Guida alla distribuzione di IOS PKI: Rollover dei certificati - Panoramica della configurazione e del funzionamento

Sommario

Introduzione

Questo documento descrive in dettaglio il rollover dei certificati su server e client PKI (Public Key Infrastructure) Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

Hardware

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

Software

- IOS
  - Per ISR-G1 - Ultima versione 15.1(4)M*
  - Per ISR-G2 - Ultima versione 15.4(3)M
- IOS-XE
  - XE 3.15 o 15.5(2)S

Nota: La manutenzione generale del software per i dispositivi ISR non è più attiva. Per eventuali correzioni di bug o miglioramenti delle funzionalità futuri, sarà necessario aggiornare l'hardware ai router serie ISR-2 o ISR-4xxx.

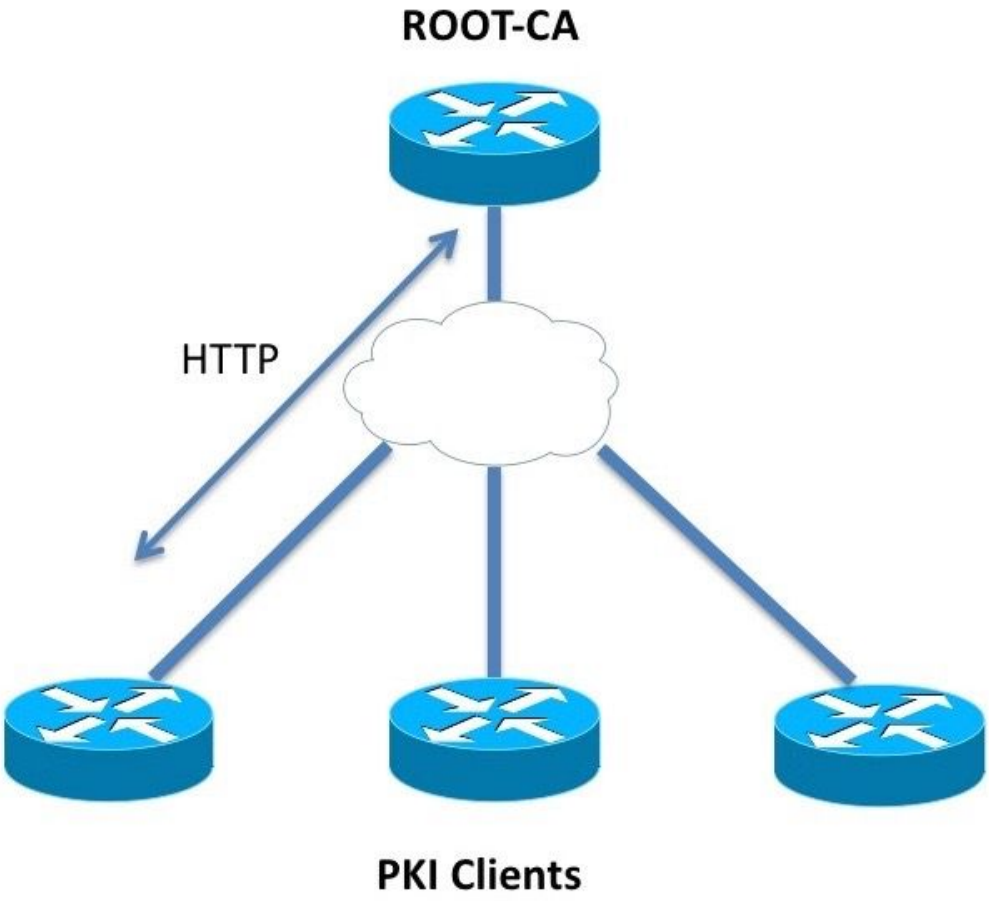
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il rollover dei certificati, noto anche come operazione di rinnovo, garantisce che alla scadenza di un certificato sia pronto un nuovo certificato. Dal punto di vista di un server PKI, questa operazione implica la generazione del nuovo certificato di rollover del server con un anticipo

considerevole per garantire che tutti i client PKI abbiano ricevuto un nuovo certificato di rollover del client firmato dal nuovo certificato di rollover del server prima della scadenza del certificato corrente. Dal punto di vista di un client PKI, se il certificato client è in scadenza ma il certificato del server CA non lo è, il client richiede un nuovo certificato e sostituisce il vecchio certificato non appena il nuovo certificato viene ricevuto e se il certificato client scade contemporaneamente al certificato del server CA, il client si assicura di ricevere prima il certificato di rollover del server CA, quindi richiede un certificato di rollover firmato dal nuovo certificato di rollover del server CA ed entrambi verranno attivati alla scadenza dei vecchi certificati.

Configurazione



Prerequisiti PKI e SCEP (Simple Certificate Enrollment Protocol)

Origine ora autorevole

In IOS, per impostazione predefinita l'origine dell'orologio è considerata non autorevole in quanto l'orologio hardware non è la migliore fonte di tempo. Poiché la PKI fa distinzione tra ore, è importante configurare un'origine del tempo valida utilizzando NTP. In una distribuzione PKI è consigliabile che tutti i client e il server sincronizzino il proprio orologio su un singolo server NTP, se necessario tramite più server NTP. Per ulteriori informazioni, vedere la Guida alla distribuzione

di PKI su IOS: Progettazione e installazione iniziali

IOS non inizializza i timer PKI senza un orologio autorevole. Sebbene l'NTP sia altamente consigliato, come misura temporanea, l'amministratore può contrassegnare l'orologio hardware come autorevole utilizzando:

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

Comunicazione HTTP

Un requisito per un server PKI IOS attivo è il server HTTP, che può essere abilitato utilizzando questo comando a livello di configurazione:

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

Questo comando abilita il server HTTP sulla porta 80 per impostazione predefinita, che può essere modificata come mostrato in precedenza.

I client PKI devono essere in grado di comunicare con il server PKI tramite HTTP alla porta configurata.

Configurazione PKI

Server - Rollover

La configurazione di rollover automatico del server PKI è simile alla seguente:

```
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
```

Il parametro di rollover automatico è definito in giorni. A un livello più granulare, il comando ha il seguente aspetto:

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

Un valore di rollover automatico pari a 90 indica che IOS crea un certificato server di rollover 90 giorni prima della scadenza del certificato server corrente e che la validità del nuovo certificato di rollover inizia contemporaneamente alla scadenza del certificato attivo corrente.

Il rollover automatico deve essere configurato con un valore tale da garantire che il certificato CA di rollover venga generato sul server PKI con molto anticipo rispetto all'esecuzione dell'operazione GetNextCACert da parte di qualsiasi client PKI della rete, come descritto nella sezione **Panoramica delle operazioni SHADOW** riportata di seguito.

Client - Rinnovo

La configurazione per il rinnovo automatico dei certificati del client PKI è simile alla seguente:

```
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
```

In questo caso, il comando **auto-enroll <percentuale> [regenerate]** indica che IOS deve eseguire il rinnovo del certificato esattamente all'80% della durata del certificato corrente.

La parola chiave **regenerate** indica che IOS deve rigenerare la coppia di chiavi RSA, nota come coppia di chiavi shadow, durante ogni operazione di rinnovo del certificato.

Prestare attenzione durante la configurazione della percentuale di registrazione automatica. In qualsiasi client PKI specificato nella distribuzione, se si verifica una condizione in cui il certificato di identità scade contemporaneamente al certificato CA emittente, il valore di registrazione automatica deve sempre attivare l'operazione di rinnovo [shadow] dopo che la CA ha creato il certificato di rollover. Fare riferimento alla sezione **Dipendenze timer PKI** *negli esempi di distribuzione.*

Prerequisiti per il rinnovo/rollover di PKI

In questo documento vengono descritte in dettaglio le operazioni di rinnovo e rollover dei certificati e pertanto questi eventi vengono considerati completati correttamente:

- Inizializzazione del server PKI con un certificato CA valido.
- Registrazione dei client PKI con il server PKI completata. Ad esempio, ogni client PKI dispone del certificato CA e di un certificato di identità, ovvero di un certificato router.

La registrazione di un client comporta questi eventi. Senza entrare troppo nei dettagli:

- Autenticazione Trustpoint
- Registrazione Trustpoint

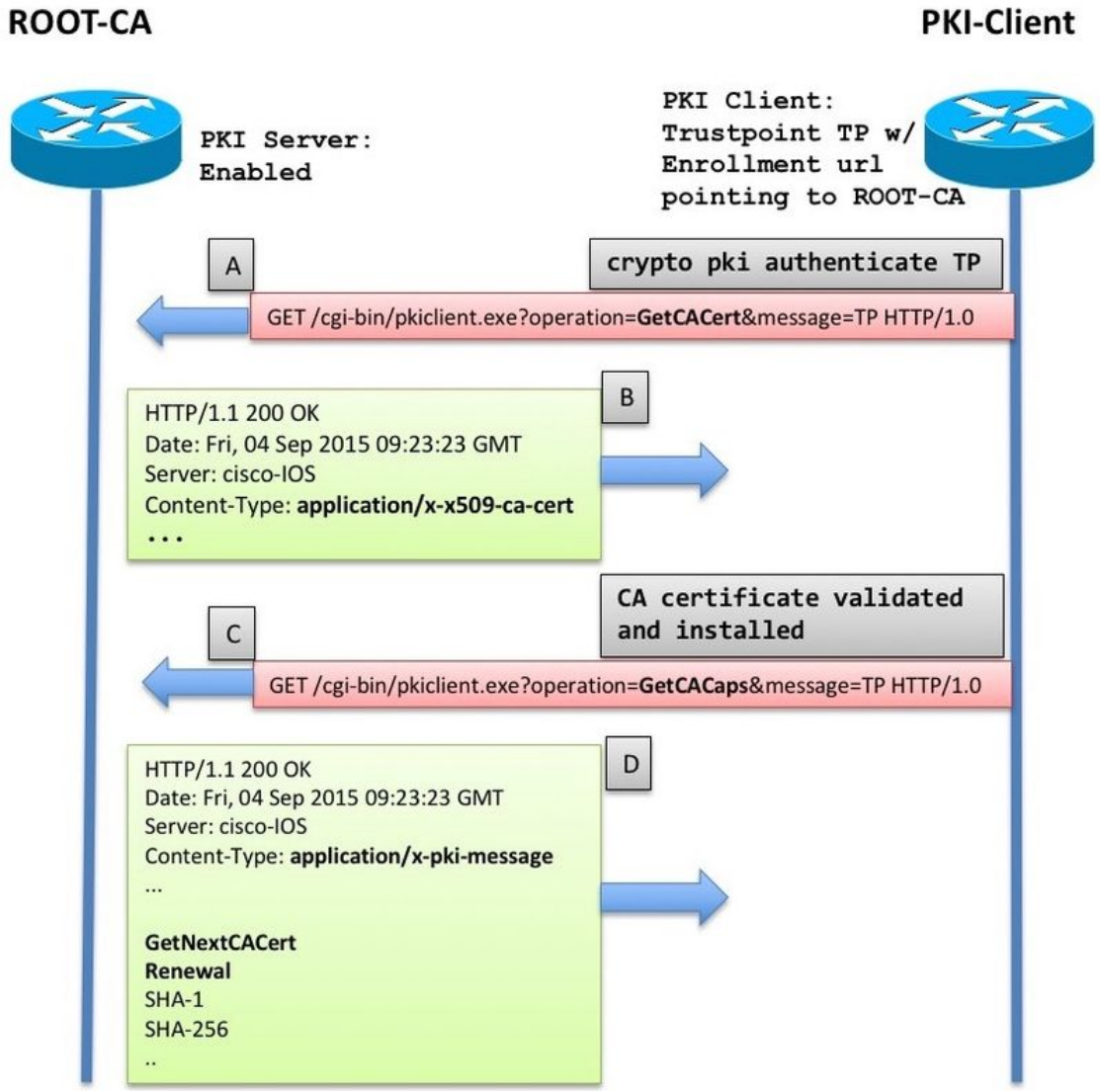
In IOS, un trust point è un contenitore di certificati. Un determinato trust point può contenere un certificato di identità attivo e/o un certificato CA attivo. Un trust point è considerato autenticato se contiene un certificato CA attivo. E viene considerato registrato se contiene un certificato di identità. Un trust point deve essere autenticato prima di una registrazione. La configurazione del server e del client PKI, insieme all'autenticazione e alla registrazione del trust point sono illustrate in dettaglio nella Guida alla distribuzione di PKI IOS: Progettazione e installazione iniziali

Dopo il recupero o l'installazione del certificato CA, il client PKI recupera le funzionalità del server PKI prima di eseguire una registrazione. In questa sezione viene illustrato il recupero delle funzionalità CA.

Capacità CA

In IOS, quando un client PKI autentica una CA, in altre parole, quando un amministratore crea un trust point su un router IOS ed esegue il comando **crypto pki authentication <trustpoint-name>**, sul router si verificano gli eventi seguenti:

- IOS invia una richiesta SCEP contenente il tipo di operazione GetCACert.
- La risposta prevista è un messaggio HTTP con un tipo di contenuto **applicazione/x-x509-ca-cert** in caso di distribuzione CA o **applicazione/x-x509-ca-ra-cert** in caso di distribuzione CA e CA. Il corpo HTTP contiene il certificato CA. [e un certificato RA in quest'ultimo caso].
- Dopo il recupero e l'installazione del certificato CA/RA, il client avvia una richiesta SCEP automatica contenente l'operazione GetCACaps.
- La risposta prevista è un messaggio HTTP con un tipo di contenuto **application/x-pki-message**, che potrebbe anche essere **text/plain** e il corpo HTTP contiene una serie di funzionalità supportate dalla CA, separate da un carattere di avanzamento riga. Una risposta tipica del server PKI IOS è come illustrato nel diagramma seguente.



La risposta viene interpretata nel modo seguente dal client PKI IOS:

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

Di queste funzionalità, il presente documento si concentra su queste due.

GetNextCACert

Quando questa funzionalità viene restituita dalla CA, IOS riconosce che la CA supporta il rollover dei certificati CA. Con questa funzionalità restituita, se il comando **auto-enroll** non è configurato nel trust point, IOS inizializza un timer SHADOW impostato sul 90% del periodo di validità del certificato CA.

Quando il timer SHADOW scade, IOS esegue l'operazione GetNextCACert SCEP per recuperare il certificato CA di rollover.

> **Nota**: se il comando di **registrazione automatica** è stato configurato nel punto di attendibilità insieme a un **URL di registrazione**, viene inizializzato un timer di rinnovo prima dell'autenticazione del punto di attendibilità. Il timer tenta costantemente di eseguire la registrazione con la CA situata nell'**URL di registrazione**, sebbene non venga inviato alcun messaggio di registrazione effettivo [CSR] finché il punto di attendibilità non viene autenticato.

> **Nota:** GetNextCACert viene inviato come funzionalità dal server PKI IOS anche se il **rollover automatico** non è configurato sul server

Rinnovo

Con questa funzionalità, il server PKI informa il client PKI che può utilizzare un certificato ID attivo per firmare una richiesta di firma del certificato per rinnovare il certificato esistente.

Per ulteriori informazioni, vedere la sezione **Rinnovo automatico client PKI**.

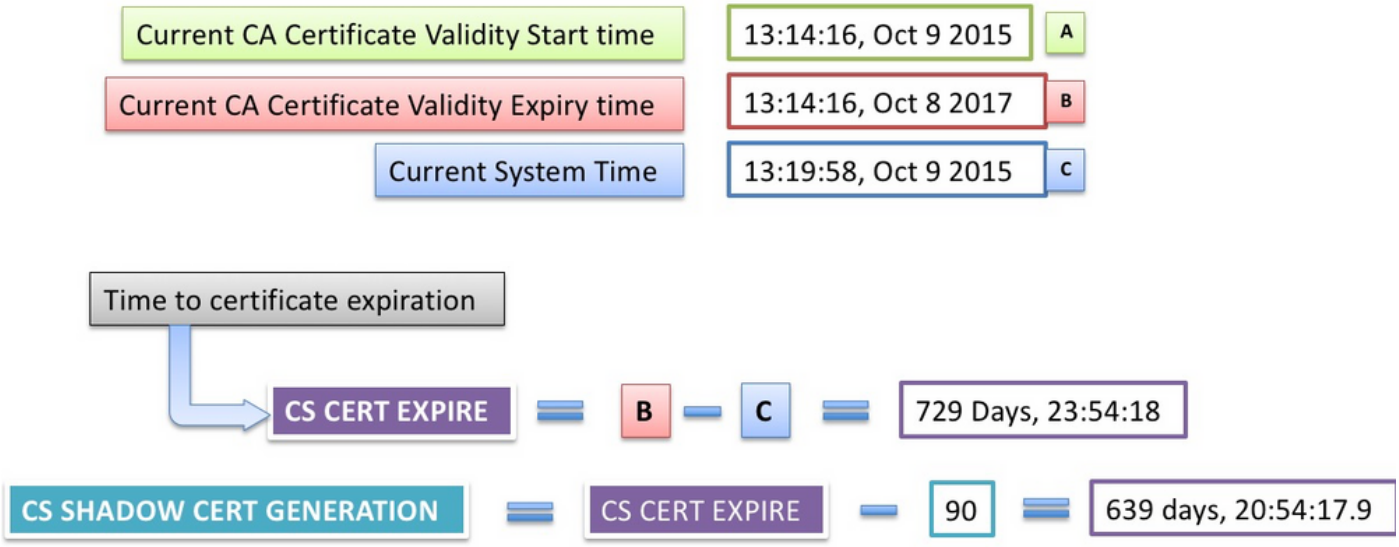
Rollover automatico server PKI

Con la configurazione sopra riportata sul server CA, è possibile visualizzare:

```
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
```

Si noti quanto segue:



Operazione di rollover

Alla scadenza del timer di **generazione del certificato SHADOW CS**:

- IOS genera prima una coppia di chiavi di rollover. Attualmente ha lo stesso nome della coppia di chiavi attiva a cui è stato aggiunto un hash #.

```
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
```

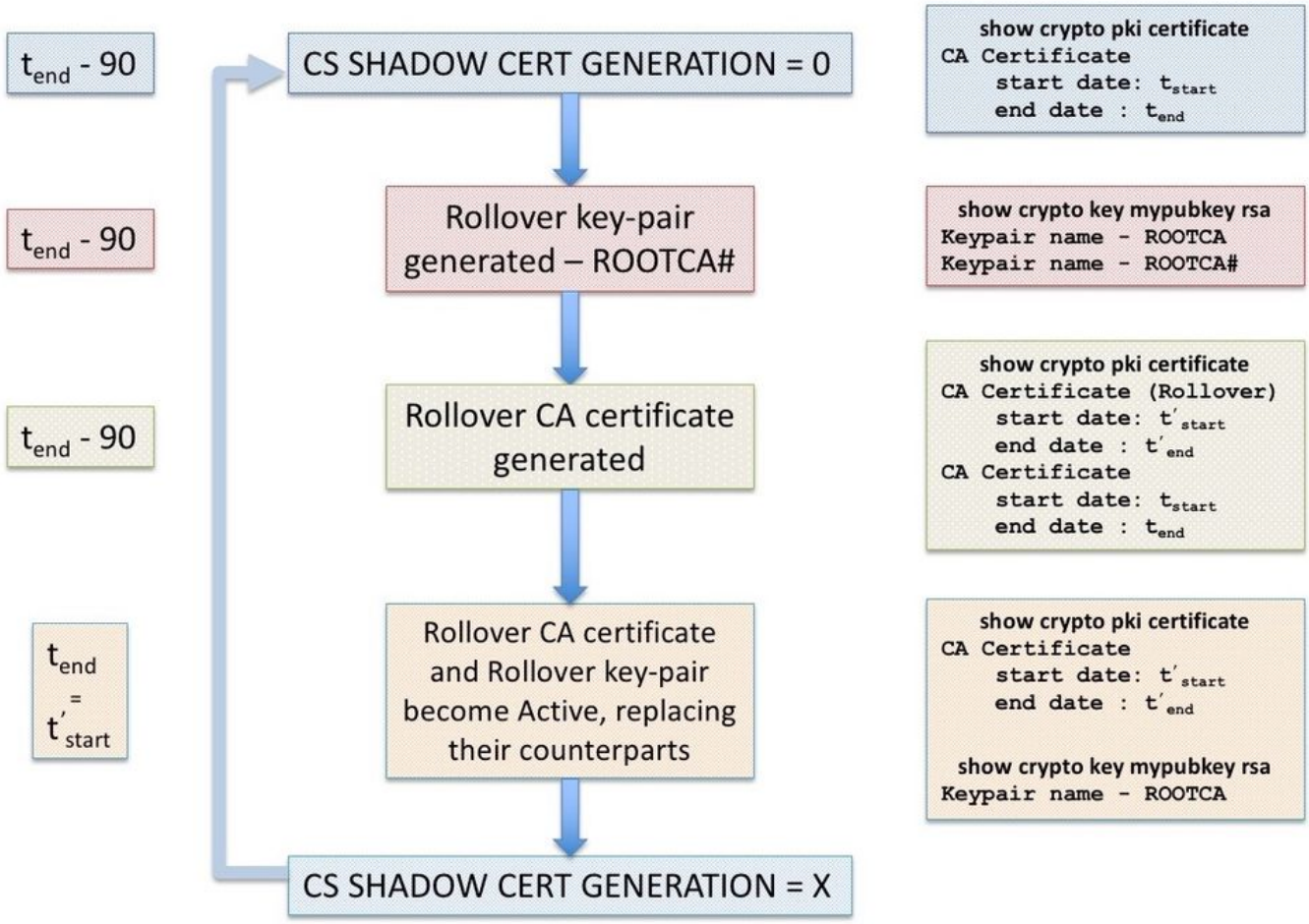
- IOS genera quindi il certificato CA di rollover, in cui la data di inizio validità corrisponde alla data di fine validità del certificato CA attivo corrente.

```
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
```



Rollover manuale del server PKI

Il server PKI IOS supporta il rollover manuale del certificato CA, ovvero un amministratore può attivare in anticipo la generazione di un certificato CA di rollover senza dover configurare il **rollover automatico** nella configurazione del server PKI. Si consiglia di configurare il **rollover automatico** per stabilire se si intende estendere la durata di un server CA distribuito inizialmente in modo da renderlo più sicuro. **I client PKI possono eseguire l'overload della CA senza un certificato CA di rollover**. *Fare riferimento alla* dipendenza dell'operazione SHADOW del client dal rollover del server PKI.

Èpossibile attivare un rollover manuale utilizzando il comando configuration level:

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

Inoltre, è possibile annullare un certificato CA di rollover per generarne uno nuovo manualmente, ma ciò non deve essere fatto da un amministratore in un ambiente di produzione, utilizzando:

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

In questo modo vengono eliminati la coppia di chiavi rsa di rollover e il certificato CA di rollover. Si sconsiglia di procedere in quanto:

- Dopo che l'autorità di certificazione ha generato il certificato di rollover, più client possono scaricare il certificato dell'autorità di certificazione di rollover e un certificato del client di rollover firmato dal certificato dell'autorità di certificazione di rollover.
- In questa fase, se il rollover viene annullato, potrebbe essere necessario registrare nuovamente il client.

Rinnovo automatico client PKI

Tipi di rinnovo dei certificati client - RINNOVO e SHADOW

IOS nel server PKI verifica sempre che la scadenza del certificato di ID rilasciato al client non superi mai la scadenza del certificato CA.

In un client PKI, IOS prende sempre in considerazione i seguenti timer prima di pianificare l'operazione di rinnovo:

- Ora di scadenza del certificato di identità da rinnovare
- Scadenza del certificato dell'emittente (CA)

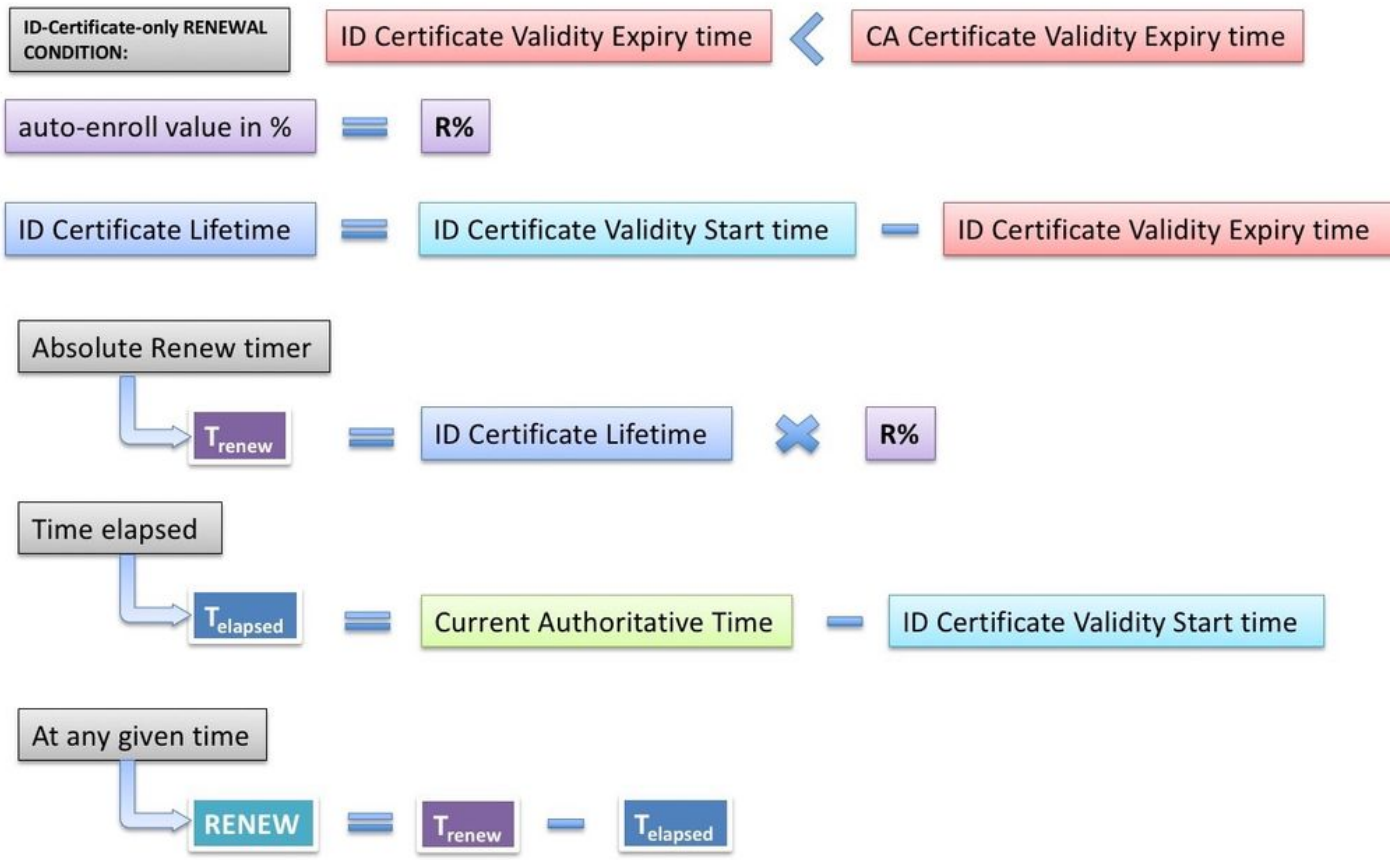
Se l'ora di scadenza del certificato di identità è diversa da quella del certificato CA, IOS esegue una semplice operazione di rinnovo.

Se l'ora di scadenza del certificato di identità è uguale a quella del certificato CA, IOS esegue un'operazione di rinnovo shadow.

RINNOVO - Rinnovo certificato di identità router

Come accennato in precedenza, il client PKI IOS esegue una semplice operazione di rinnovo se la scadenza del certificato di identità non corrisponde alla scadenza del certificato CA, in altre parole il certificato di identità che scade prima che il certificato dell'emittente attivi un semplice rinnovo del certificato di identità.

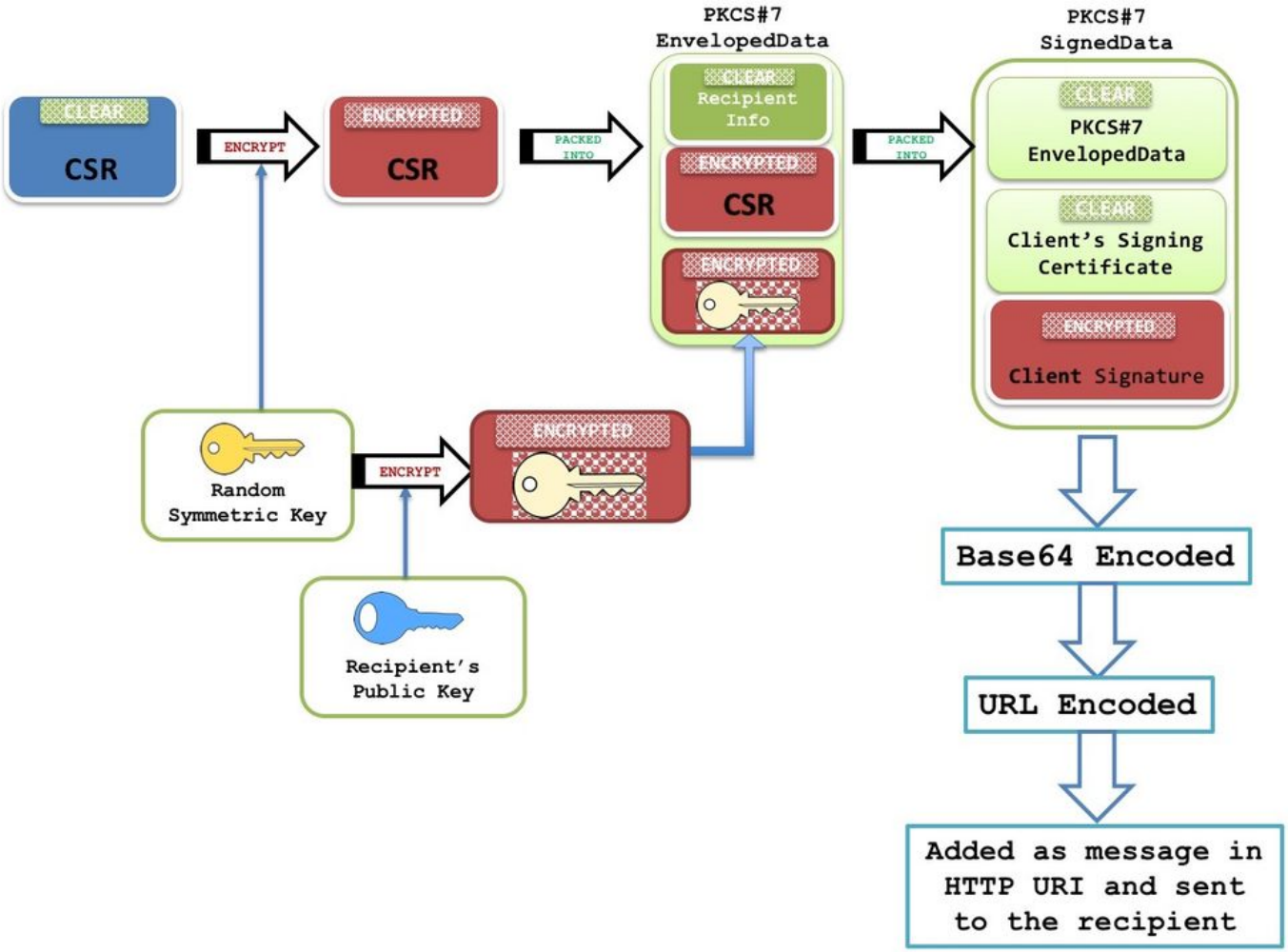
Non appena viene installato un certificato di identità, IOS calcola il timer di rinnovo per il trust-point specifico come mostrato di seguito:



Current-Authoritative-Time indica che l'orologio di sistema deve essere una fonte di tempo autorevole, come descritto di seguito. (collegamento alla sezione dell'origine ora autorevole) I timer PKI non verranno inizializzati senza un'origine ora autorevole. Di conseguenza, le operazioni di rinnovo non avranno luogo.

Alla scadenza del timer di rinnovo si verificano gli eventi seguenti:

- IOS genera una coppia di chiavi shadow se è configurata la **rigenerazione** [esempio: auto-enroll [80 regenerate]. Senza la **rigenerazione**, IOS riutilizza la coppia di chiavi RSA attualmente attiva.
- IOS crea una richiesta di certificato in formato PKCS-10, che viene quindi crittografata in una busta PKCS-7. Questa busta contiene anche RecipientInfo, che è il nome del soggetto e il numero di serie della CA di emissione. Questa busta PKCS7 viene a sua volta compressa in un file PKCS-7 con firma digitale. Durante la registrazione iniziale, IOS utilizza un certificato autofirmato per firmare il messaggio. E durante le iscrizioni successive, ossia le iscrizioni successive, IOS usa il certificato di identità attivo per firmare il messaggio. I dati firmati PKCS7 vengono inoltre incorporati nel certificato di firma, ovvero il certificato autofirmato o il certificato di identità.



Per ulteriori informazioni su questa struttura di pacchetti, consultare il documento di panoramica di SCEP

> **Nota:** Le informazioni chiave sono RecipientInfo, che è il nome del soggetto e il numero di serie della CA di emissione. La chiave pubblica di questa CA viene utilizzata per crittografare la chiave simmetrica. Il CSR nella busta PKCS7 viene crittografato utilizzando questa chiave simmetrica.

Questa chiave simmetrica crittografata viene decrittografata dalla CA ricevente utilizzando la relativa chiave privata e viene utilizzata per decrittografare la busta PKCS7 che rivela la CSR.

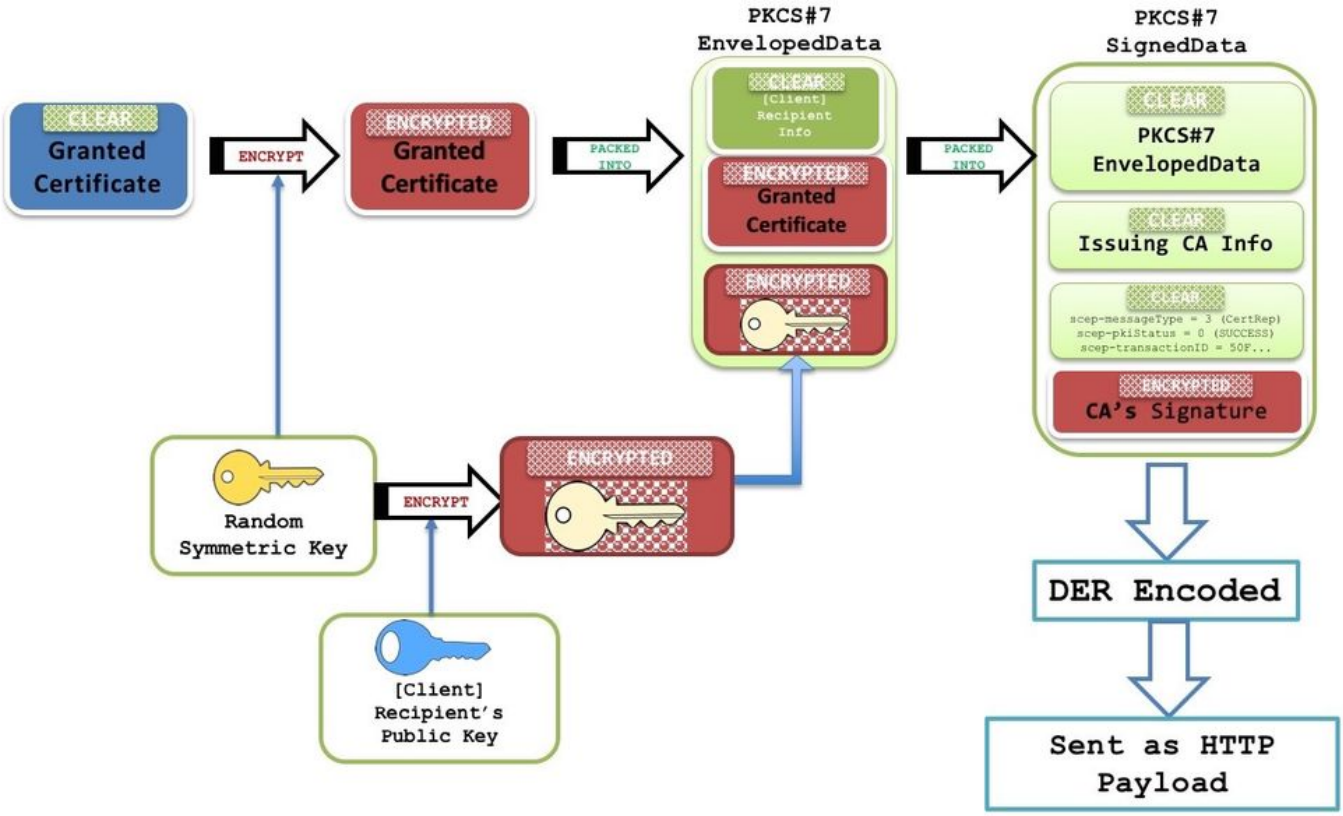
- Questo pacchetto di richiesta di firma del certificato (CSR) in formato PKCS7 viene quindi inviato alla CA con un messaggio SCEP di tipo PKCSReq e un'operazione SCEP denominata PKIOperation.
- Se la CA rifiuta la richiesta, IOS arresta il timer di rinnovo. Da questo punto in poi, per rinnovare il certificato di identità, l'amministratore deve eseguire un rinnovo manuale (collegamento alla sezione **Rinnovo manuale client PKI**)
- Se la CA invia uno stato SCEP come **in sospeso**, IOS sul client PKI avvia un timer POLL a partire da 60 secondi o 1 minuto. Ogni volta che scade un timer POLL, IOS invia un messaggio SCEP GetCertInitial tramite un'operazione PKIOperation.Quando scade il primo timer POLL, se al messaggio GetCertInitial viene risposto con uno stato SCEP Pending, un algoritmo di backoff esponenziale imposta il primo intervallo di tentativi del timer POLL su 1 minuto, il secondo intervallo di tentativi del timer POLL su 2 minuti, il terzo intervallo di

tentativi del timer POLL su 4 minuti e così via per i successivi 999 tentativi per impostazione predefinita o fino alla scadenza del certificato CA emittente.
Èpossibile configurare il conteggio del polling e il primo periodo di tentativi utilizzando:

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

- Quando il certificato viene concesso sul server PKI, al successivo messaggio SCEP GetCertInitial viene risposto con un messaggio HTTP di tipo di contenuto **applicazione/x-pki-messaggio** e un corpo contenente dati firmati PKCS#7. Questi dati firmati PKCS7 contengono lo stato SCEP **Concesso** e anche un dato in busta PKCS7. I dati della busta PKCS contengono il certificato concesso e RecipientInfo, ovvero il nome del soggetto e il numero di serie del certificato autofirmato durante la registrazione iniziale e del certificato di identità attivo durante le nuove registrazioni.

  I dati in busta PKCS7 contengono inoltre una chiave simmetrica crittografata con la chiave pubblica del destinatario, per la quale è stato concesso il nuovo certificato. Il router ricevente lo decrittografa utilizzando la chiave privata. Questa chiave simmetrica non crittografata viene quindi utilizzata per decrittografare i dati della busta PKCS#7, rivelando il nuovo certificato di identità.



- In questa fase, IOS sostituisce immediatamente il certificato di identità esistente con il nuovo certificato. E se è stata configurata la **rigenerazione**, la coppia di chiavi shadow sostituisce anche la coppia di chiavi attiva.

- Inoltre, la data di fine del nuovo certificato viene confrontata con la data di fine del certificato CA per determinare se il timer di rinnovo deve essere inizializzato o se un timer SHADOW deve essere inizializzato come spiegato di seguito <href **Types of Client Certificate Renewal -**

RENEW and SHADOW>