IOS PKI部署指南：证书滚动 — 配置和操作概述

目录

简介
先决条件
要求
使用的组件
Hardware
软件
背景信息
设置
PKI和简单证书注册协议(SCEP)前提条件
权威时间源
HTTP通信
PKI配置
服务器 — 全反
客户端 — 续约
PKI续约/滚动更新先决条件
CA功能
GetNextCACert
续约
PKI服务器自动回滚
滚动操作
PKI服务器手动回滚
PKI客户端自动续约
客户端证书续约类型 — 续约和影子
RENEW — 路由器身份证书续约
确认
SHADOW — 路由器身份和颁发CA证书续约
确认
客户端SHADOW操作对PKI服务器滚动更新的依赖性
PKI客户端注册 — 重试机制
连接重试计时器
轮询计时器
RENEW/SHADOW计时器
PKI客户端手动续约
PKI服务器 — 授权自动授予客户端续约请求
PKI计时器依赖项

简介

本文档详细介绍Cisco IOS公钥基础设施(PKI)服务器和客户端上的证书滚动更新。

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：

Hardware

- ISR-G1 [8xx、18xx、28xx、38xx]
- ISR-G2 [19xx、29xx、39xx]
- ISR-4K [43xx、44xx]
- ASR1000
- CSR1k

软件

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

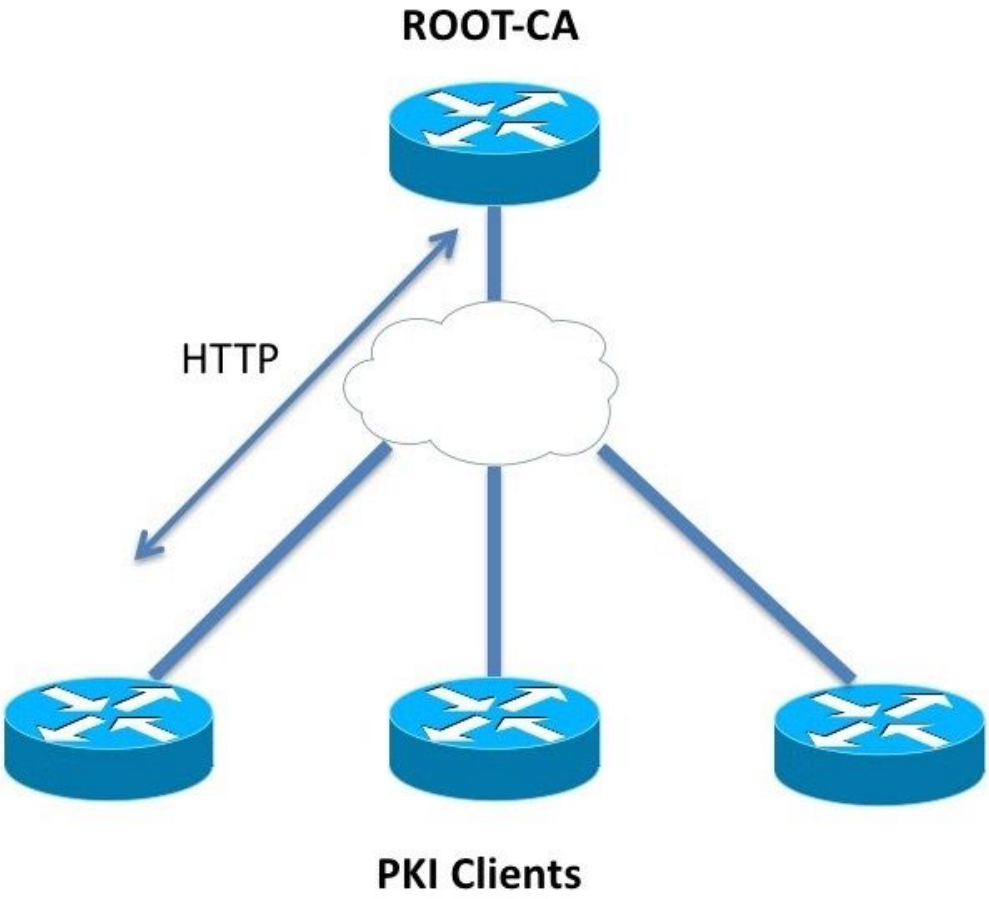
注意：ISR设备的一般软件维护不再有效，任何未来的漏洞修复或功能增强都需要硬件升级到ISR-2或ISR-4xxx系列路由器。

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

证书滚动更新也称为续约操作，可确保当证书过期时，新证书可以接管。从PKI服务器的角度来看，此操作涉及提前生成新的服务器滚动证书，以确保所有PKI客户端在当前证书过期之前都收到由新服务器滚动证书签名的新客户端滚动证书。从PKI客户端的角度来看，如果客户端证书即将过期但证书颁发机构(CA)服务器的证书未过期，客户端会请求新证书并在收到新证书后立即替换旧证书，如果客户端证书与CA服务器证书同时过期，则客户端会确保先接收CA服务器的全反证书，然后对由新CA服务器滚动更新证书签名的滚动更新证书的请求，当旧证书过期时，将激活这两个请求。

设置



PKI和简单证书注册协议(SCEP)前提条件

权威时间源

在IOS中，默认情况下，时钟源被视为非授权，因为硬件时钟不是最佳时间源。PKI对时间敏感，使用NTP配置有效时间源非常重要。在PKI部署中，建议让所有客户端和服务器通过多个NTP服务器（如果需要）将其时钟同步到单个NTP服务器。有关此内容的详细信息，请参阅《IOS PKI部署指南》：初始设计和部署

IOS不在没有授权时钟的情况下初始化PKI计时器。尽管强烈建议使用NTP，但作为临时措施，管理员可以使用以下方法将硬件时钟标记为授权：

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

HTTP通信

活动IOS PKI服务器的要求是HTTP服务器，可以使用以下config-level命令启用：

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

此命令默认在端口80上启用HTTP服务器，如上所示可以更改。

PKI客户端应能通过HTTP与PKI服务器通信到配置的端口。

PKI配置

服务器 — 全反

PKI服务器自动滚动配置如下所示：

```
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
```

自动滚动参数以天为单位定义。在更精细的级别上，命令如下所示：

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

自动滚动更新值90表示IOS在当前服务器证书到期前90天创建滚动更新服务器证书，并且此新滚动更新证书的有效性与当前活动证书的到期时间同时开始。

应使用这样的值配置自动滚动，以确保在网络中的任何PKI客户端执行GetNextCACert操作之前，在PKI服务器上提前生成滚动CA证书，如下面的**SHADOW操作概述**部分所述。

客户端 — 续约

PKI客户端自动证书续约配置如下所示：

```
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
```

此处， **auto-enroll <percentage> [regenerate]**命令指出，IOS应以当前证书生存期的80%执行证书续约。

关键字**regenerate**表示IOS应在每次证书续订操作期间重新生成RSA密钥对（称为影子密钥对）。

配置自动注册百分比时应小心。在部署中的任何给定PKI客户端上，如果出现身份证书与颁发CA证书同时过期的情况，则自动注册值应始终在CA创建滚动证书后触发[影子]续订操作。*请参阅***部署示例**下的PKI计时器依赖项部分。

PKI续约/滚动更新先决条件

本文档详细介绍证书滚动更新和续约操作，因此认为这些事件已成功完成：

- 使用有效CA证书进行PKI服务器初始化。
- PKI客户端已成功注册到PKI服务器。即，每个PKI客户端都有CA证书和身份证书（也称路由器证书）。

注册客户端涉及这些事件。不用太多细节：

- 信任点身份验证
- 信任点注册

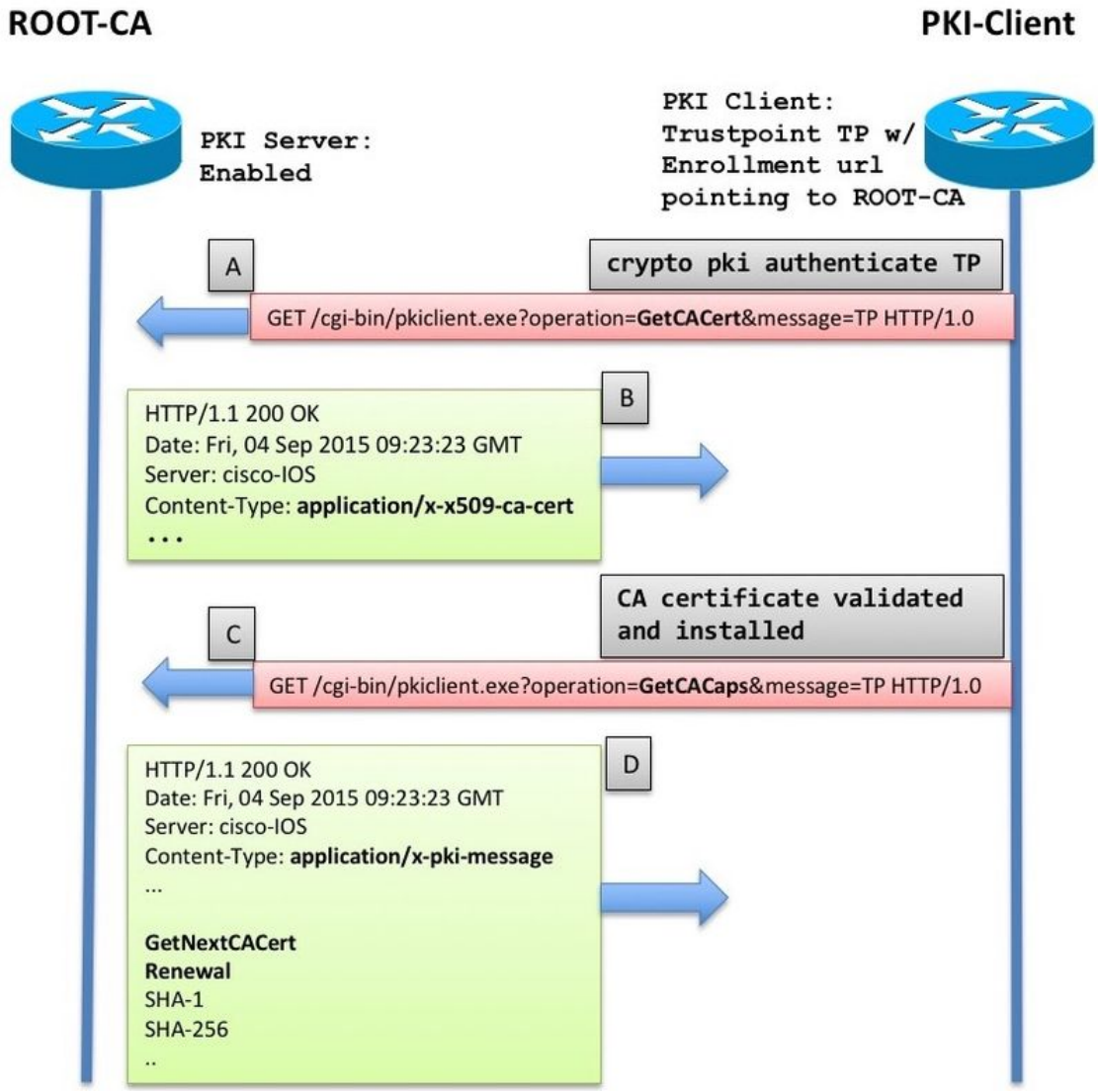
在IOS中，信任点是证书的容器。任何给定信任点都可以包含一个活动身份证书和/或一个活动CA证书。如果信任点包含活动CA证书，则该信任点被视为已通过身份验证。如果它包含身份证书，则视为已注册。注册前必须对信任点进行身份验证。PKI服务器和客户端配置以及信任点身份验证和注册在《IOS PKI部署指南》中有详细介绍：初始设计和部署

在CA证书检索/安装后，PKI客户端在执行注册之前检索PKI服务器功能。CA功能检索将在本节中介绍。

CA功能

在IOS中，当PKI客户端对CA进行身份验证时，即当管理员在IOS路由器上创建信任点并执行命令**crypto pki authenticate <trustpoint-name>时**，路由器上会发生以下事件：

- IOS发送包含GetCACert操作类型的SCEP请求。
- 在CA部署时，此处的预期响应是内容类型为**application/x-x509-ca-cert的HTTP消息，在RA和CA部署时，则为application/x-x509-ca-ra-cert**。HTTP正文包含CA证书。[和后一种情况下的RA证书]。
- 在CA/RA证书检索和安装后，客户端启动包含GetCACaps操作的自动SCEP请求。
- 此处的预期响应是包含内容类型**application/x-pki-message的HTTP消息**，该消息也可以是**text/plain**，并且HTTP正文包含CA支持的一系列功能，以换行符分隔。典型的IOS PKI服务器响应如下图所示。



响应由IOS PKI客户端解释为：

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

在这些功能中，本文档重点介绍这两项功能。

GetNextCACert

当CA返回此功能时，IOS了解CA支持CA证书滚动更新。如果返回此功能，如果**auto-enroll**命令未在信任点下配置，则IOS将初始化SHADOW计时器，该计时器设置为CA证书有效期的90%。

当SHADOW计时器到期时，IOS执行GetNextCACert SCEP操作以获取滚动CA证书。

> **注意**：如果在信任点下配置了**auto-enroll**命令以及注册URL，则RENEW计时器甚至在对信任点进行身份验证之前就已初始化，并且它会不断尝试向位于注册URL的CA进行注册，但在信任点进行身份验证之前不会发送实际注册消息[CSR]。

> **注意**：GetNextCACert由IOS PKI服务器作为功能发送，即使未在服**务器上配**置自动回滚功能

续约

通过此功能，PKI服务器通知PKI客户端它可以使用活动ID证书签署证书签名请求以更新现有证书。

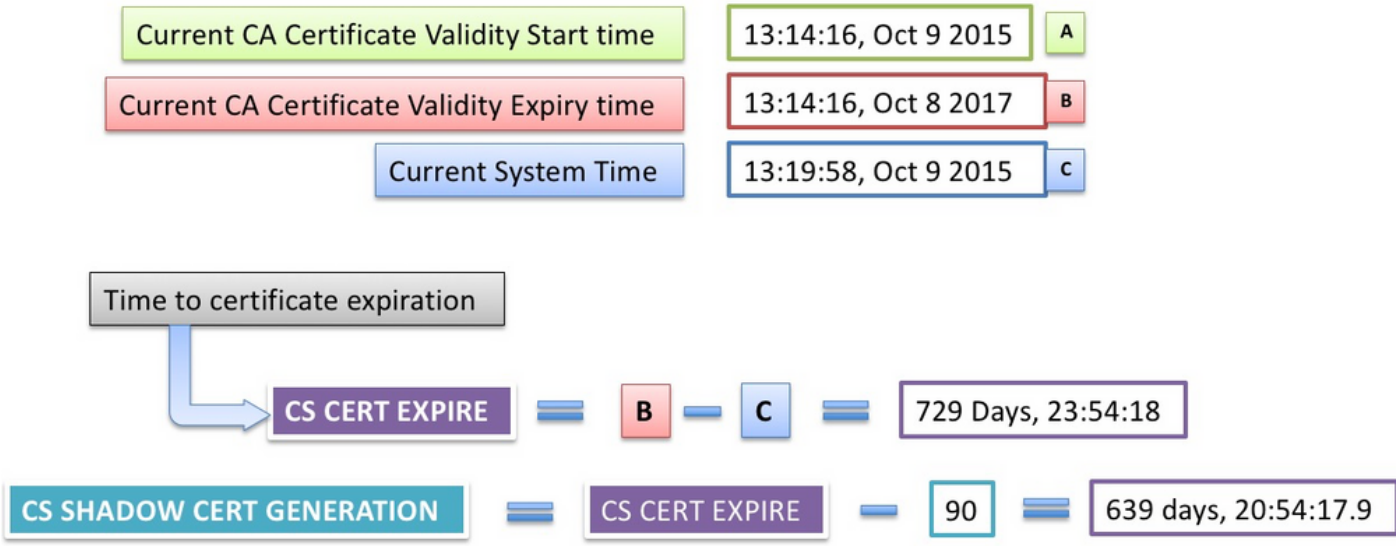
在PKI客户端自动续**约部分中，详细**说明。

PKI服务器自动回滚

在CA服务器上使用上述配置，您会看到：

```
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
```

请注意：



滚动操作

当CS SHADOW **CERT GENERATION计时器过期时：**

- IOS首先生成全反密钥对 — 当前其名称与活动密钥对相同，并附加#哈希。

```
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
```

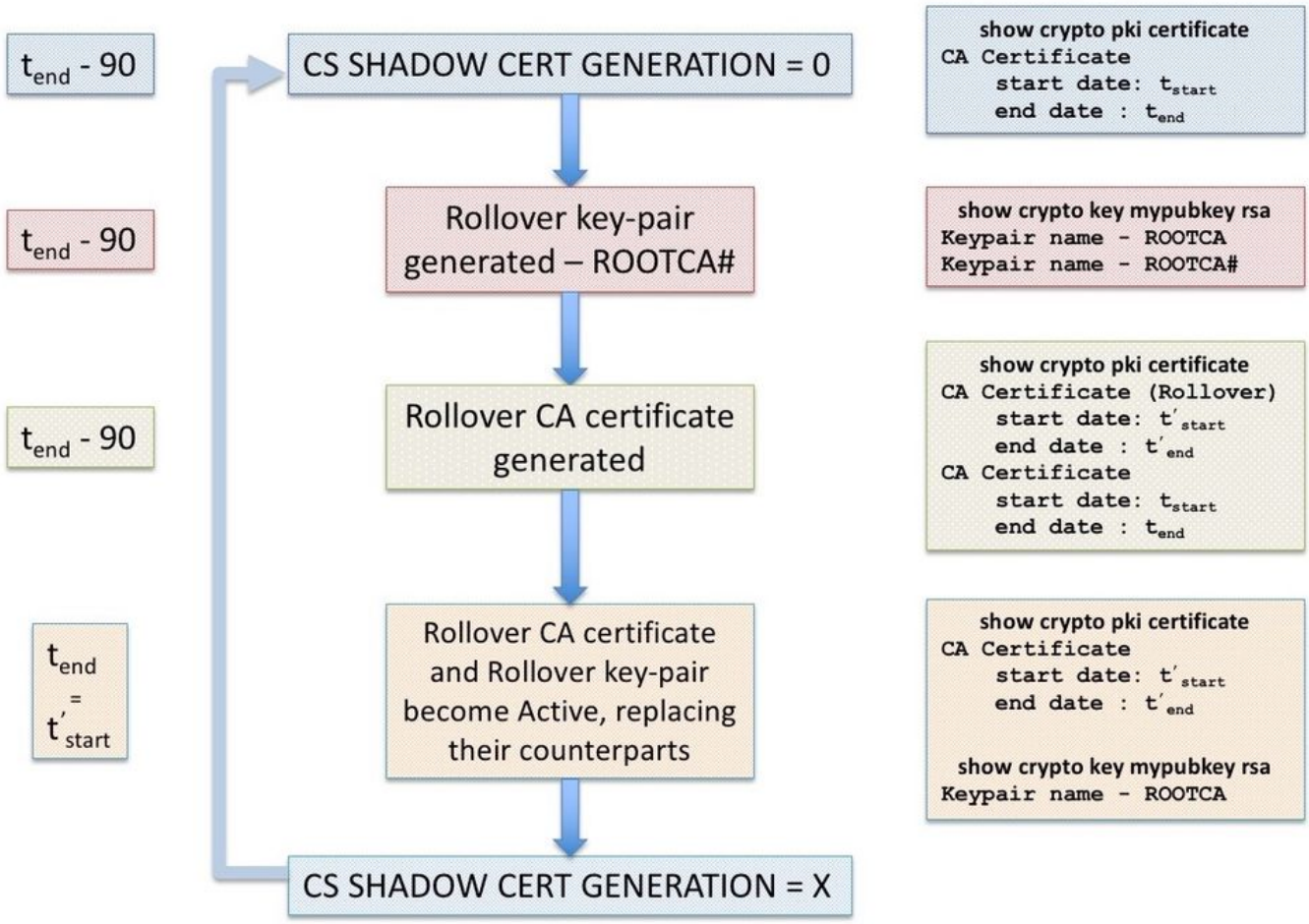
```
1818EA43 93C17CA1 C4917F43 C9199C9E F9F9C059 FDE11DA9 C7991826 43736FCE
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

- 然后，IOS生成全反CA证书，其有效性开始日期与当前活动CA证书的有效性结束日期相同。

```
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服务器手动回滚

IOS PKI服务器支持CA证书的手动滚动更新，即管理员可以提前触发滚动CA证书的生成，而无需在PKI服务器配**置下配**置自动滚动更新。强烈建议配置**自动**滚动，无论是否计划将初始部署的CA服务器的寿命延长到安全端。**PKI客户端可以使CA过载，而无需全反CA证书。***请参阅*PKI服务器全反上客户端SHADOW操作的依赖性。

使用配置级别命令可以触发手动滚动更新：

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

此外，可以取消滚动CA证书以手动生成新证书，但管理员在生产环境中不应执行以下操作：

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

这将删除全反rsa密钥对和全反CA证书。建议不要这样做，因为：

- 一旦CA生成全反证书，多个客户端可以下载全反CA证书以及由全反CA证书签名的全反客户端证书。
- 在此阶段，如果取消滚动更新，则可能需要重新注册客户端。

PKI客户端自动续约

客户端证书续约类型 — 续约和影子

PKI服务器上的IOS始终确保颁发给客户端的ID证书的到期时间不会超过CA证书的到期时间。

在PKI客户端上，在安排续约操作之前，IOS始终考虑以下计时器：

- 身份证书续约的到期时间
- 颁发者(CA)证书的到期时间

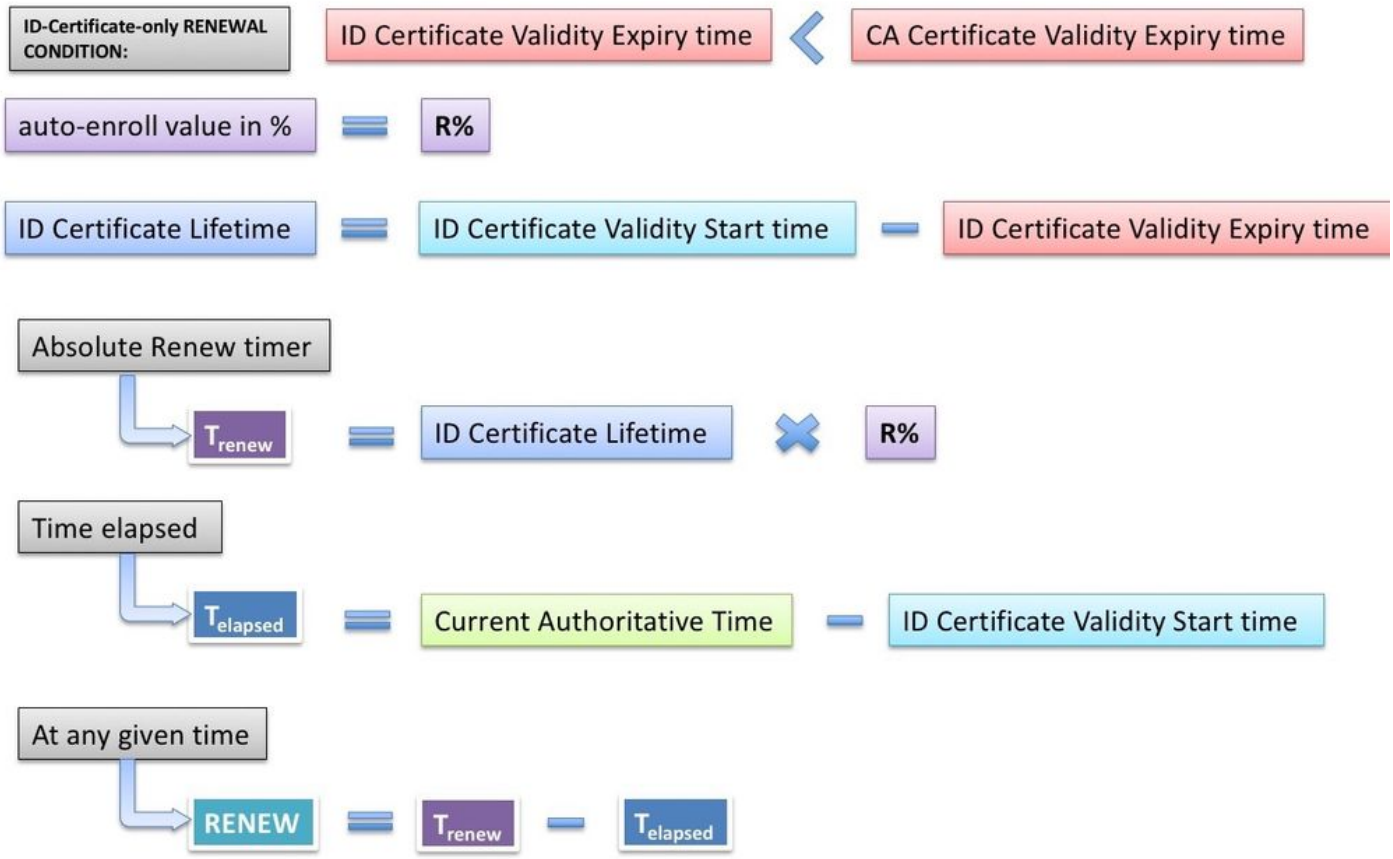
如果身份证书的到期时间与CA证书的到期时间不同，IOS将执行简单的续约操作。

如果身份证书的到期时间与CA证书的到期时间相同，IOS将执行影子续约操作。

RENEW — 路由器身份证书续约

如前所述，如果身份证书的到期时间与CA证书的到期时间不同，即在颁发者的证书触发简单身份证书的续订之前到期的身份证书，IOS PKI客户端执行简单的续订操作。

一旦安装了身份证书，IOS就会计算特定信任点的RENEW计时器，如下所示：

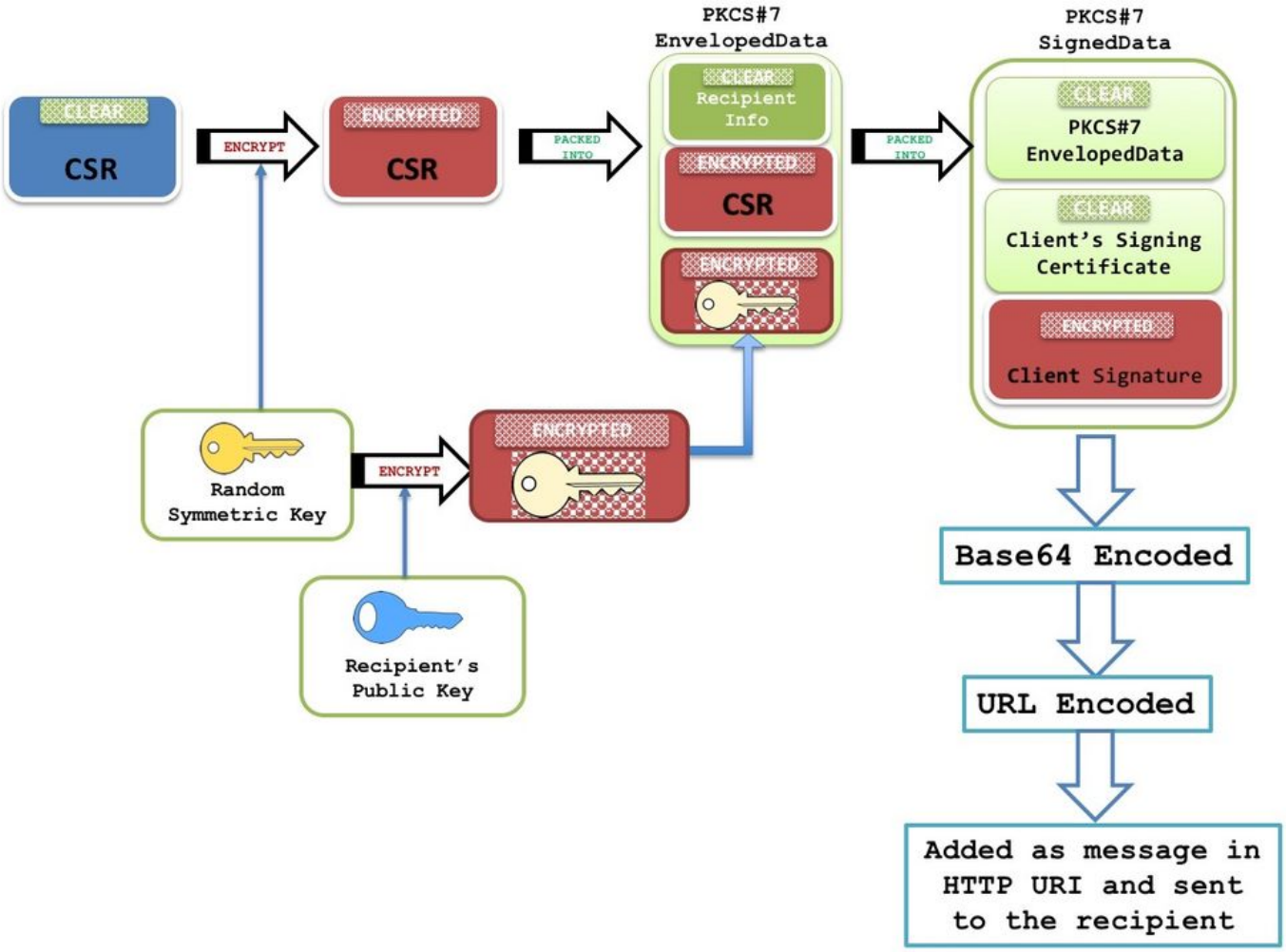


Current-Authoritative-Time表示系统时钟必须是此处所述的权威时间源。（链接到权威时间源部分）如果没有权威时间源，PKI计时器将不会初始化。因此，不会进行续约操作。

当RENEW计时器到期时，会发生以下事件：

- 如果配置了regenerate，则IOS会生**成卷**影密钥对[示例：auto-enroll 80 regenerate]。如果**不重**新生成IOS，将重新使用当前活动的RSA密钥对。
- IOS创建PKCS-10格式的证书请求，然后将其加密到PKCS-7信封中。此信封还包含RecipientInfo，该信息是颁发CA的主题名称和序列号。此PKCS7信封又打包为PKCS-7签名数据。在初始注册期间，IOS使用自签名证书签署此消息。在后续的注册（即重新注册）中

，IOS使用活动身份证书签署消息。PKCS7签名数据还嵌入签名证书，即自签名证书或身份证书。



有关此数据包结构的详细信息，请参阅SCEP概述文档

注意：此处的密钥信息是RecipientInfo，它是发出CA的主题名称和序列号，此CA的公钥用于加密对称密钥。PKCS7信封中的CSR使用此对称密钥进行加密。

此加密的对称密钥由接收CA使用其私钥解密，此对称密钥用于解密显示CSR的PKCS7信封。

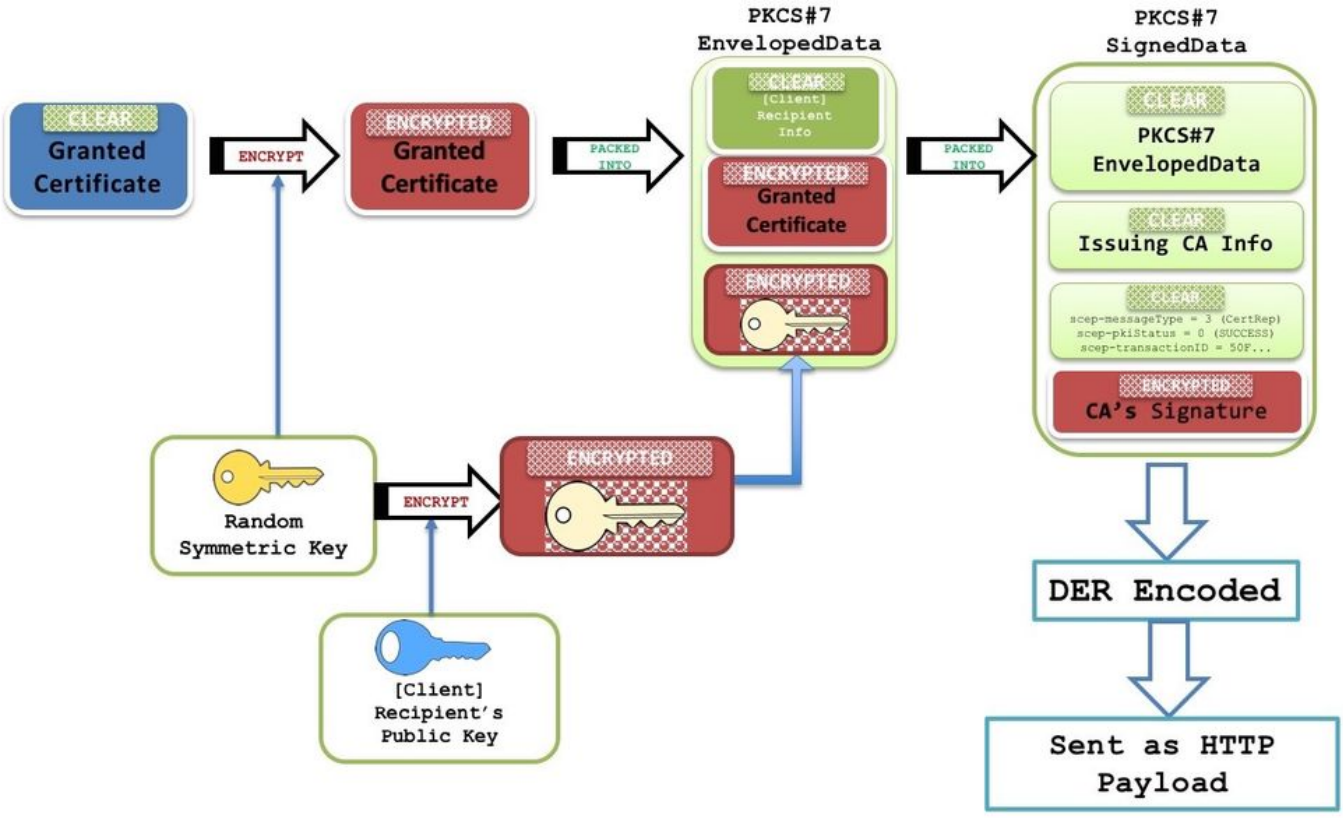
- 然后，以PKCS7格式打包的此证书签名请求(CSR)将以SCEP消息类型PKCSReq和SCEP操作PKIOperation发送到CA。
- 如果CA拒绝请求，IOS将停止RENEW计时器。从此时起，要续订身份证书，管理员必须执行手动续订(链接至PKI客**户端手动续订部**分)
- 如果CA将SCEP状态发送为**挂起**，则PKI客户端上的IOS将启动从60秒或1分钟开始的POLL计时器。每次POLL计时器到期时，IOS都会通过PKIOperation操作发送GetCertInitial SCEP消息。当第一个POLL计时器到期时，如果GetCertInitial消息以SCEP Pending状态响应，指数回退算法将第一个POLL计时器重试间隔设置为1分钟，第二个POLL计时器重试间隔设置为2分钟，默认情况下，第三次POLL计时器重试间隔为4分钟，等待接下来的999次重试，或直到颁发CA证书过期。
  可以使用以下方式配置轮询计数和第一次重试周期：

```
crypto pki trustpoint <TP>
```

```
    enrollment retry count <total retry count>
enrollment retry period <first retry period in minutes>
```

- 当证书在PKI服务器上授予时，下一条GetCertInitial SCEP消息将用内容类型**application/x-pki-message的HTTP消息和包含签名PKCS#7签名数据的**正文进行响应。此PKCS7签名数据包含SCEP状态为**已授权**，以及PKCS7已包装数据。此PKCS封装数据包含已授予的证书和RecipientInfo，后者是初始注册期间自签名证书的使用者名称和序列号，以及重新注册期间活动身份证书的序列号。

  PKCS7封装数据还包含使用收件人的公钥加密的对称密钥（新证书已为其授予）。 接收路由器使用私钥解密。然后，此清除对称密钥用于解密PKCS#7包络数据，揭示新的身份证书。



- 在此阶段，IOS会立即用新证书替换现有身份证书。如果配**置了**重新生成，则阴影密钥对也会替换活动密钥对。

- 此外，将新证书的结束日期与CA证书的结束日期进行比较，以确定是必须初始化RENEW计时器还是必须初始化SHADOW计时器，如<href **Types of Client Certificate Renew - RENEW and SHADOW>中所述**