Entrust Certificate Services

EV Multi-Domain 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.

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 (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" on page 4
- "Usual reasons that orders are delayed or rejected" on page 11
- "Ordering certificates" on page 12
- "The validation process" on page 24

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. 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/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:

When you create a CSR, a cryptographic key pair is generated. The private key remains on your computer. Back up the 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 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.	

Table 1: CSR information table

Requested	Description	Information
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.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.

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 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	

Table 2: Authorization contact information

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

Table 5: Contract signer information

Information required	Contact information
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 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)	
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	

Usual reasons that orders are delayed or rejected

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

- The authorizing organization is not the registered owner of the domain.
- The authorizing organization did 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 not 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 online 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 12
- "Step two: Provide certificate signing request (CSR) information" on page 13
- "Step three: Provide contact and business information" on page 16
- "Step four: Verify and authorize your order" on page 19
- "Step five: Provide payment " on page 22
- "Step six: Record your order number and register your account" on page 23
- "Receiving your certificate" on page 23

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 an Entrust Certificate Management Service (CMS) customer (or prospective customer) or placing a certificate order without CMS, and the method of payment you are using.

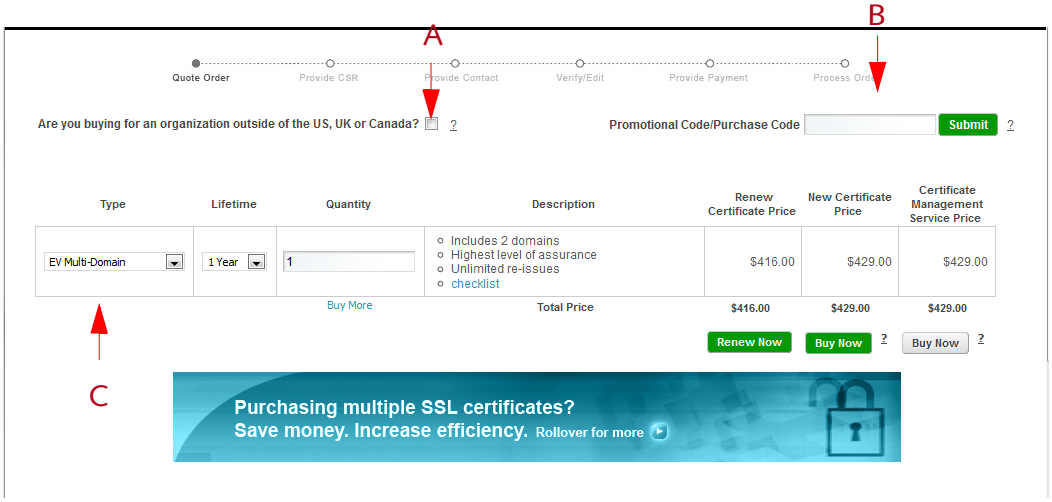
Note:

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 Certificate Services (ECS) **Quote Order** page opens with the default values for the certificate type displayed.

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 **EV Multi-Domain** from the drop-down list.
5. Under **Lifetime** select the number of years from the drop-down list.
6. Under **Quantity**, type the number of certificates to purchase.

   The prices are automatically calculated for you.
7. Click **Buy Now**.

Note:

People using a purchase code who want to buy additional certificates that are not included in the original purchase (and purchase code), can only do so after completing this transaction.

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. In **Enter a passphrase for this order**, type a passphrase for your order. 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: Example CSR file

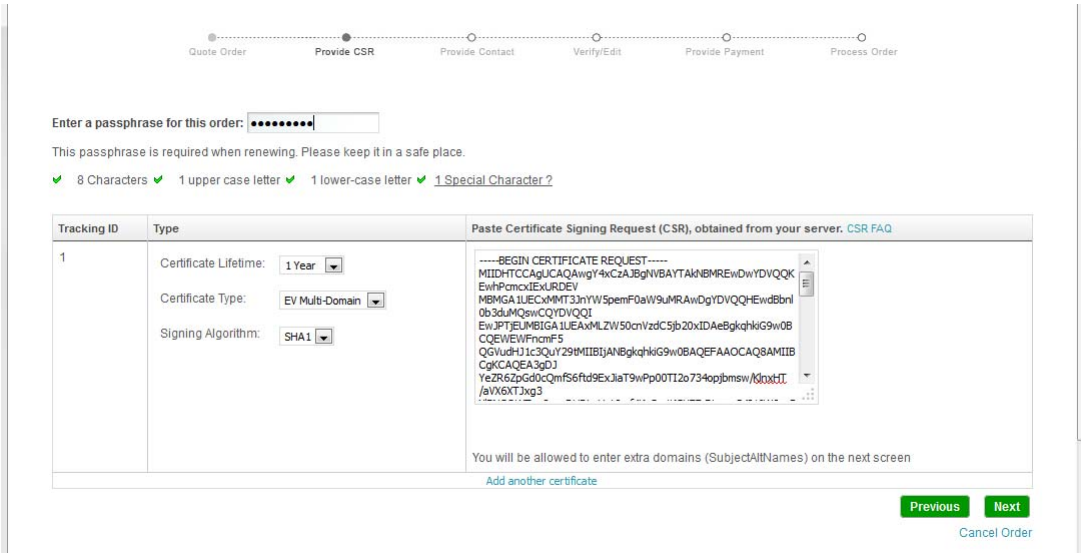

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDRzCCArACAQAwbDELMAkGA1UEBhMCVVMxDTALBgNVBAgTBE9oaW8xEDAOBgNV
BAcTB0FueVRvd24xFDASBgNVBAoTC2V4YW1wbGUuY29tMQwwCgYDVQQLEwNEZXYx
GDAWBgNVBAMTD3d3dy5leGFtcGxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAxImEXhW4x+qFiSr74SpismDNCGEnSm8suGFa4m9hKy/CFkYswDnVvxNS
0gCClbPidyjorLR2bMv58q6byH4trhFCoI+M8NYbFai8W7i48EAZnQ4BFNGHY7q2
0CW0QXzeL9SYSKXOmKcL4xgedM6kkMcAzCUJ55fHPt81Ss6ap0UCAwEAAaCCAZkw
GgYKKwYBBAGCNw0CAzEMFgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4G
A1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAO
BggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYI
KwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBv
AGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwBy
AGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAwlf0pAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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 the `-----BEGIN NEW CERTIFICATE REQUEST-----` and `-----END NEW CERTIFICATE REQUEST-----` lines.

3 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.

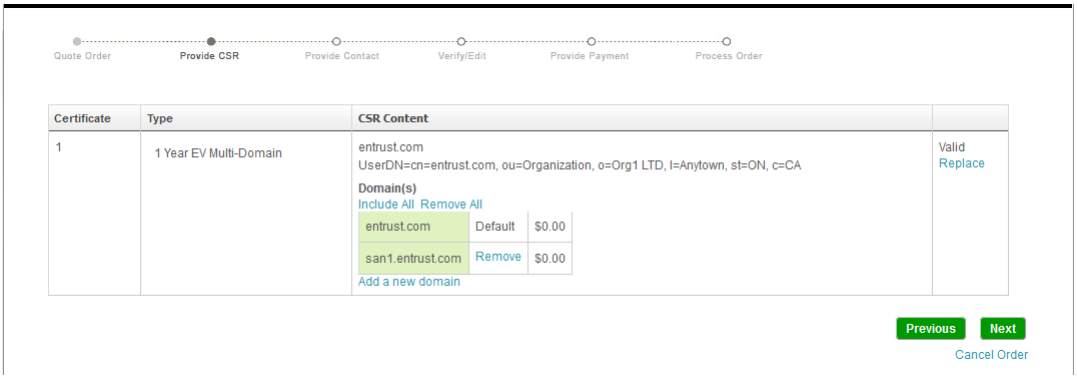
Figure 3: Entering your certificate signing request (CSR)



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

5 Click **Next**.

Figure 4: Enter additional domains



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

These 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 domains and they will be automatically added to the cost of the certificate.

7 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.

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

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 page, 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 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. Click **remove** to delete a contact.

Contact Information

Billing Contact Rosemary Zita	Required	[edit] [remove]
Authorization Contact Bob Lee	Required	[edit] [remove]
Technical Contact Alice Gray	Required	[edit] [remove]
Contract Signer	Optional	

4 Repeat these steps for each required contact, until all non-optional role check boxes disappear from the bottom of the page.

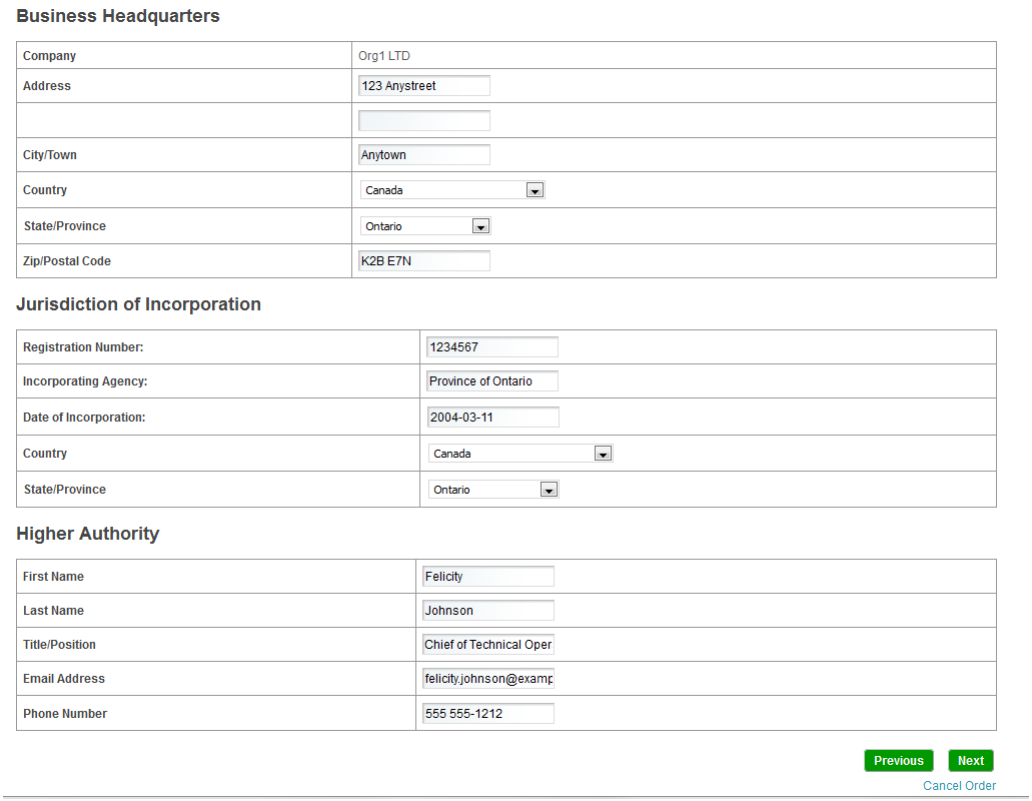
5 When you have finished entering contacts, click **Next**.

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

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.

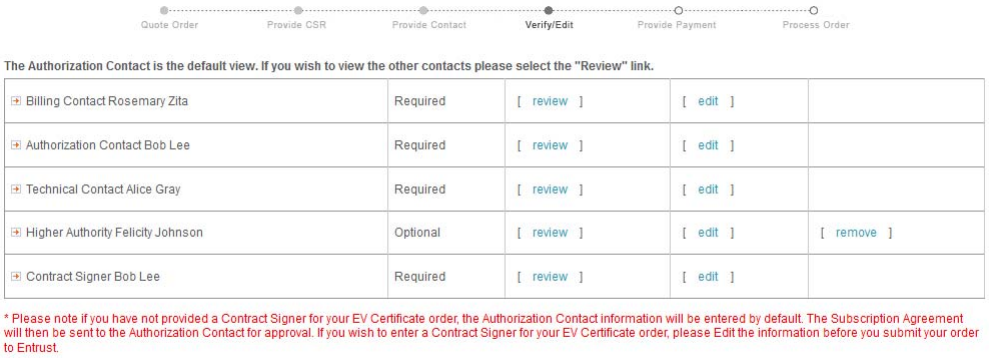
4 When you finish, click **Next**.

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 allows you to verify that the information you have entered is correct, before you proceed to the next step.

To verify and authorize your order

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



The contact information appears below.

Authorization Contact

First Name	Bob
Last Name	Lee
Title/Position	Director of Operations
Company Name	example.com
Email Address	bob.lee@example.com
Phone Number	555 555-5555
Address	123 Anystreet
City/Town	Anytown
Country	Canada
State/Province	Ontario
Zip/Postal Code	K5B 6F1

Certificate	Type	CSR Content	
1	1 Year EV Multi-Domain	doc2k3gs.gsdoc1.entrust.com UserDN=cn=doc2k3gs.gsdoc1.entrust.com,ou=example.com,o=example.com,l=Anytown,st=Ontario,c=CA **Domain(s)** doc2k3gs.gsdoc1.entrust.com	[Replace]

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

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

3 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

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

5 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 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.

Please indicate which role you are: select one...

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

Previous Next

> Blog > Twitter > Site Map > Misuse Form > CPS > Privacy Policy

Copyright 2011 Entrust ®. All rights reserved.

Entrust - One Lincoln Centre - 5400 LBJ Freeway, Suite 1340 - Dallas Texas USA 75240

Attention:

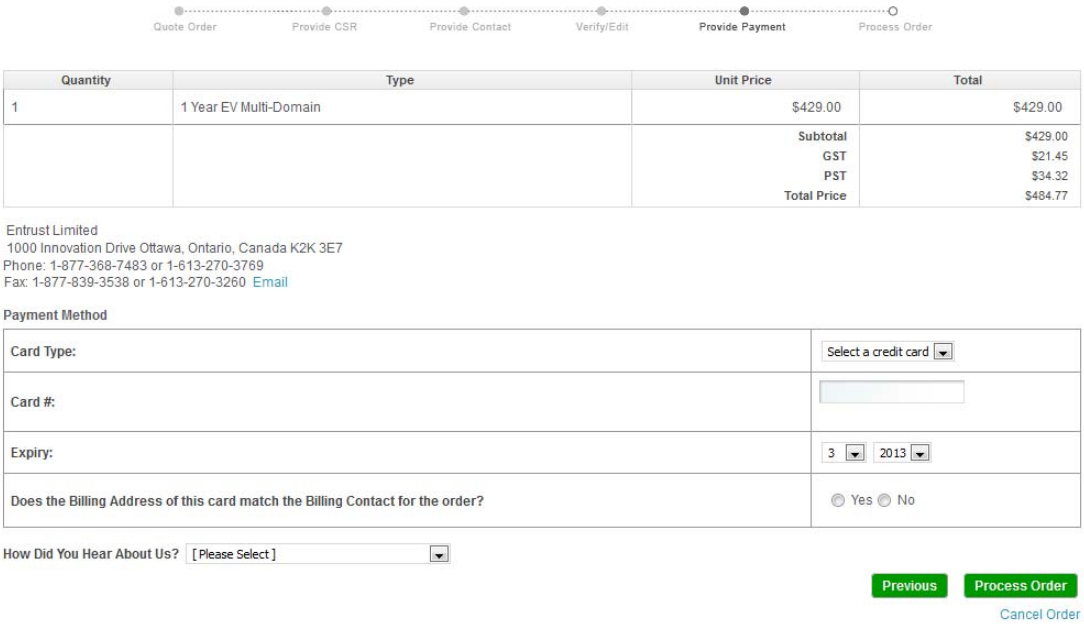
By proceeding to the next step, you declare that you are authorized to request certificates on behalf of your company and that all of the information entered during enrollment is true and correct.

6 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.



- 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 Certificate Services 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

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 is checked for 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 26)

3 The qualified independent information source is searched to obtain the following information:

- place of business address
- main switchboard phone number (applicant or a parent/subsidiary company name)
- list 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 company 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

The authorization confirmation checks are done for all 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.