

# Public Key Infrastructure Integration with the Cisco Virtual Office Solution

## Introduction

This white paper provides detailed design and implementation information relating to the deployment of Public Key Infrastructure (PKI) with the Cisco<sup>®</sup> Virtual Office.

Please refer to the Cisco Virtual Office overview at <http://www.cisco.com/go/cvo> for further information about the solution, its architecture, and its components.

Cisco IOS<sup>®</sup> Software PKI provides certificate management to support security protocols such as IPsec (IPsec), Secure Shell (SSH) Protocol, and Secure Sockets Layer (SSL). As defined in the IPsec protocol, peers must be authenticated during Internet Key Exchange (IKE) phase 1 before secure communication is established. When pairs of Cisco IOS Software routers are configured as IPsec peers, the routers can use pre-shared keys (PSKs) to authenticate each other as part of security establishment. Using PSKs may be a better choice for customers deploying a small to midsize network containing few routers.

As networks become larger in size and scale, PSK configuration becomes very complex, and managing multiple keys is difficult. PKI offers a much more secure and scalable method for midsize to large enterprise deployments—whether a full mesh of security connections for Dynamic Multipoint VPN (DMVPN) or any of the newly supported VPN technologies, or spoke-to-spoke communications, or enterprises deploying site-to-site VPN for hundreds of remote branch offices needing to communicate with each other. PKI reduces management overhead and simplifies the deployment of the network infrastructure by using digital certificate exchange instead of PSKs for device authentication.

## Document Scope

This document describes the integration of PKI within the Cisco Virtual Office deployment from a functional perspective. It explains some of the PKI enhancements available in recent Cisco IOS Software releases that strengthen the Cisco Virtual Office infrastructure. This document does not explain the details of PKI, IPsec, or any VPN concepts. You should be familiar with these concepts; for more information, you can refer to the links provided in the References section.

## PKI Overview

To help you understand the use of PKI within Cisco Virtual Office, this section provides a brief introduction to PKI.

A PKI is composed of the following entities:

- Peers communicating on a secure network
- At least one certification authority (CA) that grants and maintains certificates
- Digital certificates, which contain information such as the certificate validity period, peer identity information, encryption keys that are used for secure communication, and the signature of the issuing CA

- An optional registration authority (RA) to offload the CA by processing enrollment requests
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Each entity (router or PC) participating in the secure communication is enrolled, a process by which the entity generates a Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has its identity validated by a trusted entity (also known as a CA).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA. When peers must negotiate a secured communication session, they exchange their digital certificates. Using the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

### **RSA Key Overview**

An RSA key pair consists of a public key and a private key. When setting up a PKI, the router (also called the certificate client) must include the public key in the certificate enrollment request. After the certificate request has been granted, the public key is included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

### **Certificate Authority**

A CA, manages certificate requests and issues certificates to participating network devices. These services provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

The CA can be a third-party vendor such as Microsoft or VeriSign or a Cisco IOS Certificate Server performing the role of a CA. The deployment described in this guide uses the Cisco IOS Certificate Server.

### **Recommended Platforms and Images**

Images based on Cisco IOS Software Release 12.4(15)T are recommended for the Cisco IOS Certificate Server and Subordinate Certificate Server. The following platforms are suggested for various PKI roles:

CA: Cisco 1800 Series, 2800 Series, or 3800 Series Integrated Services Router running the Cisco IOS Certificate Server or Microsoft Certificate Authority.

Cisco Virtual Office hubs: Cisco 3800 Series Integrated Services Router or Cisco 7200 Series Router.

Cisco Virtual Office spokes: Cisco 871 Integrated Services Routers and above. For the Cisco 881 Integrated Services Router, Cisco IOS Software Release 12.4(20)T is required.

## Deployment

The CA is best placed in the subnet connected behind the management VPN gateway. The reason is that PKI certificates are crucial for Cisco Virtual Office remote spokes to establish a DMVPN tunnel with data gateways for corporate access. Initially, the spokes can be enrolled with CA as part of in-house provisioning before shipment to the remote user. If PKI certificates have expired or become invalid, the tunnel cannot be set up for corporate access. Keeping the CA under the management subnet will give the spokes secure access through the management tunnel for new enrollment or reenrollment if certificates expire or become invalid. If the certificate from the same CA is used to set up secure connections with the management and data gateways and the certificate in the spoke becomes invalid, the management tunnel will also fail. Hence it is recommended to use different CAs to set up secure connections with management and data gateways.

Digital certificates are issued to each router, including the hub and spokes. Digital certificates are very difficult to spoof, so the use of the certificates for PKI authentication helps ensure that no unauthorized spokes are connected to the VPN. Unless marked as exportable, the RSA keys cannot be exported, so RSA keys cannot be transferred to another router.

Now we will look at how to configure the CA and the routers as PKI clients. As mentioned earlier, we can use a CA provided by a third-party vendor such as Microsoft or VeriSign, or a Cisco IOS Certificate Server. The following Cisco Virtual Office deployment uses the Cisco IOS Certificate Server; this guide does not discuss the Microsoft Certificate Authority or other third-party CAs.

**Note:** The Cisco IOS Certificate Server will be used to represent the CA in the remainder of this document.

## Configuring the Cisco IOS Certificate Server

The first step in PKI deployment is to bring up the Cisco IOS Certificate Server, which is a router running Cisco IOS Software with IP connectivity enabled to reach resources such as Network Time Protocol (NTP), Trivial File Transfer Protocol (TFTP), and Domain Name System (DNS) servers necessary for proper functioning. Cisco IOS Certificate Server must be configured with ip http server to support enrollments done using Simple Certificate Enrollment Protocol (SCEP). This section describes only configurations relevant to Cisco IOS Certificate Server.

This configuration example uses a Cisco 2811 Integrated Services Router running Cisco IOS Software Release 12.4(15)T5.

```
! !!! hostname and domain name form a fully qualified domain name in
certificates !!!
hostname cvo-pki-cs
ip domain name cisco.com
! !!! clock must be in sync between Cisco IOS Certificate Server and
the clients, including timezone !!!
clock timezone PST -8
clock summer-time PDT recurring
ntp server 10.1.1.101
! !!! FTP access configuration for storing .crt, .cnm, and .crl files
in external FTP server !!!
```

```

ip ftp username ftpusr
ip ftp password cisco
ip host ftpserver 10.1.1.100
! !!! To process enrollment requests and issue certificates !!!
ip http server
!
!!! RSA key pair is generated automatically when enabling Cisco IOS
Certificate Server using 1024 bits. Optionally, RSA keys with the
rsakeypair name matching the certificate server can be generated
manually with different options such as higher modulus, exportable,
etc. Keys must be generated with the exportable option to export them
for later restoration in case of certificate server failure. However,
the user needs to take the utmost care to store keys securely as it
would be easy for someone to get access with the keys. !!!

cvo-pki-cs(config)#crypto key generate rsa general-keys label cvo-pki-
cs modulus 1024 exportable

!!! The following Cisco IOS Certificate Server configuration uses a
complete database that stores separate .crt and .cnm files for each
certificate it issues. In general, router flash memory has less
capacity to store all these files; hence, only essential files should
be stored in router flash memory, and all other files can be stored on
an external FTP server. The lifetime values shown here are for
illustration purposes only. !!!
!
crypto pki server cvo-pki-cs      !!! PKI server name must match
rsakeypair name !!!
    database level complete
    database archive pkcs12 password cisco123 !!! Keys can be auto
archived !!!
    issuer-name cn=cvo-pki-cs,ou=cvo !!! Identification of the PKI
server within Cisco Virtual Office !!!
    grant auto !!! Certificate server automatically grants enrollment
requests from routers !!!
    lifetime crl 24              !!! Every 24 hours the CRL database is
renewed and published !!!
    lifetime certificate 60      !!! Issued router (client)
certificates are valid for 60 days !!!
    lifetime ca-certificate 75   !!! Root (certificate server)
certificate is valid for 75 days !!!
    cdp-url http://10.1.1.100/cvo-pki-cs.crl    !!! PKI clients get CRL
from this location !!!
    database url ftp://10.1.1.100/pki    !!! All files are stored on this
external FTP server !!!
!
!!! The following trustpoint configuration is autogenerated when Cisco
IOS Certificate Server is enabled. Optionally, this trustpoint
configuration can be created manually before enabling Cisco IOS
Certificate Server. !!!
!
crypto pki trustpoint cvo-pki-cs
    enrollment url http://cvo-pki-cs:80    !!! Optional !!!
    serial-number
    revocation-check crl
    rsakeypair cvo-pki-cs                !!! rsakeypair name must match PKI
server name !!!

```

```

!
!!! To enable the Cisco IOS Certificate Server, enter a "no shut"
command in server config mode. !!!
!
cvo-pki-cs(cs-server)#no shutdown
!

```

**Note:** It is recommended to use the database archive command with strong password to archive RSA keys in a pkcs12 file instead of generating RSA keys with exportable option as mentioned earlier.

When Cisco IOS Certificate Server is enabled, this is how the root CA certificate appears:

```

cvo-pki-cs#show crypto pki certificates
CA Certificate                                     !!! Root CA
certificate !!!
  Status: Available
  Certificate Serial Number: 0x1
  Certificate Usage: Signature
  Issuer:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Subject:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Validity Date:
    start date: 11:38:04 PDT May 01 2008
    end   date: 11:38:04 PDT Jul 15 2008
  Associated Trustpoints: cvo-pki-cs
  Storage: nvram:cvo-pki-cs#1CA.cert

cvo-pki-cs#

```

Now, save the configuration.

### Configuring Cisco Virtual Office Routers for PKI

After the Cisco IOS Certificate Server is set up, the PKI client can enroll with the certificate server and download client certificates. For Cisco Virtual Office, both the hub and spoke are PKI clients, and they must enroll with the certificate server before using PKI authentication.

This configuration example uses a Cisco 881 Integrated Services Router running Cisco IOS Software Release 12.4(20)T.

**Note:** For certificates to be valid, the clock on the certificate server and clients must be in sync. All clients must have IP reachability to the certificate server and use the same clock source as the certificate server.

```
!  
hostname cvo-spoke  
ip domain name cisco.com  
clock timezone PST -8  
clock summer-time PDT recurring  
ntp server 10.1.1.101  
!  
!!! Generate RSA keys in the client router. If not generated now, keys  
will be autogenerated during trustpoint authentication. !!!  
  
cvo-spoke(config)#crypto key generate rsa general-keys modulus 1024  
  
!!! Create the following trustpoint configuration in config mode in  
the router !!!  
!  
ip host cvo-pki-cs 10.1.1.105  
!  
crypto pki trustpoint cvo-pki-cs  
enrollment url http://cvo-pki-cs:80  
serial-number  
  
!!! Using CRL check is desirable for Cisco Virtual Office hubs  
because it prevents any unauthorized router from setting up a secure  
session with Cisco Virtual Office hubs. The advantage of using CRL  
check improves the security of Cisco Virtual Office spokes when spoke-  
to-spoke communication is permitted. However, it can be disabled for  
Cisco Virtual Office spokes if they connect to the hub only by issuing  
a revocation-check none command. !!!  
  
revocation-check crl  
  
!!! To send enrollment requests securely, the router should use the  
internal address as the source when communicating with the certificate  
server. As defined in the Cisco Virtual Office spoke configuration,  
only the internal addresses are secured. !!!  
  
source-interface Vlan10  
  
!!! The router will attempt reenrollment after 60 percent of lifetime  
expires. If shorter lifetimes, such as 60 days, are used for router  
certificates, the auto-enroll period can be extended to 80 or 90  
percent to avoid frequent reenrollment. !!!  
  
auto-enroll 60  
  
!!! Authenticate the client router with the certificate server, to  
download the root CA certificate so that the router will encrypt the  
enrollment request with the certificate server's public key. !!!
```

```
cvo-spoke(config)#crypto pki authenticate cvo-pki-cs
```

```
!!! Now enroll with the certificate server in config mode. Including  
the serial number and IP address in the subject name and password  
fields is optional. !!!
```

```
cvo-spoke(config)#crypto pki enroll cvo-pki-cs
```

```
!!! After the certificate is received, this message will pop up in the  
console !!!
```

```
"%PKI-6-CERTRET: Certificate received from Certificate Authority"
```

```
!!! Now save the configuration to make sure the certificate is stored  
!!!
```

When enrolled, the router should have two certificates. One is its own certificate signed by the Cisco IOS Certificate Server, and the other is the root CA certificate. An example of output follows:

```
cvo-spoke#show crypto pki certificates
```

```
Certificate                               !!! Router certificate !!!  
Status: Available  
Certificate Serial Number (hex): 04  
Certificate Usage: General Purpose  
Issuer:  
  cn=cvo-pki-cs  
  ou=cvo  
  o=Cisco Systems  
  c=US  
  ea=admin@cisco.com  
Subject:  
  Name: cvo-spoke.cisco.com  
  Serial Number: FHK09312145  
  serialNumber=FHK09312145+hostname=cvo-spoke.cisco.com  
CRL Distribution Points:  
  http://10.1.1.100/cvo-pki-cs.crl  
Validity Date:  
  start date: 11:36:17 PDT May 01 2008  
  end   date: 11:38:04 PDT Jun 30 2008  
  renew date: 11:38:04 PST Jun 15 2008  
Associated Trustpoints: cvo-pki-cs  
  
CA Certificate                               !!! Root CA certificate !!!  
Status: Available  
Certificate Serial Number (hex): 01  
Certificate Usage: Signature  
Issuer:  
  cn=cvo-pki-cs  
  ou=cvo  
  o=Cisco Systems
```

```

c=US
ea=admin@cisco.com
Subject:
cn=cvo-pki-cs
ou=cvo
o=Cisco Systems
c=US
ea=admin@cisco.com
Validity Date:
start date: 11:38:04 PDT May 01 2008
end date: 11:38:04 PDT Jul 15 2008
Associated Trustpoints: cvo-pki-cs

```

```
cvo-spoke#
```

A similar trustpoint configuration is required in the hub router for enrolling with the CS, and is shown as follows. When the certificate is received, both hub and spoke can use this certificate for PKI authentication.

```

crypto pki trustpoint cvo-pki-cs
enrollment url http://cvo-pki-cs:80
serial-number
ip-address none
revocation-check crl    !!! CRL checking enabled in DMVPN hub !!!
auto-enroll 60

```

### Configuring Conditional CRL Check

In Cisco Virtual Office, spoke-to-spoke router connections are permitted, and this can allow unauthorized spokes to set up secure connections with authorized spokes within the network. It is advisable to revoke the router certificates for spokes that become unauthorized—for example, when a Cisco Virtual Office user no longer works for the enterprise. Please refer to Appendix B for examples of how to revoke certificates. In these cases, the authorized spokes need to check the CRL database periodically to identify spokes that are invalid. However, the CRL database is typically placed behind the management gateway. Hence, the routers must set up a secure connection to the management gateway to access the CRL database. After the trustpoint in a spoke is configured to check the CRLs, the spoke needs to access the CRL database to bring up any secure connection, including the secure connection to the management gateway. If the management tunnel is cleared or the spoke is reloaded, the secure connection to the management gateway will fail because the CRL cannot be downloaded.

As mentioned earlier, spokes do not need to check the validity of VPN gateway certificates because they reside within the secured network and are supposed to be valid at all times. To allow spokes to check CRLs except for specific certificates such as gateways, use the CLI to enter the match certificate command with the skip revocation-check keyword.

**Note:** Only the relevant configuration is shown here. The rest of the configuration presented earlier in the document is still required.

```
Trustpoint config in management gateway:
```

```
-----
```

```

crypto pki trustpoint cvo-pki-cs
  subject-name cn=cvo_smg      !!! Certificate is generated with
  identification !!!
  revocation-check crl

Trustpoint config in Cisco Virtual Office spoke:
-----
!!! The following spoke configuration will disable CRL checking for
the management gateway but allow CRL checking for all other
connections !!!
crypto pki trustpoint cvo-pki-cs
  revocation-check crl
  match certificate check-crl skip revocation-check  !!! Spoke will
  skip CRL checking for management gateway !!!
!
crypto pki certificate map check-crl 1
  subject-name co cn=cvo_smg    !!! Peer certificate is verified for
  this subject-name !!!
!

```

### Configuring Certificate Rollover

Cisco Virtual Office routers (clients) can renew their router certificates by reenrolling with the Cisco IOS Certificate Server before the existing router certificates expire. The timing of reenrollment is based on the auto-enroll configuration as discussed earlier. The validity of a router certificate is always bound by the lifetime of the root CA certificate. During any enrollment, the validity of the router certificate cannot be extended beyond the lifetime of the root CA certificate. However, a router can reenroll itself until the validity of the router certificate expires along with root CA certificate. After the root CA certificate expires, the router cannot successfully reenroll further. Either configure the certificate server certificate with a larger lifetime initially to allow longer validity or obtain a new certificate by reconfiguring both the certificate server and all routers as discussed earlier.

With Cisco IOS Software Release 12.4(4)T and later, the root CA certificate can be rolled over by the certificate server, a process by which the certificate server generates a shadow (or rollover) root CA certificate before the existing root CA certificate expires. Though the validity of the shadow root CA certificate starts at the expiration of the existing root CA certificate, the certificate server keeps both the root certificates for an overlapping period (or rollover period). During this overlapping period, all routers will reenroll with the certificate server and download the shadow root CA certificate along with shadow router certificates for further use. After the existing certificate expires, both the certificate server and the routers will delete the expired certificate and start using the shadow (or rolled over) certificate. In this way, root CA certificate rollover helps Cisco Virtual Office routers keep their certificates valid without incurring additional overhead for administrators to reconfigure.

To use certificate rollover, configure the certificate server as follows:

```

crypto pki server cvo-pki-cs
  auto-rollover 5      !!! Five-day overlapping period for keeping
  shadow certificate !!!

```

No specific configuration is required in client routers; they will use the same process for reenrolling their router certificates. The routers will then determine whether the validity period of their certificates ends at the same time as the validity period of the root CA certificate. If so, they will download the shadow root CA certificate along with shadow router certificates. Shadow certificates are identified by the word rollover next to the certificate title.

Rollover can be performed manually by reenrolling during the rollover period.

```
cvo-spoke(config)#crypto pki enroll cvo-pki-cs
Trustpoint cvo-pki-cs is in rollover mode.
If you successfully re-enroll this trustpoint,
a shadow certificate will be obtained.
This will not effect the router certificate.
```

```
Do you want to continue with re-enrollment? [yes/no]: yes
Shadow enrollment will begin in 30 seconds and will
proceed in the background. You will be prompted to save
the configuration when the shadow enrollment completes
```

```
cvo-spoke#show crypto pki certificates cvo-pki-cs
Router Certificate (Rollover)          !!! Shadow router
certificate !!!
  Status: Available
  Certificate Serial Number: 2F
  ...
  Validity Date:
    start date: 11:38:04 PDT Jul 15 2008    !!! Validity period
starts later !!!
    end   date: 11:38:04 PDT Sep 13 2008
  Associated Trustpoints: cvo-pki-cs

CA Certificate (Rollover)              !!! Shadow root CA
certificate !!!
  Status: Available
  Certificate Serial Number: 23
  ...
  Validity Date:
    start date: 11:38:04 PDT Jul 15 2008
    end   date: 11:38:04 PDT Sep 28 2008
  Associated Trustpoints: cvo-pki-cs

cvo-spoke(config)#
```

**Note:** If the **database archive** command is configured in the certificate server, remember to store the pkcs12 file in a secure location after the certificate server generates rollover keys and certificates.

### Managing the Certificate Database

As shown in the certificate server configuration earlier, the **database level complete** command creates .crt and .cnm files for each certificate issued, requiring a very large storage capacity when

hundreds of routers are enrolling with the certificate server. With Cisco IOS Software Release 12.4(2)T and later, this database can be split and stored in different locations for different type of files. For example, .crl and .ser files are essential for running the certificate server, so they can be stored within the certificate server router flash memory. The certificate files .crt and .cnm are huge, so they can be stored on an external FTP server. CRLs can also be stored on an external HTTP server, from which routers can download them.

**Note:** This configuration is optional, depending on user requirements for the database level and the size of the network.

```
!!! The following configuration shows the .crt and .cnm file types
stored on an FTP server and all other file types-.ser, .crl, and .p12-
stored by default in flash memory. !!!
crypto pki server cvo-pki-cs
  database level complete
  database url flash:
  database url cnm ftp://10.1.1.100/pkifiles
  database url crl publish ftp://10.1.1.100/pkifiles  !!! CRL is
published on the FTP server !!!
  database url crt ftp://10.1.1.100/pkifiles
```

At this point, integration of PKI with Cisco Virtual Office is complete. This configuration may be good enough for a smaller Cisco Virtual Office network running with a single PKI server. For larger networks distributed across multiple locations, PKI servers can also be configured to form a hierarchy using subordinate certificate servers or RA mode certificate servers. Please refer to [http://www.cisco.com/en/US/products/ps6664/products\\_ios\\_protocol\\_option\\_home.html](http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html) for information about the various roles of PKI servers.

Following is just a portion of the configuration for a subordinate certificate server deployed with a root certificate server for Cisco Virtual Office. It follows the same configuration procedures as the root certificate server except the routers use trustpoint configuration for the subordinate certificate server.

### Configuring a Subordinate Certificate Server

Because the root RSA key pairs are extremely important in a PKI hierarchy, it is often advantageous to keep them offline or archived. To support this requirement, PKI hierarchies allow for subordinate CAs that have been signed by the root authority. In this way, the root authority can be kept offline (except to issue occasional CRL updates), and the subordinate CA can be used during normal operation.

The Subordinate Certificate Server feature allows you to configure a subordinate certificate server to grant all or certain SCEP enrollment or manual certificate requests.

The subordinate certificate server provides all the same features as a root certificate server. Following are some points to remember when adding a subordinate certificate server:

- Enrollment requests that come from a subordinate certificate server must always be **manually** granted in the root certificate server.
- The root certificate server should be a Cisco IOS Certificate Server.

The same steps as for configuring the Cisco IOS Certificate Server described earlier are required to set up a subordinate certificate server: IP reachability to the root certificate server; access to other resources such as NTP, FTP, and DNS servers; IP HTTP server configuration; RSA keys generated; etc.

**Note:** Only the relevant configuration information is shown here; all other configuration details are required as for the root certificate server.

```

!!! The following trustpoint configuration should be created manually
before enabling subordinate certificate server to provide a valid
enrollment URL to the root certificate server !!!
crypto pki trustpoint cvo-pki-subcs
  enrollment url http://cvo-pki-cs:80          !!! Enrolls with root
certificate server !!!
  serial-number
  revocation-check crl
  rsakeypair cvo-pki-subcs
!
crypto pki server cvo-pki-subcs
  database level complete
  database archive pkcs12 password cisco123
  grant auto          !!! Enrollment requests are automatically
granted !!!
  lifetime crl 24
  lifetime certificate 45      !!! Valid period for router certificates
!!!
  lifetime ca-certificate 60 !!! Validity must match lifetime
certificate defined in root certificate server !!!
  cdp-url http://10.1.1.100/cvo-pki-subcs.crl
  mode sub-cs          !!! Certificate server runs in subordinate
certificate server mode!!!
  database url flash:
!

```

```

!!! The following configuration shows the client routers using a
subordinate certificate server trustpoint. The rest of the
configuration is still needed !!!
!
ip host cvo-pki-subcs 10.1.1.102
!
crypto pki trustpoint cvo-pki-subcs
  enrollment url http://cvo-pki-subcs:80
  serial-number
  revocation-check crl
  source interface Vlan10
  auto-enroll 60
!
!!! The subordinate certificate server is enabled by entering the "no
shut" command in server config mode. !!!
!
cvo-pki-subcs(cs-server)#no shutdown
!

```

### Configuring Certificate Rollover for the Subordinate Certificate Server

If certificate rollover is set up for the root certificate server, it should also be set up for the subordinate certificate server because all the routers will enroll with the subordinate certificate server. From the perspective of the root certificate server, the subordinate certificate server is also a client. Just as routers keep shadow certificates for their own certificates and also for the root CA certificate, the subordinate certificate server also downloads shadow certificates for itself and the root certificate server during rollover. Although enrollment requests that the root certificate server receives from the subordinate certificate server must be granted manually, the root certificate server can automatically grant rollover enrollment requests from the subordinate certificate server.

```

!!! The following configuration is needed in the root certificate
server !!!
!
crypto pki server cvo-pki-cs
  grant auto rollover ca-cert  !!! Root certificate server
  automatically grant rollover requests from subordinate certificate
  server !!!
  auto-rollover 5          !!! Overlapping period to keep shadow
  certificates !!!
!
!!! The following configuration is needed in subordinate certificate
server !!!
!
crypto pki server cvo-pki-subcs
  auto-rollover 4          !!! Four-day overlapping period to keep shadow
  certificates !!!

```

As earlier, no additional configuration is needed in Cisco Virtual Office routers for certificate rollover.

**Note:** The rollover period in the root certificate server should be longer than the rollover period in the subordinate certificate server. Because the subordinate certificate server itself is a client for

the root certificate server, root certificate server rollover may occasionally occur at the same time as subordinate certificate server rollover. If the subordinate certificate server rollover period occurs before the root certificate server rollover period, the subordinate certificate server can have only a subordinate certificate server rollover certificate because the root certificate server rollover certificate is not generated at that time. This may cause the subordinate certificate server to reenroll, and all the router clients as well. To avoid this situation, you should keep the rollover period longer in the root certificate server than in the subordinate certificate server. Then the subordinate certificate server will receive both the subordinate certificate server and root certificate server rollover certificates during the same enrollment. You should also use higher values for lifetime ca-certificate in the root certificate server to avoid frequent rollovers in the subordinate certificate server as a result of root certificate server rollover.

**Note:** Refer to Appendix B for detailed output.

```
cvo-pki-subcs#sh crypto pki certificates
Certificate (subordinate CA certificate)   !!! Existing subordinate CA
certificate !!!
    Status: Available
    Certificate Serial Number: 0C
    ...
Certificate (subordinate CA certificate, Rollover)   !!! Rollover
certificate !!!
    Status: Available
    Certificate Serial Number: 11
    ...
cvo-pki-subcs#
```

### PKI-AAA Authentication and Authorization

Security on the Cisco Virtual Office hub router can be strengthened by configuring PKI-AAA authorization in addition to CRL validation for each peer certificate. When a Cisco Virtual Office spoke negotiates an IPsec session with the hub, the hub router extracts a specified field from the peer certificate's subject and sends it to a RADIUS server. This field is sent as the username, and the password is preconfigured. The field that is sent as the username is specified in the trust point configuration; by default, it is the subject name, which is a fully qualified domain name.

If the RADIUS server has an entry for this username with the password set as "cisco," the query returns successfully along with the following Cisco attribute-value pairs configured for that username:

- Certificate use (cert-application)
- Certificate trustpoint (cert-trustpoint)
- Serial number (cert-serial)
- Certificate lifetime (cert-lifetime-end)

The RADIUS server returns a failure if the record is not found or the password is not "cisco." The peer certificate is not accepted if the RADIUS request fails.

If either or both cert-trustpoint and cert-serial are specified, the router compares these values with the trustpoint name and serial number extracted from the peer certificate. The certificate is accepted only if these fields match. The cert-lifetime-end value can be used to bypass the actual expiry date of the certificate—useful when an expired peer certificate needs to be accepted. A different date can be specified in the attribute-value pair and the router uses this for the expiry date calculation.

With the PKI-AAA feature, the hub accepts a certificate only if it has an entry on the RADIUS server. For more information about PKI-AAA, please refer to [http://www.cisco.com/en/US/docs/ios/12\\_3/feature/guide/g\\_pkii.html](http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/g_pkii.html).

Here is the PKI-AAA configuration:

```
aaa new-model
aaa group server radius pki-aaa-server
server <ip addr> auth-port 1812 acct-port 1813 key cisco123
!
aaa authorization network pkiaaa group pki-aaa-server
!
crypto pki trustpoint cvo-pki-subcs
enrollment url http://cvo-pki-subcs:80
authorization list pkiaaa
```

### Benefits of PKI Integration

- PKI integration reduces the need for complex management of preshared keys for Cisco Virtual Office routers.
- Security of the Cisco Virtual Office router can be increased by the use of RSA keys that are nonexportable and CRL checking to prevent sessions from unauthorized devices.
- Root certificate rollover helps the Cisco Virtual Office router renew and keep valid certificates.
- The use of a subordinate certificate server with certificate rollover extends the benefit of prolonged validity of router certificates to the hierarchical design of certificate servers for widely distributed Cisco Virtual Office networks.
- PKI integration with AAA protects Cisco Virtual Office hubs with even more security.

### Caveats/Final Notes

- A certificate server using RA mode cannot get rollover certificates automatically.
- To disconnect a user from Cisco Virtual Office, just revoking the router certificate in the certificate server is not sufficient because the hub or spokes may not get the latest CRL immediately. Hence, it is strongly recommended that the administrator manually remove the certificate from the router as well. Users can use shorter lifetimes for CRL publishing to get new CRLs published frequently. Integrating the PKI-AAA feature also helps reject session requests from disconnected spokes.
- When performing CRL checking, if the CRL is published to an internal FTP or HTTP server, IPsec sessions will fail between Cisco Virtual Office routers if the FTP or HTTP server is not

---

accessible. Hence, place the CRL in an externally accessible HTTP server or use an LDAP server.

- If Cisco Virtual Office routers lose connection with the root certificate server or subordinate certificate server during a rollover period and shadow certificates are not installed, automatic recovery is not possible. The administrator can manually reenroll to obtain shadow certificates, but if the certificate server certificate has expired, trustpoint configuration in the Cisco Virtual Office routers should be removed and reinstalled for a fresh enrollment.
- If the Cisco Virtual Office routers use the same trustpoint configuration to connect to the management gateway and to DMVPN data gateways, having an expired or invalid certificate will disconnect the user from the entire Cisco Virtual Office network. It is advisable to use different trustpoints when connecting to management and DMVPN data gateways to permit the network administrator restore the certificates securely.
- The administrator should consider any performance concerns related to PKI before deploying this solution in a large-scale network.

## References

- PKI Deployment  
[http://www.cisco.com/en/US/products/ps6664/products\\_ios\\_protocol\\_option\\_home.html](http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html)
- Implementing and Managing PKI—Cisco Documentation  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec\\_c/part20/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part20/index.htm)
- PKI-AAA [http://www.cisco.com/en/US/docs/ios/12\\_3/feature/guide/g\\_pkii.html](http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/g_pkii.html)
- Cisco Virtual Office Deployment Guides <http://www.cisco.com/go/cvo>
- Integrated EasyVPN and Dynamic Multipoint VPN  
[http://www.cisco.com/en/US/products/ps6660/products\\_white\\_paper0900aecd80267995.shtml](http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd80267995.shtml)
- Layered Security in a VPN Deployment  
[http://www.cisco.com/en/US/products/ps6660/products\\_white\\_paper0900aecd8046cbc4.shtml](http://www.cisco.com/en/US/products/ps6660/products_white_paper0900aecd8046cbc4.shtml)

## Appendix A: Configuration

### Root Certificate Server—Cisco 2800 Series Integrated Services Router

#### Full Configuration

```
cvo-pki-cs#sh startup-config
Using 2731 out of 29688 bytes
!
!
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname cvo-pki-cs
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret <removed>
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
ip cef
!
ip ftp username ftpusr
ip ftp password <removed>
no ip domain lookup
ip domain name cisco.com
ip host cvo-pki-cs 10.1.1.105
ip host ftpserver 10.1.1.100
!
crypto pki server cvo-pki-cs
database level complete
```

```
database archive pkcs12 password <removed>
 issuer-name cn=cvo-pki-cs,ou=cvo,o=Cisco
 Systems,c=US,ea=admin@cisco.com
 grant auto rollover ca-cert
 grant auto
 lifetime crl 24
 lifetime certificate 60
 lifetime ca-certificate 75
 cdp-url http://10.1.1.100/cvo-pki-cs.crl
 auto-rollover 5
 database url flash:
 database url cnm flash:
 database url crl publish ftp://10.1.1.100/pkifiles
 database url crt ftp://10.1.1.100/pkifiles
 !
 crypto pki trustpoint cvo-pki-cs
 enrollment url http://cvo-pki-cs:80
 serial-number
 revocation-check crl
 rsakeypair cvo-pki-cs
 !
 !
 crypto pki certificate chain cvo-pki-cs
 certificate ca rollover 11 nvram:cvo-pki-cs#7311.cer
 certificate ca 0B nvram:cvo-pki-cs#730BCA.cer
 !
 no crypto provisioning petitioner
 no crypto engine aim 0
 !
 !
 no crypto isakmp enable
 !
 interface FastEthernet0/0
 ip address 10.1.1.105 255.255.255.0
 duplex auto
 speed auto
 !
 interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 !
 ip default-gateway 10.1.1.101
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.101
 !
 !
 ip http server
 no ip http secure-server
```

```

!
control-plane
!
alias exec cert sh cry ca cer | i (Serial|Usage|end|Associated|Status)
alias exec i sh ip int brief
alias exec ss sh cry is sa
alias exec rr show run brie
alias exec r show runn
alias exec c config t
alias exec scr show run | b crypto isakmp
!
line con 0
line aux 0
line vty 0 4
  exec-timeout 0 0
!
ntp clock-period 17208480
ntp server 10.1.1.101
!
end

cvo-pki-cs#

```

### Subordinate Certificate Server—Cisco 2800 Series Integrated Services Router

#### Full Configuration

```

cvo-pki-subcs#show startup-config
Using 2881 out of 245752 bytes
!
!
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname cvo-pki-subcs
!
boot-start-marker
boot-end-marker
!
logging buffered 24000 debugging
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local

```

```
!
aaa session-id common
!
clock timezone PST -8
clock summer-time PDT recurring
!
!
ip cef
!
!
ip ftp username ftpusr
ip ftp password <removed>
ip domain name cisco.com
ip host cvo-pki-cs 10.1.1.105
ip host ftpserver 10.1.1.100
ip host cvo-pki-subcs 10.1.1.106
ip name-server <corporate_dns_address>
ip name-server <corporate_dns_address>
!
!
voice-card 0
  no dspfarm
!
!
crypto pki server cvo-pki-subcs
  database level complete
  grant auto
  lifetime crl 24
  lifetime certificate 50
  lifetime ca-certificate 60
  cdp-url http://10.1.1.100/cvo-pki-subcs.crl
  mode sub-cs
  auto-rollover 4
  database url flash:
  database url cnm ftp://10.1.1.100/pkifiles
  database url crl publish ftp://10.1.1.100/pkifiles
  database url crt ftp://10.1.1.100/pkifiles
!
crypto pki trustpoint cvo-pki-subcs
  enrollment url http://cvo-pki-cs:80
  serial-number
  revocation-check crl
  rsakeypair cvo-pki-subcs
!
!
crypto pki certificate chain cvo-pki-subcs
  certificate 0C nvram:cvo-pki-cs#730C.cer
  certificate ca 0B nvram:cvo-pki-cs#730BCA.cer
!
```

```
!  
interface FastEthernet0/0  
  ip address 10.1.1.106 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Async0/0/0  
  no ip address  
  encapsulation slip  
  shutdown  
!  
interface Async0/0/1  
  no ip address  
  encapsulation slip  
  shutdown  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.1.101  
!  
!  
ip http server  
no ip http secure-server  
!  
!  
control-plane  
!  
credentials  
!  
alias exec cert sh cry ca cer | i (Serial|Usage|end|Associated|Status)  
alias exec i sh ip int brief  
alias exec ss sh cry is sa  
alias exec rr show run brie  
alias exec r show runn  
alias exec c config t  
alias exec scr show run | b crypto isakmp  
!  
line con 0  
line aux 0  
line 0/0/0 0/0/1  
  stopbits 1  
  speed 115200  
  flowcontrol hardware  
line vty 0 4
```

---

```
!  
scheduler allocate 20000 1000  
ntp clock-period 17179839  
ntp server 10.1.1.101  
!  
end  
  
cvo-pki-subcs#
```

## Appendix B: Verification and Troubleshooting

### Root Certificate Server

```
cvo-pki-cs#show crypto pki server    !!! Certificate server status and
details !!!
```

```
Certificate Server cvo-pki-cs:
  Status: enabled
  State: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: cn=cvo-pki-cs,ou=cvo,o=Cisco
systems,c=US,ea=admin@cisco.com
  CA cert fingerprint: 933C312F 17290BA3 A7179EDE FE2C6E7E
  Granting mode is: auto
  Last certificate issued serial number: 0x2F
  CA certificate expiration timer: 11:38:04 PST Jul 15 2008
  CRL NextUpdate timer: 15:59:49 PDT Jun 28 2008
  Current primary storage dir: flash:
  Current storage dir for .cnm files: flash:
  Current storage dir for .crt files: ftp://10.1.1.100/pkifiles
  Database Level: Complete - all issued certs written as
<serialnum>.cer
  Auto-Rollover configured, overlap period 5 days
  Autorollover timer: 11:38:04 PST Jul 10 2008
```

```
!!! Check root CA certificate details !!!
```

```
cvo-pki-cs#show crypto pki certificates
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 0x1
  Certificate Usage: Signature
  Issuer:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Subject:
    cn=cvo-pki-cs
    ou=CVO
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Validity Date:
    start date: 11:38:04 PDT May 01 2008
    end   date: 11:38:04 PDT Jul 15 2008
  Associated Trustpoints: cvo-pki-cs
  Storage: nvram:cvo-pki-cs#1CA.cer
```

```

!!! RSA keys generated in certificate server !!!
cvo-pki-cs#show crypto key mypubkey rsa
% Key pair was generated at: 11:38:42 PDT May 01 2008
Key name: cvo-pki-cs
  Storage Device: not specified
  Usage: General Purpose Key
  Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181
00BC33EA
  .....<key data removed>
% Key pair was generated at: 11:38:42 PDT May 01 2008
Key name: cvo-pki-cs.server
Temporary key
  Usage: Encryption Key
  Key is not exportable.
Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B01B54
C037B330
  ....<key data removed>
cvo-pki-cs#

```

!!! To perform any server activities, use this CLI command. There are some differences between Cisco IOS Software Releases 12.4(15)T and 12.4(20)T. Examples given below are for essential options only. !!!

```

!!! For Cisco IOS Software Release 12.4(15)T !!!
cvo-pki-cs#cry pki server cvo-pki-cs ?
  grant      Grant enrollment requests
  info       Display info
  password   One Time Password for SCEP enrollment
  reject     Reject enrollment requests
  remove     Remove enrollment requests from database
  request    Retrieve an enrollment request
  revoke     Revoke certificate

cvo-pki-cs#

```

```

!!! To check any pending enrollment requests !!!
cvo-pki-cs#crypto pki server ect-pki-cs info request

```

```

!!! For Cisco IOS Software Release 12.4(20)T !!!
cvo-pki-cs#crypto pki server cvo-pki-cs ?
  grant      Grant enrollment requests
  password   One Time Password for SCEP enrollment
  reject     Reject enrollment requests
  remove     Remove enrollment requests from database
  request    Retrieve an enrollment request
  revoke     Revoke certificate
  trim       Trim the CRL based on the expired-certs file.
  unrevoke   Unrevoke certificate

```

```
cvo-pki-cs#
```

```
!!! To check issued certificates, CRL and pending enrollment requests  
!!!
```

```
cvo-pki-cs#show cry pki server cvo-pki-cs ?  
  certificates  Show certificates issued by this Certificate Server  
  crl           Certificate Revocation List  
  requests     Enrollment Requests  
  |            Output modifiers  
<cr>
```

```
!!! The following commands are the same on both versions !!!
```

```
!!! To manually grant enrollment requests !!!
```

```
cvo-pki-cs#crypto pki server cvo-pki-cs grant ?  
  <1-999> Request ID  
  all      all pending requests      !!! Grant all pending request  
!!!  
cvo-pki-cs#
```

```
!!! To revoke router certificate with serial number 0xDD, use this CLI  
command. This will publish a new CRL to the HTTP server, but the  
router can download this new CRL only if a CRL is not already  
available in the router cache !!!
```

```
cvo-pki-cs#crypto pki server cvo-pki-cs revoke 0xDD  
writing crl ...
```

```
!!! To reject any specific enrollment requests !!!
```

```
cvo-pki-cs#crypto pki server cvo-pki-cs reject ?  
  <1-999> Request ID  
  all      all pending requests
```

```
!!! During rollover period, the certificate server installs shadow  
certificates !!!
```

```
cvo-pki-cs#sh crypto pki certificates  
CA Certificate  
  Status: Available  
  Certificate Serial Number: 0x1  
  Certificate Usage: Signature  
  Issuer:  
    cn=cvo-pki-cs  
    ou=cvo  
    o=Cisco Systems  
    c=US  
    ea=admin@cisco.com  
  Subject:  
    cn=cvo-pki-cs  
    ou=cvo  
    o=Cisco Systems  
    c=US
```

```

    ea=admin@cisco.com
Validity Date:
    start date: 11:38:04 PDT May 01 2008
    end   date: 11:38:04 PDT Jul 15 2008
Associated Trustpoints: cvo-pki-cs
Storage: nvram:cvo-pki-cs#1CA.cer

```

```

CA Certificate (Rollover)                !!! Shadow root CA
certificate !!!
Status: Available
Certificate Serial Number: 0x13
Certificate Usage: Signature
Issuer:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea= admin@cisco.com
Subject:
    Name: cvo-pki-cs
    cn=cvo-pki-cs
    ou= cvo
    o=Cisco Systems
    c=US
    ea= admin@cisco.com
CRL Distribution Points:
    http://10.1.1.100/cvo-pki-cs.crl
Validity Date:
    start date: 11:38:04 PDT Jul 15 2008    !!! Note the validity !!!
    end   date: 11:38:04 PDT Sep 28 2008
Associated Trustpoints: cvo-pki-cs
Storage: nvram:cvo-pki-cs#10.cer

```

### Subordinate Certificate Server

```

!!! Subordinate CA certificate with rollover !!!
cvo-pki-subcs#sh crypto pki certificates
Certificate (subordinate CA certificate)    !!! Existing subordinate
server certificate !!!
Status: Available
Certificate Serial Number: 0xC
Certificate Usage: Signature
Issuer:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
Subject:
    cn=cvo-pki-subcs
    ou=cvo

```

```
o=Cisco Systems
c=US
ea=admin@cisco.com
CRL Distribution Points:
  http://10.1.1.100/cvo-pki-cs.crl
Validity Date:
  start date: 11:38:04 PDT May 01 2008
  end   date: 11:38:04 PDT Jun 30 2008
Associated Trustpoints: cvo-pki-subcs
Storage: nvram:cvo-pki-cs#C.cer
```

CA Certificate  
certificate !!!

!!! Existing root CA

```
Status: Available
Certificate Serial Number: 0xB
Certificate Usage: Signature
Issuer:
  cn=cvo-pki-cs
  ou=cvo
  o=Cisco Systems
  c=US
  ea=admin@cisco.com
Subject:
  cn=cvo-pki-cs
  ou=cvo
  o=Cisco Systems
  c=US
  ea=admin@cisco.com
Validity Date:
  start date: 11:38:04 PDT May 01 2008
  end   date: 11:38:04 PDT Jul 15 2008
Associated Trustpoints: cvo-pki-subcs
Storage: nvram:cvo-pki-cs#BCA.cer
```

Certificate (subordinate CA certificate, Rollover) !!! Shadow  
subordinate server certificate !!!

```
Status: Available
Certificate Serial Number: 0x11
Certificate Usage: Signature
Issuer:
  cn=cvo-pki-cs
  ou=cvo
  o=Cisco Systems
  c=US
  ea=admin@cisco.com
Subject:
  cn=cvo-pki-subcs
  ou=cvo
  o=Cisco Systems
  c=US
```

```

    ea=admin@cisco.com
CRL Distribution Points:
  http://10.1.1.100/cvo-pki-cs.crl
Validity Date:
  start date: 11:38:04 PDT Jun 30 2008
  end   date: 11:38:04 PDT Jul 15 2008 !!! Validity expires along
with root CA certificate !!!
  Associated Trustpoints: cvo-pki-subcs
  Storage: nvram:cvo-pki-cs#11.cer

cvo-pki-subcs#

```

### Router Clients with Subordinate Certificate Server Trustpoint

```

cvo-spoke#sh crypto pki certificates cvo-pki-subcs
Certificate
  Status: Available
  Certificate Serial Number (hex): 10
  Certificate Usage: General Purpose
  Issuer:
    cn=cvo-pki-subcs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Subject:
    Name: cvo-spoke.cisco.com
    Serial Number: FHK09312145
    serialNumber=FHK09312145+hostname=cvo-spoke.cisco.com
  CRL Distribution Points:
    http://10.1.1.100/cvo-pki-subcs.crl
  Validity Date:
    start date: 11:38:04 PDT May 01 2008
    end   date: 11:38:04 PDT Jun 15 2008
    renew date: 11:38:04 PDT May 26 2008
  Associated Trustpoints: cvo-pki-subcs

```

```

CA Certificate                                     !!! Subordinate CA certificate !!!
  Status: Available
  Certificate Serial Number (hex): C
  Certificate Usage: Signature
  Issuer:
    cn=cvo-pki-cs
    ou=cvo
    o=Cisco Systems
    c=US
    ea=admin@cisco.com
  Subject:
    cn=cvo-pki-subcs
    ou=cvo
    o=Cisco Systems

```

```
c=US
ea=admin@cisco.com
CRL Distribution Points:
  http://10.1.1.100/cvo-pki-cs.crl
Validity Date:
  start date: 11:38:04 PDT May 01 2008
  end   date: 11:38:04 PDT Jun 30 2008
Associated Trustpoints: cvo-pki-subcs
```

!!! During subordinate certificate server rollover period !!!

```
cvo-spoke#sh crypto pki certificates cvo-pki-subcs
Router Certificate (Rollover)          !!! Shadow router
certificate !!!

Status: Available
Certificate Serial Number (hex): 1B
Certificate Usage: General Purpose
Issuer:
  cn=cvo-pki-cs
  ou=cvo
  o=Cisco Systems
  c=US
  ea= admin@cisco.com
Subject:
  Name: cvo-spoke.cisco.com
  Serial Number: FHK09312145
  serialNumber=FHK09312145+hostname=cvo-spoke.cisco.com
CRL Distribution Points:
  http://10.1.1.100/cvo-pki-subcs.crl
Validity Date:
  start date: 11:38:04 PDT Jun 30 2008      !!! Validity starts at
subordinate CA certificate rollover !!!
  end   date: 11:38:04 PDT Jul 15 2008      !!! Valid until root CA
certificate expires !!!
Associated Trustpoints: cvo-pki-subcs
```

```
Certificate (subordinate CA certificate, Rollover)  !!! Shadow
subordinate CA certificate !!!

Status: Available
Certificate Serial Number (hex): 11
Certificate Usage: Signature
Issuer:
  cn=cvo-pki-cs
  ou=cvo
  o=Cisco Systems
  c=US
  ea=admin@cisco.com
Subject:
  cn=cvo-pki-subcs
  ou=cvo
  o=Cisco Systems
```

```
c=US
ea=admin@cisco.com
CRL Distribution Points:
  http://10.1.1.100/cvo-pki-cs.crl
Validity Date:
  start date: 11:38:04 PDT Jun 30 2008
  end   date: 11:38:04 PDT Jul 15 2008   !!! Validity expires along
with root CA certificate !!!
Associated Trustpoints: cvo-pki-subcs
Storage: nvram:cvo-pki-cs#11.cer
cvo-spoke#
```

### Debug Commands

The following debug commands are useful for certificate server and router clients.

```
debug crypto pki server
debug crypto pki transactions
```



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0807R)