Configuring PKI

This chapter describes the Public Key Infrastructure (PKI) support on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router). PKI allows the Cisco CG-OS router to obtain and use digital certificates for secure communication in the network.

This chapter includes the following sections:

Information About PKI

This section provides information about PKI and includes the following topics:

CAs and Digital Certificates

Certificate authorities (CAs) manage certificate requests and issue certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each device or user has a key-pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning device or user. However, the public key is known to everybody. Anything encrypted with one of the keys can be de-encrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by de-encrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Trust Model, Trustpoints, and Identity CAs

The PKI trust model is hierarchical with multiple configurable trusted CAs. You can configure each participating device with a list of trusted CAs so that a peer certificate obtained during the security protocol exchanges can be authenticated if it was issued by one of the locally trusted CAs. The Cisco CG-OS software locally stores the self-signed root certificate of the trusted CA (or certificate chain for a subordinate CA). The process of securely obtaining a trusted CA root certificate (or the entire chain in the case of a subordinate CA) and storing it locally is called *CA authentication*.

The information about a trusted CA that you have configured is called the *trustpoint* and the CA itself is called a *trustpoint CA*. This information consists of a CA certificate (or certificate chain in case of a subordinate CA) and certificate revocation checking information.

The Cisco CG-OS router can also enroll with a trustpoint to obtain an identity certificate to associate with a key-pair. This trustpoint is called an *identity CA*.

RSA Key-Pairs and Identity Certificates

You can obtain an identity certificate by generating one or more RSA key-pairs and associating each RSA key-pair with a trustpoint CA where the Cisco CG-OS router intends to enroll. The Cisco CG-OS router needs only one identity per CA, which consists of one key-pair and one identity certificate per CA.

The Cisco CG-OS software allows you to generate RSA key-pairs with a configurable key size (or modulus). The default key size is 2048 bits. You can also configure an RSA key-pair label. The default key label is the device fully qualified domain name (FQDN).

The following list summarizes the relationship between trustpoints, RSA key-pairs, and identity certificates:

- A trustpoint corresponds to a specific CA that the Cisco CG-OS router trusts for peer certificate verification for any application.

- A Cisco CG-OS router can have many trustpoints and all applications on the device can trust a peer certificate issued by any of the trustpoint CAs.
- A trustpoint is not restricted to a specific application.
- A Cisco CG-OS router enrolls with the CA that corresponds to the trustpoint to obtain an identity certificate. You can enroll your Cisco CG-OS router with multiple trustpoints, which means that you can obtain a separate identity certificate from each trustpoint. Applications employ the identity certificates as determined by those purposes specified in the certificate by the issuing CA. The purpose of a certificate is stored in the certificate as a certificate extension.
- When enrolling with a trustpoint, you must specify a RSA key-pair to be certified. This key-pair must be generated and associated to the trustpoint before generating the enrollment request. The association between the trustpoint, key-pair, and identity certificate is valid until it is explicitly removed by deleting the certificate, key-pair, or trustpoint.
- The subject name in the identity certificate is the fully qualified domain name (FQDN) for the Cisco CG-OS router.
- You can generate one or more RSA key-pairs on a device and each can be associated to one or more trustpoints. But no more than one key-pair can be associated to a trustpoint, which means only one identity certificate is allowed from a CA.
- You do not need more than one identity certificate from a trustpoint or more than one key-pair to be associated to a trustpoint. A CA certifies a given identity (or name) only once and does not issue multiple certificates with the same name. If you need more than one identity certificate for a CA and if the CA allows multiple certificates with the same names, you must define another trustpoint for the same CA, associate another key-pair to it, and have it certified.

Multiple Trusted CA Support

The Cisco CG-OS router can trust multiple CAs by configuring multiple trustpoints and associating each with a distinct CA. With multiple trusted CAs, you do not have to enroll a device with the specific CA that issued the certificate to a peer. Instead, you can configure the device with multiple trusted CAs that the peer trusts. The Cisco CG-OS router can then use a configured trusted CA to verify certificates received from a peer that were not issued by the same CA defined in the identity of the peer device.

PKI Enrollment Support

Enrollment is the process of obtaining an identity certificate for the device that is used for applications, in this case the Cisco CG-OS router, and the certificate authority (CA).

Cisco recommends that you employ an intermediate router such as the Cisco 3945 Integrated Services Router (Cisco ISR) as the Registration Authority (functioning as a CA proxy) for obtaining certificates for the Cisco CG-OS router from the CA.

The Cisco CG-OS router performs the following steps when performing the PKI enrollment process:

1. Generates an RSA private and public key-pair.
2. Generates a certificate request in standard format and forwards it to the CA.

Note The CA administrator might be required to manually approve the enrollment request at the CA server when the request is received by the CA.

3. Receives the issued certificate back from the CA, signed with the private key of the CA.
4. Writes the certificate into a nonvolatile storage area on the Cisco CG-OS router.

Multiple RSA Key-Pair and Identity CA Support

Multiple identity CAs enable the Cisco CG-OS router to enroll with more than one trustpoint, which results in multiple identity certificates, each from a distinct CA. With this feature, the Cisco CG-OS router can participate in applications with many peers using certificates issued by CAs that are acceptable to those peers.

The multiple RSA key-pair feature allows the Cisco CG-OS router to maintain a distinct key-pair for each CA with which it is enrolled. It can match policy requirements for each CA without conflicting with the requirements specified by the other CAs, such as the key length. The Cisco CG-OS router can generate multiple RSA key-pairs and associate each key-pair with a distinct trustpoint. Thereafter, when enrolling with a trustpoint, the associated key-pair is used to construct the certificate request.

Peer Certificate Verification

PKI support on a Cisco CG-OS router can verify peer certificates. The Cisco CG-OS software verifies certificates received from peers during security exchanges for applications. The applications verify the validity of the peer certificates. The Cisco CG-OS software performs the following steps when verifying peer certificates:

1. Verifies that the peer certificate is issued by one of the locally-trusted CAs.
2. Verifies that the peer certificate is valid (not expired) with respect to current time.

Import and Export Support for Certificates and Associated Key-Pairs

As part of the CA authentication and enrollment process, the subordinate CA certificate (or certificate chain) and identity certificates can be imported in standard PEM (base64) format.

The complete identity information in a trustpoint can be exported to a file in the password-protected PKCS#12 standard format. It can be later imported to the same device (for example, after a system crash) or to a replacement device. The information in a PKCS#12 file consists of the RSA key-pair, the identity certificate, and the CA certificate (or chain).

Prerequisites

You must configure the Registration Authority (RA) to proxy for the CA server before you configure the Cisco CG-OS router. (See Configuring the Registration Authority, page 6-11.)

Guidelines and Limitations

The maximum number of key-pairs you can configure on the Cisco CG-OS router is 16.

The maximum number of trustpoints you can declare on the Cisco CG-OS router is 16.

The maximum number of identify certificates you can configure on the Cisco CG-OS router is 16.

The maximum number of certificates in a CA certificate chain is 10.

The maximum number of trustpoints you can authenticate to a specific CA is 10.

When generating certificates for the Cisco CG-OS router, a different RSA key-pair must be defined for the registration authority (RA) and the certification authority (CA).

Default Settings

Table 6-1 lists the default settings for PKI parameters.

Table 6-1 Default PKI Parameters

Parameters	Default
trustpoint	None
RSA key-pair	None
RSA key-pair label	Device FQDN
RSA key-pair modulus	2048
RSA key-pair exportable	Disabled

Configuring Certificate Enrollment

The Cisco CG-OS router supports the following types of certificate enrollment:

- Simple Certificate Enrollment Protocol (SCEP)–Allows automatic enrollment of the certificates on the Cisco CG-OS router without user intervention. (See Auto Enrollment Using SCEP, page 6-5.)
- Cut-and-paste enrollment–Supports manual enrollment between the Cisco CG-OS router and CA and requires that a user manually cut-and-paste the certificate requests and resulting certificates to manage the enrollment steps between the Cisco CG-OS router and the CA. (See Manual Enrollment, page 6-17.)
- Self-signed certificate–Allows the Cisco CG-OS router to create its own self-signed certificate. (See Configuring Self-Signed Certificates on the Cisco CG-OS Router, page 6-23.)
- Importing identity information in PKCS#12 format–Imports the certificate and RSA key-pair into the Cisco CG-OS router. (See Importing Identity Information in PKCS#12 Format, page 6-25.)

Auto Enrollment Using SCEP

This section describes the process of configuring the Cisco CG-OS router to communicate and exchange certificates with a Windows CA server to allow automatic enrollment of certificates.

Additionally, this section provides details on how to configure a Cisco ISR to serve as Registration Authority (RA) and proxy for the Windows CA server (which is the Cisco recommended configuration). This section does not provide details on configuring the Windows CA server.

This section includes the following topics:

- Configuring the Cisco CG-OS Router, page 6-6
- Configuring the Registration Authority, page 6-11

Configuring the Cisco CG-OS Router

This section includes the following topics:

Configuring the Cisco CG-OS Router Hostname and IP Domain Name

You must configure the hostname and IP domain name of the Cisco CG-OS router if you have not yet configured it because the Cisco CG-OS software uses the fully qualified domain name (FQDN) of the Cisco CG-OS router as the subject in the identity certificate. Additionally, the Cisco CG-OS software uses the device FQDN as a default key label when you do not specify a label during key-pair generation. For example, a certificate named DeviceA.example.com is based on a device hostname of DeviceA and a device IP domain name of example.com.

You must configure the hostname and IP domain name for both the Cisco CG-OS router and the Registration Authority.

Caution Changing the hostname or IP domain name after generating the certificate can invalidate the certificate.

BEFORE YOU BEGIN

Confirm the IP domain name and hostname with the system administrator.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**hostname** *hostname*	Configures the hostname of the Cisco CG-OS router.
Step 3	**ip domain-name** *name*	Configures the IP domain name of the Cisco CG-OS router.
Step 4	**show hosts**	(Optional) Displays the IP domain name.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the hostname and IP domain name for the Cisco CG-OS router.

```
router# configure terminal
router(config)# hostname router_cgr01
router_cgr01(config)# ip domain-name yourcompany.com
router_cgr01(config)# copy running-config startup-config
```

Caution You must configure the Registration Authority **before** configuring auto-enrollment on the Cisco CG-OS router. (See Configuring the Registration Authority, page 6-11.) After configuring the Registration Authority (RA), you can then continue configuring the Cisco CG-OS router.

Creating an Enrollment Profile on the Cisco CG-OS Router

Specifies the use of a RA as the trustpoint source for the Cisco CG-OS router and the system that authenticates the certificate for the Cisco CG-OS router.

BEFORE YOU BEGIN

Configure the router acting as the RA. (See Configuring the Registration Authority, page 6-11.)

Configure the server acting as the CA. (See your Windows server manual.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 1	**crypto ca profile enrollment** *profile_name*	Creates or updates an existing enrollment profile.
Step 2	**enrollment url** *url*	Defines the URL of the RA that serves as CA proxy and enters the enrollment profile configuration submode. The RA must be directly connected to the Cisco CG-OS router.
Step 3	**enrollment credential {IDevID | trustpoint** *trustpoint*}	(Optional) Specifies the method of authentication identity from the existing trustpoint. When employing this command, you must use an existing trustpoint. *trustpoint*–Identifies the name of the trustpoint. IDev ID–IEEE 802.11AR security device identity assigned by Cisco. Cisco CG-OS router locates the value when IDevID is entered for this command.
Step 4	**exit**	Exits the enrollment profile configuration mode and returns the Cisco CG-OS router to the global configuration mode.

EXAMPLE

This example shows how to create an enrollment profile for the RA on the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca profile enrollment IOS_CA_RA_Profile
router_cgr01(config-enroll-profile)# enrollment url http://192.168.20.16
router_cgr01(config-enroll-profile)# enrollment credential trustpoint blueCA
router_cgr01(config-enroll-profile)# exit
router_cgr01(config)#
```

Generating an RSA Public and Private Key-Pair on the Cisco CG-OS Router

Tip When you do not configure the RSA public and private key-pair, the Cisco CG-OS router automatically generates the key-pair with a default length of 2048 bits. In this case, the key-pair is non-exportable and the PKS#12 format cannot be used for backup and restore. If you want to set a default length other than 2048 bits and want to have an exportable key-pair, follow the steps in this section.

The Cisco CG-OS router can generate RSA key-pairs to sign and/or encrypt and de-encrypt the security payload during security protocol exchanges for applications. The RSA key-pair must be generated for the Cisco CG-OS router before obtaining a certificate for the Cisco CG-OS router.

BEFORE YOU BEGIN

Create the enrollment profile. (See Creating an Enrollment Profile on the Cisco CG-OS Router, page 6-7.)

DETAILED STEPS

	Command	Purpose
Step 1	**crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*]	Generates a RSA key-pair. The maximum number of key-pairs on a device is 16. *label-string*–An alphanumeric, case sensitive string with a maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.). *size*–Values are 1024, 1536, and 2048. The default modulus size is 2048 bits. **Note** Cisco recommends that you use the 2048 setting. **Note** The security policy on the Cisco CG-OS router and on the CA (where enrollment is planned) must be considered when deciding the appropriate key modulus. By default, the key-pair is not exportable when the default value of 2048 is in use. Only exportable key-pairs can be exported in the PKCS#12 format. **Caution** You cannot change the exportability of a key-pair.
Step 2	**show crypto key mypubkey rsa**	(Optional) Displays the generated key.
Step 3	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to generate a RSA key-pair on the Cisco CG-OS router.

```
router_cgr01(config)# crypto key generate rsa label IOS_CA_RA_Key modulus 2048
router_cgr01(config)# copy running-config startup-config
```

Creating a Trustpoint on the Cisco CG-OS Router

Defines the trustpoint for all services requiring secure communications. This trustpoint will be used by the Cisco CG-OS router to obtain its certificates from the RA.

BEFORE YOU BEGIN

Configure the RA. (See Configuring the Registration Authority, page 6-11.)

Generate the key-pair for the Cisco CG-OS router. (See Generating an RSA Public and Private Key-Pair on the Cisco CG-OS Router, page 6-8.)

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca trustpoint** *name*	Declares a trustpoint that the Cisco CG-OS router can trust and enters trustpoint configuration mode. *name*–Alphanumeric, case sensitive, string with a maximum length of 64 characters. **Note** The maximum number of trustpoints that you can configure on the Cisco CG-OS router is 16.
Step 2	**enrollment profile** *name*	Ensures that the RA requests the RA mode Certificate Service (CS) certificate from the CA server.
Step 3	**rsakeypair** *rsa-keypair-label*	Enter the key-pair name generated for the Cisco CG-OS router and RA. (See Generating a RSA Public and Private Key-Pair on the RA, page 6-14.)
Step 4	**revocation-check none**	Invalidates revocation of compromised certificates.
Step 5	**serial-number**	Includes the serial number of the Cisco CG-OS router in the certificate. **Note** This command is only applicable to SCEP auto-enrollment.
Step 6	**ip-address** *ip_address*	Configures the IP address of the Cisco CG-OS router that is included in the certificate request.
Step 7	**subject-alt-name** *name*	Configures an additional user to be defined in the certificate request during enrollment. *name*–Limit of 512 characters.
Step 8	**enrollment retry count** *retry-count*	Defines the number of times that the Cisco CG-OS router attempts to contact the RA for CA authentication and enrollment before reporting a failed enrollment. *retry-count*–Range of values is 1 to 10. Default value is 3.
Step 9	**enrollment retry period** *retry-period*	Defines the period of time (in seconds) between the retry attempts of the Cisco CG-OS router to contact the RA for CA authentication. *retry-period*–Range of values is 1 to 10 seconds. Default value is 5 seconds.

	Command	Purpose
Step 10	**fingerprint** *hex-data*	Configures the expected thumbprint of the CA server certificate. **Note** Thumbprint information is found in the **Certificate > Details** window of the Windows CA Server. Matching is performed during CA authentication and enrollment without the need for user intervention. **Note** The Cisco CG-OS router only supports SHA1 fingerprints.
Step 11	**exit**	Exits the trustpoint configuration mode and returns the Cisco CG-OS router to the global configuration mode.

EXAMPLE

This example shows how to create a trustpoint for the Cisco CG-OS router.

```
router_cgr01(config)# crypto ca trustpoint IOS_CA_RA
router_cgr01(config-trustpoint)# enrollment profile IOS-CA_Profile
router_cgr01(config-trustpoint)# rsakeypair IOS_CA_RAKey serial-number
router_cgr01(config-trustpoint)# ip address 192.168.200.40
router_cgr01(config-trustpoint)# subject-alt name jsmith@anycompany.com
router_cgr01(config-trustpoint)# enrollment retry count 10
router_cgr01(config-trustpoint)# enrollment retry period 5
router_cgr01(config-trustpoint)# fingerprint
23:65:E8:DA:D9::06:FD:32:4C:18:78:2B:8D:06:6F:B9:67:C1:09:91
router_cgr01(config-trustpoint)# exit
router_cgr01(config)#
```

Authenticating the CA on the Cisco CG-OS Router

BEFORE YOU BEGIN

Configure the RA. (See Configuring the Registration Authority, page 6-11.)

Generate the key-pair for the Cisco CG-OS router. (See Generating an RSA Public and Private Key-Pair on the Cisco CG-OS Router, page 6-8.)

Create a trustpoint for the Cisco CG-OS router. (See Creating a Trustpoint on the Cisco CG-OS Router, page 6-9.)

Enroll the Cisco CG-OS router with the RA Serving as CA Proxy. (See Configuring the Registration Authority, page 6-11.)

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca authenticate** *name*	Allows the Cisco CG-OS router to authenticate with RA as the proxy for the CA server and receive its certificates.
Step 2	**show crypto ca certificates** *name*	Displays the name of the trustpoint, certificate start and expiration dates and fingerprint.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to authenticate with the CA server and its certificates.

```
router_cgr01(config)# crypto ca authenticate IOS_CA_RA
Trustpoint CA authentication in progress. Please wait for a response...
router_cgr01(config)# 2013 Jan 29 11:27:57 router_cgr01 %$ VDC-1 %$
%CERT_ENROLL-2-CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint IOS_CA_RA: CA certificates(s)
authenticated.
```

Enrolling the Cisco CG-OS Router to the CA

To enroll the Cisco CG-OS Router to the CA, enter the following command.

Command	Purpose
crypto ca enroll *trustpoint-label*	Identifies the name of the trustpoint.

Configuring the Registration Authority

The RA proxies as a CA server on behalf of the Cisco CG-OS router to obtain its certificates from the CA server.

Tip This section provides the tasks necessary to configure a Cisco ISR to serve as the Registration Authority (RA). If you already have a RA configured or are going to use a different system for the RA, then you do not need to complete the tasks in this section.

Caution You must configure a RA **before** configuring the Cisco CG-OS router.

Note For more information on the Cisco ISR, refer to the following URL: http://www.cisco.com/en/US/products/ps10536/index.html

Tip The Cisco ISR (recommended system for RA) operates with Cisco IOS rather than the Cisco CG-OS software so the command syntax differs for some configurations.

This section includes the following topics:

Configuring the RA Hostname and IP Domain Name

You must configure the hostname and IP domain name of the RA router if it is not yet configured.

Caution Changing the hostname or IP domain name after generating the certificate can invalidate the certificate.

BEFORE YOU BEGIN

Confirm the IP domain name and hostname of the RA with the system administrator.

DETAILED STEPS

To configure the hostname and IP domain name for the Cisco ISR using Cisco IOS, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**hostname** *hostname*	Configures the hostname of the RA.
Step 3	**enable secret** *password*	Specifies an encrypted password to prevent unauthorized access to the RA.
Step 4	**ip domain-name** *name*	Defines a default domain name that the RA uses to complete unqualified hostnames (such as those without a dotted-decimal domain name).
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

```
router# configure terminal
router(config)# hostname IOS_CA_RA
IOS_CA_RA(config)# enable secret No$AcceSs
IOS_CA_RA(config)# ip domain-name yourcompany.com
IOS_CA_RA(config)# copy running-config startup-config
```

Configuring the RA as Proxy for the CA Server

Configures the RA to acts as a proxy for the CA server on behalf of the Cisco CG-OS router.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto pki server** *name*	Configures the RA as a CA server and RA for the third-party CA server. The name assigned to the RA must match the trustpoint name and the RSA key-pair assigned to the Cisco CG-OS router.

	Command	Purpose
Step 3	**database level {minimal | names | complete}**	Controls what type of data is stored in the certificate enrollment database. **minimal**–Stores enough information in the database to continue issuing new certificates without conflict. Default setting. **names**–Stores the serial number and subject name of each certificate in the database, which provides enough information for the administrator to find and revoke a particular certificate, if necessary. **complete**–Stores each issued certificate in the database.
Step 4	**grant auto**	Specifies that all enrollment requests from the Cisco CG-OS router to the RA be granted automatically.
Step 5	**hash {md5 | sha1}**	Specifies the cryptographic hash function that Cisco CG-OS uses for self-signed certificates. By default, Cisco CG-OS software uses md5.
Step 6	**mode ra [transparent]**	Enters the RA certificate server mode. The transparent keyword allows the proxy CA server in RA mode to interoperate with more than one type of CA server. Specifically it allows a transparent path from the RA (CA proxy) to the actual CA server that stores the certificates.
Step 7	**ip http server**	Enables the RA to start listening on port 80 (HTTP).
Step 8	exit	Exits to the global configuration mode.

EXAMPLE

This example shows how to configure the RA to serve as proxy for the CA server.

```
IOS_CA_RA# configure terminal
IOS_CA_RA(config)# crypto pki server IOS_CA_RA
IOS_CA_RA(cs-server)# grant auto trustpoint BlueCA
IOS_CA_RA(cs-server)# hash sha1
IOS_CA_RA(cs-server)# mode ra transparent
IOS_CA_RA(cs-server)# ip http server
IOS_CA_RA(cs-server)# exit
IOS_CA_RA(config)#
```

Creating an Enrollment Profile on the RA

Enrolls with the CA server on behalf of the Cisco CG-OS router to obtain the certificates from the CA server.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto pki trustpoint** *name*	Declares a trustpoint that the RA should trust and enters trustpoint configuration mode. *name*–Alphanumeric, case sensitive, string with a maximum length of 64 characters. **Note** The maximum number of trustpoints that you can configure in Cisco IOS is 16.
Step 2	**enrollment url** *url*	Defines the address of the CA server. *url*–Specifies the address of the CA server. **Note** You can specify only one RSA key-pair per CA.
Step 3	**serial-number**	Includes the serial number of the RA in the certificate. **Note** This command is only applicable to SCEP auto-enrollment.
Step 4	**subject-name** *x-500-name*	Specifies the subject name in the certificate request. *x-500-name*–Limit of 512 characters.
Step 5	**exit**	Exits to global configuration mode.

EXAMPLE

This example shows how to enroll the RA with the CA server to obtain certificates for the Cisco CG-OS router.

```
IOS_CA_RA (config)# crypto pki trustpoint IOS_CA_RA
IOS_CA_RA (ca-trustpoint)# enrollment url http://172/27/165.157:80
IOS_CA_RA (ca-trustpoint)# serial-number
IOS_CA_RA (ca-trustpoint)# subject-name ou=ioscs RA
IOS_CA_RA (ca-trustpoint)# exit
IOS_CA_RA(config)#
```

Generating a RSA Public and Private Key-Pair on the RA

The RSA key-pair provides secure communication between the RA and the CA server.

The RA can generate RSA key-pairs to sign and/or encrypt and de-encrypt the security payload during security protocol exchanges for applications.

Note The RSA key-pair must be generated for the RA before obtaining a certificate for the RA.

Note When configuring the RSA key-pair and CA trustpoint name, you must use the same name within the RA to ensure that the certificate is generated and associated correctly.

BEFORE YOU BEGIN

Define the trustpoint (secure credentials) for all services requiring secure communications. (See Creating an Enrollment Profile on the RA, page 6-13.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*]	Generates a RSA key-pair. The maximum number of key-pairs on a device is 16. *label-string*–An alphanumeric, case sensitive string with a maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.). *size*–Values are 512, 768, 1024, 1536, and 2048. The default modulus size is 512. **Note** Cisco recommends that you use the 2048 setting. **Note** The security policy on the Cisco CG-OS router and on the CA (where enrollment is planned) must be considered when deciding the appropriate key modulus. By default, the key-pair is not exportable. Only exportable key-pairs can be exported in the PKCS#12 format. **Caution** You cannot change the exportability of a key-pair.
Step 3	**show crypto key mypubkey rsa**	(Optional) Displays the generated key.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to generate an RSA key-pair for the RA.

```
IOS_CA_RA# configure terminal
IOS_CA_RA(config)# crypto key generate rsa label IOS_CA_RA_Key modulus 2048
IOS_CA_RA(config)# copy running-config startup-config
```

Creating a Trustpoint for the RA

Defines the trustpoint (secure credentials) for all services requiring secure communications. This trustpoint will be used by the RA to obtain certificates for the Cisco CG-OS router from the CA server.

You must associate the RA with a trustpoint.

BEFORE YOU BEGIN

Generate the RSA key-pair for the RA router. (See Generating a RSA Public and Private Key-Pair on the RA, page 6-14.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *name*	Declares a trustpoint that the device should trust and enters trustpoint configuration mode. *name*–Alphanumeric, case sensitive, string with a maximum length of 64 characters. **Note** The maximum number of trustpoints that you can configure on a device is 16.
Step 3	**enrollment mode ra**	Ensures that the RA router requests the RA mode Certificate Service (CS) certificate from the CA server.
Step 4	**enrollment url** *url*	Defines the address of the CA server. *url*–Specifies the address of the CA server. **Note** You can specify only one RSA key-pair per CA.
Step 5	**serial-number**	Includes the serial number of the RA in the certificate. **Note** This command is only applicable to SCEP auto-enrollment.
Step 6	**fingerprint** *hex-data*	Defines the thumbprint of the CA server. Information is found in the **Certificate > Details** window of the CA Server.
Step 7	**revocation-check none**	(Optional) Invalidates revocation of compromised certificates.
Step 8	**rsakeypair** *rsa-keypair-label*	Enter the RSA key-pair name generated for the RA and CA. (See Generating a RSA Public and Private Key-Pair on the RA, page 6-14.)
Step 9	**show crypto pki trustpoint** *name*	(Optional) Displays information on any configured trustpoints.
Step 10	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to associate the RA with a trustpoint.

```
IOS_CA_RA# configure terminal
IOS_CA_RA(config)# crypto pki trustpoint IOS_CA_RA
IOS_CA_RA(ca-trustpoint)# enrollment mode ra
IOS_CA_RA(ca-trustpoint)# enrollment url http://<CA_Server_IP
address>:80/certserv/mscep/mscep.dll
IOS_CA_RA(ca-trustpoint)# serial-number
IOS_CA_RA(ca-trustpoint)# fingerprint 2D830B4783130C2B7B64B338835D7516
IOS_CA_RA(ca-trustpoint)# revocation-check none
IOS_CA_RA(ca-trustpoint)# rsakeypair IOS_CA_RA_Key 2048
IOS_CA_RA(ca-trustpoint)# ip http server
IOS_CA_RA(ca-trustpoint)# copy running-config startup-config
```

Authenticating the RA

Begins authentication between the Cisco CG-OS router and the RA.

BEFORE YOU BEGIN

Generate the RSA key-pair for the RA. (See Generating a RSA Public and Private Key-Pair on the RA, page 6-14.)

Create a trustpoint. (See Creating a Trustpoint for the RA, page 6-15.)

DETAILED STEPS

	Command	Purpose
Step 1	**crypto pki server** *name*	Identifies the PKI server that was configured previously. (See Configuring the RA as Proxy for the CA Server, page 6-12.)
Step 2	**no shutdown**	Enables the PKI server.

EXAMPLE

```
IOS_CA_RA# configure terminal
IOS_CA_RA(config)# crypto pki server IOS_CA_RA
IOS_CA_RA(config)# no shutdown
```

Manual Enrollment

The Cisco CG-OS software supports certificate retrieval and enrollment using manual cut-and-paste. Cut-and-paste enrollment means that you must use a terminal to cut-and-paste the certificate requests and resulting certificates sent between the Cisco CG-OS router and the CA.

You must perform the following steps when using cut-and-paste in the manual enrollment process:

1. Create an enrollment certificate request, which the Cisco CG-OS router displays in base64-encoded text form.
2. Cut-and-paste the encoded certificate request text in an e-mail or in a web form and send it to the CA.
3. Receive the issued certificate (in base64-encoded text form) from the CA in an e-mail or in a web browser download.

4. Cut-and-paste the issued certificate into the Cisco CG-OS router using the certificate import facility.

This section describes the tasks that you must perform to allow the Cisco CG-OS router to assign digital certificates to itself by using manual cut-and-paste, and includes the following topics:

Creating a Trustpoint

Defines the trustpoint (secure credentials) for all services requiring secure communications.

BEFORE YOU BEGIN

Ensure that you have access to a terminal.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto ca trustpoint** *name*	Declares a trustpoint that the Cisco CG-OS router can trust and enters trustpoint configuration mode. *name*–Alphanumeric, case sensitive, string with a maximum length of 64 characters. **Note** The maximum number of trustpoints that you can configure on the Cisco CG-OS router is 16.
Step 3	**enrollment terminal**	Enables cut-and-paste certificate enrollment on the Cisco CG-OS router.

EXAMPLE

This example shows how to create a trustpoint for the Cisco CG-OS router using manual cut-and-paste enrollment.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca trustpoint CGRca
router_cgr01(ca-trustpoint))# enrollment terminal
router_cgr01(ca-trustpoint))# exit
router_cgr01(config)#
```

Authenticating the CA

The configuration process of trusting a CA is complete only when the CA is authenticated to the Cisco CG-OS router. You must authenticate your Cisco CG-OS router to the CA by obtaining the self-signed certificate of the CA in PEM format, which contains the public key of the CA. Because the certificate of the CA is self-signed (the CA signs its own certificate) the public key of the CA should be authenticated by contacting the CA administrator to compare the fingerprint of the CA certificate.

Note In order to have a valid certificate, you must know the identity of the root CA even if there are intermediate servers in the path. The full path is identified as the *certificate chain*. The maximum number of certificates in a CA certificate chain is 10. Be sure that you cut-and-past the full certificate chain.

BEFORE YOU BEGIN

Create a trustpoint. (See Creating a Trustpoint, page 6-18.)

Obtain the CA certificate or CA certificate chain.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca authenticate** *trustpoint-name*	Cisco CG-OS router prompts you to cut-and-paste the certificate of the CA. Use the same name that you used when defining the trustpoint. The maximum number of trustpoints that you can authenticate to a specific CA is 10. **Note** For subordinate CA authentication, Cisco CG-OS requires the full chain of CA certificates ending in a self-signed CA because the CA chain is needed for certificate verification as well as for PKCS#12 format export.
Step 2	**exit**	Exits the configuration mode.
Step 3	**show crypto ca trustpoints**	(Optional) Displays the CA trustpoint CA information.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to authenticate a CA.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca authenticate BlueCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
```

```
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3J1MQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12


Do you accept this certificate? [yes/no]: yes
```

router_cgr01(config)# **exit**

router_cgr01# **copy running-config startup-config**

Generating an RSA Public and Private Key-Pair

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*]	Generates an RSA key-pair. The maximum number of key-pairs on a device is 16. *label-string*–An alphanumeric, case sensitive string with a maximum length of 64 characters. The default label string is the hostname and the FQDN separated by a period character (.). *size*–Values are 512, 768, 1024, 1536, and 2048. The default modulus size is 512. **Note** Cisco recommends that you use the 2048 setting. **Note** The security policy on the Cisco CG-OS router and on the CA (where enrollment is planned) must be considered when deciding the appropriate key modulus. By default, the key-pair is not exportable. Only the PKCS#12 format allows exportable key-pairs. **Caution** You cannot change the exportability of a key-pair.
Step 2	**show crypto key mypubkey rsa**	(Optional) Displays the generated key.

EXAMPLE

This example shows how to generate a RSA key-pair.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto key generate rsa label BlueCA_Identity modulus 2048
router_cgr01(config-trustpoint)#
```

Associating the RSA Key-Pair to the Trustpoint

BEFORE YOU BEGIN

Generate an RSA key-pair. (See Generating an RSA Public and Private Key-Pair, page 6-20.)

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca trustpoint** *trustpoint-label*	Specifies a trustpoint CA and enters trustpoint configuration mode.
Step 2	**rsakeypair** *rsa-keypair-label*	Enter the keypair name generated for the Cisco CG-OS router and RA.

EXAMPLE

This example shows how to associate an RSA key-pair to a trustpoint.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca trustpoint BlueCA
router_cgr01(config-trustpoint)# rsakeypair BlueCA_Identify
```

Generating Certificate Requests

You must generate a request to obtain identity certificates from the associated trustpoint CA for each of the RSA key-pairs of the Cisco CG-OS router. You must then cut-and-paste the displayed request into an e-mail or in a website form for the CA.

BEFORE YOU BEGIN

Create an association with the CA. (See Associating the RSA Key-Pair to the Trustpoint, page 6-21.)

Obtain the CA certificate or CA certificate chain.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca enroll** *trustpoint-label*	Generates a certificate request for an authenticated CA. *trustpoint label*–Name of the trustpoint. The maximum size is 64 characters. **Note** You must remember the challenge password. It is not saved with the configuration. You must enter this password if your certificate needs to be revoked.

EXAMPLE

This example shows how to generate a certificate request.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca enroll CGRca
Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: CGRca.cisco.com
 Include the router serial number in the subject name? [yes/no]: no
 Include an IP address in the subject name [yes/no]: yes
ip address:10.22.31.162
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Installing Identity Certificates

You can receive the identity certificate from the CA by email or through a web browser in base64 encoded text form. You must install the identity certificate from the CA by cutting and pasting the encoded text.

BEFORE YOU BEGIN

Generate a certificate request and verify receipt of the signed certificate from the CA.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca import** *trustpoint-label* **certificate**	Cisco CG-OS router prompts you to cut-and-paste the identity certificate for the CA. The maximum number of identify certificates that you can configure on the Cisco CG-OS router is 16.

EXAMPLE

This example shows how to install the identify certificate named CGRca into the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01#(config)# crypto ca import CGRca certificate
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT:
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBCDANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoT
DUNpc2NvIFN5c3RlbXMxDTALBgNVBAsTBFNHQlUxEDAOBgNVBAMTB0JsdWUgQ0Ew
HhcNMTEwNDI2MTkyNTI4WhcNMjEwNDIzMTkyNTI4WjAXMRUwEwYDVQQDEwxhbGV4
bC1NaWxhbjEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCtBHACAgCO
7+79Lm7JJ/G+PhSfga3sFp2wRMQKmoCvmus9d7vkzrHQIfzs6uaiqPT8F3SQTbWU
btr01JDfJvvuVOd/VNrwZoP9kFJHU3uOEDY767SmG2lv9XO96GcKsa/Nj8nXM6FZ
7PhuZl9NQ6QYYjEkvBWsUsQjMfL8oFckTZvPKoCdjl5WuQ14Umo6N2ST7K+UsqsL
wTkP9fyGgKsQuYJg6PBSaEu+OqfWkkvy65QWVtGGRdOmOD8EKsKpVQecVQuZ86it
o2CPcYET83LOeu35H2TVhzyuv5lUaoor02hP6swyUXsQLVg6XeyVbwzf7R8t4M2W
VPs42bHwqRHZAgMBAAGjITAfMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjANBgkqhkiG9w0BAQUFAAOCAQEAZxfmKoJb9aT/eZT5v1cCwdsM0Wh9fjON3h3L
no2r1y83jKvYhpjNhLcoF5Q0sFCPRBpq8f9vjKGHHT9j4fkQZGmsJl+l5YztuF6J
rkFmf3tzqJU9Hu8d6zh4YtdqMz57DxhMC6PbvAg1bw6KSujzxT7J0HnpFog+QkaX
MTC9JCvRWna1VOo38VsA0XYUtMrXRN7XntKzb6D33dW7VYQCSmz/McNWbOL0zlTl
B7ZKzkOH/uqG3A0fj6+LDqFyprQ62RhLTSuNKViCliR91QOE0weXm8txwLBlM8Tg
q/a6HGFzsLhOa3X1qhv2oqA5QgPyS0ixMEdzh1cxkTzTgmDjow==
-----END OF CERTIFICATE-----
router_cgr01#(config)#
```

Configuring Self-Signed Certificates on the Cisco CG-OS Router

Creates self-signed certificate for the Cisco CG-OS router.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto ca trustpoint** *name*	Declares a trustpoint that the Cisco CG-OS router can trust and enters trustpoint configuration mode. *name*–Alphanumeric, case sensitive, string with a maximum length of 64 characters. **Note** The maximum number of trustpoints that you can configure on the Cisco CG-OS router is 16.
Step 3	**revocation-check none**	(Optional) Invalidates revocation of compromised certificates.
Step 4	**enrollment selfsigned**	Generates a self-signed certificate on the Cisco CG-OS router.
Step 5	**rsakeypair** *rsa-keypair-label*	Enters the RSA key-pair name generated by the Cisco CG-OS router.
Step 6	**exit**	Exits to the global configuration mode.
Step 7	**crypto ca enroll** *trustpoint-label*	Generates a certificate request for the self-signed Cisco CG-OS router. *trustpoint label*–Name of the trustpoint. The maximum size is 64 characters.

EXAMPLE

This example shows how to create a self-signed certificate on the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01#(config)# crypto ca trustpoint SelfSignedCA
router_cgr01(config-trustpoint)# revocation-check none
router_cgr01(config-trustpoint)# enrollment selfsigned
router_cgr01(config-trustpoint)# rsakeypair PrivateKeyForSelfSignedCA 2048
router_cgr01(config-trustpoint)# exit
router_cgr01(config)# crypto ca enroll SelfSignedCA

Create the certificate request ..
The subject name in the certificate will be the name of the router.
Include the router serial number in the subject name? [yes/no]:yes
The serial number in the certificate will be: CGR1240/K9+JSJ15380008
Include an IP address in the subject name [yes/no]:no
Include the Alternate Subject Name ? [yes/no]:no
```

Importing Identity Information in PKCS#12 Format

You can import the certificate and RSA key-pair to recover from a system crash on your Cisco CG-OS router or when you replace equipment on your Cisco CG-OS router.

Note You can use only the bootflash:*filename* format when specifying the import URL.

BEFORE YOU BEGIN

Ensure that the trustpoint is empty by checking that no RSA key-pair is associated with it and no CA is associated with the trustpoint using CA authentication.

DETAILED STEPS

	Command	Purpose
Step 1	**copy** *scheme*:**//***server*/[*url*/]*filename* **bootflash:***filename*	Copies the PKCS#12 format file from the remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	**crypto ca import** *trustpoint-label* **pksc12 bootflash:***filename password*	Imports the identity certificate and associated key-pair and CA certificates for trustpoint CA. *password*–Identifies the export password of PKCS#12.
Step 4	**show crypto ca certificates**	(Optional) Displays the CA certificates.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to copy the PKCS#12 format file from the remote server and then import that file into the Cisco CG-OS router.

```
copy tftp:adminid.p12 bootflash:adminid.p12
router_cgr01# configure terminal
router_cgr01(config)# crypto ca import ConnectedGrid pkcs12 bootflash:adminid.p12 nbv123
router_cgr01(config)# copy running-config startup-config
```

Ensuring Trustpoint Configurations Persist Across Reboots

You can ensure that the trustpoint configuration persists across reboots of the Cisco CG-OS router.

The trustpoint configuration is a normal system configuration that persists across system reboots only if you copy it explicitly to the startup configuration. The certificates and RSA key-pairs associated with a trustpoint are automatically persistent if you have already copied the trustpoint configuration in the startup configuration. Conversely, if the trustpoint configuration is not copied to the startup configuration, the certificates and RSA key-pairs associated with it are not persistent since they require the corresponding trustpoint configuration after a reboot.

Always copy the running configuration to the startup configuration to ensure that the configured certificates and RSA key-pairs are persistent. Also, save the running configuration after deleting a certificate or key-pair to ensure that the deletions permanent.

The certificates associated with a trustpoint automatically become persistent when imported (that is, without explicitly copying to the startup configuration) if the specific trustpoint is already saved in startup configuration.

Cisco recommends that you create a password protected backup of the identity certificates and save it to an external server. (See Exporting Identity Information in PKCS#12 Format, page 6-26.)

Note Copying the configuration to an external server includes the certificates and RSA key-pairs.

Exporting Identity Information in PKCS#12 Format

You can export the identity certificate along with the RSA key-pair and CA certificate (or the entire chain in the case of a subordinate CA) of a trustpoint to a PKCS#12 file for backup purposes. You can import the certificate and RSA key-pair to recover from a system crash on your device.

Note You can use only the bootflash:*filename* format when specifying the export URL.

BEFORE YOU BEGIN

Generate an exportable RSA key-pair. (See Generating an RSA Public and Private Key-Pair on the Cisco CG-OS Router, page 6-8.)

Authenticate the CA. (See Authenticating the CA, page 6-19.)

Install an identity certificate. (See Installing Identity Certificates, page 6-23.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.

	Command	Purpose
Step 2	**crypto ca export** *trustpoint-label* **pkcs12 bootflash:***filename password*	Exports the identity certificate and associated key-pair and CA certificates for a trustpoint CA. The password is alphanumeric, case sensitive, and has a maximum length of 128 characters.
Step 3	**copy bootflash:***filename scheme***://**server**/**[*url*/]*filename*	Copies the PKCS#12 format file to a remote server. For the *scheme* argument, you can enter **tftp:**, **ftp:**, **scp:**, or **sftp:**. The *server* argument is the address or name of the remote server, and the *url* argument is the path to the source file on the remote server. The *server*, *url*, and *filename* arguments are case sensitive.

EXAMPLE

This example shows how to export an identity certificate to a PKCS#12 file for backup purposes.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca export ConnectedGrid pkcs12 bootflash:adminid.p12 nbv123
router_cgr01(config)# copy bootflash:adminid.p12 tftp:adminid.p12
```

Deleting Certificates from the CA Configuration

You can delete the CA certificates and identity certificates that are configured in a trustpoint. You must first delete the CA certificates, followed by the identity certificate. After deleting the identity certificate, you can disassociate the RSA key-pair from a trustpoint. You must delete certificates to remove expired or revoked certificates, certificates that have compromised (or suspected to be compromised) RSA key-pairs, or CAs that are no longer trusted.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto ca trustpoint** *trustpoint-label*	Specifies a trustpoint CA and enters trustpoint configuration mode.
Step 3	**delete ca-certificates**	Deletes the CA certificate or certificate chain.

	Command	Purpose
Step 4	**delete certificate** [**force**]	Deletes the identity certificate. You must use the **force** option if the identity certificate you want to delete is the last certificate in a certificate chain or only identity certificate in the device. This requirement ensures that you do not mistakenly delete the last certificate in a certificate chain or only identity certificate and leave the applications without a certificate to use.
Step 5	**show crypto ca certificates** [*trustpoint-label*]	(Optional) Displays the CA certificate information.
Step 6	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to delete CA certificates and identity certificate from the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto ca trustpoint admin-ca
router_cgr01(config-trustpoint)# delete ca-certificate
router_cgr01(config-trustpoint)# delete certificate
router_cgr01(config-trustpoint)# copy running-config startup-config
```

Deleting RSA Key-Pairs from the Cisco CG-OS Router

You can delete the RSA key-pairs on the Cisco CG-OS router when you believe the integrity of the RSA key-pairs are compromised or should no longer be used.

Note After you delete RSA key-pairs from the Cisco CG-OS router, ask the CA administrator to revoke the certificates of the Cisco CG-OS router at the CA. You must supply the challenge password that was created when the certificates were originally created. (See Generating Certificate Requests, page 6-22.)

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**crypto key zeroize rsa** *label*	Deletes the RSA key-pair.

	Command	Purpose
Step 3	**show crypto key mypubkey rsa**	(Optional) Displays the RSA key-pair configuration.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to delete RSA key-pairs on the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01(config)# crypto key zeroize rsa MyKey
router_cgr01(config)# copy running-config startup-config
```

Verifying the Configuration

To verify the PKI and CA configurations, use the following commands:

Command	Purpose
show crypto key mypubkey rsa	Displays information about the RSA public keys generated on the Cisco CG-OS router.
show crypto pki certificates	Displays information about CA and identity certificates.
show crypto ca trustpoints	Displays information about CA trustpoints.