Entrust.Net

Technical Information – Enrollment Guide - Web

Client Confidential

TABLE OF CONTENTS

This Enrollment Guide explains the steps you must follow to request an Entrust.net Web server certificate for your Web server. To simplify the certificate request process, we suggest that you print this guide and gather the necessary information before you complete the online certificate request form.

STEP 1: CONFIRM PROOF OF RIGHT

Because your organization's name may appear in the certificate you receive, Entrust must be sure that you have the right to use that name before issuing the certificate. This measure is designed to prevent the unauthorized use of your organization's name in a Web server.
You must submit Proof of Right by faxing suitable documentation to Entrust. The table below lists documents which can be submitted.
Note: without this Proof of Right information, Entrust cannot process your certificate request.

If your organization is:	**Submit:**
A company, corporation, partnership, or proprietorship	The company registration document, or a copy of your article of incorporation or partnership stamped by the relevant authority.
A government department or agency	An original letter signed by the department head on appropriate letterhead. The letter must include contact information for the department and for the signer's immediate superior.
A non-government organization (NGO)	An original letter signed by the Chief Executive, Chairman, or Managing Director of the NGO on appropriate letterhead.
A university	An original letter signed by the Dean or Vice-Chancellor of the requesting department on appropriate letterhead. The letter must include contact information for the University.
A Doing Business As (DBA) organization	A copy of the DBA registration papers for local levies and taxes or official correspondence indicating your right to use the name given.
A type of organization not listed here (such as the IETF)	Please contact Entrust to determine suitable documentation.

STEP 2: CSR AND DOMAIN INFORMATION

In this step, you supply information about your domain and your Certificate Signing Request (CSR), you choose the lifetime for your certificate and a passphrase, and specify the Web server software you are using.

SUPPLYING DOMAIN INFORMATION

The certificate you receive from Entrust includes the common name of your Web server (for example, www.entrust.com). This common name contains the domain name of your organization. Entrust can only issue the certificate to you if your organization is the registered owner of the domain name that appears in the Web server's common name. For example, to receive a certificate for a server named www.entrust.com your organization must be the registered owner of the domain name entrust.com.

To determine the registered owner of your domain name, look up the domain name in the appropriate WHOIS database. WHOIS databases are maintained by a group of organizations called Network Information Centers (or NICs). Each NIC is responsible for a different top-level domain or group of domains. For instance, Network Solutions (http://www.networksolutions.com/cgi-bin/whois/whois) keeps a record of the registered owners in the .com, .edu, .org, and .net domains. The table below lists Web sites for the most frequently accessed NICs. If your top-level domain is not listed, see http://www.uninett.no/navn/domreg.html.

If your domain ends with:	**See the Web site:**
.com, .edu., .org, or .net	Network Solutions
.mil	U.S. Military
.au	Australia
.ca	Canada
.fr	France
.de	Germany
.it	Italy
.jp	Japan
.mx	Mexico
.uk	United Kingdom

Please record your domain name and the name and address of the registered owner of your domain name. If you are requesting multiple certificates, record the information for each certificate. You will be asked to enter the domain information for each additional certificate in Step 5 of the online request form.

Domain name:

Name of owner:

Company Name:

Address:

GENERATING AND SUBMITTING A CSR

The Certificate Signing Request (CSR) contains your server's public key along with other information such as your server's Distinguished Name (DN). You generate the CSR using your Web server software and submit it to Entrust in the online request form. When your request is approved, the data in the request is packaged into a certificate and signed by the Entrust Certification Authority (CA).

Follow the instructions in your Web server's documentation to generate a CSR. When you go through the online request form, paste the CSR into the space provided. If your Web server is hosted by an Internet Service Provider (ISP), the ISP will be able to provide you with a CSR. For your convenience, we have provided instructions in the online request form for generating certificates using several popular Web servers. If you are ordering multiple certificates, generate a different CSR for each one. To submit each CSR simply click the "Another request" button in the online request form and paste the CSRs into the spaces provided.

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 securely back up the private key. If the private key is lost or becomes corrupt you will not be able to use your certificate.
Important: The private key is a very sensitive piece of information. Someone with access to your private key could decrypt the SSL-protected data sent and received by your Web server. Please take appropriate steps to ensure that no unauthorized people have access to the private key.

TIPS FOR CREATING THE CSR

When you create your CSR you are asked to enter information about your organization and your Web server. This information is used to create your Web server's Distinguished Name (DN). Please keep the following points in mind when you enter this information:

Country code: This is the two-letter ISO abbreviation for your country (for example, US for the United States).
State or Province: This is the name of the state or province where your organization's head office is located. 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 head office is located.
Organization: This is the name under which your organization is registered. This organization must own the domain name that will appear in the common name of your Web server. Do not abbreviate your organization's name and do not use any of the following characters: ~ ! @ # $ % ^ * / \ ( ) ?.
Organizational unit: This is normally the name of the department or group that will use the certificate.
Common name: This is the name of your Web server as it will appear in the server's URL (for example, www.entrust.com). This name must be identical to the fully qualified domain name of the Web server for which you are requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse to establish a secure connection with your site. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.

PASTING THE CSR INTO THE FORM

To submit the CSR, simply paste it into the field provided in the online request form. Remember to include the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----" lines. The CSR will look similar to this:

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBnDCCAQUACQAwXjELMAkGA1UEBhMCQ0ExEDOABgNVBAgT
B09udGFayW8xEDAOBgNVBAcTB01vbnRyYWwxDDAKBgNV
BAoTA0tGQzEdMBsGA1UEAxMUd3d3Lmlsb3ZlY2hpY2tlbi5j
b20wgZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBALmJA2FL
SGJ9iCF8uwfPW2AKkyyKo/e9aHnnwLLw8WWjhl[ww9pLietw
X3bp6Do8/7mwV3jrgQ1OIwarj9iKMLT6cSdeZ0OTNn7vvJaN
v1iCBWGNypQv3kVMMzzjEtOl2uGl8VOyeE7jImYj4HlMa+R1
68AmXT82ubDR2ivqQwl7AgEDoAAwDQYJKoZIhvcNAQEEBQAD
gYEAn8BTcPg4Owo/hGIMU2m39FVvh0M86/ZBkANQCEHxMz/z
rnydXnvRMKPSE208x3Bgh5cGBC47YghGZzdvxYJAT1vbkfCS
BVR9GBxef6/ytkuJ9YnK84Q8x+pS2bEBDnw0D2MwdOSF1sBb
1bcFfkmbpjN2N+hqrrvA0mcNpAgk8nU=
-----END NEW CERTIFICATE REQUEST-----

Entrust supports the following Web servers. You will find instructions on how to generate CSRs in the documentation that came with your Web server.

Important: When you generate the CSR you are asked to enter the name of your organization. Please enter the name exactly as it appears in your Proof of Right (you confirmed Proof of Right in Step 1). Processing may be delayed if the name in your CSR is not identical to the name in your Proof of Right.

CHOOSING A ONE- OR TWO-YEAR CERTIFICATE

Entrust offers certificates with one- or two-year lifetimes. Both certificate lifetimes provide excellent security. However, many customers choose two-year certificates to reduce the overhead associated with managing certificates for their Web servers.

Please record the lifetime you would like for your Entrust.net Web server certificate.

Certificate lifetime:

CHOOSING A PASSPHRASE

Choose a passphrase and record it in the space provided. You will need this passphrase if you ever want to revoke your certificate. You may also be asked for it if you contact Entrust support. For security reasons, please ensure that this passphrase contains: at least 8 characters, at least one lower-case and one upper-case character, and at least one non-alphanumeric character (such as "%" or "!"). Good passphrases are easy to remember but hard to guess. Important: If you write the passphrase down, please store it in a secure location.

Passphrase:

ENTERING YOUR WEB SERVER TYPE

Please record the type of Web server, i.e. the Web server software, for which you are requesting a certificate. You will be asked to select it from a list box in the online request form.

Web server:

ORDERING MULTIPLE CERTIFICATES

The online request form makes it easy to request multiple certificates. For each additional certificate you wish to request simply click "Another certificate" in the online request form and enter the domain information, CSR, passphrase, and Web server type in the spaces provided.

STEP 3: CHOOSE CONTACT PEOPLE

In the online certificate request form you are asked to identify four points of contact within your organization.

An **authorization** contact who must be a senior member of your organization and have the authority to request a certificate on behalf of your organization. This person receives a copy of the certificate when it is issued and is contacted if further information is required to process your request.

A **technical** contact who will receive the certificate when it is issued, and who 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 certificate will be installed. If your server is hosted by a third-party or ISP, someone within that organization should be listed as the technical contact.

A **security** contact who is familiar with security issues and to whom we can send security-related information such as general security news and Web security alerts. This individual may be the same person as the authorization contact or the technical contact.

A **billing** contact

AUTHORIZATION CONTACT

Please record the name, telephone number, official title, and email address of the authorization contact.

Name of authorization contact:

Company Name:

Phone number:

Title:

E-mail address:

TECHNICAL CONTACT

Please record the name, telephone number, official title, and email address of the technical contact.

Name of technical contact:

Company Name:

Phone number:

Title:

E-mail address:

SECURITY CONTACT

Please record the name, telephone number, official title, and email address of the security contact. The security contact and the technical contact are often the same person.

Name of security contact:

Company Name:

Phone number:

Title:

E-mail address:

BILLING CONTACT

Please record the name, company name, address, phone number and email address of the billing contact.

Name of billing contact:

Address:

City or Town:

State of Province:

Zip of Postal Code:

Country:

Phone Number:

E-mail address:

STEP 4: CONFIRMATION

The confirmation page contains the information you entered in each step of the online request process. This page gives you the opportunity to verify that the information you have entered is correct before proceeding to the next step. You can make corrections to the information by clicking the appropriate Edit button.

The following general information is displayed on the confirmation page:

- Industry type
- Authorization contact
- Technical contact
- Security contact
- Billing contact

In addition, the following information is displayed for each certificate you requested:

- Domain name
- Distinguished Name
- Certificate lifetime
- Web server type

STEP 5: SUBSCRIPTION AGREEMENT

In this step you are asked to read the Subscription Agreement which governs the use of Entrust.net Web server certificates. You must accept the terms and conditions to proceed to the next step.

STEP 6: SUPPLY PAYMENT INFORMATION AND CONFIRM YOUR REQUEST

You can pay for your certificate online with American Express®, Visa®, and Master Card®. Your credit card is not debited until your certificate has been issued. You receive an online receipt at the end of the payment process.

When you complete your order you will be issued an order number. Please record this number. You can use it to track the status of your request online at www.entrust.net.

ONCE YOU HAVE COMPLETED THE ENROLLMENT

The technical contact and the authorization contact will be notified by email when your certificate request has been processed. If your request was successful the email will contain a URL that you can use to retrieve your Entrust.net Web server certificate. To begin using your certificate, install it on your Web server and ensure that SSL is enabled. Consult the documentation that came with your Web server software for instructions on how to install the certificate and enable SSL.