OS IO PKI Auto-registram-se, Auto-derrubamento, e temporizadores

Índice

Introdução

Este documento descreve como as operações do Public Key Infrastructure (PKI) do ® do Cisco IOS da inscrição automática e do auto-derrubamento trabalham e como os temporizadores respectivos PKI são calculados para estas operações.

Os Certificados fixaram vidas e expiram em algum momento. Se os Certificados estão usados para propósitos de autenticação para uma solução de VPN (por exemplo), a expiração destes Certificados conduz às falhas de autenticação possíveis que conduzem à perda de conectividade de VPN entre os valores-limite. A fim evitar esta edição, estes dois mecanismos estão disponíveis para a renovação automática do certificado:

- Inscrição automática para o cliente/Roteadores do spoke
- Auto-derrubamento para o roteador de servidor do Certification Authority (CA)

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PKI e o conceito da confiança
- Configuração básica de CA no Roteadores

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Terminologia

inscrição automática

Quando um certificado em um dispositivo final está a ponto de expirar, a inscrição automática obtém um certificado novo sem rompimento. Quando a inscrição automática é configurada, o cliente/roteador do spoke pode pedir um certificado novo em algum dia antes que seu próprio certificado (conhecido como sua identidade ou certificado ID) expire.

auto-derrubamento

Este parâmetro decide quando o servidor certificado (CS) gerencie seu certificado do derrubamento (sombra); se o comando é incorporado sob a configuração CS sem nenhum argumento, o tempo padrão é 30 dias.

> Nota: Para os exemplos neste documento, o valor deste parâmetro é os *minutos 10*.

Quando um certificado no server de CA está a ponto de expirar, o auto-derrubamento permite CA de obter um certificado novo sem rompimento. Quando o auto-derrubamento é configurado, o roteador de CA pode gerar um certificado novo em algum dia antes que seu próprio certificado expire. O certificado novo, que é chamado a *sombra* ou o certificado do *derrubamento*, torna-se ativo no momento preciso que o certificado de CA atual expira.

Com o uso das duas características que são mencionadas na seção da introdução deste documento, o desenvolvimento PKI torna-se automatizado e permite-se que o spoke ou o dispositivo do cliente obtenham uma sombra/certificado de identidade do derrubamento e sombreiem-nos/certificado de CA do derrubamento antes da expiração atual do certificado de CA. Esta maneira, pode transição sem interrupção ao ID novo e certificados de CA quando seus ID e certificados de CA atuais expiram.

Ca-certificado da vida

Este parâmetro especifica a vida do certificado de CA. O valor deste parâmetro pode ser especificado nos dias/horas/minutos.

> Nota: Para os exemplos neste documento, o valor deste parâmetro é *30 minutos*.

certificado da vida

Este parâmetro especifica a vida do certificado de identidade que é emitido pelo roteador de CA.

O valor deste parâmetro pode ser especificado nos dias/horas/minutos.

Nota: Para os exemplos neste documento, o valor deste parâmetro é *20 minutos*

Configurar

Nota: Os valores de temporizador menores PKI para a *vida*, auto-*derrubamento*, e auto-*registram-se* são usados neste documento a fim ilustrar chave auto-registram-se e conceitos do auto-derrubamento. Em um ambiente de rede viva, Cisco recomenda que você usa as durações padrão para estes parâmetros.

Dica: Todo o PKI temporizador-baseou eventos, tais como o *derrubamento* e o *reenrollment*, pode ser afetado se não há nenhuma fonte de tempo autoritária. Por este motivo, Cisco recomenda que você configura o Network Time Protocol (NTP) em todo o Roteadores esse peform PKI.

Configuração do servidor de CA do Cisco IOS

Esta seção fornece um configuratinon do exemplo para o server de CA do 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: O valor que é especificado com o comando do auto-**derrubamento** é o número de dias/horas/minutos *antes da data final do certificatethat que atual de CA o* certificado do derrubamento é gerado. Consequentemente, se um certificado de CA é válido de 12:00 a 12:30, a seguir o auto-**derrubamento 0 0 10** implica que o certificado de CA do derrubamento está gerado em torno de 12:20.

Inscreva o **comando certificate cripto do pki da mostra** a fim verificar a configuração no server de CA do Cisco IOS:

```
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
```

Baseado nesta saída, o roteador inclui um certificado de CA que seja válido de 9:16 a 9:46 IST novembro 25, 2012. Desde que o auto-derrubamento é configurado pelos minutos 10, a sombra/certificado do derrubamento é esperada ser gerada por *9.36 IST* novembro 25, 2012.

A fim confirmar, incorpore o comando **cripto do temporizador do pki da mostra**:

```
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
```

Baseado nesta saída, o comando **cripto do temporizador do pki da mostra** foi emitido em 9.19 IST, e a sombra/certificado do derrubamento é esperada ser gerada dentro de 16.43 minutos:

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

Configuração do cliente/Spoke Router

Esta seção fornece um exemplo de configuração para o cliente/roteador do spoke.

```
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: **O comando auto-enroll** permite a característica Auto-inscrição no roteador. A sintaxe do comando é: **auto-registre o** [regenerate] do [val%].

Na saída precedente, a característica auto-registrar-se é especificada como 70%; isto é, em 70% do **[lifetime of current_ID_cert]**, do roteador os reenrolls automaticamente com CA.

> Dica: Cisco recomenda que você ajusta o valor auto-se registrar a 60% ou mais a fim se assegurar de que os temporizadores PKI trabalhem corretamente.

A opção *regenerada* conduz à criação de uma chave nova de Rivest-Shamir-Addleman (RSA) para finalidades do reenrollment/renovação do certificado. Se esta opção não é especificada, a chave atual RSA está usada.

Inscrição automática na ação

Termine estas etapas a fim verificar a característica Auto-inscrição:

1. Entre no **pki cripto autenticam o** comando a fim autenticar manualmente o ponto confiável no

roteador cliente:

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

Nota: Para obter mais informações sobre deste comando, refira a referência de comandos do Cisco IOS Security.

Uma vez que você incorpora o comando, uma saída similar a esta deve aparecer:

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

2. Tipo **sim** a fim aceitar o certificado de CA no roteador cliente. Então, um temporizador da **RENOVAÇÃO** começa no roteador:

```
Client-1#show crypto pki timer
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. Uma vez o temporizador da **RENOVAÇÃO** alcança zero, o roteador cliente registra-se automaticamente com CA a fim obter seu certificado de identidade. Uma vez que o certificado é recebido, inscreva o **comando certificate cripto do pki da mostra** a fim vê-lo:

```
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
```

A data da renovação é **09:30:08** e é calculada como mostrado aqui:

horas inicial + (%renewal de ID_cert_lifetime)

Ou

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

Os temporizadores PKI refletem o mesmos:

```
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. Uma vez o temporizador da **RENOVAÇÃO** expira, os reenrolls do roteador com CA a fim obter um certificado novo ID. Depois que uma renovação do certificado ocorreu, incorpore o comando **cripto CERT do pki da mostra** a fim ver o certificado novo 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
```

Observe que há já não uma *data da renovação*; em lugar de, um temporizador da **SOMBRA**

começa:

```
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
```

Está aqui a lógica do processo:

- Se a data final do certificado **ID não é igual à** data final do **certificado de CA**, a seguir calcule uma renovar-data baseada na porcentagem auto-registrar-se e comece o temporizador da **RENOVAÇÃO**.

- Se a data final do certificado **ID é igual à** data final do **certificado de CA**, a seguir nenhum processo de renovação é necessário desde que o certificado atual ID é válido somente enquanto o certificado de CA atual é válido. Em lugar de, um temporizador da **SOMBRA** é começado.

Este temporizador é calculado igualmente com base na porcentagem mencionada no **comando auto-enroll**. Por exemplo, considere as datas de validez do certificado renovado ID que são mostradas no exemplo 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
```

A vida deste certificado é 16 minutos. Consequentemente, o temporizador do derrubamento (isto é, o temporizador da SOMBRA) é 70% de 16 minutos, que iguala aproximadamente 11 minutos. Este cálculo implica que o roteador começa pedidos para seus sombra/Certificados do derrubamento em [09:30:09 + 00:11:00] = 09:41:09, que corresponde ao temporizador da SOMBRA PKI mostrado previamente neste 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-derrubamento na ação

Esta seção descreve a característica do auto-derrubamento na ação.

No server de CA do Cisco IOS

Quando o temporizador da SOMBRA expira, o certificado do derrubamento aparece no roteador 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
```

No roteador cliente

Como descrito previamente neste documento, a característica Auto-inscrição começou um temporizador da SOMBRA no roteador cliente. Quando o temporizador da SOMBRA expira, a característica Auto-inscrição permite o roteador de pedir o server de CA para o *derrubamento/certificado de CA da sombra*. Uma vez que recebida, pergunta para seu certificado do *derrubamento/sombra ID* também. Em consequência, o roteador tem dois pares de Certificados: um par que é atual e o outro par que contém os Certificados do derrubamento/sombra:

```
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

Observe a validez do certificado do derrubamento 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
```

A vida do certificado é apenas quatro minutos (em vez dos 20 minutos previstos, como configurados no server de CA do Cisco IOS). Pelo server de CA do Cisco IOS, a vida *absoluta do* certificado ID deve ser 20 minutos (que significa, para um roteador cliente dado, a soma das vidas dos Certificados ID (corrente + sombra) emitidos a ela não deve ser maior de 20 minutos).

Este processo é descrito mais aqui:

- Está aqui a validez do certificado atual ID no roteador:

```
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
```

Consequentemente, o *current_id_cert_lifetime* é 16 minutos.

- Está aqui a validez do certificado do derrubamento 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
```

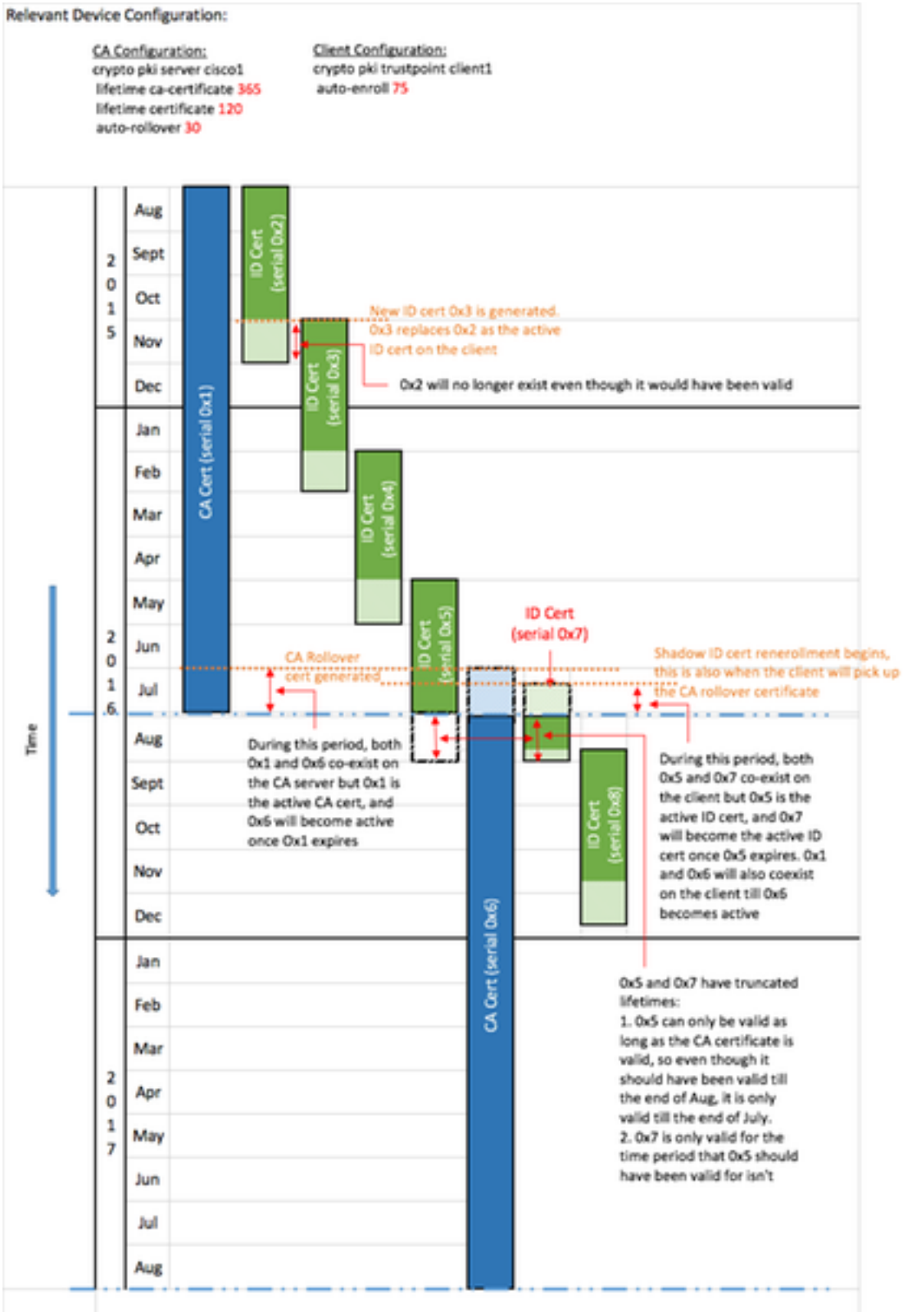
CA Certificate

```
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
```

Consequentemente, o *rollover_id_cert_lifetime* é quatro minutos.

- Pelo Cisco IOS, quando o [current_id_cert_lifetime] é adicionado ao [rollover_id_cert_lifetime], deve igualar o [total_id_cert_lifetime]. Isto é verdadeiro nesta instância.

Período da amostra PKI com derrubamento e registro



Considerações importantes

- Os temporizadores PKI exigem um pulso de disparo competente a fim funcionar corretamente. Cisco recomenda que você usa o NTP a fim sincronizar pulsos de disparo entre os roteadores cliente e o roteador de CA do Cisco IOS. Na ausência do NTP, o sistema/relógio de hardware no roteador pode ser usado. Para obter informações sobre de como configurar o relógio de hardware e fazê-lo competente, refira o manual de configuração do gerenciamento básico de sistema, Cisco IOS Release 12.4T.

- Em cima do reload de um roteador, a sincronização do NTP toma frequentemente alguns minutos. Contudo, os temporizadores PKI são estabelecidos quase imediatamente. Até à data das versões 15.2(3.8)T e 15.2(4)S, os temporizadores PKI são reavaliados automaticamente depois que o NTP é sincronizado.

- Os temporizadores PKI não são absolutos; são baseados no *tempo restante* e, são voltados a calcular consequentemente após uma repartição. Por exemplo, supõe que o roteador cliente tem um certificado ID que seja válido por 100 dias e a característica auto-se registrar seja ajustada a 80%. Então, o reenrollment é esperado ocorrer após o 80th dia. Se o roteador é recarregado no 60th dia, carreg acima e volta a calcular o temporizador PKI como mostrado aqui: (*tempo restante*) * (*%auto-enroll*) = (100-60) * 80% = 32 dias.

  Consequentemente, o reenrollment ocorre no [60 + 32] = 92nd dia.

- Quando você configura auto-se registrar e auto-rollovertimers, é importante configurar-los com valores que permitem a Disponibilidade do certificado de CA da SOMBRA no servidor PKI quando os pedidos do cliente um PKI. Isto ajuda a abrandar falhas potenciais dos serviços PKI em um ambiente em grande escala.

Informações Relacionadas

- Cisco IOS Security de distribuição com um Public-Key Infrastructure Whitepaper
- Infraestrutura de chave pública: Benefícios do desenvolvimento e características Whitepaper
- Manual de configuração da infraestrutura de chave pública
- Suporte Técnico e Documentação - Cisco Systems