IOS PKI部署指南：證書滾動更新 — 配置和操作概述

目錄

簡介

本檔案將詳細介紹Cisco IOS公開金鑰基礎架構(PKI)伺服器和使用者端上的憑證滾動更新。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

硬體

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

軟體

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

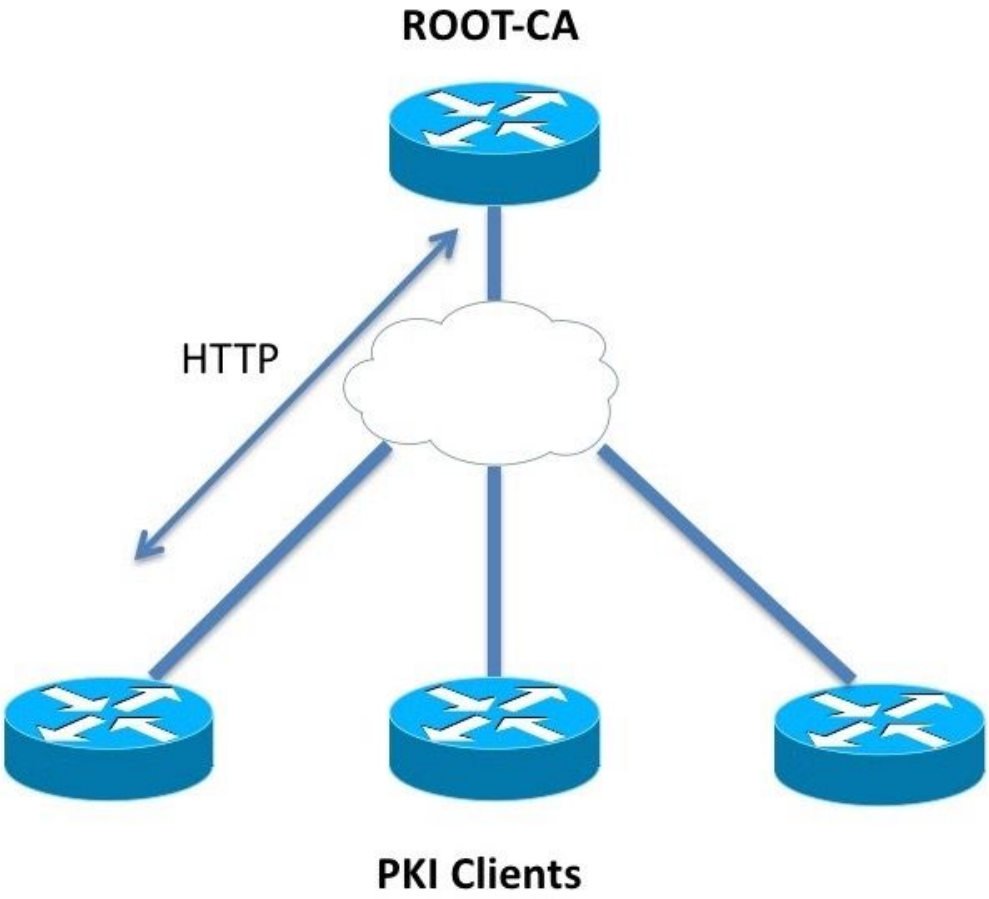
附註：ISR裝置的常規軟體維護不再處於活動狀態，任何未來的錯誤修復或功能增強都需要硬體升級到ISR-2或ISR-4xxx系列路由器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

證書滾動更新也稱為續訂操作，可確保當證書到期時，新證書可以接管。從PKI伺服器的角度來看，此操作涉及提前很長時間生成新的伺服器滾動更新證書，以確保所有PKI客戶端在當前證書過期之前都收到新伺服器滾動更新證書簽名的新客戶端滾動更新證書。從PKI客戶端的角度來看，如果客戶端證書即將到期但證書頒發機構(CA)伺服器的證書尚未到期，客戶端一收到新證書就請求新證書並替換舊證書，如果客戶端證書與CA伺服器的證書同時到期，客戶端首先確保收到CA伺服器的滾動證書，然後請求新CA伺服器的滾動證書簽名的滾動證書，舊證書到期時將啟用這兩個證書。

設定



PKI和簡單證書註冊協定(SCEP)前提條件

授權時間源

在IOS中，由於硬體時鐘不是最佳時間來源，因此預設時鐘來源會視為非授權來源。PKI對時間敏感，因此使用NTP配置有效的時間源非常重要。在PKI部署中，建議讓所有客戶端和伺服器通過多個NTP伺服器（如果需要）將其時鐘同步到單個NTP伺服器。IOS PKI Deployment Guide中會詳細介紹此問題：初始設計和部署

IOS不會在沒有授權時鐘的情況下初始化PKI計時器。雖然強烈建議使用NTP，但作為臨時措施，管理員可以使用以下方法將硬體時鐘標籤為權威的：

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

HTTP通訊

活動IOS PKI伺服器的要求是HTTP伺服器，可以使用以下config-level命令啟用該伺服器：

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

預設情況下，此命令在埠80上啟用HTTP伺服器，可以按上述方式更改。

PKI客戶端應該能夠通過HTTP與已配置的埠的PKI伺服器通訊。

PKI配置

伺服器 — 滾動更新

PKI伺服器自動滾動更新配置如下所示：

```
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
```

自動滾動更新引數以天數定義。在更精細的層級上，命令如下所示：

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

自動滾動更新值90表示IOS在當前伺服器證書到期之前90天建立滾動更新伺服器證書，並且此新滾動更新證書的有效性在當前活動證書到期時間的同時開始。

應配置自動翻轉值，以確保在網路中的任何PKI客戶端執行GetNextCACert操作之前，在PKI伺服器上提前很長時間生成翻轉的CA證書，如下面**SHADOW操作概述**一節所述。

客戶端 — 續訂

PKI客戶端自動證書續訂配置如下所示：

```
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
```

此處，**auto-enroll <percentage> [regenerate]**命令說明IOS應在當前證書生存期的80%準確執行證書續訂。

關鍵字**regenerate**表明，IOS應該在每次證書續訂操作期間重新生成名為shadow key-pair的RSA金鑰對。

設定自動註冊百分比時請務必小心。在部署中的任何特定PKI客戶端上，如果出現身份證書與頒發CA證書同時到期的情況，則自動註冊值應始終在CA建立滾動證書後觸發[shadow]續訂操作。請參閱部署示例下的**PKI計時器依賴性***部分*。

PKI續訂/更新先決條件

本文檔詳細介紹證書滾動更新和更新操作，因此認為這些事件已成功完成：

- 使用有效的CA證書初始化PKI伺服器。
- PKI客戶端已成功註冊到PKI伺服器。即每個PKI客戶端都具有CA證書和身份證書（稱為路由器證書）。

註冊客戶端涉及這些事件。不要過多地細說：

- 信任點身份驗證
- 信任點註冊

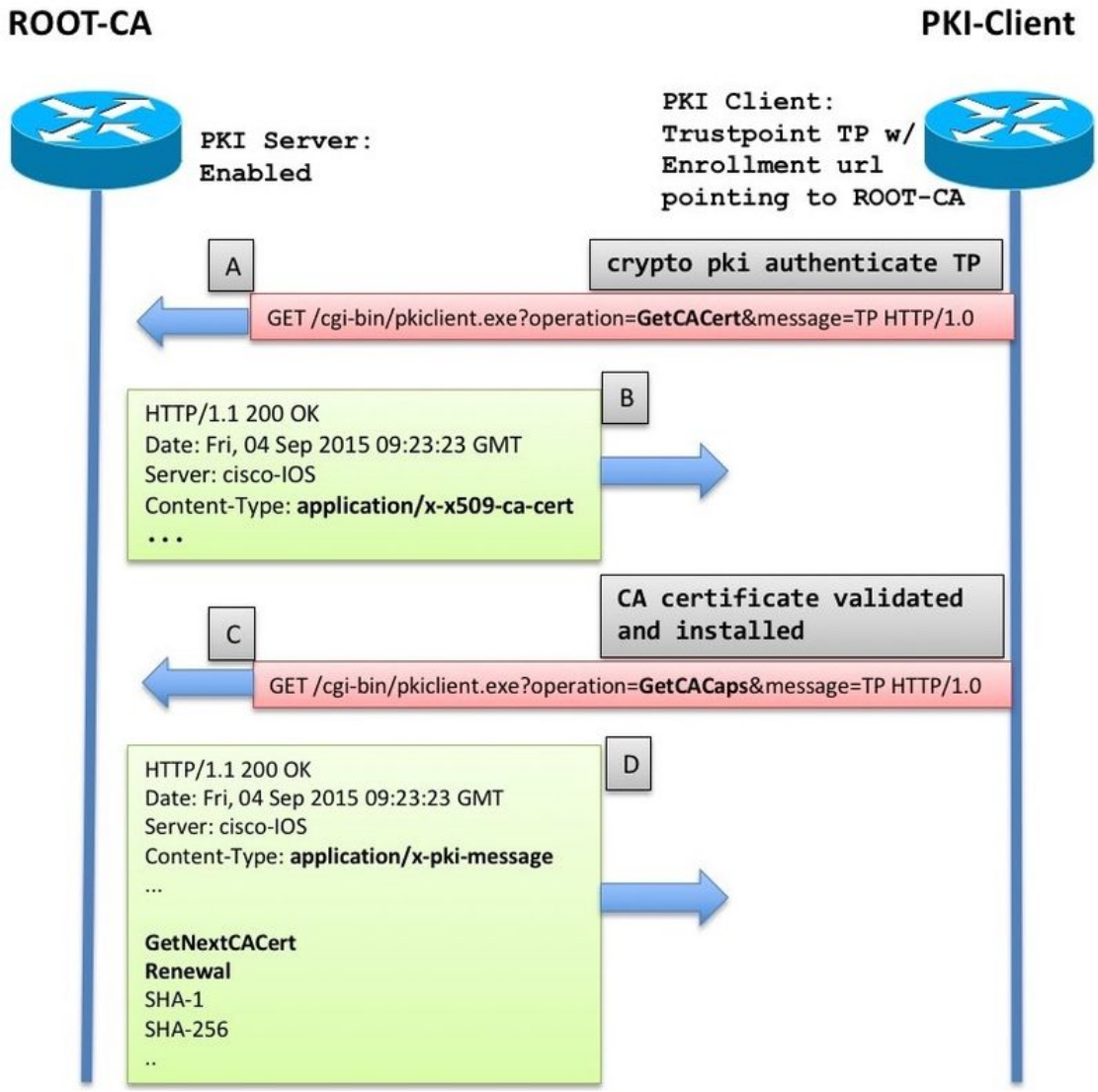
在IOS中，信任點是證書的容器。任何指定的信任點可以包含一個活動身份證書和/或一個活動CA證書。如果信任點包含活動的CA證書，則此信任點被視為已驗證。如果包含身份證書，則被視為已註冊。註冊前必須驗證信任點。IOS PKI Deployment Guide中詳細介紹了PKI伺服器和客戶端配置以及信任點身份驗證和註冊：初始設計和部署

在CA證書檢索/安裝之後，PKI客戶端在執行註冊之前檢索PKI伺服器功能。本節將介紹CA功能檢索。

CA功能

在IOS中，當PKI客戶端對CA進行身份驗證時(換句話說，當管理員在IOS路由器上建立信任點並執行命令**crypto pki authenticate <trustpoint-name>**)，以下事件在路由器上發生：

- IOS傳送包含GetCACert操作型別的SCEP請求。
- 此處預期的響應是內容型別為**application/x-x509-ca-cert**（在CA部署中）的HTTP消息，或**application/x-x509-ca-ra-cert**（在RA和CA部署中）。HTTP正文包含了CA證書。[後一種情況下為RA證書]。
- 在CA/RA證書檢索和安裝之後，客戶端啟動包含GetCACaps操作的自動SCEP請求。
- 此處預期的響應是包含內容型別**application/x-pki-message**的HTTP消息，該消息也可以是文本/純文字檔案，並且HTTP正文包含一系列由CA支援的功能，並以換行符分隔。典型的IOS PKI伺服器響應如下圖所示。



IOS PKI Client會將此響應解釋為：

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

在這些功能中，本文檔重點介紹這兩種功能。

GetNextCACert

當CA返回此功能時，IOS知道CA支援CA證書滾動更新。若在信任點下未配置**auto-enroll**命令，IOS將設定為CA證書有效期90%的SHADOW計時器初始化為已返回此功能。

當SHADOW計時器到期時，IOS會執行GetNextCACert SCEP操作以提取滾動更新CA證書。

> **註**：如果在信任點下配置了**auto-enroll**命令以及**enrollment url**，則在驗證信任點之前會初始化RENEW計時器，並且它不斷嘗試使用位於**enrollment url**的CA進行註冊，儘管在驗證信任點之前不會傳送實際註冊消息[CSR]。

> **附註**：GetNextCACert由IOS PKI伺服器作為功能進行傳送，即使伺服器上未配置**自動**滾動更

新

續約

通過此功能，PKI伺服器通知PKI客戶端它可以使用活動ID證書來簽署證書簽名請求以更新現有證書。

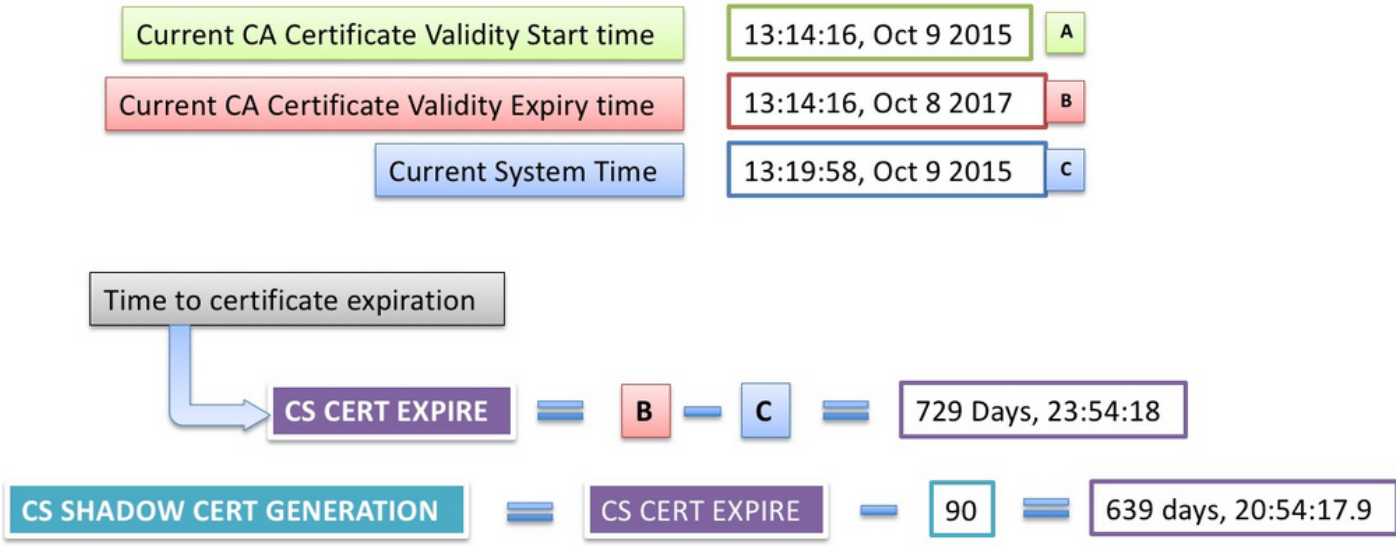
在PKI Client Auto-Renewal部分對此進行詳細說明。

PKI伺服器自動滾動更新

在CA伺服器上使用上述配置時，您會看到：

```
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
```

請注意：



滾動更新操作

CS SHADOW CERT GENERATION計時器到期時：

- IOS首先生成一個翻轉金鑰對 — 當前它與活動金鑰對具有相同的名稱，並在其中附加了#雜湊。

```
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
```

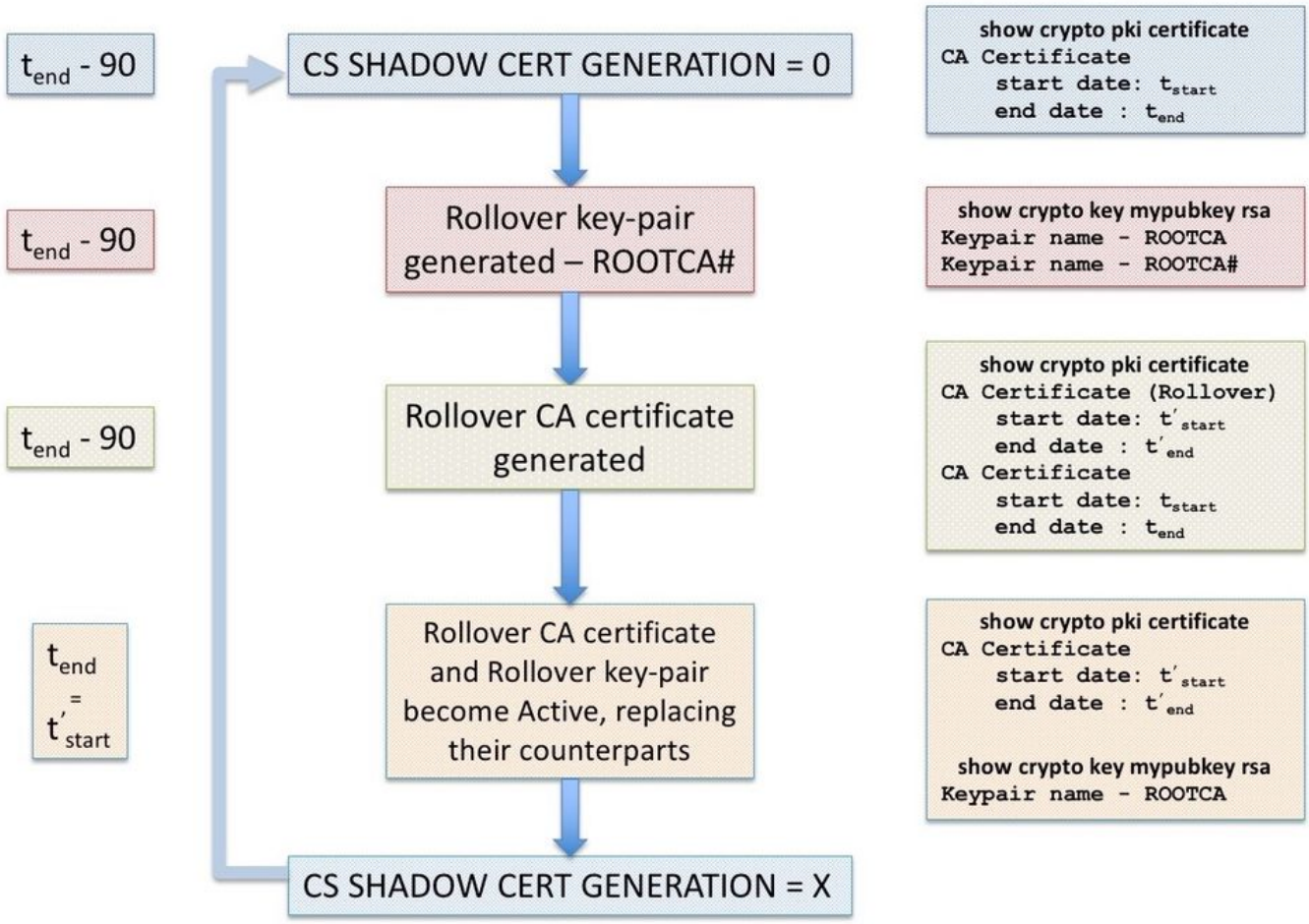
```
687F112B C9263541 BB402939 9C66D270 8D3EACED 4F63AA50 9FB340E8 38C8AC38
1818EA43 93C17CA1 C4917F43 C9199C9E F9F9C059 FDE11DA9 C7991826 43736FCE
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

- 然後IOS生成全反CA證書，其中有效開始日期與當前有效CA證書的有效結束日期相同。

```
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伺服器手動回滾

IOS PKI Server支援CA證書的手動翻轉，即管理員可以提前觸發生成翻轉CA證書，而無需在PKI伺服器配置下配置**自動翻轉**。強烈建議配置**自動回滾**，無論使用者是否計畫將初始部署的CA伺服器的生命週期延長到更安全的一端。**PKI客戶端無需翻轉CA證書即可使CA過載**。請參閱[在PKI伺服器滾動更新上依賴客戶端SHADOW操作]。

可以使用配置級別命令觸發手動滾動更新：

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

此外，還可以取消滾動更新CA證書以手動生成新的證書，但管理員不應在生產環境中執行以下操作：

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

這將刪除滾動更新rsa金鑰對和滾動更新CA證書。建議不要這樣做，因為：

- 一旦CA生成滾動更新證書，多個客戶端可以下載滾動更新CA證書以及由該滾動更新CA證書簽名的滾動更新客戶端證書。
- 在這個階段，如果取消滾動更新，則可能需要重新註冊客戶端。

PKI使用者端自動續訂

客戶端證書續訂的型別 — RENEW和SHADOW

PKI伺服器上的IOS一律確保核發給使用者端的ID憑證的到期時間不會超過CA憑證的到期時間。

在PKI客戶端上，IOS在安排續訂操作之前始終會考慮以下計時器：

- 正在續訂標識證書的到期時間
- 頒發者(CA)證書的到期時間

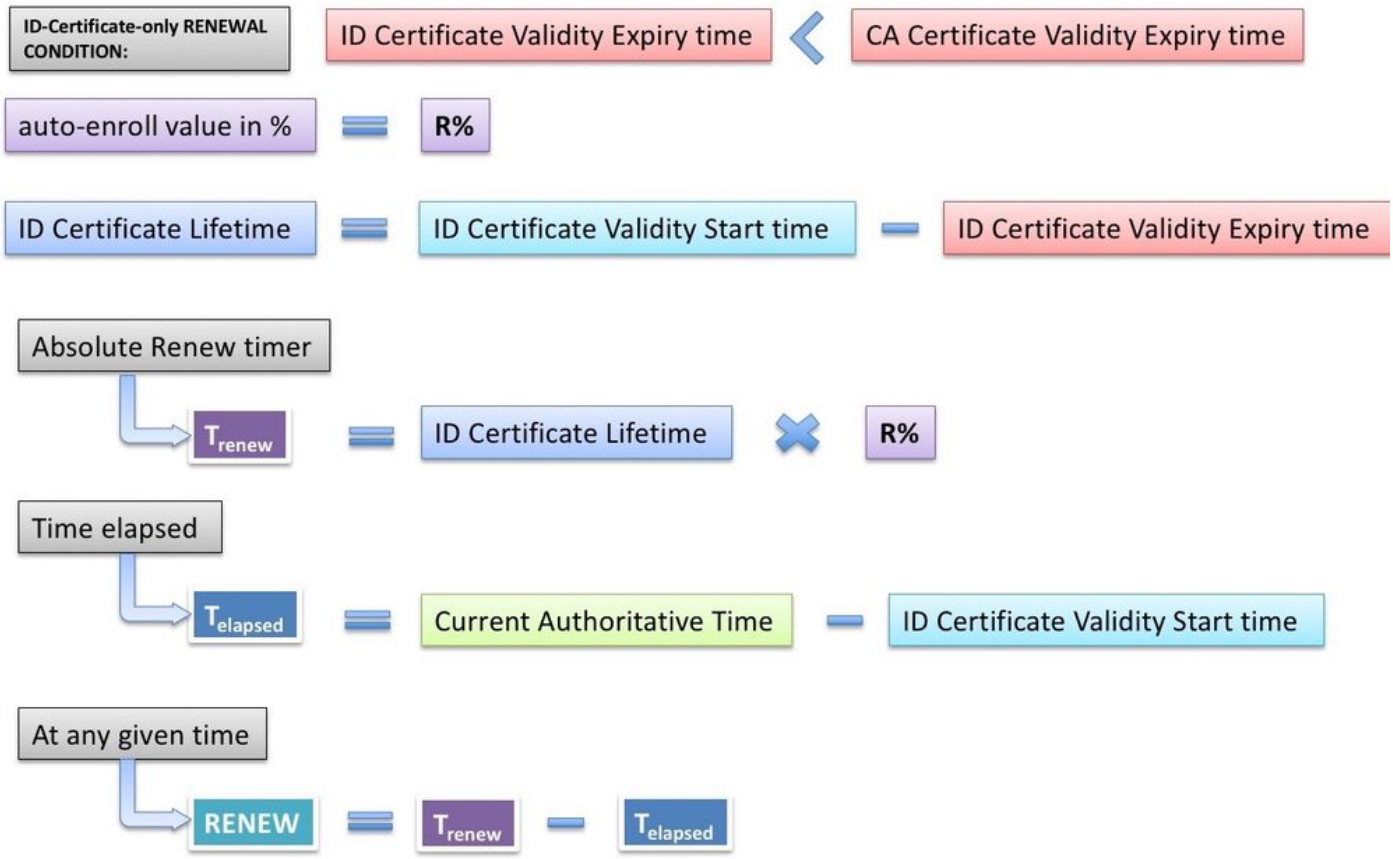
如果身份證書的到期時間與CA證書的到期時間不同，IOS會執行簡單的續訂操作。

如果身份證書的到期時間與CA證書的到期時間相同，IOS將執行卷影續訂操作。

RENEW — 路由器身份證書續訂

如前所述，如果身份證書的到期時間與CA證書的到期時間不同，IOS PKI客戶端執行簡單的續訂操作，換句話說，在頒發者的證書觸發簡單身份證書的續訂之前到期的身份證書。

一旦安裝身份證書，IOS就會計算特定信任點的RENEW計時器，如下所示：

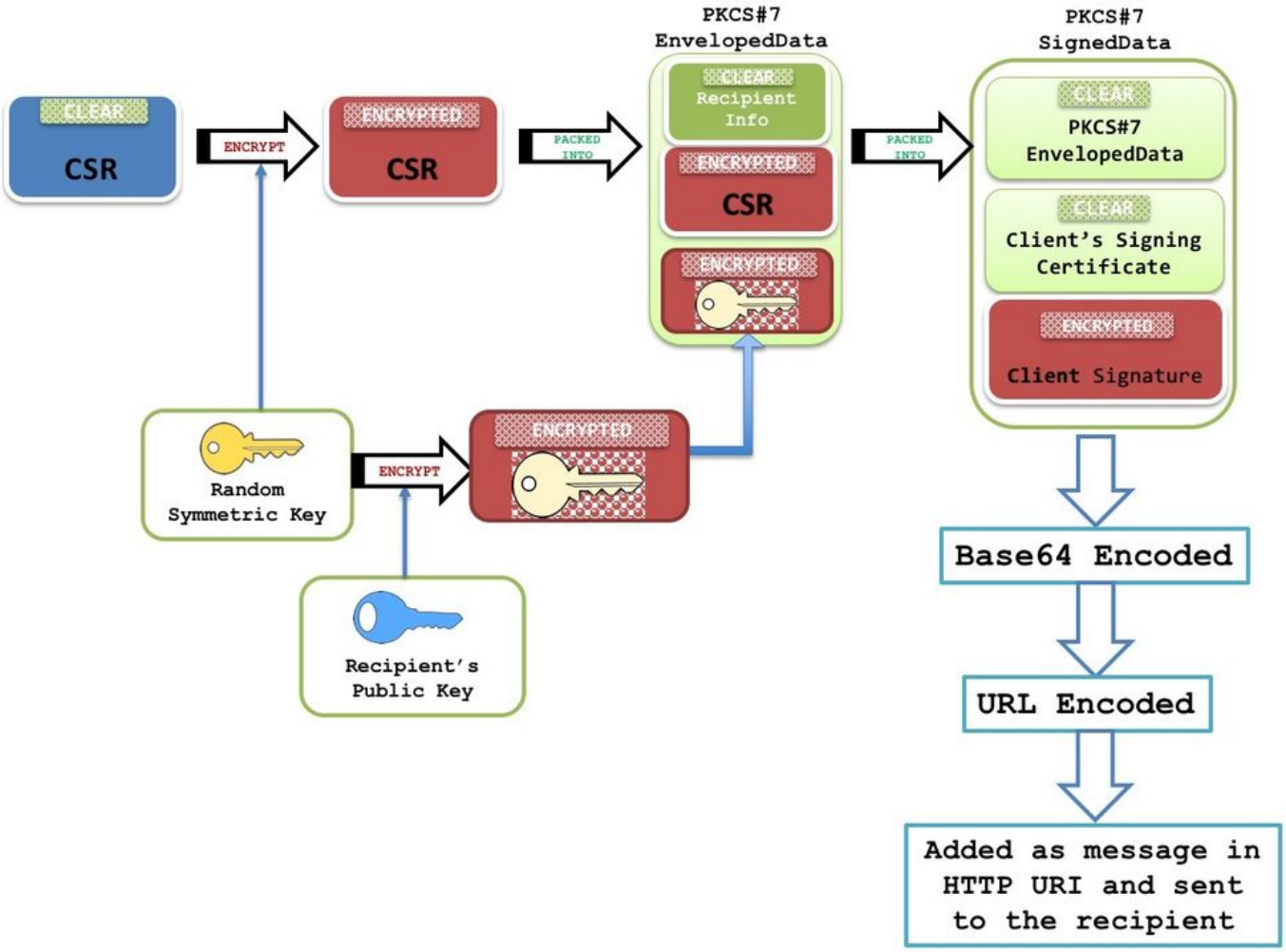


Current-Authoritative-Time表示系統時鐘必須是此處所述的權威時間源。（連結到授權時間源部分）如果沒有授權時間源，PKI計時器將無法初始化。因此，不會進行續訂操作。

當RENEW計時器到期時，發生以下事件：

- 如果已設定**regenerate**，則IOS會產生卷影金鑰對[範例：自動註冊[80 regenerate]。如果沒有**regenerate** IOS，將重新使用當前活動的RSA金鑰對。
- IOS建立一個PKCS-10格式的證書請求，然後將其加密到PKCS-7信封中。此信封還包含RecipientInfo，它是發佈CA的主題名稱和序列號。此PKCS7-envelope又打包為PKCS-7 signed-data。在初始註冊過程中，IOS使用自簽名證書對此消息進行簽名。在後續的註冊（即

重新註冊）期間，IOS使用活動身份證書對消息進行簽名。PKCS7簽名資料還嵌入了簽名證書，即自簽名證書或身份證書。



有關此資料包結構的詳細資訊，請參閱SCEP概述文檔

附註：此處的金鑰資訊是RecipientInfo，它是發佈CA的主題名稱和序列號，此CA的公鑰用於加密對稱金鑰。PKCS7信封中的CSR使用此對稱金鑰加密。

此加密的對稱金鑰由接收CA使用其私鑰解密，並且此對稱金鑰用於解密顯示CSR的PKCS7信封。

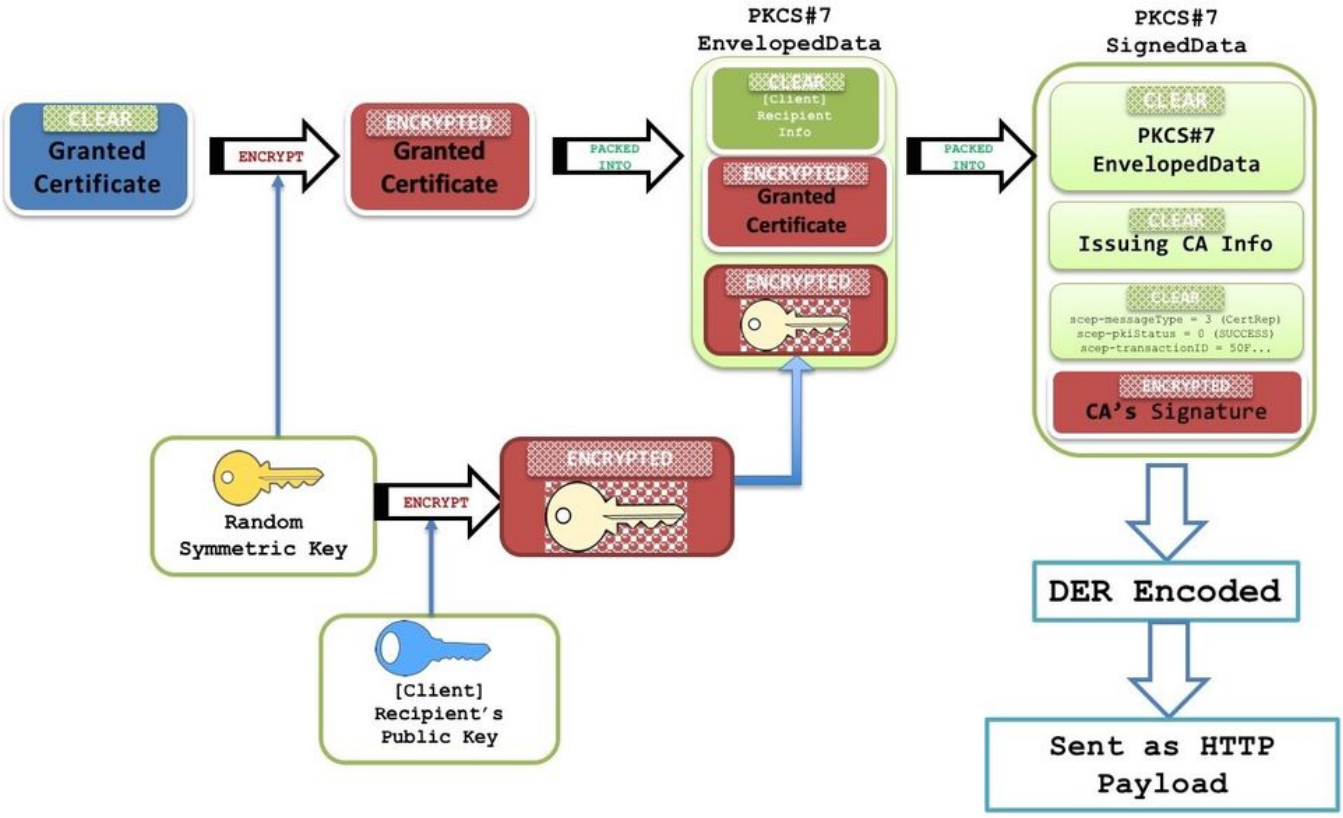
- 然後，將打包為PKCS7格式的此證書簽名請求(CSR)傳送給CA，該請求的SCEP消息型別為PKCSReq，並且執行名為PKIOperation的SCEP操作。
- 如果CA拒絕該請求，IOS將停止續訂計時器。從此以後，要續訂身份證書，管理員必須執行手動續訂(連結到**PKI client Manual-Renewal**部分)
- 如果CA將SCEP狀態傳送為**pending**，則PKI客戶端上的IOS會啟動一個POLL計時器，開始時間為60秒或1分鐘。每次POLL計時器到期時，IOS都會通過PKIOperation操作傳送GetCertInitial SCEP消息。當第一個POLL計時器到期時，如果使用SCEP Pending狀態響應GetCertInitial消息，則指數回退演算法會將第一個POLL計時器重試間隔設定為1分鐘，將第二個POLL計時器重試間隔設定為2分鐘，將第三個POLL計時器重試間隔設定為4分鐘，等等，以預設方式執行下一個999999重試或發出CA證書到期。
  可以使用以下命令配置輪詢計數和第一個重試週期：

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

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

- 在PKI伺服器上授予證書時，下一個GetCertInitial SCEP消息將用內容型別**application/x-pki-message**和包含已簽名PKCS#7簽名資料的正文進行響應。此PKCS7簽名資料包含**Granted**的SCEP狀態以及PKCS7封裝資料。此PKCS封裝資料包含已授予的證書和RecipientInfo，後者是初始註冊期間自簽名證書的主題名稱和序列號，以及重新註冊期間活動身份證書的主題名稱和序列號。

  PKCS7封裝資料還包含使用接收者的公鑰（為其授予新證書）加密的對稱金鑰。 接收路由器使用私鑰對其進行解密。然後，此清除對稱金鑰用於解密PKCS#7封裝的資料，顯示新的身份證書。



- 在這個階段，IOS會立即用新證書替換現有的身份證書。如果配置了**regenerate**，則卷影金鑰對也會替換活動的金鑰對。

- 此外，新憑證的結束日期會與CA憑證的結束日期進行比較，以確定是否必須初始化RENEW計時器或必須初始化SHADOW計時器，如以下所述<href **Types of Client Certificate Renew - RENEW and SHADOW>**