

# **Agent's Guide**

## *Red Hat Certificate System*

Version 7.1



April 2005

Red Hat, Inc.

1801 Varsity Drive  
Raleigh NC 27606-2072 USA  
Phone: +1 919 754 3700  
Phone: 888 733 4281  
Fax: +1 919 754 3701  
PO Box 13588  
Research Triangle Park NC 27709 USA

© 2001 Sun Microsystems, Inc. Used by permission. © 2005 by Red Hat, Inc. All rights reserved. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, V1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the [security@redhat.com](mailto:security@redhat.com) key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

# Contents

<b>About This Guide</b> .....	<b>7</b>
Who Should Read This Guide .....	7
What You Should Know .....	7
What's in This Guide .....	8
Conventions Used in This Guide .....	9
Documentation .....	10
<b>Chapter 1 Agent Services</b> .....	<b>13</b>
Overview of Certificate System .....	13
Agent Tasks .....	16
Certificate Manager Agent Services .....	17
Registration Manager Agent Services .....	19
Data Recovery Manager Agent Services .....	19
Online Certificate Status Manager Agent Services .....	20
Forms for Performing Agent Operations .....	21
Accessing Agent Services .....	24
Administrator/Agent Certificate Enrollment .....	24
Agent Services Entry Page .....	27
Services Summary Page .....	27
<b>Chapter 2 Working with Certificate Profiles</b> .....	<b>29</b>
About Certificate Profiles .....	29
How Certificate Profiles Work .....	31
Enabling and Disabling Certificate Profiles .....	32
Getting Certificate Profile Information .....	32
End User Certificate Profile .....	32
Policy Information .....	33

To Approve a Certificate Profile .....	33
To Disapprove a Certificate Profile .....	33
<b>Chapter 3 Handling Certificate Requests .....</b>	<b>35</b>
Managing Requests .....	35
Listing Certificate Requests .....	39
Selecting a Request .....	41
Approving Requests .....	42
Adjusting, Verifying, and Approving a Certificate Profile Request .....	43
Assigning a Request .....	44
Adjusting, Verifying, and Approving a Request .....	45
Other Options for Handling Requests .....	48
Sending an Issued Certificate to the Requester .....	49
<b>Chapter 4 Finding and Revoking Certificates .....</b>	<b>53</b>
Basic Certificate Listing .....	53
Advanced Certificate Search .....	55
Examining Certificates .....	59
Revoking Certificates .....	62
Searching for Certificates to Revoke .....	62
Revoking One or More Certificates .....	63
Revoking One Certificate .....	63
Revoking Multiple Certificates .....	64
Confirming a Revocation .....	65
Managing the Certificate Revocation List .....	66
Viewing or Examining CRLs .....	66
Updating the CRL .....	67
<b>Chapter 5 Publishing to a Directory .....</b>	<b>69</b>
Working with a Directory Server .....	69
Automatic Directory Updates .....	69
Manual Directory Updates .....	70
Updating the Directory with Changes .....	70
<b>Chapter 6 Recovering Encrypted Data .....</b>	<b>73</b>
Finding and Recovering Keys .....	73
Finding Archived Keys .....	73
Selecting a Key .....	76
Recovering Keys .....	77
Remote Recovery Authorization .....	79
Viewing Key Service Requests .....	80
Listing Key Service Requests .....	80

Selecting a Request .....	82
<b>Chapter 7 Managing OCSP Service Related Tasks .....</b>	<b>85</b>
Listing CAs Identified by Online Certificate Status Manager .....	85
Identifying a CA to Online Certificate Status Manager .....	86
Adding a CRL to Online Certificate Status Manager .....	88
Checking the Revocation Status of a Certificate .....	90
<b>Index .....</b>	<b>91</b>



# About This Guide

This guide describes the Agent Services interface that Red Hat Certificate System (CS) agent uses to administer a subsystem's certificates and keys.

This preface contains the following sections:

- Who Should Read This Guide
- What You Should Know
- What's in This Guide
- Conventions Used in This Guide
- Documentation

## Who Should Read This Guide

This guide is intended for Certificate System agents—that is, privileged users designated by the Certificate System administrator to manage requests from end entities for certificate-related services. Each installed CS manager (Certificate Manager, Registration Manager, Data Recovery Manager, and Online Certificate Status Manager) can have one or more agents.

## What You Should Know

Before reading this guide, you should be familiar with the basic concepts of public-key cryptography and the Secure Sockets Layer (SSL) protocol. These include the following topics:

- Encryption and decryption

- Public keys, private keys, and symmetric keys
- Digital signatures
- The role of digital certificates in a public-key infrastructure (PKI)
- Certificate hierarchies
- SSL cipher suites
- The purpose of and major steps in the SSL handshake

## What's in This Guide

This guide describes the duties of the agents for the various CS subsystems and explains how to accomplish each task.

Chapter 1, “Agent Services”	Provides an overview of the product and identifies the different kinds of users, including agents. The chapter also summarizes the tasks of each subsystem agent and lists the HTML forms you use to perform agent tasks. Finally, the chapter explains how to access the Agent Services pages and forms.
Chapter 2, “Working with Certificate Profiles”	Provides an overview of the profiles feature and details how an agent enables and disables profiles.
Chapter 3, “Handling Certificate Requests”	As a Certificate Manager or Registration Manager agent, you are responsible for handling requests for certificates that are made by end entities (end users, server administrators, or other CS subsystems) using manual enrollment. This chapter describes the general procedure for handling requests and explains how to handle different aspects of certificate request management.
Chapter 4, “Finding and Revoking Certificates”	Explains how, as a Certificate Manager agent, you can use the Agent Services page to find and examine a specific certificate issued by Certificate System, or retrieve a list of certificates that match specified criteria. This chapter also explains how to revoke certificates, and manage the certificate revocation list.



Chapter 5, “Publishing to a Directory”	Describes how a Certificate Manager agent can update the LDAP directory with the current status of certificates.
Chapter 6, “Recovering Encrypted Data”	Describes how to process key recovery requests, and how to recover stored encrypted data when the encryption key has been lost. This service is only available when the Data Recovery Manager is installed.
Chapter 7, “Managing OCSP Service Related Tasks”	Describes how to handle tasks related to the CS OCSP responder, Online Certificate Status Manager. This service is only available when the Online Certificate Status Manager subsystem is installed.

## Conventions Used in This Guide

The following conventions are used in this guide:

Monospaced font	<p>This typeface is used for any text that appears on the computer screen or text that you should type. It’s also used for filenames, functions, and examples.</p> <p>Example: <code>Server Root</code> is the directory where the CS binaries are kept.</p>
<i>Italic</i>	<p>Italic type is used for emphasis, book titles, and glossary terms.</p> <p>Example: This control depends on the access permissions the <i>super administrator</i> has set up for you.</p>
<b>Boldface</b>	<p>Boldface type is used for various UI components such as captions and field names, and the terminology explained in the glossary.</p> <p>Example:</p> <p><b>Rotation frequency.</b> From the drop-down list, select the interval at which the server should rotate the active error log file. The available choices are Hourly, Daily, Weekly, Monthly, and Yearly. The default selection is Monthly.</p>
Monospaced [ ]	Square brackets enclose commands that are optional.

Example:

```
PrettyPrintCert <input_file> [<output_file>]
```

<input\_file> specifies the path to the file that contains the base-64 encoded certificate.

<output\_file> specifies the path to the file to write the certificate. This argument is optional; if you don't specify an output file, the certificate information is written to the standard output.

Monospaced <>

Angle brackets enclose variables or placeholders. When following examples, replace the angle brackets and their text with text that applies to your situation. For example, when path names appear in angle brackets, substitute the path names used on your computer.

Example: Using Netscape Communicator 4.7 or later, enter the URL for the Red Hat Administration Server:

```
http://<hostname>:<port_number>
```

/

A slash is used to separate directories in a path.

Example: Except for the Security Module Database Tool, you can find all the other command-line utilities at this location:

```
<server_root>/bin/cert/tools
```

Notes and Cautions:

---

**NOTE** A note alerts you to information that may be of interest to you.

---



---

**CAUTION** A caution signals a potential risk of losing data, damaging software or hardware, or otherwise disrupting system performance.

---

## Documentation

The document set for Certificate System also contains the following guides:

*Managing Servers with Red Hat Console* - Provides background information on basic cryptography concepts and the role of Red Hat Console.

*CS Administrator's Guide* - Describes how to plan for, install, and administer CS.

*CS Command-Line Tools Guide* - Provides detailed reference information on CS tools.

*CS Customization Guide* - Provides detailed reference information on customizing the HTML-based agent and end-entity interfaces.

*CS Agent's Guide* (this guide) - Provides detailed reference information on CS agent interfaces. To access this information from the Agent Services pages, click any help button.

For the latest information about Certificate System, including current release notes, complete product documentation, technical notes, and deployment information, check this site:

<http://www.redhat.com/docs/manuals/cert-system/>



# Agent Services

This chapter describes the role of the privileged users called *agents* in managing Red Hat Certificate System (CS). It also introduces the tools that agents use to administer service requests.

This chapter contains the following sections:

- Overview of Certificate System
- Agent Tasks
- Forms for Performing Agent Operations
- Accessing Agent Services

## Overview of Certificate System

Certificate System is a highly configurable set of software components and tools for creating, deploying, and managing certificates. The standards and services that facilitate the use of public-key cryptography and X.509 version 3 certificates in a networked environment are collectively called the *public key infrastructure (PKI)* for that environment. In any PKI, a *certificate authority (CA)* is a trusted entity that issues, renews, and revokes certificates. An *end entity* is a person, router, server, or other entity that uses a certificate to identify itself.

To participate in a PKI, an end entity must *enroll*, or register, in the system. The end entity typically initiates enrollment by giving the CA some form of identification and a newly generated public key. The CA uses the information provided to *authenticate*, or confirm, the identity; it then issues the end entity a certificate that associates that identity with the public key, and signs the certificate with the CA's own private signing key.

End entities and CAs may be in different geographic or organizational areas or in completely different organizations. CAs may include third parties that provide services through the Internet as well as the root CAs and subordinate CAs for individual organizations. Policies and certificate content may vary from one organization to another. End-entity enrollment for some certificates may require physical verification, such as an interview or notarized documents, while enrollment for others may be fully automated.

To meet the widest possible range of configuration requirements, Certificate System permits the independent installation of four separate subsystems, or “managers,” that typically play distinct roles:

- **Certificate Manager**—A Certificate Manager functions as a root or subordinate certificate authority. This subsystem issues, renews, and revokes certificates, generates certificate revocation lists (CRLs). It can publish certificates to a Lightweight Directory Access Protocol (LDAP) directory and files, and CRLs to an LDAP directory, a file, and an Online Certificate Status Protocol (OCSP) responder. The Certificate Manager can be configured to accept requests from end entities, Registration Managers, or both, and can process requests either manually (that is, with the aid of a human being) or automatically (based entirely on customizable policies and procedures). When set up to work with a Registration Manager, the Certificate Manager processes requests and returns the signed certificates to the Registration Manager for distribution to the end entities. (For an overview of the role of certificate authorities and related concepts of public-key cryptography, see Appendix D of *Managing Servers with Red Hat Console*.)

Note that the publishing tasks can be performed by the Certificate Manager only. The Certificate Manager also has a built-in OCSP service, enabling OCSP-compliant clients to directly query the Certificate Manager about the revocation status of a certificate that it has issued. In certain PKI deployments, it might be convenient to use the Certificate Manager’s built-in OCSP service, instead of a Online Certificate Status Manager.

- **Registration Manager**—A Registration Manager is an optional component in the PKI and can be used to separate the registration process from the certificate-signing process. The Registration Manager performs a subset of the end-entity tasks performed by the Certificate Manager, such as enrollment or renewal, on behalf of the Certificate Manager. A Registration Manager is typically installed on a different machine from the Certificate Manager that it serves. After the Registration Manager approves requests, it forwards them to this Certificate Manager, which trusts the Registration Manager to provide reliable authentication services and therefore trusts any signed requests it submits. The Certificate Manager processes the requests and issues the certificates. The Registration Manager then distributes the certificates to the end entities.

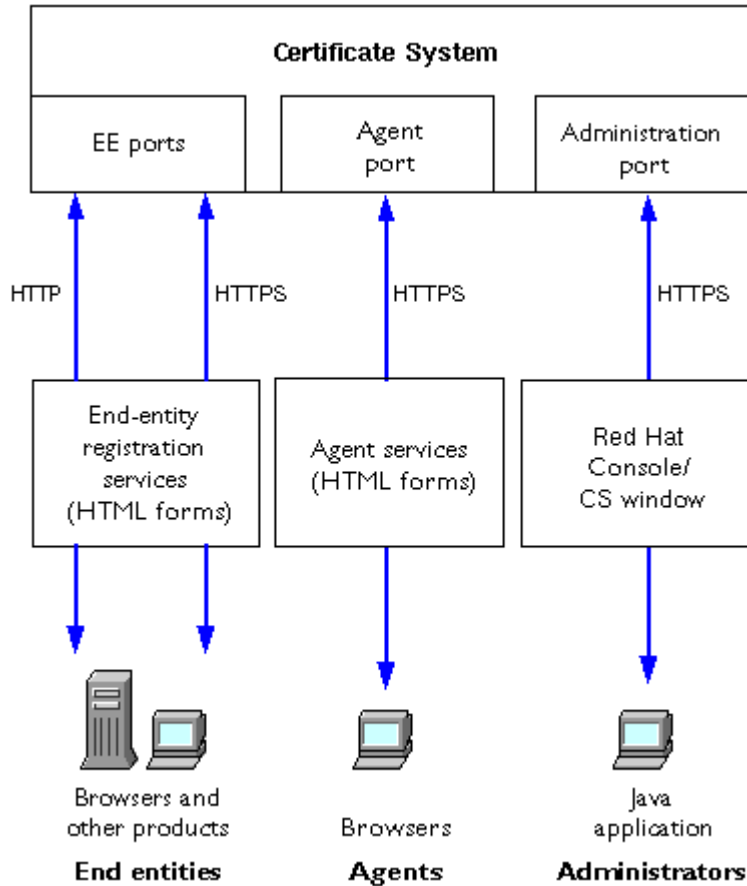
- **Data Recovery Manager**—A Data Recovery Manager oversees the long-term archival and recovery of private encryption keys for end entities. A Certificate Manager or Registration Manager can be configured to archive end entities' private encryption keys with a Data Recovery Manager as part of the process of issuing new certificates. The Data Recovery Manager is useful only if end entities are encrypting data (using applications such as S/MIME email) that the organization may need to recover someday. It can be used only with client software that supports dual key pairs—that is, two separate key pairs, one for encryption and one for digital signatures. This service is available in newer clients only; for example, Communicator versions 4.7x (with Netscape Personal Security Manager installed), Netscape 6.2, and Netscape 7.x all support generation of dual key pairs. The Data Recovery Manager archives encryption keys. It does not archive signing keys, since such archival would undermine nonrepudiation properties of dual-key certificates.
- **Online Certificate Status Manager**—A Online Certificate Status Manager performs the task of an online certificate validation authority, by enabling OCSP-compliant clients to do real-time verification of certificates. The Online Certificate Status Manager can receive CRLs from multiple Certificate Managers and clients can query the Online Certificate Status Manager for the revocation status of certificates issued by all these Certificate Managers. For example, in a PKI comprising multiple CAs (a root CA and many subordinate CAs) each CA can be configured to publish its CRL to the Online Certificate Status Manager. This way, all clients in the PKI deployment can verify the revocation status of a certificate by querying the Online Certificate Status Manager.

Note that an online certificate-validation authority is often referred to as *OCSP responder*.

Since CAs can delegate some responsibilities to subordinate CAs, a Certificate Manager might delegate responsibilities to one or more levels of subordinate Certificate Managers, and each Certificate Manager can interact with multiple Registration Managers. Therefore many complex variations are possible.

Three kinds of entities can access CS subsystems: administrators, agents, and end entities. Administrators are responsible for the initial setup and ongoing maintenance of the subsystems. Administrators can designate users with special privileges, called agents, for each subsystem. Agents manage day-to-day interactions with end entities (people, SSL-enabled servers, routers, and so on) and other aspects of the PKI. This guide describes the tasks that agents can perform. End entities access Registration Manager or Certificate Manager subsystems to enroll in a PKI and to take part in other life-cycle management operations, such as renewal or revocation.

Figure 1-1 shows the ports used by administrators, agents, and end entities. All agent and administrator interactions with CS subsystems occur over HTTPS. End-entity interactions can take place over HTTP or HTTPS.

**Figure 1-1** Certificate System and its users

## Agent Tasks

The designated agents for each subsystem are responsible for the everyday management of end-entity requests and other aspects of the PKI:

- Certificate Manager agents manage certificate requests received by the Certificate Manager subsystem, maintain and revoke certificates as necessary, and maintain global information about certificates.
- Registration Manager agents manage the certificate requests received by the Registration Manager subsystem.



- Data Recovery Manager agents initiate the recovery of lost keys, and can obtain information about key service requests and archived keys.
- Online Certificate Status Manager agents can perform tasks such as checking which CAs are currently configured to publish their CRLs to the Online Certificate Status Manager, identifying a Certificate Manager to the Online Certificate Status Manager, adding CRLs directly to the Online Certificate Status Manager, and viewing the status of OCSP service requests submitted by OCSP-compliant clients.

To perform the privileged operations of an agent, you use the CS Agent Services pages. To access these pages, you must have a personal SSL client certificate, and the CS administrator must have identified you as a privileged user in the user database. For more information on how to get set up as a privileged user, see *Administrator's Guide*.

## Certificate Manager Agent Services

The default entry page to the Certificate Manager agent services is shown in Figure 1-2. To access these pages, you must be a designated Certificate Manager agent and your client software must have a valid certificate identifying you as such.

**Figure 1-2** Certificate Manager Agent Services page

Red Hat  
Certificate System

### Agent Services

Certificate Manager

**List Requests**

Use this form to show a list of certificate requests.

Request type:

Request status:

Starting request identifier:   
(optional)

Find first  records Help

As a Certificate Manager agent, you can perform the following tasks:

- Handle certificate requests.

You can list the certificate service requests received by the Certificate Manager subsystem, assign requests to yourself, reject or cancel requests, and approve requests for certificate enrollment. See Chapter 3, “Handling Certificate Requests.”

- Find certificates.

You can search for individual certificates, or search for and list certificates by various criteria, then display the details of certificates you have found. See Chapter 4, “Finding and Revoking Certificates.”

- Revoke certificates.

If a user’s key has been compromised, you need to revoke the user’s certificate to ensure that the key is not misused. You may also need to revoke the certificates of users who have left the organization. You can use Certificate Manager Agent Services to find and revoke a specific certificate or a set of certificates. Users can also revoke their own certificates. See “Revoking Certificates” on page 62.

- Update the CRL.

The Certificate Manager maintains a public list of certificates that have been revoked, called the certificate revocation list (CRL). The list is usually maintained automatically, but you may sometimes need to use the Certificate Manager Agent Services page to update the list manually. See “Updating the CRL” on page 67.

- Publish certificates to a directory.

You can set up Certificate System to publish certificates and lists of revoked certificates in an LDAP directory. Certificate information is usually published automatically, but you may sometimes need to use the Certificate Manager Agent Services page to update the directory manually. See Chapter 5, “Publishing to a Directory.”

- Manage Certificate Profiles.

The Agent user can enable and disable Certificate Profiles. The Agent must temporarily disable a profile so the administrator can use the Admin interface to make detailed changes to the profile itself. Once the changes have been made, the agent can re-enable the profile for regular use.

## Registration Manager Agent Services

The default entry page to the Registration Manager agent services is shown in Figure 1-3. To access these pages, you must be a designated Registration Manager agent and your client software must have a valid certificate identifying you as such.

**Figure 1-3** Registration Manager Agent Services page

The screenshot shows the Red Hat Certificate System Agent Services interface. The top navigation bar includes the Red Hat logo and the text 'Certificate System' and 'Agent Services'. Below this, a sub-header reads 'Registration Manager'. A sidebar on the left contains a link for 'List Requests'. The main content area is titled 'List Requests' and includes the instruction: 'Use this form to show a list of certificate requests.' The form contains three input fields: 'Request type:' with a dropdown menu set to 'Show enrollment requests', 'Request status:' with a dropdown menu set to 'Show pending requests', and 'Starting request identifier: (optional)' with an empty text box. At the bottom of the form, there is a 'Find' button, a 'first' label, a text box containing the number '5', a 'records' label, and a 'Help' button.

As a Registration Manager agent, you can handle certificate requests. You can list the certificate service requests received by the Registration Manager subsystem, assign requests to yourself, reject or cancel requests, clone requests, and approve enrollment requests to be passed on to the Certificate Manager for issuance. The agent can also update and validate requests making use of Certificate Profiles. See Chapter 3, “Handling Certificate Requests.”

## Data Recovery Manager Agent Services

The default entry page to the Data Recovery Manager agent services is shown in Figure 1-4. To access these pages, you must be a designated Data Recovery Manager agent and your client software must have a valid certificate identifying you as such.

**Figure 1-4** Data Recovery Manager Agent Services page

As a Data Recovery Manager agent, you can perform the following tasks:

- List key recovery requests from end entities.
- List or search for archived keys.
- Initiate the recovery of private data-encryption keys.

Key recovery requires the authorization of one or more *recovery agents*. The administrator for the Data Recovery Manager designates recovery agents. Typically, several recovery agents own portions of the storage key for the Data Recovery Manager. The approval of  $m$  of a total of  $n$  agents is required to authorize key recovery. The values of  $m$  and  $n$  for your installation of the Data Recovery Manager is determined by the administrator in charge of the subsystem.

For more information on these tasks, see Chapter 6, “Recovering Encrypted Data.”

## Online Certificate Status Manager Agent Services

The default entry page to the Online Certificate Status Manager agent services is shown in Figure 1-5. To access these pages, you must be a designated Online Certificate Status Manager agent and your client software must have a valid certificate identifying you as such.

**Figure 1-5** Online Certificate Status Manager Agent Services page

As an Online Certificate Status Manager agent, you can perform the following tasks:

- Checking which CAs are currently configured to publish their CRLs to the Online Certificate Status Manager.
- Identifying a Certificate Manager to the Online Certificate Status Manager.
- Adding CRLs directly to the Online Certificate Status Manager.
- Checking the revocation status of a certificate by submitting it to the Online Certificate Status Manager.

For more information on these tasks, see Chapter 7, “Managing OCSP Service Related Tasks.”

## Forms for Performing Agent Operations

The agent services consist of a form-based HTML interface that is part of your Certificate System installation. The CS administrator designates particular users as agents for each installed subsystem (Certificate Manager, Registration Manager, Data Recovery Manager, and Online Certificate Status Manager). Only a designated agent for a subsystem can use the Agent Services interface for that subsystem. In addition, you must have a personal client SSL certificate to access the Agent Services interface.

As a subsystem agent with the proper certificate, you use the Agent Services page to access the forms you need to perform the agent tasks. Table 1-1 describes each of these HTML forms.

**Table 1-1** Forms used for agent operations

Form name	Description
List Requests (Certificate Manager and Registration Manager)	Use this form to examine, select, and process requests for certificate services. Both Certificate Manager and Registration Manager agents can use this form.  For instructions on using this form, see “Listing Certificate Requests” on page 39.
List Certificates (Certificate Manager)	Use this form to list certificates within a range of serial numbers. You can limit the list to valid certificates. Only Certificate Manager agents can use this form.  For instructions on using this form, see “Basic Certificate Listing” on page 53.
Search for Certificates (Certificate Manager)	Use this form to search for and list certificates issued by Certificate System. Only Certificate Manager agents can use this form.  This form allows you to search by subject name or by certificate type, the state of the certificate (expired, revoked, and so on), and the dates when the certificate was issued or revoked, expired, or became valid.  For instructions on using this form, see “Advanced Certificate Search” on page 55.
Revoke Certificates (Certificate Manager)	Use this form to search for and revoke certificates issued by Certificate System. Only Certificate Manager agents can use this form.  For instructions on using this form, see “Revoking Certificates” on page 62.
Update Revocation List (Certificate Manager)	Use this form to manually update the published list of revoked certificates. Only Certificate Manager agents can use this form.  For instructions on using this form, see “Managing the Certificate Revocation List” on page 66.
Update Directory Server (Certificate Manager)	Use this form to update the LDAP publishing directory with changes in certificate information (newly issued certificates, updated CRLs, and so on). Only Certificate Manager agents can use this form.  For instructions on using this form, see “Updating the Directory with Changes” on page 70.
List Requests (Data Recovery Manager)	Use this form to find and examine requests for key services. Only Data Recovery Manager agents can use this form.  For instructions on using this form, see “Viewing Key Service Requests” on page 80.

**Table 1-1** Forms used for agent operations *(Continued)*

Form name	Description
Search for Keys (Data Recovery Manager)	<p>Use this form to find and list specific archived keys. Only Data Recovery Manager agents can use this form.</p> <p>For instructions on using this form, see “Finding Archived Keys” on page 73.</p>
Recover Keys (Data Recovery Manager)	<p>Use this form to find and recover specific archived keys. Only Data Recovery Manager agents can use this form. You can select a key in the list returned by a search and initiate its recovery, which must be authorized by designated key recovery agents.</p> <p>For instructions on using this form, see “Recovering Keys” on page 77.</p>
Authorize Recovery (Data Recovery Manager)	<p>Use this form to remotely authorize a key recovery request initiated by another Data Recovery Manager agent. Key recovery agents do not have to be Data Recovery Manager agents if key recovery is handled locally; however, only key recovery agents who are also Data Recovery Manager agents can access this form.</p> <p>For instructions on using this form, see “Recovering Keys” on page 77.</p>
List Certificate Authorities (Online Certificate Status Manager)	<p>Use this form to list Certificate Managers that are currently configured to publish their CRLs to the Online Certificate Status Manager.</p> <p>For instructions, see “Listing CAs Identified by Online Certificate Status Manager” on page 85.</p>
Add Certificate Authority (Online Certificate Status Manager)	<p>Use this form to identify a Certificate Manager to the Online Certificate Status Manager.</p> <p>For instructions, see “Identifying a CA to Online Certificate Status Manager” on page 86.</p>
Add Certificate Revocation List (Online Certificate Status Manager)	<p>Use this form to add a CRL to the Online Certificate Status Manager’s internal database.</p> <p>For instructions, see “Adding a CRL to Online Certificate Status Manager” on page 88.</p>
Check Certificate Status (Online Certificate Status Manager)	<p>Use this form to check the status of OCSP service requests sent by OCSP-compliant clients.</p> <p>For instructions, see “Checking the Revocation Status of a Certificate” on page 90.</p>
Agent-Initiated User Enrollment (RA)	<p>Use this form to enable Directory based Agent-initiated User Enrollment. Once this feature is enabled agents can enroll users by using a simple enrollment form on the user’s behalf.</p>

**Table 1-1** Forms used for agent operations *(Continued)*

Form name	Description
Manage Certificate Profiles (CA,RA)	Use this form to Enable and Disable supported Certificate Profiles. Once a profile is disabled, the Administrator is free to make more detailed changes to the profile itself.
OCSP Service (CA)	Use this form to manage the operation of the CS internal OCSP service. This optional service can be enabled during the CS installation procedure.

## Accessing Agent Services

Access to the agent services forms requires certificate-based authentication. Only users who authenticate with the correct certificate and who have been granted the proper access privilege can access and use the forms. The operation uses the SSL protocol; that is, you connect to the server using HTTPS (not HTTP) on the SSL agent port. For example, if Certificate System is installed on a host named `CShost.example.com` and is running on port 8100, you invoke the Agent Services interface by using the following URL:

```
https://CShost.example.com:8100
```

The Agent Services pages are written in HTML and are intended to be customized. This document describes the default pages. If your administrator has customized these pages, yours may differ from those described here. Check with the CS administrator for information on your local installation.

## Administrator/Agent Certificate Enrollment

Immediately after installing any CS instance, the administrator must enroll for the initial administrator/agent certificate. This is the first user certificate that Certificate System issues.

The initial user is both an administrator and an agent. This person can create additional agents with the appropriate user privileges and issue them certificates. Since there is no agent yet to approve the request, a special enrollment form allows you to get this first certificate automatically.

After you submit this initial Administrator/Agent Certificate Enrollment form, it is automatically disabled, so that no one else can acquire a certificate without agent approval or some form of automated authentication. The system automatically adds the initial user to the list of agents.



To enroll for the first agent certificate, you should be working at the computer you intend to use as the agent, so that the new certificate will be installed in the browser you will be using to access the Agent Services pages. Follow these steps:

1. Open a web browser window.
2. To open the Administrator/Agent Certificate Enrollment form, type the following in a browser's URL field:

```
https://<hostname>:<admin_port>/ca/adminEnroll.html
```

where <hostname> is the fully qualified domain name of the machine on which Certificate System is installed (for example, CShost.example.com) and <admin\_port> is the TCP port specified during installation for communications over SSL with the administration console.

Because you have accessed an SSL port, Certificate System presents its server SSL certificate to your browser for authentication. This is the SSL server certificate that you created during installation. Because you just created it, it is not on your browser's list of trusted certificates. Before you see the Administrator/Agent Certificate Enrollment form, a series of dialog boxes appear that let you add the CS server certificate to your list of trusted certificates.

3. Complete the dialog boxes as instructed (the exact procedure depends on the browser you are using).
4. In the Administrator/Agent Certificate Enrollment form, enroll for a client SSL certificate as the system's first privileged user by entering the following information:

Authentication Information section:

**User ID.** The ID you entered for the CS administrator during installation.

**Password.** The password you specified for the CS administrator during installation.

Subject Name section (The subject name is the distinguished name (DN) that identifies the certified owner of the certificate.)

**Full name.** Name of administrator/agent.

**Login name.** User ID of administrator/agent.

**Email address.** Email address of administrator/agent.

**Organization unit.** Name of the organization unit to which the administrator/agent belongs.

**Organization.** Name of the company or organization the administrator/agent works for.

**Country.** Two-letter code for the administrator/agent’s country.

User’s Key Length Information section:

**Key Length.** The length of the private key that will be generated by your browser. This key corresponds to the public key that is part of the administrator/agent certificate.

5. Click Submit.
6. Follow the instructions your browser presents as it generates a key pair.
7. If authentication is successful, the new certificate will be imported into your browser, and you will be given an opportunity to make a backup copy.

Now you have a client authentication certificate in the name you specified. This special user, who was named as the initial administrator for Certificate System during installation, has been automatically designated as the first agent. This certificate allows you to access the Agent Services pages. As an agent, you can approve enrollment requests and start issuing new certificates. To access the CS windows in Red Hat Console, you use the user ID that you specified for the certificate and the corresponding password—both of which must correspond to the values you specified for the CS administrator during installation.

Note that after you submit the initial Administrative Enrollment form, it is no longer available from the agent port. If something goes wrong and you are unable to obtain the administrator/agent certificate, you must reset a parameter in the configuration file to make the initial administrative enrollment form available again. Follow these steps:

1. Stop Certificate System.

You can stop the server from either the command-line or from Red Hat Console. To do this from Red Hat Console, in the left frame of Red Hat Console, open the CS instance for which you want to display the Administrator/Agent Certificate Enrollment form. The server requests the password for the CS administrator. Enter the password. When the CS Console opens, go to the Tasks tab and click the icon labeled “Stop the Server.”

2. Go to this directory: `<server_root>/cert-<instance_ID>/config`
3. Open the `CS.cfg` file in a text editor, and find the following line:  
`CSGateway.enableAdminEnroll=false`
4. Change `false` to `true`, and save the file.
5. Start the server from the CS window where you stopped it. (Alternatively, right-click on the name of the instance in the left frame and choose Start Server.) At this point, the server asks you for the single sign-on password you specified during installation.
6. The next time you access the SSL agent port (via the browser), the Administrator/Agent Certificate Enrollment form will be available again.

## Agent Services Entry Page

Once you have obtained the initial/first agent certificate, you can view the Agent Services interface by going to the agent port.

1. Open a browser.
2. Go to the URL for the SSL agent port.

The URL is in this format: `https://<hostname>:<agent_port>`

3. In the Agent Services entry page, click the subsystem whose agent services you require.

The choices depend on which subsystems have been installed in the particular Certificate System instance. If you present a valid certificate and have been designated as an agent for a subsystem, you can access and use the Agent Services pages for that subsystem by clicking the link on this page.

If you do not yet have your certificate, click [Services Summary](#) to enroll for one. For more information, see “[Services Summary Page](#)” (the next section).

## Services Summary Page

If you want to access another gateway without looking up the port number, click [Services Summary](#) on the Agent Services entry page. The Services Summary page gives you access to each of the configured gateways: the HTTPS end-entity gateway, the HTTP end-entity gateway (if it has been enabled), and the Agent Services entry page.

If you do not yet have a certificate that allows you access to the Agent Services pages, go to one of the end-entity gateways and enroll for your certificate.



# Working with Certificate Profiles

As a Certificate Manager or Registration Manager agent, you are responsible for approving certificate profiles that have been configured by a CS administrator. You also manage and approve requests that come from certificate profile enrollments.

This chapter contains the following sections:

- About Certificate Profiles
- How Certificate Profiles Work
- Enabling and Disabling Certificate Profiles

## About Certificate Profiles

A certificate profile defines everything associated with the issuance of a particular type of certificate including the authentication method, the certificate content (defaults), constraints for values associated with that content that can be contained in this type of certificate, and the contents of the input and output forms associated with the certificate profile.

Enrollments requests are submitted to a particular certificate profile and are then subject to the defaults and constraints set up in that certificate profile whether the request is created from the input form associated with the certificate profile, or the request is created elsewhere and submitted as a pre formatted request. The certificate that is issued from a certificate profile request contains the content defined by the defaults with values derived from the values contained in the parameters associated with those defaults. The constraints provide rules for which content is allowable in the certificate, and defines allowable values for that content.

For example, a certificate profile could be set up for user certificates that defines all aspects of that certificate including the validity period of the issued certificate. A default can be set up that defines the validity period as two years. A constraint can be set up so that the validity period for certificates issued from requests submitted to this certificate profile

cannot exceed two years. When a user sends a request using the input page associated with this certificate profile, the certificate issued will contain the information specified in the defaults set up and will be valid for two years. If a user submits a pre formatted request that requests a certificate with a validity period of four years, the request will be rejected since the constraints allow a maximum of two years validity period for this type of certificate.

A set of certificate profiles have been pre built for the most common types of certificates issued. The pre built certificate profiles define defaults and constraints commonly associated with this type of certificate, associate the authentication method common for this type of enrollment, and define the needed inputs and outputs for the certificate profile.

An administrator can use these pre built certificate profiles, modify any or all of these by changing the authentication method, the defaults, the constraints used in each policy, the values assigned to any of the parameters in a policy, or the input and output. They can also create other certificate profiles either for other types of certificates, or for creating more than one certificate profile for a type of certificate. They might create more than one certificate profile for a particular type of certificate when they want to issue the same type of certificate with either a different authentication method or different definitions for the defaults and constraints. For example, an administrator might create two certificate profiles used for enrollment for SSL Server certificates where one certificate profile issues certificates with a validity period of six months and another certificate profile issues certificates with a validity period of two years.

A set of defaults and constraints have been pre built for the most commonly used certificate content and constraints. An administrator can set up additional defaults and constraints using the Certificate System SDK.

An input specifies how the enrollment page should be presented. An administrator can use inputs to add text fields to the enrollment page so that additional information can be gathered and used for the enrollment. The input values are used as values in the certificate. A set of inputs have been created allowing administrators to create an enrollment form containing the fields needed for most certificate profiles you will create. The inputs provide a certificate request field that can be added to any of the forms so that certificate requests can be pasted into this field, allowing a request to be created outside the input form with any of the request information you need.

An output specifies how the response page to a successful enrollment is presented. It usually displays the certificate in a user-readable format. A single output has been created that shows the pretty print version of the resultant certificate.

# How Certificate Profiles Work

An administrator sets up a certificate profile by associating an existing authentication plug-in, or method, with the certificate profile, enabling and configuring defaults and constraints, and defining inputs and outputs. The administrator can use the existing certificate profiles, modify the existing certificate profiles, create new certificate profiles, and delete any certificate profile that will not be used in this PKI.

Once a certificate profile is set up, it appears on the Manage Certificate Profiles page of the agent services interface where an agent can approve, and thus enable a certificate profile. Once the certificate profile is enabled, it will appear on the Certificate Profile tab of the end-entity interface where end-entity can enroll for a certificate using the certificate profile.

The Certificate Profile enrollment page contains links to each type of certificate profile enrollment that has been enabled. When an end entity selects one of those links, an enrollment page appears containing an enrollment form specific to that certificate profile. The enrollment page for this certificate profile in the end-entity interface is dynamically generated from the inputs defined for this certificate profile. If an authentication plug-in is configured, additional fields may be added that are needed to authenticate the user with that authentication method.

When the end entity submits a certificate profile request that is associated with a manual enrollment, an enrollment where no authentication plug-in is configured, the certificate profile is queued in the agent services interface as a certificate profile enrollment request, showing that it is different from the old enrollment method. The agent can change some aspects of the enrollment, reject it, change the status, or approve it. The agent can also update the request without submitting it or validate that the request adheres to the profile's defaults and constraints. The agent is bound by the constraints set up; they cannot change the request in such a way that a constraint is violated. The signed approval is immediately processed and a certificate is issued.

When a certificate profile is associated with an authentication method, the request generates a certificate automatically if the user successfully authenticates, all the information required is provided, and the request does not violate any of the constraints set up for the certificate profile.

The issued certificate contains the content defined in the defaults for this certificate profile, such as the extensions and validity period for the certificate, and the content of the certificate is constrained by the constraints set up for each default. You can set up more than one set of policies (defaults and constraints), distinguishing each set by using the same value in the Policy Set ID for each set. The server evaluates each set with each request it receives. In the case where a single certificate is issued, one set is evaluated, any other sets

are ignored. In the case where dual-key pairs are issued, the first set is evaluated with the first certificate request, and the second set is evaluated with the second certificate request. There is no need for more than one set if you are issuing a single certificate, or more than two sets if you are issuing dual-key pairs.

The request is not evaluated by the Policies set up in the Policy feature of CS. If the enrollment took place in a Registration Manager, both the Registration Manager and the Certificate Manager should have the same certificate profile implemented with the same policies.

## Enabling and Disabling Certificate Profiles

Any certificate profiles that have been configured by an administrator will be listed in the Manage Certificate Profiles page of the agent services interface. The Manage Certificate Profiles page can be accessed by clicking the Manage Certificate Profiles link in the left hand portion of the agent services interface.

The Manage Certificate Profiles page contains all of the certificate profiles that have been set up by an administrator. It shows the name of the certificate profile, a short description of the certificate profile, whether or not this is an end user certificate profile, whether or not the certificate profile has been approved and is thus enabled, and if it is approved, which agent under ID approved the request.

## Getting Certificate Profile Information

You can get information about any certificate profile by clicking the name of the certificate profile, which is linked to the Approve Certificate Profile page. This page lists information about the certificate profile and allows you to approve a certificate profile, or disapprove a previously approved certificate profile. Note, an approved certificate profile can only be disapproved by the agent who originally approved the certificate profile.

### End User Certificate Profile

If the End User Field of the certificate profile is marked true, then this certificate profile will appear as an enrollment in the end-entity interface. If the End User Field of the certificate profile is marked false, then this certificate profile will not appear in the end-entity interface. This parameter determines whether or not the certificate profile needs to be received from the end-entity interface in order to be processed. Certificate Profiles would



provide the value of false if the certificate profile is in a Certificate Manager where the certificate profile is mirroring a certificate profile in a Registration Manager. The value of false allows the Certificate Manager to process a certificate profile request received from a Registration Manager rather than the Certificate Manager's end-entity interface.

## Policy Information

Each policy has a Policy Information section which shows a table for each Policy Set. Generally, a certificate profile will have just one policy set. If the enrollment is for dual-key pairs, then there will be two Policy Sets, one for the signing key and one for the encryption key. The Policy Set defines all of the defaults and constraints that have been set up for a particular certificate that is being requested. In the case of dual-key pairs, two certificates are being requested, one for the signing key and one for the encryption key.

The Policy Set table has columns that list the following

#. The number column lists the number for this set of defaults and constraints.

**Extensions/Fields.** This column lists the defaults that are set up. The defaults define certificate content including extensions.

**Constraints.** This column lists the constraints placed on the content of this certificate. The content placed in this certificate must comply with these constraints in order to be issued.

## To Approve a Certificate Profile

To approve a certificate profile, you go to the certificate profiles Approve Certificate Profile page and click Approve at the bottom of the page. You get to the page by clicking Manage Certificate Profiles and then clicking on a certificate profile name.

Once a certificate profile is approved, it appears in the end-entity interface allowing an end-entity to use that certificate profile to enroll for a certificate.

Once a certificate profile is enabled, administrators cannot change any aspect of the certificate profile. The certificate profile must first be disapproved for an administrator to change any aspect of the certificate profile.

## To Disapprove a Certificate Profile

A certificate profile can only be disapproved, thus disabled, by the agent who approved the certificate profile.

To disapprove a certificate profile, you go to the certificate profiles Approve Certificate Profile page and click Disapprove at the bottom of the page. (You can only disapprove approved certificate profiles.) You get to the page by clicking Manage Certificate Profiles and then clicking on a certificate profile name.

Once a certificate profile is disapproved, it is unavailable for enrollment from the end-entity interface.

# Handling Certificate Requests

As a Certificate Manager or Registration Manager agent, you are responsible for handling both manual enrollment requests made by end entities (end users, server administrators, or other CS subsystems) and automated enrollment requests that have been deferred. This chapter describes the general procedure for handling requests and explains how to handle different aspects of certificate request management.

This chapter contains the following sections:

- Managing Requests
- Listing Certificate Requests
- Approving Requests

## Managing Requests

This is the typical procedure for handling certificate enrollment requests:

1. View the list of pending requests for the Certificate Manager or Registration Manager (see “Listing Certificate Requests” on page 39).
2. Select a request from the list to view it and, optionally, assign the request to yourself (see “Selecting a Request” on page 41).

3. Process the request (see “Approving Requests” on page 42 and “Other Options for Handling Requests” on page 48).

In processing a request for a certificate, you can choose to take one of the following actions:

- **Approve the request.** You can approve a request manually, or it can be approved automatically by policy modules if the request has been authenticated by an authentication module (and if the CS administrator has configured the system to do this). After a request has been approved, Certificate System issues the requested certificate (Certificate Manager) or passes it on to the Certificate Manager for issuance (Registration Manager).
- **Reject the request.** You can reject a request manually, or it can be rejected automatically by the Certificate Profile system if the request does not adhere to the profile’s defaults and constraints. If the CS administrator has configured the system to provide automatic notifications to end users, a rejected request will automatically result in such a notification being sent.
- **Cancel the request.** You can cancel a request manually, but requests are never cancelled automatically, and users do not receive automatic notification of cancelled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore don’t need to invoke automatic notification.
- **Update the request.** You can update a pending request by changing some of its values. An example of this would be changing the subject name. Also the various default values associated with a Certificate Profile can be changed by the Agent. Submitting the request update will only result in the request’s values being changed but not its state.

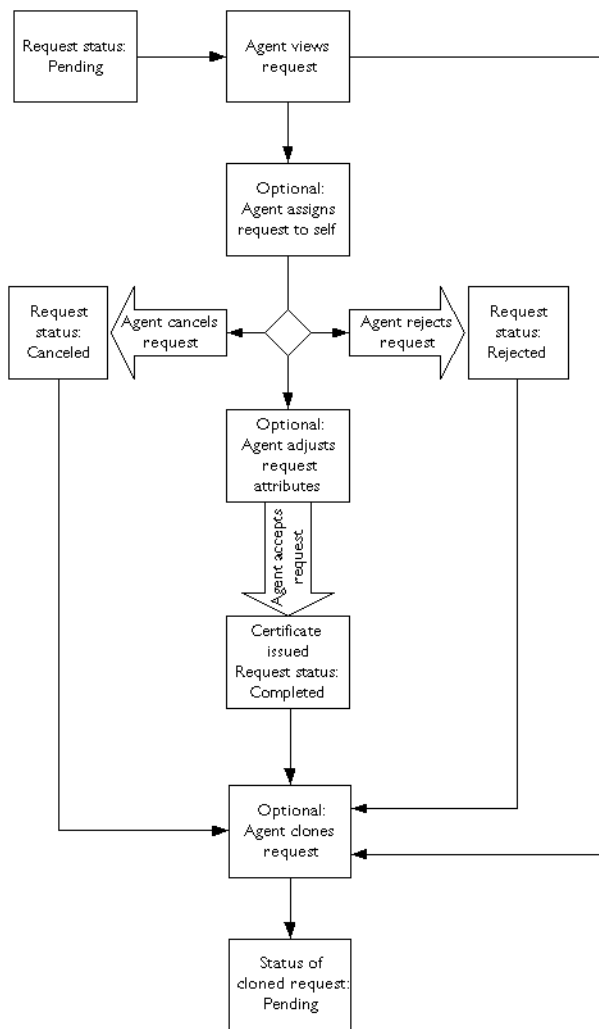
- **Validate the request.** You can validate a request that uses a Certificate Profile in order to see if the request complies with the defaults and constraints dictated by the Certificate Profile. Once again, this action merely checks the request's correctness and does not result in submission of the request.

With the exception of the Validate and Update commands, each of these actions changes the status of the certificate request. If you close the form without taking one of these actions, the request remains in the queue with the same status.

It is also possible to clone any request, whether it is still pending, canceled, rejected, or completed. This can be useful in a variety of situations. For example, if a user receives a certificate that does not work because it has been incorrectly formulated, you can locate the completed request, clone it, and correct it without requiring the user to enroll a second time. Cloning a request gives it a new request ID number and puts it into the list of pending requests, but does not change the status of the original request.

Figure 3-1 illustrates the process for handling requests and the different types of status for a request.

**Figure 3-1** The certificate request management process



# Listing Certificate Requests

The Certificate Manager or Registration Manager keeps a queue of all certificate service requests that have been submitted to it. The queue records whether a request is pending, completed, canceled, or rejected. Four types of requests can be in the queue:

- Enrollment requests
- Revocation requests
- Renewal requests
- Certificate chain requests

As a Certificate Manager or Registration Manager agent, you must review and approve manual enrollment requests; those that require review have a status of Pending.

To see a list of requests:

1. Go to the Registration Manager or Registration Manager Agent Services page (see “Accessing Agent Services” on page 24).

You must submit the proper client certificate to get access to this page.

2. Click List Requests at the top of the left frame to view the queue of requests for certificates and to issue those certificates.

The List Requests form appears.

The screenshot shows the Red Hat Certificate System Agent Services interface. The main header is "Red Hat Certificate System Agent Services". Below the header is a "Certificate Manager" tab. On the left side, there is a navigation menu with the following items: "List Requests" (highlighted), "List Certificates", "Search for Certificates", "Revoke Certificates", "Display Revocation List", and "Update Revocation List". The main content area is titled "List Requests" and contains the following form elements:

- Request type:
- Request status:
- Starting request identifier:  (optional)
- Buttons: "Find", "first", "5", "records", "Help"

3. Choose the type of requests you want to see by selecting one of the following from the “Request type” menu:
  - **Show enrollment requests**
  - **Show renewal requests**
  - **Show revocation requests**
  - **Show all requests**
4. Choose the status of requests you want to see by selecting one of the following from the “Request status” menu:
  - **Show pending requests**

These are enrollment requests that have not yet been processed but are waiting for manual review. Requests in this state may already be assigned to an issuing agent for processing.
  - **Show canceled requests**

These are requests that have been manually canceled by an agent. Users do not receive automatic notification of canceled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore do not need to invoke automatic notification.
  - **Show rejected requests**

These are requests that have been either manually rejected or rejected automatically during policy processing. If the CS administrator has configured the system to provide automatic notifications to users, a rejected request will automatically result in such a notification being sent.
  - **Show completed requests**

These are requests that have been completed. They include enrollment requests for which certificates have been issued and also completed revocation and certificate chain requests.
  - **Show all requests**

This will show all requests of the selected type, regardless of status.
5. To start the list at a specific place in the queue, enter the starting request identifier in decimal or hexadecimal form.

Use 0x to indicate a hexadecimal number; for example, 0x2A.



- Choose the number of matching requests you want to see. When you specify a number  $n$ , the system displays the first  $n$  requests after the starting sequence number that matches your specified criteria.
- Click Find to display the list of requests that match your specified criteria.

The Request Queue form appears.

Red Hat  
Certificate System Agent Services

Certificate Manager

List Requests

List Certificates

Search for Certificates

Revoke Certificates

Display Revocation List

Update Revocation List

Update Directory Server

### Request Queue

Total Number of Records Found : 2

#	Status	Type	Filed on
41	pending	enrollment (Certificate Profile)	2/20/2003 14:14:16
Subject name			Updated on
Details			UID=TestUser, E=TestUser@test.com, CN=Test User 1, OU=CS Test, O=Example Corp., C=US
			2/20/2003 14:14:17
#	Status	Type	Filed on
42	pending	enrollment (Certificate Profile)	2/20/2003 14:15:09
Subject name			Updated on
Details			UID=Test User2, E=TestUser@test.com, CN=Test User 2, OU=CS Test, O=Example Corp., C=US
			2/20/2003 14:15:09

## Selecting a Request

To select a request from the queue:

- On the Agent Services page, click List Requests, specify search criteria, and click Find to display a list of certificate signing requests.

See “Listing Certificate Requests” on page 39 for details.

- On the Request Queue form, find the particular request you want to examine.

If the request you want to see is not shown, scroll to the bottom of the list, specify an additional number  $n$ , and click Find. The system displays the next  $n$  requests that match your original search criteria.

- When you have found the request you want, click Details at the left.

The Request details form appears, showing detailed information about the selected request. Use this form to approve or otherwise handle the request. For more information, see “Approving Requests” on page 42 and “Other Options for Handling Requests” on page 48.

The screenshot shows the Red Hat Certificate System Agent Services interface. The main header is "Red Hat Certificate System Agent Services" and the sub-header is "Certificate Manager". On the left, there is a sidebar with navigation options: "List Requests" (highlighted), "List Certificates", "Search for Certificates", "Revoke Certificates", "Display Revocation List", "Update Revocation List", and "Update Directory Server". The main content area displays "Request 42" with two tables of information.

**Request Information**

<b>Request ID:</b>	42
<b>Request Type:</b>	enrollment
<b>Request Status:</b>	pending
<b>Requestor Host:</b>	10.169.24.198
<b>Creation Time:</b>	Thu Feb 20 14:15:09 PST 2003
<b>Modification Time:</b>	Thu Feb 20 14:15:09 PST 2003

**Certificate Profile Information**

<b>Certificate Profile Id:</b>	caUserCert
<b>Approved By:</b>	admin
<b>Certificate Profile Name:</b>	Manual User Dual-Use Certificate Enrollment
<b>Certificate Profile Description:</b>	This certificate profile is for enrolling user certificates.

If the system changes the state of the displayed request, and if you use your browser's Back or Forward buttons or the Go (history) menu to move to another page, the data shown can become out of date. To refresh the data, click the highlighted serial number at the top of the page.

## Approving Requests

As an agent, you can approve a certificate request. If the request was made directly to the Certificate Manager, it issues the certificate; if the request was made through a Registration Manager, the Registration Manager passes the approved request on to the Certificate Manager for issuance. Before approving a request, you can assign it to yourself, adjust the

attributes of the request, and verify that it will result in a valid certificate. To do these things, use the Request Details form that appears when you examine a selected request (as described in “Selecting a Request” on page 41). If you want to reject or cancel the request, see “Other Options for Handling Requests” on page 48.

The approval and issuing process has the following stages:

- Adjusting, Verifying, and Approving a Certificate Profile Request
- Assigning a Request
- Adjusting, Verifying, and Approving a Request
- Sending an Issued Certificate to the Requester

## Adjusting, Verifying, and Approving a Certificate Profile Request

Before you verify and approve a request, you can adjust some of the parameters, such as the subject name and validity period.

To adjust, verify, and approve a certificate request:

1. Select the certificate request from a list of requests, as described in “Selecting a Request” on page 41.
2. The certificate profile request contains several tables with information about the request:

**Request Information.** This table lists basic information about the request.

**Certificate Profile Information.** This table lists the certificate profile being used, along with basic information about that certificate profile.

**Certificate Profile Inputs.** This table lists the inputs contained in the enrollment form for this certificate profile. It also contains the values obtained from these input fields.

**Policy Information.** This table lists the policies that apply to this certificate profile. It includes the definition of the policy, the value placed in the certificate by this specific policy, and the constraints placed on this policy.

3. To change any of the information that will be contained in the certificate, such as the subject name or validity period, change the settings in the Policy Information table contained in the certificate profile request.

The policies contained in this certificate profile will be listed in this table detailing the policy, providing the specific values for this certificate, and providing the constraints for each policy. For any policy that you can change, there will either be a pull-down list allowing you to make the change, or the information will be in a field in which you can change the derived value.

When making these changes, the values you provide must be valid values within the constraint placed on a policy. If you provide a value that is outside of the constraint that is placed, the request will not validate, and you will need to change the value before a certificate will be issued.

4. Choose an action from the pull-down menu at the bottom of the page and click Submit. The actions available are as follows:

**Approve Request.** To approve the request and issue the certificate.

**Update Request.** To update the request with any information you have changed in the request. The status of the request does not change, but the information contained in the request does change.

**Validate Request.** To validate that the request conforms to the constraints placed on the issuance of this type of certificate. Validating will either tell you that the request is valid, or give you a list of any non-conforming items that need to be fixed.

**Reject Request.** To reject the request.

**Cancel Request.** To cancel the request without issuing a certificate or issuing a rejection.

## Assigning a Request

Before acting on a request, you can assign it to yourself. Assignment is not required, and it only applies if your system is configured to do older, non-profile style enrollment (for which, see “Adjusting, Verifying, and Approving a Request” on page 45). Any agent can act on an unassigned request. When a request is assigned to a particular agent, all agents can examine that request, but only the assigned agent can act on it. When a request is assigned to another agent, however, you can choose to reassign it to yourself in order to act on it.

When you view the details of an unassigned request, you can click “assign to me” to assign it to yourself. The request is immediately assigned to you, and the Request Details page reflects the assignment. If you leave the page without approving, rejecting, or canceling the request, the request remains in the queue with the status of Pending, but it is assigned to you.

## Adjusting, Verifying, and Approving a Request

Before you verify and approve a request, you can adjust some of the parameters, such as the subject name and validity period.

This procedure is for non-certificate profile based requests, so the following information will be of use only if the system is configured to do the old style enrollment. Certificate Profile based requests will be marked as a certificate profile enrollment in the request queue. In the type column of the request queue, the request will be listed as Enrollment (Certificate Profile). These requests produce a different approval form from other requests. For details about certificate profile requests with which your system is configured by default, see “Adjusting, Verifying, and Approving a Certificate Profile Request,” on page 43.

To adjust, verify, and approve a certificate request:

1. Select the certificate request from a list of requests, as described in “Selecting a Request” on page 41.
2. In the Service Request form, check the Assigned To prompt to see if the certificate request is assigned to you.
  - If the request is unassigned, you can choose to assign it to yourself. Click “assign to me.” Your CS login name appears as the assigned agent, and the “assign to me” link changes to “cancel request assignment.”
  - If the request is already assigned to you, you can choose to cancel the assignment. To cancel the request’s assignment, click “cancel request assignment.” The form then shows that the request is unassigned. You can still act upon an unassigned request.
  - If the request is assigned to another agent, you cannot act on the request unless you reassign it to yourself. Click “re-assign to me.” Your CS login name appears as the assigned agent, and the “re-assign to me” link changes to “cancel request assignment.”

3. To change the subject name, enter a new value in the Subject Name field.  
 For example, you might need to change the subject name to correct spelling errors. Nothing prevents you from issuing many different certificates with the same subject name. However, if you have installed more than one certificate with the same subject name in Netscape Navigator, it will recognize only one of them (the most recent) as valid. This is not true of Netscape Communicator and later versions, which know how to deal with multiple certificates with the same subject name.
4. If you want to change the validity period, you can set the dates directly using the menus for start and end times or you can select a predefined period from the “Length of validity period” menu. Making a selection from the “Length of validity period menu” sets the “Not valid after” date based on the “Not valid before date” and your selection.
5. Use the Extensions section to specify Netscape certificate type bits that you want to be set in the issued certificate.
  - o To specify the intended use of the certificate that you are issuing, select one or more types from the list of Netscape certificate types, as described below. If you select any of these types, the equivalent Netscape certificate type bit is set.

**Table 3-1** Netscape certificate type extension

Type	Description
SSL client	Indicates that the certificate is a personal certificate used by Netscape Navigator to establish SSL connections with servers.
SSL server	Indicates that the certificate is a server certificate used by a Red Hat server to establish SSL connections with clients.
Secure Email	Indicates that the certificate is used by an email application to send and receive signed and encrypted email.
Object signing	Indicates that the certificate is used for object signing.
Subordinate SSL CA (available only for CA certificate requests)	Allows a CA to sign and issue personal and server certificates.
Subordinate email CA (available only for CA certificate requests)	Allows a CA to sign and issue certificates for use with signed and encrypted email.
Subordinate executable object-signing CA	Allows a CA to sign and issue object-signing certificates.

Note that additional extensions can be set by means of policy modules, which must be configured by the CS administrator.

6. If you want to add extensions other than Netscape certificate type extensions, you can paste a base-64 encoding of the extension in the “Additional Extensions” field.

You can use the tools provided for generating extensions to include in CA and other certificate requests. For details about these tools, check this directory:

```
<server_root>/bin/cert/tools
```

The certificate extension text field accepts a single extension blob. If you want to add multiple extensions, you should use the `ExtJoiner` program, which is also provided in the above directory. For details about this tool, see “Extension Joiner Tool” in *CS Command-Line Tools Guide*.

7. If you want the certificate to be signed using a signature algorithm other than the default, choose an alternative from the “Signature algorithm” drop-down list:
  - o MD5 with RSA and MD2 with RSA generate a 128-bit message digest. Most existing software applications that handle certificates support only MD5. This is the default algorithm.
  - o SHA-1 with RSA generates a 160-bit message digest. Before choosing SHA-1, make sure your applications support it. Netscape Navigator 3.0 (or later) and Enterprise Server 2.01 (or later) support SHA-1. If your users have previous versions of these applications, choose MD5 as the signature algorithm, or upgrade your users to the most recent version of these applications.

Before selecting an algorithm, check with your CS administrator to make sure that Certificate System has the algorithm enabled.

8. Review the unauthenticated request attributes. These attributes were submitted by the end entity with the enrollment request. Since these attributes do not come from a trusted source (such as an authentication module in the CS server), they are “unauthenticated.” Your site policies may or may not require agents to review or validate any of these attributes.
9. Review the authenticated attributes. These attributes were generated in the CS server by authentication or policy plug-in modules. They are considered authenticated since they have been validated by or have originated in the CS server itself.
10. If the certificate request is for an SSL client certificate for a CS manager or a CS agent, you should indicate this in the last section, labeled Privileges.
  - o If the request is for a CS manager’s certificate, select the check box labeled “This certificate is for a Trusted Manager.”

- If the request is for a CS agent's certificate, select the check box labeled "This certificate is for a *name of manager* agent."

You must also type a user ID for the new manager or agent. This user ID can be the same that you specified in the certificate request, or it can be some other ID that you want to use to identify this agent or manager in the CS window of Red Hat Console, such as Agent1 or RMEng.

11. To approve the request and issue the certificate, open the drop-down menu at the bottom of the page, choose "Accept this request," then click Do It.

If the certificate conforms to policy, a page containing the new certificate appears. It includes instructions on how to help the certificate requester install the new certificate.

---

**NOTE** If, after verifying or attempting to issue the certificate, you receive the error message "The requested signature algorithm is not enabled," check with your CS administrator to make sure that the signature algorithm you selected in Step 7 is supported.

---

## Other Options for Handling Requests

If you do not want to issue the certificate in response to a certificate request, you can choose one of the other options from the command menu at the bottom of the Request Details form, then click Do It.

- **Cancel this request** changes the state of the request to Canceled. Users do not receive automatic notification of cancelled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore do not need to invoke automatic notification.
- **Reject this request** changes the state of the request to Rejected, indicating that it was unacceptable for policy reasons. If the CS administrator has configured the system to provide automatic notifications to end users, a rejected request will automatically result in such a notification being sent.
- **Clone this request** creates a copy of the request and gives the copy a new request ID number. The status of the new request is Pending. The status of the original request also remains as Pending until you accept, cancel, or reject it.



## Sending an Issued Certificate to the Requester

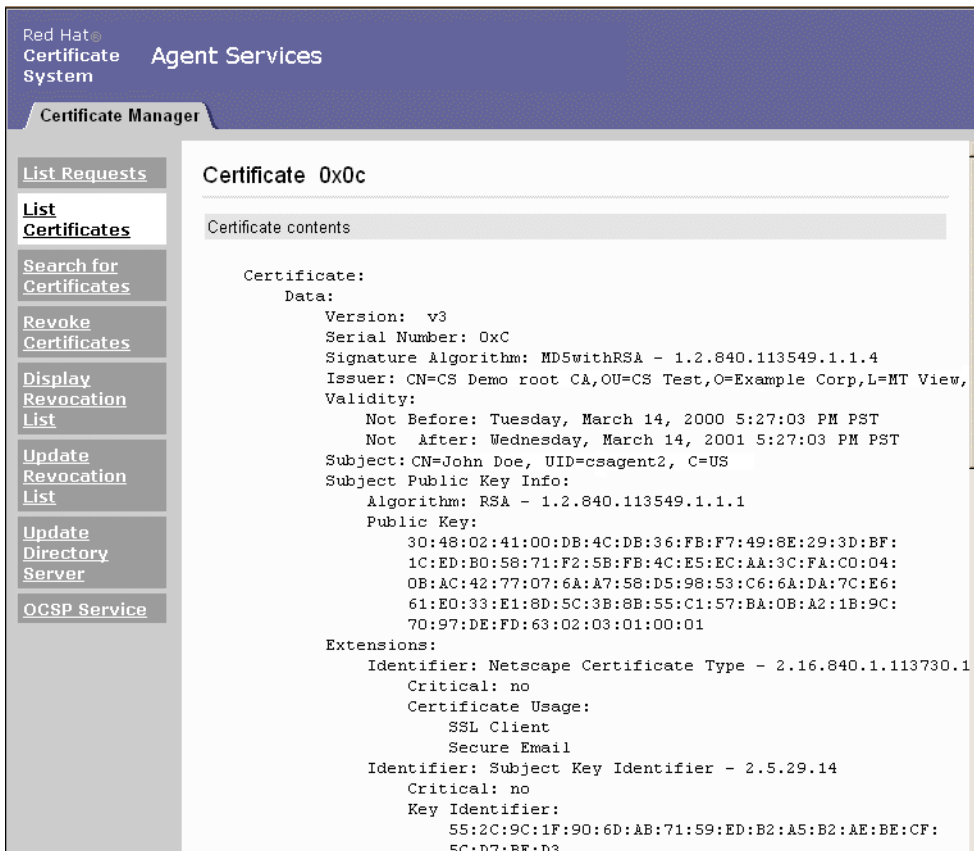
When the Certificate Manager has issued a certificate in response to a request, the user who requested it must receive a copy of it to install locally. End users install their own certificates in their client software. Server administrators install their servers' certificates in the servers that they manage.

Depending on how your Certificate System is configured, an end user who requests a certificate might receive automatic email notification of the success of the request; this email message contains either the certificate itself or a URL from which the user can get the certificate. In this case, you need not take any further action.

If your system is not configured for automatic certificate-issuance notification, or if the requester is a server administrator, you must either send the issued certificate to the requester or ask the requester to pick it up from the Certificate Manager's end-entity gateway.

Figure 3-2 shows a web page containing a new certificate. This is the page you receive in response to the command "Issue this certificate," as described in Step 11 in "Approving Requests" on page 42.) Before you issue the certificate, you should copy the requester's email address.

**Figure 3-2** A newly issued certificate page



To copy and mail a new server certificate to the requester, follow these steps:

1. Open a new email message composition window and address it to the requester.
2. From the Agent Services window where the new certificate is displayed, copy only the base-64 encoded certificate. Be sure to include the marker lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.
3. Paste the base-64 encoded certificate into the addressed email message and send the message.

To deliver a new client certificate to the requester, note the serial number of the request you approved, then follow these steps:

1. Go to the Agent Services gateway, click List Requests in the left frame, enter the serial number for the request that you approved, and click Find.

2. In the Request Queue form, click Details beside the relevant request, then right-click the certificate serial number and choose Open Frame in New Window from the pop-up menu.
3. In the new browser window containing the certificate, copy the URL from the Location or Netsite field.
4. Open a new email message composition window and address it to the requester.
5. Paste the URL into the body of the message, along with instructions to the effect that the user should go to that URL and click the Import button at the bottom of the page.

Alternatively, you can include the URL for the Agent Services gateway in the email message instead, along with the certificate serial number, and instruct the user as follows:

1. Click the Retrieval tab. The List Certificates form should appear.
2. Enter the serial number of the certificate in both serial number fields.
3. Click Find.
4. When the Search Results form appears, click Details.
5. When the certificate appears, scroll down to the bottom of the form and click Import Certificate.



# Finding and Revoking Certificates

As a Certificate Manager agent, you can use the Agent Services page to find a specific certificate issued by Red Hat Certificate System or to retrieve a list of certificates that match specified criteria. You can examine certificates that you have retrieved. You can also revoke certificates and manage the certificate revocation list.

This chapter contains the following sections:

- Basic Certificate Listing
- Advanced Certificate Search
- Revoking Certificates
- Managing the Certificate Revocation List

## Basic Certificate Listing

You can get a list of certificates quickly and easily by specifying a range of serial numbers. You can also choose to show all certificates within the range, or only those that are currently valid.

To find a specific certificate or to list certificates by serial number:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
2. Click List Certificates to display the List Certificates form in which you specify listing criteria.

Red Hat  
Certificate System Agent Services

**Certificate Manager**

**List Requests**

**List Certificates**

**Search for Certificates**

**Revoke Certificates**

**Display Revocation List**

**Update Revocation List**

**Update Directory Server**

**OCSP Service**

**List Certificates**

Use this form to list certificates whose serial numbers fall within a specified range.

Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.

Lowest serial number  (leave blank for no lower limit)

Highest serial number  (leave blank for no upper limit)

Do not show certificates that have been revoked

Do not show certificates that have expired or are not yet valid

first  records

- To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields of the List Certificates form, in either decimal or hexadecimal form.

Use 0x to indicate the beginning of a hexadecimal number; for example, 0x00000006. (Serial numbers are displayed in hexadecimal form in the Search Results and Details pages.)

- To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range (in decimal or hexadecimal form).

If you leave either the lower limit or upper limit field blank, the certificate whose number you specified plus all certificates before or after it in sequence are displayed.

- To limit the returned list to valid certificates, select one or both of the check boxes labeled with filtering methods.

You can choose not to show revoked certificates or not to show certificates that have expired or are not yet valid.

- Enter the number of certificates matching the criteria that you want to see.

For a number  $n$ , the first  $n$  matching certificates are initially displayed.

- Click Find.

Certificate System displays a list of the certificates that match your search criteria. You can select a certificate in the list and examine it in more detail or perform various operations on it. For more information, see “Examining Certificates” on page 59.

## Advanced Certificate Search

If you want to search for certificates by more complex criteria than serial number, use the advanced search form.

To perform an advanced search for certificates:

- Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
- Click Search for Certificates to display the Search for Certificates form in which you specify search criteria.

The screenshot shows the Red Hat Certificate System Agent Services interface. The top navigation bar includes the Red Hat logo, 'Certificate System', and 'Agent Services'. Below this is a 'Certificate Manager' tab. A sidebar on the left contains several menu items: 'List Requests', 'List Certificates', 'Search for Certificates' (which is highlighted), 'Revoke Certificates', 'Display Revocation List', 'Update Revocation List', 'Update Directory Server', and 'OCSP Service'. The main content area is titled 'Search for Certificates' and contains the following text: 'Use this form to compose queries based on properties of the certificate.' Below this is a paragraph: 'Each section below filters the search. Check the box at the top of the section if you want to use that filter in your search, then complete the fields. Leave a box unchecked to ignore that filter. You can click more than one box to get a combination of search criteria.' The first filter section is 'Serial Number Range', which has a checkbox labeled 'Show certificates that fall within the following range:'. Below this are two input fields: 'Lowest serial number:' and 'Highest serial number:'. Each field has a small box next to it and a note '(leave blank for no lower/upper limit)'. Below the input fields is a paragraph: 'Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.' The second filter section is 'Subject Name'.

3. To search by particular criteria, use one or more of the sections of the Search for Certificates form.

The form is quite long; scroll down to see the different sections. To use a section, select the appropriate check box, then fill in any necessary information.

**Serial Number Range.** Use this section to find a certificate with a specific serial number or to list all certificates within a range of serial numbers.

- To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields, in either decimal or hexadecimal form. Use 0x to indicate the beginning of a hexadecimal number; for example, 0x2A. (Serial numbers are displayed in hexadecimal form in the Search Results and Details pages.)
- To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range (in decimal or hexadecimal form).

If you leave either the lower limit or upper limit field blank, all certificates before or after the one you specify are displayed.

**Status.** Use this section to select certificates by their status. A certificate can have one of the following status codes:

- VALID - The certificate has been issued, its validity period has begun but not ended, and it has not been revoked.
- INVALID - The certificate has been issued, but its validity period has not yet begun.
- REVOKED - The certificate has been revoked.
- EXPIRED - The current time is later than the end of the certificate's validity period.
- REVOKED & EXPIRED - The certificate meets the criteria for both status codes.

**Subject Name.** Use this section to list certificates with a particular owner. For more information on filling in this section, see Step 4.

**Revocation Information.** Use this section to list certificates that have been revoked during a particular period or by a particular agent. For example, you can list all certificates revoked between July 1996 and January 1997, or all certificates revoked by the agent with the user name `admin`.

- To list certificates revoked within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.



- To list certificates revoked by a particular agent, enter the name of the agent. You can use wildcards in this field. (For more information on wildcard syntax, see Step 4.)

**Issuing Information.** Use this section to list certificates that have been issued during a particular period or by a particular agent. For example, you can list all certificates issued between July 1996 and January 1997, or all certificates issued by the agent with the user name `betatest`.

- To list certificates issued within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates issued by a particular agent, enter the name of the agent. You can use wildcards in this field. (For more information on wildcard syntax, see Step 4.)

**Dates of Validity.** Use this section to list certificates that become effective or expire during a particular period. For example, you can list all certificates that became valid on June 1, 1996, or that expired between January 1, 1997 and June 1, 1997.

You can also list certificates that have a validity period of a certain length of time. For example, you can list all certificates that are valid for less than one month.

- To list certificates that become effective or expire within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates that have a validity period of a certain length in time, select “not greater than” or “not less than” from the drop-down list, enter a number, and select a time unit from the drop-down list: Days, Weeks, Months, or Years.

**Basic Constraints.** Click on this checkbox to show CA certificates that are based on the Basic Constraints extension.

**Type.** Use this section to list certain types of certificates. For example, you can list all certificates for subordinate CAs. Note that this search works only for certificates containing the `netscape-cert-type` extension, which stores type information.

- For each type, choose from the drop-down list to find certificates where that type is On, Off, or Absent.
4. To find a certificate with a specific subject name, use the Subject Name section.
    - Select the check box, then enter the subject name criteria.

- Enter values for the fields you want included in your search criteria and leave the others blank.

The standard tags or components are as follows:

**Email address.** To narrow the search by email address, enter the email address in this field.

**Common name.** To find certificates associated with a specific person or server, enter the name in this field.

**UserID.** The user ID for the person whose certificate you want to find. For example, at many companies the user ID is the name used to log in to the network when starting up a computer.

**Organization unit.** To narrow the search to a specific division, department, or unit within an organization, enter the name of the unit in this field.

**Organization.** To narrow the search by organization, enter the name of the business, university, or organization in this field.

**Locality.** To narrow the search by locality, enter the name of the local area (for example, the name of the city) in this field.

**State.** To narrow the search by state or province, enter the name of the state or province in this field.

**Country.** To narrow the search by country, enter the two-letter code for the country (for example, US) in this field.

When you have entered the field values for the server to match, specify the type of search that you want performed:

- Select Exact to search for certificates that have subject names that match exactly the components you have specified and contain none of the components you have left blank. You cannot use wildcards in this type of search.
- Select Partial to search for all certificates with subject names that match at least the components you have specified but that may also have any values in the components you have left blank.

You can specify wildcard patterns in this type of search by using the question mark character (?) to match an arbitrary character and the asterisk character (\*) to match an arbitrary string of zero or more characters.

Note that placing a single asterisk in a given field in the search form specifies that the corresponding component must be in the certificate's subject name but may have any value whatsoever. To indicate that you do not care if the component is present, leave the field blank.

- After entering your search criteria, scroll to the bottom of the form and enter the number of certificates matching your specified criteria that you want to see.

For a number  $n$ , the first  $n$  matching certificates are initially displayed. The time limit of a search in seconds can also be input at this time.

- Click Find.

The Search Results form appears, showing a list of the certificates that match your search criteria. You can select a certificate in the list and examine it in more detail. For more information, see “Examining Certificates” on page 59.

The screenshot shows the Red Hat Certificate System Agent Services interface. The main content area displays search results for a certificate. The search criteria are: Issuer: CN=CS Demo root CA, OU=CS Test, O=Example Corp, L=MT View, ST=California, C=US. The total number of records found is 1. The search results table shows the following details:

Serial number	Subject name	
0x00000007	E=user1@example.com, CN=User One UID=user1, OU=Technical Publications O=Example Corp, C=US	
Version	Subject public key algorithm	
3	PKCS #1 RSA with 1024-bit key	
<b>Details</b>		
	Not valid before	Not valid after
	2/24/1999	3/23/1999
	Issued on	Issued by
	2/24/1999	csadmin

## Examining Certificates

To examine the details of a certificate, follow these steps:

- On the Agent Services page, click List Certificates or Search for Certificates, specify search criteria, and click Find to display a list of certificates.

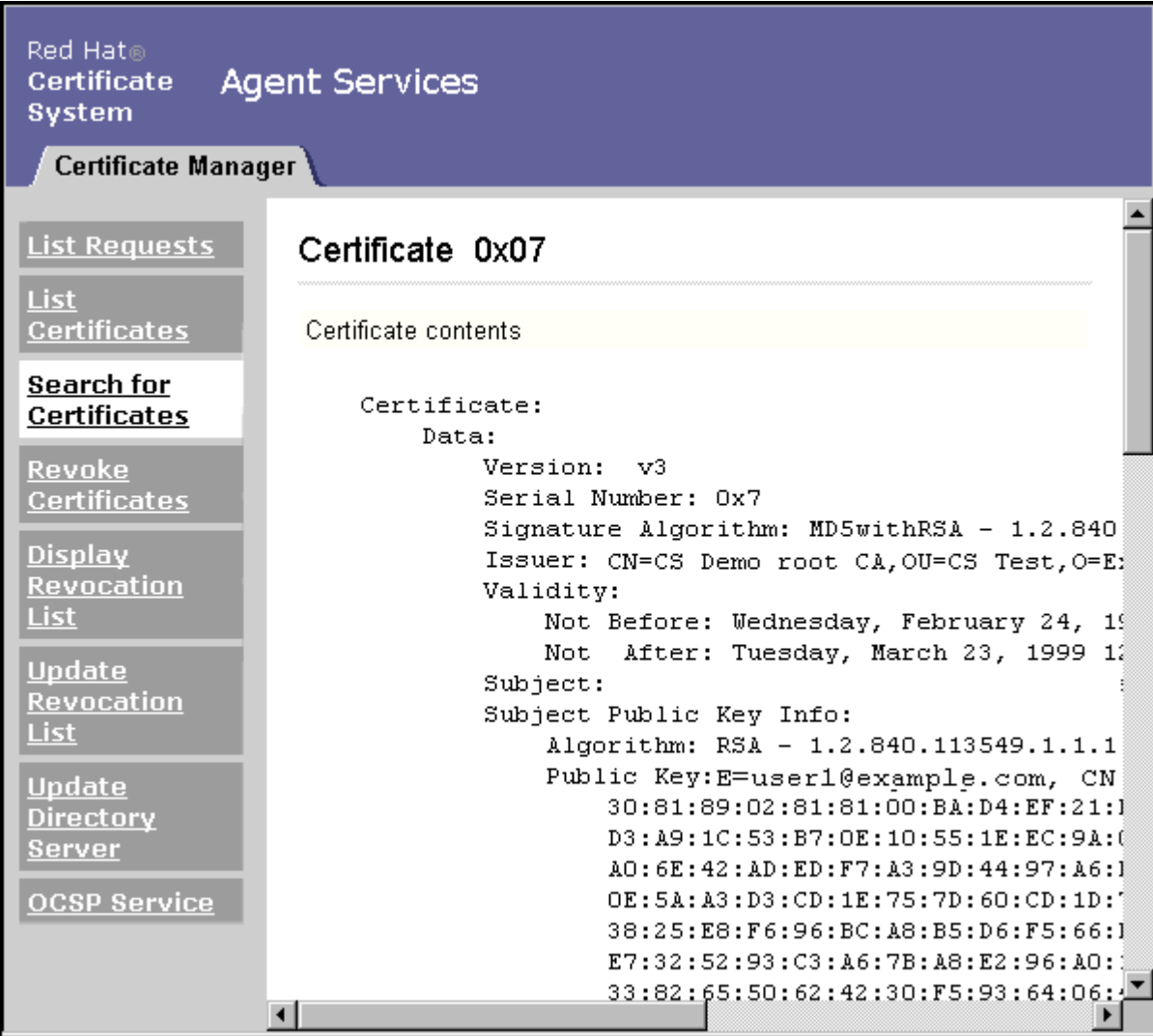
For details of how to specify criteria, see “Basic Certificate Listing” on page 53 and “Advanced Certificate Search” on page 55.

2. On the Search Results form, find the particular certificate you want to examine.

If the certificate you want to see is not shown, scroll to the bottom of the list, specify an additional number  $n$ , and click Find. The system displays the next  $n$  certificates that match your original search criteria.

3. When you have found the certificate you want, click the Details button at the left side of its entry.

The Certificate page appears. It shows the detailed contents of the selected certificate and instructions for installing the certificate in a server or in Netscape Navigator.



Red Hat®  
Certificate System

## Agent Services

### Certificate Manager

- List Requests
- List Certificates
- Search for Certificates**
- Revoke Certificates
- Display Revocation List
- Update Revocation List
- Update Directory Server
- OCSP Service

## Certificate 0x07

Certificate contents

Certificate:  
Data:

```

Version:  v3
Serial Number:  0x7
Signature Algorithm:  MD5withRSA - 1.2.840
Issuer:  CN=CS Demo root CA,OU=CS Test,O=Example.com
Validity:
    Not Before:  Wednesday, February 24, 1999 12:00:00 AM
    Not After:   Tuesday, March 23, 1999 12:00:00 AM
Subject:
Subject Public Key Info:
    Algorithm:  RSA - 1.2.840.113549.1.1.1
    Public Key:  E=user1@example.com, CN=Example.com, O=Example.com, OU=Example.com, C=US
30:81:89:02:81:81:00:BA:D4:EF:21:10:
D3:A9:1C:53:B7:0E:10:55:1E:EC:9A:0
A0:6E:42:AD:ED:F7:A3:9D:44:97:A6:1
0E:5A:A3:D3:CD:1E:75:7D:60:CD:1D:7
38:25:E8:F6:96:BC:A8:B5:D6:F5:66:1
E7:32:52:93:C3:A6:7B:A8:E2:96:A0:
33:82:65:50:62:42:30:F5:93:64:06:

```

The certificate is shown in base-64 encoded form at the bottom of the Certificate page, under the heading “Installing this certificate in a server.” In addition to its use with servers, this encoded form of the certificate can be used by CS administrators and Data Recovery Manager agents for setting up new agents and recovering private encryption keys, respectively. (For more information on key recovery, see “Finding and Recovering Keys” on page 73 in Chapter 6.)

# Revoking Certificates

Only Certificate Manager agents can revoke certificates other than their own. You need to revoke a certificate if one of the following situations occurs:

- The owner of the certificate has changed status and no longer has the right to use the certificate.
- The private key of a certificate owner has been compromised.

To revoke one or more certificates, you must search for the certificates you want to revoke using the Revoke Certificates button. While the search is similar to the one invoked by Search for Certificates, the Search Results form returned by this search gives you the option of revoking one or all of the found certificates.

## Searching for Certificates to Revoke

To search for one or more certificates to revoke:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 24).

You must submit the proper client certificate to get access to this page.

2. Click Revoke Certificates.

The search form that appears has the same search criteria sections as the Search for Certificates form.

3. Specify the search criteria by selecting the check boxes for the sections you want to use, then filling in the required information.

For details on search criteria, see “Advanced Certificate Search” on page 55.

4. Scroll to the bottom of the form and select a number of matching certificates to display.
5. Click Find.

The search returns a list of matching certificates. You have the option of revoking one or all certificates in the list.

Red Hat®  
Certificate System Agent Services

**Certificate Manager**

[List Requests](#)

[List Certificates](#)

[Search for Certificates](#)

**[Revoke Certificates](#)**

[Display Revocation List](#)

[Update Revocation List](#)

[Update Directory Server](#)

[OCSP Service](#)

### Search Results

**Issuer: CN=CS Demo root CA, OU=CS Test, O=Example Corp, L=MT View, ST=California, C=US**

Total number of records found: 1

Serial number	Subject name	
0x00000007	E=user1@example.com,CN=User One UID=user1, OU=Technical Publications O=Example Corp, C=US	
Version	Subject public key algorithm	
3	PKCS #1 RSA with 1024-bit key	
<a href="#">Details</a>	Not valid before	Not valid after
	2/24/1999	3/23/1999
<a href="#">Revoke</a>	Issued on	Issued by
	2/24/1999	csadmin

## Revoking One or More Certificates

You can revoke an entire list of certificates returned by a search, or select and revoke one of the certificates from the list.

### Revoking One Certificate

To revoke a single certificate:

1. On the Certificate Manager's Agent Services page, click Revoke Certificates, specify search criteria, and click Find to display a list of certificates.

For details of how to specify criteria, see "Basic Certificate Listing" on page 53 and "Advanced Certificate Search" on page 55.

2. On the Search Results form, find the certificate you want to revoke.

If the certificate you want to see is not shown, scroll to the bottom of the list, specify an additional number  $n$ , and click Find. The system displays the next  $n$  certificates that match your original search criteria.

3. Click the Revoke button next to the certificate that you want to revoke.
4. Confirm the revocation in the resulting form (see "Confirming a Revocation" on page 65).

## Revoking Multiple Certificates

To revoke all of the certificates found by a search:

1. On the Certificate Manager's Agent Services page, click Revoke Certificates, specify search criteria, and click Find to display a list of certificates.

For details of how to specify criteria, see "Basic Certificate Listing" on page 53 and "Advanced Certificate Search" on page 55.

2. On the Search Results page, scroll to the bottom to reach the "Revoke ALL  $n$  Certificates" button. The number shown in the button is the total number of certificates returned by the search. Note that this is usually a larger number than the number of certificates displayed on the current page.
3. Verify that all of the certificates returned by the search should be revoked (not just those displayed on the current page).
4. Click "Revoke ALL  $n$  Certificates" at the bottom of the form.
5. Confirm the revocation in the resulting form (see "Confirming a Revocation" on page 65).

---

**CAUTION** Whether you are revoking a single certificate or a list of certificates, be extremely careful that you have selected the correct one or that the list contains only the certificates you want to revoke. Once you confirm a revocation operation, there is no way to undo it.

---



## Confirming a Revocation

When you have requested the revocation of one or more certificates, the Certificate Revocation Confirmation form appears.

[List Requests](#)

[List Certificates](#)

[Search for Certificates](#)

[Revoke Certificates](#)

[Display Revocation List](#)

[Update Revocation List](#)

[Update Directory Server](#)

[OCSP Service](#)

[Manage Certificate Profiles](#)

### Certificate Revocation Confirmation

Use this form to confirm certificate revocation by selecting .

---

**Important:** When making this request you must use the br

#### Certificate Details

The details of the certificate being revoked are below:

Serial Number: 0x011  
 Subject Name: UID=TestUser, E=TestUser@test.com, CN=Test Use  
 Valid: not before: 2/20/2003 and not after: 8/19/2003

#### Select Invalidation Date

Please select the date on which it is known or suspected th

Invalidity date:

#### Select Revocation Reason

Please select reason for revocation.

Unspecified  
 Key compromised  
 CA key compromised  
 Affiliation changed

To confirm the revocation:

1. Inspect the details of the certificate and verify that it is the one you want to revoke. If you are revoking more than one certificate, the form shows details of all the listed certificates.
2. Select an Invalidation Date on which it is known or suspected that the private key was compromised or that the certificate became invalid. The Invalidation Date is presented as a set of drop down lists allowing the user to select the proper date.
3. Select a reason for the revocation. The reason applies to all the listed certificates.

4. Optionally, enter any additional comment. The comment will be included in the revocation request.
5. Click Submit.

The revocation request is submitted; it is automatically approved, and the certificate is revoked. You can see revocation requests by listing requests with a status of Completed; see “Listing Certificate Requests” on page 39.

---

**CAUTION** Whether you are revoking a single certificate or a list of certificates, be extremely careful that you have selected the correct one or that the list contains only the certificates you want to revoke. Once you confirm a revocation operation, there is no way to undo it.

---

## Managing the Certificate Revocation List

By revoking a certificate, you are notifying other users that the certificate is no longer valid. You make this notification by publishing a list of the revoked certificates, called the *certificate revocation list* (CRL), to an LDAP directory. This list is publicly available and ensures that revoked certificates are not misused.

---

**NOTE** Certificate System is currently the only Red Hat server that can check the revocation status of the certificates that it issues. With Certificate System, therefore, you can use the certificate revocation status to control access. On other Red Hat servers, you must use other forms of access control. For example, you can remove individual users from access groups to prevent them from accessing the server.

---

## Viewing or Examining CRLs

In some cases, you may need to view or examine the CRL, for example, prior to manually updating the directory with the latest CRL.

Only a Certificate Manager agent can view the CRL.

To view or display the CRL:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
2. Click Display Certificate Revocation List to display the form for viewing the CRL.

3. Select the CRL that you want to view. (If your administrator has created multiple issuing points, you will see them in the “Issuing point” drop-down list. Otherwise, you’ll only see the master CRL.)
4. Choose how you want to display the CRL by selecting one of the options from the Display Type pull down menu. The choices on this menu are as follows:
  - Cached CRL.** Choose to view the CRL from the cache rather than from the CRL itself. This option will produce faster display results than viewing the entire CRL.
  - Entire CRL.** Choose to retrieve and view the entire CRL.
  - CRL header.** Choose to retrieve and view the CRL header only.
  - Base 64 Encoded.** Choose to retrieve and view the CRL in Base 64 encoded format.
5. To examine the selected CRL, click Display.
 

The CRL appears in the browser window. You can, for example, check whether a particular certificate appears in the list. Additionally, you can also note recent changes: total number of certificates that were revoked since the last update, total number of certificates that were taken off hold since the last update, and total number of certificates that expired since the last update.

## Updating the CRL

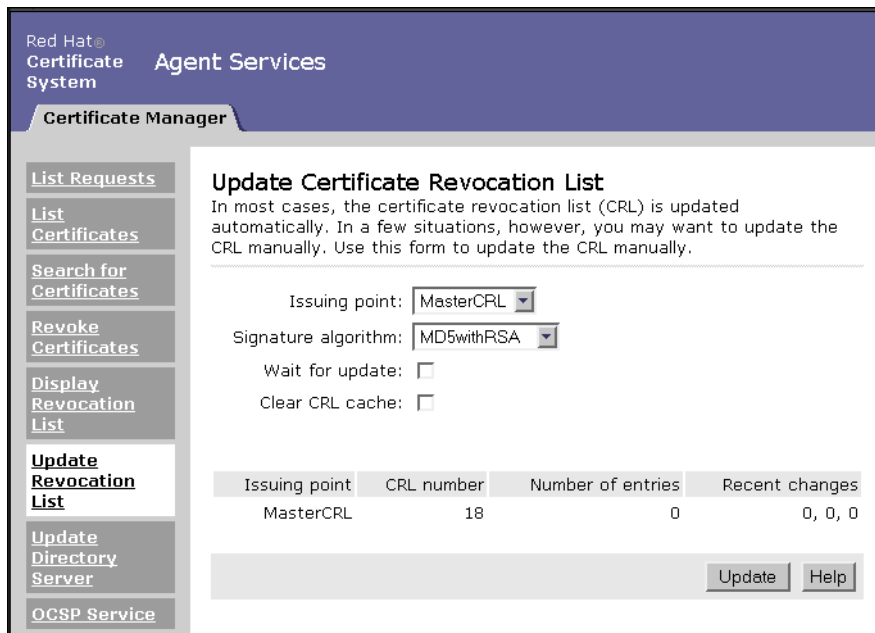
Normally, when you revoke a certificate, the CRL is automatically updated. If you are using Certificate System with an LDAP directory server, the CRL in the directory is updated automatically.

In some cases, you need to update the CRL manually. For example, you might want to remove expired certificates from the CRL to reduce its size. (Expired certificates do not need to be included in the CRL; they are already invalid because of the expiration date.) You might also want to update the CRL manually after the system has been down for any reason.

Only a Certificate Manager agent can manually update the CRL.

To manually update the CRL:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
2. Click Update Revocation List to display the form for updating the CRL.



3. Select the algorithm that you want to use to sign the new CRL.
  - o MD5 with RSA generates a 128-bit message digest. Most existing software applications that handle certificates support only MD5. This is the default algorithm.
  - o SHA-1 with RSA generates a 160-bit message digest. Before choosing SHA-1 with RSA, make sure your applications support it. Netscape Navigator 3.0 (or later) and Enterprise Server 2.01 (or later) support SHA-1.
  - o MD2 with RSA generates a 128-bit message digest. Before using MD2, make sure your applications support it.

Before selecting an algorithm, make sure that Certificate System has the algorithm enabled. Your CS administrator can let you know whether this is the case.

4. To examine CRL before updating it, click Display.
 

The CRL appears in the browser window. You can, for example, check whether a particular certificate appears in the list. Use the browser's Back button to return to the Update page.
5. To update the CRL with the latest certificate revocation information, click Update.

# Publishing to a Directory

This chapter describes the procedures for updating an LDAP directory with the current status of certificates. Only a Certificate Manager agent can update the directory.

This chapter contains the following sections:

- Working with a Directory Server
- Updating the Directory with Changes

## Working with a Directory Server

If your organization uses Red Hat Directory Server (or another LDAP directory server) to publish information about users in your organization, you can configure Certificate System to publish certificates and certificate revocation lists through the directory.

Certificate information published to the directory must be periodically updated as certificates are issued and revoked. Updates are usually published automatically but can also be published manually.

## Automatic Directory Updates

Once the CS administrator has configured Certificate System to work with Directory Server, any changes to certificate information in Certificate System are automatically updated in the directory. Updates take place at specific times:

- The first time you start Certificate System, it publishes the Certificate Manager's CA certificate to the directory.
- When Certificate System issues a new certificate, the certificate is published to the directory.

- When Certificate System revokes a certificate, the certificate is removed from the directory.
- When the CRL is created or updated, the list is published to the directory.

## Manual Directory Updates

Normally you do not need to update a directory manually; most updates are done automatically. You must update the directory manually in the following situations:

- Directory Server is down for a period of time and unable to receive changes from Certificate System.
- You want to remove expired certificates from the directory. Expired certificates are not automatically removed from the directory upon expiration. (Generally, any client using a certificate is responsible for determining that it is valid by checking its expiration date against the client's current date information.)

Using the Update Directory Server form available from the Certificate Manager Agent Services page, you make the following changes in the directory:

- Update the CRL in the directory.
- Update information on valid certificates (for example, update the server with newly issued certificates or recently renewed certificates).
- Remove expired certificates.
- Remove revoked certificates.

Note that only a Certificate Manager agent with the proper certificate can access the Update Directory Server form.

## Updating the Directory with Changes

To manually update the directory with changes:

1. Go to the Certificate Manager Agent Services page (see "Accessing Agent Services" on page 24). You must submit the proper client certificate to get access to this page.
2. Click Update Directory Server.

3. Select “Skip certificates already marked as updated” to ignore certificates in the internal database that are marked as having been published already (or removed in the case of revoked certificates).

For example, if you updated the directory once to revoke many certificates and it took several minutes, some new certificates may have been issued while the update was running. You would then use this selection and update the directory a second time to publish the new certificates (and save time by skipping all of the certificates that were just updated).

4. To publish the latest CRL, select “Update certificate revocation list to the directory.”
5. To update information on valid certificates to the directory, select “Update valid certificates to the directory.”

If you want to update only a range of certificates (for example, only the most recently issued certificates), specify the range of the serial numbers of those certificates.

6. To remove expired certificates from the directory, select “Remove expired certificates from the directory.”

If you want to remove only a range of certificates (not all expired certificates), specify the range of the serial numbers of those certificates.

7. To remove revoked certificates from the directory, select “Remove revoked certificates from the directory.”

If you want to remove only a range of certificates (not all revoked certificates), specify the range of the serial numbers of those certificates.

8. When you have finished specifying the changes that you want updated, click Update Directory.

---

**NOTE** In some circumstances, updating the directory can take considerable time. During this period, any changes made through Certificate System (for example, any new certificates issued or any certificates revoked) may not be included in the update. If you have issued or revoked any certificates during that time, you need to update the directory again to reflect those changes. Use “Skip certificates already marked as updated” the second time to update only certificates that changed (issued, revoked, expired) while the previous update was running.

---





# Recovering Encrypted Data

This chapter describes how to process key recovery requests and how to recover stored encrypted data when the encryption key has been lost. This service is available only when the Data Recovery Manager subsystem is installed. The Data Recovery Manager Agent Services page allows certified agents to accomplish these tasks.

This chapter contains the following sections:

- Finding and Recovering Keys
- Recovering Keys
- Viewing Key Service Requests

## Finding and Recovering Keys

If an end user loses a private encryption key or if a key's owner is unavailable, data encrypted with that key cannot be read unless a copy of the private key was archived when the key was created. The archived key can then be recovered and used to read the data.

As a Data Recovery Manager agent, you manage key recovery using the Data Recovery Manager's Agent Services page. You can search through archived keys, either to view them or to initiate a key recovery. Once you have initiated key recovery, a minimum number of designated key recovery agents are required to authorize the recovery. Key recovery agents may or may not also be certified Data Recovery Manager agents.

## Finding Archived Keys

You can search for archived keys to examine them or to initiate recovery. The process of selecting search criteria and selecting a key from the search results is the same in either case.

To search for and list archived keys:

1. Go to the Data Recovery Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
2. Click Search for Keys or Recover Keys to display the form in which you specify search criteria.

If you choose Recover Keys, you will have the option of initiating recovery for any key that you find.

The screenshot shows the Red Hat Certificate System Agent Services interface. The top navigation bar includes the Red Hat logo and the text 'Certificate System Agent Services'. Below this is a sub-header 'Data Recovery Manager'. A left-hand sidebar contains a list of menu items: 'List Requests', 'Search for Keys' (which is highlighted), 'Recover Keys', 'Authorize Recovery', and 'Recovery'. The main content area is titled 'Search for Keys' and contains the following text: 'Use this form to search for archived keys according to the criteria you specify.' Below this is a horizontal line, followed by the text: 'Each section lets you specify a key property. Select a property, then fill in any needed details in that section. You can combine search criteria to further narrow the search.' Another horizontal line follows, with the text: 'In the list of keys found by the search, you can click a button to display details about individual keys.' Below this is the 'Owner Name' section, which includes a checkbox labeled 'Show keys belonging to a particular owner' and an input field for the 'Owner Name'.

3. To search by particular criteria, use one or more of the different sections of the Search for Keys or Recover Keys form. To use a section, select the appropriate check box in that section, then fill in any necessary information.

**Owner Name.** Use this section to find an archived key with a specific owner name. The owner name for a key is much like the subject name for a certificate. It consists of a string that can be used in searches. Select the check box and enter the owner name for the key you want to find.

**Key identifiers.** Use this section to find an archived key with a specific key identifier or to list all keys within a range of key identifiers.

- To find a key with a specific key identifier, enter the key identifier in both the upper limit and lower limit fields. Use decimal or hexadecimal form. Use 0x to indicate the beginning of a hexadecimal number; for example, 0x2A. (Key identifiers are displayed in hexadecimal form in the Search Results and Details pages.)
- To find all keys within a range of key identifiers, enter the upper and lower limits of the key identifier range (in decimal or hexadecimal form).

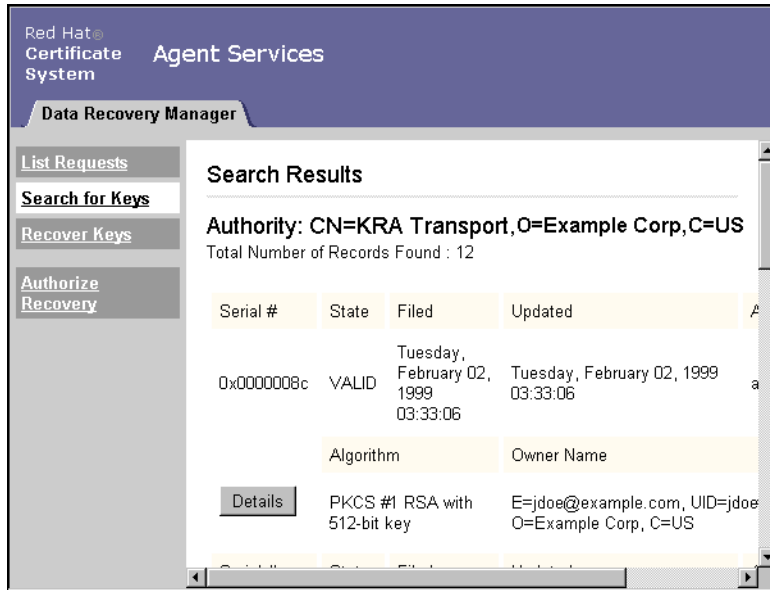
If you leave either the lower limit or upper limit field blank, all keys before or after the one you specify are displayed.

**Certificate.** Use this section to find the archived key that corresponds to a specific public key. Select the check box and paste the certificate containing the corresponding public key (in base-64 encoded form) into the text area. (You must first find and copy the encoded form of the encryption certificate associated with the key pair. Use the Certificate Manager or Registration Manager Agent Services pages to find the certificate; for instructions, see “Examining Certificates” on page 59.)

**Archiver.** Use this section to find keys that were archived by a specific server. Select the check box and enter the user ID of the Certificate Manager or Registration Manager that submitted the key archival request. Note that this information is available only for archival requests from servers that are remote from the Data Recovery Manager (that is, not installed in the same server root directory). To put a limit on the number of results returned, fill in a value for Maximum Results. To limit the time allowed for the search, enter a value for Time limit in seconds.

4. After entering your search criteria, click Show Key.

The Data Recovery Manager displays a list of the keys that match your search criteria. You can select a key in the list and examine it in more detail (described in “Selecting a Key” on page 76). If you initiated the search with the Recover Keys button, you have the option of recovering any key returned by the search (described in “Recovering Keys” on page 77).



## Selecting a Key

To select a key from the list returned by your key search:

1. On the Data Recovery Manager's Agent Services page, click Search for Keys, specify search criteria, and click Show Key to display a list of archived keys.

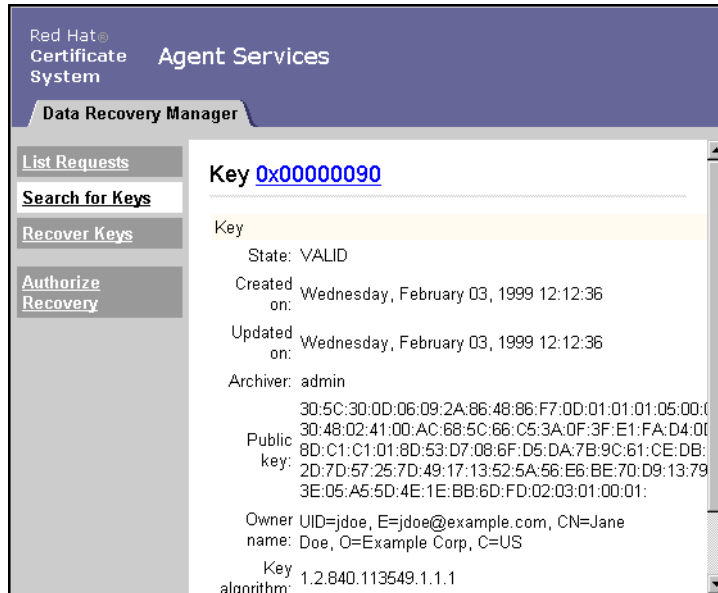
For details, see "Finding Archived Keys" on page 73.

2. On the Search Results form, find a particular key.

If the key you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of keys.

3. Click Details next to the key you want to examine.

The details of the selected key are shown in the Key details page. You cannot manipulate the key in any way.



## Recovering Keys

If you perform a search with the Recover Keys button, the Search Results form allows you to initiate the recovery of any key found.

To initiate key recovery:

1. On the Data Recovery Manager's Agent Services page, click Recover Keys, specify search criteria, and click Show Key to display a list of archived keys.

For details, see "Finding Archived Keys" on page 73.

2. On the Search Results form, find a particular key.

If the key you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of keys.

3. Click Recover next to the key you want to examine.

The details of the selected key are displayed in the Authorize Key Recovery form, which allows you to specify authorization information.

4. In the Key Recovery form, scroll to the bottom of the key information.



Red Hat  
Certificate System Agent Services

Data Recovery Manager

List Requests  
Search for Keys  
**Recover Keys**  
Authorize Recovery

Key [0x00000002](#)

Key

State: VALID  
Created on: Thursday, February 20, 2003 14:12:33  
Updated on: Thursday, February 20, 2003 14:12:33  
Archiver: cert-example  
Public key: 30:5C:30:0D:06:09:2A:86:48:86:F7:0D:86:53:90:DB:01:43:9E:FA:B8:9D:25:89:C6:51:F4:98:DA:96:A3:BB:9B:02:03:01  
Owner name: UID=drm1, E=drm1@example.com, CN=E  
Key algorithm: 1.2.840.113549.1.1.1  
Key length: 512

PKCS #12 Password:   
PKCS #12 Password again:   
Nickname (Optional):

The number of key recovery agent authorizations required to recover a key is configured by the system administrator using the CS window in Red Hat Console. The Key Recovery form has space for the required number of authorizations.

5. Specify the password that the requester will use in importing the recovered certificate/key pair package.
6. Type in the optional Nickname of the certificate that corresponds to the archived key.
7. Paste the base-64 encoded certificate that corresponds to the archived key into the text area.

Use the Certificate Manager or Registration Manager Agent Services pages to find and copy the certificate; see “Examining Certificates” on page 59.

If you searched for the archived key by using the corresponding public key, the certificate information is automatically transferred here.

8. Choose whether to authorize recovery locally.
  - o If you select this option, assemble the required number of key recovery agents and have each agent fill in his or her user name and password.

- If you deselect this option, notify the key recovery agents that a recovery has been initiated, giving them the recovery authorization reference number indicated on this form. (For information on how to provide a remote authorization, see “Remote Recovery Authorization” on page 79.)
9. Click Recover Now.
    - If you chose local authorization, the recovery is completed immediately, and the recovered certificate and key pair are sent to your browser in the form of a PKCS #12 package.
    - If you chose remote authorization, you must wait for the recovery agents to enter their authorizations. As they do so, a status page informs you of the progress. When the required number of recovery agents have completed their authorizations, the recovery is completed and the recovered certificate/key pair package is sent to your browser.
  10. In the dialog box that appears, specify the path and filename for saving the encrypted file that contains the recovered certificate and key pair.
  11. Send the encrypted file to the requesting party.
  12. Inform the requesting party of the recovery password in a secure manner.

The recovering party must use this password to import the recovered certificate/key pair package into his or her client software.

## Remote Recovery Authorization

By default, recovery authorization is local. That is, when you initiate the recovery, you assemble the required number of recovery agents, and all of them enter their IDs and passwords on the same Authorize Key Recovery form on your system. When you click Recover Now, the recovery is completed, and you receive the encrypted file that contains the recovered key and certificate.

If you deselect the local authorization option, you are choosing remote authorization. When you click Recover Now, the key recovery agents must each access the Data Recovery Manager Agent Services pages at their own locations, and use the Authorize Recovery button to enter each authorization separately. You are informed of the status of the authorizations. When all the authorizations have been entered, the recovery is completed and you receive the encrypted file that contains the recovered key and certificate.

To use the remote authorization feature, the designated key recovery agents must also be designated Data Recovery Manager agents, so that they are privileged to access the Agent Services pages directly. If you are using only local authorization, anyone can be designated as a recovery agent, since only you will need to access the recovery authorization form.

If you are a designated key recovery agent as well as a Data Recovery Manager agent, and another Data Recovery Manager agent informs you that a remote key recovery authorization has been initiated, enter your authorization as follows:

1. Go to the Data Recovery Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.
2. Click Authorize Recovery.
3. Enter the recovery authorization reference number that was part of the notification. This number identifies the particular key recovery request that you are to authorize.
4. Click Examine.
5. Enter your key recovery agent ID and password.
6. Click Grant.

The initiating agent is informed that you have completed your authorization.

## Viewing Key Service Requests

Key service requests are of two kinds:

- Key archival requests, made by remote or local Certificate Managers or Registration Managers
- Key recovery requests, made by Data Recovery Manager agents

As a Data Recovery Manager agent, you can view these requests. You can search for and list key service requests with a particular status, such as completed or rejected. You can select a key service request from the returned list and examine it in detail.

Key service requests are usually handled internally. You do not need to take any action on them unless your system is specially configured.

## Listing Key Service Requests

To list key service requests:

1. Go to the Data Recovery Manager Agent Services page (see “Accessing Agent Services” on page 24). You must submit the proper client certificate to get access to this page.



2. Click List Requests to display the List Requests form.

The screenshot shows the Red Hat Certificate System Agent Services interface. The main heading is 'Data Recovery Manager'. On the left, there is a sidebar with navigation options: 'List Requests' (selected), 'Search for Keys', 'Recover Key', and 'Authorize Recovery'. The main content area is titled 'List Requests' and contains the following form elements:

- Request type:** A pull-down menu currently set to 'Show archival requests'.
- Request status:** A pull-down menu currently set to 'Show completed requests'.
- Starting request identifier:** A text input field with '(optional)' written below it.
- Find button:** A button labeled 'Find'.
- Records field:** A text input field with 'first' on the left, '5' in the middle, and 'records' on the right.
- Help button:** A button labeled 'Help'.

Use the List Requests form to specify which key service requests to list.

3. Choose the type of requests you want to see from the “Request type” pull-down menu. You can choose to see requests to archive keys, to recover keys, or both.
4. Choose the status of requests you want to see by selecting one of the following choices from the “Request status” pull-down menu:
  - **Show canceled requests.** Unless your system is specially configured for it, there will be no cancelled requests.
  - **Show rejected requests.** Rejected requests do not comply with your company’s archival or recovery policies. Unless your system is specially configured for it, there will be no rejected requests.
  - **Show completed requests.** Completed requests include archival requests for which proof of archival has been sent and completed recovery requests.
  - **Show all requests.** All requests stored in the system.
5. To start the list at a specific place in the queue, enter the starting request identifier in decimal or hexadecimal form.

Use 0x to indicate the beginning of a hexadecimal number; for example, 0x2A. (Key identifiers are displayed in hexadecimal form in the Search Results and Details pages.)

- Choose the number of matching requests you want to see.

When you specify a number  $n$ , the system displays the first  $n$  requests after the starting request identifier that match your specified criteria.

- Click Find.

The Data Recovery Manager displays a list of the key service requests that match your search criteria. You can select a request in the list and examine it in more detail. For instructions, see “Selecting a Key” on page 76.

Red Hat  
Certificate System  
Agent Services

Data Recovery Manager

List Requests  
Search for Keys  
Recover Key  
Authorize Recovery

### Request Queue

Total Number of Records Found : 124

#	Status	Type	Filed on	Assigned to
100216	complete	recovery	12/17/1998 9:31:30	
			Updated on	Updated by
			12/17/1998 9:32:13	admin
100217	complete	recovery	12/17/1998 9:32:35	
			Updated on	Updated by
			12/17/1998 9:32:36	admin
100218	complete	recovery	12/17/1998 9:32:49	

## Selecting a Request

To select a request from the queue:

- On the Data Recovery Manager’s Agent Services page, click List Requests, specify search criteria, and click Find to display a list of key service requests.

For details, see “Listing Key Service Requests” on page 80.

2. On the Key Service Request Queue form, find a particular request.  
If the request you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of requests.
3. Click Details next to the selected request.

The details of the selected key service request appear in the Request details form. You cannot manipulate the request in any way.

The screenshot displays the Red Hat Certificate System Agent Services Data Recovery Manager interface. On the left, there is a sidebar with the following options: **List Requests** (highlighted), **Search for Keys**, **Recover Key**, and **Authorize Recovery**. The main content area is titled **Request 3** and shows the following details:

Request	Status: complete
	Type: recovery
	Created on: Thursday,
	Updated by: admin
	Updated on: Thursday,
Recovery Information	
	Key identifier: 2

If the system changes the state of the displayed request, and if you use your browser's Back or Forward buttons or the Go (history) menu to move to another page, the data shown can become out of date. To refresh the data, click the highlighted key identifier at the top of the page.



# Managing OCSP Service Related Tasks

This chapter describes how to perform Online Certificate Status Manager agent's tasks, such as identifying a CA to the Online Certificate Status Manager, adding a CRL to the Online Certificate Status Manager's internal database and so on. This service is available only when the Online Certificate Status Manager subsystem is installed. The Online Certificate Status Manager Agent Services page allows certified agents to accomplish these tasks.

This chapter contains the following sections:

- Listing CAs Identified by Online Certificate Status Manager
- Identifying a CA to Online Certificate Status Manager
- Adding a CRL to Online Certificate Status Manager
- Checking the Revocation Status of a Certificate

## Listing CAs Identified by Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Each Certificate Manager that can publish CRLs to the Online Certificate Status Manager must have its *CA signing certificate* stored in the internal database of the Online Certificate Status Manager. For instructions, see “Identifying a CA to Online Certificate Status Manager” on page 86.

At any given time, you can see the list of Certificate Managers that are currently recognized by the Online Certificate Status Manager.

To see the list of Certificate Managers:

1. Open a web browser window.

2. Go to the Online Certificate Status Manager's Agent interface. The URL is in this format: `https://<hostname>:<port>`.

The Online Certificate Status Manager Agent Services interface appears.

3. In the left frame, click List Certificate Authorities.

The resulting form should show information about the Certificate Managers (CAs) that are recognized by the Online Certificate Status Manager.

## Identifying a CA to Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Before you configure a Certificate Manager to publish CRLs to the Online Certificate Status Manager, you must identify the Certificate Manager to the Online Certificate Status Manager. You do this by storing the Certificate Manager's *CA signing certificate* in the internal database of the Online Certificate Status Manager.

The steps below explain how to store the Certificate Manager's *CA signing certificate* in the internal database of the Online Certificate Status Manager:

1. Open a web browser window.
2. Go to the Certificate Manager's end-entity interface. The URL is in `https://<hostname>:<SSL_port>` or `http://<hostname>:<port>` format.
3. Select the Retrieval tab, and in the left frame, click List Certificates.

4. In the resulting form, click Find.

A list of certificates appear.

5. Locate the Certificate Manager's CA signing certificate by looking at the subject name of the certificate.

Typically, the CA signing certificate is the first certificate the Certificate Manager issues.

6. Click Details.
7. In the resulting page, scroll to the section that says "Base 64 encoded certificate" and shows the CA signing certificate in its base-64 encoded format.

8. Copy the base-64 encoded certificate, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- marker lines, to the clipboard or a text file.

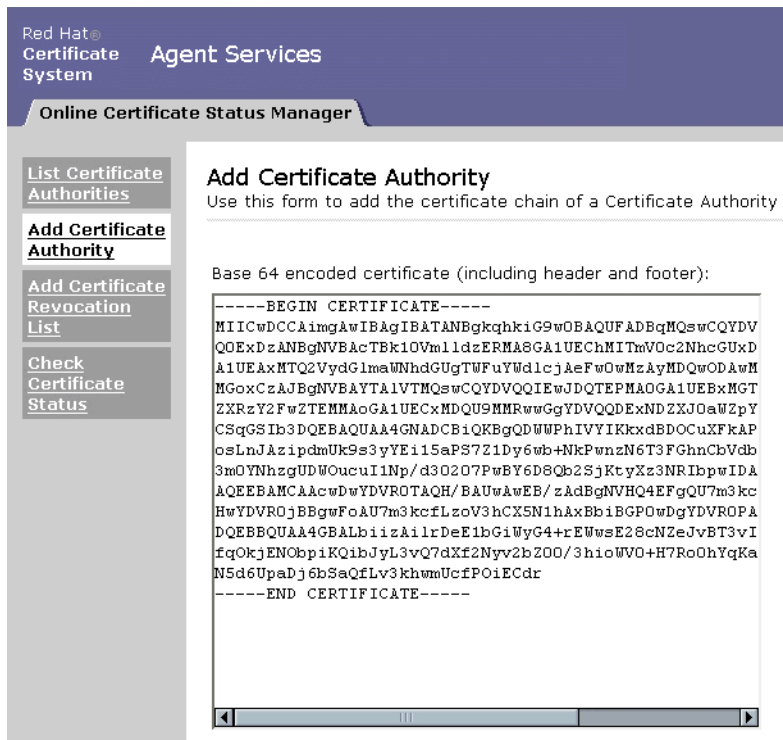
The copied information should look similar to the following example:

```
-----BEGIN CERTIFICATE-----
MIICJzCCAZCgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBCMSAwHgYDVQQKEXdOZXRz
Y2FwZSBDb21tdW5pYF
0aw9uczngjhnMVQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4XD Tk4MDgyNzE5MDAwMF
oXDTk5MDIyMzE5MDAw
MnbjdgngYoxIDAeBgNVBAoTF05ldHNjYXB1IENvbW11bm1jYXRpb25zMQ8wDQYDV
QQLewZQZW9wbGUxFzA
VBgoJkiaJkIisZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEj
MCEGCSqGSIb3Dbn dgJ
ARYUc3Vwcm15YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA
oYiYgthgtbbnjfngjn
jgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZIAIYb4QgEBAQHBAQDagCAMA0GCSq
GSIB3DQEBAUAA
-----END CERTIFICATE-----
```

9. Go to the Online Certificate Status Manager's Agent interface. The URL is in this format: `https://<hostname>:<port>`.

The Online Certificate Status Manager Agent Services interface appears.

10. In the left frame, click Add Certificate Authority.
11. In the resulting form, paste the encoded CA signing certificate inside the text area labeled "Base 64 encoded certificate (including header and footer)."



12. Click Add.

The certificate is added to the internal database of the Online Certificate Status Manager.

13. To verify that the certificate is added successfully, in the left frame, click List Certificate Authorities.

The resulting form should show information about the Certificate Manager (CA) you just added.

## Adding a CRL to Online Certificate Status Manager

There may arise a situation when a Certificate Manager is unable to publish its CRL to the Online Certificate Status Manager. In such exigencies, you can manually add a CRL to the internal database of the Online Certificate Status Manager.



To add a CRL to the internal database:

1. Open a web browser window.
2. Go to the Certificate Manager's Agent interface (see "Accessing Agent Services" on page 24). The URL is in this format: `https://<hostname>:<port>`. You must submit the proper client certificate to get access to this page.

The Certificate Manager Agent Services interface appears.

3. Click on the item Display Revocation List.
4. In the resulting form, select the desired CRL issuing point and select the option to display the CRL in base-64 encoded format and click Display.
5. In the resulting page, scroll to the section that says "Certificate revocation list base64 encoded," which shows the CRL in its base-64 encoded format.
6. Copy the base-64 encoded CRL, including the -----BEGIN CERTIFICATE REVOCATION LIST----- and -----END CERTIFICATE REVOCATION LIST----- marker lines, to the clipboard or a text file.

The copied information should look similar to the following example:

```
-----BEGIN CERTIFICATE REVOCATION LIST-----
MIICJzCCAZCgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBCMSAwHgYDVQQKEXdOZXRz
Y2FwZSBDb21tdW5pYF
0aW9uczngjhnMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDtk4MDgyNzE5MDAwMF
oXDTk5MDIyMzE5MDAw
MnbjdgngYoxIDAeBgNVBAoTF05ldHNjYXB1IENvbW11bm1jYXRpb25zMQ8wDQYDV
QLEwZQZW9wbGUxFzA
VBgoJkiaJkIisZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEj
MCEGCSqGSIb3DbnGJ
ARYUc3Vwcm15YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIaKEA
oYiYgthgtbbnjfngjn
jgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZIAyB4QgEBAQHBAQDAgCAMA0GCSq
GSIB3DQEBAUAA4GBA
Fi9FzyJlLmS+kzsue0kTXawbwamGdYql2w4hIBgdr+jWeLmD4CP4xzmKdvQ6IqD2
q8DBs91RQu9JYg129o
-----END CERTIFICATE REVOCATION LIST-----
```

7. Go to the Online Certificate Status Manager's Agent interface. The URL is in this format: `https://<hostname>:<port>`.

The Online Certificate Status Manager Agent Services interface appears.

8. In the left frame, click Add Certificate Revocation List.

9. In the resulting form, paste the encoded CRL inside the text area labeled “Base 64 encoded certificate revocation list (including the header and footer).”

10. Click Add.

The CRL is added to the internal database of the Online Certificate Status Manager.

## Checking the Revocation Status of a Certificate

You can check the revocation status of a certificate by submitting the certificate in its base-64 encoded format to the Online Certificate Status Manager:

1. Copy the base-64 encoded certificate, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- marker lines, to the clipboard or a text file.

The copied information should look similar to the following example:

```
-----BEGIN CERTIFICATE-----  
MIICJzCCAZCgAwIBAgIByrgrugr wuguvgrvhfeygyDBCMSAwHgYDVQKExdOZRz  
Y2FwZSBDb21tdW5pYF  
dih9uczngjhnMVQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4XDTk4MDgyNzE5MDAwMF  
oXDTk5MDIyMzE5MDAw  
MnbjdgngYoxIDAeBgNVBAoTF05ldHNjYXB1afkhhbfgsdbutihdhhb25zMQ8wDQYD  
VQLLEwZQZW9wbGUxZjA  
VBgoJkiaJkIisZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEj  
MCEGCSqGSIb3DbnDgJ  
ASdUc3Vwcm15YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIaKEA  
oYiYgthgtbbnjfngjn  
jgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZIAyba4QgEBAQHBAQDagCAMA0GCSq  
GSIb3DQEBAUAA  
-----END CERTIFICATE-----
```

2. Go to the Online Certificate Status Manager Agent Services page (see “Accessing Agent Services” on page 24).

You must submit the proper client certificate to get access to this page.

3. In the left frame, click Check Certificate Status.
4. In the resulting form, paste the certificate inside the text area labeled “Base 64 encoded certificate.”
5. Click Check.

The resulting form should inform you about the status of the certificate you just submitted.

# Index

## A

- accessing end-entity gateways 16, 27
- accessing forms 24
- Adjusting 43
- administrator/agent, initial enrollment 24
- agent services forms
  - accessing 24
  - Certificate Manager 17
  - Data Recovery Manager 19
  - Online Certificate Status Manager 20
  - Registration Manager 19
  - summary 21
- agents
  - requirements for 17
  - responsibilities 16
- assigning requests 44

## C

- CA
  - built-in OCSP service 14
- certificate authorities (CAs) 13
- Certificate Manager
  - agent services forms 17, 21
  - built-in OCSP service 14
  - overview 14
- certificate profile
  - approving 33
  - certificate profile information 32

- diapproving 33
- end user certificate profile 32
- policy information 33
- processing requests 43
- certificate requests
  - approving 42
  - assigning 44, 76, 82
  - examining 41
  - handling process 35
  - listing 39
  - statuses 40
  - types of 39
- Certificate System
  - directory server and 69
  - overview 13
  - subsystems 14
- certificates
  - finding 53
  - issuing to requester 49
  - searching for 55
- cloning enrollment requests 37, 48
- conventions used in this book 9
- cryptography concepts 7

## D

- Data Recovery Manager 73–83
  - agent services forms 19, 21
  - overview 15
- directory server
  - Certificate System and 69

documentation  
conventions followed 9

## E

end entities 13  
end-entity gateways, accessing 27  
enrollment requests  
    approving 42  
    assigning 44  
    cloning 37, 48  
    examining 41  
    handling process 35  
    listing 39  
    statuses 40  
enrollment, initial administrator/agent 24

## F

fonts used in this book 9  
forms  
    accessing 24  
    summary 21

## I

initial enrollment, administrator/agent 24  
introduction 13  
issuing a certificate 49

## L

List Requests form 39

## M

managers, overview 14

## N

notification of issuance 49

## O

OCSP 15  
OCSP responder  
    defined 15  
Online Certificate Status Manager 85–90  
    agent services forms 20  
    overview 15  
online certificate validation authority  
    defined 15

## P

PKI (public key infrastructure) 13  
prerequisites 7  
privileged operations and users 17  
profiles 29  
    about 29  
    approving and disapproving 32  
    enabling and disabling 32  
    how profiles work 31  
    working with 29

## R

Registration Manager  
    agent services forms 19, 21  
    overview 14  
Request details form 42

- Request Queue form 41
- request status, on List Requests form 40
- requests, enrollment
  - approving 42
  - assigning 44
  - cloning 37, 48
  - examining 41
  - handling process 35
  - listing 39
  - statuses 40
  - types of 39

## **S**

- security concepts 7, 13
- Services Summary page 27
- Show canceled requests (request status) 40
- Show completed requests (request status) 40
- Show ending requests (request status) 40
- Show rejected requests (request status) 40
- status of requests 40
- subsystems, overview 14

## **T**

- type styles used in this book 9