Entrust Managed Services PKI™

Certificates for computers, Web servers, and Web browser users

Document issue: 3.0
Date of issue: June 2009
Copyright © 2009 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:
• 1-877-754-7878 in North America
• 1-613-270-3700 outside North America

You can also email Customer Support at: support@entrust.com
Overview ................................................................. 5
  How does it work? .................................................. 6
  Using certificates with computers, Web servers, and Web browser users ... 7
    Digital certificates for computers .................................. 7
    Digital certificates for Web servers .................................. 7
    Digital certificates for Web browser users .......................... 7
  Overview of creating certificates for computers, Web servers, and browser users .................................................. 8
    The role of Administration Services ................................. 8
  Supported browsers and JRE ........................................... 10
    Supported browsers for Enrollment Server for Web ............... 10
    Supported browsers and JRE for Administration Services ....... 10

Creating an account ................................................... 13
  Logging into Administration Services ................................ 14
  Creating a computer, Web server, or browser user account ........ 17
    Creating accounts in batch .......................................... 21

Creating certificates .................................................. 23
  Creating certificates for computers .................................. 24
  Creating certificates for Web servers .................................. 28
    Generating a machine certificate signing request (CSR) ........ 28
    Submitting the certificate request ................................ 35
    Importing a Web server certificate ................................. 38
  Retrieving and importing the CA certificate into a Web server .... 42
    Retrieving the CA certificate from Managed Services .......... 42
    Importing the CA certificate into the Web server ................ 43
  Importing a cross-certificate into a Web server .................... 47
  Creating certificates for Web browser users .......................... 50
Retrieving and importing the CA certificate into a Web browser ........... 57
Importing the CA certificate using Internet Explorer ...................... 57
Importing the CA certificate using Firefox ............................... 59
Machines and applications, as well as people, are consumers of certificates. When you issue a certificate to a machine (such as a computer or Web server), or an application (such as a Web browser), you authorize and secure communication taking place across the network.

This guide documents how to create certificates for computers, Web servers, and browsers.

This chapter includes:

- “How does it work?” on page 6
- “Using certificates with computers, Web servers, and Web browser users” on page 7
- “Overview of creating certificates for computers, Web servers, and browser users” on page 8
- “Supported browsers and JRE” on page 10
How does it work?

To issue certificates to computers, Web servers, or browsers, you can use Enrollment Server for Web. This Web-based application creates and imports certificates to the local machine store or application-specific certificate store. The certificate placement in the machine store is important, as many applications require the certificate to be there for authentication purposes, such as those using 802.1x network authentication.

You can issue a certificate to a machine or application operating in a Windows or non-Windows environment.

Enrollment Server for Web is used for PKCS#10 requests and creates a 1 key-pair certificate for authentication and encryption, which may be needed to issue certificates to computers, Web servers, browsers, VPN clients, and VPN devices. These certificates also come with a fixed lifetime.

While certificates issued to computers, Web servers, or Web browsers are not automatically managed by Entrust, you can generate certificate status reports through Administration Services. Administration Services also generates certificate expiry warnings.

For more information about the role of Administration Services as it applies to issuing certificates to computers, Web servers, and browsers, see “The role of Administration Services” on page 8.

Note: Entrust does offer the ability to automatically manage credentials for Internet Information Services (IIS), Microsoft’s Web server, as well as domain controllers using Entrust Entelligence Security Provider. For more information, contact Entrust.
Using certificates with computers, Web servers, and Web browser users

This topic briefly describes the use of certificates with machines and applications.

This topic includes:

- “Digital certificates for computers” on page 7
- “Digital certificates for Web servers” on page 7
- “Digital certificates for Web browser users” on page 7

Digital certificates for computers

By issuing certificates to computers, you can designate which computers you want to authorize for network access. Once you create and import a certificate, issued by the root or subordinate certification authority (CA), onto a specific computer, that computer can authenticate to your network. By authenticating, the computer is granted access to the network.

Any computer that does not have a certificate issued by a trusted CA, cannot authenticate to the network and is thus denied access.

Certificates issued to computers can also encrypt computer-to-computer communication.

Digital certificates for Web servers

By issuing certificates to Web servers, you can encrypt Secure Socket Layers (SSL) or Transport Layer Security (TLS) connections between client browsers and Web servers. SSL and TLS ensure that information travelling between the browser and Web server, as well as between Web servers, remains confidential.

Digital certificates for Web browser users

By issuing certificates to Web browser users, you can authenticate a person or machine to a Web site, other machines, or applications in order to ensure trusted and secure online communications and transactions. To achieve this, certificates are placed in the user certificate store, or in the case of Firefox, the Firefox certificate store.
Overview of creating certificates for computers, Web servers, and browser users

To create certificates for computers, Web servers, and browser users, an administrative user must complete the following steps:

1. Create an account for the certificate through Administration Services, a Web-based application.

   **Note:** This guide assumes you have an administrator certificate from Entrust, which allows you to create other certificates. If you signed up for Entrust Managed Services PKI, but have not yet created an administrator certificate, see the Administrator Guide available under the Resources tab of www.entrust.com/managed_services.

2. Securely record the reference number and authorization code provided by Administration Services for the computer, Web server, or browser account.

3. Access Enrollment Server for Web, a Web-based application, to generate and import the certificate using the reference number and authentication code.

   **Note:** If issuing a certificate to a Web server, you must request a certificate through a PKCS#10 certificate request. The PKCS#10 request must contain a common name (CN) that matches the reference number assigned by Administration Services to the Web server account.

The role of Administration Services

Administration Services is a Web-based application that provides administrative capabilities. It is this application that is used to create all certificate accounts, regardless of where the certificate is issued (for example, users, machines, or applications). You must create accounts for certificates, as the account information is needed to populate the database so you, or Entrust, can manage them. It also allows you to obtain the reference number and authentication code, which is required to create a certificate.
While Administration Services does create certificates as well, Enrollment Server for Web has the ability to create a 1 key-pair certificate, which is needed for certificates issued to machines, and to store these certificates in the machine certificate store, which is required by some applications for authentication purposes (for example, 802.1x).
Supported browsers and JRE

You access Enrollment Server for Web and Administration Services using a browser. Both support several versions of popular browsers. Administration Services also requires a compatible Java plug-in.

For updates to the list of supported browsers and JRE, see the Platform Support & Integration Center on the Entrust TrustedCare Web site at:

https://www.entrust.com/trustedcare

Note: You must use Internet Explorer for creating and importing computer certificates.

Supported browsers for Enrollment Server for Web

Enrollment Server for Web supports the following browsers (or a later version) on Windows: Microsoft® Internet Explorer 5.0, Mozilla® Firefox 1.5, Mozilla® 1.7, and Netscape® Navigator 7.0.

Supported browsers and JRE for Administration Services

Administration Services supports the following browser versions (or a later version) on a Microsoft® Windows® operating system: Microsoft® Internet Explorer 6.0, Mozilla® Firefox 1.5, Mozilla® 1.7.2, or Netscape® Navigator 8.0. Make sure your browser as settings as shown in Table 1.

Entrust Authority Administration Services uses Entrust TruePass® technology and downloads an applet to authenticate administrators. As a result, you must ensure that one of the following Java runtime environments (JRE) is installed, and that applicable browser settings are configured. With all supported Web browsers, you must allow cookies and enable both Java and JavaScript.
You can download the Sun JRE from the following site: http://www.java.com/download.

**Table 1: Browser settings for Administration Services**

<table>
<thead>
<tr>
<th>Browser</th>
<th>Java Runtime Environment (JRE)</th>
<th>Setting Name</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer 6, 7, and 8</td>
<td>Microsoft Java Virtual Machine (JVM), Sun JRE 1.4.2+ and 1.5.+</td>
<td>First-party cookies</td>
<td>Accept or Prompt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allow per-session cookies (not stored)</td>
<td>Enable or Prompt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active scripting</td>
<td>Enable or Prompt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scripting of Java applets</td>
<td>Enable or Prompt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third-party cookies</td>
<td>Block</td>
</tr>
<tr>
<td>Mozilla Firefox 1.5, 2, and 3.0</td>
<td>Sun JRE 1.4.2+, 1.5_04+, 1.6.0_03+</td>
<td>Allow sites to set cookies</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Java</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable JavaScript</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If pop-up blocker is enabled, allowed sites</td>
<td>Administration Services sites</td>
</tr>
<tr>
<td>Mozilla 1.7.2, 1.7.10</td>
<td>Sun JRE 1.4.2 and 1.5+</td>
<td>See Mozilla Firefox 1.5</td>
<td></td>
</tr>
<tr>
<td>Netscape Navigator 8.0</td>
<td>Sun JRE 1.4.2 and 1.5+</td>
<td>Enable cookies</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Java</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable JavaScript</td>
<td>Enable</td>
</tr>
</tbody>
</table>
In order to create a certificate for computers, Web servers, or browser users, you first need to create an account. You create certificate accounts using Administration Services, a Web-based application.

This chapter includes the following topics:

- “Logging into Administration Services” on page 14
- “Creating a computer, Web server, or browser user account” on page 17
Logging into Administration Services

Once you create your administrator certificate as described in the Administrator Guide (available under the Resources tab of www.entrust.com/managed_services), you can then log in to Administration Services.

From Administration Services, you can create, modify, deactivate or reactivate accounts as well as perform other administrative functions.

Complete the following procedure to log in to Administration Services.

To log in to Administration Services

1. Enter the Administration Services URL provided by Entrust Managed Services PKI into a browser.

   The following page appears.

2. Depending on where you stored your administrator certificate, do one of the following:
<table>
<thead>
<tr>
<th>if you stored your certificate...</th>
<th>Do this</th>
</tr>
</thead>
</table>
| In the Entrust desktop security store on your computer  | **1** Click **Browse** to navigate to the location where you stored your administrator digital ID (.epf file) and click **Open**. The file name and path appear in the **Entrust Desktop Security Store File Name** field. Select **Remember Entrust Desktop Security Store File Name** to retain the path.  
**2** Enter the password you created for your certificate and click **Log in**.                                                                                                         |
| within the Windows framework or on a smart card or token.| **1** Click the **Log in with my Third-Party Security Store** link. The **Administrator Login - Third-Party Third-Party Security Store** page appears. **Note**: If logging in with a smart card or token, ensure it is connected to your computer.  
**2** Click **Display certificate list**. The **Select Certificate** dialog box appears listing one or more digital certificates.  
**3** Select your certificate from the list and click **OK**.                                                                                                                                  |
Upon successful login, the following page appears.

From this page, you can now create a computer, Web server, or browser user account. See “Creating a computer, Web server, or browser user account” on page 17
Creating a computer, Web server, or browser user account

You must create an account for each certificate you need. When you create a new account, Administration Services generates a reference number and authorization code for that account. You use this number and code later to create the certificate using Enrollment Server for Web.

Complete the following procedure to create an account for each computer, Web server, or browser user certificate you need.

To create an account

1. If you are not logged in to Administration Services, do so now (see “To log in to Administration Services” on page 14 for more information).

The main Administration Services page appears.
2 Click **Create Account** under **Account Tasks** in the main pane or under **Tasks** in the left-hand menu.

The initial **Create Account** page appears.

3 Complete the following based on the account you want to create.

<table>
<thead>
<tr>
<th>Account type</th>
<th>Do this</th>
</tr>
</thead>
</table>
| Computer or Web server        | **1** From the **User Type** drop-down list, select **Web server**.  
                              | **2** From the **Certificate Type** drop-down list, select **Web - Web Server** or your company’s specific certificate type, if one is set up for you.  |
| Web browser                   | **1** From the **User Type** drop-down list, select **Person**.  
                              | **2** From the **Certificate Type** drop-down list, select **Web - Default** or your company’s specific Web certificate type, if one is set up for you.  |

3 Click **Submit**.
A second **Create Account** page appears where you provide the organization name and other information.

**Note:** The **User Information** area varies depending on the user type selected in **Step 3**.
4 Fill out the **User Information** section based on the user type you selected in **Step 3**:

<table>
<thead>
<tr>
<th>Account type</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer or Web server</td>
<td>1 Fill in the <strong>Name</strong> field, which is typically the fully qualified domain name (FQDN) of the machine.</td>
</tr>
<tr>
<td></td>
<td>2 Optionally, fill in the <strong>Description</strong> and <strong>Email</strong> fields.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you enter a notification email address, Administration Services sends status notification messages to that address.</td>
</tr>
<tr>
<td>Web browser user</td>
<td>1 Fill in the <strong>First Name</strong> and <strong>Last Name</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>2 Optionally, fill in the <strong>Serial Number</strong>, <strong>Email</strong>, and <strong>Comment</strong> fields.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you enter an email address, Administration Services sends status notification messages to that address.</td>
</tr>
</tbody>
</table>

3 Select the member option under **Group Membership**. (The name of your company replaces the word `default group` in the image above.)

4 Set **Role** to **End User**.

5 Under **Location**, click **Select the searchbase** and select your company name from the drop-down list. (An entry for your company was created in the directory when you signed up for Entrust Managed Services PKI.)

The searchbase indicates where the account will be located in the Administration Services LDAP directory.

6 Click **Submit**.
The **Create Account – Complete** page appears. You have successfully created an account.

### Create Account - Complete

You have created the following account:

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
<th>Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC Org.</td>
<td>Example</td>
<td>End User</td>
<td>New</td>
</tr>
</tbody>
</table>

### Activation Codes

Securely distribute these codes to the account holder:

- **Name:** cn=ABC Org.,ou=Example,o=Entrust,c=US
- **Reference Number:** 8039498
- **Authorization Code:** ATFZ-7K68-8LE
- **Codes were created on:** Wednesday, April 09, 2008 2:08:58 PM
- **Codes will expire on:** Wednesday, April 23, 2008 2:08:58 PM

- **Create Local Digital ID**
- **Create Roaming Digital ID**
- **Create Third-Party Security Store**

This page lists the new account's reference number and authorization code, which you need to generate the certificate. Record this information and store it in a secure manner.

---

**Note:** The three links at the bottom of the **Activation Codes** pane do not apply to certificates issued to computers, Web servers, or browser users.

---

### Creating accounts in batch

If you want to add groups of new account in batch, click the **Create Accounts from File** option under **Account Tasks** in the main pane or under **Tasks** in the left-hand menu. This method requires an input file of precise
construction. See the *Entrust Authority Administration Services Administration Guide* for details.
Creating certificates

This chapter describes how to generate certificates and import them to your computer, Web server, or Web browser using the activation codes you received when you created the account in the previous chapter.

In order to create certificates for computers, Web servers, and browser users, you must use Enrollment Server for Web.

This chapter includes:

- “Creating certificates for computers” on page 24
- “Creating certificates for Web servers” on page 28
- “Creating certificates for Web browser users” on page 50
Creating certificates for computers

Complete the following procedure to create a certificate for a computer using Internet Explorer.

To create a certificate for a computer

1 Log in to Enrollment Server for Web:

https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start

where <admsvc_home> is the URL of your Entrust Managed Services PKI.

Note: For customers of the free 60-day evaluation of Entrust Managed Services PKI, <admsvc_home> is evaladminservices.managed.entrust.com.

The Enrollment Server for Web main page appears.

2 Click Create Computer, Device or Windows Server Certificate from the main pane, or Computer, Device or Windows Server from the left pane.
3 Enter the reference number and authorization code in the respective fields. You received this number and code from Administration Services when you created the computer account.

4 From the Provider type drop-down list, select RSA full.

5 From the CSP drop-down list select Microsoft Enhanced Cryptographic Provider v1.0.

Note: The Provider type selected determines which CSPs are visible in the CSP list. The CSP list is populated with CSPs available on the system. While the Microsoft Enhanced CSP is recommended, you can choose a different one. See http://technote.microsoft.com/en-us/library/cc962093.aspx.
6 Click **Submit Request**.
A dialog box appears confirming that the Web site is requesting a new certificate on your behalf.

7 **Click Yes** to request the certificate from Enrollment Server for Web.
A second dialog box appears asking if you want to add the certificate created by this Web site to your computer.

8 **Click Yes** to add the certificate to your computer.
A success message appears.
<table>
<thead>
<tr>
<th>Computer Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have successfully created your certificate. It has been stored in the local machine certificate store and can be used to securely identify your system to VPN gateways, and to conduct private, encrypted communication over the Internet.</td>
</tr>
</tbody>
</table>

You successfully created a certificate for your computer.
Creating certificates for Web servers

To create a certificate for a Web server, you must complete the following:

1. Generate a certificate signing request (CSR)
2. Submit the CSR
3. Import the certificate into your Web server
4. Retrieve the certification authority (CA) certificate from Entrust Managed Services PKI
5. Import the CA certificate into your Web server

Complete the following procedures to create a certificate for a Web server.

Generating a machine certificate signing request (CSR)

After you obtain activation codes for your Web server account using Administration Services as described in “Creating a computer, Web server, or browser user account” on page 17, you can start the process of creating a certificate for a Web server.

To install the certificate to the Web server, you must first generate a pair of cryptographic keys and a PKCS#10 certificate signing request (CSR). The CSR contains information used to create the certificate.

Attention: One important piece of information required in the certificate signing request (CSR) is the common name (CN). The CN in the CSR must be the reference number you obtained from Administration Services when creating the Web server account. This step is included in the procedures below.

Note: The configuration information required in the CSR—such as DN, attributes, and signature algorithm identifier—differs between Web servers. Check with your vendor documentation for configuration specifics.

Follow the procedure for your Web server to generate a CSR:

- “To generate keys and a CSR on Microsoft® IIS” on page 29
- “To generate keys and a CSR on Sun™ ONE” on page 30
To generate keys and a CSR on Microsoft® IIS

1. On the machine hosting the Web server, open the Internet Services Manager (select Start > All Programs > Administrative Tools > Internet Service Manager).
2. Expand the Web Sites folder.
3. Right-click Default Web Site and click Properties in the pop-up menu.
5. Under Secure Communications, click Server Certificate.

The Web Server Certificate Wizard appears.

6. Click Next.
7. Select Create a new certificate and click Next.
8. Select Prepare request now, but send it later and click Next.
9. On the Name and Security Settings page:
   a. Enter a name for the certificate. Entrust recommends that you use the fully qualified domain name of the Web server, for example www.myserver.com.

   **Note:** If you do not use the domain name, users connecting to your Web site receive a warning stating that the certificate name does not match the name of the Web server.

   b. In the bit length list, select the longest key length available but no greater than 2048. Shorter key sizes are less secure.
   c. Click Next.

10. In the Organization Information page:
    a. Enter your organization and department names in the Organization and Organizational unit fields, respectively.
    b. Click Next.
11 On the **Your Site’s Common Name** page, do not enter a name. Instead, enter the reference number you obtained from Administration Services in the **Common Name** field and click **Next**.

12 On the **Geographical Information** page, fill out the **Country/Region**, **State/Province**, and **City/Locality** fields and click **Next**.

13 In the **File name** field on the next page, accept the default name or enter a new path and file name for the file that will contain the Web server certificate request and click **Next**.

The **File Summary** dialog box appears.

14 Click **Next**, then **Finish** to close the wizard.

15 Click **OK** to close the dialog box.

The CSR is saved in the text file you specified in **Step 13**.

16 Open the text file. It should look similar to this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBezCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIUZIubmV0
MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L
JPsdfCsjqRs8ygoyaw4uc0Edx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBA
AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfso
Qs5JRNaQRE6B
-----END NEW CERTIFICATE REQUEST-----
```

You have generated and copied a certificate request.

17 Keep the text file open and proceed to “**Submitting the certificate request**” on page 35.

---

**To generate keys and a CSR on Sun™ ONE**

1 Open the **Sun ONE Administer Web Server** page.

2 Choose the Web Server you want to manage Enrollment Server for Web and click **Manage**.

3 Click the **Security** tab.
4 Enter a new password and click OK to create a Trust Database. This database is used to store the Web server certificate.

5 Click Request a Certificate.

6 From the Request a Certificate dialog box, select New Certificate.

7 Select the CA URL option and enter the CA URL in the CA URL field.

8 In the Key Pair Password field, enter a password. There is no password confirmation field, so type carefully to ensure that you make no mistakes.

9 In the Common Name field, enter the reference number you obtained for the Web server from Administration Services.

10 Fill out the remaining fields and click OK.

This creates a PKCS-10 request that looks something like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrZbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuZ29mdHdhcmUg
MEwwDQYJKoZIhvcNAQEBBQADgY0AwIBAgIMB±/1jvMzWcQg16lC/9tGU0K+A4
MDIQvTA0GCSqGSIb3DQEBBQUAFgEAMCIHMwIGA1UEAxMnYWJiZXIuZ29mdHdhcmUg
MEwwDQYJKoZIhvcNAQEBBQADggIBAKJwZiEJbG9QVXNlYXJ5QGhHEgQ71sP0
I4Ic9b2O3jyIaIq0TqQ4cLyXjWp0dTcVlP0Qb0tQJ7C/79k7n0Ukx6T6c5X0
-----END NEW CERTIFICATE REQUEST-----
```

11 Copy the entire certificate request to the clipboard, including the BEGIN and END lines, and paste it into Notepad or similar text editor for temporary storage.

You have generated and copied a certificate request. Proceed to “Submitting the certificate request” on page 35.

To generate keys and a CSR on Red Hat Stronghold

1 Run the genkey utility, specifying the name of the host or virtual host:

```
# bin/genkey <hostname>
```

The genkey utility prints the file names and locations of the key file and certificate file it is about to generate.
The key location is:
# <ServerRoot>/ssl/private/<hostname>.key

The certificate location is:
# <ServerRoot>/ssl/certs/<hostname>.cert

2 Press Enter.
The `genkey` utility reminds you not to overwrite an existing key pair and certificate.

3 Press Enter.
The `genkey` utility prompts you to specify the size of the key.

4 Enter a key size of at least 1024 bits. Shorter key sizes are less secure.
The `genkey` utility generates random data with which to create a unique key pair. It then prompts you for random keystrokes.

5 Type random keystrokes on your keyboard. Stop when the counter reads “0” and `genkey` beeps and displays this message:
   # 0 * -Enough, thank you

   The `genkey` utility generates the key pair and saves it in the following location:
   # ServerRoot/ssl/private/hostname.key

6 When the `genkey` utility asks if you want to use the `genreq` utility to send a CSR, enter y to send a CSR.
The `genreq` utility starts automatically, displays a lettered list of CAs, and asks which one you want to use.

7 Type the letter that corresponds to your preferred CA.

8 Type the two-letter code for your country. For example, type US for the United States, DE for Germany or JP for Japan.

9 Type the following information when prompted:
   • the full name of your province or state
   • your city, town, or other locality
   • your organization
   • your unit within the organization
10 Enter the reference number you obtained for the Web server from Administration Services in the **Common Name** field.

When `genreq` generates the CSR, it looks something like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJ0ZXQgU29mdHdcmUg
SW5jMRAwDgYDVQQLEw1nYWJiZXItiYzIuYzIubmV0
MEwwDQYJKoZIhvcNAQEBBQADgY0AMHRGk0c+L36QDAk0dGw4yWx9L
-----END NEW CERTIFICATE REQUEST-----
```

11 Copy the entire CSR to the clipboard, including the BEGIN and END lines, and paste it into Notepad or similar text editor for temporary storage.

You have generated and copied a certificate request. Proceed to “Submitting the certificate request” on page 35.

---

**To generate keys and a CSR on IBM® HTTP Server**

1 Start the iKeyMan utility. For instructions on starting this utility, refer to the [iKeyMan User Guide](#).

2 Select **Key Database File** and click **New**.

3 In the **Password Prompt** dialog box, enter a new password.

4 Ensure you select the **“Stash the Password to file”** option to create the `key.sth` file. Click **OK**.

5 Save this file into the default `key.kdb` file or create your own file name.

6 Click **OK**.

7 Select **Create** from the main user interface and click **New Certificate Request**.

The **New Key and Certificate Request** dialog box opens.
Enter information in the fields as described in Table 2 below:

**Table 2: Key and CSR information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Label</td>
<td>Enter a descriptive comment to identify the key and certificate in the database.</td>
</tr>
<tr>
<td>Keysize</td>
<td>Enter a size of at least 1024 bits. Shorter key sizes are less secure.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Enter the reference number obtained from Administration Services.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the name of your organization.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Optional. Enter the ou= value (the unit of your organization that the Web Server belongs to).</td>
</tr>
<tr>
<td>Locality</td>
<td>Optional. Enter the locale of your organization.</td>
</tr>
<tr>
<td>State/Province</td>
<td>Optional. Enter the state or province of your organization.</td>
</tr>
<tr>
<td>Zipcode</td>
<td>Optional. Enter the zip or postal code of your organization.</td>
</tr>
<tr>
<td>Country</td>
<td>Enter the two-letter code for your country. For example, enter “US” for the United States, “DE” for Germany or “JP” for Japan.</td>
</tr>
<tr>
<td>Certificate request filename</td>
<td>Enter a new name for the certificate request file, or use the default file name.</td>
</tr>
</tbody>
</table>

Click OK.
10 In the **Information** dialog box, click **OK**.

The certificate request file, when opened, should look like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMRS25jMRAwDgYDVQQLEwdUZXN0aW5nMTYwFAYDVQQDEw1nYWJiZXIxYzIubmV0MEwwDQYJKoZIhvcNAQEBBQADAQABMA0GCSqGSIb3DQEBCwUAMBQGCCsMIGbAgEB
-----END NEW CERTIFICATE REQUEST-----
```

11 Copy the entire CSR to the clipboard, including the BEGIN and END lines, and paste it into Notepad or similar text editor for temporary storage.

You have generated and copied a certificate request. Proceed to “**Submitting the certificate request**” on page 35.

### Submitting the certificate request

After generating a certificate signing request (CSR) for the Web server, you have to submit the CSR through Enrollment Server for Web. You can submit a standard request, or you can request a certificate with only encryption key usage.

Complete the following procedure to submit the CSR.

#### To submit a certificate request

1. Log in to Enrollment Server for Web:

   ```
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   where <admsvc_home> is the URL of your Entrust Managed Services PKI.
   ```

   **Note:** For customers of the free 60-day evaluation of Entrust Managed Services PKI, `<admsvc_home>` is `evaladminservices.managed.entrust.com`.

   The Enrollment Server for Web main page appears.
2. From the main pane, click **Create Certificate from PKCS#10 Request**, or click **Web Server** from the left pane.

   The **Web Server PKCS#10 Certificate Request** page opens.
Web Server PKCS#10 Certificate Request

Note: here you can request a certificate for a Web Server or any client that supports PKCS#10 request.

In the fields below, enter the reference number and authorization code that you received from the Certification Authority. You can choose to view the certificate in raw DER format or in PKCS #7.

| Reference Number: | 
| Authorization Code: | 
| Options: | displayed as PEM encoding of certificate in raw DER |

Please enter your certificate request (PKCS#10 request) in the following field. If you are requesting this certificate for a Web Server, make sure that your Common Name (CN) matches the reference number of the certificate being retrieved when generating the request. If you do not know how to generate this request, please consult your server documentation.

3 Enter the reference number and authorization code for the Web server that you obtained from Administration Services in the respective fields.

4 From the Options drop-down list, choose the format for the certificate.

Note: To determine which option to choose, find out how your Web Server processes certificates. For more information, consult your Web server documentation.
Options include:

- **Raw Distinguished Encoding Rules (DER) format**
  The DER format displays the certificate in raw text format.

- **Public-Key Cryptographic Standard #7 (PKCS7)**
  PKCS7 displays the certificate with mark-up tags.

5 Copy the certificate request you stored earlier in Notepad and paste it into the large text box.

6 Click **Submit Request**.

Managed Services generates a Web server certificate and sends it to Enrollment Server for Web.

7 Click **Download** on the page displaying your certificate.

   The dialog box that appears next varies depending on the browser you use, but the steps are similar.

- **In Internet Explorer:**
  – In the **File Download** dialog box, click **OK** to save this file to disk.
  – In the **Save As** dialog box, choose a name and path of a text file in which to save the certificate.
  – Click **Save**.

- **In Firefox:**
  – In the **Opening** dialog box, select **Save to Disk**.
  – Click **OK**.

   Firefox saves the file to the desktop.

   The certificate is saved in the text file, though the file extension may be .bin or .cer. Proceed to “Importing a Web server certificate” on page 38.

**Importing a Web server certificate**

Follow the instructions that apply to your Web server to install the certificate:

- “To import the Web server certificate on Microsoft® IIS” on page 39
- “To import the Web server certificate on Sun™ ONE” on page 39
To import the Web server certificate on Microsoft® IIS

1. Open the Internet Services Manager (select Start > Programs > Administrative Tools > Internet Service Manager).
2. In the navigation tree view, right-click Default Web Site and select Properties in the pop-up menu.
   The Web Server Certificate Wizard opens.
5. Click Next.
6. Select Process the pending request and install the certificate and click Next.
7. Click Browse to find the file that contains the text file you saved in Step 7 on page 38.

   Note: You may have to set the file type list to All Files to see your file.
8. Click Next.
9. If asked, enter the port number for the SSL connection and click Next.
10. Click Next again, then click Finish.
You have imported the Web server certificate into your Web server.

To import the Web server certificate on Sun™ ONE

1. Open the Sun ONE Administer Web Server page.
2. Choose a Web Server and click Manage.
3. Click the Security tab.
4. Click Install Certificate.
In the Certificate For frame, select This Server.

Enter your password in the Key Pair File Password field.

Select Message Text (with headers).

In the Message Text (with headers) field, copy and paste the entire certificate that you saved.

Click OK.

The Add Server Certificate Web page appears.

Click Add Server Certificate.

You have imported the Web server certificate into your Web server.

To import the Web server certificate on Red Hat® Stronghold

1 Run Stronghold’s `getca` utility, specifying the name of the host that owns this certificate and providing the path of file that contains the certificate you saved as input:

```
# getca <hostname> <path_of_file_that_contains_certificate>
```

For example:

```
# getca webserverA.YourCompany.com
c:/certificate/servercert.txt
```

This command saves the certificate in the file `hostname.cert`.

2 Restart Stronghold to implement the new certificate by entering the following command:

```
# reload-server
```

You have imported the Web server certificate into your Web server.

To import the Web Server certificate on IBM® HTTP Server

1 Start the iKeyMan utility. For instructions on starting this utility, refer to the iKeyMan User Guide.

2 Select Key Database File and click Open.

3 In the Open dialog box, enter the key database name. You created this name in Step 5 of “To generate keys and a CSR on IBM® HTTP Server” on page 33.

4 Click OK.
5 In the **Password Prompt** dialog box, enter the password you created in Step 3 of “To generate keys and a CSR on IBM® HTTP Server” on page 33.

6 Click **OK**.

7 Select **Personal Certificates** in the **Key Database** menu and click **Receive**.

8 In the **Receive Certificate from a File** dialog box, enter the name of the file that contains the certificate you saved in the **Certificate filename** text field.

9 Click **OK**.
Retrieving and importing the CA certificate into a Web server

Installing the CA certificate into a Web server is a two-part process:

- “Retrieving the CA certificate from Managed Services” on page 42
- “Importing the CA certificate into the Web server” on page 43

This topic also includes instructions on installing a cross-certificate into your Web server. This gives Web browsers secure access to Web servers that trust a cross-certified CA and vice versa. See “Importing a cross-certificate into a Web server” on page 47 for more information.

Retrieving the CA certificate from Managed Services

As the first step in installing the CA certificate, you must retrieve the Web server certificate from Enrollment Server for Web. Follow the instructions that correspond to your Web server.

- “To retrieve the CA certificate for IIS” on page 42
- “To retrieve the CA certificate on other Web Servers” on page 43

To retrieve the CA certificate for IIS

1. Access Enrollment Server for Web using the URL provided in your welcome package.

2. In the **CA Certificates** menu on the left, click **Install**. The **File Download** dialog box appears.

3. Do one of the following:
   - If you are using Firefox:
     a. Of the three check boxes, select at least **Trust this CA to identify Web sites**.
     b. Click OK.
   - If you are using Internet Explorer:
     a. Click **Open**.
     The **Certificate** dialog box appears.
     b. Click OK.
You retrieved the CA certificate and saved it to the certificate store. Proceed to “Importing the CA certificate into the Web server” on page 43.

To retrieve the CA certificate on other Web Servers

1. Access Enrollment Server for Web using the URL provided in your welcome package.
2. In the CA Certificates menu on the left, click Display.
   The CA Certificate window opens with the CA certificate included.
3. Copy the entire certificate and paste it into a similar text editor.
You retrieved the CA certificate. Proceed to “Importing the CA certificate into the Web server” on page 43.

Importing the CA certificate into the Web server

After you retrieve the CA certificate from Enrollment Server for Web, you must import it into your Web server. Follow the instructions that apply to your Web server to import the CA certificate:

- “To import the CA certificate for IIS” on page 43
- “To import the CA certificate on Sun ONE™” on page 44
- “To import the CA certificate on Red Hat® Stronghold” on page 45
- “To import the CA certificate on IBM® HTTP Server” on page 45

Note: It is also recommended that you check you Web server documentation for instructions.

To import the CA certificate for IIS

1. If necessary, change the name of the text file you saved in “To retrieve the CA certificate for IIS” on page 42 so that the extension is .cer.
2. Right-click the certificate file and select Install Certificate from the pop-up menu.
   The Certificate Import wizard appears.
3. Click Next.
4 From the Certificate Store page, select Place all certificates into the following store.
5 Click Browse.
6 From the Select Certificate Store dialog box, select Show Physical Stores.
7 Expand the Trusted Root Certification Authorities folder.
8 Select the Local Computer folder and click OK.
The Certificate Import wizard reappears.
9 Click Next and then click Finish.
A success message appears.
10 Click OK.
You have imported the CA certificate into your Web server.

To import the CA certificate on Sun ONE™
1 Open the Sun ONE Administer Web Server page.
2 Select the Web Server that will manage Enrollment Server for Web and click Manage.
3 Click the Securities tab.
4 Click Install Certificate.
5 In the Certificate For frame, select Trusted Certificate Authority (CA).
6 Enter your password in the Key Pair File Password field.
7 Select Message Text (with headers).
8 In the Message Text (with headers) field, paste the certificate that you copied in "To retrieve the CA certificate on other Web Servers" on page 43.)
9 Click OK.
The Add Server Certificate Web page appears.
10 Click Add Server Certificate.
You have imported the Web server certificate into the trust database on your Web server. Now the Sun ONE Web Server can verify signatures on all browser certificates signed by that CA.
To import the CA certificate on Red Hat® Stronghold

1. Ensure that the CA certificate is in PEM format.
2. Save the CA certificate file you copied in “To retrieve the CA certificate on other Web Servers” on page 43 making sure it has a .pem extension.
3. Go to the directory that contains the text file containing the CA certificate.
4. Enter the following command to append the CA certificate to the existing certificate file you downloaded:
   
   ```
   # cat newcert.pem >> <CA_certificate_filename>.pem
   ```

You have imported the CA certificate into your Web server. Now the Stronghold Web server can verify signatures on all browser certificates signed by that CA.

To import the CA certificate on IBM® HTTP Server

1. Start the iKeyMan utility. For instructions on starting this utility, refer to the iKeyMan User Guide.
2. Select Key Database File and click Open.
3. In the Open dialog box, enter the key database name.
4. Click OK.
5. In the Password Prompt dialog box, enter the password.
6. Click OK.
8. Open the CA Certificate (PEM encoding) page.
9. Paste the certificate that you copied in “To retrieve the CA certificate on other Web Servers” on page 43, including the BEGIN and END lines, into a file with an .arm extension.
10. Select Signer Certificates in the Key Database window and click Add.
11. In the Add CA’s Certificate from a File dialog box, select the certificate file name or browse to the file.
12. Click OK.
13 In the Label dialog box, enter a label name and click OK.
You have imported the CA certificate into your Web server. Now the IBM HTTP Server can verify signatures on all browser certificates signed by that CA.
Importing a cross-certificate into a Web server

**Note:** This option is not available for Entrust Managed Services PKI 60-day trial customers.

If Entrust has cross-certified your CA with one or more other CAs on your behalf, and you want to give Web browsers secure access to Web servers that trust a cross-certified CA and vice versa, you must install the cross-certificate chain to your Web server.

**Note:** Some Web browsers and Web servers do not support certificate chains used in cross-certification. Consult your Web server or Web browser documentation to determine if it supports certificate chains.

The configuration involves:

- Copying the certificate chain from Enrollment Server for Web
- Installing the certificate chain in your Web server

Complete the following procedure to install a cross-certificate into your Web server.

**To install a cross-certificate into your Web server**

1. Log in to Enrollment Server for Web:
   
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   
   where `<admsvc_home>` is the URL of your Entrust Managed Services PKI.

   **Note:** For customers of the free 60-day evaluation of Entrust Managed Services PKI, `<admsvc_home>` is evaladminservices.managed.entrust.com.

   The Enrollment Server for Web main page appears.
2 Click Display list under Cross-Certificates in the left pane. The Cross-certificate(s) (PEM encoding) page appears displaying the cross-certificates you can install on your Web server. This page also indicates how many cross-certificate are available to you.

3 Copy the entire cross-certificate, including the ----BEGIN CERTIFICATE---- and ----END CERTIFICATE---- lines, and paste it into a text editor.

4 Use the procedure provided to import a CA certificate into your Web server (“Importing the CA certificate into the Web server” on page 43) to import your cross-certificate.
**Note:** Whenever the procedure refers to the CA certificate file you copied, ensure you use the cross-certificate you copied in Step 3 instead. It is also recommended that you check your Web server documentation for instructions.
Creating certificates for Web browser users

Certificates issued to Web browser users provides authentication capabilities to Web servers.

When this certificate expires, each Web browser user must access Enrollment Server for Web and import a new certificate.

Users must complete one of the following procedures to install the certificate to their browser.

- “To import a certificate using Internet Explorer” on page 50
- “To import a certificate using Firefox” on page 54

To import a certificate using Internet Explorer

1. If you have not already done so, obtain a reference number and authorization code for each account in Administration Services. See “Creating a computer, Web server, or browser user account” on page 17 for more information.

2. Use Internet Explorer to access Enrollment Server for Web:
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   where <admsvc_home> is the URL of your Entrust Managed Services PKI.

   Note: For customers of the free 60-day evaluation of Entrust Managed Services PKI, <admsvc_home> is evaladminservices.managed.entrust.com.

   The Enrollment Server for Web main page appears.
3 Click **Create Web Browser Certificate** from the main pane, or **Web Browser** from the left pane.

**Note:** The Microsoft Certificate Enrollment Control from Microsoft Corporation may appear. Click to run the add-on (ActiveX control).

The **Browser Certificate Request** page appears.
Enter the reference number and authorization code in the applicable fields.

For the CSP, do the following:

- Change the service provider (CSP) type from the CSP type list if required. The CSP list automatically changes to show the CSPs available for the selected type.

- Select the appropriate cryptographic service provider (CSP) from the list in the CSP drop-down menu. If you are installing the certificate on a smart card, select the smart card's CSP.

- Select the key size for the cryptographic algorithm from the Key Size drop-down list to prevent brute force attacks.

**Note:** This option is not available for Managed Services PKI 60-day trial customers. Key length is automatically set to 1024.

The larger the key, the harder it is to crack encrypted data. Options include:
– Default (the default length is 1024)
– 512
– 1024
– 2048

6 Click **Submit Request**.

A dialog box appears while the application is completing your request.

![](Creating a new RSA exchange key.png)

7 Click **OK**.

8 Accept or decline the automatic installation of the CA certificate into the Web browser. You should accept if you want to enable server authentication. Accepting the CA certificate allows you to skip over “Retrieving and importing the CA certificate into a Web browser” on page 57.

The requested browser certificate and the CA certificate for the issuing CA are imported into the user’s Web browser. The certificate is now part of the Windows CryptoAPI and you can use it with other applications.

If the user has not retrieved the CA certificate for the Web browser, you have to mark the browser certificate as trustworthy manually. Consult your Web browser documentation for details.
To import a certificate using Firefox

1. If you have not already done so, obtain a reference number and authorization code for each account in Administration Services. See “Creating a computer, Web server, or browser user account” on page 17 for more information.

2. Use Firefox to access Enrollment Server for Web:
https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
where <admsvc_home> is the URL of your Entrust Managed Services PKI.

    Note: For customers of the free 60-day evaluation of Entrust Managed Services PKI, <admsvc_home> is evaladminservices.managed.entrust.com.

The Enrollment Server for Web main page appears.

3. In the Certificates menu on the left, click Web Browser.
The Browser Certificate Retrieval - Step 1 page appears.
Enter the reference number and authorization code that you received from the Entrust Administrator.

Click Submit Request.

The **Browser Certificate Retrieval - Step 2** page appears.

Select an option from the **Key Length** drop-down list.

Click Submit Request.
If the **Use a master password** security option is not enabled (the default), your key is generated. If this security option is enabled, the **Change Master Password** dialog box appears.

![Change Master Password dialog box](image)

When this dialog box appears:

**a.** Enter and confirm a master password if you want certificate information protected by a password.

**b.** Click **OK**.

Your key is generated.
Retrieving and importing the CA certificate into a Web browser

Web server authentication also requires that you install a CA certificate on your Web browser. The procedure varies with your browser:

- If you are using an Internet Explorer browser, see “Importing the CA certificate using Internet Explorer” on page 57.
- If you are using a Firefox browser, see “Importing the CA certificate using Firefox” on page 59.

**Note:** The first time you connect your browser to a host server that has SSL enabled, you might not be able to verify the CA signature on the Web server certificate for that server. If this happens, refer to your browser or server documentation for instructions on how to install the CA certificate from the server.

Importing the CA certificate using Internet Explorer

Complete the following procedures to retrieve and import the CA certificate using the Internet Explorer browser.

**To retrieve the CA certificate using Internet Explorer**

1. Use Internet Explorer to access Enrollment Server for Web:

   ```
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   ```

   where `<admsvc_home>` is the URL of your Entrust Managed Services PKI.

**Note:** For customers of the free 60-day evaluation of Entrust Managed Services PKI, `<admsvc_home>` is `evaladminservices.managed.entrust.com`.

The Enrollment Server for Web main page appears.
2 In the CA Certificates pane on the left, click Install. The File Download dialog box appears.

3 Save the certificate file to your computer.

You retrieved the CA certificate and saved it in Internet Explorer. Now, you must import it using the below procedure.

To import the CA certificate into Internet Explorer

1 Right-click the certificate file you just retrieved and click Install Certificate from the pop-up menu.

2 Click Next.

3 Select Place all certificates into the following store.

4 Click Browse.

5 From the Certificate Store dialog box, select Show Physical Stores.

6 Expand the Trusted Root Certification Authorities folder.

7 Click the Local Computer folder and click OK.

8 Click Next and then click Finish.

The success message appears.

9 Click OK.
You imported the CA certificate into a user's browser.

**Importing the CA certificate using Firefox**

Complete the following procedures to retrieve and import the CA certificate using the Firefox browser.

**To retrieve and import the CA certificate into Firefox browsers**

1. Use Firefox to access Enrollment Server for Web:
   
   https://<admsvc_home>/cda-cgi/clientcgi.exe?action=start
   
   where `<admsvc_home>` is the URL of your Entrust Managed Services PKI.

   **Note:** For customers of the free 60-day evaluation of Entrust Managed Services PKI, `<admsvc_home>` is evaladminservices.managed.entrust.com.

   The Enrollment Server for Web main page appears.

2. In the **CA Certificates** menu on the left, click **Install**.
   
   The **Downloading Certificate** dialog box appears.

3. Select the appropriate check boxes to specify the purpose of your CA and click **OK**.
You retrieved and imported the CA certificate into a user’s Firefox browser.