El IOS PKI Auto-alista, Auto-renovación, y los temporizadores

Contenido

Introducción

Este documento describe cómo las operaciones del Public Key Infrastructure (PKI) del ® del Cisco IOS del Autoregistro y de la auto-renovación trabajan y cómo los temporizadores respectivos PKI se calculan para estas operaciones.

Los Certificados han reparado los cursos de la vida y expiran en algún momento. Si los Certificados se utilizan para los fines de autenticación para una solución de VPN (por ejemplo), el vencimiento de estos Certificados lleva a las fallas de autenticación posibles que dan lugar a la pérdida de conectividad VPN entre los puntos finales. Para evitar este problema, estos dos mecanismos están disponibles para la renovación automática del certificado:

- Autoregistro para el cliente/los routeres radiales
- Auto-renovación para el router del servidor del Certification Authority (CA)

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- PKI y el concepto de confianza
- Configuración básica de CA en el Routers

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Terminología

Autoregistro

Cuando un certificado en un dispositivo extremo está a punto de expirar, el Autoregistro obtiene un nuevo certificado sin la interrupción. Cuando se configura el Autoregistro, el cliente/el router radial puede pedir un nuevo certificado en algún momento antes de que expire su propio certificado (conocido como su identidad o certificado ID).

auto-renovación

Este parámetro decide cuando el servidor de certificados (CS) genera su certificado de la renovación (sombra); si el comando se ingresa bajo configuración CS sin ningún argumento, el tiempo predeterminado es 30 días.

> Nota: Por los ejemplos en este documento, el valor de este parámetro es *10 minutos*.

Cuando un certificado en el servidor de CA está a punto de expirar, la auto-renovación permite a CA para obtener un nuevo certificado sin la interrupción. Cuando se configura la auto-renovación, el router de CA puede generar un nuevo certificado en algún momento antes de que expire su propio certificado. El nuevo certificado, que se llama el certificado de la *sombra* o de la *renovación*, llega a ser activo en el momento exacto que expira el certificado de CA actual.

Con el uso de las dos características que se mencionan en la sección de la introducción de este documento, el despliegue PKI se automatiza y permite que el spoke o el dispositivo del cliente consiga un certificado de identidad de la sombra/de la renovación y los sombree/el certificado de CA de la renovación antes del vencimiento actual del certificado de CA. Esta manera, puede transición sin la interrupción a los nuevos Certificados ID y de CA cuando expiran sus Certificados actuales ID y de CA.

Ca-certificado del curso de la vida

Este parámetro especifica el curso de la vida del certificado de CA. El valor de este parámetro se puede especificar en los días/las horas/los minutos.

> Nota: Por los ejemplos en este documento, el valor de este parámetro es *30 minutos*.

certificado del curso de la vida

Este parámetro especifica el curso de la vida del certificado de identidad que es publicado por el router de CA. El valor de este parámetro se puede especificar en los días/las horas/los minutos.

Nota: Por los ejemplos en este documento, el valor de este parámetro es *20 minutos*

Configurar

Nota: Valores del temporizador más pequeños PKI para el *curso de la vida*, auto-*renovación*, y auto-*alistan* se utilizan en este documento para ilustrar dominante auto-alistan y los conceptos de la auto-renovación. En un entorno de red en funcionamiento, Cisco recomienda que usted utiliza las vidas útiles predeterminadas para estos parámetros.

Consejo: Todo el PKI temporizador-basó los eventos, tales como *renovación* y el *reenrollment*, puede ser afectado si no hay fuente de tiempo válida. Por este motivo, Cisco recomienda que usted configura el Network Time Protocol (NTP) en todo el Routers ese peform PKI.

Configuración del servidor de CA del Cisco IOS

Esta sección proporciona un configuratinon del ejemplo para el servidor de CA del Cisco IOS.

```
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
```

Nota: El valor que se especifica con el comando de la auto-**renovación** es el número de días/de horas/de minutos *antes de la fecha de finalización del certificatethat actual de CA que* se genera el certificado de la renovación. Por lo tanto, si un certificado de CA es válido a partir de la 12:00 a 12:30, después la auto-**renovación 0 0 10** implica que el certificado de CA de la renovación está generado alrededor de 12:20.

Ingrese el **comando certificate crypto del pki de la demostración** para verificar la configuración en el servidor del Cisco IOS CA:

```
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
```

De acuerdo con esta salida, el router incluye un certificado de CA que es válido a partir de la 9:16 a 9:46 IST de nov el 25 de 2012. Puesto que la auto-renovación se configura por 10 minutos, se espera que el certificado de la sombra/de la renovación sea generado por *9.36 IST de* nov el 25 de 2012.

Para confirmar, ingrese el comando **crypto del temporizador del pki de la demostración**:

```
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
```

De acuerdo con esta salida, el comando **crypto del temporizador del pki de la demostración** fue publicado en 9.19 IST, y se espera que el certificado de la sombra/de la renovación sea generado en el plazo de 16.43 minutos:

[09:19:22 + 00:16:43] = **09:36:05**, que es el [end-date_of_current_CA_cert - auto_rollover_timer]; es decir, [09:46:05 - 00:10:00] = **09:36:05**.

Configuración del cliente/del router radial

Esta sección proporciona un ejemplo de configuración para el cliente/el router radial.

```
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
```

> Nota: **El comando auto-enroll** habilita la característica del Autoregistro en el router. La sintaxis del comando es la siguiente: **auto-aliste el** [regenerate] del [val%].

En la salida anterior, la característica del auto-alistar se especifica como 70%; es decir, en el 70% del **[lifetime of current_ID_cert]**, del router los reenrolls automáticamente con CA.

> Consejo: Cisco recomienda que usted fija el valor del auto-alistar hasta el 60% o más para asegurarse de que los temporizadores PKI trabajan correctamente.

La opción *regenerada* lleva a la creación de una nueva clave del Rivest-Shamir-Addleman (RSA) para los propósitos del reenrollment/de la renovación del certificado. Si esta opción no se especifica, se utiliza la clave actual RSA.

Autoregistro en la acción

Complete estos pasos para verificar la característica del Autoregistro:

1. Ingrese el **pki crypto autentican el** comando para autenticar manualmente el trustpoint en el router de cliente:

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

   Nota: Para más información sobre este comando, refiera a la referencia de comandos de la Seguridad de Cisco IOS.
   Una vez que usted ingresa el comando, una salida similar a esto debe aparecer:
   ```
   Client-1(config)#crypto pki authenticate client1
   ```
2. Tipo **sí** para validar el certificado de CA en el router de cliente. Entonces, un temporizador de la **RENOVACIÓN** comienza por el router:

   ```
   Client-1#show crypto pki timer
   PKI Timers
   | 0.086
   | 0.086 RENEW cvo-pki
   | 9:51.366 SESSION CLEANUP
   ```
3. El temporizador de la **RENOVACIÓN** alcanza una vez cero, el router de cliente se alista automáticamente con CA para obtener su certificado de identidad. Una vez que se recibe el certificado, ingrese el **comando certificate crypto del pki de la demostración** para verlo:

   ```
   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
```

La fecha de la renovación es **09:30:08** y se calcula como se muestra aquí:

hora de inicio + (%renewal de ID_cert_lifetime)

O

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

Los temporizadores PKI reflejan lo mismo:

```
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. El temporizador de la **RENOVACIÓN** expira una vez, los reenrolls del router con CA para obtener un nuevo certificado ID. Después de que haya ocurrido una renovación del certificado, ingrese el comando **crypto CERT del pki de la demostración** para ver el nuevo certificado ID:

```
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
```

Note que hay no más una *fecha de la renovación*; en lugar, un temporizador de la **SOMBRA** comienza:

```
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
```

Aquí está la lógica de proceso:

- Si la fecha de finalización del certificado **ID no es igual a la** fecha de finalización del **certificado de CA**, después calcule una renovar-fecha basada en el porcentaje del auto-alistar y comience el temporizador de la **RENOVACIÓN**.

- Si la fecha de finalización del certificado **ID es igual a la** fecha de finalización del **certificado de CA**, después no hay proceso de renovación necesario puesto que el certificado actual ID es válido solamente mientras el certificado de CA actual es válido. En lugar, se comienza un temporizador de la **SOMBRA**.

Este temporizador también se calcula sobre la base del porcentaje mencionado en el **comando auto-enroll**. Por ejemplo, considere las fechas de validez del certificado renovado ID que se muestran en el ejemplo anterior:

```
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
```

El curso de la vida de este certificado es 16 minutos. Por lo tanto, el temporizador de la renovación (es decir, el temporizador de la SOMBRA) es el 70% de 16 minutos, que iguala aproximadamente 11 minutos. Este cálculo implica que el router comienza las peticiones sus Certificados de la sombra/de la renovación en [09:30:09 + 00:11:00] = 09:41:09, que corresponde al temporizador de la SOMBRA PKI mostrado previamente en este documento:

```
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-renovación en la acción

Esta sección describe la característica de la auto-renovación en la acción.

En el servidor de CA del Cisco IOS

Cuando expira el temporizador de la SOMBRA, el certificado de la renovación aparece en el router de CA:

```
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
```

En el router de cliente

Según lo descrito previamente en este documento, la característica del Autoregistro comenzó un temporizador de la SOMBRA en el router de cliente. Cuando expira el temporizador de la SOMBRA, la característica del Autoregistro permite al router para pedir el servidor de CA para la *renovación/el certificado de CA de la sombra*. Una vez que está recibido, pregunta para su *renovación/*certificado de la *sombra ID* también. Como consecuencia, el router tiene dos pares de Certificados: el un par que es actual y el otro par que contiene la renovación/la sombra certifica:

```
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
```

Note la validez del certificado de la renovación ID:

```
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
```

El curso de la vida del certificado es apenas cuatro minutos (en vez de los 20 minutos previstos, según lo configurado en el servidor de CA del Cisco IOS). Por el servidor de CA del Cisco IOS, el curso de la vida *absoluto del* certificado ID debe ser 20 minutos (que significa, para un router de cliente dado, la suma de los cursos de la vida de los Certificados ID (corriente + sombra) publicados a ella no debe ser mayor de 20 minutos).

Este proceso se describe más a fondo aquí:

- Aquí está la validez del certificado actual ID en el 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
```

Por lo tanto, el *current_id_cert_lifetime* es 16 minutos.

- Aquí está la validez del certificado de la renovación ID:

```
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

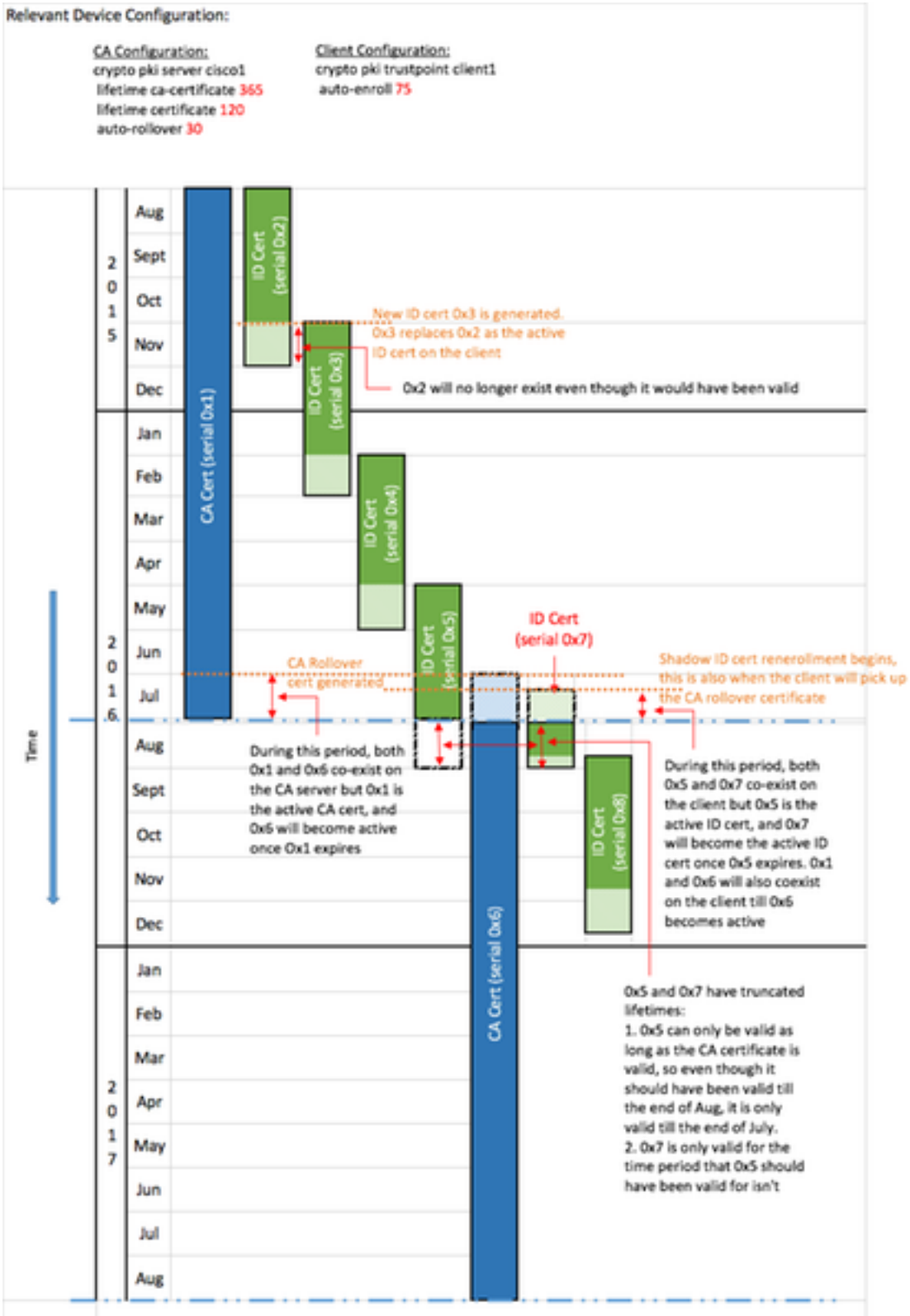
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:

```
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

Por lo tanto, el *rollover_id_cert_lifetime* es cuatro minutos.

- Por el Cisco IOS, cuando el [current_id_cert_lifetime] se agrega al [rollover_id_cert_lifetime], debe igualar el [total_id_cert_lifetime]. Éste es en este caso verdadero.

Timeline de la muestra PKI con la renovación y la inscripción



Consideraciones importantes

- Los temporizadores PKI requieren un reloj autoritario para funcionar correctamente. Cisco recomienda que usted utiliza el NTP para sincronizar los relojes entre los routeres de cliente y el router de CA del Cisco IOS. En ausencia del NTP, el sistema/el reloj de hardware en el router puede ser utilizado. Para la información sobre cómo configurar el reloj de hardware y hacerlo autoritario, refiera a la guía de configuración de la administración del sistema básico, Cisco IOS Release 12.4T.

- Sobre la recarga de un router, la sincronización del NTP tarda a menudo algunos minutos. Sin embargo, los temporizadores PKI se establecen casi inmediatamente. A partir de las versiones 15.2(3.8)T y 15.2(4)S, los temporizadores PKI se evalúan de nuevo automáticamente después de que se sincronice el NTP.

- Los temporizadores PKI no son absolutos; se basan en el *tiempo restante* y, por lo tanto, se recalculan después de una reinicialización. Por ejemplo, asuma que el router de cliente tiene un certificado ID que sea válido por 100 días y la característica del auto-alistar se fija hasta el 80%. Entonces, se espera que el reenrollment ocurra después del 80.o día. Si recargan al router en el 60.o día, arranca y recalcula el temporizador PKI como se muestra aquí: (*tiempo restante*) * (*%auto-enroll*) = (100-60) * 80% = 32 días.

  Por lo tanto, el reenrollment ocurre en [60 + 32] = 92.o día.

- Cuando usted configura el auto-alistar y auto-rollovertimers, es importante configurarlos con los valores que permiten la Disponibilidad del certificado de CA de la SOMBRA en el servidor pki cuando los pedidos de cliente uno PKI. Esto ayuda a atenuar los errores potenciales de los servicios PKI en un entorno en grande.

Información Relacionada

- Seguridad de Cisco IOS que despliega con un Public-Key Infrastructure Whitepaper
- Public Key Infrastructure: Ventajas y características Whitepaper del despliegue
- Guía de configuración del Public Key Infrastructure
- Soporte Técnico y Documentación - Cisco Systems