IOS PKI部署指南：证书反转-配置和操作概述

目录

简介

本文详细描述在Cisco IOS公共密钥基础设施(PKI)服务器和客户端的证书反转。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于下列硬件和软件版本：

硬件

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

软件

- IOS
  - ISR-G1 –最新的15.1(4)M*
  - ISR-G2 –最新15.4(3)M
- IOS-XE
  - XE 3.15或15.5(2)S

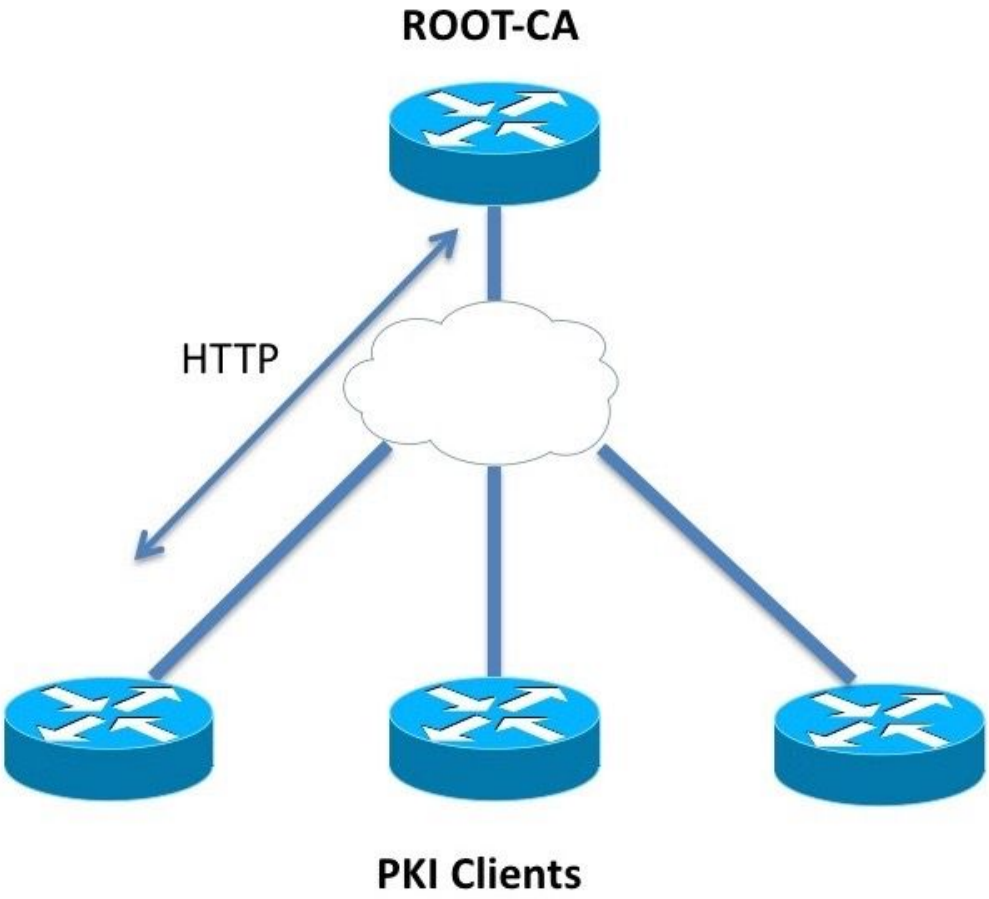
注意：ISR设备的一般软件维护不再是活跃的，所有将来故障修复或增强特性将要求硬件升级到ISR-2或ISR-4xxx系列路由器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

亦称证书反转续订操作保证，当证书超时时，新证书准备接管。从PKI服务器的观点，此操作介入很好生成新的服务器反转证书事先确保，所有PKI客户端接收新的服务器反转证书签字的一新的客户端反转证书，在当前证书超时前。从PKI客户端的观点，如果客户端证书超时，但是Certificate Authority (CA)服务器证明不是，新证书的客户端的要求和取代证书，当新证书接收，并且，如果客户端证书超时在CA服务器证明的同时，客户端确保首先接收CA服务器的反转证书，为新的CA服务器反转证书签字的反转证书然后请求，并且两个将激活，当旧有证书超时。

设置



PKI和简单Ceritificate注册协议(SCEP)前提条件

可信的时间源

默认情况下在IOS中，因为硬件时钟不是时间，最好的来源时钟源认为未授权的。使用NTP的PKI对时间敏感，配置时间有效的来源是重要的。在PKI部署，推荐安排所有客户端和服务器如果必须同步他们的时钟到单个Ntp server，通过多个NTP服务器。更多在此在IOS PKI部署指南解释：初始设计和部署

IOS不初始化PKI计时器没有一个授权时钟。虽然NTP是高度推荐的，作为临时测量，管理员能标记硬件时钟如授权使用：

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

HTTP通信

激活IOS PKI服务器的一个需求是HTTP服务器，使用此设置级别命令，可以启用：

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

默认情况下此命令启用在端口80的HTTP服务器，可以更改如上所述。

PKI客户端应该能用在HTTP的PKI服务器通信到配置端口。

PKI配置

服务器-反转

PKI服务器自动反转配置看似类似：

```
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
```

自动反转参数以几天定义。在一个更加粒状的级别，命令看起来象：

```
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
```

自动反转值为90表明IOS在当前服务器证书的终止前创建反转服务器证书90天，并且此的正确性新建的反转证书开始在当前活动证书的到期时间的同时。

应该配置自动反转与在PKI服务器确保该反转CA证书很好生成事先的这样值，在网络的所有PKI客户端执行GetNextCACert操作正如下面前**SHADOW操作概述部分所描述**。

客户端-续订

PKI客户端自动证书续订配置看似类似：

```
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
```

这里，**自动注册<percentage> [regenerate]**命令状态IOS应该执行证书续订在正确地80%当前证书的寿命。

关键字**重新生成**阐明， IOS应该重新生成叫作Shadow密钥对的RSA密钥对在每证书续订操作时。

应该保重，当配置自动注册百分比时。在部署的所有给的PKI客户端，如果情况出现身份证书超时在发出的CA证书的同时的地方，然后自动注册值应该总是触发[shadow]续订操作，在CA创建反转证书后。*参考***PKI计时器从属关系**部分在部署示例下。

PKI续订/反转前提条件

本文详细讨论证书反转和续订操作，并且这些事件认为顺利地完成：

- PKI与一个有效CA证书的服务器初始化。
- PKI客户端用PKI服务器顺利地登记。即。亦称每个PKI客户端有CA证书和一身份证书路由器证书。

登记客户端介入这些事件。没有让太多进入详细信息：

- 信任点验证
- 信任点登记

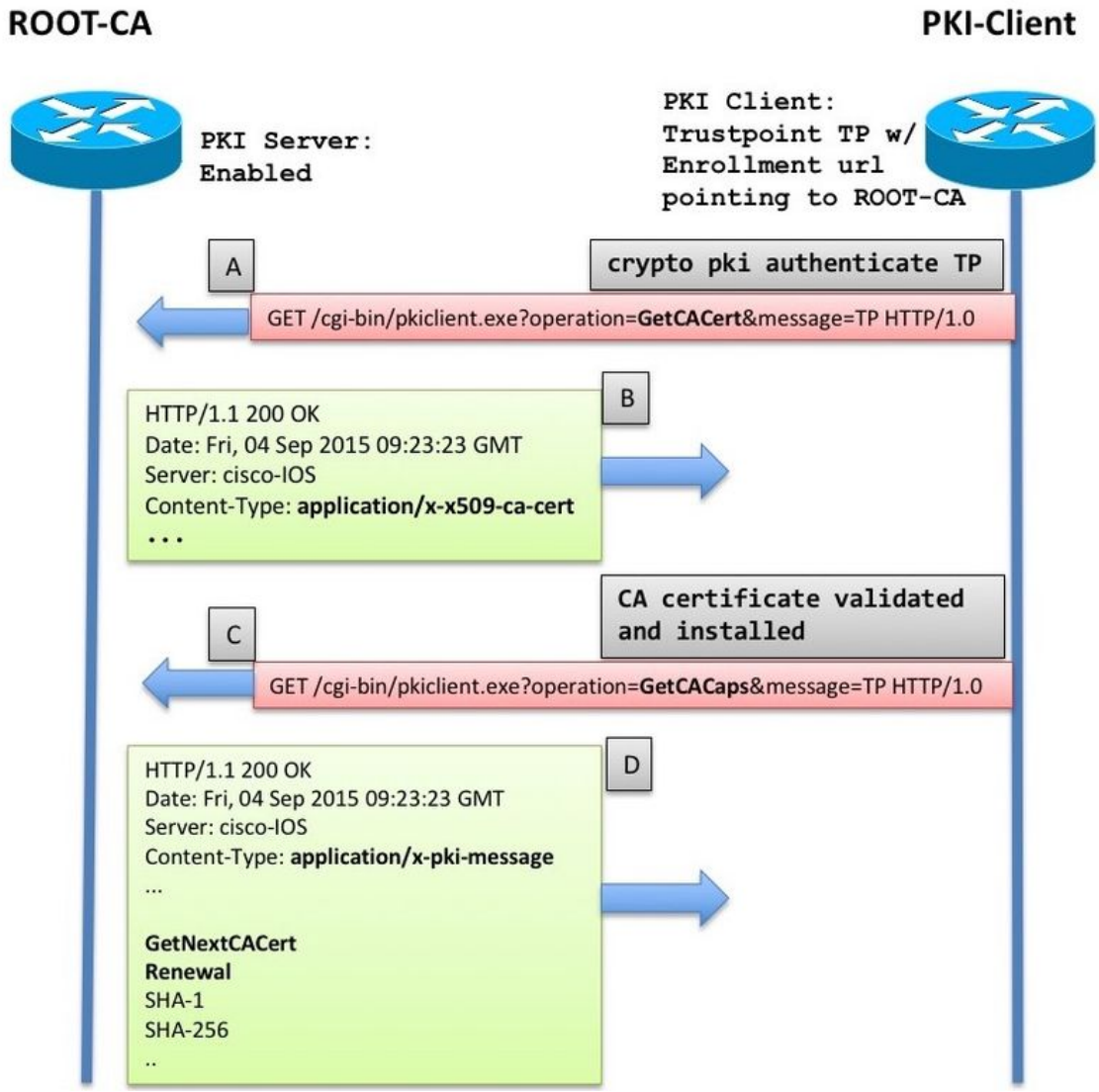
在IOS中，信任点是证书的一个容器。所有给的信任点能包含一活动身份证书和一个激活CA证书。如果包含激活CA ceryificate，信任点被认为已验证。如果包含身份证书，并且被认为登记。必须在登记前验证信任点。PKI服务器和客户端配置，与信任点验证一起和登记在IOS PKI部署指南详细报道：初始设计和部署

在CA证书检索/安装后， PKI客户端获取PKI服务器功能前面执行登记。CA功能检索在此部分解释。

CA功能

在IOS中，当PKI客户端验证CA，换句话说，当管理员创建在IOS路由器的一信任点，和在路由器执行crypto命令**pki验证<trustpoint-name>**，这些事件发生：

- IOS发送包含GetCACert操作类型的SCEP请求。
- 此处期望的响应是与**application/x-x509-ca-cert**内容类型的一个HTTP消息在CA部署的情况下或者**application/x-x509-ca-ra-cert**在RA和CA部署的情况下。并且HTTP正文包含CA证书。[and an RA certificate in the latter case]。
- 在CA/RA证书检索和安装后，客户端启动包含GetCACaps操作的一自动SCEP请求。
- 此处期望的响应是与application/x pki**消息**内容类型的一个HTTP消息，可能也是**文本/纯文本**，并且HTTP正文包含CA支持的一系列的功能，分离由换行符字符。如下图所示所显示，典型IOS PKI服务器响应是。



答复解释作为此由IOS PKI客户端：

```
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
```

这些功能，本文着重这两个。

GetNextCACert

当此功能由CA时返回， IOS了解CA支持CA证书反转。当此功能返回，如果**auto-enroll命令没有**配置在信任点下， IOS初始化设置的SHADOW计时器到90% CA证书的有效性周期。

当SHADOW计时器超时时， IOS执行GetNextCACert SCEP操作拿来反转CA证书。

> **注意**： 如果**auto-enroll命令**配置在信任点下与**登记URL一起**，更新计时器在验证信任点以前初始化，并且经常设法登记与CA查找在**登记URL**，虽然实际登记消息[CSR]没有发送，直到信任点验证。

注意：GetNextCACert发送作为功能由IOS PKI服务器，即使自动**反转**在服务没有配置

续订

以此功能， PKI服务器通知PKI客户端能使用激活ID证书签署证书签名请求更新现有的证书。

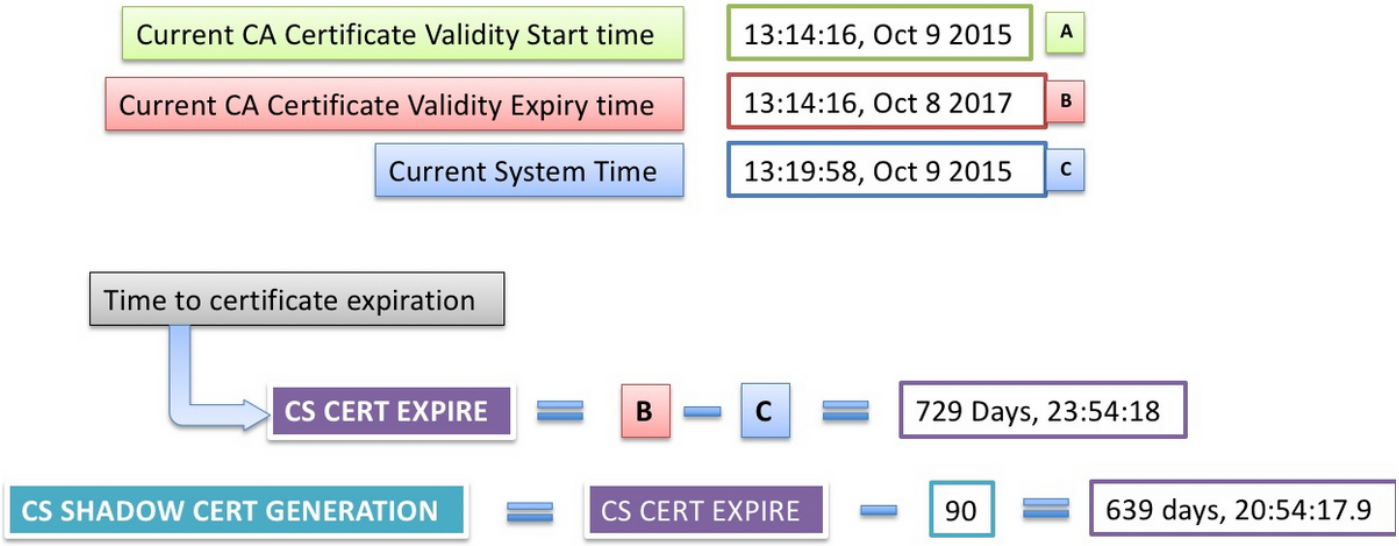
更多在此在**PKI客户端自动续签**部分。

PKI服务器自动反转

使用在CA服务器的上述配置，您看到：

```
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 80Root-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
```

注意此：



反转操作

当CS SHADOW CERT生成计时器超时：

- IOS生成最初反转的密钥对它当前有名称和活动密钥对一样与a #哈希被添附对它。

```
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
```

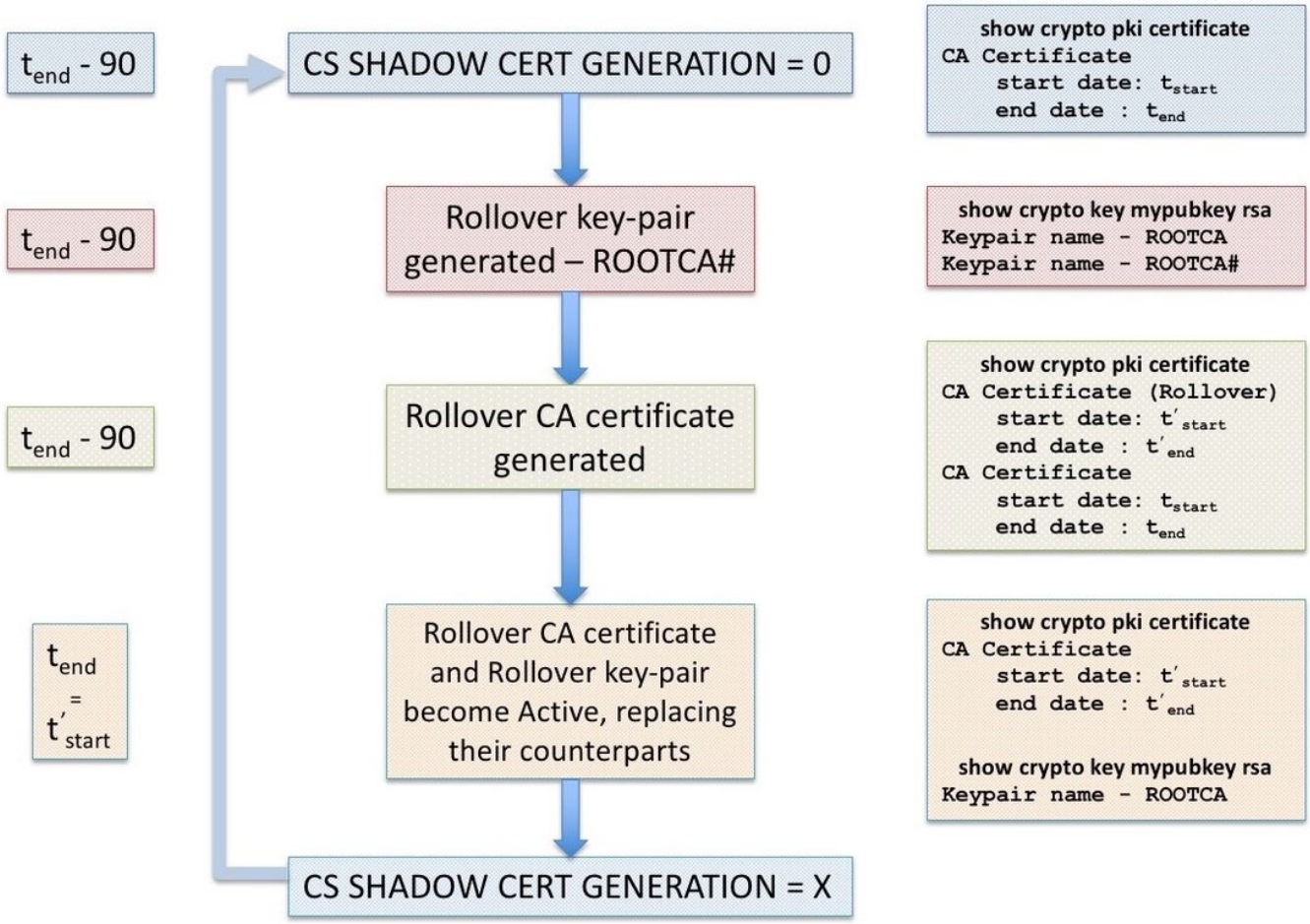
```
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

- IOS然后生成反转CA证书，正确性起始日期是相同的象当前活动CA证书的正确性结束日期。

```
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


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.cerRoot-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 daysRoot-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服务器手工反转

IOS PKI服务器支持CA证书的手工的反转，即管理员能事先触发反转CA证书的生成，无需需要配置自动反转**在**PKI服务器配置下。它是高度推荐的配置自动反转一个**是否**计划扩大一个最初部署的CA服务器的寿命在更加安全的侧。PKICLIENTS**能超载CA，不用反转CA证书。**[在PKI服务器反转的](#)参考的[Dependencyof客户端SHADOW操作。](#)

使用配置级别命令，手工的反转可以被触发：

```
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
```

并且，反转CA证书可以取消手工生成一新鲜一个，然而某事admin在生产环境不应该执行，使用：

```
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
```

这删除反转rsa密钥对和反转CA证书。这建议，由于：

- 一旦CA生成反转证书，广泛客户端可能下载反转CA证书以及反转客户端证书签字的反转CA证书。
- 在此阶段，如果反转取消，客户端可能必须被再登记。

PKI客户端自动续签

客户端证书续订的类型-更新并且遮蔽

在PKI服务器的IOS总是确保ID证书的到期时间发出对客户端从未超出CA证书的到期时间范围。

在PKI客户端， IOS总是考虑到以下计时器在安排续订操作前：

- 被更新的身份证书的到期时间
- 签发人的(CA)证书的到期时间

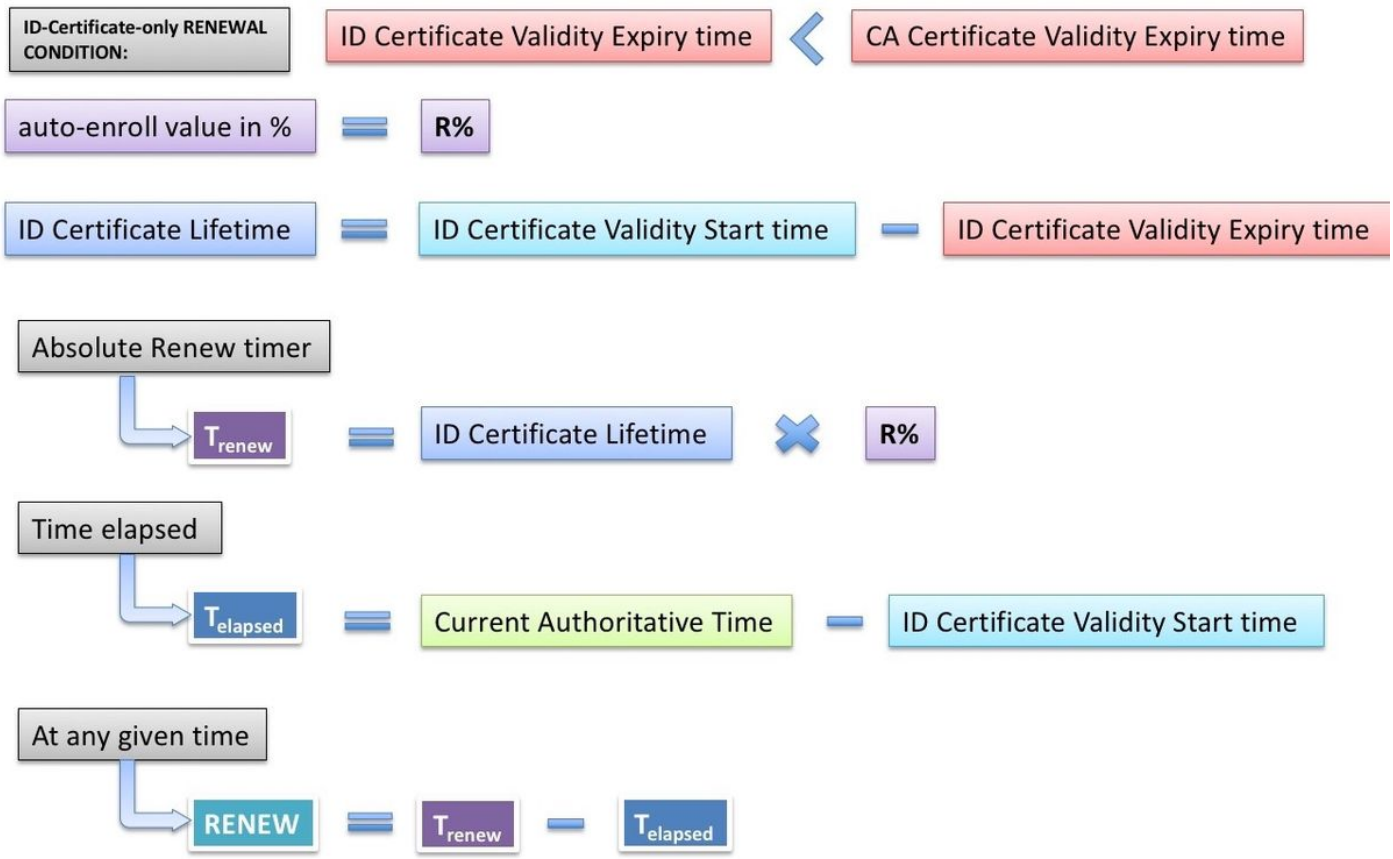
如果身份证书的到期时间不是相同的象CA证书的到期时间， IOS执行一简单续订操作。

如果身份证书的到期时间是相同的象CA证书的到期时间， IOS执行一Shadow续订操作。

更新-路由器身份证书续订

如上所述，执行一简单续订操作，如果身份证书的到期时间不是相同的象CA证书的到期时间，身份证书超时在签发人的证书前的IOS PKI客户端换句话说触发身份证书的一简单续订。

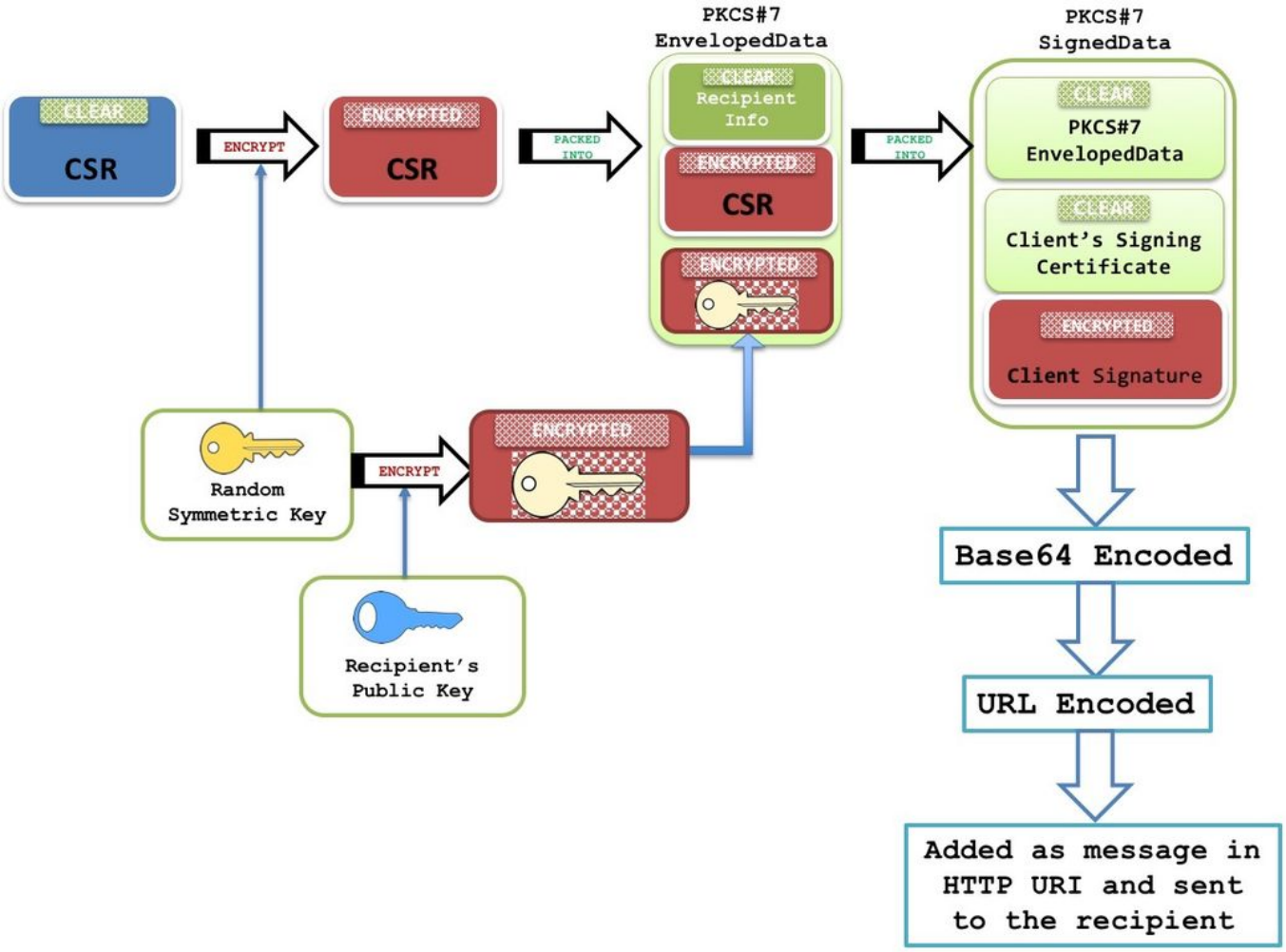
当身份证书安装， IOS计算特定托拉斯点的更新计时器如下所示：



当前授权时间意味着系统时钟必须是时间一授权来源如描述此处。(对可信的时间源部分的链路)PKI计时器不会初始化没有时间一授权来源。并且结果，续订操作不会发生。

当请更新计时器超时时，以下事件发生：

- IOS生成Shadow密钥对，如果**重新生成**配置[示例：自动注册80重新生成]。没有**再生**IOS重新使用当前活跃的RSA密钥对。
- IOS创建PKCS-10被格式化的证书请求，然后加密到PKCS-7信封。此信封也包含RecipientInfo，是subject-name和发出的CA的序列号。此PKCS7-envelope反过来被包装到PKCS-7签名数据。在最初的登记期间， IOS使用一自签名证书签署此消息。在随后的登记期间，并且，即重新登记， IOS使用活动身份证书签署消息。PKCS7签名数据也嵌入与签署的证书，即自签名证书或身份证书。



关于此数据包结构的更多信息参考的[SCEP概述文件]

> **注意**：此处关键信息是subject-name和发出的CA的序列号的RecipientInfo，并且此CA公共密钥用于加密对称密钥。使用此对称密钥，在PKCS7信封的CSR加密。

使用其专用密钥，此已加密对称密钥由接收的CA解密，并且此对称密钥用于解密显示CSR的PKCS7信封。

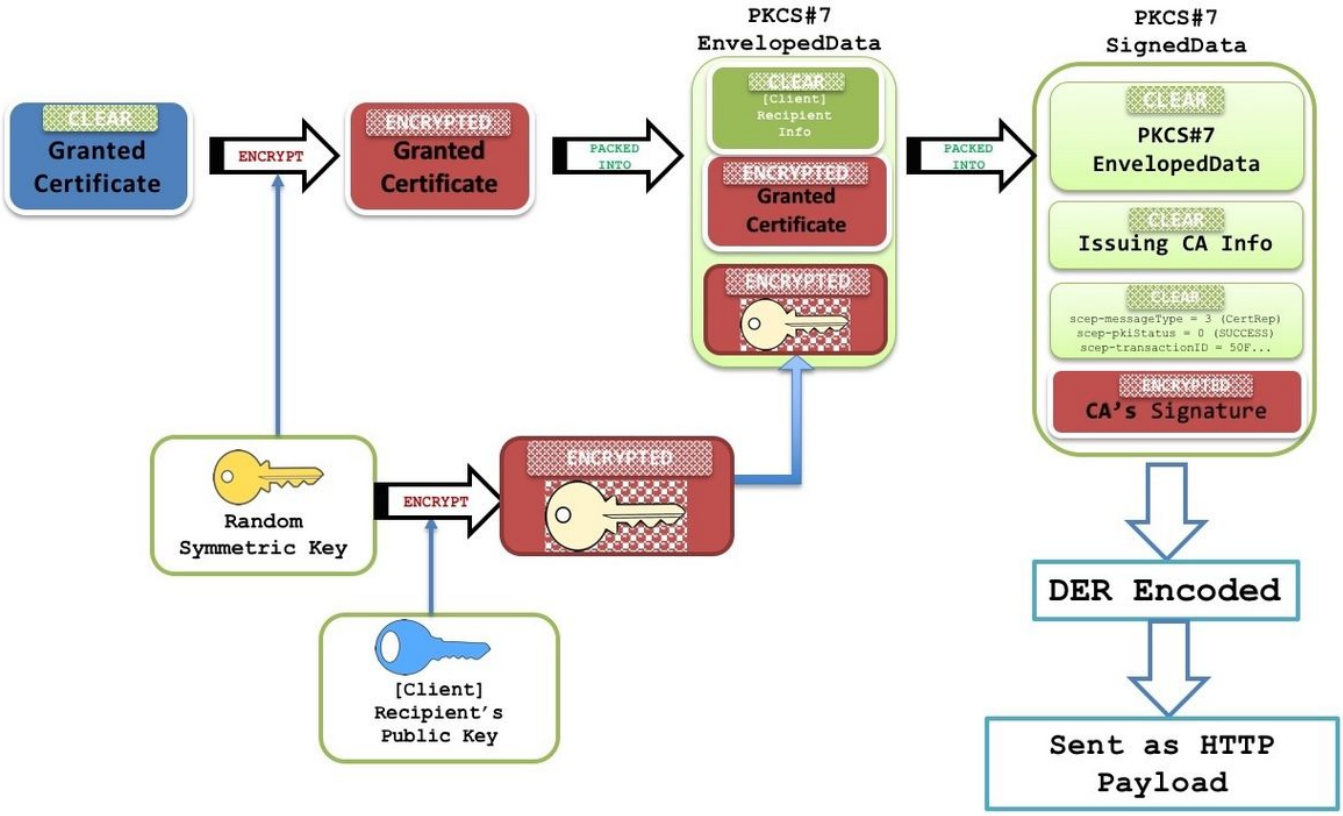
- 在PKCS7格式(CSR)包的此证书签名请求然后发送对与PKCSReq SCEP消息类型和呼叫PKIOperation的SCEP操作的CA。
- 如果CA拒绝请求， IOS终止更新计时器。从这时起，更新身份证书，管理员必须执行一手工的续订(对**PKI客户端手工续订**部分的链路)
- 如果CA发送SCEP状态如**待定**，在PKI客户端的IOS启动POLL计时器开始在60秒或1分钟。在POLL计时器超时时候， IOS通过PKIOperation操作传送GetCertInitial SCEP信息。当第一个POLL计时器超时时，如果GetCertInitial消息响应对以SCEP待定状态，指数退避算法设置第一POLL计时器重试间隔为1分钟，秒钟POLL计时器重试间隔为2分钟，第三POLL计时器重试间隔为4分钟等等下999重试次数的默认情况下或，发出的CA证书超时。
  投票计数和第一个重试次数期限可以配置使用：

```
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
```

- 当证书在PKI服务器时授权，下个GetCertInitial SCEP消息响应对与内容类型application/x pki**消息**HTTP消息和包含一个签字的PKCS-7签名数据的正文。此PKCS7签名数据包含SCEP状态如**授权**，并且PKCS7包围了数据。此PKCS被包围的数据包含授权的证书和RecipientInfo，是subject-name和自签名证书序列号在最初的登记期间和活动身份证书在重新登记期间。

  PKCS7被包围的数据也包含用收件人的公共密钥加密的对称密钥(为哪些新证书授权)。使用专用密钥，接收路由器解密它。此清楚对称密钥然后用于解密PKCS-7被包围的数据，显示新的身份证书。



- 在此阶段， IOS用新证书立即替换现有身份证书。并且，如果**重新生成**配置， Shadow密钥对替换活动密钥对。
- 并且，新证书的结束日期与CA证书的结束日期比较确定是否请更新计时器必须初始化或SHADOW计时器必须初始化作为**客户端证书续订的**解释的此处<href**类型-请更新和SHADOW>**