

Entrust Certificate Services

Advantage and Standard SSL Certificate

Enrollment Guide

Date of Issue: November 2010



Copyright © 2008-2010 Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.

Enrollment Guide

This guide is designed to help you to enroll for Entrust Certificate Services Standard or Advantage SSL Certificates.

Standard SSL certificates support secure, confidential communication between the Web server and browser certificate letting the client's browser authenticate the identity of the site being accessed.

Advantage SSL certificates create a secure, confidential communications pipe between the Web server and the browser or between servers. Use this type of certificate where identification of both the Web server and the browser is required.

When you buy an Advantage SSL certificate you can add one additional domain (using a SubjectAltName extension) plus the common name for a total of two SANs.

Before you attempt to complete the online certificate enrollment process, please print this guide and gather the necessary information. Enrolling is faster and easier if you have collected the information before beginning the enrollment process.

This Enrollment Guide explains the steps that you must follow to enroll for Entrust Standard or Advantage SSL Certificates.

Information in this guide includes the following topics:

- [“Gather this information before you begin” on page 4](#)
- [“Most frequent reasons for delayed or rejected orders” on page 9](#)
- [“Ordering certificates” on page 10](#)
- [“Verifying your information” on page 20](#)

Gather this information before you begin

Gather the following information before you begin.

Topics covered are:

- “Creating the required certificate signing requests” on page 4
- “Supplying contact information” on page 6

Creating the required certificate signing requests

To create the certificate, Entrust needs a certificate signing request (CSR) for each certificate being purchased. The CSR contains both the public key portion of your Web server's key pair and the Distinguished Name (DN) of your web server. This information is specific to each individual Web server. Create each CSR using the software on the Web server where the certificate will be used.

If you need additional information about creating a CSR, the Entrust Web site provides information for some commonly used Web servers (see http://www.entrust.net/customer_support/webserver.cfm.) If an Internet Service Provider (ISP) hosts your Web server, the ISP can provide you with a CSR or submit a request on your behalf.

Attention: When you create a CSR, a cryptographic key pair is generated. The public key is inserted into the CSR and subsequently signed by the Entrust CA. The private key remains on your computer. Be sure to back up the private key to a secure location. If the private key is lost or becomes corrupt, you will not be able to use your certificate.

Back up your Web server's private key to a secure location and take whatever other steps your organization feels are required to secure the backup. Only authorized personnel should have access to the private key. Anyone with access to your Web server's private key can potentially decrypt the data that is sent and received by your Web server.

You should obtain the following information before creating the CSR. Space is provided in Table 1 for you to record your information.

Table 1: CSR information table

Requested	Description	Information for CSR
Country code	This is the two-letter ISO abbreviation for the country where your organization's office is legally registered (for example, US for the United States).	

Table 1: CSR information table

Requested	Description	Information for CSR
State or Province	This is the name of the state or province where your organization's office is legally registered. 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 legally registered.	
Organization	<p>This is the name under which your organization's business name is legally registered. This organization must be the owner of the domain name that appears in the common name of your Entrust SSL Certificate. Do not abbreviate your organization's name and do not use any of the following special characters < > ~ ! @ ## \$ % ^ * / \ () The name must appear exactly as registered and be verifiable in the appropriate WHOIS database.</p> <p>WHOIS databases are maintained by a group of organizations called Network Information Centers (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. For more information about WHOIS databases, see http://www.internic.net/.</p>	
Organizational unit	This can be used to identify divisions within an organization. It can also be 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 (for example, http or https) or any port numbers or path names in the common name. Do not use wildcard characters such as * or ? or special characters. You may use an IP address if it is registered directly to your company.	

Note: Incorrect information about your domain is a common reason for a certificate order to be delayed or rejected. The domain ownership information held by the domain name registrar must match the information that you enter into the CSR. You should check the domain ownership before creating your CSR.

Supplying contact information

As part of the SSL certificate authorization process, you must provide Entrust with contacts who are able to verify the information you provide when ordering. An Entrust representative or delegate will contact these individuals in your company to check the information. Specific roles have been defined by the CA/Browser Forum as company contacts. A qualified individual from your company must fill each of these roles.

Optionally, you are also asked to include the DUNS number of your company or organization. The DUNS number is the nine digit unique identifier for your business. DUNS stands for Data Universal Numbering System and was created by the Dun and Bradstreet Corporation. If you do not know your DUNS number, leave this field blank.

Although the DUNS number is displayed at the bottom of each page requesting contact information, you only need to supply your company's DUNS number once.

Note: Contacts must be people in your organization. You cannot use a department name or job title instead of a person's name.

Complete the tables in the following sections. You will use this information during the enrollment process.

Note: Some terminology used by the CA/Browser Forum may differ from that used in our enrollment process. Where terminology may differ, the alternate term is shown in parenthesis.

Authorization Contact (Certificate Approver)

This individual:

- must be a senior member of the company or organization that owns the domain
- must have the authority to request an Entrust Certificate on behalf of the organization
- must not also be the Technical Contact

Entrust notifies the Authorization Contact when the certificate is issued and contacts that person if further information is required to process your certificate order.

An online consent form is sent to the Authorization Contact. The consent form enables your company to provide confirmation that:

- The Technical Contact is authorized to order certificates on behalf of the company.

- Your company has exclusive rights to the domain name in the certificate request.

If the Authorization Contact does not accept the terms of the consent form, the request cannot proceed.

Table 2: Authorization Contact information

Information required	Contact information
Name	
Title/Position	
Company Name	
Phone Number	
Email	
Address	
City/Town	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
DUNS Number (optional)	

Technical Contact (Certificate Requester)

The Technical Contact receives the Entrust 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 certificate will be installed. If your server is hosted by a third-party or ISP, someone from that organization should be listed as the Technical Contact.

Table 3: Technical Contact information

Information required	Contact information
Name	
Title/Position	
Company Name	
Phone Number	
Email	

Table 3: Technical Contact information

Information required	Contact information
Address	
City/Town	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
DUNS Number (optional)	

Billing Contact

The Billing Contact is the person in the company who should receive the invoice or credit card receipt.

Table 4: Billing Contact information

Information required	Contact information
Name	
Title/Position	
Company Name	
Phone Number	
Email	
Address	
City/Town	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
DUNS Number (optional)	

Most frequent reasons for delayed or rejected orders

Read this section to be sure that your order is processed as quickly as possible. Here are some causes for delay that Entrust has encountered in the past:

- The Authorizing Organization is not the registered owner of the domain.
- The Authorizing Organization is not using a legally registered business or organization name.
- One or more contact names provided to Entrust were job titles (for example, webmaster or security officer) instead of the full name of an employee.
- The same contact name is provided for Technical and Authorization contacts.
- A business telephone number cannot be found when verifying company or contact information. Entrust uses a third party directory to find the telephone number.
- The Authorization Contact (Certificate Approver) does not accept the terms in the consent form or does not respond Entrust's attempt to verify information.
- The Technical Contact (Certificate Requester) does not respond Entrust's attempts to verify information.

Ordering certificates

After you have gathered the information that Entrust needs to issue a certificate (see “[Gather this information before you begin](#)” on page 4), start the enrollment process. This section is a step-by-step guide to ordering certificates. Topics include:

- “[Step one: Start your order](#)” on page 10
- “[Step two: Provide certificate signing request \(CSR\) information](#)” on page 12
- “[Step three: Provide contact information](#)” on page 15
- “[Step four: Verify and authorize your order](#)” on page 16
- “[Step five: Provide payment](#)” on page 18
- “[Step six: Record your order number and register your account](#)” on page 18
- “[Receiving your certificate](#)” on page 19

Step one: Start your order

Browse to the Entrust Certificate Services (ECS) **Quote Order** page of the Entrust Web site located at the URL <https://buy.entrust.net/>. This page presents you with several options for obtaining certificates. Which option you pursue depends on whether you are a new or returning customer and what method of payment you are using.

Note: If your order is over \$1000.00 you can purchase certificates using a purchase order. To use a purchase order, contact an Entrust representative. If your order is less than \$1000.00 you must use a credit card.

If you already have a customer account

If you already have a customer account, enter your user name and password in the **Returning Customer?** pane and click **Login**. If you do not remember your password, select the **Lost Password?** link. An email with instructions for resetting your password is sent to the address you submitted in the registration process.

As you create your order, you are directed to the same Web pages as a new customer is, but the company and contact information that you have provided to Entrust is pre-entered for your convenience. (See “[To start your order](#)” on page 12.)

If you do not have a customer account

If you do not have a customer account, start the ordering process as outlined in this section. You will have an opportunity to create a customer account at the end of the ordering process.

Figure 1: Entrust Certificate Services ordering page

New Order | Renew

If you have a promotional code or purchase code, please enter it into the box below and click 'Submit'. Your order discount will be calculated and displayed below. Leave this box blank if you do not have a promotional code or purchase order number.

Promotional Code/Purchase Code

Returning Customer?
Enter an email address and passphrase from a previous order and we will pre-populate the contact information for you.

Email Address:
Password: [Lost Password?](#)

Are you buying for a server outside of U.S., Great Britain or Canada?

Type	Lifetime	Quantity?	Description	New/Renew	Certificate Price	Certificate Management Service Price
Advantage SSL	2 Year	1	<ul style="list-style-type: none"> Includes 2 domains Server and client authentication support Unlimited re-issues 	New	382	318
Buy More				Total Price	\$382.00	\$318.00

Purchasing multiple SSL certificates?
Save money. Increase efficiency. Rollover for more [▶](#)

If you have a promotional code

If you have received a promotional code from an Entrust sales representative, enter it in the box labeled **Promotional Code/Purchase Code** and click **Submit**. Using the code at the beginning of the order ensures that you are not prompted for payment at the end of the buying process.

If you have a purchase code

If you have already purchased a block of Entrust SSL Certificates from your Entrust sales representative and are entering the certificate information, enter your purchase order number in the box labeled **Promotional Code/Purchase Code** and click **Submit**. Use the code to be sure that you are not prompted for a credit card number at the end of the buying process.

Note: If you want to buy additional certificates that are not included in the original purchase (and purchase code), you can only do so after you have completed this transaction.

Purchasing certificates using a credit card

If you are purchasing certificates using a credit card, you will be prompted for credit card information at the end of the buying process.

Getting Started

Depending on your method of payment, some information may not be required.

To start your order

- 1 If the Web server where the certificate will be installed is located outside of the United States of America, Canada, or Great Britain, check the appropriate box on the interface.
- 2 Under **Type**, select **Standard** or **Advantage** from the drop down menu.
- 3 Under **Lifetime**, select the number of years from the drop down menu.
- 4 Under **Quantity**, type the number of certificates that you are buying.
- 5 If you require more than one certificate type, select **Buy More**.
The **Certificate Price** and **Total Price** are automatically calculated for you.
- 6 Click **Order**.

Step two: Provide certificate signing request (CSR) information

Entrust needs a certificate signing request (CSR) for each certificate. The CSR must be created by the Web server where the certificate will reside.

To provide the CSR information for your certificate

- 1 Type a passphrase for your order into the **Enter a passphrase for this order** field. The passphrase must have at least eight characters, use at least one upper and one lower case letter, and include at least one special character (!,@,^,& or * for example). If you record the passphrase, be sure to store it in a secure location.
- 2 Follow the instructions provided in your Web server's documentation to generate the CSR file. See the section "[Creating the required certificate signing requests](#)" on page 4 for additional information.
- 3 Open the CSR file generated by your Web server and copy the information, including the **Begin New certificate Request** and **End New Certificate Request** lines. The content of a CSR file resembles the information in Figure 2.

Figure 2: CSR file

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDRzCCArACAQAwbDELMaKGA1UEBhMCVVMxDLALBgNVBAGTBE9oaW8xEDAOBgNV
BAcTB0FueVRvd24xFDASBgNVBAoTC2V4YW1wbGUuY29tMQwwCgYDVQQLLEwNEZXYx
GDAWBgNVBAMTD3d3dy5leGFtcGxlLnVvbTCBnzANBGlKqhkig9w0BAQEFAAOBjQA
wYkCgYEAxImEXhW4x+qFiSr74SpismDNCGEnSm8suGFa4m9hKy/CFkYswDnVvxNS
0gCC1bPidyjorLR2bMv58q6byH4trhFCoI+M8NYbFai8W7i48EAznQ4BFNGHY7q2
0CW0QXzeL9SYSKXOmKcL4xgedM6kkMcAzCUJ55fHPt81Ss6ap0UCAwEAAaCCAzkw
GgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBBrMA4G
A1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCGGSIB3DQMCAGIAGDAO
BggqhkiG9w0DBAICAIawBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYI
KwYBBQUHAWewgf0GCisGAQQBgjcNAgIXge4wgesCAQEewgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuaG4AZQBsaCAAQwByAhhAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgvBAHYAaqBkAGUAcgOBiQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0GCSqGSIb3DQEBBQUAA4GBAE4Ttldb
ikk4Kpgyv7IM8tu+EkHVomPO2QzMJ4OH3HAHEIa+4IuE1mgTGFpnl6dptZL1vhO
IsmY93+gWiyLHIYtrU6uV/0vf1sRyQ0kLX7/akEs/MGtOKSFgMO0XYWtsIeVVn3
QN35X1wmvQDnt7GyegLXyuH3rDcvkA6WfVaj
-----END NEW CERTIFICATE REQUEST-----

```

Attention: Do not include any blank spaces before or after the CSR. Include -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- lines.

- 4** Paste the CSR information into the space provided in the **Provide CSR** page as shown in Figure 3. A separate space is provided for each of the certificates that you specified in **“Step one: Start your order”** on page 10.

Figure 3: Entering your certificate signing request (CSR)

Enter a passphrase for this order:

This passphrase is required when renewing. Please keep it in a safe place.

✔ 8 Characters ✔ 1 upper case letter ✔ 1 lower-case letter ✔ 1 Special Character ?

Tracking ID	Type	Paste Certificate Signing Request (CSR), obtained from your server. CSR FAQ
1	2 year Advantage	<pre>-----BEGIN NEW CERTIFICATE REQUEST----- MIIEZDCCA0wCAQAwwYmxCzAJBgNVBAYTAkNBMRwwDgYDVQ QIEwdPbnRhcmlvMRwwDgYDVQQHEwdBbnI0b3duMRwwEgYDV QQKEwtleGFtcGxlLmNvbTEUMBIGA1UECXMZLXhnbXBsZS5jb20 xJDAiBgNVBAMTG2RvYzJrM2dzLmdzZG9jMS5lbnRydXN0LmNv bTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN PEv0GjKERnUQR+BZIO5WH2DSmYRG5754NwBdXmjD5817uHB yPspSiR78Lk2IW1xOIXpPSI2dkc4LpVuCZMBXX42HZXpczmf6/aBf POOMBr+ToKFFcAXb0c/9kf67riltN3JpyJx2HzTVa4mzoMLduqEhw 5PLYFRu/yBly8XO6IW84T8UqmJfzogKwCM+sPjyQp38SDH6S8V UJRSQH2KJm2LyVHuMed34qyR4bO6WEZKINB8v1bp2Z7t9OoZ RUKhLCTJ21GsDpiXemn62oa6VXb/QknykJt8S+kN3dJwC3LIQIK7 T8mtKlM2DMERn4HtcovArff4WSeuKY7VDTOfkCAwEAAsCAZk You will be allowed to enter extra domains (SubjectAltNames) on the next screen</pre>

[Add Another Certificate](#)

- Supply a CSR for each of the certificates. To add a certificate to your order click **Add Another Certificate**. If you decide to order fewer certificates than you requested when you started the order, do not fill in the information for those certificates, and you will not be charged.
- Click **Next**.
The confirmation page appears.

Certificate	Type	CSR Content	
1	2 year(s) Advantage	Server1.example.com UserDN=cn=Server1.example.com, ou=example.com, o=example.com, l=Anytown, st=Ontario, c=CA Domain(s): Include all/Remove all <input type="text" value="Server1.example.com"/> <input type="text" value="Default"/> <input type="text"/> Add a new domain	Valid [Replace]

- Optionally, add domains to the certificate by clicking **Add a new domain** and entering more another domain. The name must be a valid domain name owned by your organization (Entrust verifies this). Different types of certificates allow
- Verify that the certificate information is correct.
If you need to change the information, click **Replace** or return to the previous page. Generate a CSR on the Web server with the correct information and use it in place of the incorrect request.
- Click **Next**.

Step three: Provide contact information

At this point you have the opportunity to enter the names and contact information of the individuals in your organization acting as the:

- Authorization Contact
- Technical Contact
- Billing Contact

This is the information that you recorded in [“Supplying contact information” on page 6](#).

To provide contact information

- 1 Type the required contact information for one of the individuals filling a role into the indicated field.. Optionally, fill in the DUNS number of your company.

Provide Contact Information

All fields are mandatory.

First Name	<input type="text" value="Alice"/>		
Last Name	<input type="text" value="Gray"/>		
Title/Position	<input type="text" value="Senior Support Specialist"/>		
Company Name	<input type="text" value="example.com"/>		
Phone Number	<input type="text" value="555-555-5555"/>		
Email Address	<input type="text" value="alice.gray@example.com"/>		
Address	<input type="text" value="1234 Anystreet"/>		
	<input type="text"/>		
City/Town	<input type="text" value="Anytown"/>		
State/Province	<input type="text" value="ON"/> ▼	Zip/Postal Code	<input type="text" value="K7M 4B2"/>
State/Province is optional outside North America.			
Country	<input type="text" value="Canada"/> ▼		

- At the bottom of the page, select the role of the contact (for example, Authorization Contact).

Authorization Contact	<input checked="" type="checkbox"/>
Billing Contact	<input type="checkbox"/>
Add	

The information that you provide to Entrust in this form will be used to notify you of Entrust products and services that we think may be of interest to you.

- Click **Add**.
- Repeat these steps for each contact. The list of contacts at the top of the page reflects the information you have provided. If you need to alter this information, click **Edit**. **Remove** deletes the contact information.

New Order | [Renew](#)

Contact Information

Authorization Contact:	Bob Lee	[Edit] [Remove]
Technical Contact:	Alice Gray	[Edit] [Remove]
Billing Contact:	Required	

- When you have finished entering contacts, click **Next**.

Step four: Verify and authorize your order

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

To verify and authorize your order

- Click **Review** beside each contact listing to display their contact information.

Authorization Contact:	Bob Lee	[Review]	[Edit]
Technical Contact:	Alice Gray	[Review]	[Edit]
Billing Contact:	Michael Fiello	[Review]	[Edit]

The contact information appears below.

Authorization Contact

Name:	Bob Lee
Title/Position:	Director of operations
Company:	example.com
Address:	Anystreet
City:	Anytown
State:	PA
Zip/Postal Code:	12345
Country:	US
Phone:	555 555-5555
Email:	bob.lee@example.com

If necessary, click **Edit** beside the listing and change the contact information.

- 2 Make a final check of the CSR content. If necessary, click **Replace** to correct the information
- 3 Read the **Subscription Agreement(s)** section. If you accept the agreement click **Next** to proceed to the payment page.

Subscription Agreement(s)

Entrust Certificate Services Subscription Agreement

Attention - read carefully: this Entrust Certificate Services Subscription Agreement ("Agreement") is a legal contract between the Subscriber and Entrust. Before continuing, please carefully read this agreement and the CPS, as amended from time to time, which is incorporated into this Agreement and which collectively contain the terms and conditions under which you are acquiring a limited right to use the Certificate Services.

The individual who clicks on the "accept" icon below or submits an application for Certificate Services, represents and warrants: (i) you have the legal authority to bind the Subscriber to the terms and conditions of this Agreement and including the CPS; (ii) Subscriber is legally bound by the terms of this Agreement. If you do not agree to the terms and conditions of this Agreement, click on the "decline" icon below and do not continue the application process.

1. Definitions: In addition to capitalized terms defined elsewhere in this Agreement or the CPS, the following capitalized words will have the meaning set out below:

By proceeding to the next step, I have read, understood and accept the Subscription Agreement.

Please indicate which role you are:

[Previous](#) [Next](#)

Attention: By proceeding to the next step, you declare that you are authorized to request certificates on behalf of your company and that all of the information you entered during enrollment is true and correct.

Step five: Provide payment

Your payment options are:

- Pay for your Entrust SSL Certificates online with American Express®, Visa® or Master Card®. Your credit card is not charged until your Entrust SSL Certificate has been issued. The Billing Contact receives an electronic receipt at the end of the payment process.

Entrust Limited, 1000 Innovation Drive Ottawa, Ontario, Canada K2K 3E7
Phone: 1-877-369-7483 or 1-613-270-3769
Fax: 1-877-839-3538 or 1-613-270-3260 [E-mail](#)

Payment Methods

Credit Card

Card Type:	Visa
Card #:	1234567890
Expiry:	3 2012 Month Year
Does the Billing Address of this card match the Billing Contact for the order?	<input checked="" type="radio"/> Yes <input type="radio"/> No

How Did You Hear About Us? [News release/product review/analyst report](#)

[Process Order](#)

[Previous](#)

- If you supplied a promotional code during the enrollment process, you will not be prompted to supply payment information unless you are purchasing additional certificates.
- If you are paying by purchase order and you have contacted an Entrust sales representative you will have received and used your purchase order code (see “[If you have a purchase code](#)” on page 11) and will not be prompted to supply further payment information. If you have not contacted a sales representative you can do so by telephone at 1-888-690-2424 within North America or +1 (613) 270-3411 outside North America.

To help our sales team, please select the option that applies to you from the **How Did You Hear About Us?** drop-down box.

Click **Process Order** to submit your certificate order to Entrust.

Step six: Record your order number and register your account

Entrust assigns a seven digit order number to your order. The number is displayed on the **Process Order** page. Record the order number and use it to identify your order in all correspondence with Entrust SSL Certificate Services Support and Verification agents.

The order number can also be used to track the status of your request online at http://www.entrust.net/customer/tracking_form.cfm

If you have not created an account with Entrust, you can do so by clicking **Register Now**. If you have an account, Entrust retains the company and contact information that you entered during enrollment. The information appears automatically when you order certificates, so you do not need to enter it again.

Receiving your certificate

Entrust validates the information in your order before issuing your Entrust SSL certificate. The validation process checks that:

- 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
- your company or organization has authorized the issuance of the Entrust SSL Certificate

If the information you provided in your order is correct and complete, your certificates are issued in 3-5 business days. If there are any problems, Entrust will contact you immediately.

After your order has been verified, Entrust notifies the Technical Contact and the Authorization Contact specified in your order. Your Technical Contact is provided with a URL to retrieve your Entrust SSL Certificates.

Consult your Web server documentation for instructions on installing the Entrust SSL Certificate and enabling SSL. If you require more information, Entrust provides installation instructions for some common Web servers at http://www.entrust.net/customer_support/webserver.cfm.

Verifying your information

This section is a high level overview of the verification process used by Entrust to validate the information supplied in your certificate enrollment request.

Checking business information

Entrust checks the business name that you supply to prevent the unauthorized use of your organization's name in a Web server certificate. To check this Entrust verifies your information using online business registration databases to confirm the business at the address provided in the order.

If Entrust is unable to locate the business registration information utilizing the online databases you will be asked to provide one of the following:

- business license
- Articles or Certificate of Incorporation
- Articles of Organization (Non-profit organization or LLC)
- DBA (Doing Business As) registration
- Fictitious Business Name Statement
- Charter documentation (Banks, Universities, Government Agencies)

Confirming contact information

In the online certificate request form, Entrust requires the customer to identify three points of contact with the organization: a Technical Contact, an Authorization Contact and a Billing Contact.

Entrust checks the contact information to be sure that the individuals are employed by the company or organization, are qualified for their role and are willing to fulfill their role.

Entrust obtains a telephone number for the authorizing company through a third party directory. The third party telephone number is obtained through one of the following:

- company telephone bill (company name, address and telephone number)
- a telephone operator (directory assistance)
- online telephone directory (for example, yellowpages.com)

Entrust will place a telephone call to the main reception desk to get in touch with the Authorization Contact. Entrust will verify with the Authorization Contact that they employ the Technical Contact, directly or through an out sourced company.

If Entrust is unable to find a third party telephone number or Entrust is unable to contact the Authorization Contact by telephone, we will send an email request for the information to the Authorization Contact, and place the order on hold. If Entrust has

not received a reply within 30 days from the date order was placed, Entrust will notify the customer and cancel the order.

Checking information from private individuals

Private individuals can apply for an Entrust SSL certificate. As a private individual, you must provide appropriate proof of right. For example:

- a photocopy of your passport or identity document, stamped and certified by a relevant authority (for example, a notary or lawyer who is qualified to certify these documents in the country where you live)

The person certifying this documentation must provide their name and telephone number for further confirmation, if required by Entrust.

- a copy of a current bank statement in your name (you may black out the financial details)
- a voided check from your bank account

If Entrust does not receive your information, we will send you an email requesting the information, and place your order on hold until it has been supplied. If you do not reply within thirty days from date when the order was placed, Entrust will notify you and cancel the order.

