IOS PKI-automatische inschrijving, automatische omloop en timers

Inhoud

Inleiding

Dit document beschrijft hoe de Cisco IOS® Public Key Infrastructure (PKI) bewerkingen van de auto-inschrijving en het auto-omvergooien werk en hoe de respectievelijke PKI-timers voor deze bewerkingen worden berekend.

Certificaten hebben vaste levensduur en verlopen op een bepaald punt. Als de certificaten voor authenticatiedoeleinden worden gebruikt voor een VPN-oplossing (bijvoorbeeld), leidt het verlopen van deze certificaten tot mogelijke authenticatiefouten die leiden tot verlies van VPN-connectiviteit tussen de eindpunten. Om deze afgifte te voorkomen zijn deze twee mechanismen beschikbaar voor automatische verlenging van het certificaat:

- Auto-inschrijving voor de client/spraakrouters
- Auto-Rollover voor de server van de certificeringsinstantie (CA)

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PKI en het vertrouwensconcept
- Basisconfiguratie van CA op routers

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Terminologie

zelfinschrijving

Wanneer een certificaat op een eindapparaat binnenkort zal verlopen, verkrijgt de automatische inschrijving een nieuw certificaat zonder verstoring. Wanneer de auto-inschrijving is geconfigureerd, kan de client-SPD-router ergens om een nieuw certificaat vragen voordat zijn eigen certificaat (bekend als zijn identiteit of ID-certificaat) is verlopen.

zelfomvergooien

Deze parameter bepaalt wanneer de certificaatserver (CS) zijn overloopcertificaat (schaduw) genereert. Als de opdracht zonder argument onder de CS-configuratie is ingevoerd, is de standaardtijd 30 dagen.

> Opmerking: Voor de voorbeelden in dit document is de waarde van deze parameter *10 minuten*.

Wanneer een certificaat op de CA server op het punt staat te verlopen, stelt het auto-omvergooien de CA in om een nieuw certificaat te verkrijgen zonder verstoring. Wanneer de auto-omlooplover is ingesteld, kan de CA router een nieuw certificaat genereren op een bepaald moment voordat het eigen certificaat afloopt. Het nieuwe certificaat, dat het *schaduw* of het *omverloopcertificaat* wordt genoemd, wordt actief op het precieze moment dat het huidige CA-certificaat vervalt.

Door gebruik te maken van de twee functies die in de sectie Inleiding van dit document worden genoemd, wordt de PKI-implementatie geautomatiseerd en krijgt het SPRAAK- of clientapparaat de mogelijkheid om een schaduw-/rolminitecertificaat en een schaduw-/rollover-CA-certificaat te verkrijgen voordat het huidige CA-certificaat afloopt. Op deze manier kan het zonder onderbreking overschakelen naar de nieuwe ID en CA certificaten wanneer zijn huidige ID en CA certificaten verlopen.

erfrechtverklaring

Deze parameter geeft de levensduur van het CA-certificaat aan. De waarde van deze parameter kan in dagen/uren/minuten worden gespecificeerd.

> **Opmerking**: Voor de voorbeelden in dit document is de waarde van deze parameter *30 minuten*.

levenslang certificaat

Deze parameter specificeert de levensduur van het identiteitscertificaat dat door de CA router wordt verstrekt. De waarde van deze parameter kan in dagen/uren/minuten worden gespecificeerd.

> **Opmerking**: Voor de voorbeelden in dit document is de waarde van deze parameter *20 minuten*

Configureren

> **Opmerking**: Kleinere PKI-timer voor *hun leven*, *automatisch* overzetten en *automatisch* registreren worden in dit document gebruikt om belangrijke concepten voor auto-inschrijving en automatisch overzetten te illustreren. In een live netwerkomgeving raadt Cisco u aan de standaard levenstijden voor deze parameters te gebruiken.

> **Tip**: alle op de PKI-timer gebaseerde gebeurtenissen, zoals *kantelen* en *opnieuw aanmelden*, kunnen worden beïnvloed als er geen gezaghebbende tijdbron is. Om deze reden, adviseert Cisco u om het Protocol van de Tijd van het Netwerk (NTP) op alle routers te configureren die PKI uitvoeren.

Cisco IOS CA-serverconfiguratie

Deze sectie verschaft een voorbeeldconfiguratie voor de 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:
```

> **Opmerking**: De waarde die met de **opdracht** voor het **automatisch** overzetten wordt gespecificeerd is het aantal dagen/uren/minuten *vóór de einddatum van het huidige CA*-certificaat dat het certificaat voor het overslaan wordt gegenereerd. Als een CA-certificaat geldig is van 12:00 tot 12:30, dan betekent **de** automatische omloopversie **0 0 10** dat het CA-certificaat wordt gegenereerd rond 12:20.

Voer de opdracht **Show crypto pki-certificaat in** om de configuratie op de Cisco IOS CA-server te controleren:

```
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
```

Op basis van deze uitvoer bevat de router een CA-certificaat dat geldig is van 9:16 tot 9:46 IST Nov 25, 2012. Aangezien het automatisch uploaden van de software 10 minuten lang is uitgevoerd, wordt het schaduw-/rollover-certificaat naar verwachting gegenereerd door *9.36 IST* nov 25 november 2012.

Typ de opdracht **Encrypt pki-**timer voor de bevestiging:

```
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
```

Op basis van deze output werd de opdracht **voor** de **show crypto-pki-**timer verleend op 9.19 IST en wordt verwacht dat het schaduw-/rolminatecertificaat binnen 16.43 minuten wordt gegenereerd:

[09:19:22 + 00:16:43] = **09:36:05**, dat is de [end-date_of_huidige_CA_cert - auto_rollover_timer]; dat wil zeggen , [09:46:05 - 00:10:00] = **09:36:05** .

Configuratie van client-SPE-router

Deze sectie verstrekt een voorbeeldconfiguratie voor de client/spaakrouter.

```
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
```

> **Opmerking**: de opdracht **auto-inschrijving** stelt de optie auto-inschrijving in op de router. De opdrachtsyntaxis is is: **auto-inschrijving** [*val%*] [*regenereren*].

In de vorige uitvoer wordt de optie voor automatische inschrijving gespecificeerd op 70%; dat wil zeggen, bij 70% van de **[levensduur van huidige_ID_cert]**, registreert de router automatisch opnieuw met de CA.

> **Tip**: Cisco raadt u aan de waarde voor automatische inschrijving op 60% of meer in te stellen om ervoor te zorgen dat de PKI-timers correct werken.

De *regenererende* optie leidt tot de creatie van een nieuwe Rivest-Shamir-Addleman (RSA)-toets voor het opnieuw inschrijven/vernieuwen van certificaten. Als deze optie niet is gespecificeerd, wordt de huidige RSA-toets gebruikt.

Automatische inschrijving in bedrijf

Voltooi deze stappen om de optie voor automatische inschrijving te controleren:

1. Typ het opdracht **crypto om** het **bestand** op de clientrouter **echt te maken** om het **betrouwbaar** punt op de clientrouter **handmatig te bevestigen**:

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

   Opmerking: Raadpleeg voor meer informatie over deze opdracht de Cisco IOS Security Opdracht Referentie.
   Zodra u de opdracht hebt ingevoerd, verschijnt er een soortgelijke uitvoer:

```
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. Typ **ja** om het CA-certificaat op de clientrouter te aanvaarden. Vervolgens begint een **RENEW**-timer op de router:

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

3. Zodra de **RENEW**-timer nul bereikt, registreert de clientrouter zich automatisch bij de CA om haar identiteitsbewijs te verkrijgen. Voer na ontvangst van het certificaat de opdracht **van het** certificaat van **"show crypto pki"** in om het te bekijken:

```
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
```

De **vernieuwingsdatum** is **09:30:08** en wordt berekend zoals hieronder aangegeven:

start-tijd + (%vernieuwing van ID_cert_leven)

Of

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

De PKI-timers weerspiegelen hetzelfde:

```
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. Zodra de timer **RENEW** verloopt, registreert de router opnieuw met de CA om een nieuw ID-certificaat te verkrijgen. Nadat een certificaat is vernieuwd, voert u de opdracht **SHOT CKI WETTEN** in om het nieuwe ID-certificaat te bekijken:

```
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
```

kennisgeving dat er niet langer een *verlengingsdatum* is; in plaats daarvan begint een **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
```

Hier volgt de proceslogica:

- Als de einddatum van het **ID-**certificaat **niet gelijk is aan** de einddatum van het **CA-certificaat, berekent u een vernieuwingsdatum op basis van het percentage van de automatische inschrijving en start u de RENEW-timer.**
- Als de einddatum van het **ID-**certificaat **gelijk is** aan de einddatum van het **CA-**certificaat, is geen vernieuwingsproces nodig aangezien het huidige ID-certificaat slechts geldig is zolang het huidige CA-certificaat geldig is. In plaats daarvan wordt er een **SHADOW-**timer gestart.

Deze timer wordt ook berekend op basis van het percentage dat in de opdracht **automatisch**

aanmelden wordt genoemd. Neem bijvoorbeeld de geldigheiddata van het hernieuwde ID-certificaat die in het vorige voorbeeld zijn weergegeven:

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

De levensduur van dit certificaat is 16 minuten. Daarom is de kanteltimer (dat wil zeggen de SHADOW-timer) 70% van 16 minuten, wat ongeveer 11 minuten overeenkomt. Deze berekening impliceert dat de router aanvragen voor zijn schaduw-/rollover-certificaten begint bij [09:30:09 + 00:11:00] = 09:41:09, wat overeenkomt met de PKI SHADOW-timer die eerder in dit document is weergegeven:

```
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-kanteling in actie

In dit gedeelte wordt de optie automatisch omrollen beschreven in actie.

Op Cisco IOS CA-server

Wanneer de SHADOW-timer verloopt, verschijnt het certificaat voor het kantelen op de 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
```

Op de clientrouter

Zoals eerder in dit document beschreven, is de automatische inschrijving optie een SHADOW-timer op de clientrouter begonnen. Wanneer de SHADOW-timer verloopt, stelt de automatische inschrijving-optie de router in staat om de CA-server te vragen voor het *omversen/schaduwCA*-certificaat. Zodra ze ontvangen is, wordt ook gevraagd naar het certificaat *voor* de *rollover/schaduw-ID*. Als resultaat hiervan heeft de router twee paar certificaten: een paar dat actueel is en het andere paar dat de rollover/schaduwcertificaten bevat:

```
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
```

Kennisgeving van de geldigheid van het certificaat van verlenging:

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

De certificaatlevensduur is slechts vier minuten (in plaats van de verwachte 20 minuten, zoals ingesteld op de Cisco IOS CA-server). Per de Cisco IOS CA server, zou de *absolute* levensduur van het certificaat van ID 20 minuten moeten zijn (wat voor een bepaalde client router betekent, de som van de leven tijden van de ID certificaten (stroom + schaduw) die aan het worden verstrekt moet niet groter zijn dan 20 minuten).

Dit proces wordt hier verder beschreven:

- Hier is de geldigheid van het huidige ID-certificaat op de router:

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

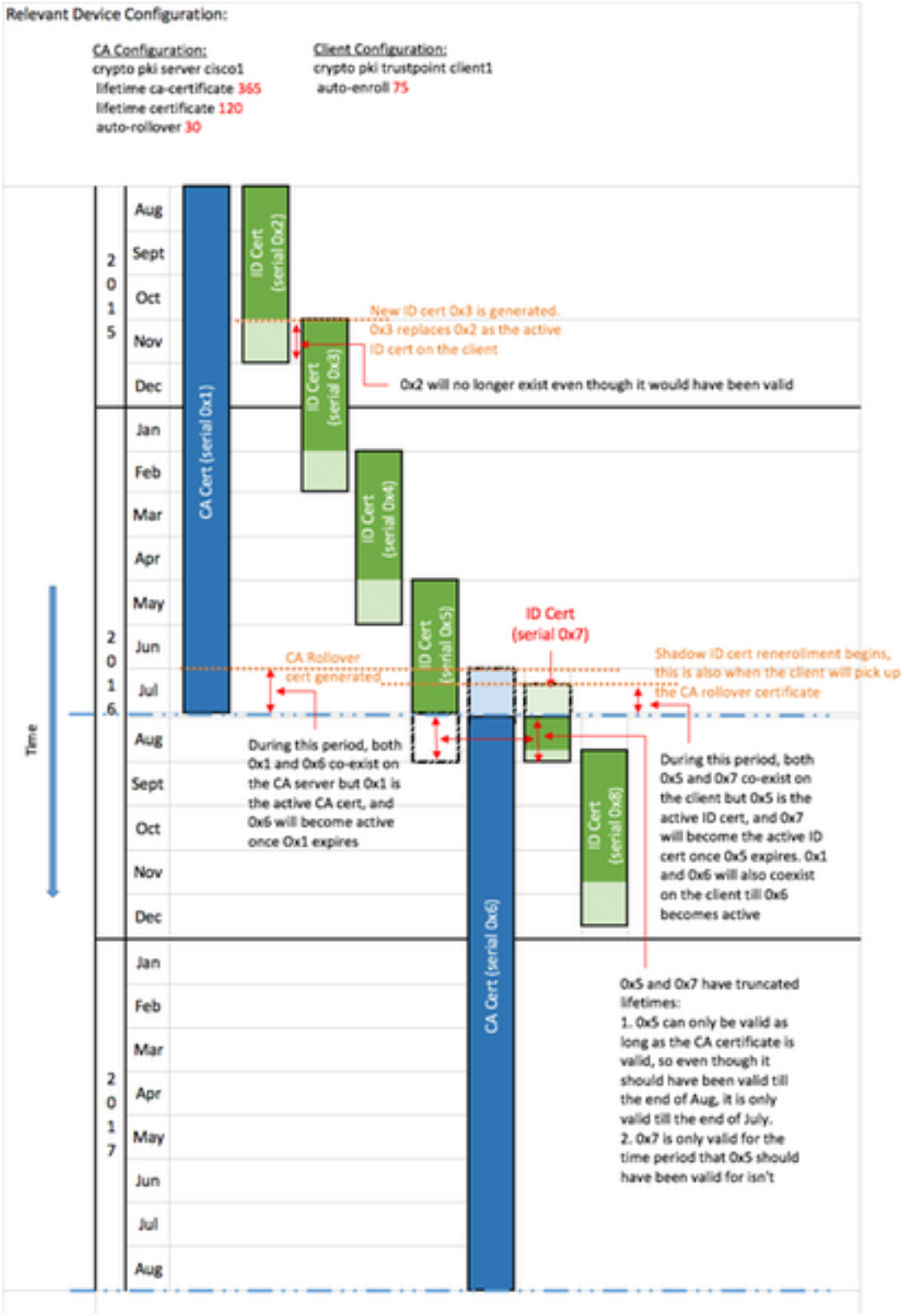
  Daarom is de *huidige_id_cert_life* 16 minuten.
- Dit is de geldigheid van het certificaat van verlenging-ID:

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

Daarom is het *rollover_id_cert_life* vier minuten.

- Per de Cisco IOS, wanneer de [huidige_id_cert_life] aan de [rollover_id_cert_leven] wordt toegevoegd, moet deze gelijk zijn aan [total_id_cert_leven]. Dat geldt in dit geval.

Steekproef tijdlijn PKI met omloopsnelheid en inschrijving



Belangrijke overwegingen

- De PKI-timers hebben een gezaghebbende klok nodig om goed te kunnen functioneren. Cisco raadt u aan NTP te gebruiken om klokken tussen de clientrouters en de Cisco IOS CA-router te synchroniseren. Bij gebrek aan NTP kan de systeem/hardwarekloktijd op de router worden gebruikt. Voor informatie over de manier waarop u de hardware-kloktijd kunt configureren en het apparaat een gezag kunt geven, raadpleegt u de Basic System Management Guide, Cisco IOS release 12.4T.

- Na het opnieuw laden van een router duurt de synchronisatie van de NTP vaak een paar minuten. De PKI-timers worden echter vrijwel onmiddellijk vastgesteld. Vanaf de versies 15.2(3.8)T en 15.2(4)S worden de PKI-timers automatisch opnieuw beoordeeld nadat NTP gesynchroniseerd is.

- De PKI-timers zijn niet absoluut; zij zijn gebaseerd op de *resterende tijd* en worden derhalve herberekend na een herstart . Ga er bijvoorbeeld vanuit dat de clientrouter is voorzien van een ID-certificaat dat 100 dagen geldig is en dat de optie voor automatische inschrijving is ingesteld op 80%. Daarna zal naar verwachting een nieuwe inschrijving plaatsvinden na de 80ste dag. Als de router op de 60e dag opnieuw wordt geladen, start deze de PKI-timer op en berekent deze opnieuw zoals hieronder wordt weergegeven: (*resterende tijd*) * (*%* auto-inschrijving) = (100-60) * 80% = 32 dagen.

  Daarom vindt opnieuw inschrijving plaats op de [60 + 32] = 92e dag.

- Wanneer u de automatische inschrijving en de auto-rollovertimers configureren is het belangrijk om ze te configureren met waarden die de SHADOW CA-certificaatbeschikbaarheid op de PKI-server toestaan wanneer de PKI-client om een computer vraagt. Dit helpt mogelijke tekortkomingen in de PKI-services in een grootschalige omgeving te verzachten.

Gerelateerde informatie

- Het implementeren van Cisco IOS Beveiliging met een Publiek-Belangrijke Infrastructuur Whitepaper
- Infrastructuur van de openbare sleutelinfrastructuur: Whitepaper over implementatievoordelen en -functies
- Configuratie-handleiding voor openbare infrastructuur
- Technische ondersteuning en documentatie – Cisco Systems