Extended Validation 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 Extended Validation (EV) certificates.

Extended Validation SSL certificates offer the highest level of online trust available and use the industry standard for EV authentication. When users visit a website secured with an EV SSL certificate, there are several distinguishable indicators:

- The address bar appears green (in high security browsers)
- A special field shows the name of the legitimate website owner along with the name of the security provider that issued the EV SSL certificate
- The name of the certificate holder and issuing CA are shown in the address bar

These visual cues offer reassurance and help increase consumer confidence in e-commerce.

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.

Extended Validation Steps

1. Acknowledgement Agreement

After enrollment, the organizational contact in the certificate enrollment must accept the Extended Validation Subscriber Agreement (aka "Acknowledgement Agreement"). This authorization document is required for certificate issuance. Online versions are available for all DigiCert brands. A new Acknowledgement Agreement isn't required for each enrollment if the organization name and organizational contact remain the same.

2. Organization Authentication

DigiCert must verify the name, registration, and good-standing status of the organization listed in the 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.

Alternatively, you can create an online presence for your organization (including 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).

3. Operational Existence

DigiCert must verify that the enrolling organization can engage in business. This process is known as Verification of Operational Existence. Operational Existence is satisfied if the organization has been registered and confirmed by the resource used during organization authentication. Alternative documentation may be requested if the above requirements aren't met.

4. Address Verification

DigiCert verifies the physical business address listed on a certificate enrollment. This must be a physical address and not a virtual office, P.O. Box, lock box, or "care of" address. If the address cannot be verified, the organizational contact may be asked to provide an alternate, verifiable address for the organization.

5. 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. If a third-party public telephone listing meeting our requirements isn't available, the customer may be asked to create a business listing through a qualified source, or to provide a legal letter signed by a CPA or attorney.

6. 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.

7. Confirmation of Organizational Contact Employment and Authority

The organizational contact must be verified to work for the organization requesting the certificate and be authorized to obtain an EV certificate on the behalf of the organization. Alternative documentation may be requested if the above requirements aren't met. Contractors are also allowed to fill this role so long as the applicant confirms they have given them permission to.

8. Verification Call

Before each certificate can be issued, a verification telephone call, using an independently obtained third-party public telephone number, must be completed with an authorized organizational contact. Alternative documentation may be requested if a third-party public telephone listing meeting our requirements isn't available.

Avoid These Common Mistakes

- Leaving out the correct organizational identifiers (i.e., Inc, Corp, LLC, Ltd, Pty Ltd, etc.) in the certificate organization name
- Abbreviating any part of the organization name
- Using a Post Office Box instead of physical location
- Designating an organizational contact who is unavailable to provide requested items
- Designating an organizational contact who does not have deemed authority
- Not including a Fully Qualified Domain Name (FQDN) in the certificate Common Name field (EV certificates cannot be issued to "intranet" sites or IP addresses)

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.

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

Extended Validation certificates are usually issued within two business days 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.