IOS PKI Auto-Enroll, Auto-Rollover und Timer

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Vorgänge für die automatische Registrierung und automatische Rollover der Cisco IOS® Public Key Infrastructure (PKI) funktionieren und wie die entsprechenden PKI-Timer für diese Vorgänge berechnet werden.

Zertifikate haben eine feste Lebensdauer und laufen irgendwann ab. Wenn die Zertifikate beispielsweise für Authentifizierungszwecke für eine VPN-Lösung verwendet werden, führt das Verfallen dieser Zertifikate zu möglichen Authentifizierungsfehlern, die zu einem Verlust der VPN-Verbindung zwischen den Endpunkten führen. Um dieses Problem zu vermeiden, stehen die folgenden beiden Mechanismen für die automatische Erneuerung von Zertifikaten zur Verfügung:

- Automatische Anmeldung für die Client/Spoke-Router
- Auto-Rollover für den CA-Server-Router (Certification Authority)

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- PKI und das Konzept des Vertrauens
- Grundlegende Konfiguration der CA auf Routern

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Terminologie

automatische Registrierung

Wenn ein Zertifikat auf einem Endgerät abläuft, erhält die automatische Anmeldung ein neues Zertifikat ohne Unterbrechung. Wenn die automatische Registrierung konfiguriert ist, kann der Client/Spoke-Router ein neues Zertifikat anfordern, bevor sein eigenes Zertifikat (seine Identität oder sein ID-Zertifikat) abläuft.

Auto-Rollover

Dieser Parameter legt fest, wann der Zertifikatsserver (CS) sein Rollover-Zertifikat (Schatten-Zertifikat) generiert. Wenn der Befehl ohne Argument unter der CS-Konfiguration eingegeben wird, beträgt die Standardzeit 30 Tage.

> **Hinweis**: Für die Beispiele in diesem Dokument beträgt der Wert dieses Parameters *10 Minuten*.

Wenn ein Zertifikat auf dem CA-Server demnächst abläuft, ermöglicht es der automatischen Rollover der CA, ein neues Zertifikat ohne Unterbrechung zu erhalten. Wenn die automatische Rollover-Funktion konfiguriert ist, kann der CA-Router ein neues Zertifikat generieren, bevor das eigene Zertifikat abläuft. Das neue Zertifikat, das als *Schatten*- oder *Rollover*-Zertifikat bezeichnet wird, wird zum Zeitpunkt des Ablaufs des aktuellen Zertifizierungsstellenzertifikats aktiviert.

Durch die Verwendung der beiden Funktionen, die im Abschnitt Einführung dieses Dokuments erwähnt werden, wird die PKI-Bereitstellung automatisiert und ermöglicht dem Spoke- oder Client-Gerät, vor Ablauf des aktuellen Zertifizierungsstellenzertifikats ein Schatten-/Rollover-Identitätszertifikat und ein Schatten-/Rollover-Zertifizierungsstellenzertifikat zu erhalten. Auf diese Weise kann es ohne Unterbrechung zu den neuen ID- und Zertifizierungsstellenzertifikaten wechseln, wenn die aktuelle ID und die Zertifizierungsstellenzertifikate ablaufen.

Lebenszeitzertifikat

Dieser Parameter gibt die Lebensdauer des Zertifizierungsstellenzertifikats an. Der Wert dieses Parameters kann in Tagen/Stunden/Minuten angegeben werden.

> **Hinweis**: Für die Beispiele in diesem Dokument beträgt der Wert dieses Parameters *30 Minuten*.

Lebenszeitbescheinigung

Dieser Parameter gibt die Lebensdauer des vom CA-Router ausgestellten Identitätszertifikats an. Der Wert dieses Parameters kann in Tagen/Stunden/Minuten angegeben werden.

Hinweis: Für die Beispiele in diesem Dokument beträgt der Wert dieses Parameters *20 Minuten*

Konfigurieren

Hinweis: In diesem Dokument werden kleinere PKI-Timer-Werte für die *Lebensdauer, automatische Rollover* und *automatische Anmeldung* verwendet, um wichtige Konzepte für die automatische Registrierung und automatische Rollover zu veranschaulichen. In einer Live-Netzwerkumgebung empfiehlt Cisco die Verwendung der Standardlebensdauer für diese Parameter.

Tipp: Alle Ereignisse, die auf einem PKI-Timer basieren, wie *Rollover* und *Neuregistrierung*, können davon betroffen sein, wenn keine autoritative Zeitquelle vorhanden ist. Aus diesem Grund empfiehlt Cisco, das Network Time Protocol (NTP) auf allen Routern zu konfigurieren, die PKI ausführen.

Cisco IOS CA-Serverkonfiguration

Dieser Abschnitt enthält eine Beispielkonfiguration für den 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

crypto pki server ios-ca
issuer-name CN=Root-CA,OU=TAC,C=IN
grant auto
hash sha512
lifetime certificate 0 0 20
lifetime ca-certificate 0 0 30
cdp-url http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
auto-rollover 0 0 10
database url flash:
```

Hinweis: Der Wert, der mit dem **Auto-Rollover-**Befehl angegeben wird, ist die Anzahl der Tage/Stunden/Minuten *vor dem Enddatum des aktuellen CA*-Zertifikats, das das Rollover-Zertifikat generiert. Wenn ein Zertifizierungsstellenzertifikat von 12:00 bis 12:30 Uhr gültig ist, impliziert die **automatische Rollover-Funktion 0 0 10**, dass das Rollover-Zertifizierungsstellenzertifikat ca. 12:20 Uhr generiert wird.

Geben Sie den Befehl **show crypto pki certificate** ein, um die Konfiguration auf dem Cisco IOS CA-Server zu überprüfen:

```
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
```

Basierend auf dieser Ausgabe verfügt der Router über ein Zertifizierungsstellenzertifikat, das vom 25. November 2012, 09:16 bis 9:46 Uhr gültig ist. Da die automatische Rollover-Funktion für 10 Minuten konfiguriert ist, wird das Schatten-/Rollover-Zertifikat voraussichtlich bis zum 25. November 2012 generiert.

Geben Sie zur Bestätigung den Befehl **show crypto pki timer** ein:

```
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
```

Basierend auf dieser Ausgabe wurde der Befehl **show crypto pki timer** bei 9,19 IST ausgegeben. Das Schatten-/Rollover-Zertifikat soll innerhalb von 16,43 Minuten generiert werden:

[09:19:22 + 00:16:43] = **09:36:05**, d. h. [end-date_of_current_CA_cert - auto_rollover_timer]; das heißt, [09:46:05 - 00:10:00] = **09:36:05**.

Client/Spoke-Router-Konfiguration

Dieser Abschnitt enthält eine Beispielkonfiguration für den 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

crypto pki trustpoint client1
enrollment url http://10.1.1.1:80
subject-name CN=Client-1,OU=TAC,c=IN
revocation-check crl
auto-enroll 70 regenerate
```

> **Hinweis**: Mit dem Befehl **zur automatischen** Registrierung wird die automatische Registrierung auf dem Router aktiviert. Die Befehlssyntax lautet: **auto-enroll** [*val%*] [*regenerate*].

In der vorherigen Ausgabe wird die Funktion zur automatischen Registrierung als 70 %

angegeben. d. h. bei 70 % der **[Lebensdauer von current_ID_cert]**, wird der Router automatisch bei der CA neu registriert.

> **Tipp**: Cisco empfiehlt, den Wert für die automatische Anmeldung auf 60 % oder mehr festzulegen, um sicherzustellen, dass die PKI-Timer ordnungsgemäß funktionieren.

Die *Neugenerierungsoption* führt zur Erstellung eines neuen Rivest-Shamir-Addleman (RSA)-Schlüssels für die erneute Registrierung/Verlängerung von Zertifikaten. Wenn diese Option nicht angegeben ist, wird der aktuelle RSA-Schlüssel verwendet.

Automatische Anmeldung in Aktion

Gehen Sie wie folgt vor, um die Funktion zur automatischen Registrierung zu überprüfen:

1. Geben Sie den Befehl **crypto pki authentication** ein, um den Trustpoint auf dem Client-Router manuell zu authentifizieren:

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

   Hinweis: Weitere Informationen zu diesem Befehl finden Sie in der Cisco IOS Security Command Reference.
   Sobald Sie den Befehl eingeben, sollte eine ähnliche Ausgabe angezeigt werden:

```
Certificate has the following attributes:
Fingerprint MD5: 006B2E44 37FBC3F1 AA14F32B CDC4462E
Fingerprint SHA1: 2999CC53 8BF65247 C0D704E9 FDC73002 A33910D4

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

2. Geben Sie **yes** ein, um das Zertifizierungsstellenzertifikat des Client-Routers zu akzeptieren. Anschließend beginnt ein **RENEW**-Timer auf dem Router:

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

3. Sobald der **RENEW**-Timer null erreicht hat, registriert sich der Client-Router automatisch bei der CA, um sein Identitätszertifikat zu erhalten. Geben Sie nach Erhalt des Zertifikats den Befehl **show crypto pki certificate** ein, um das Zertifikat anzuzeigen:

```
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
```

Das **Verlängerungsdatum** ist **09:30:08** und wird wie folgt berechnet:

Startzeit + (%Verlängerung der ID_cert_life)

oder

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

Die PKI-Timer spiegeln Folgendes wider:

```
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. Sobald der **RENEW**-Timer abläuft, meldet sich der Router bei der CA erneut an, um ein neues ID-Zertifikat zu erhalten. Geben Sie nach einer Zertifikatsverlängerung den Befehl **show crypto pki cert** ein, um das neue ID-Zertifikat anzuzeigen:

```
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
```

Beachten Sie, dass es kein *Verlängerungsdatum* mehr gibt; Stattdessen beginnt ein **SHADOW**-Timer:

```
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
```

Die Prozesslogik lautet wie folgt:

- Wenn das Enddatum des **ID-**Zertifikats **nicht** dem Enddatum des **Zertifizierungsstellenzertifikats entspricht, berechnen Sie ein Verlängerungsdatum auf der Grundlage des Prozentsatzes für die automatische Anmeldung und starten Sie den RENEW-Timer.**
- Wenn das Enddatum des **ID-**Zertifikats **dem Enddatum** des **CA-**Zertifikats entspricht, ist kein Verlängerungsprozess erforderlich, da das aktuelle ID-Zertifikat nur gültig ist, solange das aktuelle Zertifizierungsstellenzertifikat gültig ist. Stattdessen wird ein **SHADOW**-Timer gestartet.

Dieser Timer wird auch basierend auf dem im Befehl **zur automatischen Anmeldung** angegebenen Prozentsatz berechnet. Betrachten Sie beispielsweise die Gültigkeitsdaten des erneuerten ID-Zertifikats, die im vorherigen Beispiel gezeigt werden:

```
Validity Date of current ID cert:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
```

Die Lebensdauer dieses Zertifikats beträgt 16 Minuten. Daher beträgt der Rollover-Timer (der SHADOW-Timer) 70 % von 16 Minuten, was etwa 11 Minuten entspricht. Diese Berechnung impliziert, dass der Router Anfragen für seine Schatten-/Rollover-Zertifikate um [09:30:09 + 00:11:00] = 09:41:09 beginnt, was dem zuvor in diesem Dokument gezeigten PKI SHADOW-Timer entspricht:

```
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
```

Automatisches Rollover in Aktion

In diesem Abschnitt wird die Funktion zum automatischen Rollover in Aktion beschrieben.

Auf dem Cisco IOS CA-Server

Wenn der SHADOW-Timer abläuft, wird das Rollover-Zertifikat auf dem CA-Router angezeigt:

```
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
```

Am Client-Router

Wie bereits in diesem Dokument beschrieben, startete die Funktion zur automatischen Registrierung einen SHADOW-Timer auf dem Client-Router. Wenn der SHADOW-Timer abläuft, kann der Router mit der Funktion für die automatische Registrierung den CA-Server für das *Rollover-/Schatten-CA*-Zertifikat anfordern. Nach dem Empfang fragt er auch sein *Rollover-/Schatten-ID*-Zertifikat ab. Der Router verfügt daher über zwei Zertifikatpaare: ein aktuelles Paar und das andere Paar, das die Rollover-/Schattenzertifikate enthält:

```
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
```

Beachten Sie die Gültigkeit des Rollover-ID-Zertifikats:

```
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

Die Lebensdauer eines Zertifikats beträgt lediglich vier Minuten (anstelle der erwarteten 20 Minuten, wie auf dem Cisco IOS CA-Server konfiguriert). Pro Cisco IOS CA-Server sollte die *absolute* Lebensdauer des ID-Zertifikats 20 Minuten betragen (d. h. für einen Client-Router darf die Summe der Lebensdauer der ausgestellten ID-Zertifikate (aktuell + Schatten) 20 Minuten nicht überschreiten).

Dieser Vorgang wird hier genauer beschrieben:

- Die Gültigkeit des aktuellen ID-Zertifikats auf dem Router ist wie folgt:

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

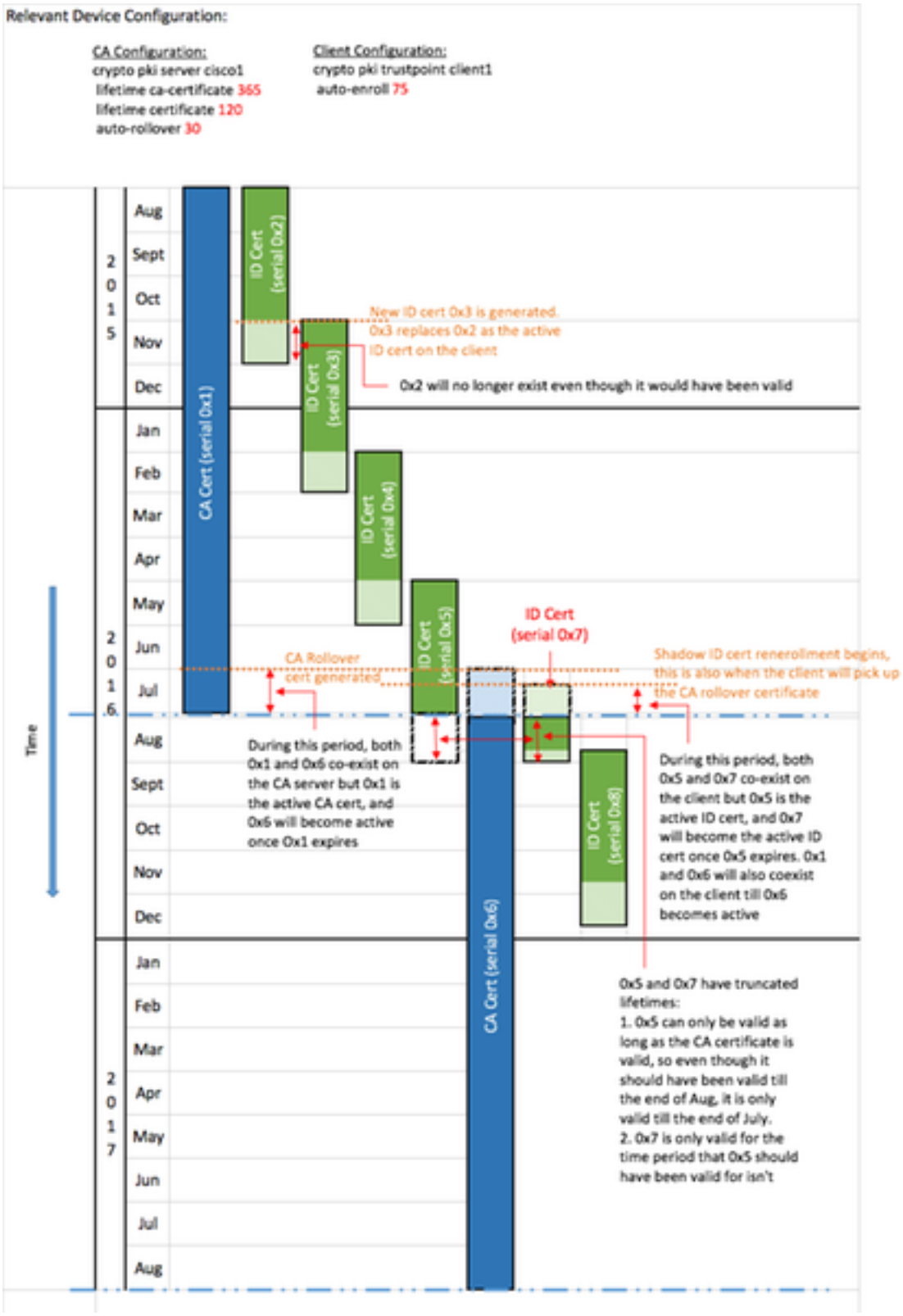
  Aus diesem Grund beträgt die *aktuelle_id_cert_life*-Laufzeit 16 Minuten.

- Die Gültigkeit des Rollover-ID-Zertifikats ist wie folgt:

```
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
```

  Daher beträgt die *Rollover_id_cert_life* vier Minuten.
- Wenn die [current_id_cert_life] zur [rollover_id_cert_life] hinzugefügt wird, muss laut Cisco IOS die [total_id_cert_life]-Einstellung entsprechen. Dies gilt in diesem Fall.

PKI-Beispielzeitleiste mit Rollover und Anmeldung



Wichtige Überlegungen

- Die PKI-Timer benötigen eine autoritative Uhr, um ordnungsgemäß funktionieren zu können. Cisco empfiehlt die Verwendung von NTP, um Uhren zwischen den Client-Routern und dem Cisco IOS CA-Router zu synchronisieren. Wenn kein NTP vorhanden ist, kann die System-/Hardware-Uhr des Routers verwendet werden. Weitere Informationen zum Konfigurieren der Hardware-Uhr und zum Festlegen der Autorität finden Sie im Konfigurationsleitfaden für die grundlegende Systemverwaltung, Cisco IOS Release 12.4T.

- Nach dem erneuten Laden eines Routers dauert die Synchronisierung des NTP häufig einige Minuten. Die PKI-Timer werden jedoch fast sofort eingerichtet. Ab Version 15.2(3.8)T und 15.2(4)S werden die PKI-Timer nach der Synchronisierung des NTP automatisch neu bewertet.

- Die PKI-Timer sind nicht absolut. Sie basieren auf der *verbleibenden Zeit* und werden daher nach einem Neustart neu berechnet. Angenommen, der Client-Router verfügt über ein ID-Zertifikat, das 100 Tage gültig ist, und die automatische Anmeldung ist auf 80 % festgelegt. Die erneute Anmeldung soll dann nach dem 80. Tag erfolgen. Wenn der Router am 60. Tag neu geladen wird, wird der PKI-Timer hochgefahren und neu berechnet, wie hier gezeigt: (*verbleibende Zeit*) * (*%automatische Anmeldung*) = (100-60) * 80% = 32 Tage.

  Daher erfolgt die erneute Anmeldung am [60 + 32] = 92. Tag.

- Wenn Sie die Timer für die automatische Registrierung und automatische Rollover konfigurieren, ist es wichtig, diese mit Werten zu konfigurieren, die die Verfügbarkeit des Zertifikats der SHADOW CA auf dem PKI-Server ermöglichen, wenn der PKI-Client dies anfordert. Dadurch können potenzielle PKI-Service-Ausfälle in einer umfangreichen Umgebung reduziert werden.

Zugehörige Informationen

- Whitepaper: Bereitstellung von Cisco IOS Security mit einer Public-Key-Infrastruktur
- Public Key-Infrastruktur: Whitepaper: Bereitstellungsvorteile und -funktionen
- Konfigurationsleitfaden für Public Key Infrastructure
- Technischer Support und Dokumentation - Cisco Systems