Entrust Authority™

Enrollment Server for Web 7.0

Enrollment Server for WAP 7.0

Installation and Configuration Guide

Document issue: 1.0

October 2003

Entrust®
Securing Digital Identities & Information

Table of contents

About this document

This book provides detailed instructions for installing and configuring Entrust Authority™ Enrollment Server for Web 7.0 on both UNIX® and Microsoft® Windows®.

Note: This guide is part of the Entrust Authority 7.0 documentation set. Use it in conjunction with the other guides.

Topics in this chapter:

Related Entrust documentation

The guides listed below are related Entrust Authority documents. The latest Entrust Authority documentation is available on the Entrust® Customer Support Web site at https://www.entrust.com/support/documentation/index.cfm.

Entrust Authority Security Manager 7.0 guides

The following sections provide some detail about some of the key guides that form the Entrust Authority Security Manager 7.0 documentation set.

Entrust Authority Security Manager 7.0 Installation Guide for UNIX with Informix®

This guide describes how to install, configure, and initialize Security Manager on a UNIX server with an Informix® database.

Entrust Authority Security Manager 7.0 Installation Guide for UNIX with Oracle®

This guide describes how to install, configure, and initialize Security Manager on a UNIX server with an Oracle® database.

Entrust Authority Security Manager 7.0 Installation Guide for Windows

This guide describes how to install, configure, and initialize Security Manager on a Microsoft Windows server.

Entrust Authority Security Manager 7.0 Operations Guide for UNIX

This guide covers Master User tasks, including using the command-line interface to Entrust Authority Security Manager Control for a UNIX environment.

Entrust Authority Security Manager 7.0 Operations Guide for Windows

This guide covers Master User tasks, including using the command-line interface to Entrust Authority Security Manager Control for a Microsoft Windows environment.

Entrust Authority Security Manager Control Command Shell 7.0 for Windows and UNIX

This quick reference card contains a list of all Security Manager Control Command Shell commands, including a description, parameters, and examples for each.

Entrust Authority Security Manager Bulk Commands 7.0 for Windows and UNIX

This quick reference card contains a list of all Security Manager bulk commands, including a description, parameters, and examples for each.

Entrust Authority Security Manager Administration 7.0 guide

The following section provides some detail about the guide that forms the Entrust Authority Security Manager Administration 7.0 documentation set.

Entrust Authority Security Manager Administration 7.0 Installation Guide

This guide describes how to install the Administration Services. It also includes everything you'll need to know before you install the software, including architecture and general security considerations.

Entrust Authority Security Manager Administration 7.0 User Guide

This guide describes how to configure and customize Security Manager using Security Manager Administration for your environment.

Typographic conventions

The following typographic conventions are used throughout this guide:

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards	Click **Next**.
Italicized text	Used for book or document titles	*Entrust® Identification Server 7.0 Administration Guide*
Blue text	Used for hyperlinks to other sections in the document	Refer to "Related Entrust documentation" on page 6.
Underlined blue text	Used for Web links	For more information, visit our Web site at www.entrust.com.
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must type	Locate and double-click the executable file called `AppServerRuntimes_setupwin32.exe`.
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values)	Navigate to `<install_path>\Tools\dvt`.

Note and Attention text

Throughout this guide you will see paragraphs that have ruled lines above and below the text. These paragraphs provide key information with two levels of importance, as shown below.

Note: Hints, tips, and information that must be emphasized to help you get the best from your software.

Attention: Issues that, if ignored, may seriously affect performance, security, or the operation of your software.

Getting help

Entrust recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support and professional services available to you.

Technical Support

Entrust offers a variety of technical support programs to help you keep the Enrollment Server for Web up and running. To learn more about the full range of Entrust technical support services, visit our Web site at:

http://www.entrust.com/support/

If you are registered in our support program, you can use our Web-based support services at:

https://www.entrust.com/support/contact/index.htm

The Customer Support Extranet Web site offers technical resources including online versions of Entrust product documentation, white papers and technical notes, and a comprehensive Knowledge Base.

Note: You must have an account to use the Customer Support Extranet Web site. To create an account, go to http://www.entrust.com/xtranet/support.

When you contact Entrust Customer Support, please provide as much of the following information as possible:

- Your contact information
- Product name, version, and operating system information
- Your deployment scenario
- Description of the problem
- Copy of log files containing error messages
- Description of conditions under which the error occurred
- Description of troubleshooting activities you have already performed

Telephone numbers

For telephone assistance between 8:00 AM and 8:00 PM Eastern Standard Time (EST), Monday to Friday, call one of the numbers below:

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

E-mail address

The e-mail address for Customer Support is:

customer.support@entrust.com

Online

To submit a question online, go to the following Web address:

https://www.entrust.com/support/supportinfo/index.htm

Professional Services

The Entrust team assists e-businesses around the world to deploy and maintain secure transactions and communications with their partners, customers, suppliers and employees. We offer a full range of professional services to deploy our e-business solutions successfully for wired and wireless networks, including planning and design, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Entrust solution in-house or subscribe to hosted services, Entrust Professional Services will design and implement the right solution for your e-business needs. For more information about Entrust Professional Services please visit our Web site at:

http://www.entrust.com

Chapter 1

About Enrollment Server for Web

The Enrollment Server for Web 7.0 (formerly known as Entrust/WebConnector) distributes certificates to:

- standard Web browsers
- e-mail clients
- Web servers for SSL, TLS, S/MIME and object-signing applications
- Microsoft Windows devices that use certificates from the Local Computer certificate store (for example, VPN devices, Domain Controllers, Internet Authentication Service (IAS) server and clients, and so on).

Topics in this chapter:

What is a Web certificate?

A certificate is the electronic equivalent of a passport. For more detailed information about certificates, refer to the "Glossary" on page 107 or to the "Entrust Authority Security Manager 7.0 guides" on page 6.

A Web certificate is any certificate that is distributed to an application over a network such as the World Wide Web. For example, the following applications might use Web certificates:

- Web browsers
- Web servers
- e-mail clients
- VPN devices
- Domain Controllers
- IAS servers and clients

Use Web certificates for a variety of purposes. For example, use them to allow your Web browser users to authenticate themselves to your Web sites and vice versa. Mutual authentication allows all parties to trust that the other parties are who they claim to be. It ensures trusted and secure online communications and transactions.

Web certificates also allow Web servers to establish an encrypted connection with browsers using the SSL or TLS protocols. SSL and TLS ensure that the information travelling between the browser and the Web server remains confidential.

Why issue Web certificates?

Issue Web certificates to:

- send digitally signed and encrypted e-mail

  Secure Multi-purpose Internet Mail Extension (S/MIME) is a standard security protocol used for sending and receiving encrypted e-mail.

- establish a secure Web session

  Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are standard security protocols for establishing secure, encrypted channels over networks.

- verify the authenticity of downloaded software by object- or code-signing

For example, distribute Web certificates to users if they need to exchange secure e-mail using applications that are not Entrust Ready, or to establish secure connections to your Web sites using Security Manager as your CA.

The following table lists some other alternatives to Enrollment Server for Web.

Entrust Ready alternative	Description
Entrust Entelligence™ E-mail Plug-in	Provides secure internal and external e-mail communications when used with e-mail applications such as Microsoft® Outlook™ and Lotus® Notes™.
Entrust TruePass™	Secures Web sites and digitally signs data to bind electronic transactions.

For more information about these products, refer to http://www.entrust.com/solutions/index.htm.

What is Enrollment Server for Web?

Enrollment Server for Web 7.0 is composed of a CGI (common gateway interface) program with accompanying HTML files that distributes certificates to standard Web browsers, e-mail clients, and Web servers for SSL, S/MIME, and object-signing applications.

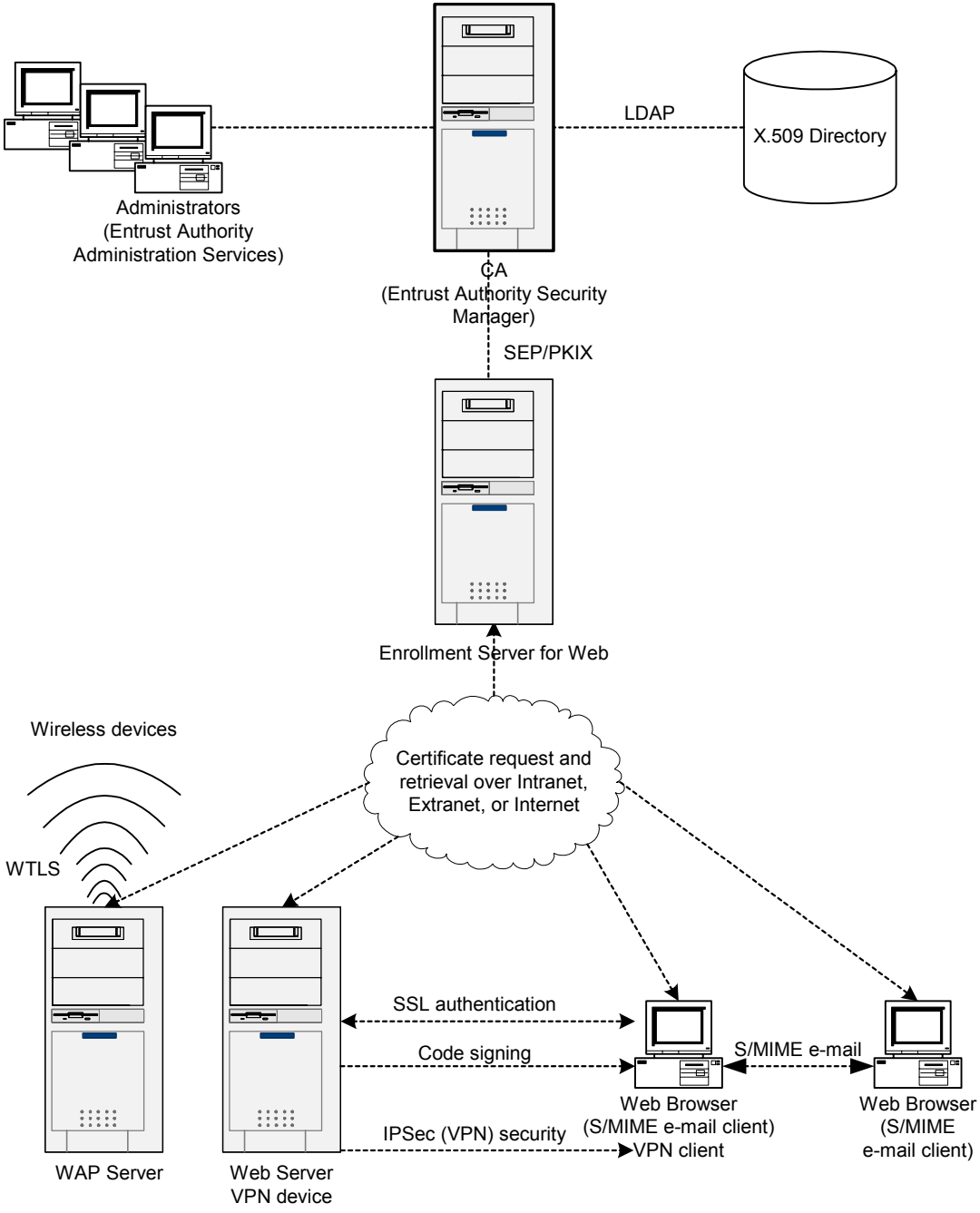
Enrollment Server for Web 7.0 provides the following functionality:

- accepts requests over a network (for example, the Internet) for Web certificates
- forwards requests for Web certificates to Security Manager
- provides an HTML-based interface that allows certificates to be retrieved from Security Manager

Install the Enrollment Server for Web on a Web server and access it through a Web browser or browser suite. A browser suite is a browser which includes an e-mail application.

Enrollment Server for Web uses Security Manager as its Certification Authority (CA). On request, Security Manager issues certificates to users who are browsing the Web or sending e-mail from their browsers. Security Manager also issues certificates to Web servers to enable secure communications with Web browsers. Figure 1 on page 15 shows a high-level view of the role that Enrollment Server for Web plays in distributing Web certificates to applications over a network.

Figure 1: Role of Enrollment Server for Web



What is Enrollment Server for WAP?

Enrollment Server for WAP, which is installed as part of the Enrollment Server for Web, distributes WTLS certificates to WAP devices such as WAP servers, cellphones, pagers, and so on.

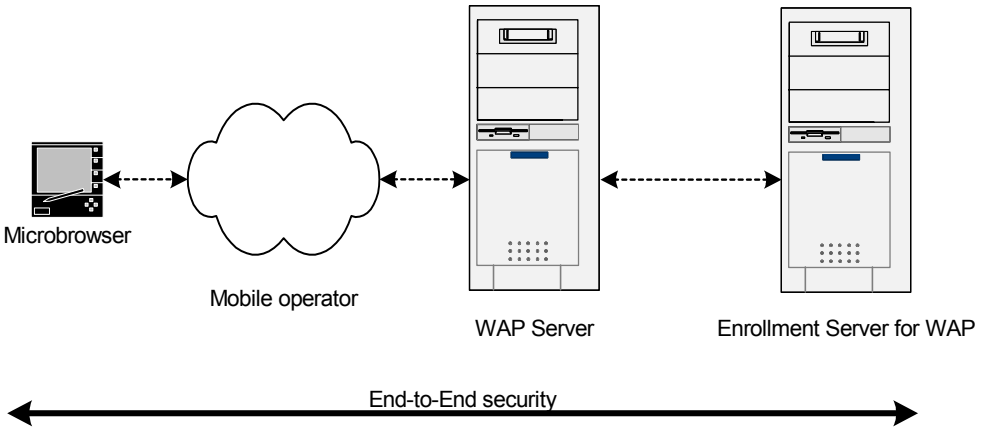
Wireless Application Protocol, or WAP, is the standard protocol for enabling secure wireless transactions. It enables users to receive Internet content (Web sites) and software applications (such as e-mail) securely on WAP devices.

A WTLS certificate is any certificate that allows you to create a secure connection between your WAP server and a mobile device.

This document includes a "Glossary" on page 107 describing many key terms used in the WAP industry.

Figure 2 illustrates the Entrust wireless security solution.

Figure 2: The Entrust wireless security solution



Chapter 2

Installing Enrollment Server for Web

This chapter describes how to install Enrollment Server for Web.

Topics in this chapter:

Overview

The chapter provides instructions on installing or upgrading the Enrollment Server for Web. To install and configure Enrollment Server for Web, complete the steps outlined in the following worksheet.

Step...	Instructions found here...	Completed
1. Prepare your environment for installation.	"Preparing for installation" on page 20	
2. Install Enrollment Server for Web.	"Installing Enrollment Server for Web" on page 17 If you are upgrading from 5.1, complete "Upgrading from 5.1 to 7.0" on page 25 instead.	
3. Configure the Web server hosting Enrollment Server for Web by creating the document and CGI directory aliases.	"Post-installation tasks" on page 27	
4. Access the Web pages to ensure you have properly installed Enrollment Server for Web.	"Accessing the Enrollment Server" on page 33	
5. Issue a certificate for the Web server hosting the Enrollment Server for Web.	• "Creating a Web server or user entry" on page 39 • "Generating a certificate request (CSR)" on page 42 • "Submitting the certificate request" on page 49 • "Importing Web server certificates" on page 50	
6. For server authentication, enable SSL or TSL on the Web server hosting Enrollment Server for Web.	"Enabling SSL and TLS" on page 58	

Step...	Instructions found here...	Completed
7. For server or client authentication and data encryption, install the CA certificate on the Web server hosting the Enrollment Server for Web and the Web browser. To validate the certificate for the Web server hosting the Enrollment Server for Web, install the CA certificate in the browser administering Enrollment Server for Web.	"Issuing CA certificates" on page 55	
8. Optional. Customize Enrollment Server for Web. For example, modify the HTML template pages, or configure Enrollment Server to support cross-certified CAs.	"Customizing Enrollment Server for Web" on page 89	
9. Distribute certificates.	• "Issuing certificates for Web servers and browsers" on page 37 • "Issuing certificates for computers, devices, and Windows® servers" on page 71 • "Issuing certificates for WAP servers" on page 79	

Preparing for installation

Before you install the Enrollment Server for Web, ensure you have completed the pre-installation tasks shown in the following checklist.

After completing the tasks in the checklist, proceed to "Installing the Enrollment Server for Web" on page 21.

Table 1: Pre-installation checklist

Have you...	For details, see...	Completed
Installed and configured the Security Manager?	"Entrust Authority Security Manager 7.0 guides" on page 6	
Updated the machine to meet system requirements (memory, Web server, Web browser, and so on)?	*Enrollment Server for Web 7.0 ReadMe*	
Ensured the machine on which you are about to install Enrollment Server for Web can communicate with Security Manager?	"Ensuring connectivity" on page 20	
Logged in as a root user with appropriate read/write permissions?	Your operating system documentation. Ensure you have read/write permissions on the directory in which you will install Enrollment Server for Web.	

Ensuring connectivity

Before you install Enrollment Server for Web, ensure the machine that will host Enrollment Server for Web can connect to the machine that hosts Security Manager.

To check connectivity, ping the Security Manager machine or use the telnet utility.

Attention: For security reasons, do not install Enrollment Server for Web on the same machine as Security Manager.

Installing the Enrollment Server for Web

Complete the following procedures to download and install Enrollment Server for Web.

Topics in this section:

Downloading the installation files

Follow the instructions below to download the Enrollment Server installation files for Windows and UNIX.

To download the installer

1 Browse to the downloads page on the Entrust Customer Support Web site. You should have received an e-mail from Entrust that included:

- instructions on how to access the downloads page
- your user ID and password required to access the downloads page

2 Save one of the following files, depending on your operating system, to any directory on the machine that will host the Enrollment Server:

- `EnrollmentServer70Win32.exe`
- `EnrollmentServer70Sol.bin`
- `EnrollmentServer70HPUX.bin`

Attention: If you are using FTP to transfer the file to your UNIX machine, set the transfer method to binary.

You have finished downloading the Enrollment Server for Web installer.

3 Choose one of the options shown in the following table.

If...	Refer to...
The machine supports the GUI installer (for example, Windows)	"Installing Enrollment Server using the GUI installer" on page 22
The machine does not support a GUI	"Installing Enrollment Server using the command-line installer" on page 23

Installing Enrollment Server using the GUI installer

Complete the procedure in this section to install the Enrollment Server for Web on a Windows® machine or on a UNIX® machine that supports GUI installers.

Attention: The installer assumes that your system uses the default TCP ports for HTTP (80) or HTTPS (443) for your Web server. If it does not, complete "To configure Internet Shortcuts for non-default ports" on page 34 after installation.

To install the Enrollment Server using the GUI installer

1. Open the temporary folder to which you have downloaded or extracted the installation file.
2. Complete one of the following:
   - on Windows, double-click the `EnrollmentServer70Win32.exe` executable
   - on UNIX, enter one of the following commands, depending on your operating system:

     `./EnrollmentServer70Sol.bin`

     `./EnrollmentServer70HPUX.bin`

   The Welcome dialog box appears.
3. Proceed through the Enrollment Server installer until you come to the Security Manager information dialog box.
4. Enter the Security Manager information in the appropriate fields. You can find these values in the `entrust.ini` file that was created during the Security Manager installation.

   When you enter the distinguished name, copy the entire name from the `entrust.ini` file starting with `o=`.
5. Click **Next**.

   The Web Server IP Address dialog box appears.
6. Enter the Web server's IP address or fully qualified domain name (for example, "`www.myserver.com`"). Use the IP address of the machine on which you are installing Enrollment Server for Web.
7. Proceed through the remainder of the Enrollment Server for Web installer.

   You have installed the Enrollment Server for Web software.

   Proceed to "Post-installation tasks" on page 27.

Installing Enrollment Server using the command-line installer

Complete the procedure in this section to install the Enrollment Server for Web on a UNIX machine using the command-line installer.

Attention: The installer assumes that your system uses the default TCP ports for HTTP (80) or HTTPS (443) for your Web server. If it does not, complete "To configure Internet Shortcuts for non-default ports" on page 34 after installation.

To install Enrollment Server using the command-line installer

1. Change to the directory where you extracted the Enrollment Server for Web installation files.

   For example:

   ```
   cd /opt/ESweb
   ```

2. Execute one of the following commands, depending on your operating system, to run the installer:

   ```
   ./EnrollmentServer70Sol.bin -console
   ```

   ```
   ./EnrollmentServer70HPUX.bin -console
   ```

3. Proceed through the Enrollment Server installer until you are asked for Security Manager and Directory information.
4. Type the Security Manager and Directory information as follows:
   - the Distinguished Name of the Security Manager

Note: When you enter the distinguished name, copy the entire name from the `entrust.ini` file starting with `o=`.

   - the IP address or fully qualified domain name (for example, `www.myserver.com`) of the machine hosting the Security Manager
   - the port at which Security Manager is listening (by default, 709)
   - the IP address or fully qualified domain name of the machine hosting the Directory
   - the port at which the Directory is listening (by default, 389)

   You can find these values in the `entrust.ini` file that was created during the Security Manager installation.
5. Type the Web server's IP address or fully qualified domain name. Use the name of the machine on which you are installing Enrollment Server for Web.

6 Proceed through the remainder of the Enrollment Server for Web installer.

You have installed the Enrollment Server for Web software.

Proceed to "Post-installation tasks" on page 27.

Upgrading from 5.1 to 7.0

If you have previously installed the Enrollment Server for Web 5.1 (formerly known as Entrust/WebConnector), you can upgrade the software without uninstalling 5.1 and re-installing 7.0.

During the upgrade the installer creates a new directory structure in your previous installation directory (by default `/Entrust/WebConnector`) and updates all files except for the following:

- `<ES_web_root>/docs/config/clientcgi.ini` configuration file
- the following Internet Shortcuts located in the `<ES_web_root>/docs` directory:
  - `cda`
  - `cdas`
  - `wapcda`
  - `wapcdas`
- any log files in the `<ES_web_root>/log` directory
- any files in the `<ES_web_root>/certs` folder

Note: Before running the Enrollment Server for Web 7.0 installer, ensure you have updated Security Manager to 7.0 and completed all other tasks listed in "Preparing for installation" on page 20.

To run the upgrader, complete the instructions in the "Installing the Enrollment Server for Web" on page 21 section. The installer will not ask you for Security Manager information, because the connection to your PKI is already established.

After installation, you do not need to update the alias directories you have already created on the Web server that point to the `<ES_web_root>/cgi` or `<ES_web_root>/docs` folder. You also do not need to re-issue any certificates.

Chapter 3

Post-installation tasks

This chapter describes how to define the document and CGI directories for Enrollment Server for Web using the Web server application, and how to access your Enrollment Server for Web HTML pages.

Topics in this chapter:

Configuring the Web server hosting the Enrollment Server

Complete the task in this section that applies to the Web server hosting the Enrollment Server for Web. These procedures ensure your Web server can access the CGI scripts and documents installed with Enrollment Server for Web.

If you are upgrading from a previous version of Enrollment Server for Web, you do not have to complete this procedure.

Topics in this section:

Configuring Microsoft® IIS

To configure IIS 5.0 or 6.0 for Enrollment Server for Web, complete the following tasks:

- add the CGI virtual directory (see "To add the CGI virtual directory" on page 28)
- add the document virtual directory (see "To add the document virtual directory" on page 29)

To add the CGI virtual directory

1. Start the Internet Service Manager (**Start > Programs > Administrative Tools > Internet Service Manager**).
2. In the tree view, under the **DNS name** folder, right-click **Default Web Site**.
3. Click **New > Virtual Directory** in the pop-up menu.

   The IIS Virtual Directory Creation Wizard prompts for an alias, a path, and the type of permissions that are required for the virtual directory.
4. Set the alias to "`cda-cgi`" in the **Alias** field.
5. Set the path to "`Drive:\<ES_for_Web_root>\cgi`" in the **Path** field. For example, "`c:\Program Files\Entrust\Enrollment Server for Web\cgi`".
6. Ensure the following permissions are selected:
   - **Read**
   - **Run scripts**
   - **Execute**

7 Click **Next** and then **Finish**.

You have created the CGI virtual directory. The directory is placed in the **Default Web Site** folder. Proceed to "To add the document virtual directory" on page 29.

To add the document virtual directory

1 Go back to the Internet Service Manager.

2 In the tree view, under the **DNS name** folder, right-click **Default Web Site**.

3 Click **New > Virtual Directory** in the pop-up menu.

The IIS Virtual Directory Creation Wizard prompts for an alias, a path, and the type of permissions that are required for the virtual directory.

4 Set the alias to "`cda-docs`" in the **Alias** field.

5 Set the path to "`Drive:\<ES_for_Web_root>\docs`" in the **Path** field. For example, "`c:\Program Files\Entrust\Enrollment Server for Web\docs`".

6 Ensure the following permissions are selected:

- **Read**
- **Write**

7 Click **Next** and then **Finish**.

8 Save the settings and exit the Internet Service Manager.

You have created the document virtual directory. Proceed to "Accessing the Enrollment Server" on page 33.

Configuring Sun™ ONE

To configure the Sun ONE Web server for Enrollment Server for Web, complete the following tasks:

- add the CGI alias directory (see "To add the CGI alias directory" on page 29
- add the documentation alias directory (see "To add the document alias directory" on page 30)

To add the CGI alias directory

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

2 Choose the Web server which will manage Enrollment Server for Web and click **Manage**.

3 Click **Class Manager**.

4 Select the **Programs** tab.

5 In the **URL prefix** field, enter "`cda-cgi`". Do not preface "`cda-cgi`" with a slash.

6 In the **CGI Directory** field, enter the path of your CGI directory. For example:

```
c:\Program Files\Entrust\Enrollment Server for Web\cgi
```

7 Click **OK**, and then click **OK** again.

8 Apply your changes.

9 Ensure that the Enrollment Server for Web has execute access to this CGI directory.

You have now added the CGI alias directory. Proceed to "To add the document alias directory" on page 30.

To add the document alias directory

1 Select the **Content Mgmt** tab.

2 In the left frame, click **Additional Document Directories**.

3 In the **URL prefix** field, enter "`cda-docs`". Do not preface "`cda-docs`" with a slash.

4 In the **Map to Directory** field, enter the location of your Enrollment Server for Web HTML templates. For example:

```
c:\Program Files\Entrust\Enrollment Server for Web\docs
```

5 Click **OK**, and then click **OK** again.

6 Apply your changes.

7 Ensure that the Enrollment Server for Web has read access to this document directory.

You have now added the document alias directory.Proceed to "Accessing the Enrollment Server" on page 33.

Configuring Red Hat® Stronghold

To configure the Stronghold Web server for Enrollment Server for Web, complete the following task.

To add the CGI and document directories

1. Locate the `httpd.conf` file for Stronghold.
2. Open the `httpd.conf` file using any text editor.
3. Add the following two lines to the `httpd.conf` file:

   ```
   ScriptAlias /cda-cgi/ "<ES_for_Web_root>/cgi"
   Alias /cda-docs/ "<ES_for_Web_root>/docs"
   ```

   where `<ES_for_Web_root>` is the complete path to the directory. For example, `/opt/entrust/enrollmentserver`.
4. Save your changes.
5. Restart the Web server.

You have created two alias directories: the CGI directory and the document directory. Proceed to "Accessing the Enrollment Server" on page 33.

Configuring IBM® HTTP Server

To configure the IBM HTTP Server for Enrollment Server for Web, complete one of the following tasks:

- "To add the CGI and document alias directories using the Administration GUI" on page 31
- "To add the CGI and document alias directories manually" on page 32

To add the CGI and document alias directories using the Administration GUI

1. Open the IBM HTTP Server Administer Web server page.
2. In the left frame called "**IBM Administration Server**", select **Mappings**.
3. Click **Aliases**.
4. Under "**Defined aliases**", click **Add**.
5. In the **Alias** field, enter "`/cda-docs/`". Ensure you enter the preceeding and succeeding slashes.
6. In the **Actual Directory or filename** field, enter the path to your `<ES_for_Web_root>\docs` directory. For example:

   ```
   /c:\Program Files\Entrust\Enrollment Server for Web\docs/
   ```

Note: Ensure you include the preceeding and succeeding slashes.

7 Click **Close**.

8 Under "**Defined aliases for directories containing scripts**", click **Add**.

9 In the **Alias** field, enter "`/cda-cgi/`". Ensure you enter the preceeding and succeeding slashes.

10 In the **Actual Directory or filename** field, enter the path to your `<ES_for_Web_root>\docs` directory. For example:

```
/c:\Program Files\Entrust\Enrollment Server for Web\cgi/
```

Note: Ensure you include the preceeding and succeeding slashes.

11 Click **Close**.

12 Click **Submit**.

13 Restart the Web server.

You have created two alias directories: the CGI directory and the document directory. Proceed to "Accessing the Enrollment Server" on page 33.

To add the CGI and document alias directories manually

1 Locate the `httpd.conf` file for IBM HTTP Server.

2 Open the `httpd.conf` file using any text editor.

3 Add the following two lines to the `httpd.conf` file:

```
ScriptAlias /cda-cgi/ "/<ES_for_Web_root>/cgi/"
Alias /cda-docs/ "/<ES_for_Web_root>/docs/"
```

where `<ES_for_Web_root>` is the complete path to the directory. For example, `c:/Program Files/Entrust/Enrollment Server for Web.`

4 Save your changes.

5 Restart the Web server.

You have created two alias directories: the CGI directory and the document directory. Proceed to "Accessing the Enrollment Server" on page 33.

Accessing the Enrollment Server

You can access the Enrollment Server for Web and the Enrollment Server for WAP pages in three different ways:

- from a Web browser (see "Accessing the Enrollment Server from a Web browser" on page 33)
- from an Internet Shortcut (see "Accessing the Enrollment Server from an Internet Shortcut" on page 34)
- from the Start menu (see "Accessing the Enrollment Server from the Start Menu" on page 35)

If you cannot access your Enrollment Server for Web using one of the following URLs, ensure that:

- your Web server is running
- you have created the required aliases for the Enrollment Server directories
- you have restarted the Web server if necessary.

Check your Web server to ensure it is functioning properly and listening at the port you have specified. Also check connectivity between the Enrollment Server for Web and the Security Manager.

Accessing the Enrollment Server from a Web browser

To access the home pages for the Enrollment Server for Web or the Enrollment Server for WAP, type in one of the following URLs in a Web browser:

- URL for Enrollment Server for Web:

  `http<s>://<yourserver.domain.com>:<port>/cda-cgi/clientcgi.<exe>?action=start`

- URL for Enrollment Server for WAP:

  `http<s>://<yourserver.domain.com>:<port>/cda-cgi/clientcgi.<exe>?action=wapstart`

where:

- *https* is used if you have enabled SSL
- *<yourserver.domain.com>* is the name or IP address of the server
- *<port>* is the port number. Specify the port number if it is different from the default 80 or 443 port numbers.
- *<exe>* is used on Windows only

Accessing the Enrollment Server from an Internet Shortcut

During installation, four URL files are created in the <ES_for_Web_root>\docs folder. You can use the following files to access the Enrollment Server for Web or Enrollment Server for WAP:

- cda

  Opens the Enrollment Server for Web home page if you have not enabled SSL.

- cdas

  Opens the Enrollment Server for Web home page if you have enabled SSL.

- wapcda

  Opens the Enrollment Server for WAP home page if you have not enabled SSL.

- wapcdas

  Opens the Enrollment Server for WAP home page if you have enabled SSL.

If your Web server is listening at a port other than 80 or 443, you need to modify these files. To modify these files, complete the following task.

To configure Internet Shortcuts for non-default ports

1. Open the Enrollment Server for Web Internet Shortcut you are using in any text editor. For example, open either <ES_for_Web_root>/docs/cda or <ES_for_Web_root>/docs/cdas.
2. Add the port number after your Web server name or IP address. For example, change:

   ```
   http://webserverA.yourCompany.com/cda-cgi/clientcgi.exe?
   action=start
   ```

   to:

   ```
   http://webserverA.yourCompany.com:88/cda-cgi/clientcgi.exe?
   action=start
   ```

3. Save your changes.
4. Open the Enrollment Server for WAP Internet Shortcut you are using in any text editor. For example, open either <ES_for_Web_root>/docs/wapcda or <ES_for_Web_root>/docs/wapcdas.
5. Repeat Step 2 and Step 3 for this Internet Shortcut.

Accessing the Enrollment Server from the Start Menu

You can also access the Internet Shortcut files located in the `<ES_for_Web_root>\docs` directory through the Windows Start menu.

The following options are available from **Start > Programs > Enrollment Server for Web**:

- Enrollment Server for WAP (non-secure site)

  Opens the Enrollment Server for WAP home page if you have not enabled SSL.

- Enrollment Server for WAP (secure site)

  Opens the Enrollment Server for WAP home page if you have enabled SSL.

- Enrollment Server for Web (non-secure site)

  Opens the Enrollment Server for Web home page if you have not enabled SSL.

- Enrollment Server for Web (secure site)

  Opens the Enrollment Server for Web home page if you have enabled SSL.

If the Web server located on the Enrollment Server machine does not listen at the default 80 or 443 ports, complete "To configure Internet Shortcuts for non-default ports" on page 34 to point the Enrollment Server to the correct port.

Uninstalling the Enrollment Server

To uninstall the Enrollment Server for Web on UNIX, go to the `<ES_for_Web_root>/_uninst` directory and run the uninstaller executable.

On Windows, go to **Start > Control Panel > Add or Remove Programs** and remove "Entrust Authority Enrollment Server for Web".

Uninstalling the Enrollment Server does not remove any files located in the `<ES_for_Web_root>/certs` or `/log` directory, nor does it delete the certificates you have issued. For instructions on removing any of the certificates you have distributed using Enrollment Server for Web or Enrollment Server for WAP, refer to the documentation of that machine, Web browser, or device.

Uninstalling Enrollment Server for Web also uninstalls Enrollment Server for WAP.

Chapter 4

Issuing certificates for Web servers and browsers

This chapter describes how to obtain certificates for Web servers (including the one hosting Enrollment Server for Web) and for users' Web browsers.

Topics in this chapter:

Overview

This chapter provides instructions for obtaining Web server and Web browser certificates. The following sections explain when you would issue certificates to Web browsers and Web servers, and which tasks in this chapter to complete.

Issuing Web server certificates

To obtain certificates for your Web server so that you can enable SSL or S/MIME, perform the following tasks in sequence:

- "Creating a Web server or user entry" on page 39
- "Generating a certificate request (CSR)" on page 42
- "Submitting the certificate request" on page 49
- "Importing Web server certificates" on page 50
- Optional. "Enabling SSL and TLS" on page 58

You must issue a certificate for the Web server which hosts the Enrollment Server for Web.

Issuing Web browser certificates

To obtain certificates for Web browsers to enable client authentication, complete the following tasks in sequence:

- "Creating a Web server or user entry" on page 39
- "Importing Web browser certificates" on page 52

In order for your users to use Enrollment Server for Web to issue certificates, they must have a browser certificate.

Creating a Web server or user entry

You need a reference number and authorization code (together called "activation codes") from Security Manager Administration for each new certificate request. To create an activation code, create a Web server or user entry.

Topics in this section:

Guidelines for adding new users

The following guidelines apply when you are adding new users using Security Manager Administration:

- If you are using a Sun ONE Web server, do not use a serial number in the DN because the Web server will not work properly.
- A single identity cannot be set up as both a Web user and a user. You need to create two separate identities for such users. Entrust recommends that you store the Web users in a different search base than the users.

Note: This guide assumes that you are using Security Manager Administration to add new users. If you are using Entrust Authority Administration Services, refer to its documentation for instructions.

Creating Web server and user entries

Complete the procedure below that applies to you:

To create a Web server entry

1. Log in to Security Manager Administration as an administrative user.
2. Click **Users > New User**.

   The **New User** dialog box opens.
3. In the **Naming** property page, **Person** appears in the **Type** list, by default. Click the arrow and choose **Web server.**
4. Type your server's fully qualified domain name in the **Name** field, for example "`www.myserver.com`".

5 Optionally, type a description of the Web server in the **Description** field.

6 In the **Add to** list, select the search base under which the Web server will be added. By default, **CA Domain Searchbase** is listed first and is often the top level searchbase in an organization. For details on search bases, refer to the Security Manager documentation (see "Related Entrust documentation" on page 6).

7 Click the **Certificate** property page.

8 Click **Category** and select **Web**.

9 In the **Type** list, click **Web server**.

10 Optionally, if the certificate extension fields are displayed, type the certificate extension variables into the fields. If you don't have this information, or need additional information, refer to the Security Manager documentation.

11 Click **OK**.

The **Operation Completed Successfully** dialog box opens. This dialog box displays the Web server's reference number and authorization code.

12 Record the reference number and authorization code.

Note: If you exit Security Manager Administration now and restart it later, you will not see the user (that is, the Web server) you added in the above procedure in the **User** list. This absence does not mean that the server entry is gone. To see it, right-click **Users** and click **New Search** in the pop-up menu. Accept all the default values in the **New Search** dialog box, and then click **Find** to update the display.

You have now created a user entry for the Web server and have obtained its reference number and authorization code. Use these activation codes to obtain a Web server certificate.

Proceed to "Generating a certificate request (CSR)" on page 42.

To create a user entry

1 Log in to Security Manager Administration as an administrative user.

2 Click **Users > New User**.

The **New User** dialog box opens.

3 In the **Naming** property page, **Person** appears in the **Type** list, by default. If it does not, click the arrow and select **Person**.

4 In the **First Name** and **Last Name** fields, type the user's first and last names, respectively.

5 Optionally, in the **Serial Number** and **Email** fields, type the user's serial number (for example, the employee number) and e-mail address.

To let users send encrypted e-mail using Enrollment Server for Web and S/MIME-compatible e-mail applications, the **Use e-mail (subjectAltName)** value under **Security Policy** in the tree view must read either "`mail`" or "`rfc822mailbox`". The default setting is "`mail`". For more information, refer to the Security Manager documentation (see "Related Entrust documentation" on page 6).

6 In the **Add to** list, select the searchbase under which the user belongs. By default, **CA Domain Searchbase** is listed first and is often the top level searchbase in an organization. For details on search bases, refer to the Security Manager documentation.

7 Click the **Certificate** property page.

8 Click **Category** and select **Web**.

9 In the **Type** list, click **Default**.

10 Click **OK**.

The **Operation Completed Successfully** dialog box opens. This dialog box displays the activation codes for this certificate request.

11 Record the reference number and authorization code.

Note: If you exit Security Manager Administration now and restart it later, you will not see the user you added in the **User** list. This absence does not mean that the user entry is gone. To see it, right-click **Users** and click **New Search** in the pop-up menu. Accept all the default values in the **New Search** dialog box, and then click **Find** to update the display.

You have now created a user entry and have obtained a reference number and authorization code. Use these activation codes to obtain browser certificates for users.

Proceed to "Importing Web browser certificates" on page 52.

Generating and submitting certificate requests

This section provides instructions on how to generate a Web server certificate and submit it to Security Manager using Enrollment Server for Web.

Topics in this section:

Generating a certificate request (CSR)

After you obtain activation codes for your Web server, you can issue the Web server a certificate, called a Web server certificate, using Enrollment Server for Web. To install the Web server certificate into the Web server, you must generate a pair of cryptographic keys and a certificate signing request (CSR). The CSR contains information that Security Manager uses to create the Web server certificate.

Follow the instructions that apply to your Web server to generate a certificate request:

To generate keys and a CSR on Microsoft® IIS

1. On the machine hosting the Web server, open the Internet Services Manager (click **Start > Programs > Administrative Tools > Internet Service Manager**).
2. Right-click **Default Web Site** and click **Properties** in the pop-up menu.
3. Click **Directory Security** in the dialog box that opens.
4. Under **Secure Communications**, click **Server Certificate**.

   The **Web Server Certificate Wizard** appears.
5. Click **Next**.
6. Click **Create a new certificate**, then click **Next**.
7. Ensure that **Prepare request now, but send it later** is selected and click **Next**.
8. 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 will receive a warning stating that the certificate name does not match the name of the Web server.

9 In the **bit length** list, select a bit length no greater than 2048 bits.

If you choose a bit length less than 768, your certificate lasts for 12 months, by default. If you are using a key between 768 and 2048 bits, your certificate lasts for 24 months, by default. If you customize the lifetime of the certificate in Security Manager, you cannot exceed these default values.

10 In the **Organization and Organizational unit** fields, enter your organization and department names, respectively.

11 In the **Common Name** field, enter the reference code you obtained for the Enrollment Server for Web and click **Next**.

12 Fill out the **Country/Region**, **State/Province**, and **City/Locality** fields and click **Next**.

13 Ensure that the time zone is correct and click **Next**.

14 In the **File name** field, use the default, or enter a new path and file name for the file that will contain the Web server certificate request.

15 Click **Next**.

The **File Summary** dialog box opens.

16 Click **Next**, then **Finish**, then **OK** to generate the CSR.

The CSR is saved in the file you specified in Step 14.

17 Open the file. It should look similar to this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuYzIubmV0
MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L
JPsdfCsjqRs8ygoyaw4ucOEdx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBB
AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfsI
Qs5JRNagVBW
-----END NEW CERTIFICATE REQUEST-----
```

18 Copy the CSR to the clipboard, including the BEGIN and END lines.

You have generated a certificate request and copied it to the clipboard. Proceed to "Submitting the certificate request" on page 49.

To generate keys and a CSR on Sun™ ONE

1. Open the **Sun ONE Administer Web Server** page.
2. Choose the Web server which will 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**.

   The **Request a Certificate** dialog box opens.
6. 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 in "Creating a Web server or user entry" on page 39.
10. Fill out the remaining fields and click **OK**.

    A PKCS-10 request is created and should look something like this:

    ```
    -----BEGIN NEW CERTIFICATE REQUEST-----
    MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
    YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
    SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuYzIubmV0
    MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L
    JPsdfCsjqRs8ygoyaw4ucOEdx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBB
    AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfsI
    Qs5JRNagVBW
    -----END NEW CERTIFICATE REQUEST-----
    ```
11. Copy the entire certificate request to the clipboard, including the BEGIN and END lines.

    You have generated a certificate request and copied it to the clipboard. Proceed to "Submitting the certificate request" on page 49.

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>
   ```

   genkey prints the filenames and locations of the key file and certificate file it is about to generate.

The key is stored in:

```
# <ServerRoot>/ssl/private/<hostname>.key
```

The certificate is stored in:

```
# <ServerRoot>/ssl/certs/<hostname>.cert
```

2 Press the Enter key.

genkey reminds you not to overwrite an existing key pair and certificate.

3 Press the Enter key.

genkey prompts you to specify the size of the key.

4 Enter a key size between 512 or 1024 bits.

Note: If you choose a key length less than 768, your certificate lasts for 12 months, by default. If you choose a key between 768 and 1024 bits, your certificate lasts for 24 months, by default. If you customize the lifetime of the certificate in Security Manager, you cannot exceed these default values.

---

genkey 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
```

genkey generates the key pair and saves it in the following location:

```
# ServerRoot/ssl/private/hostname.key
```

genkey asks if you want to use the genreq utility to send a CSR.

6 Type "Y" to send a CSR.

The genreq utility is launched automatically. genreq 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. Refer to Security Manager documentation (see "Related Entrust documentation" on page 6) for a complete list of country codes.

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

- the fully-qualified domain name of your Web site, for example "www.myserver.com".

genreq generates the CSR, which looks something like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuYzIubmV0
MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L
JPsdfCsjqRs8ygoyaw4ucOEdx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBB
AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfsI
Qs5JRNagVBW
-----END NEW CERTIFICATE REQUEST-----
```

10 Copy the entire CSR to the clipboard, including the BEGIN and END lines.

You have generated a certificate request and copied it to the clipboard. Proceed to "Submitting the certificate request" on page 49.

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 then click **New**.

3 In the **Password Prompt** dialog box, enter a new password and click **OK**. Ensure you select the "**Stash the Password to file**" option to create the key.sth file.

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

5 Click **OK**.

6 Select **Create** from the main User Interface, and then click **New Certificate Request**.

The **New Key and Certificate Request** dialog box opens.

7 Enter information in the fields as described in Table 2 below:

Table 2: Key and CSR information

Field	Description
Key Label	Enter a descriptive comments that will identify the key and certificate in the database.
Keysize	Enter a size for the key between 512 and 1024 bits. If you choose a key length less than 768, your certificate lasts for 12 months, by default. If you choose a key between 768 and 1024 bits, your certificate lasts for 24 months, by default. If you customize the lifetime of the certificate in Security Manager, you can not exceed these default values.
Common Name	Enter the reference number obtained from the Security Manager Administration in "Creating a Web server or user entry" on page 39.
Organization Name	Enter the name of your organization.
Organization Unit	Optional. Enter the ou= (unit of your organization that the Web server belongs to) value.
Locality	Optional. Enter the locale of your organization.
State/Province	Optional. Enter the state or province of your organization.
Zipcode	Optional. Enter the zip or postal code of your organization.

Table 2: Key and CSR information

Field	Description
Country	Enter the two-letter code for your country. For example, enter "US" for the United States, "DE" for Germany or "JP" for Japan. Refer to Security Manager documentation (see "Related Entrust documentation" on page 6) for a complete list of country codes
Certificate request filename	Enter a new name for the certificate request file, or use the default file name.

8 Click **OK**.

9 In the **Information** dialog box, click **OK**.

The certificate request file, when opened, should look similar to this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBEzCBzgIBADB7MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5p
YTEQMA4GA1UEBxMHT2FrbGFuZDEbMBkGA1UEChMSQzJOZXQgU29mdHdhcmUg
SW5jMRAwDgYDVQQLEwdUZXN0aW5nMRYwFAYDVQQDEw1nYWJiZXIuYzIubmV0
MEwwDQYJKoZIhvcNAQEBBQADOwAwOAIxAJukoQhq4LanG2k+LnRTGJAcgv9L
JPsdfCsjqRs8ygoyaw4ucOEdx+WdnM0x36NcQIDAQABMA0GCSqGSIb3DQEBB
AUAAzEABRLR6IkG70oNG1MnvuMDeWou4kIvc98ysjssCNKsDKsHAXBSEbfsI
Qs5JRNagVBW
-----END NEW CERTIFICATE REQUEST-----
```

10 Copy the entire CSR to the clipboard, including the BEGIN and END lines.

You have generated a certificate request and copied it to the clipboard. You can now paste the certificate request into Enrollment Server for Web to generate a certificate. Proceed to "Submitting the certificate request" on page 49.

Submitting the certificate request

After generating a Web server certificate request (CSR) for the Web server, submit the certificate request to Security Manager through Enrollment Server for Web.

To submit the request

1. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **Certificates** menu on the left, click **Web server**.

   The **Web server Certificate Request** page opens.
3. Enter the reference number and authorization code for the Web server that you obtained while completing the following procedure: "To create a Web server entry" on page 39.
4. In the **Options** field, choose the format for the Web server certificate. The choices are:
   - raw Distinguished Encoding Rules (DER) format

     DER format displays the certificate in raw text format.
   - Public-Key Cryptographic Standard #7 (PKCS7).

     PKCS7 displays the certificate with mark-up tags.

   To determine which option to choose, find out how your Web server processes certificates. For more information, consult your Web server documentation.
5. Paste the certificate request that you copied to the clipboard into the large text box.
6. Click **Submit Request**.

   Security Manager generates a Web server certificate and sends it to Enrollment Server.
7. Do one of the following depending on your browser:
   - If you are using Netscape, copy the entire certificate to the clipboard. Proceed to "Importing Web browser certificates" on page 52.
   - If you are using Internet Explorer:
     – click **Download** on the page displaying your certificate.
     – 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**.

     The certificate is saved in the text file you specified. Proceed to "Importing Web server certificates" on page 50.

Importing certificates

This section provides instructions for importing Web server and Web browser certificates.

Topics in this section:

Importing Web server certificates

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

To import the Web server certificate on Microsoft® IIS

1. Open the Internet Services Manager (click **Start > Programs > Administrative Tools > Internet Service Manager**).
2. In the tree view, right-click **Default Web Site** and click **Properties** in the pop-up menu.
3. Click the **Directory Security** tab.
4. Under **Secure Communications**, click **Server Certificate**.

   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 certificate and click **Next**.
8. 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 the Web server which will manage Enrollment Server for Web and click **Manage**.
3. Click the **Security** tab.
4. Click **Install Certificate**.

5 In the **Certificate For** frame, select **This Server**.

6 Enter your **Key Pair File Password**.

7 Select **Message Text (with headers)**.

8 In the **Message Text (with headers)** field, paste the entire certificate that you downloaded.

9 Click **OK**.

The **Add Server Certificate** Web page appears.

10 Click **Add Server Certificate**.

You have imported the Web server certificate into the Entrust database on your Web server.

To import the Web server certificate on Red Hat® Stronghold

1 Paste the Web server certificate that you just copied to the clipboard into any text editor.

2 Save the file.

3 Run Stronghold's `getca` utility, specifying the name of the host that owns this certificate and providing the certificate file 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`.

4 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 4 of "To generate keys and a CSR on IBM® HTTP Server" on page 46.

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 46.

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 a valid Base64-encoded file in the **Certificate filename** text field.

If the CA who issues your certificate is not a trusted CA in the key database you might be unable to import the certificate. To store the CA certificate and designate the CA as trusted, refer to "Issuing CA certificates" on page 55.

9 Click **OK**.

Importing Web browser certificates

To gain access to secure Web sites, Web browsers need to have a browser certificate. Browser certificates allow Web browsers to authenticate themselves to Web servers (including the Web server hosting your Enrollment Server).

The Enrollment Server for Web administrator should inform the Web browser users of the URL for the Enrollment Server for Web so that they can request their browser certificates.

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

Before importing the certificate, you might want to edit the available CSP types. To do so, refer to "Customizing the CSP list" on page 90.

To import a browser certificate

1 If you have not already done so, obtain a reference number and authorization code for each user. Refer to "To create a user entry" on page 40 for instructions.

2 Instruct the user to access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.

3 In the **Certificates** menu on the left, click **Web Browser**.

4 Enter the reference number and authorization code in the appropriate fields.

5 Do one of the following depending on your browser:

- If you are using Internet Explorer, select the appropriate cryptographic service provider (CSP) from the list in the **CSP** field. If you are installing the certificate on a smart card, select the smart card's CSP.

  Change the service provide (CSP) type from the **CSP type** list if required. The CSP list automatically changes to show the CSPs available for the selected type. Click **Submit Request**.

- If you are using Netscape, click **Submit Request**, then select the appropriate cryptographic module from the list. If you are installing the certificate on a smart card, select the smart card's cryptographic module.

6 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 64.

The requested browser certificate and the CA certificate for the issuing CA are imported into the user's Web browser. 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.

Chapter 5

Issuing CA certificates

To authenticate servers and clients, enable SSL and distribute the CA certificate to users' browsers and your Web servers. This chapter provides instructions for distributing the CA certificate.

Topics in this chapter:

Overview

This chapter outlines how to enable SSL and TLS and how to retrieve and import a CA certificate so that you can enable server and client authentication.

Note: If you installed a browser certificate and chose to import the CA certificate at the same time (see "To import a browser certificate" on page 52), you have already imported the CA certificate and do not have to complete the procedures in this section.

When to issue CA certificates

There are two scenarios in which CA certificates are necessary:

- when authenticating a server, the user's browser uses the CA certificate to verify the CA signature on the Web server certificate
- when authenticating a client, the Web server uses the CA certificate to verify the CA signature on the browser certificate.

Note: IIS Web servers also check the CRL to authenticate the user. See "Enabling CRL checking on Microsoft® IIS" on page 98 for details.

Users who connect to sites secured with Web server certificates issued by your CA must import your CA certificate into their browsers.

Note: If you are using cross-certified CAs, refer to "Supporting cross-certified CAs" on page 93 to configure Enrollment Server for Web to support this feature.

Enabling client authentication

To enable client authentication, you must:

- import the CA certificate for a trusted CA into the Web server hosting the Enrollment Server for Web and your users' browsers
- remove any untrusted CAs from the browsers or Web server

Complete the following tasks in this chapter to import the CA certificate into the Web server hosting the Enrollment Server for Web and your users' Web browsers:

- "Enabling SSL and TLS" on page 58
- "Distributing the CA certificate" on page 62
- "Retrieving and importing the CA certificate into a Web browser" on page 64
- "Retrieving and importing the CA certificate into the Web server" on page 66

Enabling server authentication

To enable server authentication, you must:

- import the CA certificate for a trusted CA into the Web server hosting the Enrollment Server for Web and other Web servers
- remove any untrusted CAs from the Web servers

Complete the following tasks in this chapter to import the CA certificate into the Web server hosting the Enrollment Server for Web and your other Web servers:

- "Enabling SSL and TLS" on page 58
- "Distributing the CA certificate" on page 62
- "Retrieving and importing the CA certificate into the Web server" on page 66

Enabling SSL and TLS

After you have imported a Web server certificate for the Web server hosting Enrollment Server for Web, the next step is to enable the SSL and TLS protocols. These protocols are necessary for the encryption of transmitted data and server authentication.

To enable SSL and TLS, first follow the instructions that apply to your Web server and then test the SSL/TLS implementation.

Topics in this section:

Enabling SSL and TLS on Microsoft® IIS

These instructions assume you will use SSL 3 and TLS 1 to secure sessions to the Web server.

To enable SSL and TLS on IIS

1. Open the Internet Service Manager (click **Start > Programs > Administrative Tools > Internet Service Manager**).
2. In the tree view, right-click **Default Web Site** and click **Properties** in the pop-up menu.

   The **Default Web Site** dialog box opens.
3. Click the **Directory Securities** tab.
4. Under **Secure Communications**, click **Edit**.
5. Select **Require secure channel (SSL)** and click **OK**.

Note: To minimize the possibility that your Enrollment Server for Web installation might be compromised, Entrust recommends that you configure your server to use 128-bit encryption for SSL sessions. This configuration only allows browsers that support 128-bit encryption to connect to your secure server. The majority of browsers today support 128-bit encryption. To enable this setting, check **Encryption Settings.**

---

6. Click **OK**, and **OK** again to close all dialog boxes.

   The **Inheritance Overrides** dialog box opens.
7. Click **Select All**, and then click **OK**.

You have enabled SSL and as a result, TLS is automatically enabled. From now on, users and Enrollment Server for Web administrative users will have to visit the site using "`https`" in the URL instead of "`http`".

8 Test if you have enabled SSL by accessing Enrollment Server for Web using the HTTPS protocol. For further information, refer to "Accessing the Enrollment Server" on page 33.

Enabling SSL on Sun™ ONE

Before you can secure your Enrollment Server for Web, enable JavaScript in the Web browser used to administer that server.

Once you have enabled JavaScript, you are ready to enable SSL on your Enrollment Server for Web.

To enable SSL on Sun™ ONE

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

2 Choose the Web server which will manage Enrollment Server for Web and click **Manage**.

3 Click the **Preferences** tab.

4 In the left frame, click **Edit Listen Sockets**.

5 Set Security to **On**.

6 Accept the default port and click **OK**.

7 Save and apply your changes.

You have enabled SSL on your Enrollment Server for Web.

If you have not installed the CA certificate into your Enrollment Server for Web, you are asked to accept the CA certificate for this session or forever. You can choose to accept it for this session, and then install it later.

From now on, users and Enrollment Server for Web administrators must visit the site using "`https`" in the URL instead of "`http`".

8 Test if you have enabled SSL by accessing Enrollment Server for Web using the HTTPS protocol. For further information, refer to "Accessing the Enrollment Server" on page 33.

When logging in to the secure site, Sun ONE may generate a "**Certificate Name Check**" message. This message is generated because the site uses the fully qualified domain name (for example, `webserverA.yourCompany.com`), but the certificate contains the host name (for example, `webserverA`). You can ignore this message. If you enter the name correctly in Security Manager Administration, you do not see the message.

Enabling SSL and TLS on Red Hat® Stronghold

These instructions assume you will use SSL 3 and TLS 1 to secure sessions to the Web server.

To enable SSL and TLS on Red Hat® Stronghold

1. Open the Web server configuration file (`httpd.conf`) in any text editor.
2. In the `VirtualHost <hostname>:secure-port` section of the host's configuration file, enter the following line:

   ```
   # SSLFlag on
   ```

3. Enter the following command to enable SSL 3 and TLS 1:

   ```
   # SSLProtocol SSLv3 TLSv1
   ```

4. Save your changes.
5. Restart your Web server.

   From now on, users and Enrollment Server for Web administrators must visit the site using "`https`" in the URL instead of "`http`".
6. Test if you have enabled SSL by accessing Enrollment Server for Web using the HTTPS protocol. For further information, refer to "Accessing the Enrollment Server" on page 33.

Enabling SSL on IBM® HTTP Server

These instructions assume you will use SSL 3 to secure sessions to the Web server.

To enable SSL on IBM® HTTP Server

1. Open the Web server configuration file (`httpd.conf`) in any text editor.
2. Copy the following lines into the file, depending on your operating system:

   ```
   LoadModule ibm_ssl_module <ssl_library>
   Listen 443
   <VirtualHost _default_:443>
   ServerName <myserver.mydomain.com>
   DocumentRoot "<path_to_htdocs>"
   SSLEnable
   SSLClientAuth none
   </VirtualHost>
   SSLDisable
   ```

```
Keyfile "<path_to_key.kdb>"

SSLV2Timeout 100

SSLV3Timeout 1000
```

where:

- <*ssl_library*> is `modules/IBMModuleSSL128.dll` on Windows and `libexec/mod_ibm_ssl_128.so` on UNIX
- <*myserver.mydomain.com*> is the fully qualified name of the Web server
- <*path_to_htdocs*> is the complete path to the `htdocs` folder. For example: `<c:/program files/ibm http server/htdocs`
- <*path_to_key.kdb*> is the complete path to your key file. For example: `c:/program files/ibm http server/key.kdb`

3 Save your changes.

4 Restart your Web server.

From now on, users and Enrollment Server for Web administrators must visit the site using "`https`" in the URL instead of "`http`".

5 Test if you have enabled SSL by accessing Enrollment Server for Web using the HTTPS protocol. For further information, refer to "Accessing the Enrollment Server" on page 33.

Distributing the CA certificate

The Certification Authority (CA) certificate, also called the "root certificate", contains the verification public key of the CA. Web browsers and Web servers use the CA certificate to verify the CA signature on the certificates they receive when attempting to set up secure sessions.

Note: Most of the options for distributing the CA certificate work with most browsers. If you do not know whether an option will work with a particular browser, consult the browser documentation.

Distributing the certificate securely

The security between users is based on the trust each user has for the CA. Therefore, CA certificate distribution over the Web is not a secure way to establish trust. To improve trust, consider some of the following suggestions:

- Publish the CA certificate on a server that is authenticated by a Web server certificate. The Web server certificate is issued by another CA which the user already trusts.
- Compare the "fingerprint" (hash value) of the CA certificate to a fingerprint distributed to the end user in a secure manner (in this case the server need not be secure).
- Distribute the CA certificate on disk or from a trusted, secure, and well-known FTP site.
- Send the CA certificate in a signed message if there is a pre-existing trust relationship that you can use.

Distributing the CA certificate by diskette

The Enrollment Server for Web administrator saves the file"`cacert.der`" to diskette and distributes the diskette securely to browser users. To import the CA certificate into their browsers, users open the file as a URL (for example, "`file://a:\cacert.crt`"). The user's browser automatically imports the certificate.

Distributing an encrypted CA certificate by e-mail

The Enrollment Server for Web administrator encrypts the file "`cacert.der`" and sends it by way of e-mail. To import the CA certificate into their browsers, users decrypt the file, save it to their hard drive, and open it as a URL (for instance, they

would open the URL "`file://c:\cacert.crt`"). Their browsers will automatically import the certificate.

Distributing the CA certificate from a non-SSL server

The Enrollment Server for Web administrator distributes the CA certificate from a server that has SSL turned off. This may be an option if you are distributing the CA certificate to browsers within a secure Intranet behind a firewall.

Retrieving and importing the CA certificate into a Web browser

Once you have secured your Enrollment Server for Web, Entrust recommends that you enable server authentication by retrieving and importing the CA certificate into users' browsers. Server authentication also requires that you install a CA certificate on your Web server hosting the Enrollment Server for Web. Refer to "Retrieving and importing the CA certificate into the Web server" on page 66 for instructions.

Consult the following table for instructions on how to retrieve import the CA certificate.

If you...	Then...
are using an Internet Explorer browser	"Retrieving and importing the CA certificate using Internet Explorer" on page 64
are using a Netscape browser	"Retrieving and importing the CA certificate using Netscape®" on page 65

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.

Retrieving and 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. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **CA Certificates** menu on the left, click **Install**.
3. Save the file in any location when you are given the option to open or save it.

You have retrieved the CA certificate from Security Manager and have saved it in Internet Explorer. Proceed to "To import the CA certificate into Internet Explorer" on page 65.

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...**.

   The **Certificate Store** dialog box appears.
5. 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 message "The import was successful" appears.
9. Click **OK**.

   You have imported the CA certificate into a user's browser. You can now use it to verify your Enrollment Server for Web's identity.

Retrieving and importing the CA certificate using Netscape®

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

To retrieve and import the CA certificate into Netscape® browsers

1. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **CA Certificates** menu on the left, click **Install**.

   The **Downloading Certificate** dialog box opens.
3. Select the appropriate check boxes to specify the purpose of your CA and click **OK**.

   You have retrieved and imported the CA certificate into a user's browser. Use it to verify your Enrollment Server for Web's identity.

Retrieving and importing the CA certificate into the Web server

Entrust recommends that you enable client authentication by retrieving and importing the CA certificate into your Enrollment Server for Web. Client authentication also requires that you install a browser certificate on users' browsers.

Installing the CA certificate into the Enrollment Server for Web is a two part process:

- "Retrieving the CA certificate from Security Manager" on page 66
- "Importing the CA certificate into the Web server" on page 67

In addition to importing the CA certificate, IIS Web servers require you to configure a CRL check to enable client authentication. See "Enabling CRL checking on Microsoft® IIS" on page 98 for details.

Retrieving the CA certificate from Security Manager

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

- "To retrieve the CA certificate on Microsoft® IIS" on page 66
- "To retrieve the CA certificate on other Web servers" on page 67

To retrieve the CA certificate on Microsoft® IIS

1. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **CA Certificates** menu on the left, click **Install**.

   The **File Download** dialog box appears.
3. Click **OK** to download the file.

   The **Save As** dialog box appears.
4. Enter a path and name for the text file in which to save the certificate.
5. Click **Save**.

   You have retrieved the CA certificate from Security Manager and have saved it in Internet Explorer. Proceed to "Importing the CA certificate into the Web server" on page 67.

To retrieve the CA certificate on other Web servers

1. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
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 into the clipboard.

   You have now retrieved the CA certificate from Security Manager. Proceed to "Importing the CA certificate into the Web server" on page 67.

Importing the CA certificate into the Web server

After you have retrieved the CA certificate from Security Manager, you must import it into the Web server that administers the Enrollment Server for Web and then import it into other Web servers. Follow the instructions that apply to your Web server to import the CA certificate:

- "To import the CA certificate using Internet Explorer on IIS" on page 68
- "To import the CA certificate on Sun ONE™" on page 68
- "To import the CA certificate on Red Hat® Stronghold" on page 69
- "To import the CA certificate on IBM® HTTP Server" on page 69

Note: You cannot import a CA certificate into an Internet Explorer 4.0 browser.

To import the CA certificate using Internet Explorer on IIS

1. Right-click the certificate 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...**.

   The **Certificate Store** dialog box appears.
5. Select **Show Physical Stores** and click **OK**.
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 message "The import was successful" appears.
9. Click **OK**.

   You have imported the CA certificate into your Web server. If you want to enable client authentication, proceed to "Enabling CRL checking on Microsoft® IIS" on page 98.

To import the CA certificate on Sun ONE™

1. Open the **Sun ONE Administer Web Server** page.
2. Choose the Web server which 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 the **Trusted Certificate Authority (CA)** option.
6. Enter your Key Pair File Password.
7. Select the **Message Text (with headers)** option.
8. In the **Message Text (with headers)** field, paste the certificate that you copied to the clipboard.
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. Open a text editor and paste the CA certificate you copied to the clipboard.
3. Save the file with a `.pem` extension.
4. Go to the directory that contains the text file containing CA certificate.
5. 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**.
7. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
8. Open the CA Certificate (PEM encoding) page. Copy and paste the entire certificate, including the BEGIN and END lines, into a file with an `.arm` extension.
9. Select **Signer Certificates** in the **Key Database** window, then click **Add**.
10. In the **Add CA's Certificate from a File** dialog box, select the certificate file name, or browse to the file.
11. Click **OK**.
12. 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.

Chapter 6

Issuing certificates for computers, devices, and Windows® servers

This chapter details how you can issue Entrust certificates for computers, CAPI-enabled devices, and servers that import them from the Microsoft Local Computer certificate store.

Topics in this chapter:

Overview

Enrollment Server for Web can issue certificates and import them into the Microsoft Local Computer Certificate Store. Devices and machines such as the following can then retrieve the certificate and use it negotiate a secure session:

- CAPI-enabled VPN devices such as routers, gateways, firewalls, and remote access devices
- Windows Internet Authentication Service (IAS) servers and clients
- Domain controllers

For a definition of Microsoft Certificate Store, refer to "Glossary" on page 107.

You need to perform the following tasks to configure your system to issue these certificates:

- Configure Security Manager with certificate information. See "Configuring the certificate definitions" on page 73 for instructions.
- Generate the certificate using Internet Explorer 5.0 or above. These versions of Internet Explorer include CAPI. See "Creating a computer, device, or Windows® server entry" on page 76 for instructions.
- Install the certificate into a device or machine that supports CAPI, such as the Windows 2000 VPN client or server. See "Retrieving the computer, device, or Windows® server certificate" on page 77 for instructions.

Configuring the certificate definitions

Complete the following procedures, in sequence, to configure the certificate definitions (`master.certspec`) file for your device.

- "Exporting the certificate definitions file" on page 73
- "Creating a new certificate type" on page 74
- "Adding a certificate extension to the certificate type" on page 74
- "Processing the certificate definitions file" on page 75

Note: This guide assumes you have kept the default certificate definitions file name: `master.certspec`.

Exporting the certificate definitions file

The Entrust Authority Security Manager database stores certificate information in the `master.certspec` file. By editing the `master.certspec` file, you can create a customized computer, device, or Windows server certificate.

To export the certificate definitions file

1. Log in to Security Manager Administration as a Security Officer.
2. Click **File > Certificate Definitions > Export**.

   The **Save As** dialog box opens.
3. Type a file name and path and click **Save**.

   By default the file is named "`master.certspec`".

   When the `master.certspec` file has been successfully created, a dialog box opens.
4. Click **OK**.

   You have exported the `master.certspec` file. Proceed to "Creating a new certificate type" on page 74.

Attention: The `master.certspec` file is located on the Security Manager Administration server. As a Security Officer, you are responsible for this file. Entrust does not recommend that you keep copies of this file, because they increase the risk off overwriting a newer version of the file with an older version.

Creating a new certificate type

Create a new certificate type for your computer, device, or Windows server by editing the `master.certspec` file. The certificate type is what appears in the **Type** list under the **Certificate** tab in the **New User** dialog box of the Security Manager Administration.

Creating a new certificate type

1. Open the `master.certspec` file in a text editor.
2. Locate the `[Certificate Types]` section header.
3. On a new line in the `[Certificate Types]` section, type the following:

   `web_<Type_name>=web,<Type_name>,<Type_description>;`

   where <*Type_name*> and <*Type_description*> are the name and description, respectively, of the certificate type that appears in the list of certificate types in the **New User** dialog box. For example, if you type the line

   `web_VPN=web,VPN,VPN certificate;`

   the word "`VPN`" will appear in the **Type** list under the **Web** category.
4. Optionally, add a comment that describes the purpose of the certificate type.

   Comments are not required, but they may help you remember the purpose of the certificate type the next time you edit the file.
5. Save your changes.

   You have created a certificate type that will appear in the **Type** list in the **New User** dialog box. Proceed to "Adding a certificate extension to the certificate type" on page 74.

Adding a certificate extension to the certificate type

A certificate extension defines the extra content included in certificates of a specific certificate type. Define a computer, device, or Windows server certificate extension in the `master.certspec` file that will include device-specific or computer-specific information.

Note: If you are adding a certificate extension for an IAS server or client, ensure the IAS certificates contain the Server Authentication certificate purpose, also known as Enhanced Key Usage (EKU). The EKU for IAS uses the following object identifier (OID): `1.3.6.1.5.5.7.3.1`.

To add a certificate extension to the certificate type

1. In the `master.certspec` file, locate the `[Extension Definitions]` section header.
2. On a new line in this section, enter the subsection header using the following format:

   `[web_<`*`Type name`*`> Verification Extensions]`

   where <*Type name*> represents the Type name as defined in the `[Certificate Types]` section (see "Creating a new certificate type" on page 74). For example, "VPN".

   Subsection headers must appear in square brackets and are case-sensitive.
3. In the subsection you just created, enter the following lines, as appropriate:
   - for VPN devices:

   ```
   keyusage=2.5.29.15,c,m,BitString,1111
   extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.8.2.2
   ```

   - for IAS servers or clients:

   ```
   extkeyusage=2.5.29.37,n,m,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.1
   ```
4. Save your changes.

   You have added a certificate extension to the certificate type. This extension adds customized information to the certificate. Proceed to "Processing the certificate definitions file" on page 75.

Processing the certificate definitions file

When you process the file, Security Manager Administration checks for errors and writes them to a log file that you specify (named `master.log` by default).

To process the certificate definitions file

1. In Security Manager Administration, click **File > Certificate Definitions > Import**.

   The **Open** dialog box opens.
2. Select the `master.certspec` file in the **Open** dialog box and click **Open**.

   A dialog box appears when the certificate has finished processing.
3. Click **OK**.

   You have processed the `master.certspec` file. Proceed to "Creating a computer, device, or Windows® server entry" on page 76.

Creating and retrieving the entry

This section provides instructions on creating and retrieving a computer, device, or Windows server entry.

Topics in this section:

Creating a computer, device, or Windows® server entry

Create a new user entry for the computer, device, or Windows server in Security Manager Administration. Enrollment Server for Web uses the activation codes to generate a certificate.

Note: If you are creating an entry for an IAS server or client, complete the "To add the FQDN to the IAS certificate" on page 77 procedure after creating the user entry. Otherwise, skip this task.

To create a user entry

1. Log in to Security Manager Administration as an administrative user.
2. Click **Users > New Users**.

   The **New User** dialog box appears.
3. Follow the Security Manager documentation to fill out the **Naming** property page. You can choose **Person** or **Web server** as the user type.
4. On the **Certificate** property page, click **Category** and select **Web**.
5. In the **Type** list, click the certificate type that you created for the device.
6. Type the certificate extension variables into the **Certificate Extension** fields.
7. Click **OK**.

   The **Operation Completed Successfully** dialog box appears. This dialog box displays the device's reference number and authorization code.
8. Record the reference number and authorization code.

   You have created a user entry for the device. Proceed to "Retrieving the computer, device, or Windows® server certificate" on page 77, or, if you are creating an IAS user entry, proceed to "To add the FQDN to the IAS certificate" on page 77.

To add the FQDN to the IAS certificate

Complete the following procedure to ensure the IAS user entry contains the fully qualified domain name (FQDN) of the IAS server in the `Subject Alternative Name` property.

1. Double-click on the IAS user entry you just created.
2. In the **Email (SubjectAltName)** field on the **General** page, enter the FQDN of the IAS server computer. For example, `IASServer.yourCompany.com`.
3. Click **OK**.

Retrieving the computer, device, or Windows® server certificate

When you retrieve the computer, device, or Windows server certificate using Enrollment Server for Web, the certificate is downloaded into the appropriate Local Computer Certificate Store on the machine.

To retrieve the certificate in Enrollment Server for Web

1. Access Enrollment Server for Web from the computer or device. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **Certificates** menu on the left, click **Computer, Device, or Windows Server**.
3. Enter the reference number and authorization code. See "To create a user entry" on page 76 for details.
4. Select the appropriate Cryptographic Server Provider (CSP) from the list. If you are installing the certificate on a smart card, select the smart card's CSP. Change the CSP type in the **CSP type** list. This list automatically changes to show the CSPs available for the selected CSP type.

   For example, if you are generating an IAS certificate, select one of the following options:

   - the "**RSA and SChannel**" CSP type and the "**Microsoft RSA SChannel Cryptographic provider**" CSP
   - the "**Diffie-Hellman and SChannel**" CSP type and the "**Microsoft DH SChannel Cryptographic provider**" CSP
5. Click **Submit Request**.

   The requested certificate is placed in the Local Computer Certificate Store.
6. Restart the computer to ensure that the certificate is used.

Note: If you are also issuing certificates for IAS access clients, ensure the CA certificate is installed on the IAS server (see "Issuing CA certificates" on page 55 for instructions). If your IAS access client is a computer, install the certificate in the Local Computer Certificate Store, otherwise, if your client is a user, install the certificate in the Current User Certificate Store.

To create a user certificate and install it in the Current User Certificate Store, click **Web Browser** in the **Certificates** menu on the left. To create a computer certificate and install it in the Local Computer Store, click **Computer, Device, or Windows Server** in the **Certificates** menu.

Chapter 7

Issuing certificates for WAP servers

Enrollment Server for WAP 7.0, installed with Enrollment Server for Web, distributes certificates to WAP servers.

This chapter assumes that you have already installed and configured Enrollment Server for WAP and a WAP server.

Topics in this chapter:

Overview

Use the Enrollment Server for WAP to distribute certificates to WAP servers and wireless devices so that you can establish secure connections between them.

Follow these steps to set up your WAP server using Enrollment Server for WAP:

Step...	Instructions found here...	Completed
1. Ensure Enrollment Server for Web is installed and that you have completed the required post-installation tasks.	• "Installing Enrollment Server for Web" on page 17 • "Post-installation tasks" on page 27	
2. Edit the certificate definitions file in Security Manager to include the Wireless Transport Layer Security (WTLS) certificate type.	"Configuring the certificate definitions" on page 81	
3. Ensure that a WAP server is installed and running.	Your WAP server documentation.	
4. Create an entry for the WAP server in Security Manager Administration.	"Creating a WAP server entry" on page 83	
5. Generate a certificate request from your WAP server.	"Generating a certificate request" on page 84	
6. Enter the activation codes and certificate request and submit the request to Security Manager.	"Retrieving certificate request" on page 84	
7. Install the WTLS certificate on the WAP server.	Your WAP server documentation.	
8. Distribute the CA certificate and save the file generated by Enrollment Server for WAP.	"Exporting and importing the CA certificate" on page 86	
9. Optional. Install the CA certificate on the WAP server.	Your WAP server documentation.	
9. Optional. Customize the HTML pages.	"Customizing HTML template pages" on page 90	
10. Distribute certificates to your wireless devices.	Your wireless device documentation.	

For background information on Enrollment Server for WAP, refer to "What is Enrollment Server for WAP?" on page 16.

Configuring the certificate definitions

Before you can issue a certificate to your WAP server, edit the certificate definitions file (`master.certspec`) to include the WTLS certificate type.

Topics in this section:

Note: This guide assumes you have kept the default certificate definitions file name: `master.certspec`.

Exporting the certificate definitions file

The Entrust Authority Security Manager database stores certificate information in the `master.certspec` file. By editing the `master.certspec` file, you can create a customized computer, device, or Windows server certificate.

To export the certificate definitions file

1. Log in to Security Manager Administration as a Security Officer.
2. Click **File > Certificate Definitions > Export**.

   The **Save As** dialog box opens.
3. Type a file name and path and click **Save**.

   By default the file is named "`master.certspec`".

   When the `master.certspec` file has been successfully created, a dialog box opens.
4. Click **OK**.

   You have exported the `master.certspec` file. Proceed to "Creating a new certificate type" on page 82.

Attention: The `master.certspec` file is located on the Security Manager Administration server. As a Security Officer, you are responsible for this file. Entrust does not recommend that you keep copies of this file, because they increase the risk off overwriting a newer version of the file with an older version.

Creating a new certificate type

Create a new certificate type for your computer, device, or Windows server by editing the `master.certspec` file. The certificate type is what appears in the **Type** list under the **Certificate** tab in the **New User** dialog box of the Security Manager Administration.

Creating a new certificate type

1. Open the `master.certspec` file in a text editor.
2. Scroll down to the following line, and delete the semi-colon (;) that precedes it:

   ```
   ;wtls_server_cert=web,WTLS Server Certificate, Sample WTLS
   Server Certifi_continue=cates
   ```

3. Scroll down to the following lines (grouped together) and delete the semi-colon (;) that precedes each:

   ```
   ;[wtls_server_cert Advanced]
   ;formatWTLS=1
   ```

4. Save your changes.

   You have created a certificate type that will appear in the **Type** list in the **New User** dialog box. Proceed to "Processing the master.certspec file" on page 82.

Processing the master.certspec file

When you process the file, Security Manager Administration checks for errors and writes them to a log file that you specify (named `master.log` by default).

To process the master.certspec file

1. In Security Manager Administration, click **File > Certificate Definitions > Import**.

   The **Open** dialog box opens.

2. Select the `master.certspec` file in the **Open** dialog box and click **Open**.

   A dialog box appears when the certificate has finished processing.

3. Click **OK**.

   You have processed the `master.certspec` file to include WTLS certificates. Proceed to "Creating a WAP server entry" on page 83.

Creating and retrieving the entry

Complete the procedures in this section to create an entry, generate a certificate request (CSR), and retrieve the certificate request using Enrollment Server for Web.

Topics in this section:

Creating a WAP server entry

Security Manager Administration lets you create WTLS certificates for WAP servers. A WAP server uses a WTLS certificate to identify itself as a trusted server. This WTLS certificate is issued and signed by the CA.

Before you can issue the WTLS certificate, you must create an entry for the WAP server in Security Manager Administration as described in the procedure below.

To create an entry for the WAP server

1. Log in to Security Manager Administration.
2. Click **Users > New User**.

   The **New User** dialog opens.
3. In the **Naming** property page, click **Web Server** in the **Type** drop-down list. Type a name for the server in the **Name** field and any descriptive information about the server in the **Description** fields. You need only enter a name. All other fields are optional. Do not select **Create profile.**
4. Click the **Certificate** property page.
5. In the **Category** list, click **Web**.
6. In the **Type** drop-down list, click **WTLS server certificate**.
7. Click **OK**.

   The **Operation Completed Successfully** dialog box opens.

   This dialog box displays a reference number and authorization code. You need only the reference number to generate a WTLS certificate request (see "Generating a certificate request" on page 84), but you need both values to retrieve the WTLS certificate from Security Manager.
8. Record these values securely.

   You have now created an entry for the WAP server.

Generating a certificate request

The procedure you follow to generate a certificate request depends on the type of WAP server you are using (for example, Nokia or Motorola).

After you generate and save a certificate request, you'll use it to create a WAP server certificate using Enrollment Server for WAP.

Consult your WAP server documentation for instructions on generating a certificate request.

Retrieving certificate request

Now that you have created an entry for the WAP server in Security Manager, exported the CA certificate, and generated a certificate request using the WAP server, you need to submit a WTLS certificate request.

To retrieve a WTLS certificate request

1. Access the Enrollment Server for WAP. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **Certificates** menu on the left, click **WAP Server Certificate**.

   The **Server Certificate Retrieval** page opens.
3. Enter the reference number and authorization code generated by Security Manager in the designated fields.
4. Choose a certificate type in the **Request Options** drop-down list.
   Your choices are:
   - **NokiaCSR**. Choose Nokia CSR is you are using a Nokia WAP server;
   - **PKCS#10**. For all other WAP servers, choose PKCS #10.

   For more information, consult your WAP server documentation.
5. Paste the certificate request (received from the WAP server) in the text field.

   Be sure to copy the entire certificate request, including the BEGIN and END lines.
6. Click **Submit Request** to send your request to the CA for certification.

   After you successfully submit the request, Security Manager returns your WTLS certificate. The WTLS certificate should look something like this:

```
-----BEGIN WTLS CERTIFICATE-----
AQIBAAQJOyBXQVA7IENBOhQkfzv1XwcBAAQNOyBXQVA7IENBOyAxMwIAAAMBAAE
AYPDGZoXbiNwesK72wrYw4+RG4AFZPMI6vu88nghImlsxF028WU8RXsb1JzWbJx
WojKF55/PGOzFqbD8lw6A#4DtY7H8>CBb7BPPq3cpO0YK/teNwztuZT/lzP/i6E
2sfxwCAUrplcPm9ovbkWIkxWFkFeVfuIp8Rid2SzDqhUt^nD#eG/al75dsEu/vR
jaO7LfLm92n7jS1LJNXZmL+cB/CfuPsU7i+lk0LI/mBWMzCG5+lLgj3y8O4WU1P
```

```
pXMPpX1NXoDrwPPDS5ugaf1Sz+POrvqP8N4p4bGHqbD8lw6A#4DtY7H8>CBE=

-----END WTLS CERTIFICATE-----
```

7 Copy the entire certificate request (including the BEGIN and END lines) and paste this information into a new text file.

You have now submitted a WTLS certificate request. You can now install it on the WAP server. Consult your WAP server documentation for instructions on how to install the certificate.

Exporting and importing the CA certificate

Users who connect to a WAP server or gateway that is secured by a server certificate issued by your CA must have a copy of your CA certificate. The CA certificate is used to verify the server certificate.

Topics in this section:

Exporting the CA certificate

The procedure below describes how to distribute the CA certificate from the command line.

Note: You can also obtain the CA certificate as described in "Retrieving the CA certificate" on page 87. But to obtain the CA certificate using that procedure, you must have already received a server certificate at least once.

To export the CA certificate at the command line (entsh)

1. Click **Start > Programs > Security Manager> Security Manager Master Control Command Shell**.

   The **Entrust Master Control Command Shell** window opens.

2. At the prompt, type one of the following commands:

   ```
   ca cert export -binary -wtls <filename>
   ```

   ```
   ca cert export -pem -wtls <filename>
   ```

   where `<filename>` is the name of the CA certificate. For example, `c:\\temp\\cacert.bin` or `c:\\temp\\cacert.pem`.

Note: The certificate mechanism used in binary and pem differs: binary uses base 2 encoding, pem uses base 64. Choose the file type used by your WAP server. Consult your WAP server documentation to determine which of the two formats your server requires.

   A message appears on screen requesting that you confirm the action.

3. Click **OK**.

   You have now exported the CA certificate.

Retrieving the CA certificate

After you successfully retrieve the WTLS certificate, you can retrieve the CA certificate. Not all WAP servers require a CA certificate; consult your WAP server documentation for more information on when a CA certificate is required.

Note: You can only retrieve the CA certificate in the manner described below if you have already obtained a server certificate (or have already obtained a server certificate at least once).

To retrieve the CA certificate

1. Access the Enrollment Server for WAP. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **Certificates** menu on the left, click **CA Certificate**.

   The **CA Certificate Retrieval** page opens.
3. Copy the entire CA certificate (including the BEGIN and END lines) and paste this information into a new text file.
4. Save the file.

   You have retrieved the CA certificate.

   You can now install the CA certificate on your WAP server. Consult your WAP server documentation for instructions on how to install the certificate.

Chapter 8

Customizing Enrollment Server for Web

This chapter details additional operations that you can use to extend the Enrollment Server for Web functionality and customize its appearance and content.

Topics in this chapter:

Customizing HTML template pages

The HTML templates used by Enrollment Server for Web are fully customizable. Customize the contents of these HTML pages to include company-specific information.

Attention: The Enrollment Server for Web tags are identified by the following characters:
`<!-- tagname -->`
Do not edit the Enrollment Server for Web tag names. Enrollment Server cannot recognize tags whose names have changed.

Topics in this section:

Customizing the security policy page

If your company has an established security policy relating to online or Web-based transactions, you can include this information in the Enrollment Server user interface. Users can click the **Security Policy** link to view the company's security policy.

Add this information by modifying the `cdapolicy.htm` file located in the `<ES_for_Web_root>/docs` directory.

Customizing the About page

In addition to the version number of the software, you can include information on your company's implementation of Enrollment Server for Web through the **About Enrollment Server for Web** link. For example, you might provide information to users explaining how to retrieve certificates.

Add this information by modifying the `cdahome.htm` file located in the `<ES_for_Web_root>/docs` directory.

Customizing the CSP list

You can change the list of Cryptographic Security Providers (CSPs) located on the following pages:

- Browser Certificate Request page (opens when you click the **Web browser** link in the **Certificates** menu on the left)
- Computer Certificate Request page (opens when you click the **Computer, Device, or Windows servers** link in the **Certificates** menu on the left)

To customize the list, modify the Visual Basic scripts on the following HTML pages located in the `<ES_for_Web_root>/docs/html` folder:

- `cdaibcert.htm` contains the CSP list for Web browser certificates
- `iecert.htm` contains the CSP list for Web server and computer, device and server certificates

To change the Visual Basic scripts, find and modify the `DisplayProviders` function in the code. For example:

```
Sub DisplayProviders
...
' CSP type 2
Enroll.providerType = 2
csp = ""
csp = Enroll.enumProviders(0,0)
If Len(csp) > 0 Then
set el = document.createElement("OPTION")
el.text = "RSA Signature"
el.value = 2
document.all.cryptProvType.add(el)
End if

' CSP type 3
Enroll.providerType = 3
csp = ""
csp = Enroll.enumProviders(0,0)
If Len(csp) > 0 Then
set el = document.createElement("OPTION")
el.text = "Digital Signature Standard (DSS)"
el.value = 3
document.all.cryptProvType.add(el)
end if
```

```
...
```

You can add or comment out CSP types to customize the list for your organization.

Customizing style sheets

To customize the fonts and colours of the user interface, modify the `style.css` file located in the `<ES_for_Web_root>/docs/css` directory.

For example, to change the colour of the links on the home page and the menu on the left, edit this line:

```
a {
color: #992A78;
}
```

Customizing the company logo

To add your company logo to the top left corner of the HTML pages, replace the `customer_logo.gif` file located in the `<ES_for_Web_root>/docs/images` directory with your own logo.

Supporting cross-certified CAs

If you have two or more Certification Authorities (CAs) that are cross-certified, you can configure the Enrollment Server for Web to reflect this cross-certification. This gives Web browsers secure access to Web servers that trust a cross-certified CA and vice versa.

For more information about cross-certification, refer to the Security Manager guides (see "Related Entrust documentation" on page 6).

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.

Support cross-certified CAs by installing all the required cross-certificates in the Enrollment Server for Web so that the entire certificate chain is presented to the Web browser during server authentication. This configuration is a two-step process:

- copying the certificate chain to the `<ES_for_Web_root>/certs` folder
- installing the cross-certificate(s) into the Enrollment Server for Web

To explain this process further, this section contains two examples:

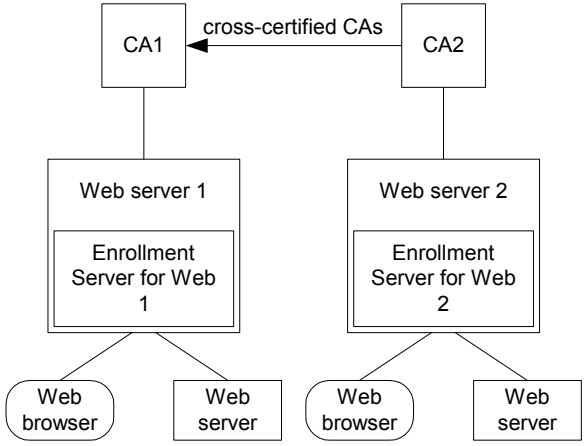
- one for two cross-certified CAs ("Supporting two cross-certified CAs" on page 94)
- one for more than two cross-certified CAs ("Supporting more than two cross-certified CAs" on page 96).

Supporting two cross-certified CAs

Read the example below and complete the procedure to configure Enrollment Server for Web for cross-certification when you have two cross-certified CAs.

In the following example, **CA2** is the root CA.

Figure 3: Example of a cross-certification configuration



In this example, Enrollment Server for Web was first installed and configured on **Web server 1**, and uses **CA1**. Web browsers and other Web servers belonging to **CA1** have certificates signed by **CA1**.

A second CA was created (**CA2**). **CA2** was cross-certified with **CA1**. As a result of that cross-certification, **CA1** created and digitally signed a cross-certificate containing the verification public key of **CA2**. Consequently, users in **CA2** are assured that **CA1** trusts **CA2**. Installing this cross-certificate on **Web server 2** will allow Web browsers and Web servers which trust **CA1** to connect to **Web server 2** because:

- **Web server 2** was issued a certificate that was signed by **CA1**
- the user already trusts **CA1**

Before issuing Web server and browser certificates to Web servers and Web browsers belonging to **CA2** using **Enrollment Server for Web 2**, configure **Enrollment Server for Web 2** to reflect the cross-certification of the CAs using the following procedures.

Note: Enrollment Server for Web only supports unilateral (that is, one way) cross-certification. In this model there is one common root of trust which can be cross-certified with many other CAs.

To copy the certificate chain to a file

1. Log in to Security Manager Administration as a Security Officer.
2. Connect to the CA that signed the cross-certificate containing the verification public key of the CA to which Enrollment Server for Web connects (in our example **Enrollment Server for Web 2** connects to **CA2**). In the example, you would connect to **CA1**.

Note: If the CA is not an Entrust CA, consult your CA documentation for information on how to export the certificate chain in PKCS #7 and save it as a file.

---

3. In the tree view, double-click **Certification Authority (CA)**.
4. Double-click **Cross-Certified CAs**.

   A list of all cross-certificates appears.
5. Right-click the cross-certificate signed by the CA to which you are connected (**CA1** in the example). This cross-certificate contains the verification public key of the CA to which Enrollment Server for Web connects (**CA2** in the example).
6. Click **Write cross-certificate I signed to file** in the pop-up menu.

   A dialog box appears.
7. Save the certificate chain using the `xcert.der` filename and the binary PKCS #7 format.

   This file contains the self-signed CA certificate and the cross-certificate signed by the CA. Enrollment Server for Web needs this file to indicate which cross-certificates to install in the Enrollment Server for Web (**Web server 2** in our example).
8. Copy the `xcert.der` file to a diskette and transfer it to the following directory on the Enrollment Server for Web (**Web server 2** in our example):

   ```
   <ES_for_Web_root>/certs
   ```

To install the cross-certificates in the Enrollment Server for Web

1. Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.
2. In the **Cross-Certificates** menu on the left, click the **Cross-certificates for Web server** link.

   Enrollment Server for Web shows a list of cross-certificates to install on the Enrollment Server for Web.
3. Install each certificate in the chain on your Web server. Consult your server documentation for instructions on importing cross-certificates.

You have configured the Enrollment Server for Web for cross-certification (**Web server 2** in our example).

Web browsers and Web servers under **CA1** can now access and trust secure sites under **CA2**. A cross-certificate from **CA1** accompanies all certificates issued by **CA2**. The root of trust is **CA1**.

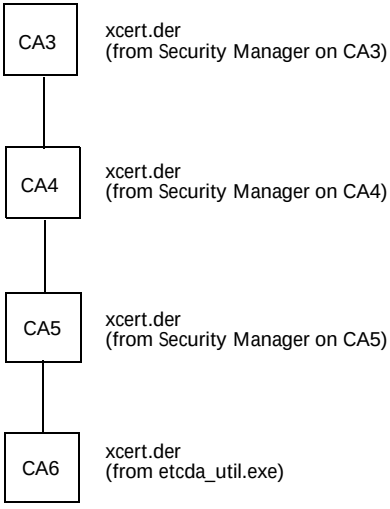
After you have configured **Enrollment Server for Web 2** with the cross-certificate signed by **CA1**, you can configure many more cross-certified CAs with certificates issued by **CA1**. All of the cross-certified CAs will share the same root of trust, which is **CA1**.

Supporting more than two cross-certified CAs

If you have not already done so, review the example of "Supporting two cross-certified CAs" on page 94.

The following example shows **CA3** as the root CA. The links between CAs illustrate the chain. As in the previous example, each CA is connected to a Web server running Enrollment Server for Web. For example, **CA3** is connected to **Enrollment Server for Web 3**.

Figure 4: Another example of a cross-certification configuration



In this example, Enrollment Server for Web was first installed and configured on **Web server 3**, and uses **CA3**. Web browsers and other Web servers belonging to **CA3** have certificates signed by **CA3**.

Three other CAs were created (**CA4**, **CA5**, **CA6**).

In the certificate chain:

- **CA3** was cross-certified with **CA4**.
- **CA4** was cross-certified with **CA5**
- **CA5** was cross-certified with **CA6**

Before issuing Web server and browser certificates to Web servers and Web browsers belonging to **CA6** using **Enrollment Server for Web 6**, configure **Enrollment Server for Web 6** to reflect the cross-certification of the CAs.

Copy the `xcert.der` files from each of the CAs in the chain (excluding **CA6**). In this example you will need three of these files:

- one from **CA3**
- one from **CA4**
- one from **CA5**.

Combine these files using the command-line utility `etcda_util.exe`. Import the resulting `xcert.der` file into **Enrollment Server for Web 6** by adding it to the `<ES_for_Web_root>/certs` directory and completing the "To install the cross-certificates in the Enrollment Server for Web" on page 95 procedure.

Finding certificates, enabling CRL checking, and modifying CA information

This section provides instructions on finding certificates, when and how to enable CRL checking for certificates, and modifying CA information.

Topics in this section:

Enabling CRL checking on Microsoft® IIS

For client authentication, IIS must not only have the CA certificate installed, but must also check the CRL to determine whether the user has been revoked. To perform the CRL check, certificates must include a valid `CRLDistributionPoint` entry that points to a combined CRL. For information on combined CRLs and CRL distribution points, see the Security Manager documentation ("Related Entrust documentation" on page 6).

Complete the following procedure to create a combined CRL file and add a `CRLDistributionPoint` entry to certificates.

To create the combined CRL file and add a CRLDistributionPoint entry

1. Open the `entmgr.ini` file in a text editor. By default, the `entmgr.ini` file is located in the `\entmgrdata\manager` folder on the Entrust Authority drive.
2. Locate the `[Advanced Settings]` section or add it if it does not exist.
3. In the `[Advanced Settings]` section, add the following lines:

   ```
   UseCombinedCRL=1

   CombinedCRLLifetime=36
   ```

   - `UseCombinedCRL=1` enables combined CRLs
   - `CombinedCRLLifetime=36` sets the combined CRL lifetime to between 4 and 336 hours.
4. Add a `[CRL]` section.
5. In the `[CRL]` section, add the following entry:

   `CombinedCRLFile=<`*`Entrust_Authority_Drive`*`>\crl\CRLFile.crl`

where <*Entrust_Authority_Drive*> is the drive where Entrust Authority is installed.

6 Save your changes.

7 Add a [CDP] section.

8 In the [CDP] section, add the following lines:

```
1=ldap://<Server>/<CRL>?certificateRevocationList?base
2=http://<your_company_URL/location/CRL_name>.crl
```

where <*your_company_URL/location/CRL_name*> is the location of the CRL file.

Security Manager substitutes "<Server>" for the LDAP server address and port number, and "<CRL>" for the LDAP DN of the certificate's CRL.

9 Save and close the entmgr.ini file.

10 Restart Entrust Authority.

You have now created a combined CRL and created a CRL distribution point which are used to authenticate the client.

Finding certificates and checking their status

The **Find Certificate** link in the **Tasks** menu allows users and administrators to search for certificates in a network Directory and check whether the certificate is valid or revoked. The Certification Authority to which Enrollment Server for Web connects uses this Directory.

Complete the following steps to find certificates and certificate status information.

To find certificates and check their status

1 Access Enrollment Server for Web. For instructions, refer to "Accessing the Enrollment Server" on page 33.

2 In the **Tasks** menu on the left, click the **Find Certificate** link.

3 Type the name of the user whose certificates you want to find in the **Name** field.

The **Name** field is mandatory. Your search automatically returns all users matching the criteria if an asterisk (*) is used in this field.

4 Optionally, fill in the **E-mail** field with the e-mail address of the user you are searching for.

The "searchSubjectAltName" setting in the [Configuration] section of the clientcgi.ini file located in the <ES_for_Web_root>/client/cgi directory allows you to configure certificate searches by e-mail information stored in the subjectAltName extensions in certificates.

- Add and set `searchSubjectAltName` to `true` to include both the e-mail (`SubjectAltName`) and mail RDN in the user's DN.
- Add and set `searchSubjectAltName` to `false` to include only the e-mail (`SubjectAltName`) in the user's DN.

  The default is `false`.

The Security Manager Administrator and the First Officer are never displayed in the search results list. There is a maximum of 200 users that can be displayed at once.

5 Once you have specified a search expression, click **Certification Authority** in the **Searchbase**.

6 Click **Search Directory.**

If your search finds users matching the criteria specified in the search expression, the list of user Distinguished Names (DNs) is displayed in a search results list on a Web page. Click on one of the links to make a selection.

7 Select a certificate to retrieve by clicking one of the DN links.

8 Click on one of five possible actions outlined below:

- **Import as your personal certificate.** The certificate is imported into your browser and can be used to identify yourself to other people and Web sites. This applies to Netscape Navigator only.
- **Import as another user's certificate**. The certificate of another user is imported into your browser and can be used to send encrypted and/or signed e-mail. This option is only available for Netscape Communicator 4.0 or later, and only if the owner of the certificate has an e-mail attribute as part of their Distinguished Name (DN).
- **Display as PEM encoding of certificate in raw DER.** The raw Distinguished Encoding Rules (DER) format of the certificate is displayed on a Web page in Privacy Enhanced Mail (PEM) encoding. This applies to Microsoft Internet Explorer only.
- **Displayed as PEM encoding of certificate in PKCS #7.** The Public-Key Cryptographic Standard #7 (PKCS #7) format of the certificate is displayed on a Web page in Privacy Enhanced Mail (PEM) encoding. This applies to Microsoft Internet Explorer only.
- **Verification of certificate.** The status of the certificate is displayed as valid or revoked.

9 Click **Retrieve**.

Modifying CA information

If you change your Security Manager CA information (for example, the DN, IP addresses, and so on), you need to update the Enrollment Server for Web. To do so, complete the following procedure.

To modify CA information

1. Open the `clientcgi.ini` file located in the `<ES_for_Web_root>/docs/config` directory in any text editor.
2. Update the `Manager`, `Server` or `cadn` settings.
3. Remove the CA certificate file (by default, `cacert.der`) located in the `<ES_for_Web_root>/certs` directory.
4. Re-issue a new Web server or Web browser CA certificate. For instructions, refer to "Issuing CA certificates" on page 55.

Issuing customized certificates

Enrollment Server for Web takes advantage of the certificate definitions (`master.certspec`) file in Entrust Authority. This file allows Entrust Administrators to configure their Security Manager to issue customized certificates and distribute these certificates to standard Web browsers and Web servers.

For example, you can use the `master.certspec` file to customize certificate types (such as VPN certificates), to set the Netscape base URL, and to set the Netscape revocation URL.

Once you have customized the `master.certspec` file, create a user entry and retrieve the certificate using Enrollment Server for Web. For detailed instructions, refer to "Issuing certificates for Web servers and browsers" on page 37 or "Issuing certificates for computers, devices, and Windows® servers" on page 71.

Topics in this section:

Note: This guide assumes you have kept the default certificate definitions file name: `master.certspec`.

Exporting the certificate definitions file

The Entrust Authority Security Manager database stores certificate information in the `master.certspec` file. By editing the `master.certspec` file, you can create a customized certificate.

Attention: The `master.certspec` file is located on the Security Manager Administration server. As a Security Officer, you are responsible for this file. Entrust does not recommend that you keep copies of this file, because they increase the risk off overwriting a newer version of the file with an older version.

To export the certificate definitions file

1. Log in to Security Manager Administration as a Security Officer.
2. Click **File > Certificate Definitions > Export**.

   The **Save As** dialog box opens.
3. Type a file name and path and click **Save**.

By default the file is named "`master.certspec`".

When the `master.certspec` file has been successfully created, a dialog box opens.

4 Click **OK**.

You have exported the `master.certspec` file.

Modifying the certificate definitions file

Figure 5 on page 104 shows an editable section of the certificate definitions file. For an explanation of the entire file, consult the Security Manager documentation (see "Related Entrust documentation" on page 6).

To edit this file, open it in any text editor and add your customized certificate type and optionally a certificate extension. After you have saved your changes, go to "Processing the certificate definitions file" on page 105.

Figure 5: Enrollment Server for Web information in the certificate definitions file

To use netscapeBaseUrl and netscapeRevocationUrl verification extensions, remove the semicolons from these two lines.

Put your site name here.

To use the netscapeComment verification extension, remove the semicolons from these two lines.

These two verification extensions are used in the web_server certificate type.

These two verification extensions are used in the web_codesign certificate type.

```
; ------------------------------------------------------------------
; To use netscapeBaseUrl and netscapeRevocationUrl, uncomment the two
; definitions below by removing the semicolon preceding them. Also,
; replace your.site.name with the name of your site.
; ------------------------------------------------------------------
; netscapeBaseUrl=2.16.840.1.113730.1.2,n,IA5String,https://your.site.name/cda-cgi/
;netscapeRevocationUrl=2.16.840.1.113730.1.3,n,IA5String,clientcgi.exe?action=check
_continue_=Revocation&
;
; ------------------------------------------------------------------
; The netscapeComment extension is optional. To use it, uncomment its
; definition by removing the semicolon preceding "netscapeComment=...",
; below.  You may modify the text "Default web certificate..." as
; desired.
; ------------------------------------------------------------------
; netscapeComment=2.16.840.1.113730.1.13,n,IA5String,Default web certificate issued by
; Enrollment Server for Web.

[web_server Verification Extensions]
;*****************************************************************************
;* Sample Web Server Certificate Type
;*
;*     The server certificate type is designed for use by SSL servers.
;*****************************************************************************
; ------------------------------------------------------------------
; <ASN1> keyUsage::=BIT STRING {digitalSignature(0), keyEncipherment(2)}
; ------------------------------------------------------------------
keyUsage=2.5.29.15,n,BitString,101
;
; -------------------------------------------------
; <ASN1> netscapeCertType::=BIT STRING {sSLServer(1)}
; -------------------------------------------------
netscapeCertType=2.16.840.1.113730.1.1,n,BitString,01
;

[web_codesign Verification Extensions]
;*****************************************************************************
;* Sample Code Signing Certificate Type
;*
;*     The web_codesign certificate type is designed to verify code
;*     signed either by Netscape or Microsoft code signing
;*     technologies.
;*****************************************************************************
; -------------------------------------------------
; <ASN1> keyUsage::=BIT STRING {digitalSignature(0)}
; -------------------------------------------------
keyUsage=2.5.29.15,n,BitString,1
;
; ---------------------------------------------------
; <ASN1> netscapeCertType::=BIT STRING {objectSigning(3)}
; ---------------------------------------------------
netscapeCertType=2.16.840.1.113730.1.1,n,BitString,0001
```

Processing the certificate definitions file

When you process the file, Security Manager Administration checks for errors and writes them to a log file that you specify (named `master.log` by default).

To process the certificate definitions file

1. In Security Manager Administration, click **File > Certificate Definitions > Import**.

   The **Open** dialog box opens.

2. Select the `master.certspec` file in the **Open** dialog box and click **Open**.

   A dialog box appears when the certificate has finished processing.

3. Click **OK**.

   You have now processed the `master.certspec` file and your changes are effective immediately.

Viewing log files

Enrollment Server for Web records all events, with all pertinent data, in text files located in the following directory:

```
<ES_for_Web_root>/logs
```

Enrollment Server for Web logs each event, including warnings or errors, along with the date, the time, the client IP address, the client browser version, and a brief description of the action. The Enrollment Server for Web log filenames have the following format:

```
CDAOperations<YYMMDD-HHMMSS>.log
```

Enrollment Server for Web creates a new log file every time you access it. To modify this behaviour, modify the `lastLogFileAccessed` setting in the `<ES_for_Web_root>/docs/cgi/clientcgi.ini` file. For example:

```
lastLogFileAccessed=..\logs\mylog.log
```

Three types of events are logged by Enrollment Server for Web. They are:

- Alarm: an error which requires corrective action
- Warning: an error which might be of interest
- Event: a normal occurrence, but of possible interest

For each event logged by Enrollment Server for Web, there is an associated error level. The different levels of error are:

- Internal CDA: Enrollment Server for Web encountered an error.
- Internal Web Server: The Enrollment Server for Web encountered an error or is not configured properly.
- External Browser: The end user's Web browser failed to communicate properly with Enrollment Server for Web.
- External Browser User: Invalid data provided by the end user.
- External CMS-API: A CMS-API function call within Enrollment Server for Web did not complete successfully.
- External Entrust Authority: Entrust Authority encountered an error and could not complete the request.

Glossary

activation codes

The "reference number" and "authorization code" that are generated when an Entrust Administrator adds or recovers a user using the Entrust Authority Security Manager Administration feature, or when users add or recover themselves using Entrust Authority Self-Administration Server.

Users enter this information in Enrollment Server for Web when enrolling for a digital certificate.

Administrator

An Administrator (with an uppercase "A") is a trusted person who uses Security Manager Administration Services to add users to Security Manager and to do other frequent operations such as deactivate users, revoke users' keys, set up users for key recovery, and create new encryption key pairs for users.

Depending on the organization's security policy, the Administrator may also be able to change default browser certificate lifetimes and default encryption and verification policies. They can also review audit logs and issue new CRLs.

administrator

The word "administrator" (with a lowercase "a") refers generally to all predefined administrative roles which comprise Security Officers, Administrators, Directory Administrators, and Auditors.

authentication

The process of proving your identity.

authorization code

An alphanumerical code (for example, CMTJ-8VOR-VFNS) generated when an administrative user creates a new user or recovers an existing user, required along with its corresponding "reference number". Authorization codes can only be used once.

browser certificate

A certificate issued to end-users. The browser certificate contains the signature of the CA that issued it.

CA

Certification Authority. Part of Security Manager that ensures the trustworthiness of electronic identities. It issues electronic identities in the form of public key certificates, policy certificates, cross-certificates, certificate revocation lists, and authority revocation lists. Finally, it signs the certificates with its signing key, thereby ensuring the integrity of the electronic identity.

See "certificate".

CA certificate

A certificate issued to a CA containing the CA verification public key. The Web server and users' browsers must import this certificate and use the verification public key contained within it to verify the CA signature on Web server and browser certificates when setting up a secure session.

The CA certificate is also imported into the browser used to administer the Enrollment Server for Web. The browser uses the CA certificate to verify the identity of the Web server when the Enrollment Server for Web administrator attempts to connect to it.

CA signing key pair

The key pair of the CA. It comprises the CA signing private key and CA verification public key. The CA signing private key digitally signs client certificates and the CA verification public key verifies digital signatures.

CA signing private key

The private key portion of the CA signing key pair. The CA signing private key is used to sign browser and Web server certificates digitally. The signature on these certificates can be verified with the CA verification public key. A CA signs all certificates it issues using the CA signing key.

CA verification public key

The public key portion of the CA signing key pair. It verifies client certificates that have been signed by the CA signing private key.

CAPI

See "CryptoAPI".

CDP

CRL Distribution Point. Points uniquely distributed throughout a Directory containing multiple CRLs, that enable user's certificates to contain a pointer to the appropriate distribution point in order for Entrust client software, such as Security Provider, to find the corresponding CRL for a given certificate.

certificate

A collection of publicly available information about an entity that is signed by the "CA" and stored in an LDAP-compliant Directory. A certificate is used to identify people and resources uniquely over networks such as the Internet. Certificates also enable secure, confidential communication between two parties.

A certificate typically includes a variety of information pertaining to its owner and to the CA that issued it, including the name of the holder and other identification information required to uniquely identify the holder (such as the URL of the Web server using the certificate), or an individual's e-mail address; the holder's public key, the name of the Certification Authority that issued the certificate, a serial number, and the validity period (or lifetime) of the certificate (a start and an end date).

The CA issues all certificates according to the format and structure of the X.509 version 3 standard.

certificate store

Contains user and machine certificates, and keeps track of the CSP associated with each certificate.

See "Microsoft Local Computer Certificate Store".

certificate type

Determines how Security Manager customizes a particular issued certificate.

CGI

Common Gateway Interface program. A CGI program is any program designed to accept and return data that conforms to the CGI specification. The program could be written in any programming language, including C, Perl, Java, or Visual Basic.

CGI programs are programs that allow Web users to dynamically interact with Web servers. For example, when a user fills out and submits an online form, the Web server uses a CGI program to process the form's data. The Web server can then provide a personalized response based on this information.

CRL

Certificate Revocation List. A signed and timestamped certificate containing the serial numbers of public key certificates that have been revoked, and a reason for each revocation.

Other users access this information from the Directory to check the trustworthiness of the certificates of the users for whom they intend to encrypt files.

cross-certification

A process by which two CAs securely exchange keying information so that each can effectively certify the trustworthiness of the other's keys. Once two (or more) domains have cross-certified, users within those domains can validate each other's certificates.

CryptoAPI

Microsoft Cryptographic Application Programming Interface. Microsoft Windows API that provides PKI client capabilities to the desktop operating system, allowing applications to take advantage of desktop cryptographic functionality built in by Microsoft.

CAPI has two layers. An interface layer is exposed to the client applications. Underneath is a layer of drivers that perform the cryptographic functions such as encrypting and hashing. The drivers are called Cryptographic Service Providers (CSP). See "CSP".

CSP

Cryptographic Service Provider. Acts as an interface between Microsoft CryptoAPI and private key stores, and performs all cryptographic operations for Microsoft applications and any third-party applications that are properly built on the Windows security framework, such as encrypting and decrypting data, verifying signatures, signing data, and verifying certificates.

CSP type

Cryptographic Service Provider type. A group of organized CSPs with each group having its own set of data formats.

CSR

Certificate Signing Request. Contains information that Security Manager uses to create Web server certificates.

decrypt

The act of restoring an encrypted file to its original, unprotected state.

decryption private key

Decrypts data that has been encrypted with its corresponding "encryption public key". For example, Bob is the only user who has access to his decryption private key, which he uses to decrypt information that has been encrypted for him by other users with his encryption public key.

digital ID

Set of cryptographic data that defines an entity, consisting of a public portion (user's public certificates) and a private portion (user's private keys), and can be used to verify one's identity.

digital signature

Provides a guarantee to a recipient that the signed file came from the person who sent it, and that it was not altered since it was signed. Any other user who has the corresponding verification public key can verify the signature. A digital signature is the result of making a mathematical summary (known as a hash) of data and encrypting the hash using a user's signing private key.

Directory

An LDAP-compliant directory service that contains the names of all Security Manager users and acts as a repository for users' encryption public key certificates.

The Directory is an online database that updates dynamically—that is, it updates as changes are made to the information it contains. It also contains entries for the Certification Authority, optionally, the Directory Administrator, and the organization itself. The Directory also keeps updated lists of revoked certificates (CRLs), and lists of revoked cross-certificates (ARLs).

DN

Distinguished Name. The complete name of Directory entry that uniquely identifies a person or entity; DNs of all Entrust Authority Security Manager users are stored in the Directory.

Dual Band

A cellular phone that can operate on two of three different GSM frequencies in Europe and North America: 900, 1800, and 1900MHz.

See "Tri-Band".

encrypt

The act of rendering a file completely unreadable. This means no one, including the owner of the file can read the file's contents until it is decrypted. Only the owner and the authorized recipients can decrypt the file. The owner determines authorized recipients.

encryption public key

Encrypts data that can be decrypted with the corresponding "decryption private key".

end user

Refers to a user who has successfully enrolled for an Entrust digital ID.

Enrollment Server for WAP

Issues certificates to devices that must use WAP to communicate.

See"WAP".

Enrollment Server for Web

The Web server that hosts Enrollment Server for Web. You must issue the Web server hosting the Enrollment Server for Web a Web server certificate. To validate the Web server certificate, the CA's certificate must be installed on the browser that administers the Enrollment Server for Web.

Entrust Administrator

See "Administrator".

Entrust security store

A password protected file that acts as a storage medium for user's Entrust digital IDs when created with an Entrust CSP.

GPRS

General Packet Radio System. A packet-based wireless communications service designed to boost the speed of mobile cellular phone networks from 9.6Kbytes to 115Kbytes per second and allows users continuous connection to the Internet.

GSM	Global System for Mobile Communication. The standard used by most international mobile phone networks. GSM currently uses three different frequencies in Europe, Asia, and North America. See "Tri-Band".
HTTPS	HyperText Transfer Protocol Secure. A protocol for Web sites that require SSL.
IAS	Microsoft Internet Authentication Service. Used to authenticate, authourize, and account for dial-up, VPN, wireless, and Ethernet connections to your network.
IBM HTTP Server	An IBM Web server application supported by Enrollment Server for Web.
IIS	Microsoft Internet Information Server. This is a Web server application supported by Enrollment Server for Web.
IPSec	IP Security. IPSec is a set of standard protocols developed by the Internet Engineering Task Force (IETF) so that data can be exchanged securely at the IP layer. For IPSec to work, the sending and receiving devices must share a verification public key to authenticate each other.
key	A special number that an encryption algorithm uses to change data, making that data secure.
key lifetime	The length of time a key is valid. All keys have a specific lifetime except the decryption private key which never expires.
key pairs	Asymmetric keys come in pairs. Security Manager uses asymmetric keys in both encryption and digital signature operations.
key recovery	Process of generating new activation codes for a user who has lost their security store or has forgotten their password.
key store	Holds private keys for users and machines and makes them accessible to the "CSP" that manages it.
key update	Replaces old key pairs with new ones. During key update, new public key certificates that have no relation to the old keys and certificates are created and users receive new keys and certificates securely.
Microbrowser	The software built into cellular phones, personal digital assistants, and SIM cards that enables these devices to access and display WAP pages from the Internet. See"SIM card".
Microsoft Local Computer Certificate Store	Contains certificates, CRLs, and Certificate Trust Lists (CTLs) that are used by CAPI-enabled devices such as VPN, Internet Authentication Services (IAS), domain controllers, and so on.

non-repudiation

Irrefutable evidence that makes it impossible to reject the validity of one's signature on a file or transaction.

An Entrust digital signature provides non-repudiation. It also provides authentication (guarantees who signed the data) and data integrity (recipients of signed data are alerted if the data has been tampered with).

PDA

Personal Digital Assistant. A digital personal organizer that offers e-mail, word processing, and spreadsheet functions.

private key

The portion of a key pair that is kept secret by the owner of the key pair.

public key

The portion of a key pair that is available in the Directory.

recovery

The operation performed on users who have lost or corrupted their security store. It generates a new signing key pair and retrieves the current encryption public key certificate, decryption private key history, verification public key certificate, and CA verification public key certificate.

reference number

A number (for example, 91480165), obtained from an Security Manager administrator, which is used along with an "authorization code" to create a new certificate. A reference number can only be used once.

revoking browser certificates

The process of stopping a user from using Entrust. You must revoke a user's encryption and verification certificates when the user is no longer trusted (for example, if you suspect that an attacker has compromised their Entrust profile and password). You can also revoke certificates even when there is no suspicion of compromise (for instance, when a user's DN changes).

S/MIME

Secure Multi-Purpose Internet Mail Extensions. S/MIME is a secure method of sending e-mail that uses the RSA encryption system. S/MIME is included in most Web browsers and is used by various other vendors that make messaging products.

Security Officer

A predefined administrative role in Security Manager. The main role of a Security Officer is to set and administer an organization's security policy and to cross-certify with other organizations, if required. In many organizations, Security Officers are responsible for setting policies to protect sensitive and valuable data and assigning secure electronic identities in the form of certificates.

By default, Security Officers can also add, deactivate, and delete other Security Officers, Administrators, Directory Administrators, and end users. They can also increase the number of users in a CA.

See "Administrator".

Security Manager — Refers to the family of core Entrust products. Security Manager comprises an encryption engine, a Directory, a database, and administration tools. Security Manager is required as the basis for all managed security solutions from Entrust.

Security Manager Administration — The application in which you administer an Security Manager system. Security Officers, Entrust Administrators, and other administrative users can use Security Manager Administration to set the security policy, add users, deactivate users, reactivate users, and so on.

Security Manager user — Anyone who uses Entrust Entelligence™ Desktop Manager (and other Entrust Ready applications), Security Manager Administration, or Entrust Authority Security Manager Control.

security store — The storage medium for a user's Entrust digital ID.

See "Entrust security store".

signing private key — Encrypts a hash value that is decrypted with the corresponding verification public key. A user, for example Alice, is the only one who has access to her signing private key. Alice uses her signing private key to encrypt the hash value of a file she is signing. Users verify the signature by successfully decrypting the hash value using Alice's verification public key.

SIM card — Subscriber Identity Module card. A SIM card is the chip included in each WAP-enabled cellular phone and personal digital assistant that contains information about the user (for example, the user's address).

smart card — An electronic memory card about the size of a credit card used primarily for storing data. Smart cards can contain an integrated circuit that can make decisions.

Smart cards can be used to retrieve and store certificates.

Smartphone — A device that combines the functionality of a mobile cellular phone in a PDA.

See "PDA".

SMS — Short Message Service.Text messages that are sent and which can be received by cellular phones.

SSL

Secure Sockets Layer. A security protocol that provides communications privacy over the Internet. The protocol uses a private key to encrypt data transferred between client and server applications. The protocol allows these applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The protocol also allows Web sites and users to authenticate one another's certificates.

The next generation of SSL is a protocol known as Transport Layer Security (TLS). See "TLS".

Both Netscape and Microsoft browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. Typically, Web pages that require SSL start with `https` instead of `http`.

Stronghold

A Web server application supported by Enrollment Server for Web.

symmetric key

A single key that both encrypts and decrypts the same data.

Sun ONE

A Sun Web server application supported by Enrollment Server for Web.

third-party trust

A situation in which two people implicitly trust each other, even though they have not previously established a personal relationship. In this situation, two people can trust each other if they both have a relationship with a common third party, because the third party can vouch for the trustworthiness of the two people.

The need for third-party trust is fundamental to any large-scale implementation of a network security product. Public-key cryptography requires access to users' public keys. However, in a large-scale network, it is impractical and unrealistic to expect each user to have previously established relationships with all other users. Plus, because users' public keys must be widely available, the link between a public key and a person must be guaranteed by a trusted third party to prevent masquerading. In effect, users implicitly trust any public key certified by the third party because their organization owns and securely operates the third-party certification agent.

TLS

Transport Security Layer. A newer version of SSL developed by the Internet Engineering Task Force (IETF). It is a protocol for transmitting encrypted data over TCP or IP networks. It allows users and Web sites to encrypt private information and authenticate one another's certificates.

See "SSL".

Tri-Band

A phone that can operate on three different GSM frequencies:

- 900MHz
- 1800MHz
- 1900MHz

This enables cellular phones and personal digital assistants to use networks in Europe, Asia, and parts of North America.

See "GSM".

verification public key

The public key portion of a signing key pair used to verify data that has been signed by the corresponding "signing private key". The verification public key is stored in a certificate called the verification public key certificate. This certificate is digitally signed by the Certification Authority (CA) to verify that the public key within it is the authentic public key of the identified user.

VPN

Virtual Private Network. A private network that is connected together through public wires such as the Internet. These networks can maintain privacy over public wires by using encryption and other security mechanisms to exclude unauthorized users from gaining access or tampering with the data. Enrollment Server for Web allows you to issue certificates to VPN devices.

WAP

Wireless Application Protocol. WAP is a global specification for a set of protocol that let users of wireless devices, such as cellular phones and personal digital assistants, to access the Internet, World Wide Web, newsgroups, e-mail and other services.

WBMP

Wireless Bitmap. A graphic file format. WBMP graphics can be displayed on WAP devices such as cellular phones and personal digital assistants.

Web server certificate

A certificate issued to a Web server that enables SSL and contains the signature of the CA that issued it.

WML

Wireless Markup Language. WML is the open language used in scripting WAP pages that allows text to be displayed on cellular phones and personal digital assistants.

WTLS

Wireless Transport Layer Security. WTLS is a session layer in the WAP architecture. WTLS provides connection-based services to the application layer.

Security Manager can issue WTLS certificates using a wide variety of CA hardware devices.

Index

E

G

I

K

M

N

O

P

R

S

T

U

V

W