# The Partner Guide to Certificate Validation & Management

digicert®

## Table of Contents

## Introduction

DigiCert is one of the fastest-growing security solutions companies in the world. We simplify PKI and SSL/TLS, and provide identity, authentication, and encryption solutions for the web and the Internet of Things (IoT).

As today's threat landscape evolves, we're relentless in driving new technology to protect the world's information. Validation is an important part of this vision. As such, DigiCert has driven and adopted the Certificate Authority and Browser Forum (CA/B Forum) Baseline Requirements to strengthen the security of SSL operations and validation processes.

We undergo a yearly audit to ensure our validation practices abide by published standards for DV, OV, and EV SSL certificate orders. Our trusted reputation comes from years of operating secure infrastructure for the Internet, which has allowed us to validate nearly one million organizations to date.

DigiCert puts its customers first and takes pride in having the industry's highest-rated customer support. We know we will only be successful if our customers are happy and continue to choose us.

As a valued partner, your thorough understanding of our validation practices is essential to giving customers a positive experience. We created this guide to help you navigate the validation process.

DigiCert utilizes a multi-step validation process prior to issuing a certificate. This process involves certain automatic and manual steps that are taken by DigiCert's internal systems and validation staff to ensure the following:

Depending on the certificate type being ordered, DigiCert may verify that:

- The organization and organizational contact personnel are not listed on any of the government-denied entity lists or are subject to embargoes, sanctions or other restrictions.
- The organization has government-issued credentials such as articles of incorporation or a business license that allow it to conduct business.
- The organization is entitled to request a certificate for the domain for which the certificate is issued OR has obtained legal right to obtain that certificate for that domain name from the owner of the domain.
- The organization's contact personnel can be verified via a third-party phone number as an employee of the organization that is ordering the certificate.
- The organization is operating at a verified physical address.
- Any order information that has been flagged as being inconsistent with the order is carefully reviewed.

This comprehensive guide will provide detailed information for everything from enrolment to issuance, in a handy, easy-to-read manner.

## Certificate Types

DigiCert SSL/TLS Certificates are designed to meet whatever needs the customer may have. Regardless of server type or the number of servers or domains they need secured, one of the following SSL certificates will fit the customer's needs:

1. **Domain-Validated (DV) SSL** certificates provide encryption with domain-only validation, and verify that the requestor is affiliated with use of the domain.
2. **Organization-Validated (OV)** SSL Certificates provide full business validation and verification of business identity and domain control.
3. **Extended Validation (EV)** SSL certificates utilize a more stringent level of validation and provide the industry's highest level of assurance available today.
4. **Code Signing IDs** provide full business validation. The ID generates a digital signature that provides validation of the code / source and assurance of code integrity. These certificates are used to sign software, and are not webserver certificates like the previous three types.

---

The level of validation varies by certificate category and product type. Some of the products can be issued to individuals. Contact your account manager to find the best certificate to meets your needs.

---

## General Security Checks

When an organization submits an application for a certificate, DigiCert performs several security checks, including searching government databases to ensure the organization is officially registered and in good standing. DigiCert also searches several third-party databases to ensure the organization is not involved in fraudulent activity, such as phishing or social engineering. DigiCert ensures that the products issued are checked against **government**, **phishing**, **domain fraud** and **contact** blacklists. Additionally, code signing certificates are checked against a malware blacklist.

DigiCert ensures that it does not sell products to customers from embargoed countries, which the U.S. Government forbids U.S. companies—and their non-U.S. locations—from doing. Embargoed countries/regions may change at any time, but currently include:

- Cuba
- Iran
- Syria
- Sudan
- North Korea
- Crimea

## Organization Validation

In products that require organization validation (like OV, EV and Code Signing), DigiCert will attempt to confirm the **registration** of the organisation with the appropriate authority that oversees the legal registration of organizations.

The enrolling organization is validated by the querying of registration records for the organization name listed in the application with a government registration authority. It is also validated by requesting official company documentation, such as business license, Articles of Incorporation, Sales & Use License, or other relevant documents.

The Organization requesting a certificate must be an active entity, confirmed by the government authority responsible for registering businesses within the specific jurisdiction (locality, state, country) referenced in the certificate request.

An exact match between the enrolled organization name and name in the certificate is **required**. DigiCert cannot accept any misspellings, unregistered acronyms, or abbreviations in the Organization name.

---

Note: Certificates require an **exact** match between the enrolled Organization and confirmed name, including corporate identifiers (e.g., Inc., Corp, LLC, Ltd, Pty Ltd, etc.).

---

DigiCert has access to an extensive number of global Qualified Government Independent Sources (QGIS). In most cases, DigiCert can find a Registration Record document on file in one of the many government or private databases that DigiCert has access to.

Examples of QGIS include:

- California Secretary of State (for corporations filed in the State of California, U.S.)
- City of Chicago, IL (Chicago business licenses)
- National Credit Union Administration (United States federal credit unions)
- UK Companies House
- Kamer van Koophandel (KVK) (companies registered in The Netherlands)
- New Zealand Companies Office
- State Administration for Industry & Commerce of the People's Republic of China

---

Note: For OV certificates, Qualified Independent Information Sources (QIIS) (like Dun & Bradstreet) may be considered for use in the absence of listing in a suitable QGIS; however, the government source is always considered the most up-to-date in case of variance among sources.

---

When a resource is not available or DigiCert cannot validate the organization within the available resources, DigiCert may request a current, **Government Issued Business Document**, often called a "Registration Records Document". Registration Record is a document that gives a company or organization the right to do business. If a Registration Record document is required for your customer's organization, DigiCert will contact the organizational contact on the enrolment and request a copy of an acceptable Registration Record document.

Examples of acceptable documents include:

- Business License/Certificate
- Certificate of Incorporation
- Business Registration Certificate
- Certificate of Existence with Status in Good Standing
- Certificate/Articles of Organization
- Public Records Filing for a New Business Entity
- Certificate of Formation
- Certificate of Assumed Business Name
- Trade Name Renewal Form
- Trade Name Registration Form
- Doing Business As registration document
- Fictitious Business Name Statement
- Statement of Partnership Agreement
- General Excise Tax License
- Zoning Permit
- Transaction Privilege Tax License
- Sellers Permit
- Sales & Use Tax Permit
- Restatement and Revision of Partnership Agreement
- Privilege License
- Organization Action in Writing of Incorporation
- Occupational Tax Certificate/License
- Notary Public Identification Card
- Merchant's Certificate of Registration
- Filing receipt
- Filing endorsement

- Employer Identification Number Application
- Declaration of Proprietorship or Partnership Registration
- Corporation Estimated Tax Form
- Corporation Annual Report
- Corporate Charter
- Certificate/Articles of Amendment
- Certificate of Withholding Identification Number
- Certificate of Payment of Business Tax
- Certificate of Ownership for Unincorporated Business or Profession
- Certificate of Exempt Status
- Certificate of Change of Resident Agent and/or Location of Registered Office
- Certificate of Authority
- Certificate of Acceptance of Appointment by Resident Agent

Once an **acceptable** Registration Record document is received from the customer, DigiCert must then **validate** it by contacting the issuing authority. If DigiCert can't confirm the validity of the document with the issuing authority, DigiCert **may** use selected third parties to verify the organization's existence.

---

Note: Any time documentation is required for an order, it may delay the issuing time of that certificate. Certificates cannot be issued until the provided documentation is in order and has been verified with the issuing agency. For this reason, timely submission of documentation is essential.

---

As indicated above, the items that are being verified with the "government authority" resources are:

1. The organization name in the enrolment (must be an exact match to the business registration).
2. The jurisdiction (territory of registration).
3. The organization status (must state "active" or equivalent, any inactive/revoked or equivalent organizations cannot obtain an SSL certificate and must update their status).

---

Note: Validation of the Organisation Name must be completed in the jurisdiction of the organization's incorporation.

---

Completing the validation in the jurisdiction of incorporation means for instance, that an organization registered in California where the Registration Record document shows it is a foreign corporation registered in Delaware, DigiCert must confirm the organization's status is active in Delaware's records.

## TRADE NAMES

In OV certificates, the organization can enroll with a trade name, if the trade name is duly registered and DigiCert is able to validate it in connection to the certificate request.

---

Please note that despite trade names being accepted in the Organization Name field within the certificate, the trade mark (even registered) is **not** acceptable.

---

In **EV** certificates, if the customer wants to use the trade name, then the name **must** appear in conjunction with the verified organization name (incorporated name).

**Example:** Alphabet Soup (ABC Inc.)

**Trade Name:** Alphabet Soup

**Organization Name:** ABC Inc.

## ULTIMATE VALIDATION. EXTERNAL REPORTS.

Please note, if DigiCert cannot validate information on the order, other potential mechanisms are in place for confirmation. DigiCert **may** be able to order external reports or obtain a Legal Opinion Letter or Attestation Letter (also known as a "lawyer letter") confirming the Registration Record documents.

In this case, the process can take longer and there is no guarantee that the Registration Record document can eventually be confirmed. Therefore, it is highly advised that enrolling organizations are properly registered and status remains active with their respective local government authorities.

## FOREIGN ORGANIZATION NAMES

For organizations registered in Latin or non-Latin characters, DigiCert will check and update the name of the organization with a translation. DigiCert will rely both on language specialists and third party options to provide the translated name.

To include a Latin character name in the EV certificate that is not a direct Romanization of the registered name, (e.g. an English Name) the CA MUST verify that the Latin character name is in one of the following third-party sources:

- Qualified Government Independent Sources (QGIS)
- Qualified Independent Information Sources (QIIS) in examples like Duns & Bradstreet or Hoovers
- Legal Opinion Letter

### TRANSLITERATIONS (ROMANIZATIONS)

For organizations registered in non-Latin characters, if required, DigiCert will check and eventually update the name of the organization with transliterations (change letter by letter) using:

- A system officially recognized by the government in the applicant's jurisdiction of incorporation
- A system recognized by the International Organization for Standardization (ISO)
- A system recognized by the United Nations
- Legal Opinion Letter

## Validation for Certificates with Only Personal Birth Given Name

For certificates where only the **personal birth given name** is used, documentation such as a copy of a passport, driver's license, or other additional relevant document is required.

---

Note: These certificates are Individual Validated (IV) certificates and Organization Validation (OV) certificates for business entities registered under personal birth given name (generally sole proprietorships).

---

The documents provide critical information for a DigiCert certificate and may be submitted as supporting documentation to confirm the validation criteria of the individual enrolling for the certificate. The copy of the **ID document** submitted must be reviewed for legitimacy and absence of fraud or forgery:

- Passport
- Driver's license
- Government Issued Identification Document

An exact match between the enrolled Individual name and name in ID document name is **required**. DigiCert cannot accept any misspellings or abbreviations in the name.

The following documents are NOT acceptable as sources of verification for Individual Applicants:

- Educational Institution Identification Card
- Employment Identification Card
- Business Card
- Club or Fraternity Membership Card
- Library Card
- Firearms Owner Identification Card
- Commercially Produced Identification Card

## VALIDATION FOR INDIVIDUAL VALIDATED (IV) CERTIFICATES

Applicants **without** valid QGIS/QIIS Business Entity registration under their birth given name **are** considered **Individual Applicants**.

Symantec, Thawte, & GeoTrust branded certificates are not available for individual applicants at this time. **However, DigiCert offers IV Certificates under an Individual's personal birth given name** upon supply of validation documentation, such as a copy of a passport, copy of a driver's license, or other relevant document.

## BUSINESS ENTITIES APPLICANTS: ORGANIZATION VALIDATED (OV)

For sole proprietorship certificate applications, DigiCert is **required to check the registration** of the organization in a valid QGIS or QIIS Business Registration respective to the registration requirements (or lack thereof) in the applicants jurisdiction.

If the sole proprietor also has a registered **trade name**, the certificate organization name may be in any of the following formats: Legal Name only, Trade Name only (for OV), or Both Assumed Name & Legal Name in the specific format "Trade Name (Legal Name)".

**Trade Name:** Alphabet Soup
**Legal Name:** Bob Garcia

**Example 1:** Bob Garcia
**Example 2:** Alphabet Soup
**Example 3:** Alphabet Soup (Bob Garcia)

---

Note: Example 2 is not permitted for EV certificates.

---

## Domain Validation

Before DigiCert can issue a certificate, domain names listed in the certificate application must be validated to ensure that the specified domain name has been approved by the registered owner of the domain name.

Domains are validated by gathering information about the domain name's ownership records, which are available publicly online or approved global domain name registrars. **WHOIS** is a public protocol for getting information about who owns a domain name. A WHOIS record for a domain name typically shows the registrant (owner) company and address, and the name and contact details for an administrative and technical contact.

Information from WHOIS may be supplemented through the administrative contact associated with the domain name registrar listed on record or by querying the top-level domain extension **registrar** who governs the administration of the top-level domain name extension.

---

Note: "Internal," or intranet, domains (not containing a fully-qualified domain name, i.e. "localhost" or "test.corp") are no longer allowed per industry guidelines (CA Browser Forum).

---

Please note that validation may be supplemented by the review of the **content on the web site** listed in the request to ensure that the content published on the stated web site does not infringe in any of the sections prohibited under the official DigiCert subscriber agreement, which must be accepted before the submission of an application for a certificate.

### CONFIRMATION OF DOMAIN CONTROL VALIDATION (DCV) - EMAIL APPROVAL

The **preferred method** for domain approval on a certificate is sending an **email** message to the contacts listed on the WHOIS domain registration record or using generic email addresses, which are typically only available to persons controlling the domain name administration.

Acceptable e-mail addresses for Domain Control Verification (DCV):

- Email address listed in the WHOIS domain registration record for the domain specified in the certificate request.
- One of the following generic email aliases at the domain specified in the certificate:

  admin@
  administrator@
  webmaster@
  hostmaster@
  postmaster@

Once the DCV is received, the recipient must click on the link provided to approve or reject the request. This process confirms the certificate request is affiliated with the domain owner. Note: DigiCert can also call the **phone number** listed on the WHOIS record and get verbal authorization.

## CONFIRMATION OF DOMAIN CONTROL VALIDATION - PRACTICAL DEMONSTRATION

Practical Demonstration/File Auth is a method of domain approval that confirms the customer's control over the domain by having a random value, which is provided by DigiCert, present on the webpage: [domain name]/.well-known/pki-validation/fileauth.txt

Once this code is updated, DigiCert can check it and if present, consider the validation for the domain completed.

## CONFIRMATION OF DOMAIN CONTROL VALIDATION - DNS RECORD VIA TXT OR CNAME

Domain Name System (DNS) is another method of domain approval that is like Practical Demonstration/File Auth in the sense that confirmation of the domain is approved by having a random value provided by DigiCert updated on the **DNS** record. The preference to update the TXT or CNAME record is up to the customer. However, some registrars will have restrictions on what is allowable for CNAME, in which case the only option would be TXT.

Once this code is updated, DigiCert can check it and if present, consider the validation for the domain completed.

## CONFIRMATION OF DOMAIN CONTROL VALIDATION – CNAME TARGET

When the requested domain is owned by another organization, a CNAME procedure, called the **CNAME Target**, allows DigiCert to approve a domain request for the enrolling organization. Please note the following differences:

- For DNS CNAME to work, the domain owner must list their DNS CNAME record to list the random token provided by DigiCert.
- For CNAME Target to work, the domain owner of the pending domain would have to list the CNAME record with a domain name that DigiCert has already approved for another organization. The way this works is that the domain owner and the "other organization" are working together, so CNAME target is a way for DigiCert to confirm the two are working together.

---

Note: CNAME Target will only work if all parties involved (DigiCert, partners, certificate requestor, and domain owner) agree and have completed the necessary steps.

---

## CONFIRMATION OF DOMAIN CONTROL VALIDATION - EMAIL APPROVAL FOR PARTNERS

Note: DigiCert has introduced the "selection" of the DCV recipients at the time of the enrolment. The Partner Portal also includes a "resend" feature, which allows DCVs to be re-sent to same email or to other alternatives (always one of the WHOIS email or one of the 5 aliases).

Partners do not need to contact DigiCert to send or resend the Domain Control Validation email. However, it is important to note that every time a new email is sent, the links in all previous emails are invalidated and will no longer work.

## Organizational Unit

As part of the CA/B Forum Baseline Requirements for SSL Certificates, the Organizational Unit entered in the Certificate Signing Request (CSR) during the enrolment must be validated.

The Organizational Unit field must **NOT** contain any of the following:

- **Unverified** legal names (e.g., "Corp", "Ltd.", etc.)
- **Unverified** trading names (e.g., "Trading as")
- **Unverified** trademarks (e.g., "(tm)")
- **Unverified** persons names (e.g., "Marc Smith")
- Domain names & IP addresses

The Organizational Unit field may contain:

- Department names
- Server names (if it is not a domain name)
- General words and phrases

You may leave the Organizational Unit field blank, or enter information from the allowable items listed above.

Any information entered in the Organizational Unit field must be verified. If DigiCert is unable to verify the information and it falls under the "not allowed" section, DigiCert's validation representatives must update/remove it from the CSR before the certificate can be issued.

## Confirmation of Operational Existence (EV ONLY)

Certification Authority and Browser Forum Extended Validation guidelines stipulate organizations requesting Extended Validation must have their Operational Existence confirmed.

The Operational Existence requirement is satisfied if the enrolling organization has been registered and in existence for more than three years, as confirmed by the Qualified Government Independent Sources (QGIS) resource used during organization authentication.

---

Note: When enrolling for an EV certificate, please ensure with your customer that the organization has been registered for more than three years; or, if not, advise that additional evidence might be required.

---

If the organization is registered for **less than three years**, DigiCert can confirm Operational Existence by using:

- Qualified Independent Information Sources (QIIS) in examples like Duns & Bradstreet or Hoovers
- Qualified Tax Information Sources (QTIS)
- Bank confirmation letter confirming a demand deposit account (this document/information must be verbally confirmed directly with the financial institution, via a third party phone number before DigiCert can accept it).
- Legal Opinion Letter or Attestation Letter confirms demand deposit account

## Address Validation

In the products that require organization validation (like OV, EV and Code Signing), DigiCert will validate the address listed on a certificate enrolment. Verified information and requirements vary by product type; however, all discrepancies must be corrected prior to certificate issuance.

All organization addresses for applicants must be **validated** via:

- Qualified Government Independent Sources (QGIS), such as the ones used to complete the validation of the organisation
- Qualified Independent Information Sources (QIIS), such as Yellow pages or White pages
- Qualified Independent Information Sources (QIIS), such as Google, Dun & Bradstreet, Hoovers, Bloomberg, Manta, or other address verification sites
- A Legal Opinion Letter or Attestation Letter

### ORGANIZATION VALIDATION ADDITIONAL SOURCES

For **OV orders only**, the following **documents** may be submitted as supporting documentation to confirm the validation criteria for the address of the organisation enrolling for the certificate:

- Bank statement
- Bank letter
- Credit card statement
- Utility bill (including cable, phone, or Internet bill)
- Rental agreement
- Tax receipt
- Business license
- Another government-issued document

### EXTENDED VALIDATION REQUIREMENT: PHYSICAL ADDRESS CONSIDERATIONS

The address in the enrolment must be a physical address and not a Post Office (P.O.) Box address, and must be a verified business address for the enrolling organization or its verified parent, subsidiary, or affiliate. Please note that:

- Parent/subsidiary/affiliate must be within the same country as country of jurisdiction
- Subsidiaries are required to be majority owned

---

Note: In certificates where the Organization is registered outside its jurisdiction of incorporation a Legal Opinion Letter is required.

---

If the address does not match, the organizational contact may be asked to provide an alternate, verifiable address for the organization. The order must be updated to reflect the verified address.

## Validation of Verified Phone number

In the products that require organization validation (like OV, EV and Code Signing), DigiCert must be able to contact the customer's organization, and confirm that the certificate has been ordered by that customer. To begin this process, our Validation team will try to obtain an independently verified (validated through a third party) phone number for the organization.

The phone number must be listed under the organization name (or verified registered trade name, parent/subsidiary/affiliate) in the country on the certificate request. The phone number must be obtained through a DigiCert approved third party resource, such as:

- Qualified Government Independent Sources (QGIS), such as the ones used to complete the validation of the organisation
- Qualified Independent Information Sources (QIIS), such as Yellow pages or White pages
- Qualified Independent Information Sources (QIIS), such as Google, Dun & Bradstreet, Hoovers, Bloomberg, Manta, or other address verification sites
- A Legal Opinion Letter or Attestation Letter

### ORGANIZATION VALIDATION ADDITIONAL SOURCES

For **OV orders only**, the same documents used to check the address are acceptable sources of information for a verified phone number. Please keep in mind, the document must contain the phone number for the customer. If the document does not list the verified number as provided by the issuer of the document, it cannot be accepted.

---

Note: DigiCert cannot accept invoices from virtual PBX companies, virtual office/call forwarding services, and Voice over IP (VOIP) services that do not list phone numbers on invoices.

---

### EXTENDED VALIDATION REQUIREMENT: PHYSICAL ADDRESS MATCH

As an additional requirement for EV certificates, DigiCert must obtain a phone number under the name of the applicant, a parent/subsidiary, or affiliate of the applicant, by **matching** the applicant, Parent/Subsidiary, or Affiliate's authenticated **Places of Business** (address).

## Contact Requirements

DigiCert verifies the contact information listed on a certificate enrolment. Verified information and requirements vary by product type and brand. However, all discrepancies must be corrected prior to certificate issuance.

---

Note: Please ensure your customers are aware of the certificate enrolment and respond to all contact attempts in a timely manner, as failure to do so may result in delayed certificate issuance.

---

For all contacts, any email address is allowed, however, it is preferred that the email addresses are affiliated with the enrolling organization and are not free email addresses.

Each order is required to have an **organizational contact**.

- The organizational contact should be listed with the full name; however, aliases are acceptable.
- The organizational contact is not required to be a full-time employee of the applicant's organization. However, it is required that the contact is an authorized representative of the organization.
- The certificate is delivered to the organizational contact.

Regarding the **technical contact**.

- It is not required to have a technical contact listed on the order.
- If provided, the technical contact should be listed with the full name; however, aliases are acceptable.

Some orders (EV and code signing) may require an additional contact. EV certificates require an **EV Approver and Signer** and code signing certificates require a **Code Signing Certificate Requester**. This contact can be the same person as the organizational contact. The requirements for this contact include:

- The full name of the contact must be listed
- The job title must be listed in the contact information
- Employment with organization is preferred but not required

## Request Authenticity

For OV orders, one of the most important steps in the validation process is the Request Authenticity step, which is normally completed via a phone call. DigiCert uses the verified phone number of the enrolling organization to reach the organizational contact and confirm the legitimacy of the order.

### VALIDATION OF AUTHENTICITY WITH A VERIFICATION CODE:

Completing the verification phone call on a first attempt won't always be successful. If DigiCert calls a verified phone number and is only able to reach the customer's voicemail, DigiCert may be able to leave a verification code in the message.

The idea is that once the customer is available to complete the verification call, rather than having to make an outbound call to the verified number once more, the customer can **call DigiCert back** with the code to complete verification.

### REQUEST AUTHENTICITY: ORGANIZATIONAL CONTACT AUTHORITY CONFIRMATION

DigiCert can speak to any employee of the enrolling organization (including the organization contact) to verbally confirm the authenticity of the applicant representative's certificate request.

### EV APPROVER AND SIGNER AND THE CODE SIGNING CERTIFICATE REQUESTER

In EV or code signing certificates, DigiCert must be able to contact the enrolling organization to confirm that the EV approver and signer or the code signing certificate requester has the "authority" to purchase the certificate on behalf of the organization.

All EV orders require **confirmation of the EV approver** and their contact details. DigiCert will verify the contact details of the EV approver through a **verified phone number** of the organization. DigiCert will then complete confirmation (verbal or via e-mail) of the "Delegation Agreement" with the verified EV approver.

## Domain Validated Certificates Specifics

Domain-Validated (DV) SSL certificates provide encryption with **domain-only** validation. These certificates are not validated at the organizational level, but provide validation that the requester is affiliated with use of the domain.

Validation of DV products consists of confirming that the domain name listed in the certificate request is registered, and that the domain approver has control over the domain.

Upon enrolment, an approval request e-mail (also referred to as the "Approver E-mail") is sent to the e-mail selected during the enrolment process. The e-mail **options** provided during the enrolment process include:

- Any e-mail address listed in the public domain registration record ("WHOIS" report), or
- Any one of the following pre-approved e-mail aliases at the domain for the certificate enrolment:
  - admin@
  - administrator@
  - hostmaster@
  - webmaster@
  - postmaster@

**Example:** If the certificate Common Name is www.abc.com, a valid approver e-mail address would be 'admin@abc.com'.

Once the "Approver E-mail" is received, the recipient must click on the link provided to approve or reject the request. This process confirms the approver is affiliated with the domain owner.

As a DigiCert Partner, you can resend the Approver E-mail within your Partner Centre.

---

Note: If a DV certificate request is for a major corporation, well-known trademark, any financial institution or flagged content, additional checks on the domain may be performed for security purposes.

---

If the Approver E-mail process cannot be completed, in special cases the procedure for **practical demonstration** or **DNS check** can be requested to complete validation.

## Legal Opinion Letters

If DigiCert is unable to confirm any of the validation steps of the order, a Legal Opinion Letter may be requested. The Legal Opinion Letter verifies certificate and organization details using one document.

Confirmation of one or more of the following items can be requested:

- Organization registration
- Registered trade names
- Employment & authority of the organizational contact
- Organization's business address & phone number
- Organization's operational existence

### LEGAL OPINION LETTER REQUIREMENTS

Legal opinion letter must be completed by an:

- **Attorney** (solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the applicant's jurisdiction of incorporation or any jurisdiction where the applicant maintains a confirmed office or physical facility.

OR

- **Certified Public Accountant** (chartered accountant, or equivalent) licensed to practice accounting in the country of the applicant's jurisdiction of incorporation or any jurisdiction where applicant maintains an office or physical facility.

OR

- **Qualified Government Officials (OV ONLY)** (based on country regulations) in the country of the applicant's jurisdiction of incorporation or any jurisdiction where applicant maintains an office or physical facility.

  These may include clerks, bailiffs, registrars, judges, justices of the peace and police officers.

  Notaries Publics (outside of the US and Canada) who are a government official or legal can sometimes sign the Legal Opinion Letter.

The signer completing the letter will be verified with the registered bar association or board of accountancy in the appropriate jurisdiction. In addition, we must obtain verified contact details for the signer through their respective registration authority to verify the letter directly with the signer. If DigiCert is unable to verify the signer or their contact details, then DigiCert will not be able to accept the letter for validation.

Note: Please verify who can sign the attestation letter for each of your orders, as it can change from country to country.

## Best Practices

Maintaining control certificate issuance and management can be difficult. SSL administrators at large organizations manage thousands (if not millions) of certificates. How do you ensure certificates are deployed and managed correctly day after day, week after week? We recommend the following best practices: start automating, organize your team, execute timely approvals, use notifications to your advantage, and monitor your network.

Our goal is to get your order to you as quickly as possible, while strictly adhering to the Validation requirements. DigiCert will not issue out a certificate which has not yet passed all validation steps, doing so would jeopardize the integrity of the certificate.

Note: Validation is done on an account basis. If you want multiple certificates added to the same account, please enrol all certificates with the same details (Organization, Address, Contacts details) during enrolment and link domain requests to that Organization account.

### CSR BEST PRACTICES

- Minimum key size is 2048
- Never abbreviate the State field
- Never enter a passphrase in it
- Do not enter the additional company name
- Do not enter an e-mail address in it
- Avoid leaving the OU field blank (simply entering IT will suffice)

### START AUTOMATING

APIs break down barriers between companies, allowing developers to use various technologies to build apps. APIs are the best way to save time by automating and customizing your certificate management, and they can help you keep track of important certificate details:

- Expiration dates
- SSL endpoint errors
- Certificate requests from customers

- Revocation status
- Issuing CA

Make things easier for yourself and use the certificate management platform that allows you to:

- Use an MPKI (Managed PKI) solution
- View a comprehensive dashboard
- Automate via API
- Discover certificates
- Segment and assign user roles
- Set up notifications and escalation paths

The platform you use is the key to maintaining control of your portfolio and managing the certificate lifecycle, including issuance, installation, inspection, remediation, and renewal.

## ORGANIZE YOUR TEAM

A fundamental part of certificate management is managing the individuals involved with your portfolio. You want to have the right key players, segment them by department or team, assign each the right level of access, ensure each knows what he or she is responsible for, and keep each up to date on the processes you have in place.

Managing certificate requests from across the country or across the world becomes a much more manageable task when you divide (organize) individuals into departments, divisions, or units. Regardless of what option you choose, it allows you to segment requests based on location, IP address, internal team, or another classification.

---

Note: These small details help when you have incoming requests with incomplete information. You'll know who to go to retrieve the rest of the information. It also helps track down the right person when there is an expired certificate.

---

### ROLE ASSIGNMENT:

Assigning user roles to each member of your team is crucial to maintaining control of your PKI. If each person has the correct level of access to your management platform, you'll enjoy a less stressful renewal process and more streamlined tracking.

Evaluate each person, where they become part of the process, and what role they play. Whether they are a regular user or should be an admin to approve requests, assigning each person with a role within your certificate management platform gives him or her the right capabilities.

### TRAIN YOUR TEAM:

Keeping your team up to date on your processes and educating them about new technology or implementations is a continuous process. Your system admins and developers need a technical knowledge of how to maintain and deploy certificates. They're allies and you should consult with them for input about all these components when appropriate.

## EXECUTE TIMELY APPROVALS

Streamlined and fast approvals are critical for high-volume issuance and are another important part of maintaining control of your portfolio.

Once you have organized your customers, verification emails should be sent to the appropriate admin(s) for approval to accelerate issuance. The segments you have in place speed up the approval process because all the admin will have to do is verify the accuracy of information and then approve. This saves you the time of hunting someone down to get answers and avoids prolonging deployment.

## USE NOTIFICATIONS TO YOUR ADVANTAGE

You should be notified—at the very least—about certificate expiration; but notifications can also be helpful in other parts of the certificate lifecycle, like when there are pending cert requests, recent revocations, or certificates that need to be reissued.

When a certificate is up for renewal and the owner has not renewed within the set timeframe, you'll need to immediately know who the owner is, whether the cert is being used, and on which server it's being installed. The sooner you see the notification, the sooner you can follow-up and request the renewal.

---

Note: Escalation at the right time brings awareness before it's too late. Setting these types of checks will help you avoid outages caused by expiring certificates.

---

## MONITOR YOUR NETWORK

Lack of visibility into your network results in more worry for you. A Partner platform may have the capability to pull certificate information from your network scans into a comprehensive dashboard view. Use the dashboard for more thorough inspection.

A dashboard view gives you quick insights into your certificate network. Just from a glance, you can assess your overall network health. You can also see upcoming certificate expirations, vulnerable certificate endpoints, and pending certificate requests from other team members. These are just a few examples of the insights gained from using a dashboard to monitor your network.

## GENERAL EXPEDITION FOR CERTIFICATES

To expedite the issuance of your order please ensure that:

- The enrolment is placed under the legal organisation name and jurisdiction
- The organization is active and in good standing
- The domain administrator is aware of the requirement of the domain validation Control.
- The organizational contact is a permanent employee of the enrolling organization (where applicable).

Notifications or request for information are sent to the organizational and/or technical contacts on the order. Please ensure your customers are aware of the certificate enrolment, and respond to our requests in a timely manner. Failure to do so may result in delayed certificate issuance.

As a partner, if you are not a contact on the order, you may reference the order status and reach out to us.

## EXTENDED VALIDATION

If an Organization would like to list its 'trading as' or 'doing business as' name in the certificate, it can **only** appear in the Organization Name field under the following conditions:

- The trading name must be verified with the appropriate government agency as being valid and belonging to the organization.
- The name must appear in conjunction with the verified organization name (incorporated name)

  **Example:** Alphabet Soup (ABC Inc.)

  **Trade name:** Alphabet Soup

  **Organization name:** ABC Inc.

If the full Organization name plus Trading name exceeds our 64-character limit, then **only** the organization name may be used. Remember that the EV approver and signer must complete the EV delegation of agreement.

## CODE SIGNING

- The code signing certificate requester must confirm that the certificate was requested for the organization
- A malware check on the code is performed
- The code signing certificate must be downloaded into the same web browser from which the CSR was generated

© 2018 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.