Contents

Introduction

This document describes how the Cisco IOS® Public Key Infrastructure (PKI) operations of auto-enrollment and auto-rollover work and how the respective PKI timers are calculated for these operations.

Certificates have fixed lifetimes and expire at some point. If the certificates are used for authentication purposes for a VPN solution (for example), the expiry of these certificates leads to possible authentication failures that result in loss of VPN connectivity between the endpoints. In order to avoid this issue, these two mechanisms are available for automatic certificate renewal:

- Auto-Enrollment for the client/spoke routers
- Auto-Rollover for the Certification Authority (CA) server router

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- PKI and the concept of trust
- Basic configuration of CA on routers

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Terminology

auto-enrollment

When a certificate on an end device is about to expire, auto-enrollment obtains a new certificate without disruption. When auto-enrollment is configured, the client/spoke router can request a new certificate at some time before its own certificate (known as its identity or ID certificate) expires.

auto-rollover

This parameter decides when the Certificate Server (CS) generates its rollover (shadow) certificate; if the command is entered under the CS configuration without any argument, the default time is 30 days.

> **Note**: For the examples in this document, the value of this parameter is *10 minutes*.

When a certificate on the CA server is about to expire, auto-rollover enables the CA to obtain a new certificate without disruption. When auto-rollover is configured, the CA router can generate a new certificate at some time before its own certificate expires. The new certificate, which is called the *shadow* or *rollover* certificate, becomes active at the precise moment that the current CA certificate expires.

With the use of the two features that are mentioned in the Introduction section of this document, the PKI deployment becomes automated and allows the spoke or client device to get a shadow/rollover identity certificate and shadow/rollover CA certificate prior to the current CA certificate expiry. This way, it can transition without interruption to the new ID and CA certificates when its current ID and CA certificates expire.

lifetime ca-certificate

This parameter specifies the lifetime of the CA certificate. The value of this parameter can be specified in days/hours/minutes.

> **Note**: *30 minutes*.

lifetime certificate

This parameter specifies the lifetime of the identity certificate that is issued by the CA router. The value of this parameter can be specified in days/hours/minutes.

> **Note**: *20 minutes*

Configure

Note: *lifetime*, *auto-rollover*, and *auto-enroll* are used in this document in order to illustrate key auto-enroll and auto-rollover concepts. In a live network environment, Cisco recommends that you use the default lifetimes for these parameters.

Tip: All of the PKI timer-based events, such as *rollover* and *reenrollment*, can be affected if there is no authoritative time source. For this reason, Cisco recommends that you configure Network Time Protocol (NTP) on all of the routers that peform PKI.

Cisco IOS CA Server Configuration

This section provides an example configuratinon for the Cisco IOS CA server.

```
RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up
```

Note: **auto-rollover** command is the number of days/hours/minutes *before the end date of the current CA certificate*that the rollover certificate is generated. Therefore, if a CA certificate is valid from 12:00 to 12:30, then **auto-rollover 0 0 10** implies that the rollover CA certificate is generated around 12:20.

Enter the **show crypto pki certificate** command in order to verify the configuration on the Cisco IOS CA server:

```
RootCA#show crypto pki certificate
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

Based on this output, the router includes a CA certificate that is valid from 9:16 to 9:46 IST Nov 25, 2012. Since auto-rollover is configured for 10 minutes, the shadow/rollover certificate is expected to be generated by *9.36 IST* Nov 25, 2012.

In order to confirm, enter the **show crypto pki timer** command:

```
RootCA#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:22.283 IST Sun Nov 25 2012
PKI Timers
| 12:50.930
| 12:50.930 SESSION CLEANUP
```

```
CS Timers
| 16:43.558
| 16:43.558  CS SHADOW CERT GENERATION
| 26:43.532 CS CERT EXPIRE
| 26:43.558 CS CRL UPDATE
```

Based on this output, the **show crypto pki timer** command was issued at 9.19 IST, and the shadow/rollover certificate is expected to be generated within 16.43 minutes:

[09:19:22 + 00:16:43] = **09:36:05**, which is the [end-date_of_current_CA_cert - auto_rollover_timer]; that is, [09:46:05 - 00:10:00] = **09:36:05**.

Client/Spoke Router Configuration

This section provides an example configuration for the client/spoke router.

```
Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up
```

> **Note**: The **auto-enroll** command enables the auto-enrollment feature on the router. The command syntax is: **auto-enroll** [*val%*] [*regenerate*].

In the previous output, the auto-enroll feature is specified as 70%; that is, at 70% of the **[lifetime of current_ID_cert]**, the router automatically reenrolls with the CA.

> **Tip**:

The *regenerate* option leads to the creation of a new Rivest-Shamir-Addleman (RSA) key for certificate reenrollment/renewal purposes. If this option is not specified, the current RSA key is used.

Auto-Enrollment In Action

Complete these steps in order to verify the auto-enrollment feature:

1. Enter the **crypto pki authenticate** command in order to manually authenticate the trustpoint on the client router:

   ```
   Client-1(config)#crypto pki authenticate client1
   ```

   Note: For more information on this command, refer to the Cisco IOS Security Command Reference.

   Once you enter the command, an output similar to this should appear:

   ```
   Client-1(config)#crypto pki authenticate client1
   ```

2. Type **yes** in order to accept the CA certificate on the client router. Then, a **RENEW** timer begins on the router:

   ```
   Client-1#show crypto pki timer
   ```

```
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. Once the **RENEW** timer reaches zero, the client router automatically enrolls itself with the CA in order to obtain its identity certificate. Once the certificate is received, enter the **show crypto pki certificate** command in order to view it:

```
Client-1#show crypto pki certificate
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:16:57 IST Nov 25 2012
end date: 09:36:57 IST Nov 25 2012
renew date: 09:30:08 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

The **renew date** is **09:30:08** and is calculated as shown here:

start-time + (%renewal of ID_cert_lifetime)

Or

09:16:57 + (70% * 20 minutes) = **09:30:08**

The PKI timers reflect the same:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:01.714 IST Sun Nov 25 2012
```

```
PKI Timers
| 1:21.790
| 1:21.790 SESSION CLEANUP
| 11:06.894  RENEW client1
```

4. Once the **RENEW** timer expires, the router reenrolls with the CA in order to obtain a new ID certificate. After a certificate renewal has occurred, enter the **show crypto pki cert** command in order to view the new ID certificate:

```
Client-1#show crypto pki cert
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:55.063 IST Sun Nov 25 2012
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

   Notice that there is no longer a *renew date*; instead, a **SHADOW** timer begins:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

Here is the process logic:

- If the end-date of the **ID** certificate **is not equal** to the end-date of the **CA** certificate, then calculate a renew-date based on the auto-enroll percentage and start the **RENEW** timer.

- If the end-date of the **ID** certificate **is equal** to the end-date of the **CA** certificate, then no renewal process is necessary since the current ID certificate is valid only as long as the current CA certificate is valid. Instead, a **SHADOW** timer is started.

This timer is also calculated based on the percentage mentioned in the **auto-enroll** command. For example, consider the validity dates of the renewed ID certificate that are shown in the previous example:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

The lifetime of this certificate is 16 minutes. Therefore, the rollover timer (that is, the SHADOW timer) is 70% of 16 minutes, which equals approximately 11 minutes. This calculation implies that the router begins requests for its shadow/rollover certificates at [09:30:09 + 00:11:00] = 09:41:09, which corresponds to the PKI SHADOW timer shown previously in this document:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922 IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618  SHADOW client1
```

Auto-Rollover In Action

This section describes the auto-rollover feature in action.

On the Cisco IOS CA Server

When the SHADOW timer expires, the rollover certificate appears on the CA router:

```
RootCA#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:36:28.184 IST Sun Nov 25 2012
CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
 start date: 09:46:05 IST Nov 25 2012
end   date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
CA Certificate
Status: Available
```

```
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

At the Client Router

As described previously in this document, the auto-enrollment feature began a SHADOW timer on the client router. When the SHADOW timer expires, the auto-enrollment feature enables the router to request the CA server for the *rollover/shadow CA* certificate. Once received, it queries for its *rollover/shadow ID* certificate as well. As a result, the router has two pairs of certificates: one pair that is current and the other pair that contains the rollover/shadow certificates:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
```

```
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Notice the validity of the rollover ID certificate:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
```

```
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

The certificate lifetime is just four minutes (instead of the expected 20 minutes, as configured on the Cisco IOS CA server). Per the Cisco IOS CA server, the *absolute* ID certificate lifetime should be 20 minutes (which means, for a given client router, the sum of the lifetimes of the ID certificates (current + shadow) issued to it must not be greater than 20 minutes).

This process is further described here:

- Here is the validity of the current ID certificate on the router:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
```

```
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Therefore, the *current_id_cert_lifetime* is 16 minutes.

- Here is the validity of the rollover ID certificate:

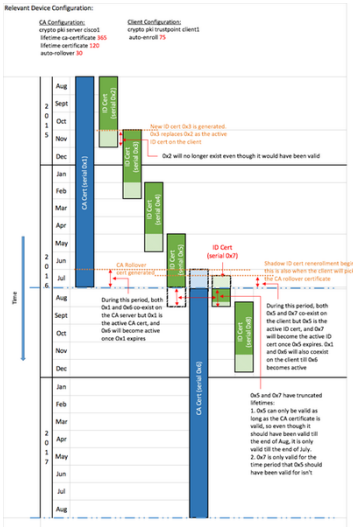
```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
```

```
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Therefore, the *rollover_id_cert_lifetime* is four minutes.

- Per the Cisco IOS, when the [current_id_cert_lifetime] is added to the [rollover_id_cert_lifetime], it must equal the [total_id_cert_lifetime]. This is true in this instance.

Sample PKI Timeline with Rollover and Enrollment



Important Considerations

- The PKI timers require an authoritative clock in order to function properly. Cisco recommends that you use NTP in order to synchronize clocks between the client routers and the Cisco IOS CA router. In the absence of NTP, the system/hardware clock on the router can be used. For information on how to configure the hardware clock and make it authoritative, refer to the Basic System Management Configuration Guide, Cisco IOS Release 12.4T.

- Upon the reload of a router, the synchronization of the NTP often takes a few minutes. However, the PKI timers are established almost immediately. As of Versions 15.2(3.8)T and 15.2(4)S, the PKI timers are automatically reevaluated after NTP is synchronized.

- The PKI timers are not absolute; they are based on the *remaining time* and are, therefore, recalculated after a reboot. For example, assume the client router has an ID certificate that is valid for 100 days and the auto-enroll feature is set to 80%. Then, reenrollment is expected to occur after the 80th day. If the router is reloaded on the 60th day, it boots up and recalculates the PKI timer as shown here: (*remaining time*) * (*%auto-enroll*) = (100-60) * 80% = 32 days.

  Therefore, reenrollment occurs on the [60 + 32] = 92nd day.

- When you configure the auto-enroll and auto-rollovertimers, it is important to configure them with values that allow SHADOW CA certificate availability on the PKI server when the PKI client requests one. This helps mitigate potential PKI services failures in a large-scale environment.

Related Information

- **Deploying Cisco IOS Security with a Public-Key Infrastructure Whitepaper**
- **Public Key Infrastructure: Deployment Benefits and Features Whitepaper**
- **Public Key Infrastructure Configuration Guide**
- **Technical Support & Documentation - Cisco Systems**