Domain Validated Enrollment Tips

Guide to Successful Certificate Enrollment

At DigiCert, we're committed to protecting the world's information and creating processes and procedures to ensure trustworthiness on the web. This guide will help you understand our authentication and verification practices, and navigate the enrollment process for Domain Validated (DV) certificates.

A Domain Validated certificate is considered an entry-level SSL certificate and can be issued quickly. DV certificates provide encryption with domain-only authentication—meaning the only verification check is to ensure the applicant owns the domain where they plan to use the certificate.

Certificate processing time can vary depending on:

- The accuracy of the information provided by the customer in the Certificate Signing Request (CSR) and during enrollment.
- The customer's responsiveness to DigiCert's request for information. If you'd like to decrease the processing time, make sure you have control over a domain and complete your Domain Control Validation (DCV) as soon as possible.

Domain Validation Steps

1. Domain Approval

DigiCert approves domains through a process called Domain Control Validation (DCV).
In this procedure, DigiCert sends an authorization email with authentication instructions to the registered owners of the domain(s) listed publicly on a WHOIS record.

We can send the email to five addresses associated with the domain (e.g., the admin@, administrator@, webmaster@, hostmaster@, and postmaster@.) We don't send the authorization email to the certificate requestor or account administrator.

DigiCert also offers an option to create a website via a practical demonstration, or the customer can edit their DNS TXT records to include a DigiCert provided code.

2. Security Check

All Domain Validated certificates go through security checks. In some cases, like for major corporations, well-known trademarks, and financial institutions, an order may be flagged. If flagged, the order must be manually reviewed by the Authentication team to ensure authenticity.

3. Payment

A credit card is the only form of payment accepted for DV certificates. If payment fails, the customer receives an automated message requesting they update their credit card details. Occasionally, customers may need to contact their financial institution to approve the charge. If this is the case, the customer needs to contact DigiCert following the update to retry the payment.

Avoid These Common Mistakes

- Failing to select an approver email during enrollment.
- Untimely approval of certificate request from approver email.
- Issues with credit card used to make the purchase.

Things to Know Before Enrollment

CSR Fields

Every SSL/TLS certificate requires a Certificate Signing Request (CSR) to finalize the certificate issuance. CSR details must reflect the enrolling organization's business information—the organization whose website will be secured with the certificate.

Fields in the CSR include:

Organization: Your full company name or personal name as legally registered in your locality.

Common Name*: The fully qualified domain name (FQDN) and hostname of the organization's website being secured with the certificate (e.g., www.knowledge.digicert.com).

Country: The two-digit code for your country (e.g., US for United States). For countries outside the United States, see the list of SSL Certificate Country Codes.

State: The state/province/territory where the organization is registered to do business. It must be fully spelled out (e.g., California vs. CA).

Locality: The city where the organization is registered to do business. It must be fully spelled out (e.g., Mountain View vs. Mtn View).

Organizational Unit: An optional field that is generally whichever unit of your company that is ordering the certificate, such as accounting, marketing, etc.

* The Common Name field is the only field that appears on the certificate.

Contacts

There are many contacts associated with an order. All contacts listed should be made aware of the order and be able to respond to inquiries in a timely manner.

Organizational Contact: An employee of the enrolling organization; it doesn't have to be the approver of the order.

Technical Contact: The individual who enrolls for, receives, and installs the SSL/TLS certificate.

Billing Contact: The individual who handles billing- and payment-related matters for the certificate order.

Average Processing Times

Domain Validated certificates are usually issued within minutes after the organization approves the enrollment. However, this time may increase if an order is flagged for a security review. On average, it takes DigiCert one business day to process each email, document submission, or fax received from a customer. The Authentication team must validate the information using non-biased, third-party sources.

If you need help with or have questions about the authentication process, please email us at: auth_support@digicert.com.