IOS PKI-Bereitstellungsleitfaden: Tool-Rollover - Überblick über Konfiguration und Betrieb

Inhalt

Einführung

Dieses Dokument beschreibt ausführlich die Zertifikatsweiterleitung auf Cisco IOS Public Key

Infrastructure (PKI)-Servern und -Clients.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

Hardware

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

Software

- IOS
  - Für ISR-G1 - Neueste Version 15.1(4)M*
  - Für ISR-G2 - Neueste 15.4(3)M
- IOS-XE
  - XE 3.15 oder 15.5(2)S

Hinweis: Die allgemeine Softwarewartung für ISR-Geräte ist nicht mehr aktiv. Für künftige Bugfixes oder Funktionsverbesserungen ist ein Hardware-Upgrade auf ISR-2- oder ISR-4xxx-Router erforderlich.

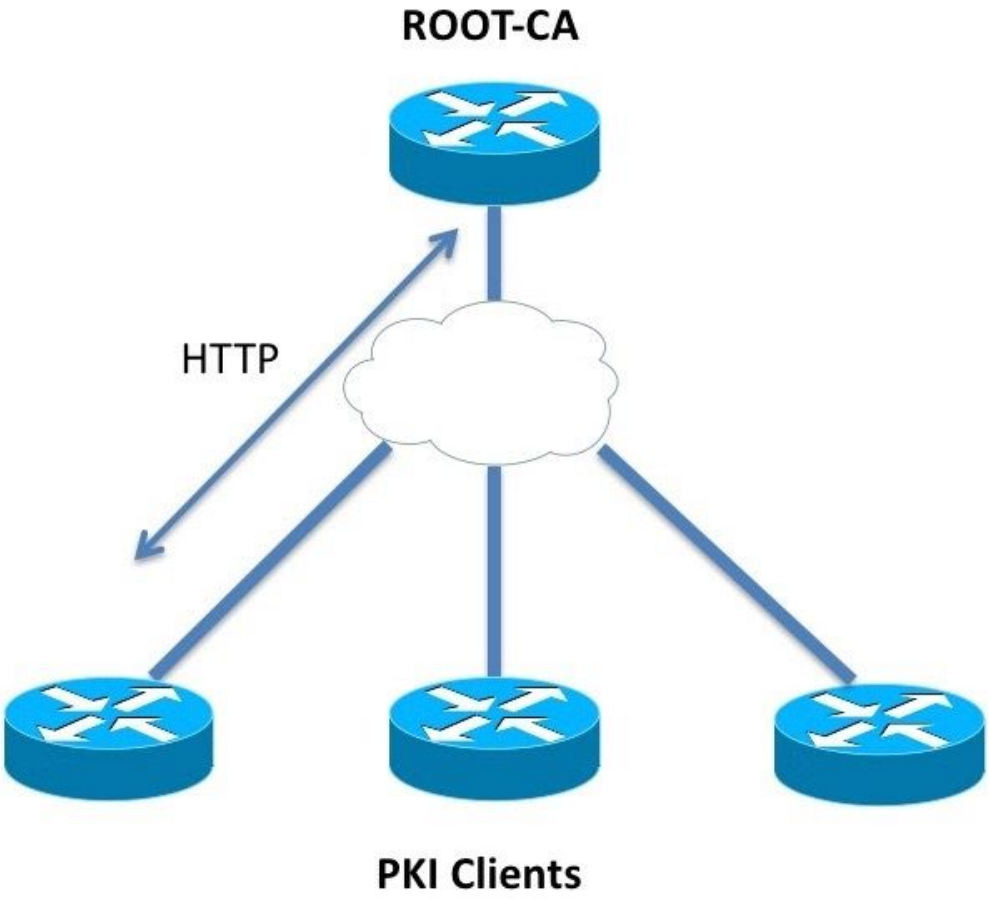
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Hintergrundinformationen

Durch das Rollover von Zertifikaten, auch als Verlängerungsvorgang bezeichnet, wird sichergestellt, dass ein neues Zertifikat nach Ablauf eines Zertifikats übernommen werden kann. Aus Sicht eines PKI-Servers bedeutet dieser Vorgang, dass das neue Server-Rollover-Zertifikat rechtzeitig im Voraus generiert wird, um sicherzustellen, dass alle PKI-Clients ein neues Client-Rollover-Zertifikat erhalten haben, das vom neuen Server-Rollover-Zertifikat signiert wurde, bevor das aktuelle Zertifikat abläuft. Wenn das Clientzertifikat abläuft, das Zertifikat des CA-Servers aber

nicht, fordert der Client ein neues Zertifikat an und ersetzt das alte Zertifikat, sobald das neue Zertifikat eingegangen ist. Wenn das Clientzertifikat gleichzeitig mit dem Zertifikat des CA-Servers abläuft, stellt der Client sicher, dass er zuerst das Rollover-Zertifikat des CA-Servers erhält und fordert dann einen Rollover an Zertifikat, das vom neuen CA-Server-Rollover-Zertifikat signiert wurde, und beide werden aktiviert, wenn alte Zertifikate ablaufen.

Einrichtung



Voraussetzung für PKI und Simple Certificate Enrollment Protocol (SCEP)

Autoritäre Zeitquelle

In IOS gilt die Taktquelle standardmäßig als nicht autoritär, da die Hardware-Uhr nicht die beste Zeitquelle ist. Da PKI zeitabhängig ist, ist es wichtig, eine gültige Zeitquelle mithilfe von NTP zu konfigurieren. Bei einer PKI-Bereitstellung wird empfohlen, dass alle Clients und der Server ihre Uhr mit einem einzigen NTP-Server synchronisieren, gegebenenfalls über mehrere NTP-Server. Weitere Informationen hierzu finden Sie im IOS PKI Deployment Guide: Erstmaliges Design und erstmalige Bereitstellung

IOS initialisiert PKI-Timer nicht ohne eine autoritative Uhr. Obwohl NTP dringend empfohlen wird, kann der Administrator die Hardware-Uhr als temporäre Maßnahme wie folgt als autoritär markieren:

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

HTTP-Kommunikation

Eine Voraussetzung für einen aktiven IOS-PKI-Server ist der HTTP-Server, der mithilfe des folgenden Befehls auf Konfigurationsebene aktiviert werden kann:

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

Dieser Befehl aktiviert standardmäßig den HTTP-Server an Port 80, der wie oben gezeigt geändert werden kann.

PKI-Clients sollten über HTTP mit dem PKI-Server kommunizieren können.

PKI-Konfiguration

Server - Rollover

Die automatische Rollover-Konfiguration des PKI-Servers sieht wie folgt aus:

```
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
```

Der Parameter für die automatische Rollover-Funktion wird in Tagen definiert. Auf detaillierterer Ebene sieht der Befehl wie folgt aus:

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

Ein Auto-Rollover-Wert von 90 gibt an, dass das IOS 90 Tage vor Ablauf des aktuellen Serverzertifikats ein Rollover-Server-Zertifikat erstellt. Die Gültigkeit dieses neuen Rollover-Zertifikats beginnt mit dem Ablaufdatum des aktuellen aktiven Zertifikats.

Auto-Rollover sollte mit einem solchen Wert konfiguriert werden, der sicherstellt, dass das Rollover-CA-Zertifikat lange im Voraus auf dem PKI-Server generiert wird, bevor ein PKI-Client im Netzwerk GetNextCACert-Vorgang ausführt, wie im Abschnitt **SHADOW-Vorgangsübersicht** beschrieben.

Client - Verlängerung

Die Konfiguration der automatischen Zertifikatsverlängerung für den PKI-Client sieht wie folgt aus:

```
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 gibt der Befehl **auto-enroll <percentage> [regenerate]** an, dass das IOS eine Zertifikatsverlängerung mit genau 80 % der Lebensdauer des aktuellen Zertifikats durchführen soll.

Das Schlüsselwort **regenerate** gibt an, dass IOS das RSA-Schlüsselpaar, das Schattenschlüsselpaar, bei jedem Verlängerungsvorgang für Zertifikate neu generieren soll.

Bei der Konfiguration des Prozentsatzes für die automatische Anmeldung ist darauf zu achten. Wenn bei einem bestimmten PKI-Client in der Bereitstellung eine Bedingung auftritt, bei der das Identitätszertifikat gleichzeitig mit dem ausstellenden Zertifizierungsstellenzertifikat abläuft, sollte der Wert für die automatische Registrierung immer den [Schatten] Verlängerungsvorgang auslösen, nachdem die Zertifizierungsstelle das Rollover-Zertifikat erstellt hat. In den Bereitstellungsbeispielen *finden Sie* im Abschnitt **Abhängigkeiten** des PKI-Timers weitere Informationen.

Voraussetzungen für PKI-Verlängerungen/Rollover

In diesem Dokument werden die Vorgänge für das Rollover und die Verlängerung von Zertifikaten detailliert beschrieben. Daher werden diese Ereignisse als erfolgreich angesehen:

- PKI-Serverinitialisierung mit einem gültigen CA-Zertifikat.
- PKI-Clients wurden erfolgreich beim PKI-Server registriert. d. h. jeder PKI-Client verfügt über das Zertifizierungsstellenzertifikat und ein Identitätszertifikat, auch Router-Zertifikat.

Die Registrierung eines Clients umfasst diese Ereignisse. Ohne zu viel ins Detail zu gehen:

- Trustpoint-Authentifizierung
- Trustpoint-Registrierung

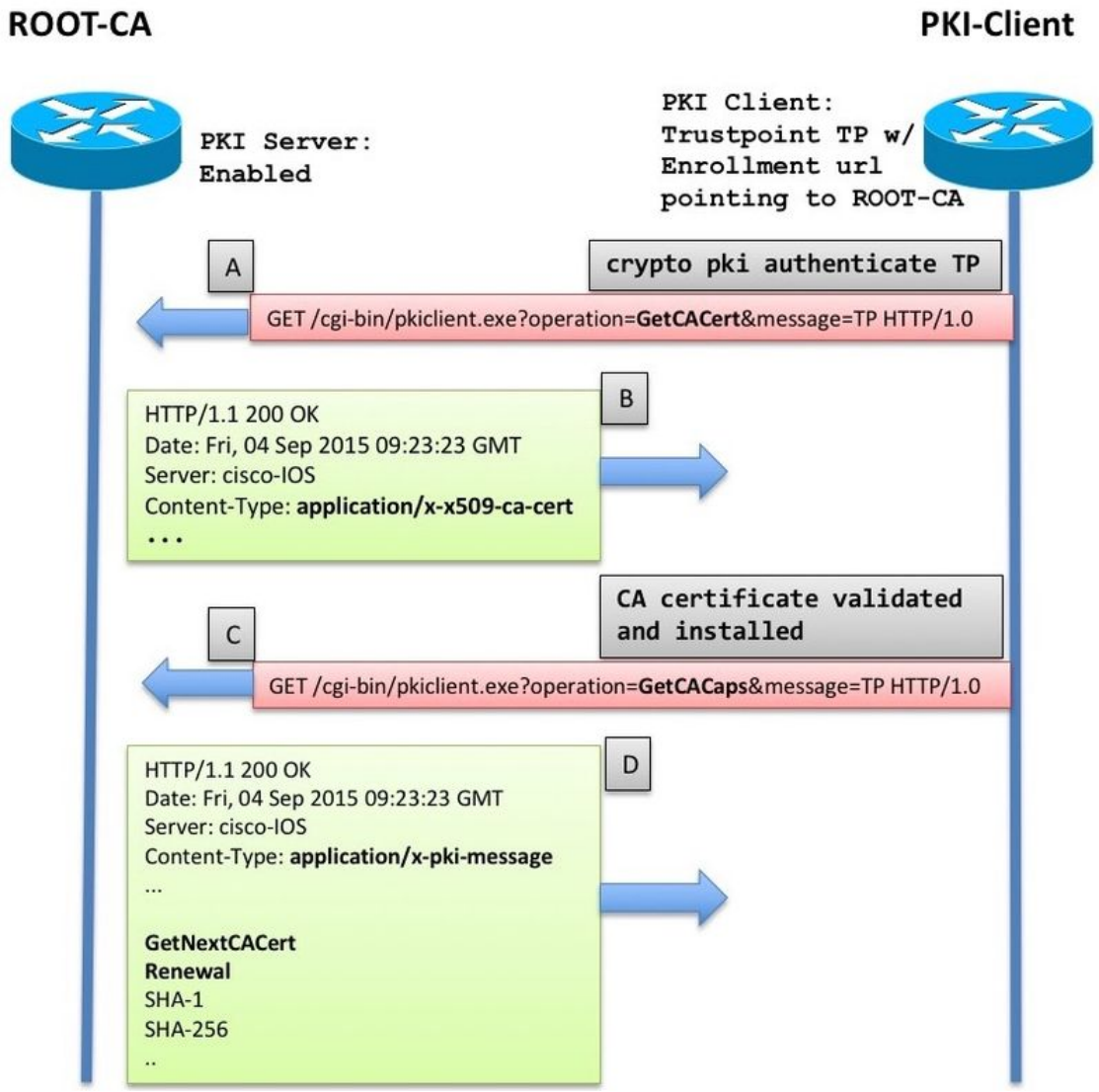
In IOS ist ein Trustpoint ein Container für Zertifikate. Jeder Trustpoint kann ein aktives Identitätszertifikat und/oder ein aktives Zertifizierungsstellen-Zertifikat enthalten. Ein Trustpoint gilt als authentifiziert, wenn er ein aktives CA-Zertifikat enthält. Sie gilt als registriert, wenn sie ein Identitätszertifikat enthält. Ein Trustpoint muss vor der Registrierung authentifiziert werden. Die Konfiguration von PKI-Servern und -Clients sowie die Authentifizierung und Registrierung von Vertrauenspunkten werden im IOS PKI Deployment Guide detailliert beschrieben: Erstmaliges Design und erstmalige Bereitstellung

Nach dem Abruf/der Installation des Zertifizierungsstellenzertifikats ruft der PKI-Client die PKI-Serverfunktionen ab, bevor er eine Registrierung durchführt. Der Abruf von CA-Funktionen wird in diesem Abschnitt erläutert.

CA-Funktionen

Wenn in IOS ein PKI-Client eine CA authentifiziert, d. h. wenn ein Administrator einen Vertrauenspunkt auf einem IOS-Router erstellt und den Befehl **crypto pki authentifiziert <trustpoint-name>**, finden diese Ereignisse auf dem Router statt:

- IOS sendet eine SCEP-Anforderung, die den GetCACert-Betriebstyp enthält.
- Die erwartete Antwort ist eine HTTP-Nachricht mit einem Inhaltstyp der **Anwendung/x-x509-ca-cert** im Fall einer CA-Bereitstellung oder **application/x-x509-ca-ra-cert** im Fall einer RA- und einer CA-Bereitstellung. Der HTTP-Text enthält das CA-Zertifikat. [und im letzteren Fall ein RA-Zertifikat].
- Nach dem Abruf und der Installation des CA/RA-Zertifikats initiiert der Client eine automatische SCEP-Anforderung, die den GetCACaps-Vorgang enthält.
- Die erwartete Antwort hier ist eine HTTP-Nachricht mit einem Inhaltstyp der **Anwendung/x-pki-Nachricht**, die auch **text/simple** sein kann und der HTTP-Text eine Reihe von Funktionen enthält, die von der CA unterstützt werden, getrennt durch ein Zeilenvorschubzeichen. Eine typische IOS PKI Server-Antwort ist im folgenden Diagramm dargestellt.



Die Antwort wird vom IOS PKI-Client folgendermaßen interpretiert:

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

Im Mittelpunkt dieses Dokuments stehen diese beiden Funktionen.

GetNextCACert

Wenn diese Funktion von der CA zurückgegeben wird, versteht IOS, dass die CA Rollover von CA-Zertifikaten unterstützt. Wenn diese Funktion zurückgegeben wird und der Befehl **zur automatischen Registrierung** nicht unter dem Vertrauenspunkt konfiguriert ist, initialisiert IOS einen SHADOW-Timer, der auf 90 % der Gültigkeitsdauer des Zertifizierungsstellenzertifikats festgelegt ist.

Wenn der SHADOW-Timer abläuft, führt IOS einen GetNextCACert-SCEP-Vorgang aus, um das Zertifikat der Rollover-Zertifizierungsstelle abzurufen.

> **Hinweis**: Wenn der Befehl **zur automatischen Registrierung** unter dem Vertrauenspunkt zusammen mit einer **Registrierungs-URL konfiguriert wurde**, wird ein RENEW-Timer bereits vor der Authentifizierung des Vertrauenspunkts initialisiert. Er versucht ständig, sich bei der CA in der **Registrierungs-URL** anzumelden, obwohl bis die Authentifizierung des Vertrauenspunkts abgeschlossen ist, keine tatsächliche Registrierungsnachricht [CSR] gesendet wird.

> **Hinweis**: GetNextCACert wird vom IOS PKI-Server als Funktion gesendet, selbst wenn der **automatische Rollover** auf dem Server nicht konfiguriert ist.

Verlängerung

Mit dieser Funktion informiert der PKI-Server den PKI-Client, dass er ein aktives ID-Zertifikat verwenden kann, um eine Zertifikatssignierungsanfrage zu unterzeichnen, um das vorhandene Zertifikat zu erneuern.

Weitere Informationen hierzu finden Sie im Abschnitt **PKI Client Auto-Renewal**.

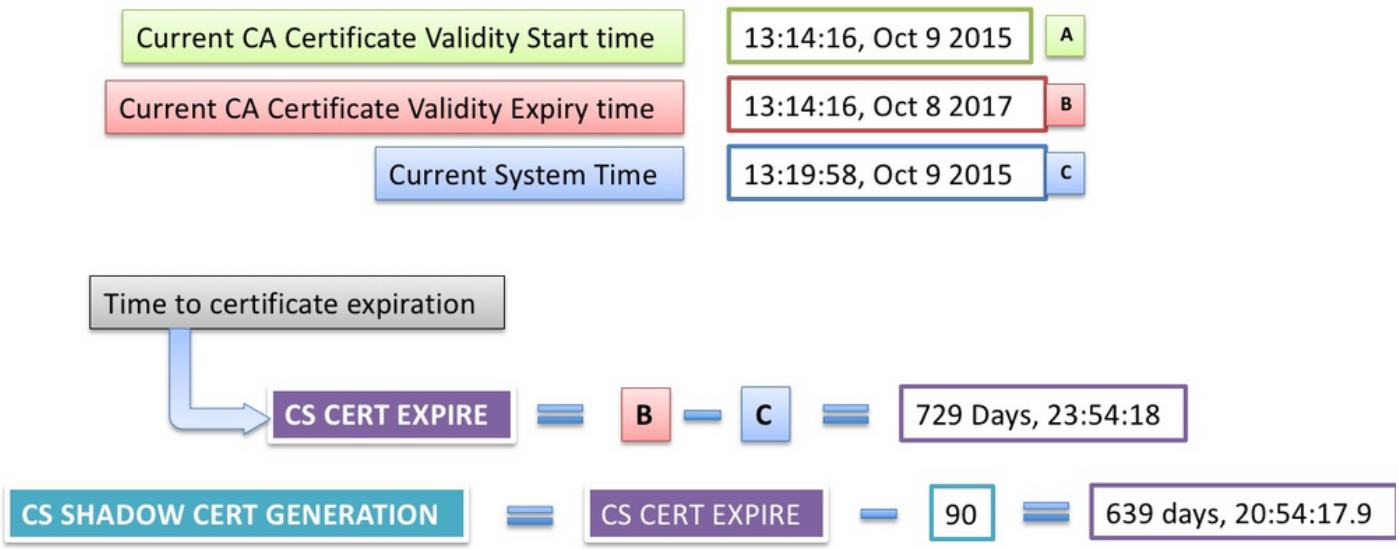
Auto-Rollover für PKI-Server

Bei der obigen Konfiguration auf dem CA-Server sehen Sie:

```
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
```

Beachten Sie Folgendes:



Rollover-Betrieb

Wenn der Zeitgeber **CS SHADOW CERT GENERATION** abläuft:

- IOS generiert zunächst ein Rollover-Schlüsselpaar. Derzeit hat es denselben Namen wie das aktive Schlüsselpaar, an das ein # Hash angehängt ist.

```
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
```

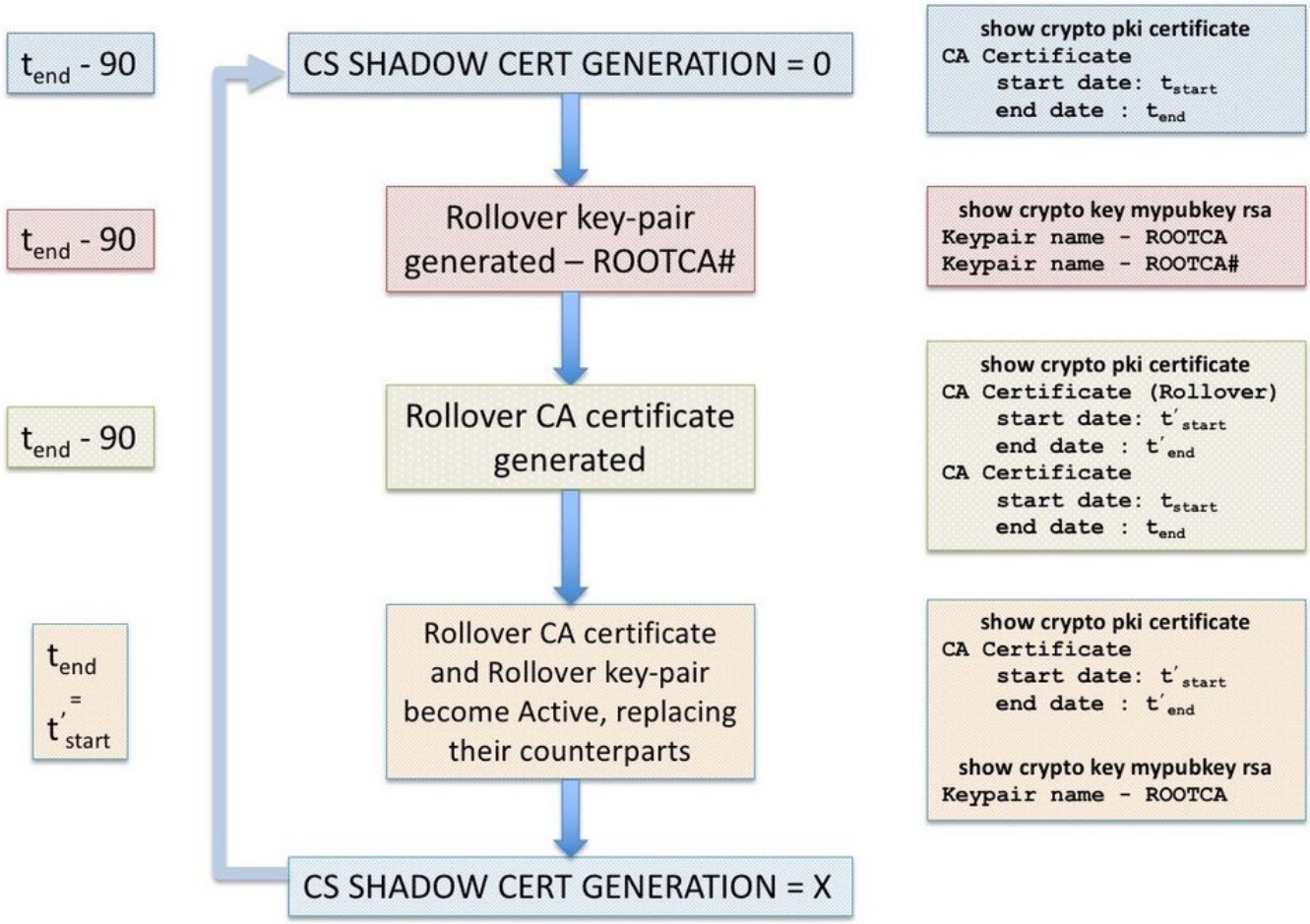
- IOS generiert dann das Rollover-Zertifizierungsstellenzertifikat, wobei das Gültigkeitsstartdatum mit dem Gültigkeitsenddatum des aktuellen aktiven Zertifizierungsstellenzertifikats identisch ist.

```
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
```



PKI-Server - Manueller Rollover

Der IOS PKI Server unterstützt die manuelle Rollover-Funktion des Zertifizierungsstellenzertifikats, d. h. ein Administrator kann die Generierung eines Rollover-Zertifizierungsstellenzertifikats im Voraus auslösen, ohne unter der PKI-Serverkonfiguration den **automatischen Rollover** konfigurieren zu müssen. Es wird dringend empfohlen, die **automatische Rollover-Funktion** zu konfigurieren, unabhängig davon, ob eine Verlängerung der Lebensdauer eines ursprünglich bereitgestellten CA-Servers geplant ist oder nicht, um die Sicherheit zu erhöhen. **PKI-Clients können die CA ohne ein Rollover-CA-Zertifikat überladen**. *Weitere Informationen finden Sie unter* Abhängigkeiten von Client-SHADOW-Operation auf PKI-Server-Rollover.

Ein manuelles Rollover kann mit dem Befehl auf Konfigurationsebene ausgelöst werden:

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

Außerdem kann ein Rollover-Zertifizierungsstellenzertifikat abgebrochen werden, um manuell ein neues zu generieren. Dies sollte ein Administrator jedoch in einer Produktionsumgebung nicht tun. Hierzu werden folgende Funktionen verwendet:

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

Dadurch werden das Rollover-RSA-Schlüsselpaar und das Rollover-CA-Zertifikat gelöscht. Dies wird aus folgenden Gründen abgelehnt:

- Sobald die Zertifizierungsstelle das Rollover-Zertifikat generiert hat, können mehrere Clients das Rollover-Zertifizierungsstellenzertifikat sowie ein Rollover-Client-Zertifikat herunterladen, das vom Rollover-Zertifizierungsstellenzertifikat signiert wird.
- Wenn der Rollover in dieser Phase abgebrochen wird, muss der Kunde möglicherweise erneut registriert werden.

PKI-Client - automatische Verlängerung

Arten von Client-Zertifikatsverlängerungen - VERLÄNGERN und SHADOW

IOS auf dem PKI-Server stellt immer sicher, dass die Ablaufzeit des dem Client ausgestellten ID-Zertifikats niemals über die Ablaufzeit des Zertifizierungsstellen-Zertifikats hinausgeht.

Auf einem PKI-Client berücksichtigt IOS immer folgende Timer, bevor der Verlängerungsvorgang geplant wird:

- Ablaufdatum des zu verlängernden Identitätszertifikats
- Ablaufzeit des Zertifikats des Emittenten

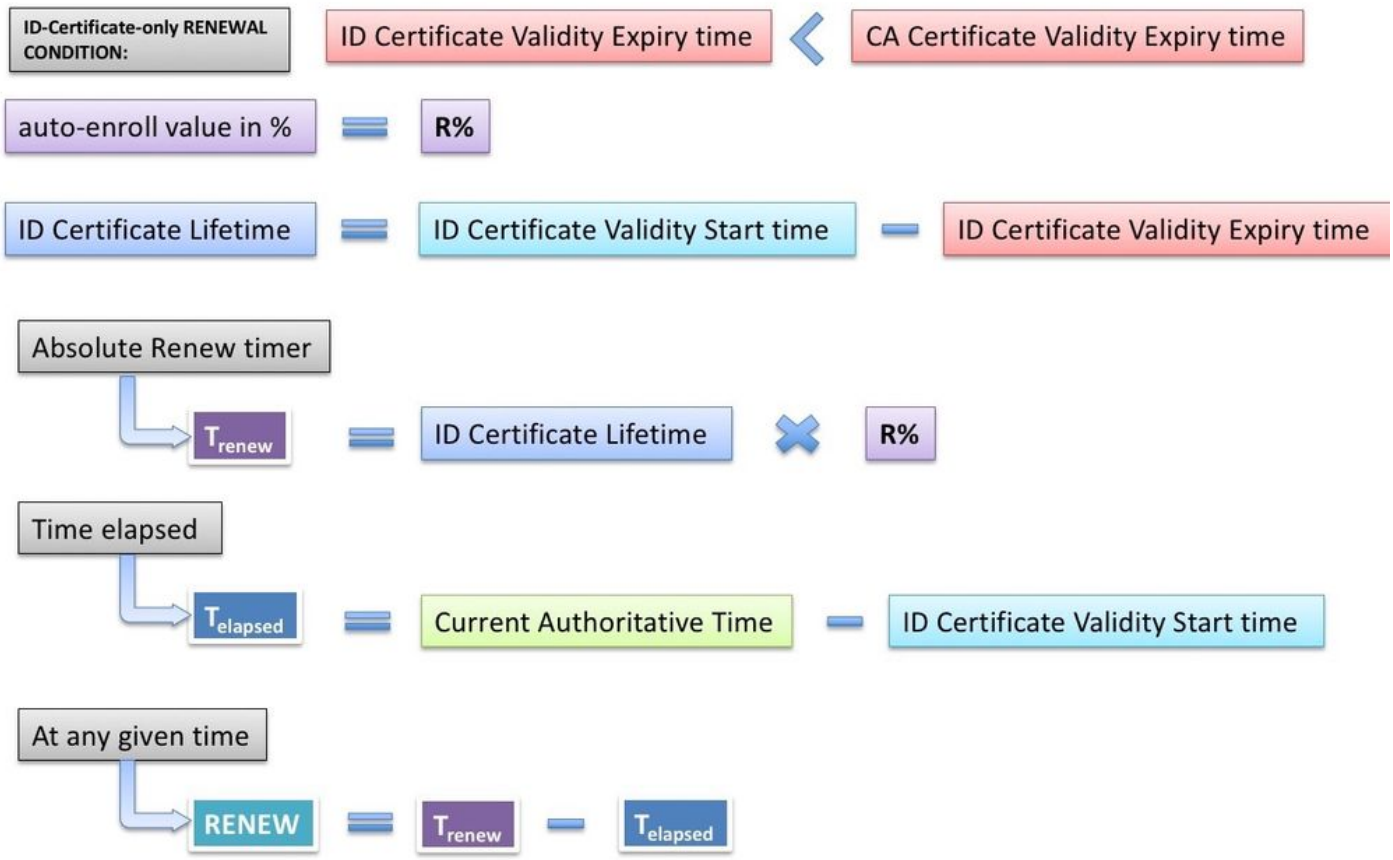
Wenn die Ablaufzeit des Identitätszertifikats nicht mit der Ablaufzeit des Zertifizierungsstellenzertifikats übereinstimmt, führt das IOS einen einfachen Verlängerungsvorgang durch.

Wenn die Ablaufzeit des Identitätszertifikats mit der Ablaufzeit des Zertifizierungsstellenzertifikats übereinstimmt, führt das IOS einen Schattenverlängerungsvorgang durch.

VERLÄNGERN - Verlängerung des Router Identity Certificate

Wie bereits erwähnt, führt der IOS PKI-Client einen einfachen Verlängerungsvorgang durch, wenn die Ablaufzeit des Identitätszertifikats nicht mit der Ablaufzeit des Zertifizierungsstellenzertifikats identisch ist, d. h. das Identitätszertifikat, das abläuft, bevor das Zertifikat des Emittenten eine einfache Verlängerung des Identitätszertifikats auslöst.

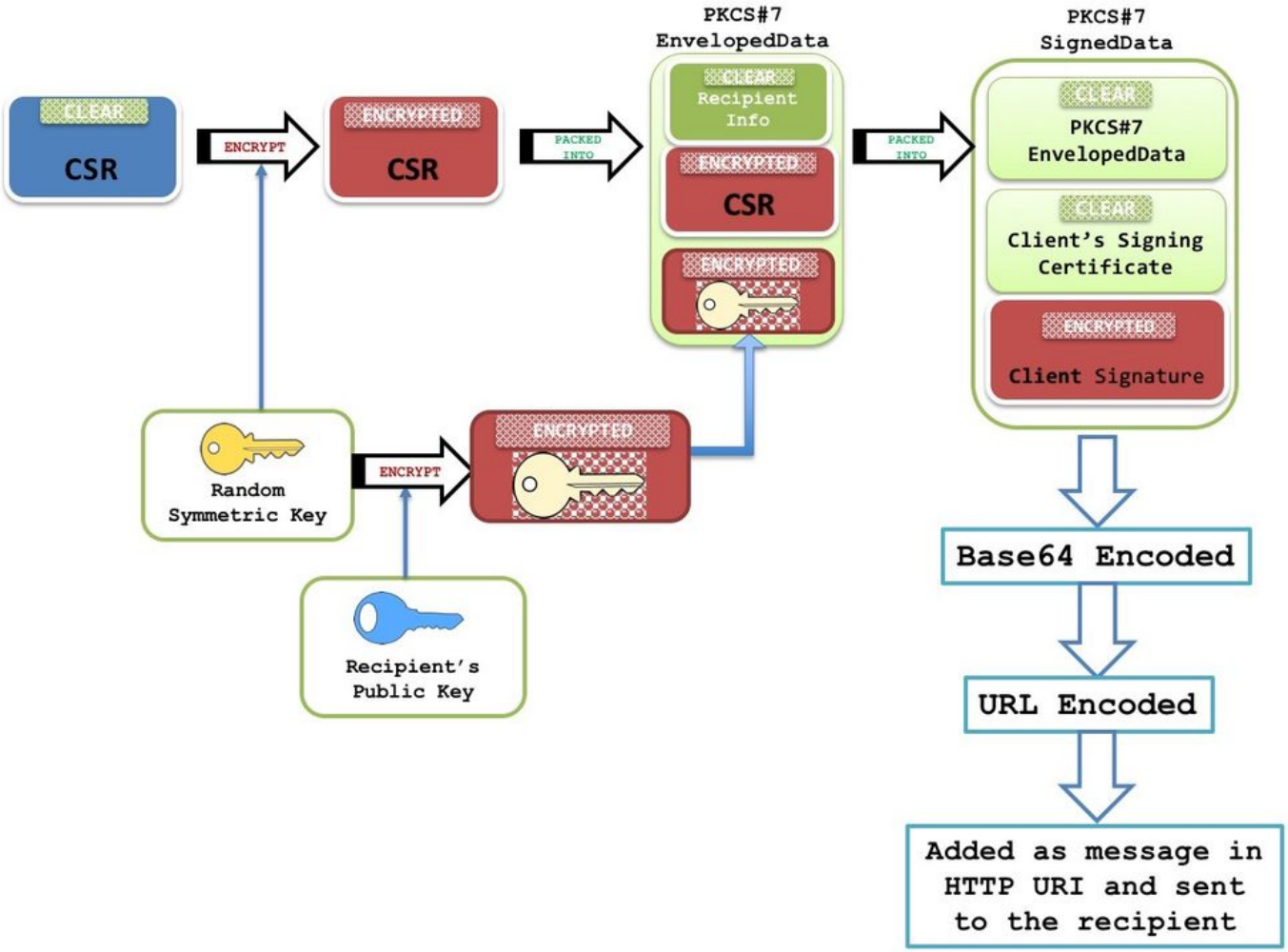
Sobald ein Identitätszertifikat installiert ist, berechnet IOS den RENEW-Timer für den jeweiligen Vertrauenspunkt, wie unten gezeigt:



Current-Authoritative-Time bedeutet, dass die Systemuhr eine maßgebliche Zeitquelle sein muss, wie hier beschrieben. (link to Authoritative Time Source Section) PKI-Timer werden ohne eine autoritative Zeitquelle nicht initialisiert. Folglich wird es nicht zu einer Erneuerung kommen.

Die folgenden Ereignisse finden nach Ablauf des RENEW-Timers statt:

- IOS generiert ein Schattenschlüsselpaar, wenn eine **Neugenerierung** konfiguriert ist [Beispiel: auto-enroll 80 regenerate]. Ohne **Neugenerierung** verwendet IOS das derzeit aktive RSA-Schlüsselpaar erneut.
- IOS erstellt eine PKCS-10-formatierte Zertifikatsanforderung, die dann in einen PKCS-7-Umschlag verschlüsselt wird. Dieser Umschlag enthält auch die RecipientInfo, die den Betreffnamen und die Seriennummer der ausstellenden Zertifizierungsstelle darstellt. Dieser PKCS7-Umschlag ist wiederum in PKCS-7 signierte Daten gepackt. Bei der Erstregistrierung verwendet IOS ein selbstsigniertes Zertifikat, um diese Nachricht zu signieren. Während der nachfolgenden Anmeldungen, d. h. der erneuten Anmeldung, verwendet IOS das aktive Identitätszertifikat, um die Nachricht zu signieren. Die PKCS7-signierten Daten sind ebenfalls in das Signaturzertifikat eingebettet, d. h. entweder in das selbstsignierte Zertifikat oder das Identitätszertifikat.



Weitere Informationen zu dieser Paketstruktur finden Sie im SCEP-Übersichtsdokument

> **Hinweis**: Die wichtigsten Informationen sind die RecipientInfo, die den Betreffnamen und die Seriennummer der ausstellenden CA darstellt. Der öffentliche Schlüssel dieser CA wird zur Verschlüsselung des symmetrischen Schlüssels verwendet. Der CSR im PKCS7-Umschlag wird mit diesem symmetrischen Schlüssel verschlüsselt.

Dieser verschlüsselte symmetrische Schlüssel wird von der empfangenden CA mithilfe des privaten Schlüssels entschlüsselt, und dieser symmetrische Schlüssel wird verwendet, um den PKCS7-Umschlag zu entschlüsseln, der die CSR-Nachricht preisgibt.

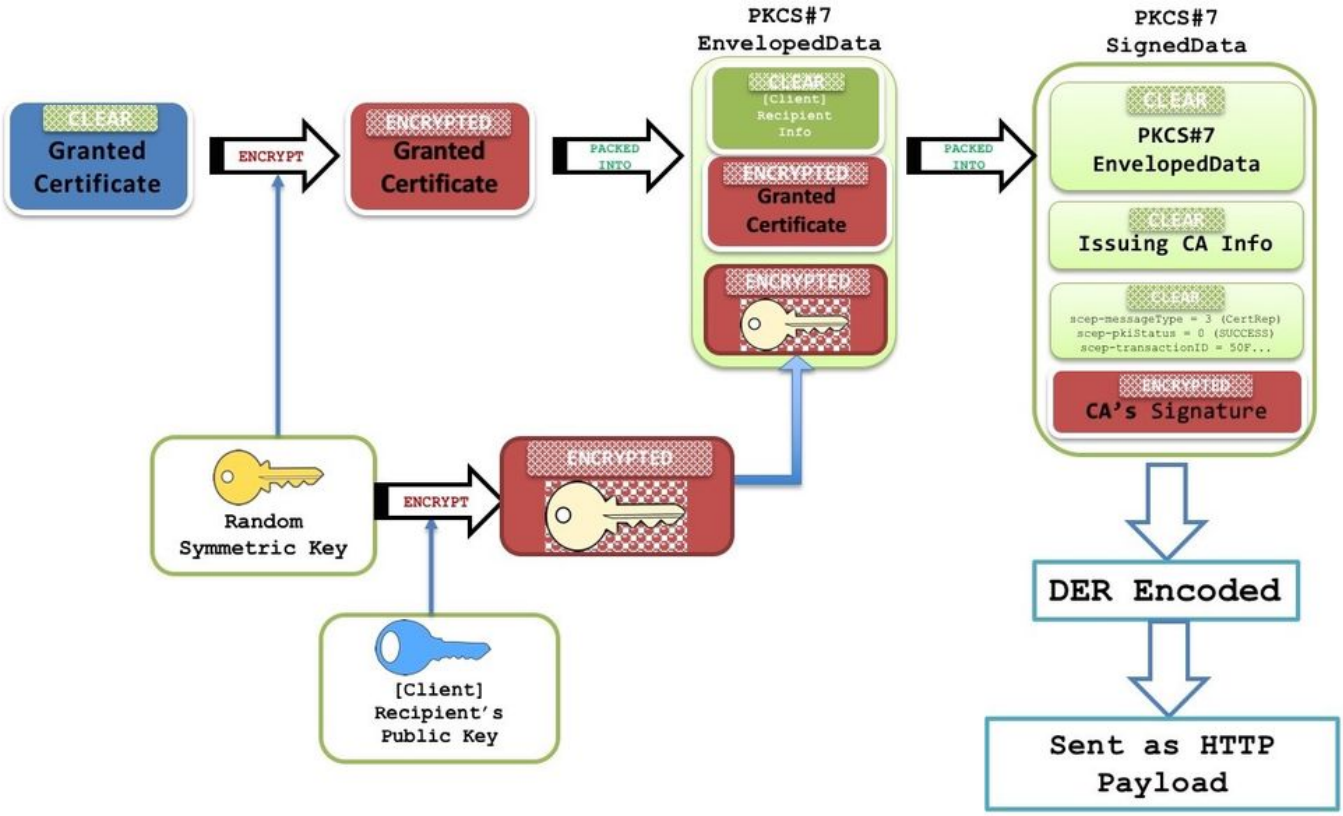
- Diese CSR-Anfrage (Certificate Signing Request) im PKCS7-Format wird dann mit einem SCEP-Nachrichtentyp PKCSReq und einem SCEP-Vorgang mit der Bezeichnung PKIOperation an die CA gesendet.
- Wenn die CA die Anforderung zurückweist, beendet IOS den RENEW-Timer. Um das Identitätszertifikat zu verlängern, muss der Administrator ab diesem Zeitpunkt eine manuelle Verlängerung vornehmen (Link zum Abschnitt **Manuelle Verlängerung** des **PKI-Clients**).
- Wenn die CA einen SCEP-Status als **ausstehend** sendet, startet IOS auf dem PKI-Client einen POLL-Timer, der mit 60 Sekunden oder 1 Minute beginnt. Bei jedem Ablauf eines POLL-Timers sendet IOS GetCertInitial-SCEP-Nachricht über einen PKIOperation-Vorgang.Wenn der erste POLL-Timer abläuft, wenn die GetCertInitial-Nachricht mit einem SCEP-Pending-Status beantwortet wird, legt ein exponentieller Backoff-Algorithmus das erste POLL-Timer-Wiederholungsintervall auf 1 Minute, das zweite POLL-Timer-Intervall auf 2

Minuten Das LL Timer-Wiederholungsintervall beträgt standardmäßig 4 Minuten usw. für die nächsten 999 erneuten Versuche oder bis das Zertifikat der ausstellenden Zertifizierungsstelle abläuft.
Die Umfrageanzahl und der erste Wiederholungszeitraum können wie folgt konfiguriert werden:

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

- Wenn das Zertifikat auf dem PKI-Server erteilt wird, wird die nächste GetCertInitial-SCEP-Nachricht mit einer HTTP-Nachricht vom Inhaltstyp **application/x-pki-message** und einem Text mit signierten PKCS#7-Daten beantwortet. Diese PKCS7-signierten Daten enthalten den SCEP-Status "**Granted**" und auch PKCS7-umhüllte Daten. Diese PKCS-umhüllten Daten enthalten das erteilte Zertifikat und die RecipientInfo, d. h. den Betreffnamen und die Seriennummer des selbstsignierten Zertifikats während der Erstregistrierung und des aktiven Identitätszertifikats während der erneuten Anmeldung.

  Die PKCS7-umhüllten Daten enthalten auch einen symmetrischen Schlüssel, der mit dem öffentlichen Schlüssel des Empfängers verschlüsselt ist (für den das neue Zertifikat erteilt wurde). Der empfangende Router entschlüsselt diesen mithilfe des privaten Schlüssels. Dieser klare symmetrische Schlüssel wird dann zum Entschlüsseln der PKCS#7-umhüllten Daten verwendet, um das neue Identitätszertifikat preiszugeben.



- In dieser Phase ersetzt IOS das vorhandene Identitätszertifikat sofort durch das neue Zertifikat. Wenn eine **Neugenerierung** konfiguriert wurde, ersetzt das Schattenschlüsselpaar auch das aktive Schlüsselpaar.

- Darüber hinaus wird das Enddatum des neuen Zertifikats mit dem Enddatum des

Zertifizierungsstellenzertifikats verglichen, um zu bestimmen, ob der RENEW-Timer initialisiert werden muss oder ein SHADOW-Timer initialisiert werden muss, wie hier <href Typen der Client-Zertifikatverlängerung - RENEW und SHADOW> erklärt wird.