IOS PKI-implementatiegids: certificaatvernieuwing - Overzicht en bediening

Inhoud

Inleiding

Dit document beschrijft gedetailleerd de certificaatoverdracht op Cisco IOS PKI-servers en -clients van Public Key Infrastructuur (PKI).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

Hardware

- ISR-G1 [8xx, 18xx, 28xx, 38xx]
- ISR-G2 [19xx, 29xx, 39xx]
- ISR-4K [43xx, 44xx]
- ASR1k
- CSR1k

in Cisco IOS®-software

- IOS
  - Voor ISR-G1 - laatste 15.1(4)M*
  - Voor ISR-G2 - laatste 15.4(3)M
- IOS-XE
  - XE 3.15 of 15.5(2)S

Opmerking: Algemeen softwareonderhoud voor ISR-apparaten is niet langer actief, toekomstige bug-fixes of functieverbeteringen zouden een hardwareupgrade naar ISR-2 of ISR-4xxx Series routers vereisen.

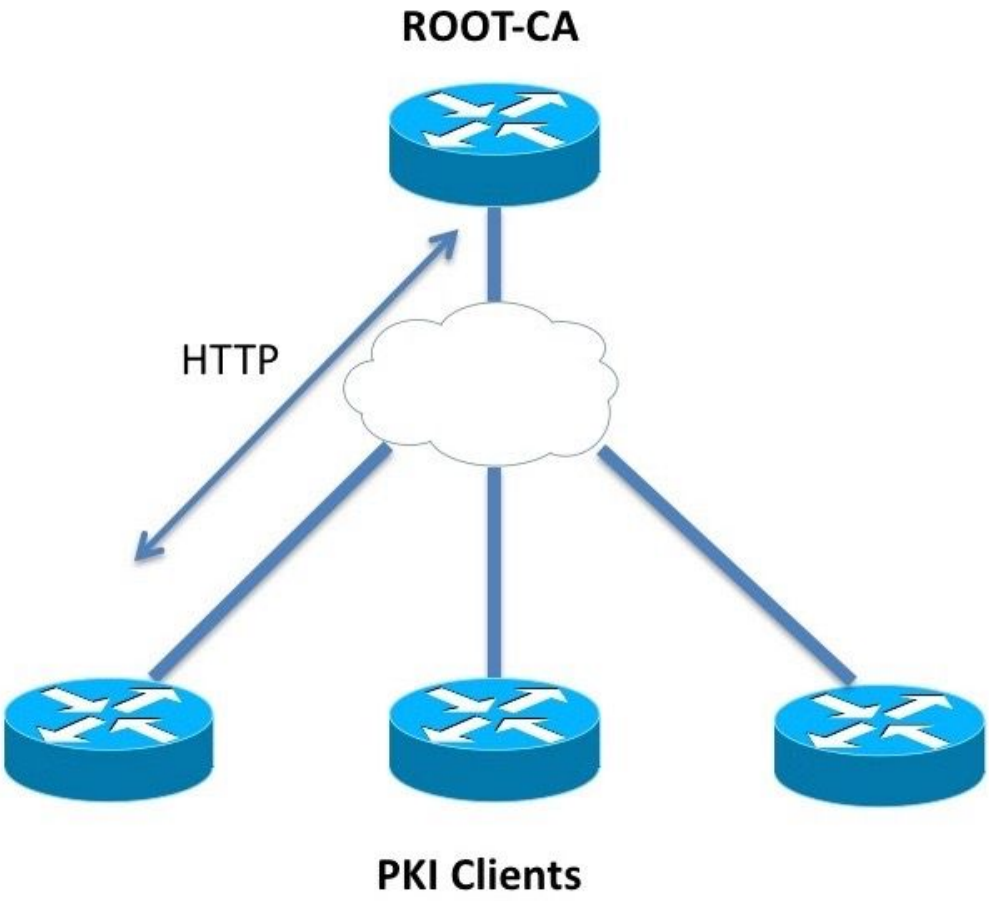
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De verlenging van het certificaat, ook bekend als vernieuwingsoperatie, zorgt ervoor dat wanneer een certificaat afloopt, een nieuw certificaat klaar is om over te nemen. Vanuit het oogpunt van een PKI Server houdt deze handeling in dat het nieuwe certificaat voor het kantelen van de server ruim van tevoren wordt gegenereerd om er zeker van te zijn dat alle PKI-klanten een nieuw certificaat voor het kantelen van de client hebben ontvangen dat door het nieuwe certificaat voor het kantelen van de server is ondertekend voordat het huidige certificaat afloopt. Vanuit het

oogpunt van een PKI-client, indien het client-certificaat vervalt maar het certificaat van de CA-server niet is, vraagt de klant om een nieuw certificaat en vervangt hij het oude certificaat zodra het nieuwe certificaat is ontvangen, en indien het client-certificaat vervalt op hetzelfde moment als het certificaat van de CA-server, zorgt de client ervoor dat het certificaat van de CA-server eerst wordt ontvangen en vraagt hij om een rollover-certificaat ondertekend door het nieuwe certificaat van het serveromverloopcertificaat van CA, en beide zullen worden geactiveerd wanneer de oude certificaten verlopen.

Instellen



PKI- en Eenvoudig certificeringsprotocol (SCEP) voorvereisten

Waarschuwing tijdbron

In IOS wordt de klokbron standaard als niet-gezaghebbend beschouwd, omdat de hardwarekloktijd niet de beste bron van de tijd is. Aangezien PKI tijdgevoelig is, is het belangrijk om een geldige bron van tijd te vormen met NTP. Bij een PKI-toepassing wordt aanbevolen alle clients en de server te laten synchroniseren met één NTP-server, indien nodig door meerdere NTP-servers. Meer daarover wordt in de IOS PKI-implementatiegids uitgelegd: Aanvankelijk ontwerp en implementatie

IOS formatteert de PKI-timers niet zonder een gezaghebbende klok. Hoewel NTP sterk wordt aanbevolen, kan de beheerder als tijdelijke maatregel de hardwarekloktijd als gezaghebbend aanduiden met:

```
Router(config)# clock calendar-valid
```

HTTP-communicatie

Een vereiste voor een actieve IOS PKI Server is HTTP server, die kan worden geactiveerd met deze configuratie-level opdracht:

```
ip http server <1024-65535>
```

Deze opdracht maakt HTTP-server standaard mogelijk op poort 80, die kan worden gewijzigd zoals hierboven wordt weergegeven.

PKI-clients moeten met de PKI-server via HTTP naar de geconfigureerde poort kunnen communiceren.

PKI-configuratie

Server - Rollover

De automatische kantelconfiguratie van de PKI-server ziet er zo uit:

```
crypto pki server ROOTCA
 database level complete
 database archive pkcs12 password 7 01100F175804575D72
 issuer-name CN=RootCA,OU=TAC,O=Cisco
 grant auto
 lifetime certificate 365
 lifetime ca-certificate 730
 database url ftp://10.1.1.1/DB/ROOTCA/
 auto-rollover 90
```

De auto-omloopparameter wordt in dagen gedefinieerd. Op een meer granulair niveau ziet de opdracht er uit:

```
auto-rollover <days> <hours> <minutes>
```

Een waarde van 90 auto-omloopdatums geeft aan dat de IOS 90 dagen voor het verstrijken van het huidige servercertificaat een certificaat voor rollover-server aanmaakt en dat de geldigheid van dit nieuwe omverloopcertificaat tegelijk met de vervaltijd van het huidige actieve certificaat begint.

Auto-rollover moet zo worden geconfigureerd dat het certificaat voor kantelen CA ruim van tevoren op de PKI-server wordt gegenereerd voordat een PKI-client in het netwerk GetNextCACert-handeling uitvoert zoals wordt beschreven in het gedeelte **SHADOW-overzicht** hieronder.

Clientvernieuwing

De automatische configuratie van de PKI-client voor vernieuwing van het certificaat ziet er zo uit:

```
crypto pki trustpoint Root-CA
  enrollment url http://172.16.1.1:80
  serial-number
  ip-address none
  password 0 Rev0cati0n$Passw0rd
  subject-name CN=spoke-1.cisco.com,OU=CVO
  revocation-check crl
  rsakeypair spoke-1-RSA
   auto-enroll 80
```

Hier staat, de **auto-inschrijving <percentage> [regenereert]** opdracht dat IOS certificatievernieuwing moet uitvoeren op precies 80% van de levensduur van het huidige certificaat.

Het sleutelwoord **regenereert** staten dat IOS het belangrijkste-paar van RSA zou moeten regenereren dat als schaduw zeer belangrijk-paar bekend is tijdens elke certificaat vernieuwingsoperatie.

Let goed op bij het configureren van het percentage automatische inschrijving. Op elke PKI-cliënt in de installatie, indien een voorwaarde ontstaat wanneer het identiteitsbewijs op hetzelfde tijdstip als het certificaat van uitgifte van CA afloopt, moet de waarde van de auto-inschrijving altijd de [schaduw] vernieuwingsoperatie starten nadat de CA het certificaat van wederomloop heeft aangelegd. *Raadpleeg het* gedeelte **PKI Timer-**afhankelijkheden onder de voorbeelden van implementaties.

PKI-vernieuwing/Rollover-voorwaarden

In dit document worden de herhalings- en vernieuwingsoperaties van de certificaten uitvoerig behandeld en worden deze gebeurtenissen als succesvol beschouwd:

- Initialisatie van PKI-server met een geldig CA-certificaat.
- PKI-klanten zijn met succes bij de PKI-server ingeschreven. d.w.z. elke PKI-cliënt heeft het CA-certificaat en een identiteitsbewijs, ook bekend als een routercertificaat.

Het betreden van een cliënt impliceert deze gebeurtenissen. Zonder te veel in detail te gaan:

- Verificatie van schaalpunten
- inschrijving van schaalpunten

In IOS is een betrouwbaar punt een container voor certificaten. Elk betrouwbaar punt kan één actief identiteitsbewijs en/of één actief CA-certificaat bevatten. Een betrouwbaar punt wordt als echt beschouwd als het een actief CA-certificaat bevat. Het wordt als ingeschreven beschouwd als het een identiteitsbewijs bevat. Een betrouwbaar punt moet vóór een inschrijving geauthentiseerd zijn. PKI Server- en clientconfiguratie, evenals verificatie en inschrijving van vertrouwenspunten, worden in detail behandeld in IOS PKI-implementatiegids: Aanvankelijk ontwerp en implementatie

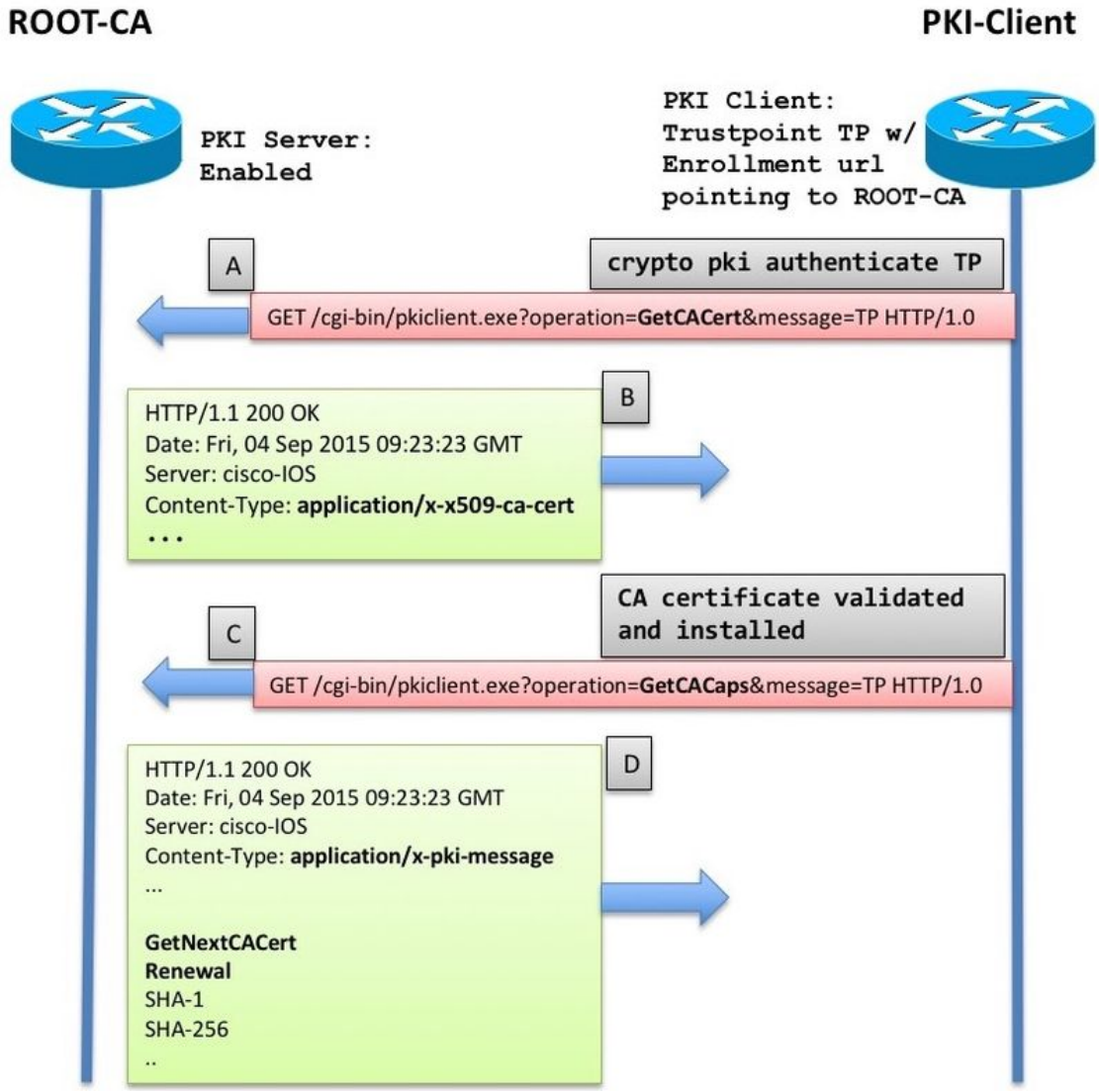
Na de CA certificatenwinning/installatie, wint de PKI client de PKI servermogelijkheden terug alvorens een inschrijving uit te voeren. CA-functies ophalen wordt in deze sectie uitgelegd.

CA-functies

In IOS, wanneer een PKI-client een CA authentiek verklaarde, met andere woorden, wanneer een

beheerder een betrouwbaar punt op een IOS-router maakt en het commando **crypto-encryptie** uitvoert **om <trustpoint-name>te authentiseren**, vinden deze gebeurtenissen plaats op de router:

- IOS verstuurt een SCEP-verzoek met het type GetCACert-handeling.
- De verwachte reactie hier is een HTTP-bericht met een type **toepassing/x-x509-ca-cert** in geval van een CA-inzet, of **toepassing/x-x509-ca-ra-cert** in geval van een RA en een CA-inzet. En het HTTP lichaam bevat het CA certificaat. [en een RA-certificaat in het laatste geval].
- Na het ophalen en installeren van het CA/RA certificaat, opent de client een automatisch SCEP verzoek met GetCACaps-handeling.
- De verwachte reactie hier is een HTTP-bericht met een content-type van **applicatie/x-pki-bericht**, dat ook **tekst/simpel** kan zijn en het HTTP-orgaan bevat een reeks functies ondersteund door de CA, gescheiden door een lijnvoerteken. Een typische IOS PKI Server-respons is zoals in het onderstaande schema wordt getoond.



De reactie wordt als volgt geïnterpreteerd door de IOS PKI-client:

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

Van deze mogelijkheden richt dit document zich op deze twee.

GetNextCACert

Wanneer deze mogelijkheid door CA wordt teruggegeven, begrijpt IOS dat CA de Rollover van CA-certificaat ondersteunt. Als deze mogelijkheid wordt teruggegeven, als de opdracht **automatisch registreren** niet is ingesteld onder het vertrouwde punt, formatteert IOS een SHADOW-timer die is ingesteld op 90% van de geldigheid van het CA-certificaat.

Wanneer de SHADOW-timer verloopt, voert IOS GetNextCACert SCEP-handeling uit om het certificaat van Rollover CA te halen.

> **Opmerking**: Als **de** opdracht **automatisch registreren** is geconfigureerd onder het trustpunt in combinatie met een **inschrijvingsregel**, wordt een RENEW-timer gestart voordat hij het vertrouwenspunt echt authentiek maakt en probeert deze constant bij de CA in te schrijven op de **inschrijvingsregel**, alhoewel er geen feitelijk inschrijvingsbericht [CSR] wordt verstuurd tot het vertrouwenspunt echt is.

> **Opmerking:** GetNextCACert wordt verzonden als een mogelijkheid door de IOS PKI-server, ook al is **de** automatische omloopsnelheid niet ingesteld op de server

Verlengen

Met deze mogelijkheid informeert de PKI-server de PKI-client dat ze een actief ID-certificaat kan gebruiken om een certificaatondertekeningsaanvraag te ondertekenen om het bestaande certificaat te verlengen.

Meer hierover in het gedeelte **Auto-Verlengen van client** in **PKI**.

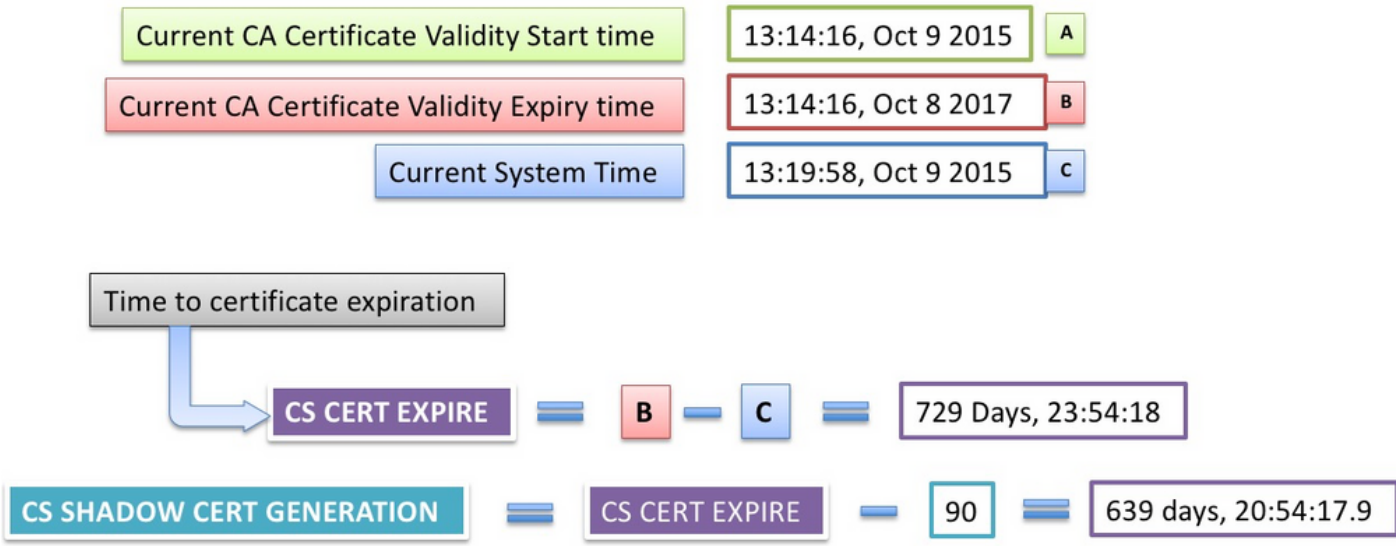
Auto-Rollover voor PKI-servers

Met de bovenstaande configuratie op de CA Server ziet u:

```
Root-CA#show crypto pki certificates
CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
   ou=TAC
   o=Cisco
 Subject:
   cn=RootCA
   ou=TAC
   o=Cisco
 Validity Date:
   start date: 13:14:16 CET Oct 9 2015
   end   date: 13:14:16 CET Oct 8 2017
 Associated Trustpoints: ROOTCA

Root-CA#terminal exec prompt timestamp

Root-CA#show crypto pki timers
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 13:19:58.946 CET Fri Oct 9 2015
PKI Timers
|        7:49.003
 |        7:49.003  SESSION CLEANUP
 |  3d 7:05:24.003  TRUSTPOOL
CS Timers
|     5:54:17.977
 |     5:54:17.977  CS CRL UPDATE
 |639d23:54:17.977  CS SHADOW CERT GENERATION
 |729d23:54:17.971  CS CERT EXPIRE
```

Let op:



Rollover-handeling

Wanneer de timer voor de **CS SHADOW CERT GENERATION** vervalt:

- IOS genereert eerst een rollover-key-paar - het heeft momenteel dezelfde naam als het actieve key-paar met een # hash als bijlage aan deze knop toegevoegd.

```
Jul 10 13:14:16.510: CRYPTO_CS: shadow generation timer fired.
Jul 10 13:14:16.510: CRYPTO_CS: key 'ROOTCA#' does not exist; generated automatically

Root-CA# show crypto key mypubkey rsa
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 13:19:19.652 CET Mon Jul 10 2017

% Key pair was generated at: 13:14:16 CET Oct 9 2015
Key name: ROOTCA
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
```

```
Key is not exportable.
Key Data&colon;
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B07127
360CF006 13B259CE 7BB8158D E6BC8AA4 8A763F73 50CE64B0 71AC5D93 ED59C936
F751D810 70CEA8C8 B0023B4B 0FB9A538 A1C118D3 5530D46D C4B4DC14 3BD1D231
48B0C053 A781D0C7 86DEE9DE CCA58C18 B5804B29 911D1D57 76B3EC3F 42D38C3A
1E0F8DD9 1DE228B9 95AC3C10 87C132FC 75956338 258727F6 1A1F0818 83020301 0001

% Key pair was generated at: 13:14:18 CET Jul 10 2017
Key name: ROOTCA#
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data&colon;
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00BF2A52
687F112B C9263541 BB402939 9C66D270 8D3EACED 4F63AA50 9FB340E8 38C8AC38
1818EA43 93C17CA1 C4917F43 C9199C9E F9F9C059 FDE11DA9 C7991826 43736FCE
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

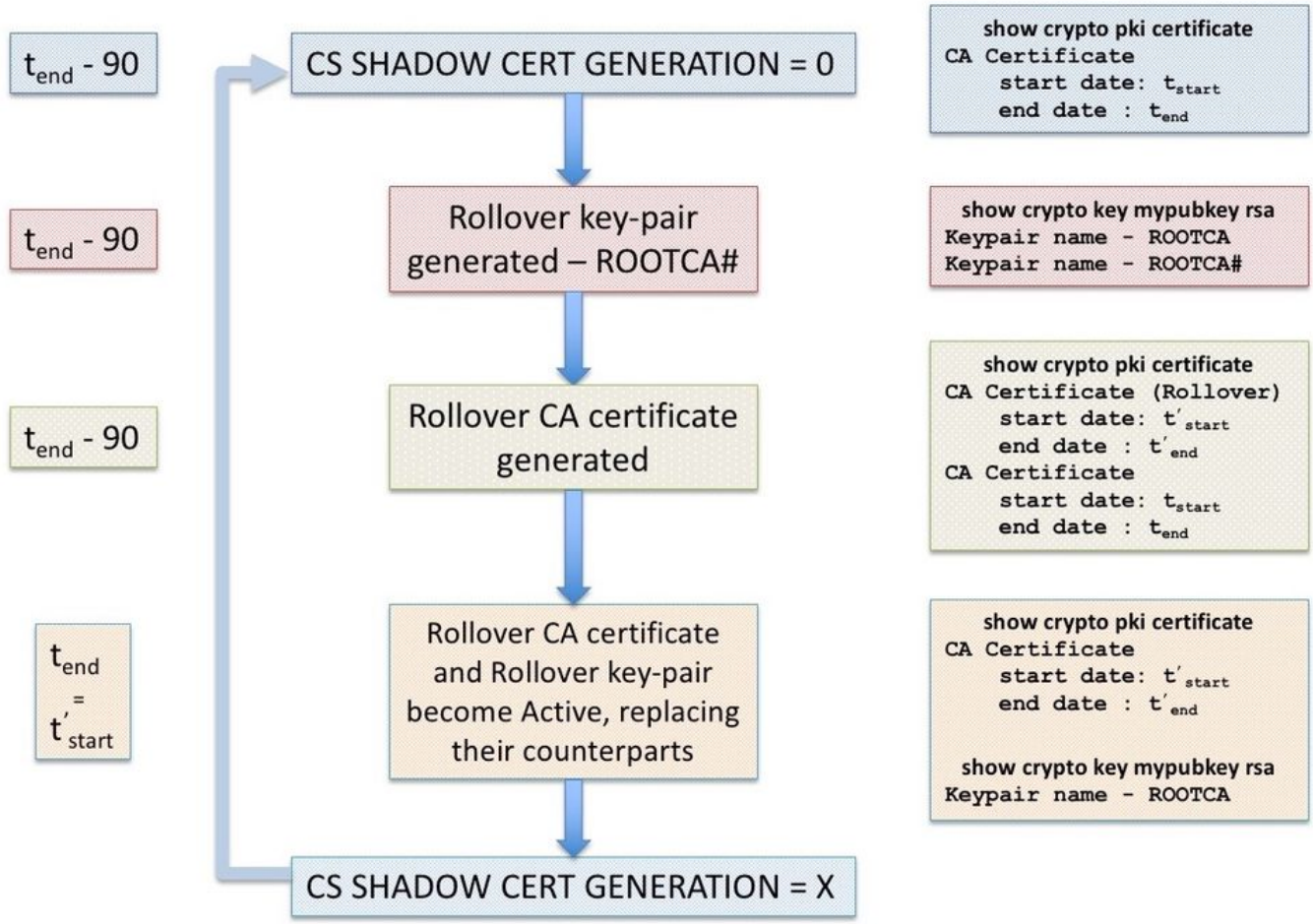
- IOS genereert vervolgens het CA-certificaat, waar de datum van de geldigheidstart dezelfde is als de datum van de geldigheideinddatum van het huidige actieve CA-certificaat.

```
Jul 10 13:14:18.326: CRYPTO_CS: shadow CA successfully created.
Jul 10 13:14:18.326: CRYPTO_CS: exporting shadow CA key and cert
Jul 10 13:14:18.327: CRYPTO_CS: file opened: ftp://10.1.1.1/DB/ROOTCA/ROOTCA_00001.p12
```

```
Root-CA# show crypto pki certificates
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 13:14:46.820 CET Mon Jul 10 2017

CA Certificate (Rollover)
 Status: Available
 Certificate Serial Number (hex): 03
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
   ou=TAC
   o=Cisco
 Subject:
   Name: RootCA
   cn=RootCA
   ou=TAC
   o=Cisco
 Validity Date:
   start date: 13:14:16 CET Oct 8 2017
   end   date: 13:14:16 CET Oct 8 2019
 Associated Trustpoints: ROOTCA

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
   ou=TAC
```

```
    o=Cisco
  Subject:
    cn=RootCA
    ou=TAC
    o=Cisco
  Validity Date:
    start date: 13:14:16 CET Oct 9 2015
     end   date: 13:14:16 CET Oct 8 2017
  Associated Trustpoints: ROOTCA
  Storage: nvram:RootCA#1CA.cer

Root-CA# show crypto pki server
Certificate Server ROOTCA:
Status: enabled
State: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=RootCA,OU=TAC,O=Cisco
CA cert fingerprint: CC748544 A0AB7832 935D8CD0 214A152E
Granting mode is: manual
Last certificate issued serial number (hex): 6
CA certificate expiration timer: 13:14:16 CET Oct 8 2017
CRL NextUpdate timer: 19:11:54 CET Jul 10 2017
Current primary storage dir: unix:/iosca-root/
Database Level: Complete - all issued certs written as <serialnum>.cer
 Rollover status: available for rollover
Rollover CA certificate fingerprint: 031904DC F4FAD1FD 8A866373 C63CE20F
 Rollover CA certificate expiration time: 13:14:16 CET Oct 8 2019
Auto-Rollover configured, overlap period 90 days

Root-CA# show run | section chain ROOTCA
crypto pki certificate chain ROOTCA
 certificate ca rollover 03
  30820237 308201A0 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  2F310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
  0F300D06 03550403 1306526F 6F744341 301E170D 31373130 30383132 31343136
  5A170D31 39313030 38313231 3431365A 302F310E 300C0603 55040A13 05436973
  636F310C 300A0603 55040B13 03544143 310F300D 06035504 03130652 6F6F7443
  4130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100BF2A
  52687F11 2BC92635 41BB4029 399C66D2 708D3EAC ED4F63AA 509FB340 E838C8AC
  381818EA 4393C17C A1C4917F 43C9199C 9EF9F9C0 59FDE11D A9C79918 2643736F
  CEA80D0C EE2378F2 3B6AC5FC 3B4A7A01 20D391BE 8FA9AFD2 12E05A28 64661023
  3CE0E58D 9323AA0E D2A5B1C1 40122E6E 3D98A7D9 74E23639 0270A89C E3BF0203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1419FCA4 DDE84233 F79C066F
  93CCF6B3 E14F8355 31301D06 03551D0E 04160414 19FCA4DD E84233F7 9C066F93
  CCF6B3E1 4F835531 300D0609 2A864886 F70D0101 04050003 81810065 AC780BB4
  2398D765 BE4C4C0A 0D0F16C0 82530D85 99933BDC 8388C46D 926145D8 B0BA275A
  93AAB497 FC876F6A E951C138 F5D652AE C0C25E2A FDD80BAA C6BD5A78 E439158F
  5544F30F 33C59E22 1994A8D3 AADC1287 BD15A104 55CB5DC3 49A9401A 8DB3940A
  5054EA21 99CCE4F3 40B471FE DEB4BB38 AC3ACD48 4CDDCBC9 9829D3
      quit
certificate ca 01
  30820237 308201A0 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  2F310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
  0F300D06 03550403 1306526F 6F744341 301E170D 31353130 30393132 31343136
  5A170D31 37313030 38313231 3431365A 302F310E 300C0603 55040A13 05436973
  636F310C 300A0603 55040B13 03544143 310F300D 06035504 03130652 6F6F7443
  4130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100B071
  27360CF0 0613B259 CE7BB815 8DE6BC8A A48A763F 7350CE64 B071AC5D 93ED59C9
  36F751D8 1070CEA8 C8B0023B 4B0FB9A5 38A1C118 D35530D4 6DC4B4DC 143BD1D2
  3148B0C0 53A781D0 C786DEE9 DECCA58C 18B5804B 29911D1D 5776B3EC 3F42D38C
  3A1E0F8D D91DE228 B995AC3C 1087C132 FC759563 38258727 F61A1F08 18830203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
```

```
01FF0404 03020186 301F0603 551D2304 18301680 148D421A BED6DCAD B8CFE4B4
1B2C7E41 C73428AC 9A301D06 03551D0E 04160414 8D421ABE D6DCADB8 CFE4B41B
2C7E41C7 3428AC9A 300D0609 2A864886 F70D0101 04050003 8181008C 3495278E
DA6C14B0 533E746D 8DA743AF 06BE4088 913BF9BC A94576FA BC86EFD1 1DFE6B9F
0D244144 473C67AD 24414A20 84E9B083 D1720766 0A698C29 115482C6 2FB57E86
95CDECF2 29662362 866CDC91 730ADBB3 BDBBDC3C EA5301B0 150658E7 AF722BD7
6B5C2D6A 661A4FED CDA32DE5 D6C2CE7A 544086DC F957A87C 2C07FF
    quit
```



Handmatig kantelen van de PKI-server

IOS PKI Server ondersteunt het handmatig uploaden van het CA certificaat, d.w.z. dat een beheerder de generatie van een CA-certificaat vooraf kan activeren zonder dat hij de **auto-omvergooi** onder de PKI-serverconfiguratie hoeft te configureren. Het is sterk aanbevolen om de **auto-omvergooien** te configureren of niet iemand van plan is de levensduur van een aanvankelijk uitgezette CA server te verlengen om op de veiliger kant te zijn. **PKI-klanten kunnen de CA overladen zonder een CA-certificaat voor het kantelen**. *Raadpleeg* Dependency of Client SHADOW operation op PKI Server Rollover.

Er kan een handomdraai worden geactiveerd met de opdracht voor het configuratieniveau:

```
crypto pki server <Server-name> rollover
```

Bovendien kan een CA-certificaat omverwerpen om zelf een fris certificaat te genereren, maar een beheerder dient dit niet te doen in een productieomgeving, met behulp van:

```
crypto pki server <Server-name> rollover cancel
```

Hiermee worden de rollover rsa key-pair en het rollover CA-certificaat verwijderd. Dit wordt

geadviseerd om:

- Zodra de CA het overloopcertificaat genereert, kunnen meerdere klanten het overloopcertificaat van CA downloaden evenals een overloopclient-certificaat dat door het overloopcertificaat van CA is ondertekend.
- In dit stadium, indien het kantelen wordt geannuleerd, moet de cliënt misschien opnieuw worden ingeschreven.

PKI-clientautomatische vernieuwing

Soorten verlenging van clientcertificaten - VERLENGEN EN SCHADUWEN

IOS op de PKI-server zorgt er altijd voor dat de vervaltijd van het aan de client afgegeven ID-certificaat nooit verder gaat dan de vervaltijd van het CA-certificaat.

Op een PKI-client houdt IOS altijd rekening met de volgende timers voordat u de hervernieuwingshandeling voorbereidt:

- Vervaltijd van de verlenging van het identiteitsbewijs
- Vervaltijd van het certificaat van de uitgevende instelling (CA)

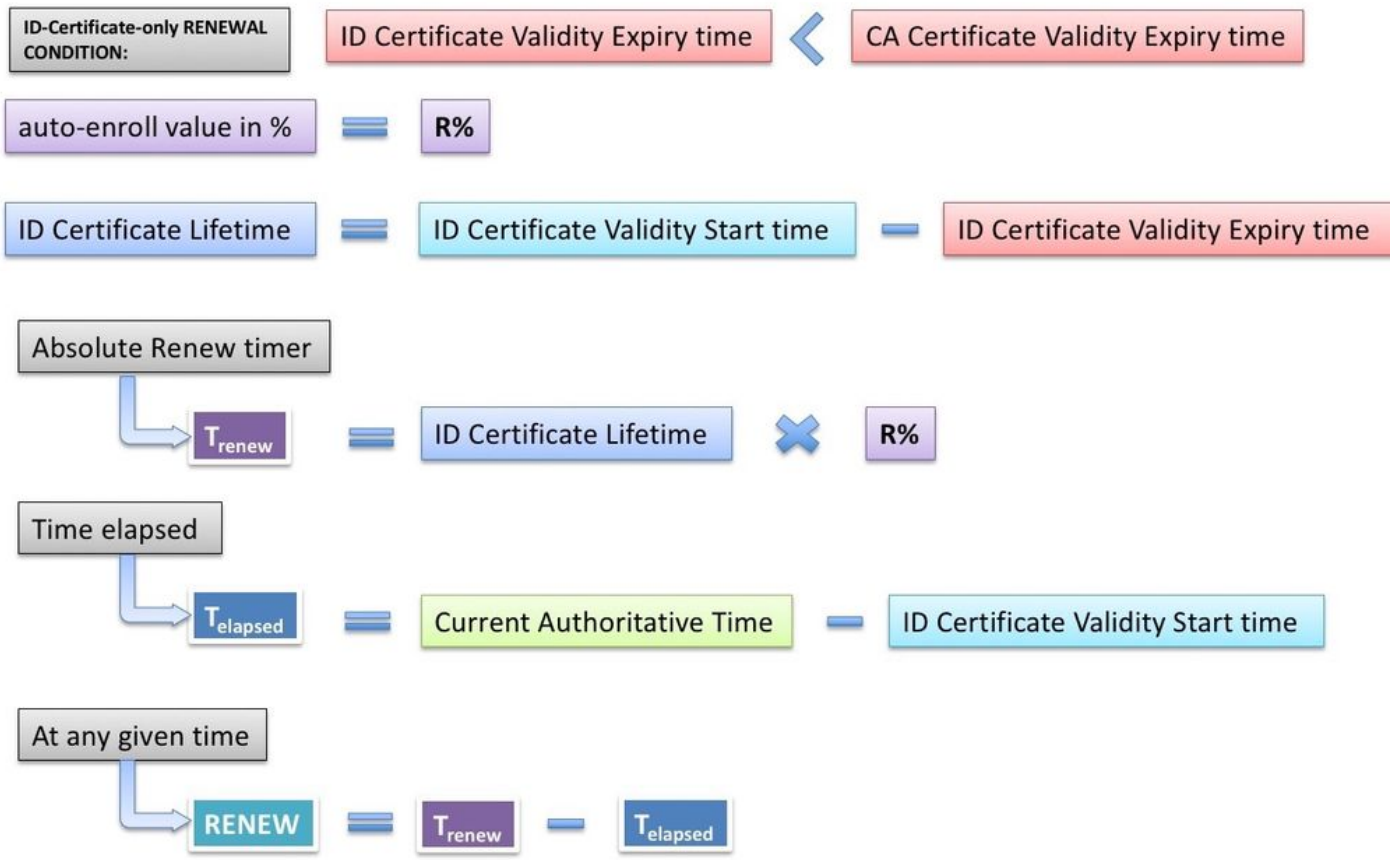
Als de vervaltijd van het identiteitsbewijs niet de tijd van het verlooptijd van het CA certificaat is, IOS voert een eenvoudige hernieuwing uit.

Als de Vervaltijd van het Identiteitscertificaat hetzelfde is als de vervaltijd van het CA certificaat, voert IOS een schaduwvernieuwing operatie uit.

VERLENGEN - Verlenging van identiteitsbewijs van router

Zoals eerder vermeld, verricht IOS PKI-cliënt een eenvoudige hernieuwing indien de vervaltijd van het identiteitsbewijs niet dezelfde is als de vervaltijd van het CA-certificaat, d.w.z. het identiteitsbewijs dat vervalt voordat het certificaat van de uitgevende instelling een eenvoudige verlenging van het identiteitsbewijs met zich meebrengt.

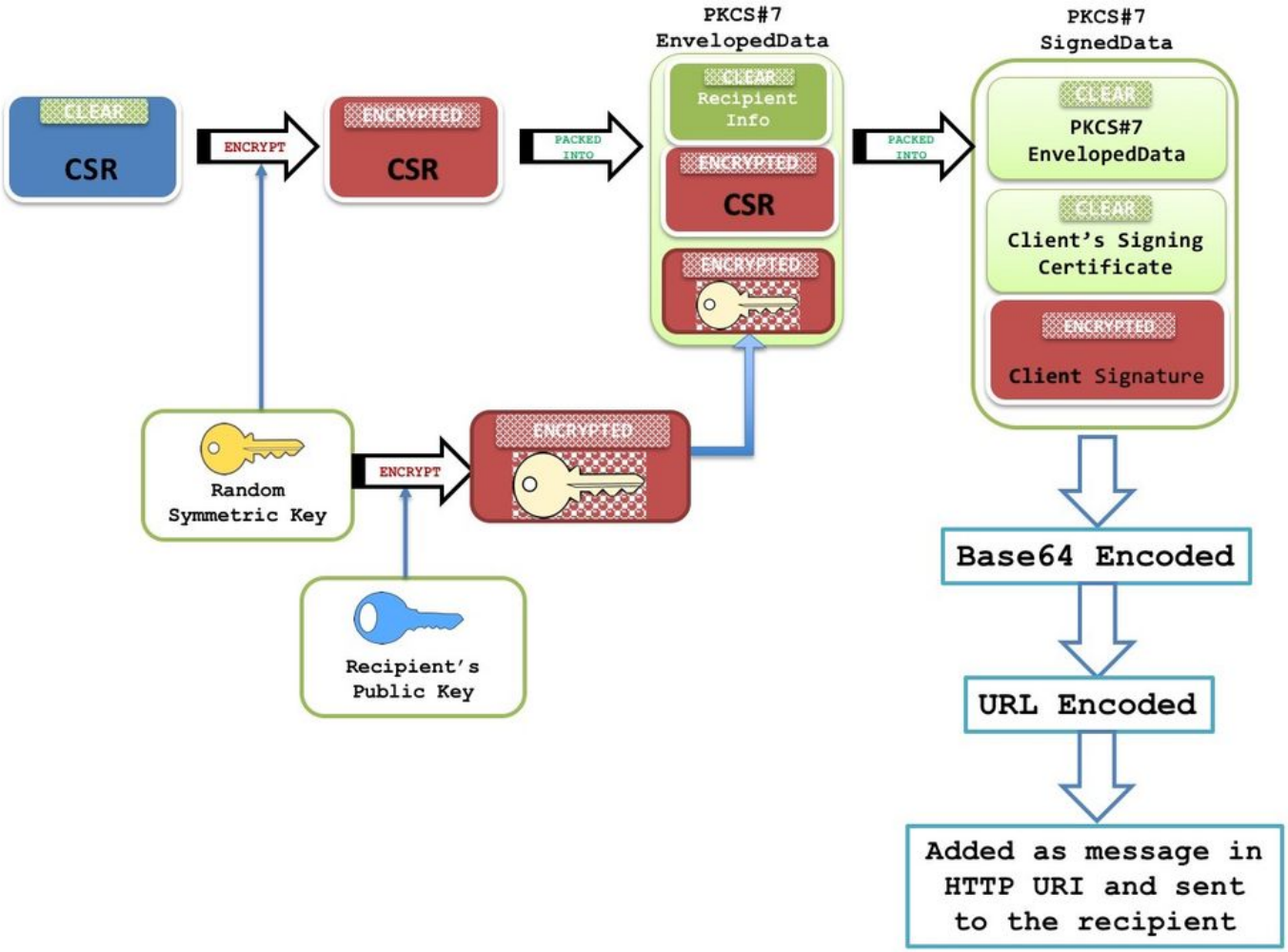
Zodra een identiteitsbewijs is geïnstalleerd, berekent IOS de RENEW-timer voor het specifieke trust-punt zoals hieronder wordt weergegeven:



De huidige tijd-gezaghebbend-tijd betekent dat de systeemklok een gezaghebbende bron van tijd moet zijn zoals hier beschreven wordt. (link naar een gezaghebbende sectie van de Tijdbron) PKI-timers zullen niet worden geïnitialiseerd zonder een gezaghebbende bron van de tijd. Als gevolg daarvan zal er geen vernieuwingsoperatie plaatsvinden.

De volgende gebeurtenissen vinden plaats wanneer de RENEW-timer verstrijkt:

- IOS genereert een schaduwtoetsenbord als **regenereren** is ingesteld [voorbeeld: auto-inschrijving 80 regenereren]. Zonder **regenereren** IOS gebruikt u het momenteel actieve RSA key-paar opnieuw.
- IOS maakt een geformatteerd PKCS-10 certificaatverzoek in, dat dan in een PKCS-7 envelop wordt versleuteld. Deze enveloppe bevat ook de ontvangerInfo, die de onderwerp-naam en het serienummer van de uitgevende CA is. Deze PKCS7-enveloppe wordt op zijn beurt verpakt in een ondertekende PKCS-7-data. Tijdens de eerste inschrijving gebruikt IOS een zelfondertekend certificaat om dit bericht te ondertekenen. En tijdens de volgende inschrijvingen, d.w.z. herinschrijvingen, gebruikt IOS het actieve identiteitscertificaat om het bericht te ondertekenen. De door PKCS7 ondertekende gegevens zijn ook opgenomen in het ondertekeningscertificaat, d.w.z. het zelf ondertekende certificaat of het identiteitsbewijs.



Raadpleeg voor meer informatie over deze pakketstructuur het SCEP - Overzicht document

> **Opmerking:** De belangrijkste informatie hier is de Ontvangende Info die de onderwerp-naam en het serienummer van de uitgevende CA is, en de openbare sleutel van deze CA wordt gebruikt om de symmetrische sleutel te versleutelen. De CSR in de PKCS7 envelop wordt versleuteld met deze symmetrische sleutel.

Deze versleutelde symmetric-key wordt gedecrypteerd door de ontvangende CA met behulp van zijn private sleutel, en deze symmetrische toets wordt gebruikt om de PKCS7-envelop te decrypteren die de CSR onthult.

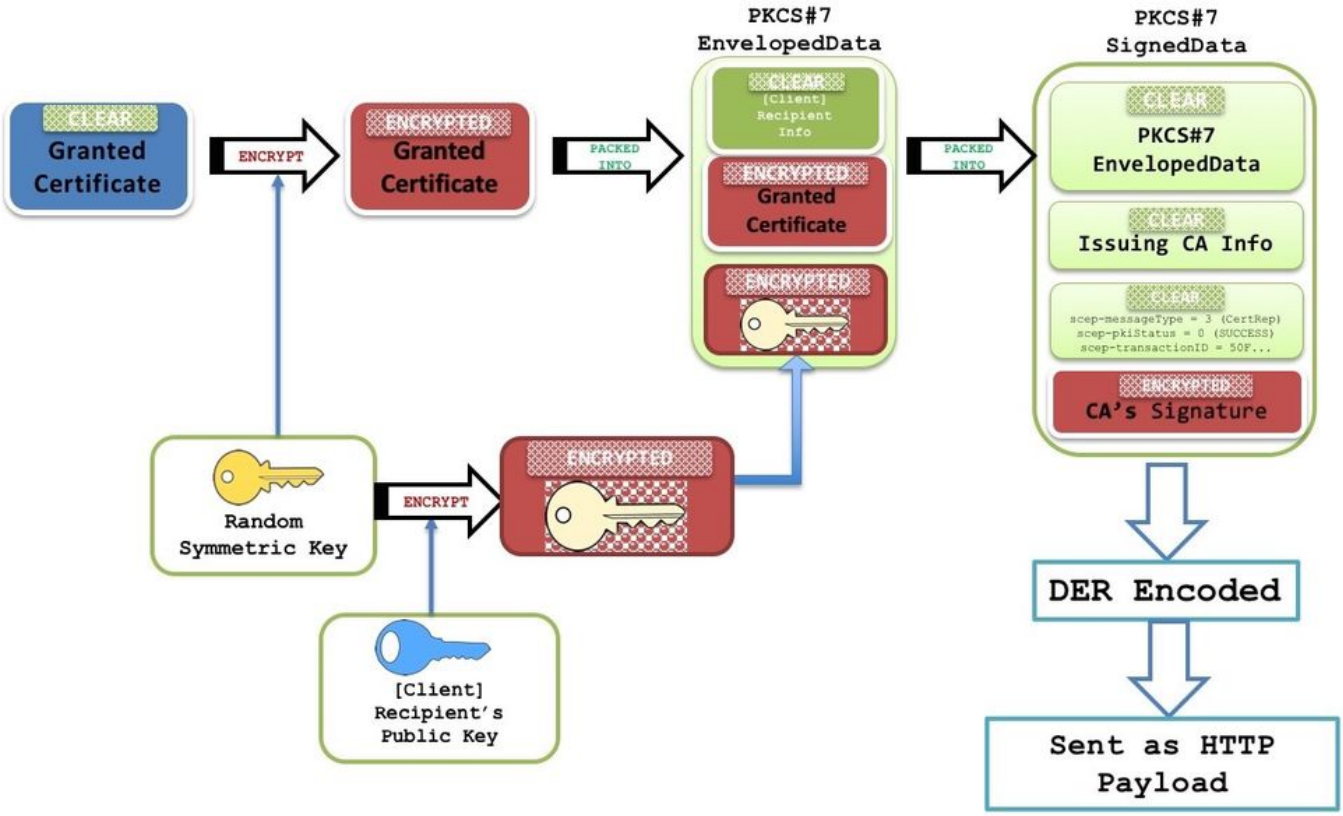
- Dit certificaatverzoek (CSR), verpakt in PKCS7-formaat, wordt vervolgens naar de CA verzonden met een SCEP-berichttype van PKCSReq en een SCEP-operatie genaamd PKIOperation.
- Als de CA het verzoek afwijst, stopt IOS de RENEW-timer. Vanaf dit punt op moet de beheerder om het identiteitsbewijs te vernieuwen een handmatige vernieuwing uitvoeren (link naar **PKI client Manual-Renewal** sectie)
- Als CA een status als **hangend** SCEP stuurt, start IOS op de PKI client een POLL-timer vanaf 60 seconden of 1 minuut. Elke keer dat een POLL-timer afloopt, stuurt IOS GetCertInitiële SCEP-bericht via een PKIO-bewerking. Als de eerste POLL-timer afloopt, als op het GetCertInitiële bericht wordt gereageerd met een SCEP-wachtstatus, wordt het eerste POLL-timer opnieuw op 1 minuut gezet, wordt de timer opnieuw op 2 minuten uitgezet, wordt de derde POLL-timer opnieuw uitgezet tot 4 minuten Dus voor de volgende 999 opnieuw per

default of tot het afgeven van het CA-certificaat afloopt.
De Polen telling en de eerste herstartperiode kunnen worden ingesteld met behulp van:

```
   crypto pki trustpoint <TP>
     enrollment retry count <total retry count>
enrollment retry period <first retry period in minutes>
```

- Wanneer het certificaat wordt verleend op de PKI Server, wordt het volgende GetCertInitiële SCEP bericht beantwoord met een HTTP bericht van het type **toepassing/x-pki-bericht** en een lichaam dat een getekend PKCS#7 ondertekende gegevens bevat. Deze door PKCS7 ondertekende gegevens bevatten de SCEP status als **toegekend**, en ook een PKCS7-enveloppe. Deze gegevens zijn verpakt in PKCS en bevatten het afgegeven certificaat en de ontvangstinformatie, de naam en het serienummer van het zelfgetekende certificaat tijdens de eerste inschrijving en van het actieve identiteitsbewijs tijdens de herinschrijving.

  De gegevens met een enveloppe van PKCS7 bevatten ook een symmetrische sleutel die versleuteld is met de openbare sleutel van de ontvanger (waarvoor het nieuwe certificaat werd toegekend). Het ontvangen van router decrypteert het met de privé sleutel. Deze duidelijke symmetrische sleutel wordt dan gebruikt om de PKCS#7 enveloped data te decrypteren, wat het nieuwe identiteitscertificaat onthult.



- In deze fase vervangt IOS het bestaande identiteitsbewijs onmiddellijk door het nieuwe certificaat. Als **regenereren** werd ingesteld, vervangt het schaduwpaar ook het actieve sleutelpaar.

- Ook wordt de einddatum van het nieuwe certificaat vergeleken met de einddatum van het CA-certificaat om te bepalen of de RENEW-timer moet worden geïnitialiseerd of een SHADOW-timer moet worden geïnitialiseerd zoals hier wordt uitgelegd <href **Typen clientcertificaatvernieuwing - RENEW en SHADOW>**