Entrust Cloud

EV Multi-Domain Certificate Enrollment Guide

Date of Issue: March 2016
Document issue: 1.0

Entrust Datacard™

Obtaining technical support

For support assistance by you can email Customer Support at support@entrust.com or visit our Web site at www.entrust.com.

Entrust Datacard

Enrolling for your certificate

Entrust EV (extended validation) Multi-Domain SSL certificates provide all the benefits of an Advantage SSL Certificate but conform to 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 a padlock at the top. Mousing over the padlock displays the issuer and organization name, and country in most browsers.

Before starting the online certificate enrollment process, 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

Gather the following information before you begin.

Topics covered in these sections are:

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. Create each CSR using the software 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/ssl-technical/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.

Tools for creating a command-line request in OpenSSL or KeyTool are available on the Entrust Website. OpenSSL users, click here. For KeyTool users, click this link.

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 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—the full name of the state or province.	
Locality	This is usually the name of the city where your organization's office is legally registered.	

Entrust Datacard™

Table 1: CSR information table

Requested	Description	Information
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.example.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.

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.

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 term used by the CA/Browser Forum 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 name	
Street address	
City	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
Phone	
Email	

Entrust Datacard

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 operation of the Web server on which the Entrust EV Multi-Domain Certificate will be installed. If your Web 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	
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 name	
Street address	
City	

Table 4: Billing contact information

Information required	Contact information
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 name	
Street address	
City	
State/Province (optional if outside North America)	
ZIP/Postal Code	
Country	
Phone	
Email	

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

Entrust Datacard

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 6: Higher authority information

Information required	Contact information
Name	
Title/Position	
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 company name is extracted 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 7: Jurisdiction of incorporation (optional)

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

Table 7: Jurisdiction of incorporation (optional)

Information required	Contact information
Country	

Business headquarters

Entrust requires the address of your business headquarters.

Table 8: Business headquarters

Information required	Contact information
Address	
City/Town	
State/Province	
ZIP/Postal Code	
Country	

Entrust Datacard

Why orders may be delayed or rejected

To be sure that your order is processed as quickly as possible, check your order for these problems:

- The Entity is not the registered owner of the domain.
- The Entity name provided is not the 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.
- Higher Authority contact information is not provided.
- Please ensure the following contacts are aware that verbal confirmation will be required to complete the EV order: Higher Authority, Contract Signer, Authorizing Contact (also referred to as Certificate Approver), and Certificate Requester. Entrust will contact these individuals by telephone via a number provided by a qualified third-party source.

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

To begin ordering certificates, browse to the Entrust **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 an Entrust Cloud Enterprise certificate management service customer (or prospective customer) or placing a certificate order without this service, and the 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 smaller than $1000.00, you must use a credit card.

To start your order

1 To begin ordering certificates, browse to https://buy.entrust.net/ and select the type of certificate to buy. The Entrust **Quote Order** page opens with the default values for the certificate type displayed.

Entrust Datacard

Figure 1: Entrust 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**.

   • If you use a purchase code, your purchase is limited to the certificates in the order you placed through our sales representative. You will not be asked for a credit card at the end of the process.

   • If you received a promotional code from Entrust, the percentage of the cost indicated in the promotion is deducted from your purchase at the end of the buying process (for example, if the promotion is for a free EV Multi-Domain certificate the certificate will cost you nothing). You cannot add additional certificates to the order.

4 Under **Type** (C), select **EV Multi-Domain** from the drop-down list.

5 Under **Lifetime** select the number of years from the drop-down list (lifespan of the certificate).

6 Under **Quantity**, type the number of certificates to purchase.

   The prices are automatically calculated for you.

7 Click **Buy Now**.

> **Note:**
>
> If you are using a purchase code but you want to buy additional certificates (that are not included in the original purchase), you must do so in a separate transaction.

Step two: Provide certificate signing request (CSR), additional protected domains, and malware scan 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 Check that you are ordering the type of certificate that you want. Check the certificate lifespan. You can change these on this page. If you are buying several different certificates, indicate the type and lifespan for each.

2 Select the Signing Algorithm. SHA-2 is the preferred choice. Select the ? icon for for more 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: Example CSR file

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDRzCCArACAQAwbDELMAkGA1UEBhMCVVMxDTALBgNVBAgTBE9oaW8xEDAOBgNV
BAcTB0FueVRvd24xFDASBgNVBAoTC2V4YW1wbGUuY29tMQwwCgYDVQQLEwNEZXYx
GDAWBgNVBAMTD3d3dy5leGFtcGxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAxImEXhW4x+qFiSr74SpismDNCGEnSm8suGFa4m9hKy/CFkYswDnVvxNS
0gCClbPidyjorLR2bMv58q6byH4trhFCoI+M8NYbFai8W7i48EAZnQ4BFNGHY7q2
0CW0QXzeL9SYSKXOmKcL4xgedM6kkMcAzCUJ55fHPt81Ss6ap0UCAwEAAaCCAZkw
GgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4G
A1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAO
BggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYI
KwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAwlf0pAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAE4Ttldb
ikK4Kpgyvv7IM8tU+EkHVoMPO2QzMJ4OH3HAHEIa+4IuE1mgTGFpn16dptZL1vhO
Ismy93+gWiycLHIYtru6uV/0vf1sRyQ0kLX7/akEs/MGtOKSFgMO0XYWtsIeVVn3
QN35X1wmvQDnt7GyegLXyuH3rDcvkA6WFVaj
-----END NEW CERTIFICATE REQUEST-----
```

4 Copy the CSR text and paste it 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 12. Do not include any blank spaces before or after the CSR. Include the -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- lines.

Figure 3: Entering your certificate signing request (CSR)

5   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, do not fill in the information for those certificates, and you will not be charged.

6   Click **Next**.

Figure 4: Enter additional domains

7   Click **Add a new domain** to enter any additional domains. This is optional. Enter the domain and click **Done**.

These domains are added to the certificate as SubjectAltName (SAN) extensions. EV Multi-Domain certificates allow one additional free domain (SAN) for a total of two domains. For an additional per-domain fee, you can add any number of additional

Entrust Datacard

domains and they will be automatically added to the cost of the certificate. This is calculated using to the number domains and the lifespan of the certificate.

If you received a promotional code from Entrust, the percentage of the cost indicated in the promotion is deducted from the cost of the SAN at the end of the buying process You cannot add additional SANs to the order if you use a promotional code.

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**.

Select your SiteLock Malware scan

Entrust includes free SiteLock malware protection for one of the sites specified in your certificate. Use the pull-down menu to select the site where the scan will run. If you do not want to use the malware scan, select **Disable Security Bundle**. For more information about the bundled SiteLock malware protection click here.

Step three: Provide contact and business information

Enter the names and contact information of individuals in your organization who will assume the roles of:

•   authorization contact

•   technical contact

•   billing contact

•   contract signer (optional)

This is the information that you acquired in "Supplying contact information" on page 5. If you do not supply a contract signer the authorization contact is used for this role.

To provide contact information

1 At the bottom of the **Provide Contact Information** pane, select the role of a contact (for example, authorization contact).

Provide Contact Information

All fields are mandatory.

First Name	Alice
Last Name	Gray
Title/Position	Support Specialist
Email Address	ice.gray@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
☐ Contract Signer (optional)

Add

2 Enter the required contact information for the 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 you provided. If you need to alter this information, click **edit** beside a name. Click **remove** to delete a contact.

Contact Information

⊞ Billing Contact	Required	
⊞ Authorization Contact	Required	
⊞ Technical Contact alice gray	Required	[edit] [remove]
⊞ Contract Signer	Optional	

4 Repeat these steps for each required contact, until all of the required roles are filled.

5 Identify your role and indicate if you want to receive additional information about Entrust or SiteLock products.

I am the: Technical Contact ▾ listed above.

If you would like to learn more about other products and services from Entrust and our partners that can benefit you, please provide your consent below.

☑ I CONSENT, for Entrust to use the above contact information to contact me about Entrust products and services that Entrust believes may be of interest to me.

☐ I CONSENT, for Entrust to provide the above contact information to Entrust's partner, SiteLock, for the purpose of SiteLock contacting me about SiteLock products and services that SiteLock believes may be of interest to me.

Entrust Datacard Corporation and its affiliates assumes no responsibility for what SiteLock does with your information. Entrust Datacard Corporation and its affiliates do not assume any obligations or liability for and do not make any representations, warranties or conditions of any kind in relation to the SiteLock products and/or services.

[Previous] [Next]

Cancel Order

6 When you have finished, click **Next**.

Provide company and Higher Authority information

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

1 In the **Business Headquarters** pane, enter the mailing address of the headquarters of your company. The company name and much of the information is carried forward from the previous page.

Business Headquarters

Company	Org1 LTD
Address	123 Anystreet
City/Town	Anytown
Country	Canada
State/Province	Ontario
Zip/Postal Code	K2B E7N

Jurisdiction of Incorporation

Registration Number:	1234567
Incorporating Agency:	Province of Ontario
Date of Incorporation:	2004-03-11
Country	Canada
State/Province	Ontario

Higher Authority

First Name	Felicity
Last Name	Johnson
Title/Position	Chief of Technical Oper
Email Address	felicity.johnson@examp
Phone Number	555 555-1212

Previous   Next

Cancel Order

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

3   Optionally, supply contact information for an 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. Your company must identify a Higher Authority contact before the certificate can be issued.

Entrust Datacard

4   Read the agreement information and select your role.

Subscription Agreement(s)

Entrust Certificate Services Subscription Agreement

Attention - read carefully: this Entrust Certificate Services Subscription Agreement ("Agreement") is a legal contract between You (as defined below) and Entrust (as defined below). 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:

Please indicate which role you are: select one...   ▼
By proceeding to the next step; I have   select one...   cept the Subscription Agreement.
                                           Authorization Contact
                                           Billing Contact
                                           Technical Contact

Previous   Next

Cancel Order

5   When you finish, click **Next**.

Step four: Select your account owner and verify and authorize your order

Entrust provides an Entrust Cloud account free-of-charge to help you manage your certificates. You can access this account using the email address that you provide (your user name) and a password as your first factor authentication and your choice of second factor authentication. A link to your account and a temporary password will be sent to you by email. When you log in to your account you must change the password before you can continue.

While you can add orders to an existing account and place orders using your account, you cannot have more that one Entrust Cloud account with the same user name.

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

To select your account owner, and verify and authorize your order

1   Select an owner for the Entrust Cloud account from the pull-down menu. This should be the person who will manage the certificates in the order (reissue certificates if required, renew certificates, or place future orders, for example).

2   If you supply a cell phone number for second factor authentication Entrust will send your second factor authorization to that number when you log in. If you leave this

blank, you can configure an alternate form of second factor authentication when you log in to your account.

Select Owner for your Account

Select a contact to be the owner of the account for this order. If the account does not already exist, it will be created automatically and login details will be sent by email to this contact.

Account owner:	Technical Contact - alice gray (agray@example.com)
Mobile number for multifactor authentication (optional):	5553214567 ?
Confirm Mobile:	5553214567

○ This is a North American number starting with the area code.
○ This is an international number starting with the country code.

3   Optionally, click **Review** beside each contact listing, to display their contact information.

Quote Order   Provide CSR   Provide Contact   Verify/Edit   Provide Payment   Process Order

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 Bob Lee	Required	[review]	[edit]	
⊞ Technical Contact Alice Gray	Required	[review]	[edit]	
⊞ Higher Authority Felicity Johnson	Optional	[review]	[edit]	[remove]
⊞ Contract Signer Bob Lee	Required	[review]	[edit]	

* Please note if you have not provided a Contract Signer for your EV Certificate order, the Authorization Contact information will be entered by default. The Subscription Agreement will then be sent to the Authorization Contact for approval. If you wish to enter a Contract Signer for your EV Certificate order, please Edit the information before you submit your order to Entrust.

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

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

◎ **Entrust Datacard**

5 Review the other information for errors.

Jurisdiction of Incorporation

Registration Number:	TS-142356745
Incorporating Agency:	Province of Ontario
Date of Incorporation:	19990106
State/Province	ON
Country	CA

Business Headquarters

Company	example.com
Address	123 Anystreet
City/Town	Anytown
State/Province	ON
Zip/Postal Code	K5B 6F1
Country	CA

Higher Authority

First Name	Frank
Last Name	Jones
Title/Position	Vice President
Email Address	frank.jones@example.com
Phone Number	555 555-5555

6 Read the **Subscription Agreement(s)** section.

7 Select your role from the drop-down list under the agreement text.

Subscription Agreement(s)

Entrust Certificate Services Subscription Agreement

Attention - read carefully: this Entrust Certificate Services Subscription Agreement ("Agreement") is a legal contract between You (as defined below) and Entrust (as defined below). 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:

Please indicate which role you are: select one...
By proceeding to the next step; I have [ ] ccept the Subscription Agreement.

select one...
Authorization Contact
Billing Contact
Technical Contact

Previous   Next

Cancel Order

⚠️ **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.

8   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 is issued. The billing contact will receive an electronic receipt at the end of the payment process.

Quote Order .... Provide CSR .... Provide Contact .... Verify/Edit .... **Provide Payment** .... Process Order

Quantity	Type	Unit Price	Total
1	1 Year EV Multi-Domain	$429.00	$429.00
		Subtotal	$429.00
		GST	$21.45
		PST	$34.32
		Total Price	$484.77

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 Email

Payment Method

Card Type:	Select a credit card ▼
Card #:	
Expiry:	3 ▼ 2013 ▼
Does the Billing Address of this card match the Billing Contact for the order?	○ Yes ○ No

How Did You Hear About Us? [Please Select] ▼

Previous   Process Order
Cancel Order

* 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 and are not prompted to supply further payment information.

- 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 EV Multi-Domain certificate order to Entrust.

Step six: Record your order number and register your account

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

You can also 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 certificate. The validation process checks that:

- your company or organization (authorizing organization) has the legal right to conduct business under the 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 is received, Entrust contacts the authorization contact specified in your order by email. The message contains a link where the contact can consent to the order. That step is required to further process the order.

If you specified a higher authority, that person also receives an email message asking them to confirm that the authorization contact and the contract signer are authorized for those roles.

Once the validation process is complete, Entrust sends a URL to your technical contact by email, leading to a Web site where you can retrieve your Entrust EV Multi-Domain SSL Certificates.

Consult the documentation that came with your Web server software for instructions about 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/knowledge-base/index.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

Business verification is necessary to confirm that the organization requesting the certificate is a legal and active entity, and 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 is checked for the following information:

   • Legal business name
   • Registration number
   • Status
   • Incorporating agency
   • Date of incorporation
   • Jurisdiction (city, state/province, country)
   • Registered 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.

3 The qualified independent information sources (QIIS) are searched to obtain the following information:

- Place-of-business address
- Main switchboard phone number (applicant or a parent/subsidiary company name)

- Lists of executives

If this information cannot 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 is 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 Entity is the registered owner of the domain name used in the certificate being requested.

  Entrust uses the appropriate Internet Corporation for Assigned Names and Number (ICANN) 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

Entrust confirms the following for each contact:

- Higher Authority
  – is at a Director-level or above, or is in direct line-of-management of the Contract Signer and/or the Certificate Approver/Authorizing Contact.
  – is employed by the company
  – is willing to confirm that the Contract Signer and the Certificate Approver are company employees who have the right to assume their EV roles
- Contract Signer
  – accepts and verbally confirms they accepted the service agreement
- Certificate Approver / Authorizing Contact
  – accepts and verbally confirms their acceptance of the online consent form

       – verbally confirms the Technical Contact is authorized to receive the certificate

- Certificate Requester
  – verbally confirms they have requested the certificate to have Extended Validation

Entrust Datacard