DATASHEET

Organization Validated Enrollment Tips

A Guide for 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 Organization Validated (OV) certificates.

All Organization Validated certificates are fully authenticated. Taking slightly longer to issue than Domain Validated certificates, these certificates are only granted once the organization passes validation procedures and checks to confirm the existence of the business, the ownership of the domain, and the user's authority to apply for 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. Also, be aware that we will call a verified phone number to complete organization authentication. This call usually takes place within 24 hours of the certificate request.

Organization Validation Steps

1. Organization Authentication

DigiCert must verify the name, registration, and good-standing status of the organization listed in the Certificate Signing Request (CSR) with the appropriate Government Registration Agency in its country, state, or city of jurisdiction.

The organizational identifiers (i.e., Inc, Corp, LLC, Ltd, Pty Ltd, etc.) are required in the CSR, and cannot be added if they don't appear on the official business registration documents. Misspellings, unregistered acronyms, or abbreviations aren't allowed. CSR location details (country, state, and locality) must match the official jurisdiction of the business.

If unable to validate the organization, DigiCert may request a government-filed business registration document under the organization name (note: this may delay processing).

Submitting these documents will help us validate your organization, and we'll contact the registering authority (RA) to confirm the details before we proceed. If the document you provide doesn't list the current address for your organization, you must also provide a recent utility bill or bank statement addressed to your company at the current address.

Alternatively, you can create an online presence for your organization (including the legal name, address, and phone number) by listing your organization with a third-party business directory, such as Google My Business (https://www.google.com/business/) or Dun & Bradstreet (http://www.dnb.com/solutions/government/duns-number-request-guide.html).

2. Domain Authentication

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.

3. Telephone Verification

Before a certificate can be issued, a verification telephone call—using a public telephone number obtained from an independent third-party—must be completed with an authorized organizational contact. Alternative documentation may be requested if a third-party public telephone listing that meets our requirements isn't available. If DigiCert is unable to reach the authorized organizational contact directly, a voicemail may be left on the contact's personal voicemail with a security code to return our call.

4. Payment

Payment must be cleared before certificate issuance. A credit card is strongly recommended for payment as it is the most quickly processed form of payment.

Avoid These Common Mistakes

- Enrolling with an incorrect or abbreviated organization name in the CSR organization name field. The organization name in the CSR must exactly match official records.
- Designating an organizational contact who is unavailable to provide a requested item.
- Not using a credit card payment may delay issuance. Other forms of payment, like purchase orders (POs), must meet minimum requirements for acceptance. Additionally, wire transfer and checks require bank-cleared funds before an order can be issued.

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. (e.g., https://www.digicert.com/ssl-certificate-country-codes.htm)

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.

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 or contractor representing 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

Organization Validation certificates are usually issued within two hours if no additional documentation is required. However, this time may increase depending on the availability of the organization's public information. 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.