

Entrust Certificate Services

EV Multi-domain Certificate

Enrollment Guide

Date of Issue: October 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.

Obtaining technical support

For support assistance by telephone call one of the numbers below:

- 1-866-267-9297 in North America
- 1-613-270-2680 outside North America

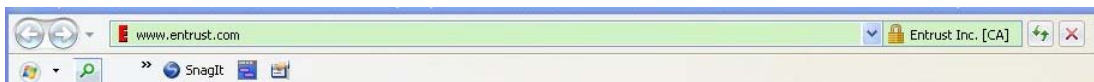
You can also email Customer Support at:

- ssl@entrust.com

Enrollment Guide

Entrust EV Multi-domain (extended validation) SSL certificates provide all of the benefits of an Advantage SSL Certificate but conform to the more stringent EV verification standards set by the CA/Browser Forum. Pages from Web sites protected by these certificates display a green address bar and gold padlock at the top and display the issuer and organization name, and country (in Microsoft® Internet Explorer 7 or higher browsers with Windows XP, Vista or Windows 7).

Figure 1: Browser address bar



Before starting 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 apply for Entrust EV Multi-domain SSL Certificates.

Information in this guide includes the following topics:

- ["Gather this information before you begin" on page 4](#)
- ["Common reasons for delayed or rejected orders" on page 12](#)
- ["Ordering certificates" on page 13](#)
- ["The validation process" on page 26](#)

Gather this information before you begin

Gather the following information before you begin.

Topics covered in these sections are:

- “Creating the required certificate signing requests” on page 4
- “Supplying contact information” on page 5
- “Supplying information about your company or organization” on page 9

Creating the required certificate signing requests

To create the certificate, Entrust needs a certificate signing request (CSR) for each certificate 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 the 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
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.	

Table 1: CSR information table

Requested	Description	Information
State or Province	This is the name of the state or province where your organization's office is legally registered. 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 legally registered.	
Organization	This is the name under which your organization's business is legally registered. This organization must be the owner of the domain name that will appear in the common name of your Entrust EV Multi-domain 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. For more information about WHOIS databases, see http://www.internic.net/ .	
Organizational unit	This can be used to identify divisions within an organization or it could be a trade name.	
Common name	This is the fully qualified domain name (FQDN) 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. EV Multi-domain certificates cannot be issued to an internal domain or an IP address.	

Note: Incorrect information about your domain is a common reason for an EV Multi-domain 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 Extended Validation authorization process, you must provide Entrust with contacts who are able to verify your certificate information. An Entrust representative or delegate will contact these individuals in your company to check this 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.

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. This information is used 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

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 on-line 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	
Street address	
City	
State/Province (optional if outside North America)	

Table 2: Authorization Contact information

Information required	Contact information
ZIP/Postal Code	
Country	
Phone	
Email	

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 EV Multi-domain 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	
Street address	
City	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
Phone	
Email	

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	
Street address	
City	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
Phone	
Email	

Contract Signer (optional)

The individual who signs the subscription agreement on behalf of the company. The same person can fill the Authorization Contact (Certificate Approver) role.

If you specify a Contract Signer, the subscription agreement is sent to that person. The agreement must be accepted before the order can be processed.

Table 5: Contract Signer information

Information required	Contact information
Name	
Title/Position	
Company	
Street address	
City	
State/Province (optional if outside North America)	

Table 5: Contract Signer information

Information required	Contact information
ZIP/Postal Code	
Country	
Phone	
Email	

Supplying information about your company or organization

You must supply specific information about your company to Entrust. This enables Entrust to validate your certificate information.

The authorization company name is extracted from the from the organization field (o=) of the DN in the CSR. If the information is not correct Entrust corrects it and advises you of the change.

Jurisdiction of incorporation (optional)

If you know the jurisdiction in which your company is incorporated, provide the information. If you do not know this information, leave this pane blank in the online enrollment form.

The incorporating agency is the governing body under which you are incorporated. If you are incorporated at the state level this could be the Commonwealth of Pennsylvania, for example.

Table 6: Jurisdiction of incorporation (optional)

Information required	Contact information
Registration number	
Incorporating agency	
Date of incorporation	
City/Town (if applicable)	
State/Province (if applicable)	
Country	

Business headquarters

Entrust requires the address of your business headquarters. Optionally, 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.

Table 7: Business headquarters

Information required	Contact information
Address	
City/Town	
State/Province	
ZIP/Postal Code	
Country	
DUNS number (optional)	

Higher Authority

The Higher Authority confirms the identity of the other contacts. A Higher Authority can be a corporate executive, legal counsel, company director or the direct manager of the Contract Signer or Authorization Contact. The person acting as the Higher Authority cannot also be the Contract Signer or Authorization Contact.

You do not have to list a Higher Authority when you enroll for a certificate, however your company must supply this contact to Entrust before the certificate order can be filled. If you do not list a Higher Authority, your Authorization and Technical Contacts will be reminded that one is required. If you list a Higher Authority when you enroll, the person filling that role will be advised of the role's requirements by email.

Table 8: Higher Authority information

Information required	Contact information
Name	
Title/Position	
Company	
Street address	
City	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	

Table 8: Higher Authority information

Information required	Contact information
Phone	
Email	

Common reasons for delayed or rejected orders

Be sure that your order is processed as quickly as possible. Familiarize yourself with these common reasons for delayed orders:

- The Authorizing Organization is not the registered owner of the domain.
- The Authorizing Organization does not submit their full legally registered business or organization name.
- One or more contact names provided to Entrust are job titles (webmaster or security officer, for example) instead of the full name of an employee.
- The same name is provided for the Higher Authority, Technical and Authorizing contacts.
- A business phone number cannot be found when verifying company or contact information.
- Higher Authority contact information is never provided.
- The Higher Authority contact does not respond to Entrust's attempt to verify information. Verification must be done live, by telephone using a telephone number that Entrust has obtained from a third party resource.
- The Contract Signer contact does not respond to Entrust's attempt to verify that they signed the subscription agreement.
- The Authorization Contact (Certificate Approver) does not accept the terms in the consent form or does not respond to Entrust's attempt to verify information.
- The Technical Contact (Certificate Requester) does not respond to 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), you can start the enrollment process. This section contains step-by-step instructions for ordering certificates. Topics include:

- “[Step one: Start your order](#)” on page 13
- “[Step two: Provide certificate signing request \(CSR\) information](#)” on page 15
- “[Step three: Provide contact and business information](#)” on page 18
- “[Step four: Verify and authorize your order](#)” on page 21
- “[Step five: Provide payment](#)” on page 23
- “[Step six: Record your order number and register your account](#)” on page 24
- “[Receiving your certificate](#)” on page 25

Step one: Start your order

To begin ordering certificates, 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. If you use a purchase order, contact an Entrust representative. If your order is smaller 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 but the company and contact information that you have already provided to Entrust is pre-entered for your convenience. (See “[To start your order](#)” on page 15.)

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 2: Entrust Certificate Services ordering page

The screenshot shows the Entrust Certificate Services ordering page. At the top, a progress bar indicates the steps: Quote Order, Provide CSR, Provide Contact, Verify/Edit, Provide Payment, and Process Order. Below the progress bar, there are two main sections: a promotional code field and a returning customer login section. The promotional code field is labeled "Promotional Code/Purchase Code" and has a "Submit" button. The returning customer login section is titled "Returning Customer?" and includes fields for "Email Address:" and "Password:", along with a "Login" button and links for "Lost Password?". Below these sections, there is a checkbox for "Are you buying for a server outside of U.S., Great Britain or Canada?". The main part of the page is a table of certificate options. The table has columns for "Type", "Lifetime", "Quantity?", "Description", "New/Renew", "Certificate Price", and "Certificate Management Service Price". The first row shows "EV Multi-Domain" with a dropdown arrow, "1 Year" with a dropdown arrow, "5" in a text box, and a description: "Includes 2 domains, Highest level of assurance, Unlimited re-issues, checklist". The "New/Renew" column shows "New", and the "Certificate Price" and "Certificate Management Service Price" columns both show "1995". Below the table, there is a "Buy More" link and a "Total Price" row showing "\$1,995.00" for both the certificate price and the management service price. At the bottom of the table, there are two "Order" buttons. Below the table is a banner for "Purchasing multiple SSL certificates? Save money. Increase efficiency. Rollover for more" with a play button icon and a padlock icon.

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
EV Multi-Domain <input type="button" value="v"/>	1 Year <input type="button" value="v"/>	<input type="text" value="5"/>	Includes 2 domains Highest level of assurance Unlimited re-issues checklist	New	1995	1995
Buy More				Total Price	\$1,995.00	\$1,995.00

Purchasing multiple SSL certificates?
Save money. Increase efficiency. Rollover for more

Please Note: This site is currently designed to work with IE and Mozilla based browsers only.

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 EV Multi-domain 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**. By using the code you can be sure that you will not be 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 **EV Multi-domain** 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**.

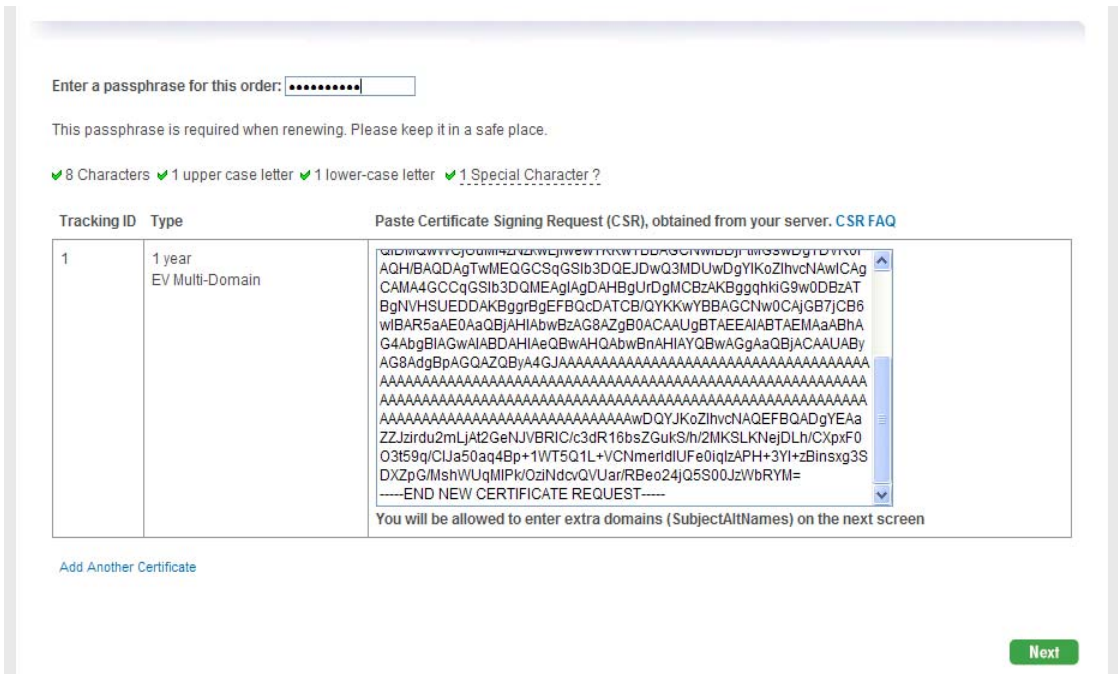
Step two: Provide certificate signing request (CSR) information

To create the certificate, 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.

Figure 4: Entering your certificate signing request (CSR)



- 5 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, do not fill in the information for those certificates and you will not be charged.
- 6 Click **Next**.

Figure 5: Enter additional domains



- 7 Click **Add a new domain** to enter any additional domains. These are added to the certificate as SubjectAltName (SAN) extensions. EV Multi-domain certificates are

allowed one additional free domain (SAN) for a total of two domains. You can purchase any number of additional domains.

- 8 Verify that the certificate information is correct.

If you need to change the information, click **Replace** or return to the previous page. You will have to generate a CSR with the correct information and use it in place of the incorrect request.

- 9 If the information on the page is correct, click **Next**.

Step three: Provide contact and business 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
- Contract Signer

This is the information that you acquired in [“Supplying contact information”](#) on page 5.

To provide contact information

- 1 Fill in the required contact information for one of the individuals filling a role.

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"/>

- 2 At the bottom of the page, select that person's role (for example, Technical Contact).

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

Authorization Contact	<input type="checkbox"/>
Technical Contact	<input checked="" type="checkbox"/>
Billing Contact	<input type="checkbox"/>
Contract Signer	<input type="checkbox"/>
<input type="button" value="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.

- 3 Click Add.

- Repeat these steps for each contact. The list of contacts at the top of the page updates to reflect the contact information. If you need to alter this information, click **Edit**. **Remove** deletes the information for that contact.

New Order | Renew

Contact Information

Authorization Contact:	Joyce Smith	[Edit] [Remove]
Technical Contact:	Alice Gray	[Edit] [Remove]
Billing Contact:	Required	
Contract Signer:	Optional	

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

Provide information about your company

Entrust requires information about your company in order to complete the verification process. This is the information you gathered in the section [“Supplying information about your company or organization”](#) on page 9.

To provide information about your company


- In the **Business Headquarters** pane, fill in the mailing address of the headquarters of your company. The company name is extracted from the DN in your certificate signing request. Optionally, fill in the DUNS number of your company.

Business Headquarters

Company	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"/>
Country	<input type="text" value="Canada"/> ▼		
DUNS Number	<input type="text"/>		

- 2 Optionally, supply the information requested in the **Jurisdiction of Incorporation** pane. If you do not know this information, leave these fields blank.

Jurisdiction of Incorporation

Registration Number	<input type="text" value="7-2345564"/>
Incorporating Agency	<input type="text" value="Commonwealth of Pennsylvania"/>
Date of Incorporation (mm/dd/yy)	<input type="text" value="11/20/2002"/> 
State/Province	<input type="text" value="PA"/>
Country	<input type="text" value="United States"/>

- 3 Optionally, supply the requested contact information for a individual who will act as a Higher Authority. If you cannot supply that information at this time, Entrust will contact your company for the information before the transaction is completed.

Higher Authority

First Name	<input type="text" value="Bob"/>
Last Name	<input type="text" value="Lee"/>
Title	<input type="text" value="Senior Manager Operations"/>
Phone Number	<input type="text" value="555-555-5555"/>
Email Address	<input type="text" value="bob.lee@example.com"/>

- 4 When you have finished, 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 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]
✚ Contract Signer:	Bob Lee	[Review]	[Edit]

The contact information appears below.

Technical Contact

Name:	Alice Gray
Title/Position:	IT Specialist
Company:	example.com
Address:	Anystreet
City:	Anytown
State:	PA
Zip/Postal Code:	12345
Country:	US
Phone:	555 555-5555
Email:	alice.gray@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.

Certificate	Type	CSR Content	
1	2 year(s) EV	www.example.com UserDN=cn=www.example.com, ou=Dev, o=example.com, l=AnyTown, st=Ohio, c=US Subject Alt Name:	[Replace]

- 3 Read the **Subscription Agreement(s)** section. If you agree, select your role from the drop down menu.

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 entered during enrollment is true and correct.

- 4 Click **Next** to proceed to the payment page.

Step five: Provide payment

Your payment options are:

- Pay for your Entrust EV Multi-domain SSL Certificates online with American Express®, Visa® or Master Card®. Your credit card is not debited until your

Entrust EV Multi-domain SSL Certificate has been issued. The Billing Contact will receive an electronic receipt at the end of the payment process.



Quantity	Item Description	Unit Price	Total
1	1 Year EV Multi-Domain Certificate	\$399.00	\$399.00
		Subtotal	\$399.00
		GST	\$19.95
		PST	\$31.92
		Total Amount	\$450.87

Entrust Limited, 1000 Innovation Drive Ottawa, Ontario, Canada K2K 3E7
 Phone: 1-877-368-7483 or 1-613-270-3769
 Fax: 1-877-839-3538 or 1-613-270-3260 [E-mail](#)

Payment Methods

Credit Card

Card Type:	<input type="text" value="Visa"/>
Card #:	<input type="text" value="1234567890"/>
Expiry:	<input type="text" value="3"/> <input type="text" value="2012"/> <small>Month Year</small>
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?

- If you supplied a promotional code or purchase order 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 14](#)) 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 EV Multi-domain 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 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 EV Multi-domain 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 EV Multi-domain SSL Certificate

If the information you provided in your application is correct and complete, the verification and certificate issuance process typically takes 5-10 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 EV Multi-domain SSL Certificates.

Consult the documentation that came with your Web server software for instructions on installing the Entrust EV Multi-domain 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

The validation process

This section of the guide contains a high level overview of the validation process used by Entrust to verify the information in your certificate enrollment request.

For more detailed information, see the http://www.cabforum.org/EV_Certificate_Guidelines.pdf

Anti-phishing high-risk check

Entrust determines if the company requesting the certificate is on the anti-phishing high risk list.

Business check

The business verification is necessary to confirm that the organization requesting the certificate has the right to use the business name submitted in the organization (o=) field in the certificate's DN.

This is verified using the following steps:

- 1** The Incorporating Agency or Registration Agency or Qualified Government Information Source in the Applicant's Jurisdiction of Incorporation information, is checked to obtain the following information:
 - legal business name
 - registration Number
 - status
 - incorporating Agency
 - date of incorporation
 - jurisdiction (city, state/province, country)
 - registrant agent (name and address)
- 2** Entrust determines the type of business as:
 - Private Organization

A non-governmental legal entity (whether ownership interests are privately held or publicly traded), whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation.
 - Government Entity

A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, or county).
 - Business Entity

Any entity that is neither a Private Organization nor a Government Entity. Examples include general partnerships, unincorporated associations and sole proprietorships. (These businesses require additional paperwork. See [“Principal Individual Face-to-Face Validation” on page 28](#))

3 The Qualified Independent Information Source is searched to obtain the following information:

- place of business address
- main switch board phone number (Applicant or a Parent/Subsidiary Company name)
- list of executives

If this information can not be found using the Qualified Independent Information Source (QIIS) then Entrust can accept a legal or accountant letter stating the place of business and main switch board phone number. The legal or accountant letter will be validated using a third party phone number.

For Government Entities, the Qualified Government Information Source can be used to locate the information.

Domain check

The domain check verifies that:

- The company is the registered owner of the domain name used in the certificate being requested.

Entrust uses the appropriate ICANN (Internet Corporation for Assigned Names and Number) approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA) database to verify this information.

- The registrant name on the registrant inquiry is the Applicant or a Parent/Subsidiary Company.

Authorization confirmation

The authorization confirmation checks are done for all of the contacts provided.

- Higher Authority

Entrust checks:

- that the individual is qualified for this role
- that the individual is employed by the company
- that the Higher Authority is willing to confirm that the Contract Signer and the Authorization Contact (Certificate Approver) are company employees who have the right to assume these roles

- Contract Signer

After the EV Multi-domain certificate enrollment agreement is accepted Entrust confirms that the name and job title provided for the Contract Signer is accurate and that the individual is aware of the transaction.

- **Authorization Contact**

After the Authorization Contact (Certificate Approver) accepts the online consent form, Entrust confirms that the individual:

- accepted the on-line consent
- is an employee of the company
- is authorized to request Entrust EV Multi-domain SSL Certificates on behalf of their company

- **Technical Contact (Certificate Requester)**

Entrust confirms that this individual submitted the request for the Entrust EV Multi-domain SSL Certificate on behalf of their company.

Principal Individual Face-to-Face Validation

Where a business is not an organization (for example, if the business is a sole proprietorship) a Principal Individual associated with the business must be validated by a Third Party Validator in a face-to-face setting.

Face-to-face validation

In the case of face-to-face validation, the business (for example, the sole proprietorship) arranges for a qualified Third Party such as a notary or lawyer to have a face-to-face meeting with a person filling the Individual Principle role. During the meeting, the Principle Individual presents the required documentation to the the third party.

The qualified Third Party Validator may be an employee of the Certification Authority, a latin notary, a notary (or equivalent in Applicant's jurisdiction), a lawyer, or accountant. The Principal Individual or Individuals must present the following documentation (Vetting Documents) directly to the Third-Party Validator:

A Personal Statement that includes the following information:

- full name or names by which a person is, or has been, known (including any and all other names used)
- residential address at which the Principle Individual can be located
- date of birth
- an affirmation that all of the information contained in the Certificate Request is true and correct

A current, signed, government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

- a passport
- a drivers license
- a personal identification card
- a concealed weapons permit
- a military identification

At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

- Acceptable financial institution documents include:
 - a major credit card, provided that it contains an expiration date and has not expired
 - a debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired
 - a mortgage statement from a recognizable lender that is less than six months old
 - a bank statement from a regulated financial institution that is less than six months old

Acceptable non-financial documents include:

- recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill)
- a copy of a statement for a payment of a lease provided the statement is dated within the past six months
- a certified copy of a birth certificate
- a local authority tax bill for the current year
- a certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers

The Third-Party Validator performing the face-to-face validation:

- attests to the signing of the Personal Statement and the identity of the signer
- identifies the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator attests that a copy of the current signed government-issued photo identification document is a full, true, and accurate reproduction of the original.

Entrust does the following:

- Cross-checking of Information

Entrust obtains the original signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. Entrust reviews the documentation to determine if

the information is consistent, matches the information in the application and identifies the Individual.

- Verification of Third-party validator

Entrust independently verifies that the Third-Party Validator is a legally-qualified latin notary or notary (or legal equivalent in applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Principal Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.