Entrust Certificate Services

Standard and Advantage SSL Certificate

Enrollment Guide

Software release: 11.2

Date of Issue: May 2013

Document issue: 2.0

Entrust®
Securing Digital Identities
& Information

Copyright © 2008-2013 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

Use this guide to help you enroll for Entrust Certificate Services Standard or Advantage SSL Certificates.

- Standard SSL certificates support secure, confidential communication between the Web server and browser. The client's browser can check the authenticity of the Web site being accessed.
- Advantage SSL certificates also create a secure, confidential communications pipe between the Web server and the browser but can be used 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 domains for each certificate.

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

This guide explains the steps 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 common reasons for delayed or rejected orders" on page 9
- "Ordering certificates" on page 10
- "Verifying your information" on page 21

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. Create each CSR on the Web server where the certificate will be used.

The Entrust Web site provides information on generating a CSR for some commonly used Web servers (see http://www.entrust.net/knowledge-base/index.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:

Creating a CSR generates a cryptographic key pair. The public key is inserted into the CSR and subsequently signed by the Entrust CA. The private key remains on your computer.

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 or CA for Canada).	
State or Province	This is the name of the state or province where your organization's office is legally registered.	

Table 1: CSR information table

Requested	Description	Information for CSR
Locality	This is usually the name of the city where your organization's office is legally registered.	
Organization	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. 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/.	
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 protected by 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.

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 to check the information. Specific roles are defined by the CA/Browser Forum as company contacts. A qualified individual from your company must fill each of these roles.

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 CA/Browser Forum 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	

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	
Address	
City/Town	

Table 3: Technical contact information

Information required	Contact information
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	

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	

Most common reasons for delayed or rejected orders

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

- 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 gather 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 11
- "Step three: Provide contact information" on page 14
- "Step four: Verify and authorize your order" on page 16
- "Step five: Provide payment" on page 18
- "Step six: Record your order number" on page 19
- "Receiving your certificate" on page 19

Step one: Start your order

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

Getting Started

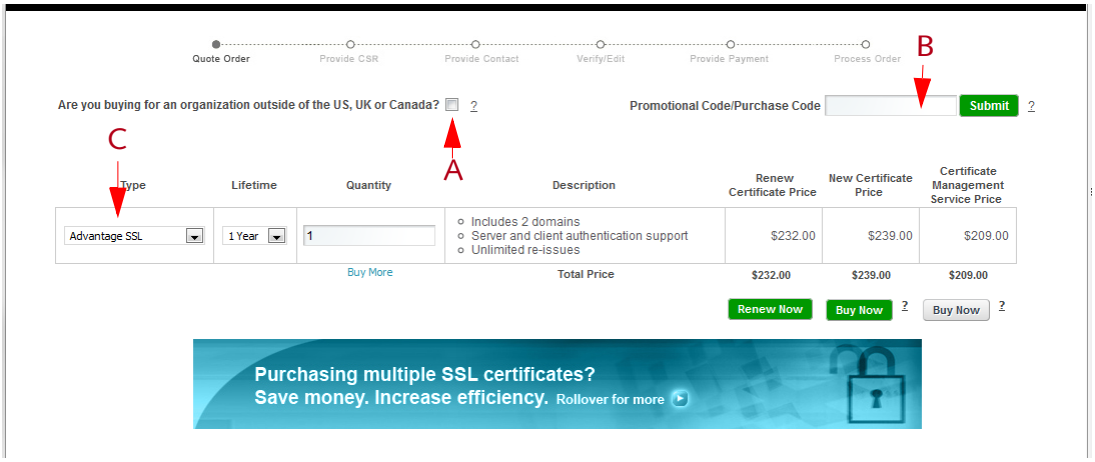
Depending on your method of payment, some information may not be required.

To start your order

1. Browse to the Entrust Certificate Services (ECS) Web site located at the URL https://buy.entrust.net/ and click Standard or Advantage.

   The **Quote Order** page opens presenting you with several options for obtaining certificates depending if you are purchasing certificates with the Entrust Certificate Management Service or not, and what method of payment you are using.

Figure 1: Entrust Certificate Services ordering page



2. If you are installing the certificate on a machine located outside of the United States, Canada, or Great Britain, check the applicable box (A).
3. If you received a promotional code or purchase code from an Entrust sales representative, enter it in the box (B) labeled **Promotional Code/Purchase Code,** and click **Submit**.

   By using the code, you will not be prompted for a credit card number at the end of the buying process.
4. Under **Type** (C), select either **Advantage SSL** or **Standard SSL** from the drop-down list.
5. Under **Lifetime** select the number of years before the certificate expires from the drop-down list.
6. Under **Quantity**, type the number of certificates to purchase.
7. If you require more than one certificate type (that is, both an Advantage and Standard), select **Buy More** and provide the lifetime and quantity.

   The **Certificate Price** and **Total Price** are automatically calculated for you.
8. Click **Buy Now**.

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.

Before continuing, generate a CSR for each certificate. Each CSR must be created by the Web server where the certificate will reside. 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.

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. 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.

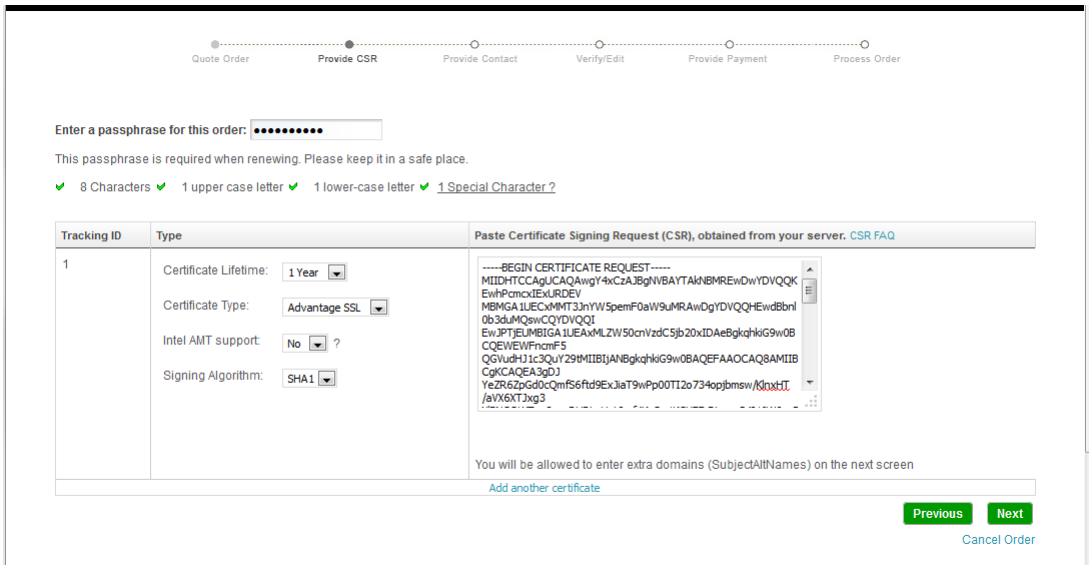
Figure 2: Sample CSR file


```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDRzCCArACAQAwbDELMAkGA1UEBhMCVVMxDTALBgNVBAgTBE9oaW8xEDAOBgNV
BAcTB0FueVRvd24xFDASBgNVBAoTC2V4YW1wbGUuY29tMQwwCgYDVQQLEwNEZXYx
GDAWBgNVBAMTD3d3dy5leGFtcGxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAxImEXhW4x+qFiSr74SpismDNCGEnSm8suGFa4m9hKy/CFkYswDnVvxNS
0gCClbPidyjorLR2bMv58q6byH4trhFCoI+M8NYbFai8W7i48EAZnQ4BFNGHY7q2
0CW0QXzeL9SYSKXOmKcL4xgedM6kkMcAzCUJ55fHPt81Ss6ap0UCAwEAAaCCAZkw
GgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4G
A1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAO
BggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYI
KwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAs0mlwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAE4Ttldb
ikK4Kpgyvv7IM8tU+EkHVoMPO2QzMJ4OH3HAHEIa+4IuE1mgTGFpn16dptZL1vhO
Ismy93+gWiycLHIYtru6uV/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.

3 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 certificate that you specified in "Step one: Start your order" on page 10.

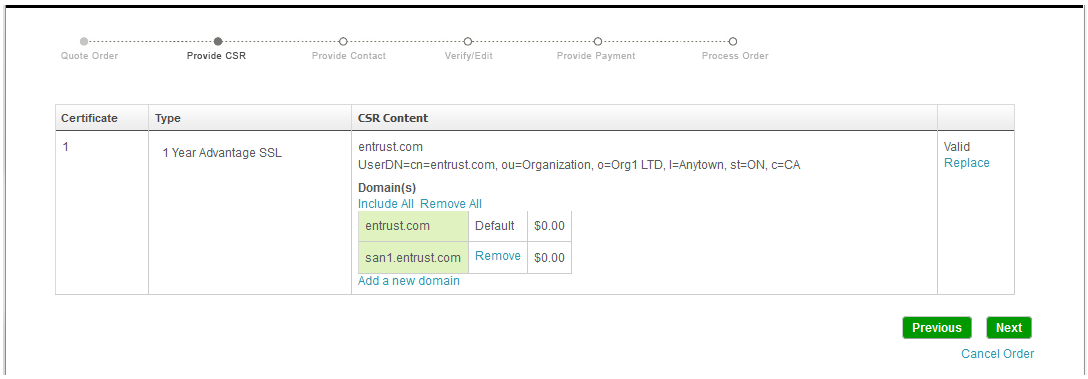
Figure 3: Entering your certificate signing request (CSR)



4 To add another certificate to your order, click **Add Another Certificate**. Supply a CSR for each of the certificates. 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.

5 Click **Next**.

The confirmation page appears.



For an Advantage SSL certificate, you can add one additional domain at no extra cost. Click **Add a new domain** and enter another domain. The name must be a valid domain name owned by your organization (this information will be verified). The extra domain is added to the certificate as a SubjectAltName (SAN) extension.

If you notice a mistake in the name after adding the domain, remove it and add one with the correct name. Only two domains can be included in the final certificate (the default domain and one of your choosing), however you can remove and include domain names to edit your selection.

Note:
If your CSR has more than two domains, they will appear in this list. Select the one that you wan to add to the certificate.

6 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.

7 Click **Next**.

Step three: Provide contact information

You must enter the names and contact information of individuals in your organization who will assume the roles of:

- 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 Below the **Provide Contact Information** pane, select the role of a contact (for example, technical contact).

Contact Information

Billing Contact	Required	
Authorization Contact	Required	
Technical Contact	Required	

Provide Contact Information

All fields are mandatory.

First Name	Bob
Last Name	Lee
Title/Position	Support Specialist
Email Address	bob.lee@example.com
Phone Number	555 555-1123
Company Name	example co
Address	123 Anystreet
City/Town	Anytown
Country	Canada
State/Province	Ontario
Zip/Postal Code	K2B E7N

Add as (check all that apply) :

Note: Entrust requires you to provide different contacts for the authorization and technical contacts.

- ☐ Billing Contact
- ☐ Authorization Contact
- ☑ Technical Contact

Add

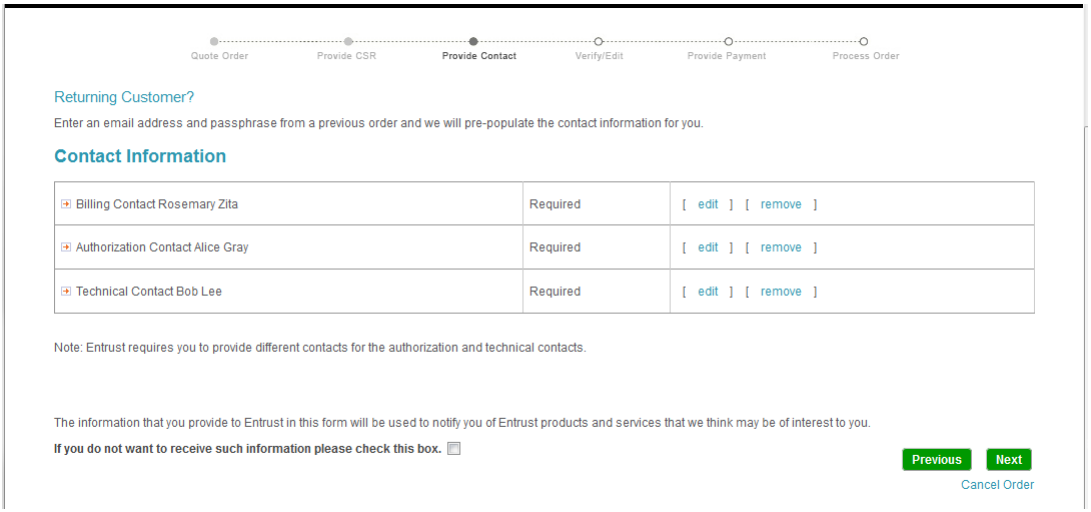
2 Type the required contact information for one individual who will fill the indicated role.

3 Click **Add**.

The list of contacts at the top of the page is updated to reflect the contact information. If you need to alter this information, click **edit** beside a name, or click **remove** to delete a contact.

4 Repeat these steps for each contact. (The **Provide Contact Information** pane disappears after you complete all contacts.)

.



5 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

1 Optionally, click **review** beside each contact listing to display their contact information.

The Authorization Contact is the default view. If you wish to view the other contacts please select the "Review" link.

Billing Contact Rosemary Zita	Required	[review]	[edit]	
Authorization Contact Alice Gray	Required	[review]	[edit]	
Technical Contact Bob Lee	Required	[review]	[edit]	

Authorization Contact

First Name	Alice
Last Name	Gray
Title/Position	Director of Operations
Email Address	alice.gray@example.co
Phone Number	555 555-1212
Company Name	Org1 LTD
Address	123 Anystreet
City/Town	Anytown
Country	Canada
State/Province	Ontario
Zip/Postal Code	K2B E7N

The contact information appears below.

If you need to change any contact information, click **edit** beside the listing and make the change.

2 Make a final check of the CSR content. If necessary, click **Replace** to correct the information.

Certificate	Type	CSR Content	
1	1 Year Advantage SSL	entrust.com UserDN=cn=entrust.com, ou=Organization, o=Org1 LTD, l=Anytown, st=ON, c=CA Domain(s) entrust.com san1.entrust.com	[Replace]

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.

Previous Next

Cancel Order

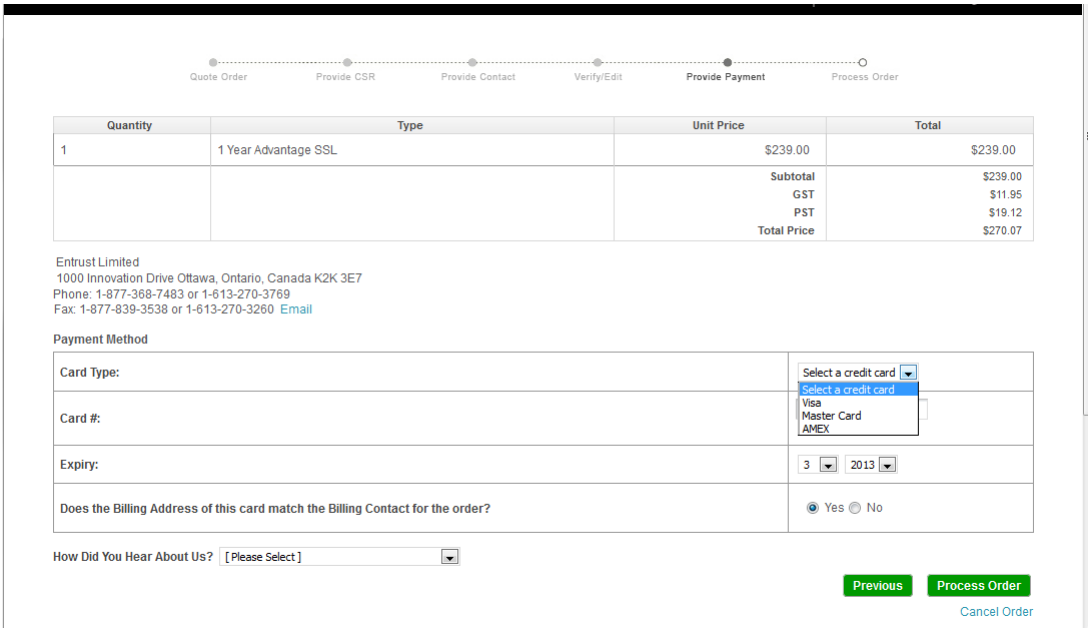
3 Read the **Subscription Agreement(s)** section. If you accept the agreement and are ready to complete the order, click **Next** to proceed to the payment page.

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

If you have already elected to pay by purchase order and used the purchase order code given to you by an Entrust sales representative you are not prompted to supply further payment information. Otherwise 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.



- .If you have not contacted a sales representative and you want to pay by purchase order, you can do so by telephone at:

– 1-888-690-2424 within North America

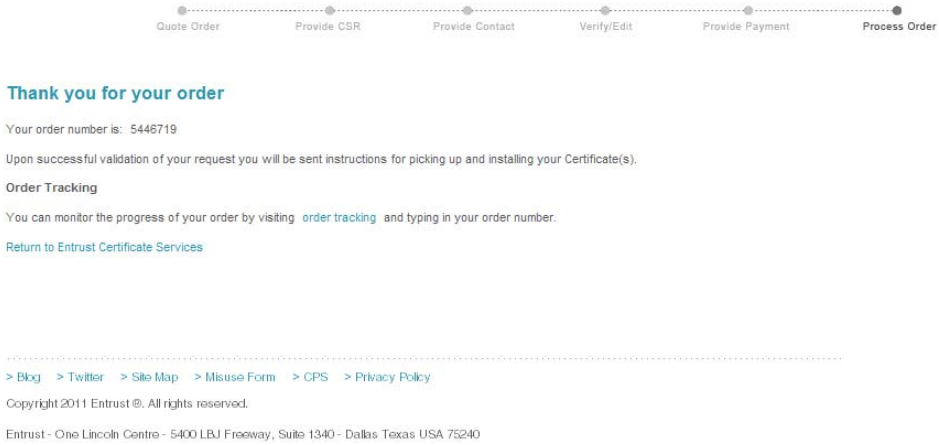
– +1 (613) 270-3411 outside of North America.

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

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

Step six: Record your order number

Entrust assigns a number to your order. The number appears on the **Process Order** page. Record the order number and use it to identify your order in any correspondence with Entrust SSL Certificate Services support and verification agents.



You can use the order number to track the status of your request online at http://www.entrust.net/customer/tracking_form.cfm

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 three to five 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/knowledge-base/index.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.