use cases.

Supported public Certificate Authorities (CAs)



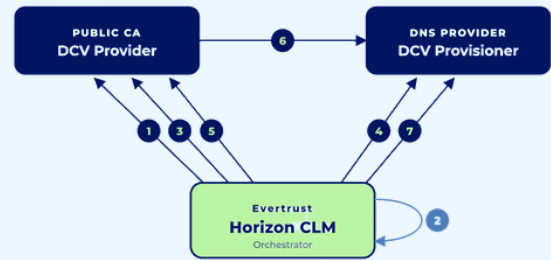
Supported DNS provisioners



How it works

Evertrust centralizes every step of DCV automation, request, provision, validate, and clean up, to make public certificate operations scalable.

- 1) List registered domains
- 2) Filter domains where DCV is needed
- 3) Request DCV challenge for specific domain
- 4) Provision DCV challenge
- 5) Request DCV validation
- 6) Validate DCV challenge
- 7) Cleanup DCV challenge



LICENSING MODEL

Capability	Included in Evertrust CLM license	Advanced DCV module
DOMAIN CONTROL VALIDATION (DCV) AUTOMATION		
Start DCV automation Identify domains where validation is required	✓	✓
Public CA coverage Automate DCV challenge retrieval and validation across supported public CAs.	Single CA	Multi-CA
DNS challenge provisioning Automatically create the required DNS proof records.	1 provisioner of customer's choice	All supported provisioners
Validation frequency Run DCV checks on a scheduled cadence to keep validation coverage current as lifetimes shrink.	Standard	High-frequency
Domain scale Scale DCV automation from a single top domain to large enterprise domain portfolios.	Up to 1 top domain	Tier-based domain model
Multi-CA governance Manage DCV policies centrally across multiple public CAs from one control plane.	-	✓
Audit & alerting Track DCV activity with audit trails, eventing, and alerts for validation status and failures.	-	✓
New integrations Expand coverage as new CA and DNS provisioner integrations are released.	-	Included as released

ADVANCED DOMAIN MODULE PACKAGES

Starter	1-20 top domains
Scale	Up to 100 top domains
Enterprise	Up to 300 top domains
Enterprise+	Unlimited top domains

A "top domain" refers to a primary domain namespace such as example.com or example.fr. Subdomains like dev.example.com or api.example.com are associated with that same top domain.

* Domain count is assessed based on the public certificate scope to be managed. Final licensing scope is confirmed during the commercial qualification process.

ABOUT

Evertrust helps organizations automate, govern, and scale digital certificate operations across complex hybrid environments through certificate lifecycle management and public key infrastructure solutions.