CHAPTER 17

Public Key Infrastructure

The Public Key Infrastructure (PKI) windows enable you to generate enrollment requests and RSA keys, and manage keys and certificates. You can use the Simple Certificate Enrollment Process (SCEP) to create an enrollment request and an RSA key pair and receive certificates online, or create an enrollment request that you can submit to a Certificate Authority (CA) server offline.

If you want to use Secure Device Provisioning (SDP) to enroll for certificates, see Secure Device Provisioning.

Certificate Wizards

This window allows you to select the type of enrollment you are performing. It also alerts you to configuration tasks that you must perform before beginning enrollment, or tasks that Cisco recommends you perform before enrolling. Completing these tasks before beginning the enrollment process helps eliminate problems that may occur.

Select the enrollment method Cisco SDM uses to generate the enrollment request.

Prerequisite Tasks

If Cisco SDM finds that there are configuration tasks that should be performed before you begin the enrollment process, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco SDM and complete the configuration. If Cisco SDM does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Simple Certificate Enrollment Protocol (SCEP)

Click this button if you can establish a direct connection between your router and a Certificate Authority (CA) server. You must have the server's enrollment URL in order to do this. The wizard will do the following:

- Gather information from you to configure a trustpoint and deliver it to the router.
- Initiate an enrollment with the CA server you specified in the trustpoint.
- If the CA server is available, display the CA server's fingerprint for your acceptance.
- If you accept the CA server fingerprint , complete the enrollment.

Cut and Paste/Import from PC

Click this button if your router cannot establish a direct connection to the CA server or if you want to generate an enrollment request and send it to the CA at another time. After generation, the enrollment request can be submitted to a CA at another time. Cut-and-Paste enrollment requires you to invoke the Digital Certificates wizard to generate a request, and then to reinvoke it when you have obtained the certificates for the CA server and for the router.

Note Cisco SDM supports only base-64-encoded PKCS#10-type cut and paste enrollment. Cisco SDM does not support importing PEM and PKCS#12 type certificate enrollments.

Launch the selected task button

Click to begin the wizard for the type of enrollment that you selected. If Cisco SDM has detected a required task that must be performed before enrollment can begin, this button is disabled. Once the task is completed, the button is enabled.

Welcome to the SCEP Wizard

This screen indicates that you are using the SCEP wizard. If you do not want to use the Simple Certificate Enrollment Process, click **Cancel** to leave this wizard.

After the wizard completes and the commands are delivered to the router, Cisco SDM attempts to contact the CA server. If the CA server is contacted, Cisco SDM displays a message window with the server's digital certificate.

Certificate Authority (CA) Information

Provide information to identify the CA server in this window. Also specify a challenge password that will be sent along with the request.

Note The information you enter in this screen is used to generate a trustpoint. The trustpoint is generated with a default revocation check method of CRL. If you are editing an existing trustpoint with the SCEP wizard, and a revocation method different from CRL, such as OCSP, already exists under the trustpoint, Cisco SDM will not modify it. If you need to change the revocation method, go to Router Certificates window, select the trustpoint you configured, and click the **Check Revocation** button.

CA server nickname

The CA server nickname is an identifier for the trustpoint you are configuring. Enter a name that will help you identify one trustpoint from another.

Enrollment URL

If you are completing an SCEP enrollment, you must enter the enrollment URL for the CA server in this field. For example,

```
http://CAuthority/enrollment
```

The URL must begin with the characters http://. Be sure there is connectivity between the router and the CA server before beginning the enrollment process.

This field does not appear if you are completing a cut-and-paste enrollment.

Challenge Password and Confirm Challenge Password

A challenge Password can be sent to the CA for you to use if you ever need to revoke the certificate. It is recommended that you do so, as some CA servers do not issue certificates if the challenge Password is blank. If you want to use a challenge Password, enter that password and then reenter it in the confirm field. The challenge Password will be sent along with the enrollment request. For security purposes, the challenge password is encrypted in the router configuration file, so you should record the password and save it in a location you will remember.

This password is also referred to as a challenge password.

Advanced Options Button

Advanced options allow you to provide more information to enable the router to contact the CA server.

Advanced Options

Use this window to provide more information to enable the router to contact the CA server.

HTTP Proxy and HTTP Port

If the enrollment request will be sent through a proxy server, enter the proxy server IP address, and the port number to use for proxy requests in these fields.

Certificate Subject Name Attributes

Specify the optional information that you want to be included in the certificate. Any information that you specify be included in the certificate request will be placed in the certificate, and be viewable by any party to whom the router sends the certificate.

Include router's fully qualified Domain Name (FQDN) in the certificate.

It is recommended that the router's fully qualified domain name be included in the certificate. Check this box if you want Cisco SDM to include the router's fully qualified domain name in the certificate request.

Note If the Cisco IOS image running on the router does not support this feature, this box is disabled.

FQDN

If you enabled this field, enter the routers FQDN in this field. An example of an FQDN is

```
sjrtr.mycompany.net
```

Include router's IP Address

Check if you want to include a valid IP address configured on your router in the certificate request. If you check this box, you can manually enter an IP address, or you can select the interface whose IP address you want to be used.

IP Address

Click if you want to enter an IP address, and enter an IP address configured on the router in the field that appears. Enter an IP address that has been configured on the router or an address that has been assigned to the router.

Interface

Select a router interface whose IP address you want to be included in the certificate request.

Include router's serial number

Check this box if you want the serial number of the router included in the certificate.

Other Subject Attributes

The information you enter in this window will be placed in the enrollment request. CAs use the X.500 standard to store and maintain information for digital certificates. All fields are optional, but it is recommended that you enter as much information as possible.

Common Name (cn)

Enter the common name to be included in this certificate. This would be the name used to search for the certificate in the X.500 directory.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, Development, or Engineering might be organizational units

Organization (o)

Enter the organization or company name. This is the X.500 organizational name.

State (st)

Enter the state or province in which the router or the organization is located.

Country (c)

Enter the country in which the router or the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Note If the Cisco IOS image running on the router does not support this attribute, this field is disabled.

RSA Keys

You must include an RSA public key in the enrollment request. Once the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data sent to the router. The private key is kept on the router and used to decrypt the data sent by peers, and also used to digitally sign transactions when negotiating with peers.

Generate new key pair(s)

Click this button if you want to generate a new key to use in the certificate. When you generate a key pair, you must specify the modulus to determine the size of the key. This new key appears in the RSA Keys window when the wizard is completed.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Generate separate key pairs for encryption and signature

By default, Cisco SDM creates a general purpose key pair that is used for both encryption and signature. If you want Cisco SDM to generate separate key pairs for encrypting and signing documents, check this box. Cisco SDM will generate usage keys for encryption and signature.

Use existing RSA key pair

Click this button if you want to use an existing key pair, and select the key from the drop-down list.

Save to USB Token

Check the **Save keys and certificates to secure USB token** checkbox if you want to save the RSA keys and certificates to a USB token connected to your router. This checkbox appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

Summary

This window summarizes the information that you provided. The information that you provided is used to configure a trustpoint on the router and begin the enrollment process. If you enabled **Preview commands before delivering to router** in the Preferences dialog, you will be able to preview the CLI that is delivered to the router.

If you are performing an SCEP enrollment

After the commands are delivered to the router, Cisco SDM attempts to contact the CA server. If the CA server is contacted, Cisco SDM displays a message window with the server's digital certificate.

If you are performing a cut-and-paste enrollment

After the commands are delivered to the router, Cisco SDM generates an enrollment request and displays it in another window. You must save this enrollment request and present it to the CA server administrator in order to obtain the CA server's certificate, and the certificate for the router. The enrollment request is in Base64 encoded PKCS#10 format.

After you obtain the certificates from the CA server, you must restart the Cut and Paste wizard, and select **Continue an unfinished enrollment** to import the certificates to your router.

Cisco SDMCisco SDMEnrollment Status

This window informs you of the status of the enrollment process. If errors are encountered during the process, Cisco SDM displays the information it has about the error.

When status has been reported, click **Finish**.

Cut and Paste Wizard Welcome

The Cut and Paste wizard lets you generate an enrollment request and save it to your PC so that you can send it to the Certificate Authority offline. Because you cannot complete the enrollment in a single session, this wizard completes when you generate the trustpoint and the enrollment request and save it to your PC.

After you have submitted the enrollment request to the CA server manually, and received the CA server certificate and the certificate for your router, you must start the Cut and Paste wizard again to complete the enrollment and import the certificates to the router.

Enrollment Task

Specify whether you are beginning a new enrollment or you are resuming an enrollment with an enrollment request that you saved to the PC.

Begin New Enrollment

Click **Begin new enrollment** to generate a trustpoint, an RSA key pair and an enrollment request that you can save to your PC and send to the CA server. The wizard completes after you save the enrollment request. To complete the enrollment after you have receive the CA server certificate and the certificate for your router, re-enter the Cut and Paste wizard and select **Continue with an unfinished enrollment**.

Continue with an unfinished enrollment

Click this button to resume an enrollment process. You can import certificates you have received from the CA server, and you can generate a new enrollment request for a trustpoint if you need to.

Enrollment Request

This window displays the base-64-encoded PKCS#10-type enrollment request that the router has generated. Save the enrollment request to the PC. Then, send it to the CA to obtain your certificate.

Save:

Browse for the directory on the PC that you want to save the enrollment request text file in, enter a name for the file, and click **Save**.

Continue with Unfinished Enrollment

If you are continuing with an unfinished enrollment you need to select the trustpoint associated with the unfinished enrollment, and then specify the part of the enrollment process you need to complete. If you are importing a CA server certificate or a router certificate, the certificate must be available on your PC.

Select CA server nickname (trustpoint)

Select the trustpoint associated with the enrollment you are completing.

Import CA and router certificate(s)

Choose this option if you want to import both the CA server's certificate and the router's certificate in the same session. Both certificates must be available on the PC.

This option is disabled if the CA certificate has already been imported.

Import CA certificate

Choose this option to import a CA server certificate that you have saved on your PC. After you import the certificate, Cisco SDM will display the certificate's digital fingerprint. You can then verify the certificate and accept or reject it.

This option is disabled if the CA certificate has already been imported.

Import router certificate(s)

Choose this option to import a certificate for your router saved on your PC. After you import the router certificate, Cisco SDM will report on the status of the enrollment process.

Note You must import the CA server's certificate before you import the router's certificate.

Generate enrollment request

Choose this option if you need to generate an enrollment request for the selected trustpoint. The router will generate an enrollment request that you can save to the PC and send to the CA.

Cisco SDM generates a base-64 encoded PKCS#10 enrollment request.

Import CA certificate

If you have the CA server certificate on your hard disk, you can browse for it and import it to your router in this window. You can also copy and paste the certificate text into the text area of this window.

Browse Button

Click to locate the certificate file on the PC.

Import Router Certificate(s)

If you have one or more certificates for your router granted by the CA on your hard disk, you can browse for it and import it to your router.

Import more certificates

If you generated separate RSA key pairs for encryption and signature, you receive two certificates for the router. Use this button when you have more than one router certificate to import.

Remove certificate

Click the tab for the certificate you need to remove and click **Remove** certificate.

Browse

Browse to locate the certificate and import it to the router.

Digital Certificates

This window allows you to view information about the digital certificates configured on the router.

Trustpoints

This area displays summary information for the trustpoints configured on the router and allows you to view details about the trustpoints, edit trustpoints, and determine if a trustpoint has been revoked.

Details Button

The Trustpoints list only displays the name, enrollment URL, and enrollment type for a trustpoint. Click to view all the information for the selected trustpoint.

Edit Button

A trustpoint can be edited if it is an SCEP trustpoint, and if the CA server's certificate and the router's certificate have not both been successfully imported. If the trustpoint is not an SCEP trustpoint, or if both the CA server and router certificate associated with an SCEP trustpoint have been delivered, this button is disabled.

Delete Button

Click to delete the selected trustpoint. Deleting a trustpoint destroys all certificates received from the associated certificate authority.

Check Revocation Button

Click to check whether the selected certificate has been revoked. Cisco SDM displays a dialog in which you select the method to use to check for revocation. See Revocation Check and Revocation Check, CRL Only for more information.

Name	Trustpoint name.

CA Server	The name or IP address of the CA server.
Enrollment Type	One of the following: • SCEP—Simple Certificate Enrollment Protocol. The enrollment v accomplished by connecting directly to the CA server • Cut and Paste—Enrollment request was imported from PC. • TFTP—Enrollment request was made using a TFTP server.

Certificate chain for trustpoint *name*

This area shows details about the certificates associated with the selected trustpoint.

Details Button

Click to view the selected certificate.

Refresh Button

Click to refresh the Certificate chain area when you select a different trustpoint in the Trustpoints list.

Type	One of the following: • RA KeyEncipher Certificate—Rivest Adelman encryption certific • RA Signature Certificate—Rivest Adelman signature certificate. • CA Certificate—The certificate of the CA organization. • Certificate—The certificate of the router.
Usage	One of the following: • General Purpose—A general purpose certificate that the router us authenticate itself to remote peers. • Signature—CA certificates are signature certificates.
Serial Number	The serial number of the certificate
Issuer	The name of the CA that issued the certificate.

Status	One of the following: • Available—The certificate is available for use. • Pending—The certificate has bee applied for, but is not available
Expires (Days)	The number of days the certificate can be used before it expires.
Expiry Date	The date on which the certificate expires.

Trustpoint Information

The Trustpoints list in the Router Certificates window displays the key information about each trustpoint on the router. This window displays all the information provided to create the trustpoint.

Certificate Details

This window displays trustpoint details that are not displayed in the Certificates window.

Revocation Check

Specify how the router is to check whether a certificate has been revoked in this window.

Revocation Check

Configure how the router is to check for revocations, and order them by preference. The router can use multiple methods.

Use/Method/Move Up/Move Down

Check the methods that you want to use, and use the **Move Up** and **Move Down** buttons to place the methods in the order you want to use them.

- OCSP—Contact an Online Certificate Status Protocol server to determine the status of a certificate.
- CRL—Certificate revocation is checked using a certificate revocation list.

- None—Do not perform a revocation check.

CRL Query URL

Enabled when CRL is selected. Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

OCSP URL

Enabled when OCSP is selected. Enter the URL of the OCSP server that you want to contact.

Revocation Check, CRL Only

Specify how the router is to check whether a certificate has been revoked in this window.

Verification

One of the following:

- None—Check the Certificate Revocation List (CRL) distribution point embedded in the certificate.
- Best Effort—Download the CRL from the CRL server if it is available. If it is not available, the certificate will be accepted.
- Optional—Check the CRL only if it has already been downloaded to the cache as a result of manual loading.

CRL Query URL

Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

RSA Keys Window

RSA keys provide an electronic encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adelman. The RSA system is the most commonly used encryption and authentication algorithm, and is included as a part of Cisco IOS. To use the RSA system, a network host generates a pair of keys. One is called the *public key*, and the other is called the *private key*. The Public key is given to anyone who wants to send encrypted data to the host. The Private key is never shared. When a remote hosts wants to send data, it encrypts it with the public key shared by the local host. The local host decrypts sent data using the private key.

RSA keys configured on your router

Name	The key name. Key names are automatically assigned by Cisco SDM. The "HTTPS_SS_CERT_KEYPAIR" and "HTTPS_SS_CERT_KEYPAIR.serve shown as Read-Only. Similarly, any key that is locked/encrypted on the rou displayed with icons that indicate their status.
Usage	Either General Purpose or Usage. General purpose keys are used to encrypt sign the certificate. If separate keys are configured to encrypt data and to s certificates, these keys are labelled Usage keys.
Exportable	If this column contains a checkmark the key can be exported to another rou becomes necessary for that router to assume the role of the local router.

Key Data

Click to view a selected RSA key.

Save Key to PC Button

Click to save the data of the selected key to your PC.

Generate RSA Key Pair

Use this window to generate a new RSA key pair.

Label

Enter the label of the key in this field.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The larger the modulus size, the more secure the key is. However keys with larger modulus sizes take longer to generate and longer to process when exchanged.

Type

Select the type of key to generate, **General Purpose**, or **Usage**. General purpose keys are used for both encryption and signing of certificates. If you generate Usage keys, one set of keys will be used for encryption, and a separate set will be used for certificate signing.

Key is exportable checkbox

Check if you want the key to be exportable. An exportable key pair can be sent to a remote router if it is necessary for that router to take over the functions of the local router.

Save to USB Token

Check the **Save keys to secure USB token** checkbox if you want to save the RSA keys to a USB token connected to your router. This checkbox appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

USB Token Credentials

This window appears when you add or delete credentials, such as an RSA key pair or digital certificates, that have been saved on a USB token. For the deletion to take place, you must provide the USB token name and PIN.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

USB Tokens

This window allows you to configure USB token logins. This window also displays a list of configured USB token logins. When a USB token is connected to your Cisco router, Cisco SDM uses the matching login to log in to the token.

Add

Click **Add** to add a new USB token login.

Edit

Click **Edit** to edit an existing USB token login. Specifiy the login to edit by choosing it in the list.

Delete

Click **Delete** to delete an existing USB token login. Specifiy the login to delete by choosing it in the list.

Token Name

Displays the name used to log in to the USB token.

User PIN

Displays the PIN used to log in to the USB token.

Maximum PIN Retries

Displays the maximum number of times Cisco SDM will attempt to log in to the USB token with the given PIN. If Cisco SDM is unsuccessful after trying for the number specified, it will stop trying to log in to the USB token.

Removal Timeout

Displays the maximum number of seconds that Cisco SDM will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router.

If Removal Timeout is empty, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Displays the configuration file that Cisco SDM attempts to find on the USB token. The configuration file can be a CCCD file or a .cfg file.

CCCD refers to a boot configuration file. On USB tokens, a CCCD file is loaded using TMS software.

Add or Edit USB Token

This window allows you to add or edit USB token logins.

Token Name

If you are adding a USB token login, enter the USB token name. The name you enter must match the name of the token that you want to log in to.

A token name is set by the manufacturer. For example, USB tokens manufactured by Aladdin Knowledge Systems are named eToken.

You can also use the name "usbtoken*x*", where *x* is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

If you are editing a USB token login, the Token Name field cannot be changed.

Current PIN

If you are adding a USB token login, or if you are editing a USB token login that has no PIN, the Current PIN field displays <None>. If you are editing a USB token login which has a PIN, the Current PIN field displays ******.

Enter New PIN

Enter a new PIN for the USB token. The new PIN must be at least 4 digits long and must match the name of the token you want to log in to. If you are editing a USB token login, the current PIN will be replaced by the new PIN.

Reenter New PIN

Reenter the new PIN to confirm it.

Maximum PIN Retries

Choose the maximum number of times Cisco SDM will attempt to log in to the USB token with the given PIN. If Cisco SDM is unsuccessful after trying for the number specified, it will stop trying to log in to the USB token.

Removal Timeout

Enter the maximum number of seconds that Cisco SDM will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router. The number of seconds must be in the range 0 to 480.

If you do not enter a number, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Specify a configuration file that exists on the USB token. The file can be a partial or complete configuration file. The file extension must .cfg.

If Cisco SDM can log in to the USB token, it will merge the specified configuration file with the router's running configuration.

Open Firewall

This screen is displayed when Cisco SDM detects firewall(s) on interfaces that would block return traffic that the router needs to receive. Two situations in which it might appear are when a firewall will block DNS traffic or PKI traffic and prevent the router from receiving this traffic from the servers. Cisco SDM can modify these firewalls so that the servers can communicate with the router.

Modify Firewall

This area lists the exit interfaces and ACL names, and allows you to select which firewalls that you want Cisco SDM to modify. Select the firewalls that you want Cisco SDM to modify in the Action column. Cisco SDM will modify them to allow SCEP or DNS traffic from the server to the router.

Note the following for SCEP traffic:

- Cisco SDM will not modify firewall for CRL/OCSP servers if these are not explicitly configured on the router. To permit communication with CRL/OCSP servers, obtain the correct information from the CA server administrator and modify the firewallsusing the Edit Firewall Policy/ACL window.
- Cisco SDM assumes that the traffic sent from the CA server to the router will enter through the same interfaces through which traffic from the router to the CA server was sent. If you think that the return traffic from CA server will enter the router through a different interface than the one Cisco SDM lists, you need to open the firewall using the Edit Firewall Policy/ACL window. This may occur if asymmetric routing is used, whereby traffic from the router to the CA server exits the router through one interface and return traffic enters the router through a different interface.
- Cisco SDM determines the exit interfaces of the router the moment the passthrough ACE is added. If a dynamic routing protocol is used to learn routes to the CA server and if a route changes—the exit interface changes for SCEP traffic destined for the CA server—you must explicitly add a passthrough ACE for those interfaces using the Edit Firewall Policy/ACL window.
- Cisco SDM adds passthrough ACEs for SCEP traffic. It does not add passthrough ACEs for revocation traffic such as CRL traffic and OCSP traffic. You must explicitly add passthrough ACEs for this traffic using the Edit Firewall Policy/ACL window.

Details Button

Click this button to view the access control entry that Cisco SDM would add to the firewall if you allow the modification.

Open Firewall Details

This window displays the access control entry (ACE) that Cisco SDM would add to a firewall to enable various types of traffic to reach the router. This entry is not added unless you check **Modify** in the Open Firewall window and complete the wizard.