

Application Note

Cisco Router and Security Device Manager **Public Key Infrastructure Management**

Introduction

This document gives an example of how to enroll a Cisco IOS® Software router to a certificate authority (CA).

Public Key Infrastructure Introduction

Public Key Infrastructure (PKI) provides a hierarchical framework for managing the digital security attributes of entities that engage in secured communications. In addition to human users, the following entities also participate in the PKI: encryption gateway, secure Web servers, and other resources that require close control of identity and encryption.

Each PKI participant holds a digital certificate issued by a certificate authority. The certificate contains numerous attributes that are used when parties negotiate a secure connection. These attributes must include the certificate validity period and end-host identity information. Optional attributes can be included, depending on the requirement and capability of the PKI.

The certificates contain two components of asymmetric encryption: a public key and a private key¹. Data that is encrypted with the public key can be decrypted with the private key, and conversely. The parties who need to encrypt their communications exchange their public keys (contained in the certificate), but do not disclose their private keys. The sending party uses the receiving party's public key to encrypt message data and forward the ciphertext (encrypted data) to the other party. The receiving party then decrypts the ciphertext with the assigned private key. The public key is shared without any restrictions, but the private key is never shared.

Enrolling in a Certificate Authority

Enrollment is the process of obtaining a certificate. It occurs between the end host desiring the certificate and the authority in the PKI that is responsible for providing certificates. The end hosts that participate in a PKI must obtain a certificate, which is presented to the parties with whom they communicate when they need a secured communications channel. The enrollment process for an end host:

1. The end host generates a private-public key pair.
2. The end host generates a certificate request, which is forwarded to the certificate authority.
3. After the request is approved, the certificate authority signs the certificate request with its private key and returns the completed certificate to the end host.

¹ A public key and a private key are called a RSA key pair.



4. The end host writes a certificate into a nonvolatile storage area: PC hard disk or NVRAM on Cisco Systems® routers.

Certificate Validation

After participating PKI entities have enrolled, they are ready to negotiate secure connections with each other.

In most cases, secure communication between two parties is initiated by an application process, such as ISAKMP for an IP Security (IPSec) negotiation or HTTP for a Secure Sockets Layer (SSL) negotiation. The end hosts eventually exchange their certificates for mutual verification. The steps during a certificate validation between two parties follow:

1. The certificate is presented within its validity period.
2. The certificate authority that signed the certificate is a component of the appropriate PKI.
3. The certificate is not on a revocation list.

If the certificate passes all the validity criteria, the parties use the public key contained within the certificates to negotiate the IPSec Security Associations (SAs). All data to be transmitted through the Security Association is encrypted by the peers' public keys, and is decrypted by the receiving party, using the assigned private keys. IPSec Security Associations are generally set with a rekey interval, which causes a renegotiation of the key used on the Security Association. When renegotiation occurs, the peer is asked to retransmit its certificate, and the verification process repeats.

PKI and Accurate Time

When Cisco IOS Software router pairs present their certificates to each other, the validity data is one of the first parameters checked within the certificate. If the current date of the router is within the validity period of the certificate, the router goes on to check the validity of other certificate components. The router must have access to the correct time, through either manual configuration of the system clock or accurate time sources (Network Time Protocol [NTP] is recommended).

Cisco IOS Software Support for PKI

The following definitions should help in the understanding of the various keywords and their relationships with the actual components of the PKI:

- Enrollment URL—The router must contact the certificate authority in order to enroll in the PKI. Cisco IOS Software can enroll with the certificate authority using the Simple Certificate Enrollment Protocol (SCEP), which uses HTML as the application protocol. The certificate-authority documentation should offer the enrollment URL, which varies from vendor to vendor.
- Enrollment interface—By default, the router originates the enrollment request from the same interface that transmits the request. If a different interface address is included in the enrollment, the user selects the IP address or interface that is used.
- Router fully qualified domain name (FQDN)—FQDN is configured only if it varies from the host and domain name offered in the Cisco IOS Software configuration.



IPSec VPN Deployment with Digital Certificates

Smaller networks can use preshared keys to establish device identity. These keys are essentially a password configured on both sides of the connection that must match in order to set up the VPN tunnel. However, it becomes more difficult to generate and track unique cryptography information as a VPN grows. Larger-scale VPNs require a more scalable and secure infrastructure to ease deployment and management burdens. PKI responds to this requirement for scalability and security by reducing the workload necessary to manage key information; it does this by automating the distribution of cryptographic material.

To implement PKI, you must establish a certificate authority, which is either a server or external service (for example, Verisign). The certificate authority generates PKI certificates in response to “enrollment” requests for each device (for example, a Cisco IOS Software router) that is participating in the VPN.

For more information about PKI, refer to the reference list at the end of this document.

PKI Supported by Cisco SDM

Cisco® Router and Security Device Manager (SDM) allows you to generate enrollment requests and RSA keys, and manage keys and certificates. You can use Cisco SCEP to create an enrollment request and an RSA key pair and receive certificates online, create an enrollment request that you can submit to a certificate-authority server offline, or use Cisco Easy Secure Device Deployment (EZSDD) to enroll for a certificate.

Simple Certificate Enrollment Protocol

Cisco IOS Software uses SCEP to communicate with a PKI. Cisco SCEP supports the secure transportation of important information and certificates between the different components of a PKI.

You can use Cisco SCEP if there is a direct connection between your router and a certificate-authority server. You must have the enrollment URL of the server to do this.

Cut and Paste or Import from PC

If your router cannot establish a direct connection to the certificate-authority server or if you want to generate an enrollment request and send it to the certificate-authority server at another time, you should use Cut-and-Paste enrollment. Cut and Paste is a complex manual process. Cut-and-Paste style enrollment also provides an example of how other devices that may not support Cisco SCEP can be manually enrolled with a certificate-authority server.

Cisco Easy Secure Device Deployment

You can use Cisco EZSDD to enroll your router with a certificate-authority server. Cisco SDM transfers you to the Cisco EZSDD Web browser-based application to complete the enrollment process. When the process is complete, Cisco SDM displays the Certificates window, where you can view the certificates that you have obtained from the certificate-authority server.

To learn what you need to do to prepare for Cisco EZSDD enrollment, visit:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332.



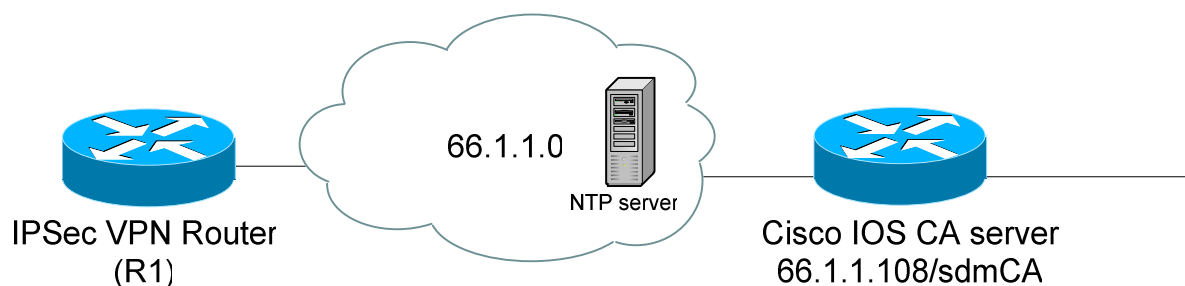
Deployment Scenarios

The following examples demonstrate how to enroll a Cisco IOS Software router (which is going to be an endpoint in an IPSec VPN tunnel) to a certificate-authority server to obtain a root and ID certificate for IPSec authentication from the certificate-authority server using Cisco SCEP and Cut and Paste.

The examples use a Cisco IOS Software router as the certificate-authority server, but many other certificate-authority server implementations are possible (Microsoft, Netscape, etc.). If you use a Cisco IOS Software router as the certificate-authority server, this router also can function as the other end of the VPN tunnel, but it does not have to (that is, you can dedicate one router as the certificate-authority server, and use the other router or routers for IPSec VPN tunnel termination).

Figure 1 illustrates the network for the sample configuration.

Figure 1. Network Diagram [EDITS: CAP S: Server]



Prerequisite Tasks

If the Cisco SDM finds that configurations need to be performed before you begin the enrollment process, it alerts you to the tasks on the message window. A link is provided next to the text so that you can go to that part of the Cisco SDM and complete the configuration. Prerequisite tasks include the following:

- Secure Shell (SSH) Protocol credential—Cisco SDM requires you to provide your SSH credentials before beginning; your system administrator should provide you with SSH credentials (username and password).
- NTP server—Your router must have accurate time for certificate enrollment to work. Identifying an NTP server from which your router can obtain accurate time provides a time source that is not affected if the router needs to be rebooted. If your organization does not have an NTP server, you can use a publicly available server, such as the server described at the following URL:
<http://www.eecis.udel.edu/~mills/ntp/clock2a.html>.
- Domain Name System (DNS) server—Specifying DNS servers helps ensure that the router can contact the certificate server. DNS configuration is required to contact the certificate-authority servers if the servers are entered as names and not as IP addresses.
- Domain or host name—It is recommended that you configure a domain and host name before beginning enrollment.



In the example, the Cisco IOS Software router is configured with host name (R1), domain name (cisco.com), and NTP server for PKI deployments. Prerequisite task configurations are not covered in this example, but they can easily be configured using Cisco SDM.

This sample configuration uses a Cisco IOS Software router as a certificate-authority server with IP address = 66.1.1.108 and Trustpoint = sdmCA. The trustpoint is effectively the name of the certificate-authority server (which may or may not be the same as the router host name in the case of a router acting as a certificate-authority server).

Configuration Steps for PKI Enrollment Using Cisco SDM

Enroll the Cisco IOS Software router to the certificate-authority server (generate and receive certificate).

At *Configure Mode*, select the *VPN*, expand *VPN Components*, expand *Public Key Infrastructure*, and then select *Certificate Wizards*.

In this case, the SSH credentials have not been verified, and the NTP has not been configured; messages are displayed on the screen (Figure 2).

Figure 2. Prerequisite and Recommended Tasks



The screenshot shows the Cisco SDM interface with the 'VPN' tab selected. The left sidebar contains a tree view of VPN components, with 'Certificate Wizards' highlighted. The main window displays the 'Certificate Wizards' configuration page. It includes a 'Select an enrollment method' section with a description of the wizard. Below this is a 'Prerequisite/Recommended tasks' section with two links: 'Enter Credentials' and 'Configure NTP/SNTP'. Three enrollment methods are listed: 'Simple Certificate Enrollment Protocol (SCEP)' (selected), 'Cut-and-Paste / Import from PC', and 'EzSDD'. A 'Launch the selected task' button is at the bottom right. The status bar at the bottom shows 'VPN' and the timestamp '22:54:51 UTC Tue Sep 28 2004'.

From the message window, click [Enter Credentials](#) to enter SSH credentials; your network administrator should provide the username and password. The message is removed when the SSH credentials are verified.

Contact your network administrator to find out the address and authentication parameters (key number and value) of the NTP time server for your network. From the message window, click [Configure NTP/SNTP](#) to configure an accurate time for certificate enrollment to work. You will be directed to the Add NTP Server Properties screen. Enter the NTP server IP address, check *Prefer*, and enter the authentication key information.

Go back to the Certificate wizard (Figure 3).

Cisco SDM supports three methods to enroll a router with a Certification Authority (as shown in Figure 3, PKI Enrollment): Cisco SCEP, Cut-and-Paste or Import PC, and Cisco EZSDD. The third option on the Certificate Wizards window is a Cisco IOS Software-exclusive mechanism to securely introduce a security router to a network infrastructure, so that the device can retrieve a “bootstrap” configuration to automate the remaining security and networking configuration tasks.



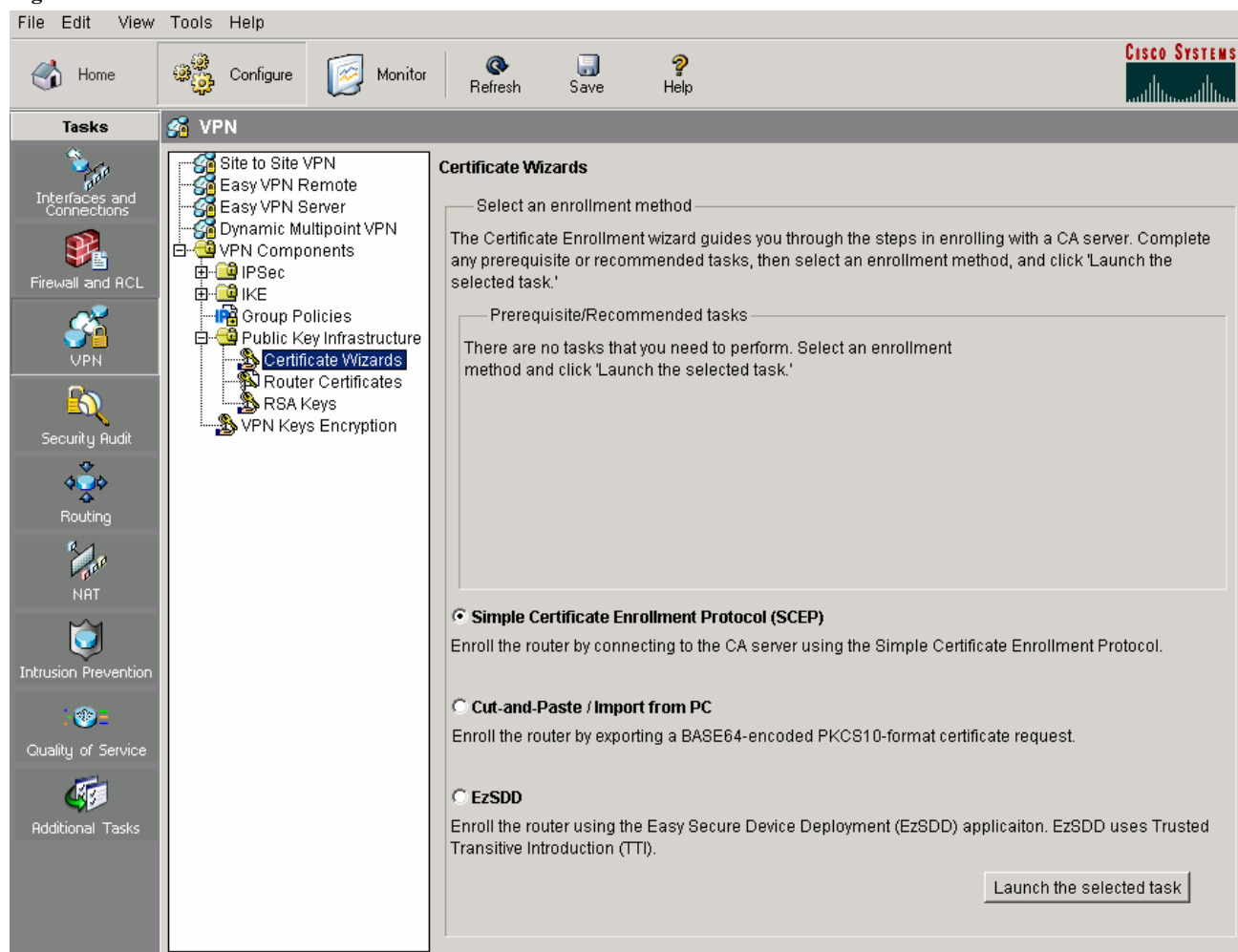
Of the two options for configuring certificate enrollment, Cisco SCEP is generally adequate. Cisco Systems developed SCEP for Cisco IOS Software in 1998, as a method to support online certificate enrollment. Because SCEP enrollment occurs online, a highly motivated and clever attacker may be able to compromise the enrollment process. However, this is very unlikely, because the attacker would need to compromise multiple communication sessions and channels to successfully attack a Cisco SCEP enrollment. In circumstances where highly secure out-of-band enrollment is required, Cut-and-Paste enrollment offers an option for enrollment where all enrollment activity may be human-carried, for example, on a floppy disk or CD, in a USB Flash memory drive, or even printed on hard copy.

Certification Generation Using Cisco SCEP

Select *Simple Certificate Enrollment Protocol (SCEP)*, and click *Launch the selected task* to launch the SCEP wizard.

This wizard guides you through the process of obtaining a certificate-authority server certificate and router certificate(s) using the Cisco SCEP. The wizard prompts you for all the information required for the enrollment request.

Figure 3. PKI Enrollment





To configure the certificate-authority server information (Figure 4), enter the following information:

1. The nickname for the CA server is *sdmCA*.
2. The enrollment URL is <http://66.1.1.108>.
3. Leave the revocation password blank (in the example, the router does not have a certificate to revoke).
4. For *Advanced Options...* in the example, skip HTTP proxy configuration².
5. Click *Next*.

Figure 4. Certificate-Authority Information

² If there is no direct Internet connection to the server, or you need to send the enrollment request through a proxy server, enter HTTP Proxy and HTTP Port by bringing up the *Advanced Options* screen.



The specified certificate subject name attributes are included in the certificate request and placed in the certificate. The information is viewable by any party to whom the router sends the certificate. It is important to note that the certificate issued to the SCEP client must have the same name attributes set, so consult your company's policy before specifying the attributes. In the example, the FQDN and the router serial number are specified.

Certificate authorities have specific guidelines on how to answer each of the attributes; these guidelines may vary by certificate authority.

To configure the certificate subject name attributes (Figure 5), do the following:

1. Check *Include your router's Fully Qualified Domain Name (FQDN)*, and use the default FQDN default: *R1.cisco.com*.
2. Check *Include router's IP address*, and select *IP address: 66.1.1.100*.
3. Check *Include router's serial number*.

Figure 5. Certificate Subject Name Attributes

SCEP Wizard

PKI Wizard

Certificate Subject Name Attributes

This information will be included in the certificate request.

☒ Include router's Fully Qualified Domain Name (FQDN)

FQDN: (e.g. foo.cisco.com)

☒ Include router's IP address

Enter a valid IP address from your router or select an interface from your router, in which case the IP address on that interface will be included in the subject name.

☒ IP address:

☐ Interface:

☒ Include router's serial number

© 2004 Cisco Systems, Inc. All rights reserved.



4. (Optional) To specify additional information to be placed in the enrollment request and the certificate, click *Other Subject Attributes...* (Figure 6).

All fields are optional, but it is recommended that you enter as much information as possible.

- Common Name: www.cisco.com (the common name of the system)
- Organization Unit: *Security Technology Group (sj-18)* (usually used to identify which host the certificate belongs to)
- Organization: *Cisco Systems Inc.*
- State: *CA*
- Country: *US*
- E-mail: *stg-sdm@cisco.com*

Figure 6. Other Subject Attributes

Other Subject Attributes

Enter the subject attributes to be included in the router's certificate. Common name (cn) is the minimum recommended entry.

Subject Name Attributes

Common Name (cn):

Organization Unit (ou):

Organization (o):

State (st):

Country (c):

Email (e):

OK Cancel Help

5. Click *Next*.



For RSA keys, in this scenario, there is no existing key pair (Figure 7); use default value, and click *Next*.

Figure 7. RSA Keys

SCEP Wizard

PKI Wizard

RSA Keys

The router uses a public key and a private key, called an RSA key pair, used to encrypt data and to sign certificates. The public key is distributed to any peer that needs to send encrypted data to the router. The private key is not distributed. Data encrypted using the public key is decrypted using the private key.

The router's digital certificate contains the public key. When the router requests a digital certificate from a Certificate Authority (CA) server, it sends its public key for inclusion in the digital certificate.

You can use an existing key pair or generate a new key pair.

☒ **Generate new key pair(s)**

The modulus determines the size of the key. Enter the modulus below.

Modulus: (Range: 512 - 2048)

By default the router generates a single key pair for both encryption and signature. Check the box below to generate one key pair for encryption and another key pair for signature.

☐ Generate separate key pairs for encryption and signing

☐ **Use existing RSA Key pair**

RSA Key pair:

< Back Next > Finish Cancel Help

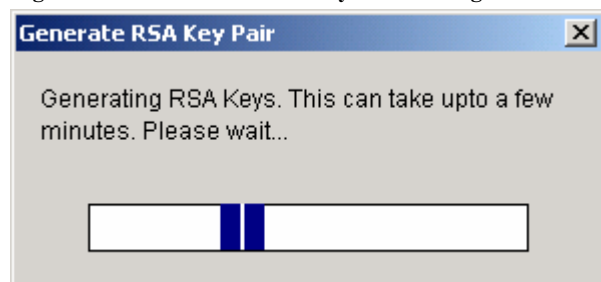
The Cisco SDM automatically detects if a firewall is applied to the interface(s) connecting the router to the certificate-authority server. If the firewall blocks communication between the certificate-authority server and the router, it also blocks the certificate issued by the certificate-authority server from reaching your router. The Cisco SDM can modify the firewall applied to the interfaces easily without breaking the enrollment task.



Check the information on the Summary window; if the information you entered is correct, click *Next*.

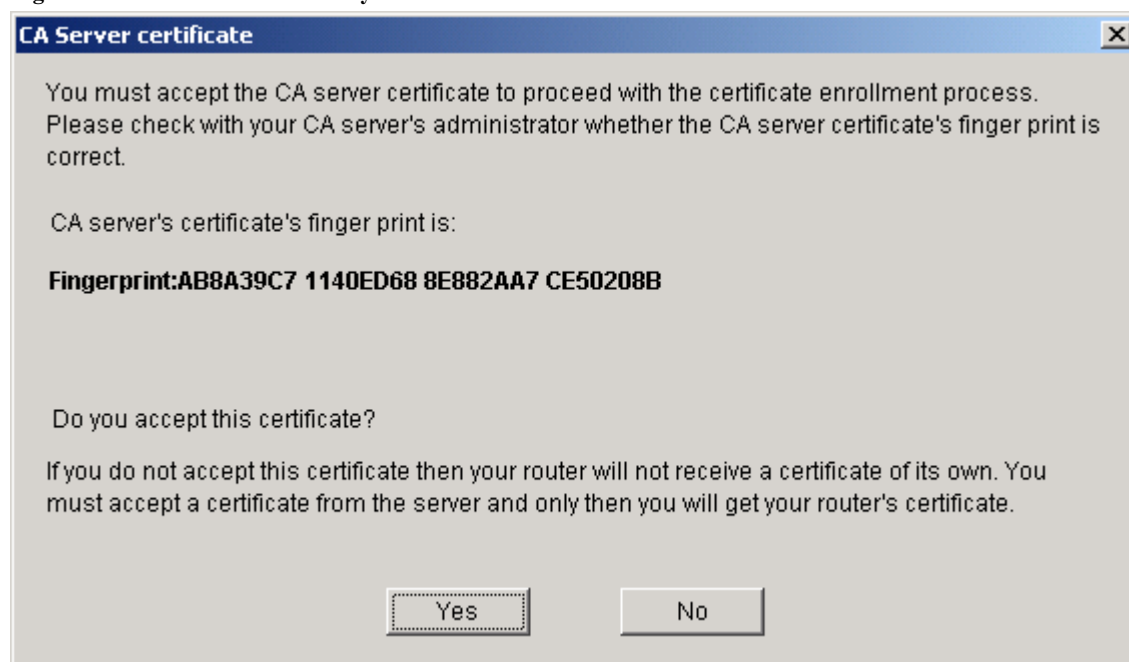
When the router finishes generating the RSA key pair (Figure 8), click *Deliver*, and then click *OK*. [CORRECT?]

Figure 8. Generate RSA Key Pair Message



When the router starts to contact the certificate-authority server, you will be prompted for accepting the certificate-authority server certificate (Figure 9); click *Yes*.

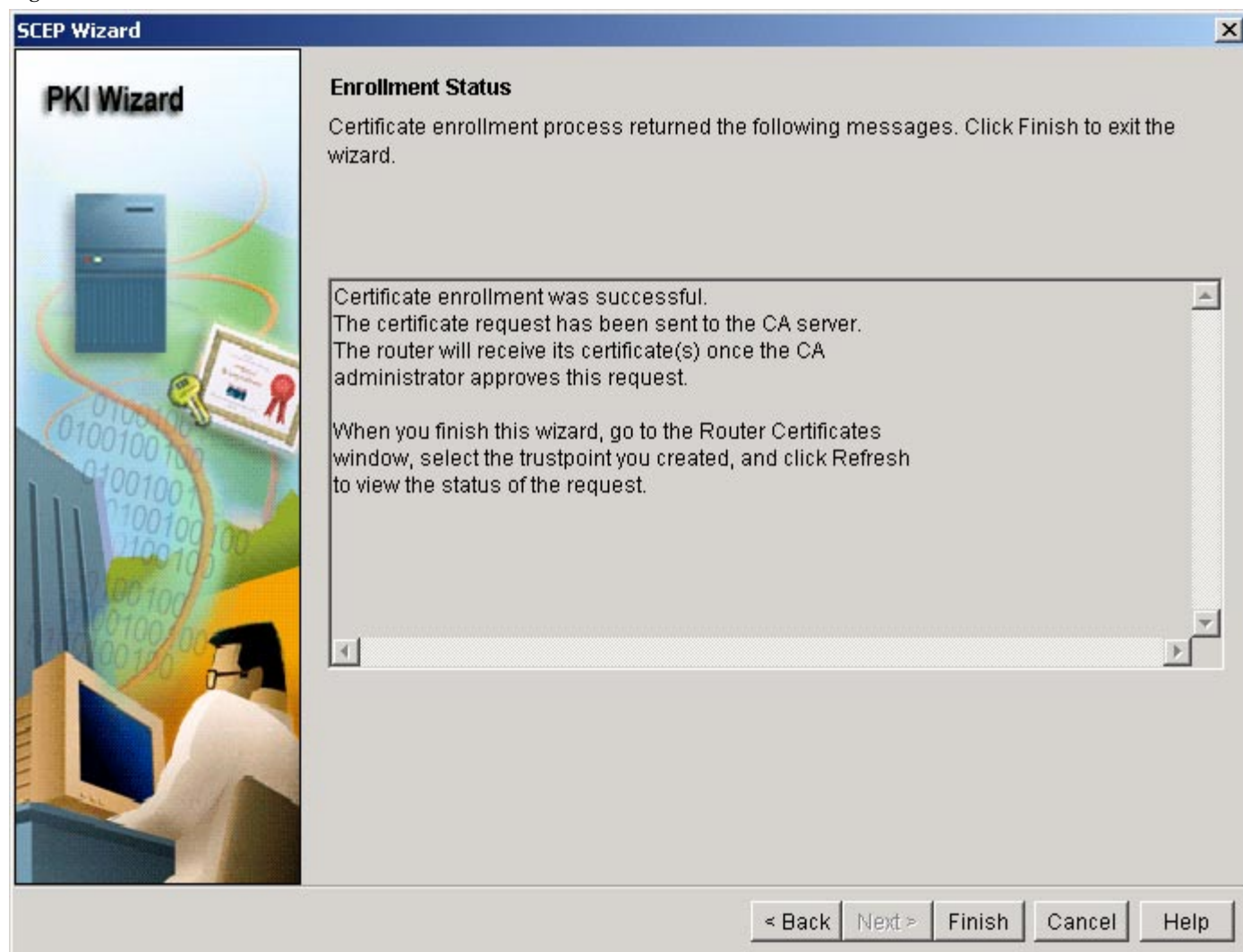
Figure 9. Certificate-Authority Server Certificate





The router then starts to enroll to the certificate-authority server again. When the certificate enrollment process is finished, the Enrollment Status message window displays; click *Finish* if no error occurs (Figure 10).

Figure 10. Enrollment Status





Verification

To check the certificates, you can go to *Configure Mode*, select *VPN*, expand *VPN Components*, expand *Public Key Infrastructure*, select *Router Certificates*, and then click *Refresh*.

You should see the Trustpoints *sdmCA* with Enrollment Type *SCEP*, and two certificates, Certificate and CA Certificate (Figure 11); in this case, the certificate-authority server certificate has serial number 01, and the certificate generated for this router has serial number 07.

Figure 11. Router Certificates

The screenshot shows the Cisco IOS configuration interface. The left sidebar contains a navigation tree with the following items: Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, Quality of Service, and Additional Tasks. The 'VPN' item is expanded, showing a sub-tree with: Site to Site VPN, Easy VPN Remote, Easy VPN Server, Dynamic Multipoint VPN, VPN Components, IPsec, IKE, Group Policies, Public Key Infrastructure, Certificate Wizards, Router Certificates (selected), RSA Keys, and VPN Keys Encryption.

The main area is titled 'Router Certificates'. It shows a list of trustpoints configured on the router. The 'sdmCA' trustpoint is selected, and its details are displayed below. The details include the Name, Enrollment URL, and Enrollment Type. Below this, there is a section for the 'Certificate Chain for trustpoint: sdmCA' which displays a table of certificates.

Name	Enrollment URL	Enrollment Type
sdmCA	http://66.1.1.108	SCEP

Type	Usage	Serial Number	Issuer	Status	Expires (Date)
Certificate	General Purpose	07	sdmCA	Available	364
CA Certificate	Signature	01	sdmCA	Available	1094



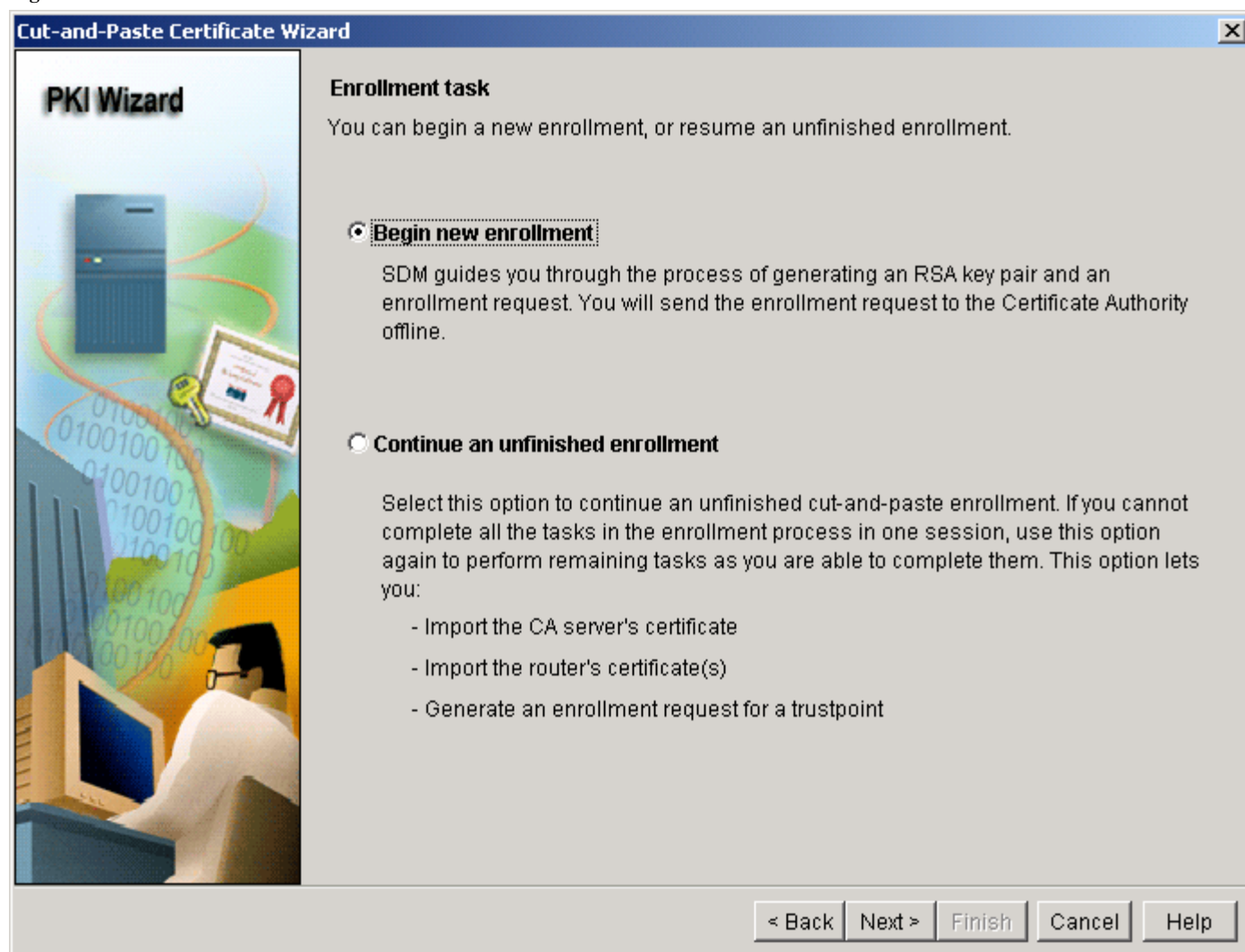
Certification Generation Using Cut and Paste or Import from PC

If you want to enroll to a certificate-authority server through Cut and Paste, you must submit the enrollment request and receive the certificates offline; you cannot complete the enrollment process in a single session. The wizard allows you to generate an RSA key pair and an enrollment request in one session, and then resume the enrollment process in another session when you have obtained the certificates.

Select *Cut Paste/Import from PC* (Figure 3), and click *Launch the selected task* to launch the wizard.

Select *Begin new enrollment* (Figure 12) to start the first session of Cut-and-Paste enrollment.

Figure 12. Cut-and-Paste Certificate Wizard





To configure the certificate-authority server information (Figure 13), enter the following:

1. The nickname for the certificate-authority server is *sdmCA*.
2. Leave the Challenge Password (in this example, the router does not have a certificate to revoke).
3. Click *Next*.

Figure 13. Certificate-Authority Server Information

The screenshot shows a window titled "Cut-and-Paste Certificate Wizard" with a close button in the top right corner. On the left side, there is a vertical banner labeled "PKI Wizard" featuring an illustration of a server, a certificate, and a person at a computer. The main area of the window is titled "Certificate Authority(CA) Information" and contains the following text: "Enter information needed to identify the certificate authority and a password to include in the enrollment request". Below this, there are two sections: "Certificate Authority Details" and "Challenge Password". In the "Certificate Authority Details" section, there is a label "* CA Server Nickname:" followed by a text box containing the value "sdmCA". The "Challenge Password" section contains a paragraph of explanatory text, followed by labels for "Challenge Password:" and "Confirm Challenge Password:", each followed by an empty text box. At the bottom left of the main area, a note states "* indicates a required field." At the bottom right, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

PKI Wizard

Certificate Authority(CA) Information

Enter information needed to identify the certificate authority and a password to include in the enrollment request

Certificate Authority Details

* CA Server Nickname:

Challenge Password

You can include a password in the enrollment request. This can be used as a challenge password or phrase required to obtain a certificate, or as a revocation password that you verbally communicate to the Certificate Authority administrator when revoking the router's certificate. Make a note of the password you enter.

Challenge Password:

Confirm Challenge Password:

* indicates a required field.

< Back Next > Finish Cancel Help



The specified certificate subject name attributes are included in the certificate request and placed in the certificate. The information is viewable by any party to whom the router sends the certificate. It is important to note that the certificate issued to the SCEP client must have the same name attributes set, so consult your company's policy before specifying the attributes. In the example, the FQDN and router serial number are specified.

Certificate authorities have specific guidelines on how to answer each of the attributes; these guidelines may vary by certificate authority.

To configure the certificate subject name attributes (Figure 5), do the following:

1. Check *Include your router's Fully Qualified Domain Name (FQDN)*, and use the default FQDN default: *R1.cisco.com*.
2. Check *Include router's IP address*, and select *IP address: 66.1.1.100*.
3. Check *Include your router's serial number in the certificate*.
4. (Optional) To specify additional information to be placed in the enrollment request and the certificate, click *Other Subject Attributes...* (Figure 6).

All fields are optional, but it is recommended that you enter as much information as possible.

- Common Name: www.cisco.com (the common name of the system)
- Organization Unit: *Security Technology Group (sj-18)* (usually used to identify which host the certificate belongs to)
- Organization: *Cisco Systems, Inc.*
- State: *CA*
- Country: *US*
- E-mail: *ste-sdm@cisco.com*

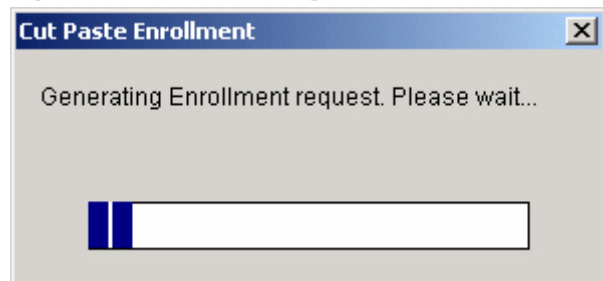
5. Click *Next*.

For RSA keys, in this scenario there is no existing key pair; use the default value, and click *Next*.

When the router finishes generating the RSA key pair, click *Deliver*.

The router then starts to generate the Cut-and-Paste enrollment request (Figure 14).

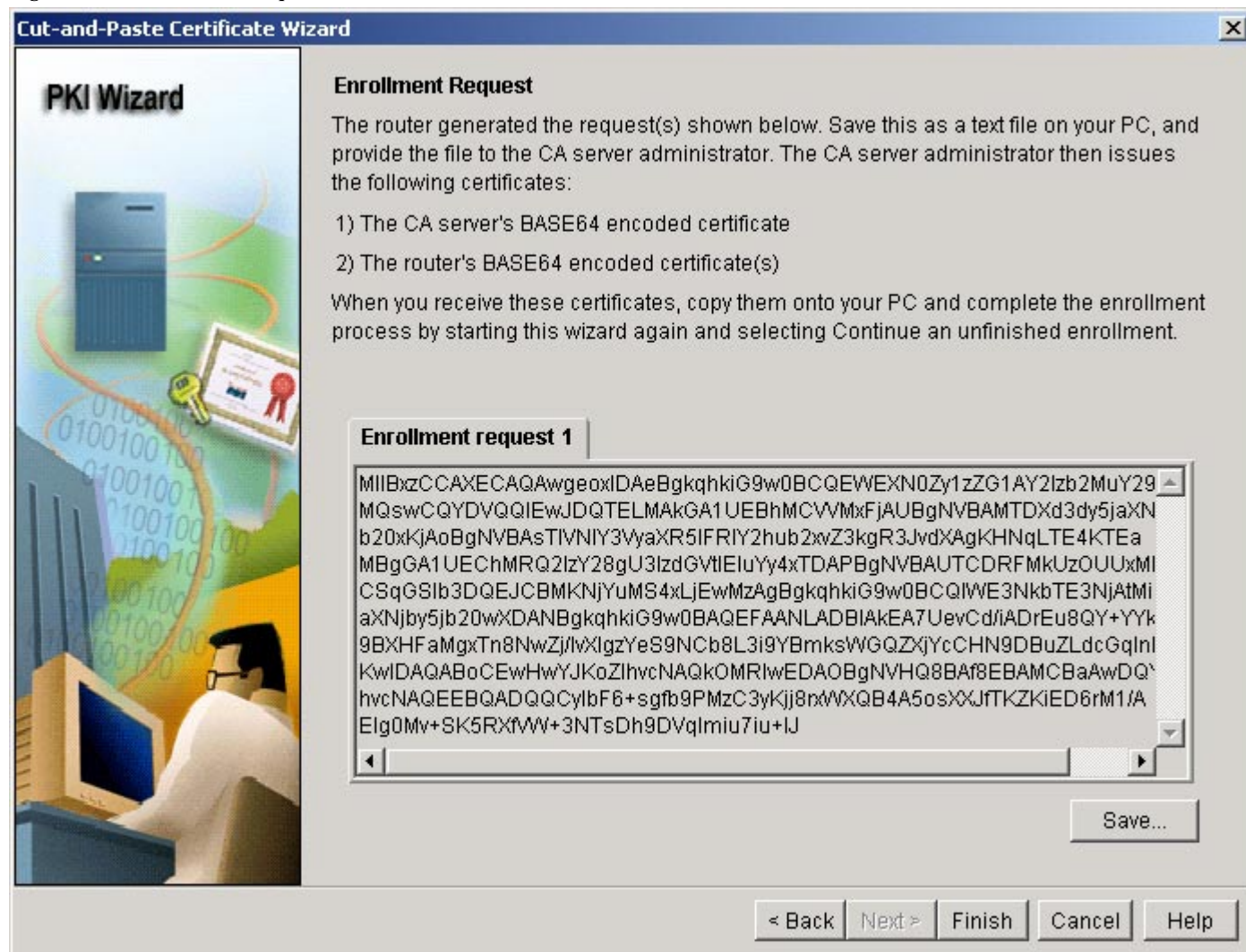
Figure 14. Enrollment Request





To save the enrollment request (Figure 15) to your local PC, click *Save*.

Figure 15. Enrollment Request



Having finished RSA key pair and enrollment request generation, now you have to obtain the certificate-authority server certificate and your router certificate manually using the saved enrollment request. The procedure is not covered in this example; consult your system administrator to find out how to obtain the certificates.

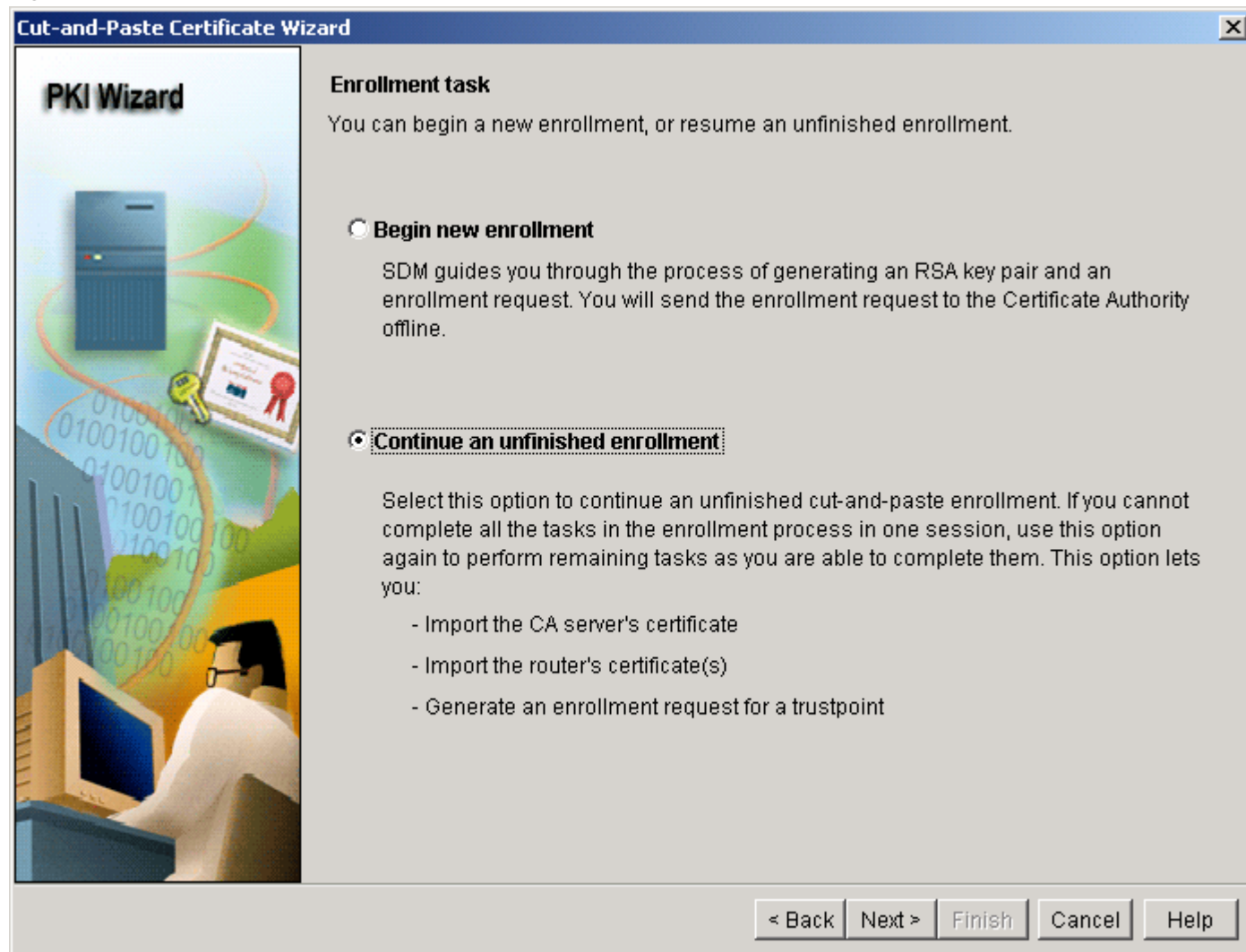


Go back to the Certificate Wizards main page, and at *Configure Mode*, select the *VPN*, expand *VPN Components*, expand *Public Key Infrastructure*, and then select *Certificate Wizards* to continue Cut-and-Paste enrollment after obtaining the certificate-authority server certificate and your router certificate.

Select *Cut and Paste/Import from PC* (Figure 3), and click *Launch the selected task* to launch the wizard.

Select *Continue an unfinished enrollment* (Figure 16) to start the second session of Cut-and-Paste enrollment.

Figure 16. Cut-and-Paste Certificate Wizard





You can cut and paste the certificate-authority certificate text into the window (Figure 17), or click *Browse...* to import the .txt from your local PC. Click *Next*.

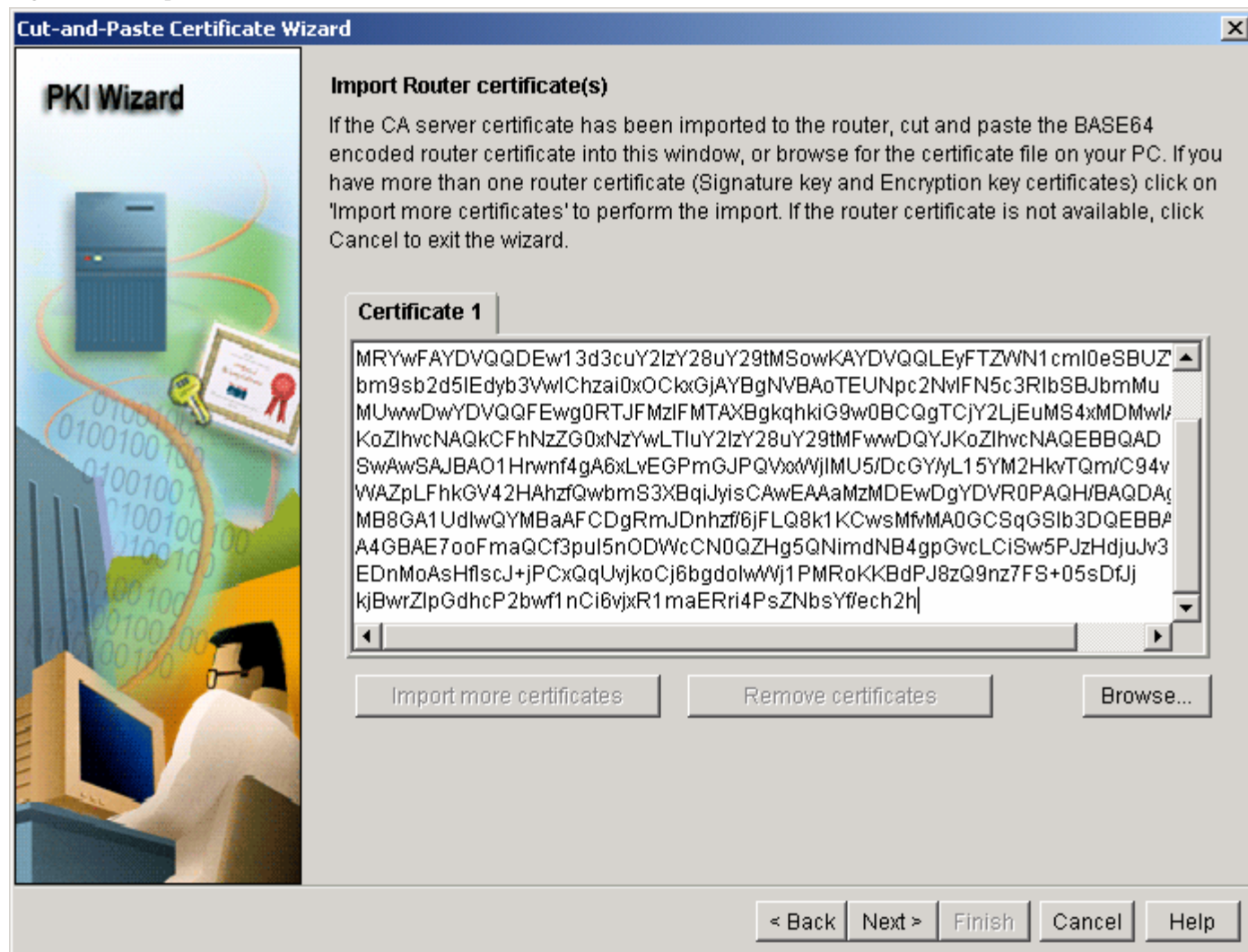
Figure 17. Import Certificate-Authority Certificate





You can cut and paste the router certificate text into the window (Figure 18), or click *Browse...* to import the .txt from your local PC. Click *Next*.

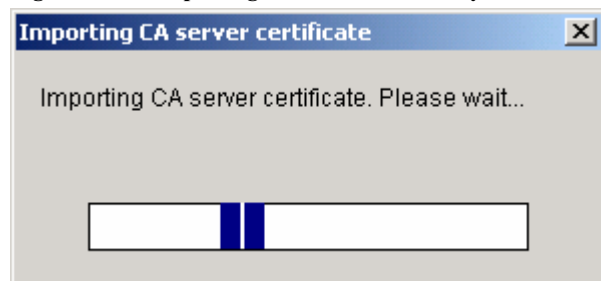
Figure 18. Import Router Certificate(s)



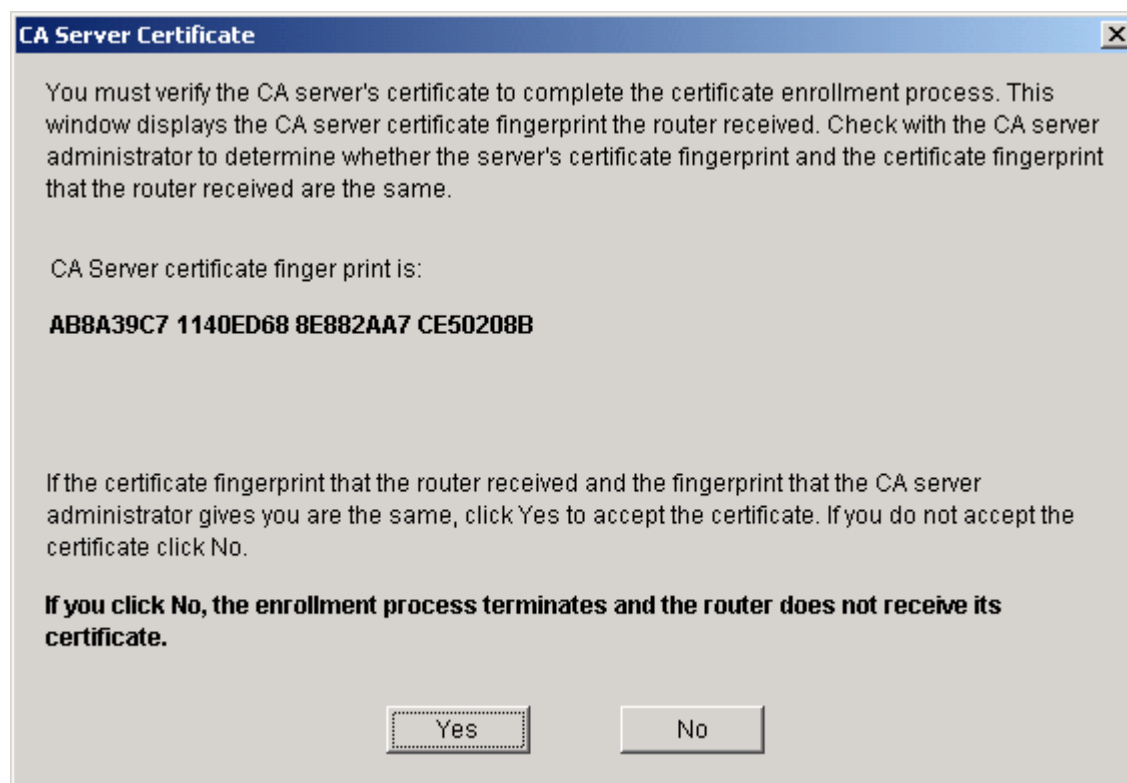


The router then starts to import the certificate-authority server certificate (Figure 19).

Figure 19. Importing Certificate-Authority Server Certificate



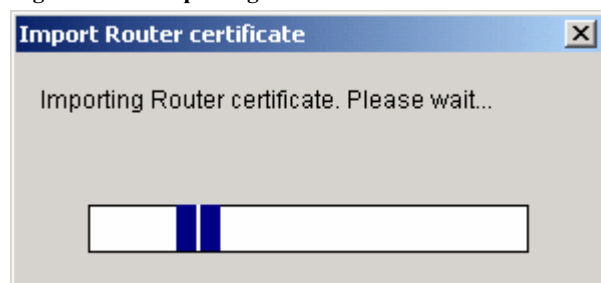
Click *Yes* upon verification of the certificate-authority server certificate to complete the certificate enrollment process.



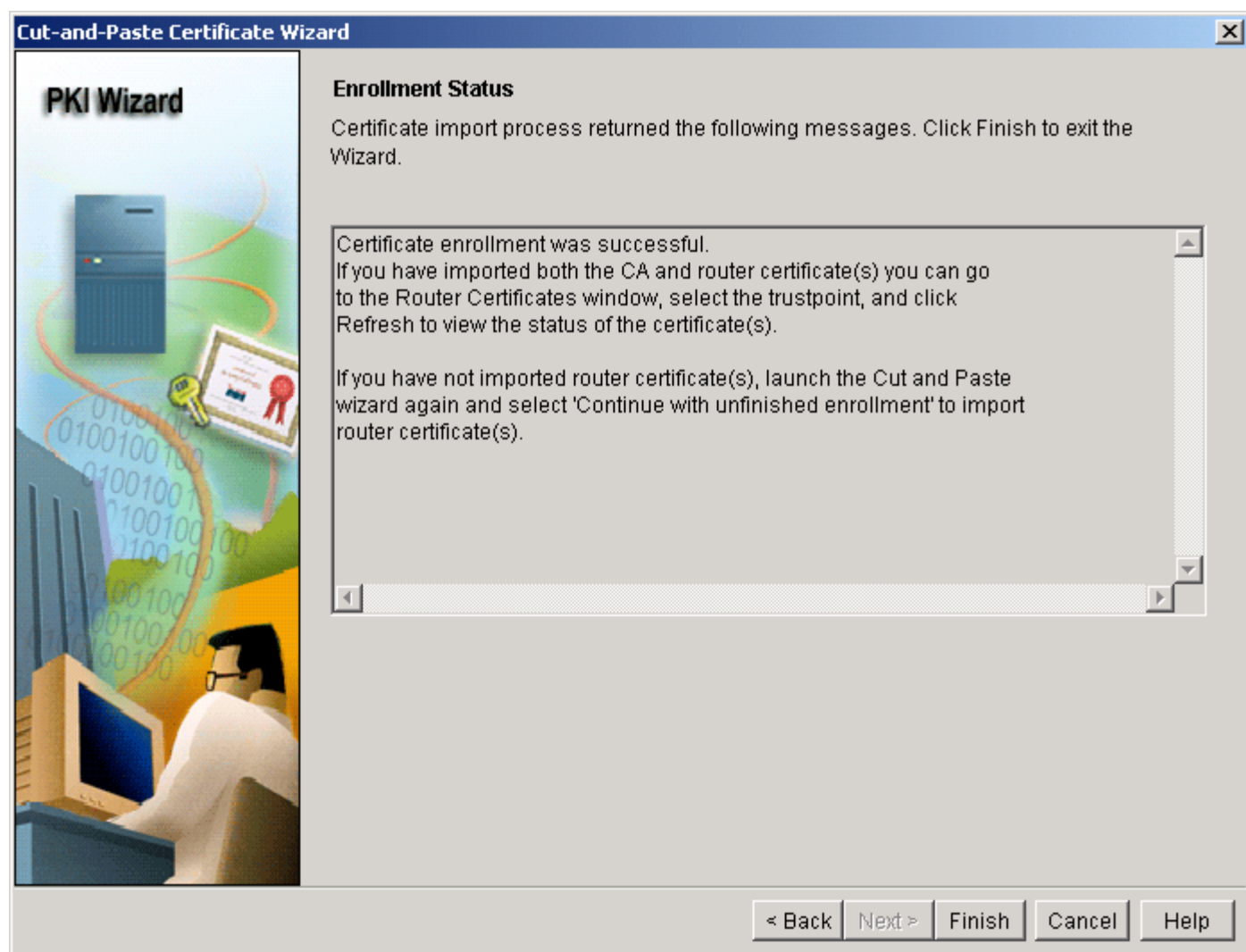


The router then starts to import the certificate-authority server certificate (Figure 20).

Figure 20. Importing Router Certificate



Click *Finish* to exit the wizard when the certificate import process is finished.





Verification

To check the certificate, you can go to *Configure Mode*, select *VPN*, expand *VPN Components*, expand *Public Key Infrastructure*, select *Router Certificates*, and then click *Refresh*.

You should see the Trustpoints *sdmCA* with Enrollment Type *Cut & Paste*, and two certificates, Certificate and CA Certificate (Figure 21); in this case, the certificate-authority server certificate has serial number 01, and the certificate generated for this router has serial number 0C.

Figure 21. Router Certificates

The screenshot shows the Cisco IOS configuration interface for VPN. The left sidebar contains a tree view with the following items: Site to Site VPN, Easy VPN Remote, Easy VPN Server, Dynamic Multipoint VPN, VPN Components (expanded), IPsec, IKE, Group Policies, Public Key Infrastructure (expanded), Certificate Wizards, Router Certificates (selected), RSA Keys, and VPN Keys Encryption. The main content area is titled "Router Certificates" and displays the configuration for the trustpoint "sdmCA".

Trustpoints

Trustpoints configured on your router

Name	Enrollment URL	Enrollment Type
sdmCA	terminal	Cut & Paste

Certificate Chain for trustpoint:sdmCA

Type	Usage	Serial Number	Issuer	Status	Expires (Date)
Certificate	General Purpose	0C	cn=sdmCA,	Available	364
CA Certificate	Signature	01	cn=sdmCA,	Available	1018



Cisco IOS Software Command-Line Interface

If you want to use the command-line interface (CLI) to configure PKI instead of the Cisco SDM, use the following CLI steps show you how to use SCEP to enroll a CA server.

Configure and enroll the cryptographic router (R1) to the certificate server.
Do the following:

1. Generate the RSA keys on R1:

```
R1(config)#crypto key generate rsa
```

- The name for the keys is *R1.cisco.com*.
- Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. Choosing a key modulus greater than 512 may take a few minutes.
- How many nits in the modules [WHY BRACKETS HERE?] [512]: [NOTE: THIS AREA OF TEXT IS VERY CONFUSING; IT DOES NOT HAVE THE SAME FORMAT OR TONE AS BEFORE; IT APPEARS THAT IT WAS ADDED AS AN AFTERTHOUGHT, MAYBE LIFTED FROM ANOTHER DOC; NOT SURE WHAT THE PERCENT SIGNS MEAN; ARE THEY BULLETS? PLS CLARIFY; I HAVE TRIED TO FIGURE OUT WHAT YOU WANT TO SAY, BUT MAY BE WRONG; PLS CHECK THIS SECTION CAREFULLY]

```
% Generating 512 bit RSA keys ...[OK] [IS THIS WHAT USER SEES? SHOULD IT ALSO BE A BULLET?]
```

2. To declare to the certificate authority that your router should use (Cisco IOS Software certificate authority in this example) and specify characteristics for the trustpoint certificate authority, use the following commands beginning in global configuration mode:

```
R1(config)#crypto ca trustpoint sdmCA
R1(ca-trustpoint)#enrollment url http://66.1.1.108
R1(ca-trustpoint)#password
R1(ca-trustpoint)#rsakeypair R1.cisco.com
R1(ca-trustpoint)#auto-enroll
```

3. To retrieve the root certificate from the certificate-authority server:

```
R1(config)#crypto ca authenticate sdmCA
```



- The certificate has the following attributes:
 - Fingerprint: AB8A39C7 1140ED68 8E882AA7 CE50208B

% Do you accept this certificate? [yes/no]:yes [IS THIS WHAT THE USER SEES? SHOULD IT BE A BULLET?]

The trustpoint certificate-authority certificate is accepted if [WHAT?].

4. To enroll and generate [WHAT?], use the following command:

R1(config)#crypto ca enroll sdmCA

- Start certificate enrollment.
- Create a challenge password. You will need to verbally provide this password to the certificate-authority administrator in order to revoke your certificate.
- For security reasons your password will not be saved in the configuration, so you should make a note of it.

[NOT SURE WHAT THOSE TWO ITEMS ARE]

Password:

Reenter password:

- The FQDN in the certificate is *R1.cisco.com*.
- The subject name in the certificate is *R1.cisco.com*.
- Include the router serial number in the subject name? [yes/no]: *yes* [NOT SURE HERE]
- The serial number in the certificate is *0F1BE72E*.
- Include an IP address in the subject name? [no]: *no* [NOT SURE HERE]
- Request certificate from CA? [yes/no]: *yes* [NOT SURE HERE]

The certificate request is then sent to the certificate authority, and the certificate request fingerprint is displayed. The **show crypto pki certificate** command also shows the fingerprint.

.....

R1#show crypto pki certificate

[I AM NOT SURE HOW TO FORMAT THE FOLLOWING; PLS MAKE IT LOOK LIKE THE STYLE OF THE REST OF THE DOC]

Certificate

Status: Available

Certificate Serial Number: 06



Certificate Usage: General Purpose

Issuer:

cn=sdmCA

Subject:

Name: R1.cisco.com

IP Address: 66.1.1.100

Serial Number: 0F1BE72E

serialNumber=F1BE72E+ipaddress=66.1.1.100+hostname=R1.cisco.com

o=Cisco Systems, Inc.

ou=Security Technology Group (sj-18)

cn=www.cisco.com

c=US

st=CA

ea=ste-sdm@cisco.com

Validity Date:

start date: 13:41:19 PCTime Aug 20 2004

end date: 13:41:19 PCTime Aug 20 2005

Associated Trustpoints: sdmCA

Certificate-Authority Certificate

Status: Available

Certificate Serial Number: 01

Certificate Usage: Signature

Issuer:

cn=sdmCA

Subject:

cn=sdmCA

Validity Date:

start date: 10:44:09 PCTime Aug 20 2004

end date: 10:44:09 PCTime Aug 20 2007

Associated Trustpoints: sdmCA



The enrollment procedure requires the knowledge of PKI infrastructure: the public-private key pair (or RSA key pair), a certificate revocation list (CRL), the root certificate, and the Cisco IOS CLI.

In summary, by using the Cisco SDM PKI wizards, you can conduct the same complex PKI enrollment easily and quickly with minimum knowledge of Cisco IOS Software commands and PKI knowledge.



References

- Certificate server data sheet:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/certs_ds.pdf

- Cisco IOS Software certificate server:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_ioscs.pdf



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)