

# Entrust SSL Certificate Enrollment Guide

The following Enrollment Guide is designed to assist customers in the certificate enrollment process by explaining the necessary steps that must be followed when applying for an Entrust SSL Certificate.

This guide will assist customers with purchase of a Standard (SSL Web server certificate) and Mutual (SSL Web server certificate for Server to Server authentication).

To ensure a quick and smooth enrollment experience, we suggest that you print this guide and gather the necessary information before you attempt to complete the online certificate buy process.

The online certificate enrollment process consists of the following steps:

[Step 1: CSR and Domain information](#)

[Step 2: Providing Order Contacts](#)

[Step 3: Verify your Order Information](#)

[Step 4: The Subscription Agreement](#)

[Step 5: Supply payment information and confirm your request](#)

## Step 1: CSR and Domain information

Step 1 of the online Entrust SSL Certificate buy process will prompt you to supply a Certificate Signing Request (CSR), specify a certificate lifetime, provide a passphrase which will be associated with your order, and finally to identify the type of web server upon which the certificate will be installed.

### Generating and submitting a CSR

The Certificate Signing Request (CSR) is generated with your web server software, and contains both the public key portion of your web server's key pair and the Distinguished Name (DN) of your web server.

Please follow the instructions provided in your web server's documentation to generate a Certificate Signing Request (CSR) for each Entrust SSL Certificate you will require. Entrust also provides documentation for some of the popular [web servers](#).

If an Internet Service Provider (ISP) hosts your Web server, the ISP can provide you with a Certificate Signing Request (CSR) or submit a request on your behalf.

### Backing up your web server's private key

The generation of a Certificate Signing Request also includes the generation of a web server key pair. It is very important to back up the private key as it directly corresponds with the Entrust SSL Certificate you will receive from Entrust.

If the private key is deleted, over written or becomes corrupt you will not be able to use your Entrust SSL Certificate and will have to purchase a replacement certificate from Entrust.

The private key is a very sensitive piece of information. Someone with access to your private key could decrypt SSL-protected data sent and received by your Web server. Please take appropriate steps to ensure that only authorized personnel have access to the web server's private key.

Entrust provides documentation for backing up a web server private key for many common web servers: [http://www.entrust.net/customer\\_support/webserver.cfm](http://www.entrust.net/customer_support/webserver.cfm).

### Tips for creating your Certificate Signing Request (CSR)

When you create your Certificate Signing Request (CSR), your web server application will prompt you for information about your organization and your web server. This information is used to create your web server certificate's Distinguished Name (DN).

Please keep the following points in mind when you supply this information:

## Entrust SSL Certificate Enrollment Guide

- **Country code:** This is the two-letter ISO abbreviation for the country (for example, US for the United States) where your organization's office is legally registered.
- **State or Province:** This is the name of the state or province where your organization's office is located. Please enter the full name of the state or province. Do not abbreviate.
- **Locality:** This is usually the name of the city where your organization's office is located.
- **Organization:** This is the name under which your organization is legally registered. This organization must be the owner of the domain name that will appear in the common name of your Entrust SSL Certificate. Do not abbreviate your organization's name and do not use any of the following characters: '< > ~ ! @ ## \$ % ^ \* / \ ( )'

**You will be required to provide a replacement Certificate Signing Request if the organization name in your CSR is not identical to the legally registered name.**

If you do not have a registered company name, [you may use your full personal](#) name.

- **Organizational unit:** This can be used to identify divisions within an organization or a trade name.
- **Common name:** This is the fully qualified domain name of the web server that will receive the certificate. For example, www.entrust.com or buy.entrust.net. Do not include the protocol specifier (i.e., http:// or https://) or any port numbers or pathnames in the common name. Do not use wildcard characters such as '\*' or '?', and do not use an IP address.

**Most web browsers will display a warning message when connecting to your web site if the web server's fully qualified domain name does not match the common name in the certificate.**

If you are not sure of the ownership of your domain name as listed with the [domain name registrar](#), you should look up this information before submitting your certificate request.

**The domain ownership information held by the domain name registrar, must match the information contained within your application.** This is one of the primary causes for application delays or rejection.

### Pasting the Certificate Signing Request (CSR) into the online enrollment form

To submit your Certificate Signing Request (CSR), simply paste it into the field provided in step 1 of the online enrollment form.

A Certificate Signing Request (CSR) looks similar to the following example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDoABgNVBAgT
B09udGFayW8xEDA0BgNVBACjB01vbnRyYWxwDDAKBgNV
BAoTA0tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2t1bi5j
b20wgZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FL
SGJ9iCF8uwfPW2AKkyyKo/e9aHnnwLLw8WWjhl[ww9pLietw
X3bp6Do8/7mwV3jrgQl0Iwarj9iKMLT6cSdeZ0OTNn7vvJaN
v1iCBWGNypQv3kVMMzzjEtO12uG18VOyeE7jImYj4H1Ma+R1
68AmXT82ubDDR2ivqQw17AgEDoAAwDQYJKoZIhvcNAQEBBQAD
gYEAn8BTcPg4Owo/hGIMU2m39FVvh0M86/ZBkANQCEHxMz/z
rnydXnvrMKPSE208x3Bgh5cGBC47YghGZzdvxYJAT1vbkfCS
BVR9GBxef6/ytkuJ9YnK84Q8x+pS2bEBDnw0D2MwdOSF1sBb
1bcFfkmbpjN2N+hqrrvA0mcNpAgk8nU=
-----END NEW CERTIFICATE REQUEST-----
```

# Entrust SSL Certificate Enrollment Guide

**Important:** Do not include any blank spaces before or after the CSR, and remember to include the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----" lines.

## Selecting a certificate lifetime

Entrust provides Entrust SSL Certificate with a lifetime of either one or two years. In this step you must select your desired certificate lifetime.

Please record the lifetime you would like for your Entrust SSL Certificate.

<b>Certificate lifetime:</b>	
------------------------------	--

## Providing an enrollment passphrase

Supply a passphrase for your enrollment and record it in the space provided. You will need this enrollment passphrase to simplify the certificate renewal process and to revoke your certificate on-line.

For security reasons, your passphrase must contain at least 8 characters, at least one lower-case and one upper-case character, and at least one non-alphanumeric character (such as "%" or "!"). Good passphrases are easy to remember but hard to guess.

**Important:** If you write the passphrase down, please store it in a secure location.

<b>Passphrase:</b>	
--------------------	--

## Supply your web server type

Please record the type of web server, (i.e. the web server software), for which you are requesting an Entrust SSL Certificate. You will be asked to select it from a drop down list in the online request form.

<b>Web server:</b>	
--------------------	--

**At the end of step 1 you can either proceed to step 2 by selecting "Next" or you may enter another certificate request by selecting "Another Certificate?".**

After selecting "Next" or "Another Certificate?" the following information will be extracted from your Certificate Signing Request(CSR) and displayed for your review:

- Common/domain name
- Organizational Unit
- Organization
- City
- State/Province
- Country

Please verify that the displayed information is correct before proceeding to step 2 of the online enrollment application.

If any of the information is incorrect, you must generate a new Certificate Signing Request (CSR) and use the back button to re-enter a corrected Certificate Signing Request (CSR). If the displayed information is correct, and you do not require additional certificates, you may select "Next Step" to proceed to step 2 of the online enrollment application.

## Entrust SSL Certificate Enrollment Guide

Should you choose to enter another certificate request you will be taken back to the beginning of step 1, where you will be prompted to supply information for your second certificate.

### Step 2: Providing Order Contacts

Please provide Entrust with the following three points of contact within your organization.

- **Authorization Contact** - must be a senior member of the organization that owns the domain and has the authority to request an Entrust SSL Certificate on behalf of the organization. This person will receive notification when the certificate is issued and is contacted if further information is required to process your request. Please record the name, address information, telephone number, official title, and email address of the authorization contact.

<b>Full Name of authorization contact:</b>	
<b>Title:</b>	
<b>Company Name:</b>	Extracted from your CSR
<b>Phone number:</b>	
<b>E-mail address:</b>	
<b>Address:</b>	
<b>City/Town:</b>	
<b>State/Province:</b>	Not applicable outside North America
<b>ZIP/Postal Code:</b>	
<b>Country:</b>	

- **Technical Contact** - will receive the Entrust SSL Certificate when it is issued, and is notified about certificate renewals and updates. The technical contact is usually the person responsible for the daily operation of the Web server on which the Entrust SSL Certificate will be installed.

If your server is hosted by a third-party or ISP, someone within that organization should be listed as the technical contact.

Please record the name, address information, telephone number, official title, and email address of the technical contact.

**Note:** You are provided with the following choices: "Same as Authorization Contact", and "Other" to simplify the collection of information. When you select either of the first two options, the form will be updated with the company name and address information from the specified contact.

<b>Full Name of Technical Contact:</b>	
--	--

## Entrust SSL Certificate Enrollment Guide

<b>Title:</b>	
<b>Company Name:</b>	Provide extracted name from CSR or Other as options
<b>Phone number:</b>	
<b>E-mail address:</b>	
<b>Address:</b>	
<b>City/Town:</b>	
<b>State/Province:</b>	Not applicable outside North America
<b>ZIP/Postal Code:</b>	
<b>Country:</b>	

- **Billing Contact**

Please record the name, address information, company name, address, phone number and email address of the billing contact.

**Note:** You are provided with the following choices: "Same as Authorization Contact", "Same as Technical Contact" and "Other" to simplify the collection of information. When you select either of the first two options, the form will be updated with the company name and address information from the specified contact.

<b>Full Name of Billing Contact:</b>	
<b>Title:</b>	
<b>Company Name:</b>	
<b>Phone number:</b>	
<b>E-mail address:</b>	
<b>Address:</b>	
<b>City/Town:</b>	
<b>State/Province:</b>	Not applicable outside North America
<b>ZIP/Postal Code:</b>	
<b>Country:</b>	

# Entrust SSL Certificate Enrollment Guide

## PLEASE NOTE:

- The Authorization Company Name is extracted from the Certificate Signing Request (CSR) from the 'organization' field (o=) and can only be changed by submitting a new Certificate Signing Request (CSR) with the correct information.
- If the Technical contact does not work for the same company as the Authorization contact, Entrust will automatically forward an on-line consent form to the Authorization contact.

The Authorization contact will need to accept the terms in the Consent Form.

Your order will be cancelled if the terms specified within the online Consent Form are **not** accepted.

- State/Province field is only applicable in North America. When information is entered, it **MUST** be a valid State or Province in North America.
- If your organization employs more than 25 people, you must provide different names as authorization and technical contact.
- A technical or authorization contact must be the name of a physical person and not a department name.
- If you do **NOT** wish to receive information on Entrust products and services, select the check box provided at the bottom of Step 2.

## Step 3: Verify your Order Information

The order confirmation page contains the information you entered in each step of the online enrollment. This page provides you the opportunity to verify that the information you have entered is correct before proceeding to the next step.

You can make corrections to the following general information by selecting the appropriate 'Edit' button.

- Authorization contact
- Technical contact
- Billing contact

In addition, the following information is displayed (but cannot be modified) for each Entrust SSL Certificate you requested:

- Domain name
- Distinguished Name
- Certificate Type
- Certificate lifetime
- Web server type

## Step 4: The Subscription Agreement

In this step you are prompted to review the Subscription Agreement, which governs the use of Entrust SSL Certificate.

You must accept the terms and conditions to proceed to the next step.

# Entrust SSL Certificate Enrollment Guide

## Step 5: Supply payment information and confirm your request

You can pay for your Entrust SSL Certificate online with American Express®, Visa®, and Master Card®. Your credit card is not debited until your Entrust SSL Certificate has been issued. You will receive an electronic receipt at the end of the payment process.

If you had supplied a promotional code during the enrollment process, you will not be prompted to supply payment information.

If you wish to pay for your Entrust SSL Certificate by purchase order, purchase orders require pre-approval from an Entrust sales representative.

Please contact 1-888-690-2424 (within North America only) (+1 (613) 270-3411 outside North America), if you require assistance.

When you have provided your payment information, select 'Submit' and your order will be assigned a seven (7)-digit order number.

Please record this number.

You can use it to track the status of your request online at [https://buy.entrust.net/buy/customer/tracking\\_form.cfm?resellerNum=1456154&sourceID=0](https://buy.entrust.net/buy/customer/tracking_form.cfm?resellerNum=1456154&sourceID=0)

### Validation of your Order

Entrust and/or D&B will perform a limited verification of the information in your order before issuing your Entrust SSL Certificate. The following information will be verified:

- Your company or organization (Authorizing organization) has the legal right to conduct business under the organization name specified in your application;
- Your company or organization is the registered owner of the domain name contained in your CSR;
- The information in your CSR is correct; and
- Your company or organization has authorized the issuance of the Entrust SSL Certificate.

**If the information you provided in your application is correct and complete, the verification and certificate issuance process typically takes 3-5 business days.**

If there are any problems, we will contact you immediately.

### Certificate Issuance

Once Entrust has successfully verified your order; the technical contact and the authorization contact specified on your order will receive an email notification. Your technical contact will be provided with a URL to retrieve your Entrust SSL Certificate(s).

To begin using your Entrust SSL Certificate, install it on your web server and ensure that SSL is enabled.

Consult the documentation that came with your Web server software for instructions on how to install the Entrust SSL Certificate and enable SSL. Entrust also provides installation instruction for some of the popular [web servers](#).

# Entrust SSL Certificate Enrollment Guide

## Common Reasons for Delay or Rejection of an Entrust SSL Certificate Order

Please review the following principal reasons for order delay or rejection:

- Authorizing organization is not the registered owner of the domain.
- Authorizing organization is not using a legally registered business or organization name.
- A contact name as provided is an organizational position (i.e: webmaster or security officer) instead of the full name of an employee.
- Only one contact name is provided for Technical and Authorizing contacts in a company with 25 or more employees.
- A business phone number cannot be found through a third party directory.
- Incorrect information contained in the CSR.
- Authorization contact does not accept the terms in the Consent Form or does not respond to telephone call from Entrust or D&B to verify information within the order.

# Entrust SSL Certificate Enrollment Guide

## Enrolling as a Private Individual

Private individuals who wish to apply for an Entrust SSL Certificate are requested to review the following enrollment and verification guidelines.

### Providing Proof of Right

Entrust will require valid Proof of right to verify the identity of the applicant. The following information is required by Entrust to perform this verification:

- A photocopy of their passport/identity document stamped and certified by a relevant authority in the country where they live. The person certifying this documentation needs to provide their name and telephone number for further confirmation if necessary.
- A copy of a current bank statement in their name (They may black out their financial details).
- A voided check from their bank account.

### Domain Ownership

The domain ownership information held by the domain name registrar must match the Private Individual name as specified during enrollment.

If you are not sure of the ownership of your domain name as listed with the domain name registrar, you should look up this information before submitting your Entrust SSL Certificate request.

***This is one of the Primary causes for application delays for rejections***

### Confirming Employment of the Technical Contact

Entrust will locate a telephone number for the application through a third party directory, and will verify the order with the Private Individual.

# Entrust SSL Certificate Enrollment Guide

## Reviewing your Domain Registration Information

To determine the registered owner of your domain name, look up the domain name in the appropriate WHOIS database.

WHOIS databases are maintained by a group of organizations called Network Information Centers (or NICs). Each NIC is responsible for a different top-level domain or group of domains. For instance, Network Solutions (<http://www.networksolutions.com/cgi-bin/whois/whois>) keeps a record of the registered owners in the .com, .edu, .org, and .net domains.

The table below lists Web sites for the most frequently accessed NICs. If your top-level domain is not listed, see <http://www.uninett.no/navn/domreg.html>.

<b>If your domain ends with:</b>	<b>See the Web site:</b>
.com, .edu., .org, or .net	<a href="#">Network Solutions</a>
.mil	<a href="#">U.S. Military</a>
.au	<a href="#">Australia</a>
.ca	<a href="#">Canada</a>
.fr	<a href="#">France</a>
.de	<a href="#">Germany</a>
.gr	<a href="#">Greece</a>
.it	<a href="#">Italy</a>
.jp	<a href="#">Japan</a>
.mx	<a href="#">Mexico</a>
.uk	<a href="#">United Kingdom</a>
.sg	<a href="#">Singapore</a>