Symantec™ Managed PKI®

Integration Guide for Cisco® 3745 and Cisco® 2811 Routers

Symantec

Symantec™ Managed PKI® Integration Guide for Cisco® 3745 and Cisco® 2811 Routers

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated July 10, 2013

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1

Integrating Managed PKI Certificates with Cisco® 3745 and Cisco® 2811 Routers

Managed PKI certificates can be integrated with many common applications to enable secure communications and online access. This document describes how to integrate Managed PKI certificates with Cisco 3745 and Cisco 2811 routers to enable the router to securely authenticate itself to networks and other devices with which it communicates.

Partner Information

Table 1-1 Partner Information

Partner Name	Cisco Systems, Inc.
Product Name	Cisco 3745 Multiservice Access Router, Cisco 2811 Integrated Services Router

Integration Architecture

The following diagram describes how the Managed PKI certificate integrates with the Cisco 3745 and 2811 routers to provide secure authentication.

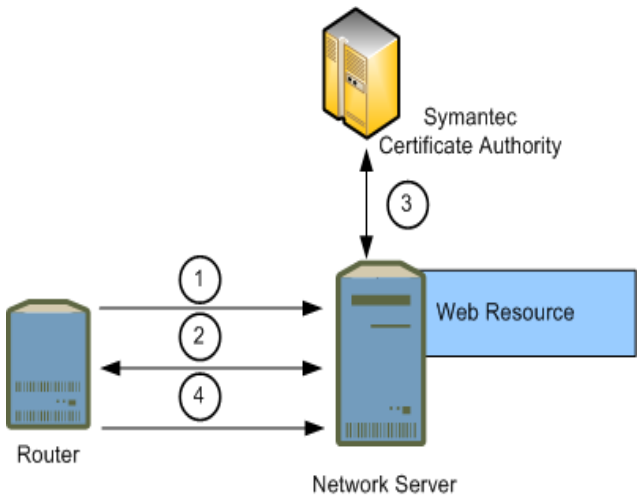

Figure 1-1 Authenticating a Cisco router with a Managed PKI certificate

1. The router accesses a server on the network
2. The network server requests authentication from the router. The router provides the Managed PKI certificate as authentication.
3. The network server authenticates the certificate and its issuing chain with the Symantec Certificate Authority.
4. The network server allows the router to access the network resource.

Pre-requisites

These procedures assume you have access to a Managed PKI account with a private CA. Contact your Symantec representative for assistance obtaining an account.

These procedures have been tested on the Cisco 3745 Multiservice Access Router and Cisco 2811 Integrated Services Router. You must have access to Privileged mode on the router. Managed PKI certificates may work with other Cisco routers, but Symantec has not qualified other routers and does not provide procedures or support for them.

Integration Workflow

Figure 1-2 describes the general steps required to set up the Managed PKI account and integrate Managed PKI certificates with Cisco 3745 and 2811 routers.

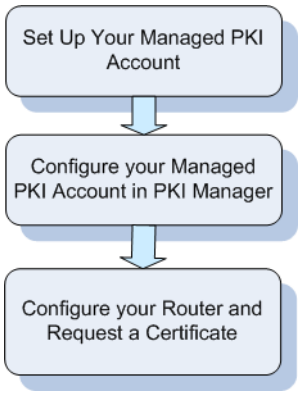

Figure 1-2 Managed PKI integration workflow

Task 1. Set up your Managed PKI account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

- You will need to complete and return the following documents. As needed, your Symantec representative will assist you with obtaining and completing these forms.
  - Master Service Agreement
  - Issuing Authority Naming Application (also known as the CA Naming Document)
  - Symantec Services Order Form
  - Purchase Order, credit card, or reference number
- You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. Refer to PKI Manager and its online help for details on configuring Managed PKI.

Task 2. Configure your certificate profiles in PKI Manager

As the Managed PKI administrator, configure your Cisco certificate profiles using PKI Manager. When defining your certificate profile, some selections you make will restrict options later on (for example, if you select **SCEP** as the Enrollment method the Authentication method will be restricted to **Enrollment code**). Otherwise, you can set any values necessary for your needs.

Refer to PKI Manager and the online help for details on configuring certificate profiles.

However, for Managed PKI certificates that can be used by Cisco routers, you should consider the following:

- For the certificate profile template, select **IPSec Authentication**.
- For the Enrollment method, select one of the following:
  - Select **SCEP** if you will enroll for Managed PKI certificates using a Simple Certificate Enrollment Protocol (SCEP) request. The seat ID for the Managed PKI certificate will be the CN value.
  - Select **CSR** if you will enroll for Managed PKI certificates using a Certificate Signing Request (CSR). The seat ID for the Managed PKI certificate will be the DNS name.

  You can select only one Enrollment method per certificate profile. If you will enroll for Managed PKI certificates using more than one method, create a separate certificate profile for each.

Once you save the certificate profile, PKI Manager displays the certificate enrollment URL. You will need to provide the enrollment URL to any device or user that will enroll for a certificate using this certificate profile.

Task 3. Configure your router and request a certificate

The remainder of this document describes how to configure your Cisco router and enroll for Managed PKI certificates. Refer to the appropriate chapter, based on how you will enroll for Managed PKI certificates:

- Chapter 2 "Obtain Managed PKI Certificates using a SCEP Request."
- Chapter 3 "Obtain Managed PKI Certificates using a CSR Enrollment."

Chapter 2

Obtain Managed PKI Certificates using a SCEP Request

If you will enroll for Managed PKI certificates using a SCEP request, complete the procedures in this chapter to enroll for a certificate and configure your router to accept these certificates.

This chapter describes the following procedures:

Obtain a Managed PKI Certificate for the Router

To obtain a certificate for the router, you first add the router as a user in PKI Manager, and then enroll that user for a certificate.

1. As the Managed PKI administrator, click **Add users** from the *Manage users* page of PKI Manager.
2. Select that you will add **A single user** and enter the seat ID for the router (typically an email address for the administrator or group alias that manages the router). Click **Continue**.
3. You are prompted for additional information:
   a. Enter a unique first and last name for this user.
   b. If you did not enter an email address in Step 1, you will be prompted for one now. Enter an email address for the administrator or group alias that manages the router.
   c. Make sure that the **I want to enroll this user for a certificate** check box is not selected.
   d. Click **Continue**. PKI Manager creates the user.
4. Create a comma-separated value (.csv) file containing the seat ID you entered for the user in Step 2 and the enrollment code for the user. If you will have the system generate an enrollment code, do not include this value.

   An example file would look similar to the following:

   ```
   cisco_router@organization.com,123456
   ```
5. From the *Manage users* page of PKI Manager, click **Enroll users**.
   a. In the *Choose certificate profile* drop-down, select the certificate profile you created in Task 2, "Configure your certificate profiles in PKI Manager", "Configure your certificate profiles in PKI Manager" on page 3.
   b. In the *Enrollment code for picking up certificate* drop-down, select **CSV file has enrollment codes** or **System generated enrollment code**, as appropriate.
   c. Click **Find** under *Upload .csv file* and navigate to the file you created in Step 4.
   d. Identifies whether PKI Manager should send an enrollment email to the user.
6. Click **Continue**.

PKI Manager enrolls the user for a certificate and displays the enrollment code. Provide that enrollment code when enrolling for the certificate.

Configure the Router and Install the Certificate

Once you have enrolled for a certificate on behalf of the router, you will need to configure the router. This includes synchronizing the router clock, setting privileges and debugging levels, clearing any existing certificate keys, and installing the new certificate and the certificate chain.

Enter the commands listed in Table 2-1 to configure the router and install the certificate:

Table 2-1 Steps for configuring the router and installing the certificate

Step	Action	Command
1	Log into the router as a user with access to Privileged mode.	#Login as <user name> #Sent username ‘’<user name>’’ #<router name> password: <user password>
2	Enable Privileged mode	# enable #Password: <user password>
3	Enable debugging (this is optional, but assists with troubleshooting any issues):	# debug crypto pki transactions debug crypto pki messages
4	Enter configuration mode on the router.	#terminal monitor #configure terminal
5	Remove any previous domain names or CA identities for this certificate chain (for example, ones added during testing). <domain name> is the domain name for the router, if configured.	#no ip domain-name <domain name> #no crypto ca identity <domain name>
6	Remove any existing keys (for examples, ones added during testing).	#crypto key zeroize rsa <key-pair-name>
7	Set the domain name for the router. This is only required if you are using a relative host name to identify the router rather than fully qualified domain names.	#ip domain name <domain name>
8	Generate the key for the certificate that will be installed on the router. <key-pair-name> should be a unique name for the key you will generate. <key size> is 2048 or higher.	#crypto key generate rsa general-keys label <key-pair-name> modulus <key size>
9	Create the CA identity. The CA identity should be the name of the trustpoint on the router.	#crypto ca identity <trustpoint name>
10	Set the parameters used when enrolling for the certificate for the router.	#enroll url <URL displayed in PKI Manager for the certificate profile from Task 2, "Configure your certificate profiles in PKI Manager", on page 3> #password 0 <enrollment code for the certificate> #enroll retry count <number of times to retry the enrollment before timing out> #enroll retry period <time in minutes to wait for each attempt before timing out> #subject-name cn=<certificate common name> #exit
11	Obtain the CA certificate. This will download the CA chain for the router’s certificate and save it to the router’s trustpoint.	#crypto ca authenticate <trustpoint name>

Table 2-1 Steps for configuring the router and installing the certificate (Continued)

Step	Action	Command
12	Enroll for the certificate for the router. This will request a certificate for the router, and if approved, download it to the router's trustpoint.	`#crypto ca enroll <trustpoint name>`
13	Exit configuration mode on the router.	`#exit`
14	Verify that the certificates were successfully installed. The new certificate will be displayed, along with any other certificates on the router. You can also view the issued certificate and its issuing CA in PKI Manager by searching for the certificate on the *Manage certificates* page.	`#show crypto ca certificates`

Configure the Router to Renew the Certificate

You can configure the router to renew the certificate when it reaches a specific percentage of its validity period.

1 Track the certificate expiration using PKI Manager:

   a As the Managed PKI administrator, click **Add reports** from the *Manage Reports* page.

   b Create a Certificate Information or Expiring end user certificates report for the certificate profile you created in Task 2, "Configure your certificate profiles in PKI Manager", "Configure your certificate profiles in PKI Manager" on page 3.

2 When the certificate is due to expire, enroll for a replacement certificate using the procedures in Step 4 and Step 5 under "Obtain a Managed PKI Certificate for the Router" on page 5.

3 Enter the commands listed in Table 2-2 to configure the router to automatically replace the expiring certificate using a new private key.

Table 2-2 Steps for configuring the router to auto-renew the certificate

Step	Action	Command

1	Log into the router as a user with access to Privileged mode.	`#Login as <user name>`
		`#Sent username ''<user name>''`
		`#<router name> password: <user password>`

2	Set the name of the CA under which the certificate will be renewed. This should be the same trustpoint name used when enrolling for the original certificate. You can view the original certificate and its issuing CA in PKI Manager by searching for the certificate on the *Manage certificates* page.	`#configure terminal#crypto ca trustpoint <trustpoint name>` `#crypto ca trustpoint <trustpoint name>`
3	Set the URL the router will access when requesting renewal.	`#enrollment url <URL>`

4	Set the parameters the router will use when requesting renewal.
	<percentage> is the percentage of the validity period remaining before the router will request renewal. For example, if you set this to 90 for a one-year certificate, a new certificate will be requested 36.5 days before the old certificate expires.
	<password> is the enrollment code for the replacement certificate.
	<keypair name> is the name of the key pair to renew.
		`#auto-enroll <percentage> regenerate`
		`#password <password>`
		`#rsakeypair <keypair name> 2048`
		`#exit`

Table 2-2 Steps for configuring the router to auto-renew the certificate (Continued)

Step	Action	Command
5	Set the CA certificate name. This will download the CA chain for the renewal certificate and use it to authenticate the renewed certificate.	`#crypto ca authenticate <trustpoint name>>`

Chapter 3

Obtain Managed PKI Certificates using a CSR Enrollment

If you will enroll for Managed PKI certificates using a CSR, complete the procedures in this chapter to enroll for a certificate and configure your router to accept these certificates.

This chapter describes the following procedures:

Generate a CSR

Enter the commands listed in Table 3-1 to generate a CSR on the router:

Table 3-1 Steps for generating a CSR

Step	Action	Command
1	Log into the router as a user with access to Privileged mode.	#Login as <user name> #Sent username ''<user name>'' #<router name> password: <user password>
2	Enable Privileged mode	# enable #Password: <user password>
3	Enable debugging (this is optional, but assists with troubleshooting any issues):	# debug crypto pki transactions debug crypto pki messages
4	Enter configuration mode on the router.	#terminal monitor #configure terminal
5	Create a CA trustpoint.	#crypto ca trustpoint <trustpoint name> #enrollment terminal #crl optional #subject-name cn=<certificate common name> #fqdn <fully-qualified domain name for the router> #rsakeypair <keyfile name> #exit
6	Generate the key for the certificate that will be installed on the router. <keyfile name> should be a unique name for the key you will generate. <key size> is 2048 or higher.	#crypto key generate rsa general-keys label <keyfile name> exportable modulus <key size>
7	Generate the CSR to be used to enroll for the certificate.	crypto ca enroll <trustpoint name>

Enroll for a Certificate

To enroll for a certificate, you will need to request a using the CSR generated in "Generate a CSR" on page 9, and then approve the request in PKI Manager.

1 Using a standard text editor, open the CSR generated in "Generate a CSR" on page 9. Copy the contents of the CSR into your clipboard.

2 As the Managed PKI administrator, access the URL displayed in PKI Manager for the certificate profile from Task 2, "Configure your certificate profiles in PKI Manager", "Configure your certificate profiles in PKI Manager" on page 3.

3 Complete the following:

- For **DNS name**, enter the fully-qualified domain name you configured for the CA trustpoint. You can enter any additional DNS names.
- For **Email address**, enter an email address for the administrator or group alias that manages the router.
- Select **Paste CSR** and paste the contents of your clipboard into the **Paste CSR below:** textbox. Click **Continue**.

4 On the *Manage users* page of PKI Manager, search for the name of the user. Use the DNS name you entered when you submitted the CSR in Step 3.

5 Click **Manage this request** in the details pane for the user, and review the certificate request details.

6 In the *Approval status* drop-down box, select **Approved** and click **Save**.

After the certificate request is approved, Managed PKI will send an email to the address entered in Step 3 of "Enroll for a Certificate" on page 10. The email will contain the router certificate and the issuing CA.

Import the Certificate into the Router

1 Export the certificate from .p7b to .cer format:

a Open the user certificate from the email received in Step 6 of "Enroll for a Certificate" on page 10 using Window's Crypto Shell Extensions utility.

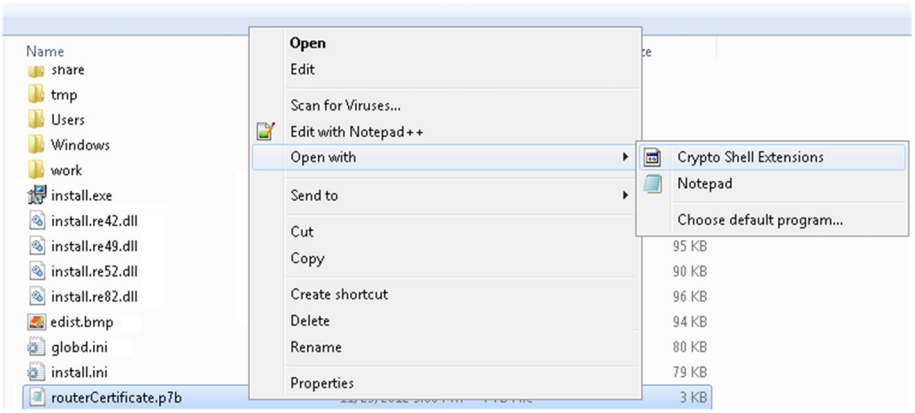

Figure 3-1 Opening with Crypto Shell Extension utility

b Right-click the certificate and select **All Tasks → Export**.

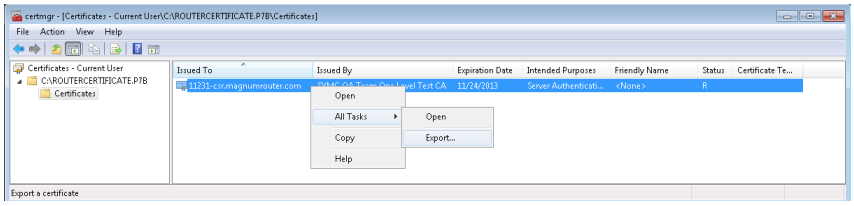

Figure 3-2 Opening the Certificate Export Wizard

c The *Certificate Export Wizard* appears. Click **Next** and then select **Base-64 encoded X.509 (.CER)** as the *Export File Format*.

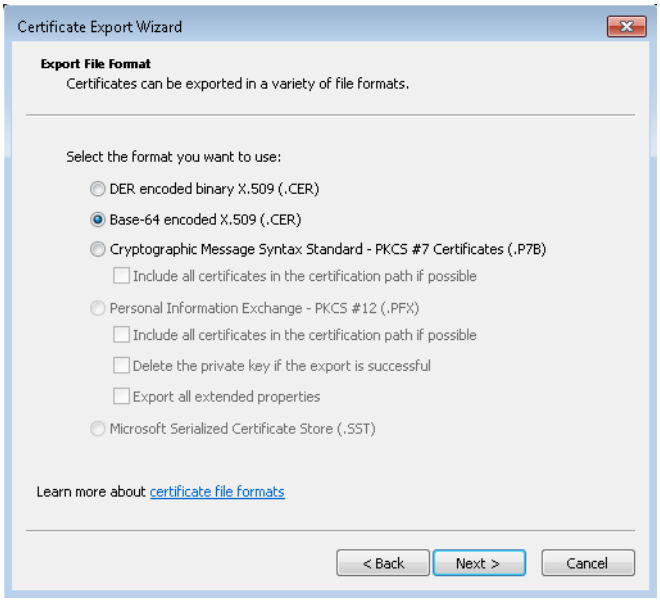

Figure 3-3 Choosing an export format

d Click **Next** to save the file in the new format.

2 Enter the commands listed in Table 3-2 to import the certificate into the router.

Table 3-2 Steps for importing the certificate into the router

Step	Action	Command
1	Set the CA certificate name.	`#crypto ca authenticate <fully-qualified domain name for the router>`
2	You are prompted for the CA certificate. Using a standard text editor, open the CA certificate from the email received in Step 6 of "Enroll for a Certificate" on page 10 and copy the contents of the file into your clipboard. Paste the contents of your clipboard into the router.	`N/A`
3	Import the CA certificate.	`#crypto ca import <fully-qualified domain name for the router> certificate`

Table 3-2 Steps for importing the certificate into the router (Continued)

Step	Action	Command
4	You are prompted for the certificate. Using a standard text editor, open the base64-encoded file you created in Step 1 and copy the contents of the file into your clipboard. Paste the contents of your clipboard into the router.	`N/A`
5	Exit configuration mode on the router.	`#exit`
6	Verify that the certificates were successfully installed. The new certificate will be displayed, along with any other certificates on the router. You can also view the issued certificate and its issuing CA in PKI Manager by searching for the certificate on the *Manage certificates* page.	`#show crypto ca certificates`