Guía de despliegue IOS PKI: Renovación del certificado - Configuración y Información general de funcionamiento

Contenido

Introducción

Este documento describe la renovación del certificado en los servidores y los clientes del Public Key Infrastructure (PKI) del Cisco IOS detalladamente.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

Hardware

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

Software

- IOS
  - Para ISR-G1 – El último 15.1(4)M*
  - Para ISR-G2 – 15.4(3)M más finales de
- IOS-XE
  - XE 3.15 o 15.5(2)S

Nota: El mantenimiento de software general para los dispositivos ISR es no más activo, cualesquiera arreglos de bug o mejora de las características futuros requerirían una actualización de hardware a los routeres de la serie ISR-2 o del ISR-4xxx.

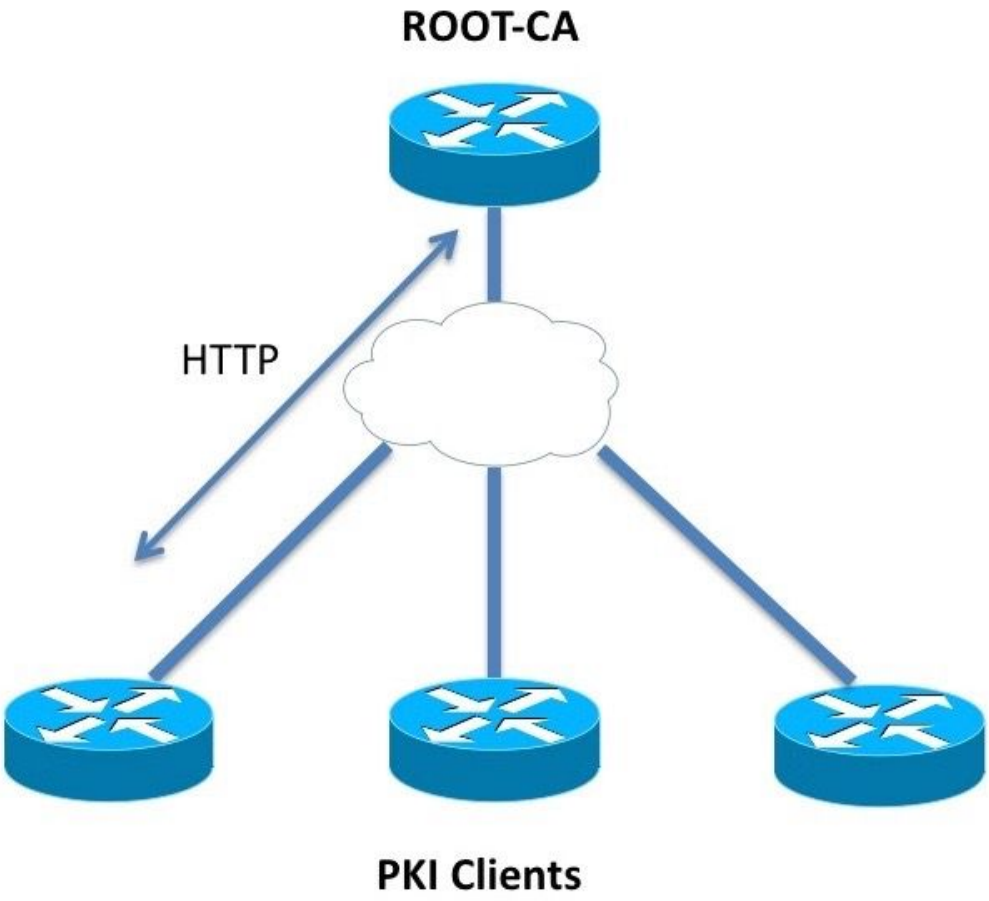
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La renovación del certificado también conocida como operación de la renovación se asegura de que cuando expira un certificado, un nuevo certificado está listo para asumir el control. Desde el punto de vista de un servidor pki, esta operación implica el generar del nuevo receptor de papel del certificado de la renovación del servidor por adelantado para aseegurarse que todos los clientes PKI han recibido un nuevo certificado de la renovación del cliente firmado por el nuevo certificado de la renovación del servidor antes de que expire el certificado actual. Desde el punto

de vista de un cliente PKI, si está expirando el certificado del cliente pero no es el certificado de servidor del Certificate Authority (CA), los pedidos de cliente un nuevo certificado y substituyen el certificado viejo tan pronto como se reciba el nuevo certificado, y si el certificado del cliente está expirando al mismo tiempo que el certificado de servidor de CA, el cliente se aseegura recibir el certificado de la renovación del servidor de CA primero, y entonces petición un certificado de la renovación firmado por el nuevo certificado de la renovación del servidor de CA, y ambos serán activados cuando expiran los Certificados viejos.

Configuración



PKI y requisito previó simple del Enrollment Protocol de Ceritificate (SCEP)

Fuente de tiempo válida

En el IOS, por abandono la fuente de reloj se considera ser NON-autoritaria puesto que el reloj de hardware no es la mejor fuente de tiempo. PKI que es sensible al tiempo, es importante configurar una fuente válida de tiempo usando el NTP. En un despliegue PKI, se recomienda para hacer que todos los clientes y el servidor sincronicen su reloj a un solo servidor NTP, a través de los

servidores NTP múltiples si procede. Más en esto se explica en el Guía de despliegue IOS PKI: Diseño inicial y despliegue

El IOS no inicializa los temporizadores PKI sin un reloj autoritario. Aunque el NTP se recomiende altamente, como medida temporal, el administrador pueda marcar el reloj de hardware como usar autoritario:

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

Comunicación HTTP

Un requisito para un servidor pki activo IOS es el servidor HTTP, que puede ser habilitado usando este comando del config-nivel:

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

Este comando habilita al servidor HTTP en el puerto 80 por abandono, que se puede cambiar como se muestra arriba.

Los clientes PKI deben poder comunicar con el servidor pki sobre el HTTP al puerto configurado.

Configuración PKI

Servidor - Renovación

La configuración automática de la renovación del servidor pki parece:

```
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
```

El parámetro de la auto-renovación se define en los días. En un nivel más granular, el comando parece:

```
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
```

Un valor de la auto-renovación de 90 indica que el IOS crea un certificado de servidor de la renovación 90 días antes del vencimiento del certificado de servidor actual, y la validez de este nuevo certificado de la renovación comienza al mismo tiempo que la época del vencimiento del certificado activo actual.

la Auto-renovación se debe configurar con tal valor que se aseegure ese el certificado de CA de la renovación se genere en el receptor de papel del servidor pki por adelantado antes de que

cualquier cliente PKI en la red realice la operación de GetNextCACert según lo descrito en la sección de **Información general de funcionamiento de la SOMBRA** abajo.

Cliente - Renovación

La configuración automática de la renovación del certificado del cliente PKI parece:

```
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
```

Aquí, auto-**aliste a los** commandes sates del **[regenerate] del <percentage>** que el IOS debe realizar la renovación del certificado en el exactamente 80% del curso de la vida del certificado actual.

Los estados del **regenerado de la** palabra clave que el IOS debe regenerar el par clave RSA conocido como par clave de la sombra durante cada operación de la renovación del certificado.

El cuidado debe ser tomado mientras que configura auto-aliste el porcentaje. En cualquier cliente dado PKI en el despliegue, si se presenta una condición donde el certificado de identidad expira al mismo tiempo que el certificado de CA de publicación, después el valor del auto-alistar debe accionar siempre la operación de la renovación del [shadow] después de que CA haya creado el certificado de la renovación. *Refiera a la* sección de las **dependencias del temporizador PKI** conforme a los ejemplos de despliegue.

Requisitos previos de la renovación/de la renovación PKI

Este documento dirige las operaciones de la renovación y de la renovación del certificado detalladamente, y por lo tanto estos eventos se consideran ser completados con éxito:

- Inicialización del servidor pki con un certificado de CA válido.
- Han alistado a los clientes PKI con éxito con el servidor pki. es decir. Cada cliente PKI tiene el certificado de CA y un certificado del router del certificado de identidad aka.

Alistar a un cliente implica estos eventos. Sin conseguir demasiado en el detalle:

- Autenticación del trustpoint
- Inscripción del trustpoint

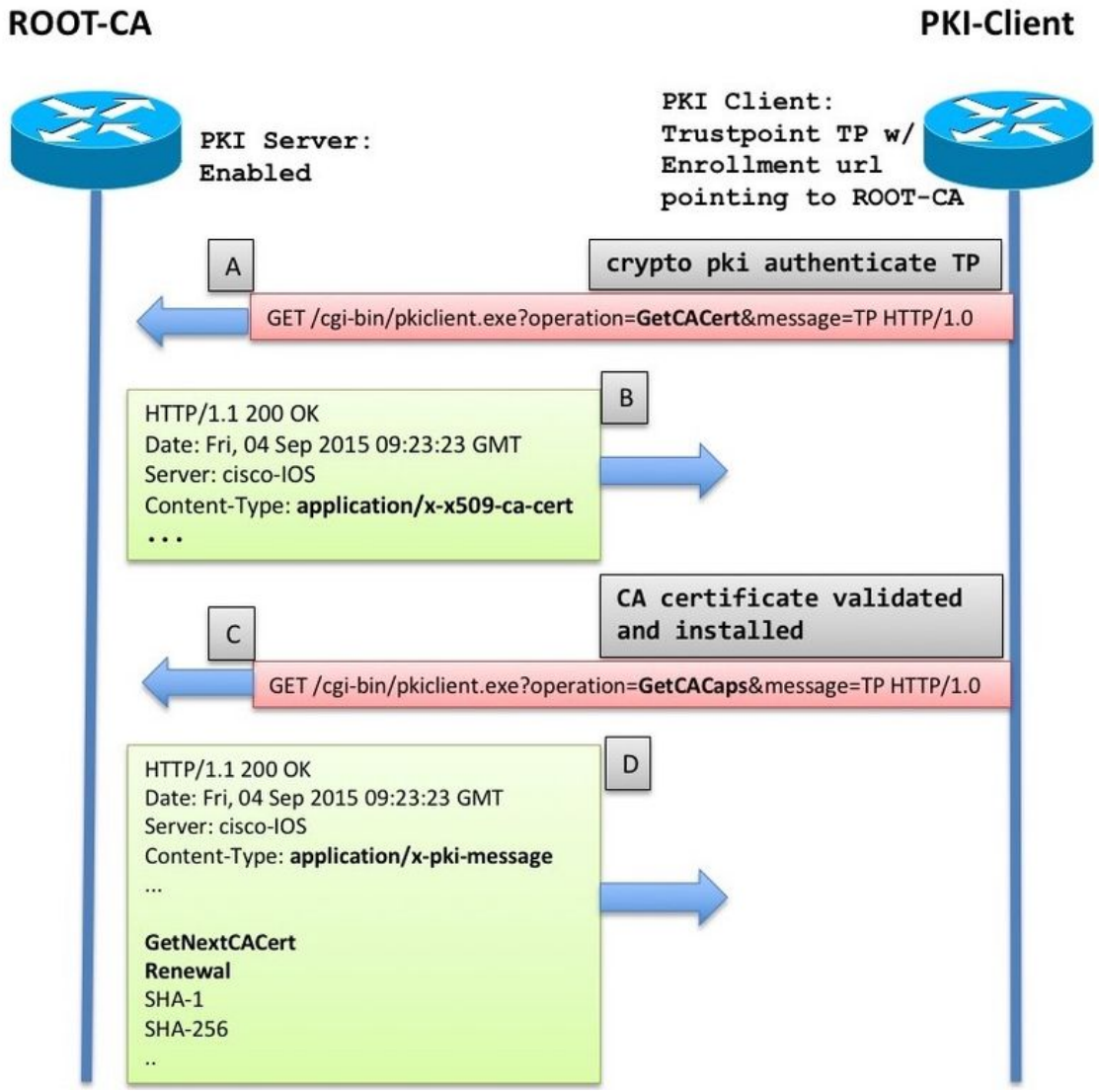
En el IOS, un trustpoint es un envase para los Certificados. Cualquier trustpoint dado puede contener un certificado de identidad activo y/o un certificado de CA del active. Un trustpoint se considera autenticado si contiene un ceryificate activo de CA. Y se considera alistado si contiene un certificado de identidad. Un trustpoint se debe autenticar antes de una inscripción. Cubren al servidor pki y la configuración del cliente, junto con la autenticación del trustpoint y la inscripción detalladamente en el Guía de despliegue IOS PKI: Diseño inicial y despliegue

Después de la extracción/de la instalación del certificado de CA, el cliente PKI extrae las capacidades del servidor pki antes de realizar una inscripción. La extracción de las capacidades de CA se explica en esta sección.

Capacidades de CA

En el IOS, cuando un cliente PKI autentica CA, es decir cuando un administrador crea un trustpoint en un router IOS, y ejecuta el comando crypto que el **pki autentica el <trustpoint-name>**, estos eventos ocurren en el router:

- El IOS envía una petición SCEP que contiene el tipo de operación de GetCACert.
- La respuesta esperada aquí es un mensaje HTTP con un tipo de contenido de **application/x-x509-ca-cert** en caso de un despliegue de CA, o **application/x-x509-ca-ra-cert** en caso de un RA y de un despliegue de CA. Y el cuerpo HTTP contiene el certificado de CA. [and an RA certificate in the latter case].
- Después de la recuperación de certificados y de la instalación CA/RA, el cliente inicia una petición automática SCEP que contiene la operación de GetCACaps.
- La respuesta esperada aquí es un mensaje HTTP con un tipo de contenido de **application/x-pki-message**, que podría también ser **texto/llano** y el cuerpo HTTP contiene una serie de capacidades soportadas por CA, separado por un carácter del avance de línea. Una respuesta típica del servidor pki IOS está tal y como se muestra en del diagrama a continuación.



La respuesta es interpretada como esto por el cliente IOS PKI:

```
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
```

De estas capacidades, este documento se centra en estos dos.

GetNextCACert

Cuando esta capacidad es vuelta por CA, el IOS entiende que CA soporta la renovación del certificado de CA. Con esta capacidad vuelta, si no configuran al **comando auto-enroll** bajo el trustpoint, el IOS inicializa un temporizador de la SOMBRA fijado hasta el 90% del período de validez del certificado de CA.

Cuando expira el temporizador de la SOMBRA, el IOS realiza la operación de GetNextCACert SCEP para traer el certificado de CA de la renovación.

> Nota: Si han configurado al **comando auto-enroll** bajo el trustpoint junto con un **URL de la inscripción**, un temporizador de la RENOVACIÓN se inicializa incluso antes de autenticar el trustpoint, e intenta constantemente alistar con CA situado en el **URL de la inscripción**, aunque no se envíe ningún [CSR] real del mensaje de la inscripción hasta que se autentique el trustpoint.

> Nota: GetNextCACert es enviado como capacidad por el servidor pki IOS incluso si la auto-**renovación** no se configura en el servicio

Renovación

Con esta capacidad, el servidor pki informa al cliente PKI que puede utilizar un certificado activo ID para firmar un pedido de firma de certificado de renovar el certificado existente.

Más en esto en la sección de la Auto-**renovación del cliente PKI**.

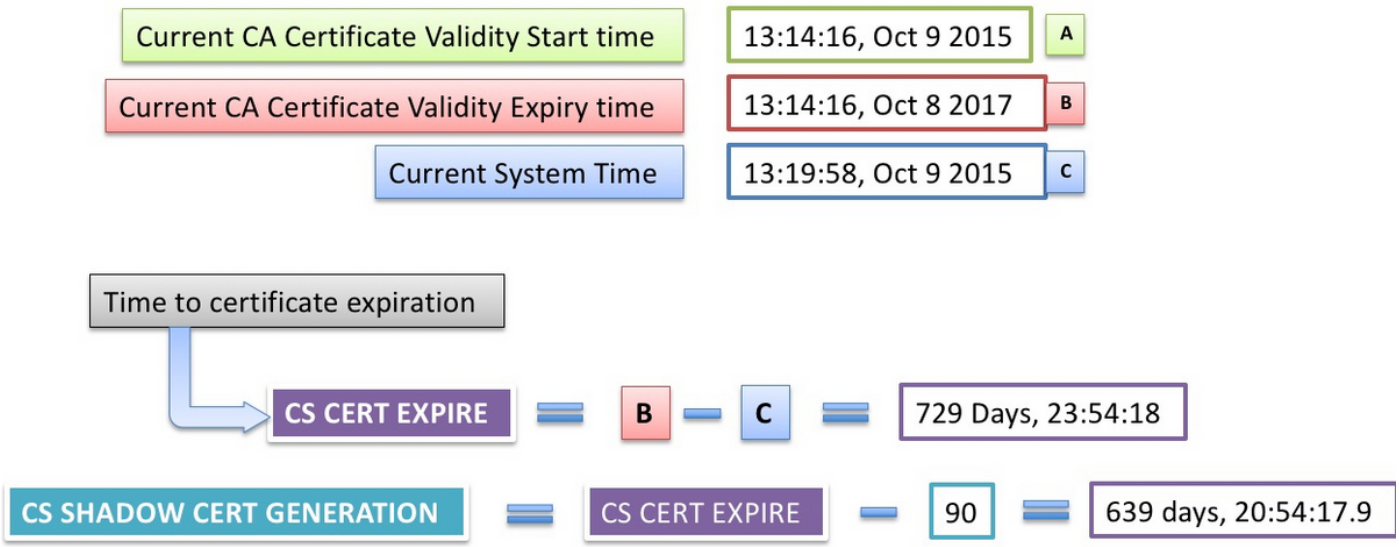
Auto-renovación del servidor pki

Con la configuración antedicha en el servidor de CA, usted ve:

```
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
```

Note esto:



Operación de la renovación

Cuando expira el temporizador de la **GENERACIÓN de la SOMBRA CERT CS**:

- El IOS genera un par clave de la renovación primero – tiene actualmente el mismo nombre que el par clave activo con a # hash añadido al final del fichero a él.

```
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
```

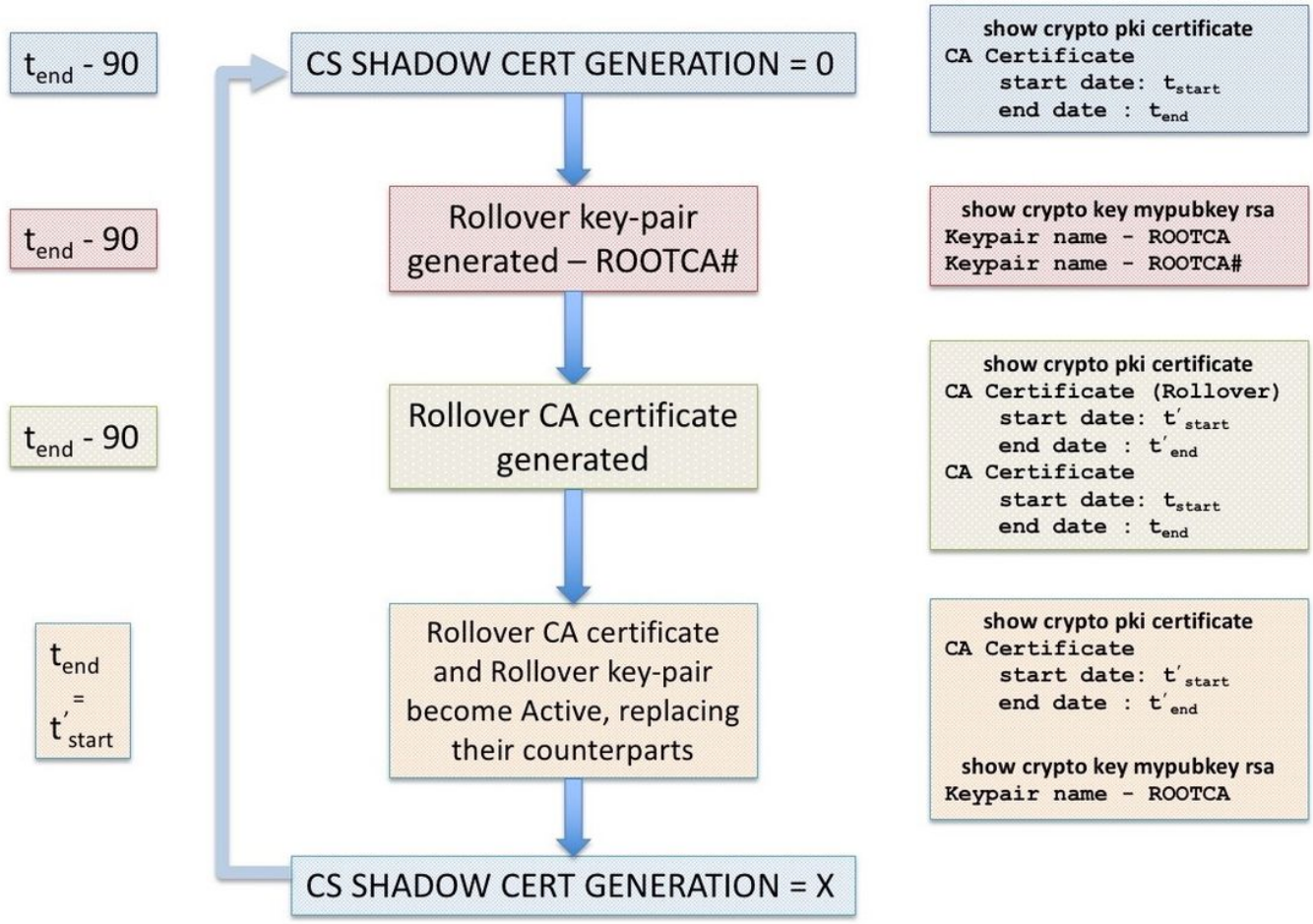
- El IOS entonces genera el certificado de CA de la renovación, donde está lo mismo la Fecha de inicio de la validez que la fecha de finalización de la validez del certificado de CA activo actual.

```
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
```



Manual-renovación del servidor pki

El servidor pki IOS soporta la renovación manual del certificado de CA, es decir un administrador

puede accionar la generación de un certificado de CA de la renovación por adelantado sin la necesidad configurar la auto-renovación **bajo** configuración de servidor pki. Se recomienda altamente para configurar la auto-renovación **independientemente de si** una planea prolongar el curso de la vida de un servidor inicialmente desplegado de CA para estar en el lado más seguro. PKICLIENTS **puede sobrecargar CA sin un certificado de CA de la renovación.** Refiera a la operación de la SOMBRA del cliente de Dependencyof en la renovación del servidor pki.

Una renovación manual se puede accionar usando el comando del nivel de la configuración:

```
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
```

Y también, un certificado de CA de la renovación se puede cancelar para generar fresco manualmente, no obstante algo un admin no debe hacer en un entorno de producción, el usar:

```
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
```

Esto borra el par clave rsa de la renovación y el certificado de CA de la renovación. Esto se aconseja contra porque:

- Una vez que CA genera el certificado de la renovación, los clientes múltiples pueden descargar el certificado de CA de la renovación así como un certificado del cliente de la renovación firmados por el certificado de CA de la renovación.
- En esta etapa si la renovación está cancelada, el cliente puede tener que re-ser alistado.

Auto-renovación del cliente PKI

Teclea de la renovación del certificado del cliente - RENUEVE y SOMBREE

El IOS en el servidor pki se aseegura siempre que la época del vencimiento del certificado ID publicado al cliente nunca va más allá de la época del vencimiento del certificado de CA.

En un cliente PKI, el IOS toma siempre los temporizadores siguientes en la consideración antes de programar la operación de la renovación:

- Tiempo del vencimiento del certificado de identidad que es renovado
- Tiempo del vencimiento del certificado del emisor (CA)

Si la época del vencimiento del certificado de identidad no es lo mismo que la época del

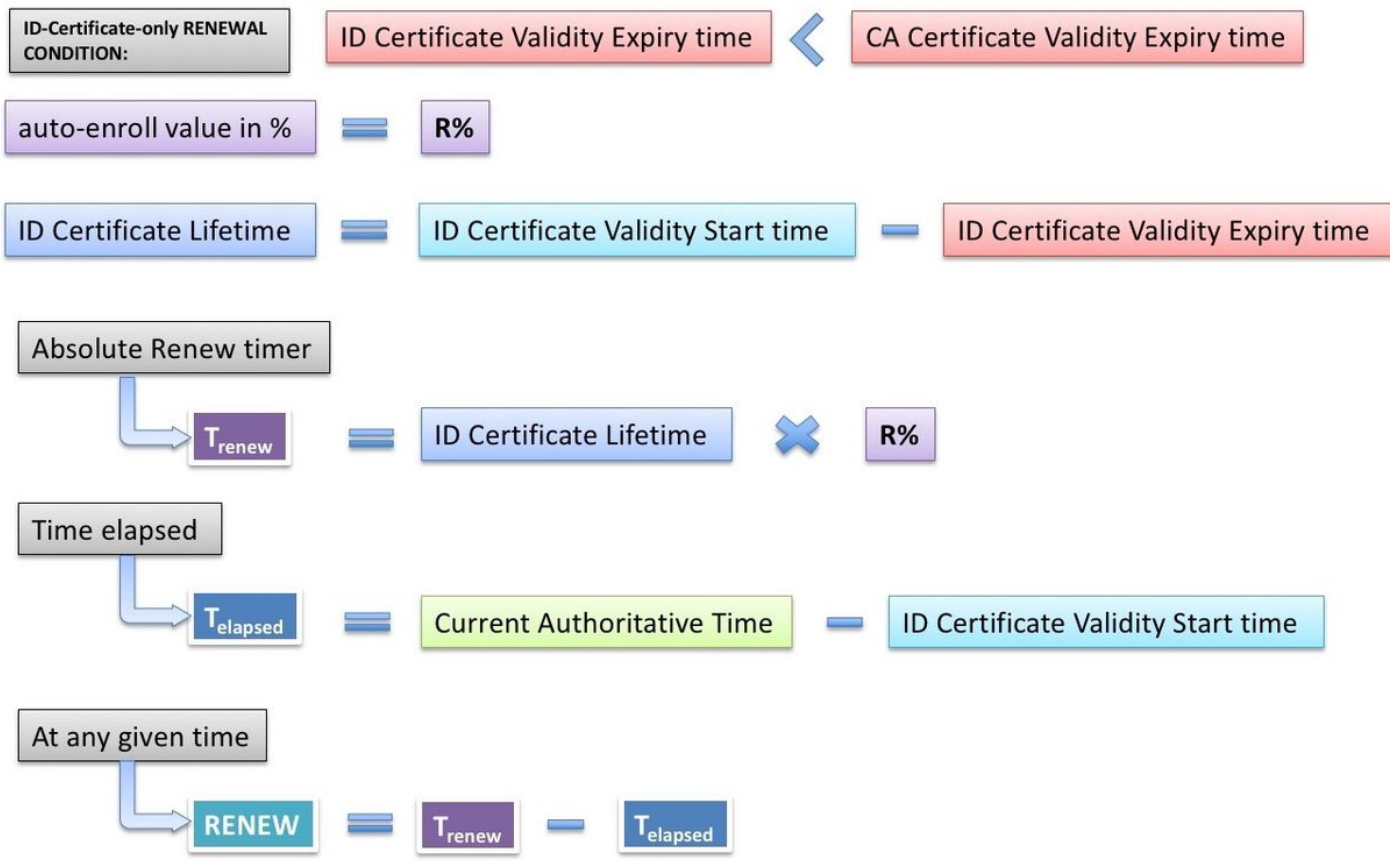
vencimiento del certificado de CA, el IOS realiza una operación simple de la renovación.

Si la época del vencimiento del certificado de identidad es lo mismo que la época del vencimiento del certificado de CA, el IOS realiza una operación de la renovación de la sombra.

RENUEVE - Renovación del certificado de identidad del router

Como se mencionó antes, el cliente IOS PKI realiza una operación simple de la renovación si la época del vencimiento del certificado de identidad no es lo mismo que la época del vencimiento del certificado de CA, es decir el certificado de identidad que expira antes del certificado del emisor acciona una renovación simple del certificado de identidad.

Tan pronto como un certificado de identidad esté instalado, el IOS calcula el temporizador de la RENOVACIÓN para la confianza-punta específica como se muestra abajo:

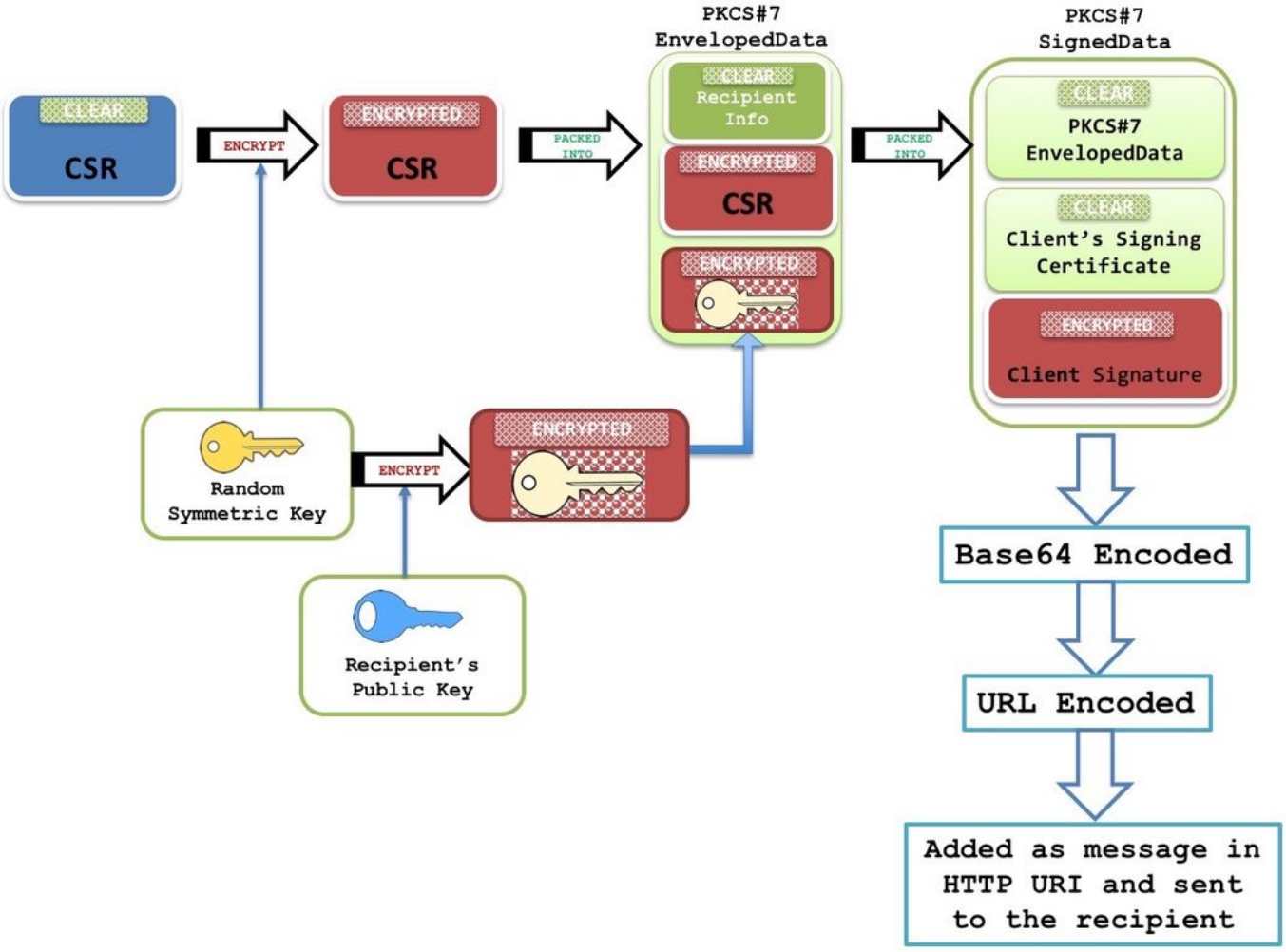


El Actual-Autoritario-tiempo significa que el reloj del sistema tiene que ser una fuente autoritaria de tiempo según lo descrito aquí. (link a la sección de la fuente de tiempo válida) los temporizadores PKI no serán inicializados sin una fuente autoritaria de tiempo. Y por consiguiente, la operación de la renovación no ocurrirá.

Los eventos siguientes ocurren cuando RENUEVE el temporizador expira:

- El IOS genera un par clave de la sombra si se configura el **regenerado** [ejemplo: auto-aliste el regenerado 80]. Sin el IOS **regenerado** reutiliza actualmente - el par clave activo RSA.
- El IOS crea un pedido de certificado formatado PKCS-10, que entonces se cifra en un sobre PKCS-7. Este sobre también contiene el RecipientInfo, que es el tema-nombre y el número de serie de CA de publicación. Este PKCS7-envelope a su vez pila de discos en un PKCS-7 firmar-DATA. Durante la inscripción inicial, el IOS utiliza un certificado autofirmado para firmar

este mensaje. Y durante las inscripciones subsiguientes, es decir las reinscripciones, IOS utilizan el certificado de identidad activo para firmar el mensaje. Los datos firmados PKCS7 también se integran con el certificado de firma, es decir el certificado autofirmado o el certificado de identidad.



Para más información sobre esta estructura de paquete refiera al documento de descripción general SCEP

Nota: La información fundamental aquí es el RecipientInfo que es el tema-nombre y el número de serie de CA de publicación, y la clave pública de este CA se utiliza para cifrar la clave simétrica. El CSR en el sobre PKCS7 se cifra usando esta clave simétrica.

Esta clave simétrica cifrada es desencriptada por CA de recepción usando su clave privada, y esta clave simétrica se utiliza para desencriptar el sobre PKCS7 que revela el CSR.

- Este pedido de firma de certificado (CSR) embalado en el formato PKCS7 entonces se envía a CA con un Tipo de mensaje SCEP de PKCSReq y una operación SCEP llamada PKIOperation.
- Si CA rechaza la petición, el IOS para el temporizador de la RENOVACIÓN. Desde aquí, renovar el certificado de identidad, el administrador debe realizar un renewal manual (el link a la sección de la Manual-**renovación del cliente PKI**)
- Si CA envía un estado SCEP como **pendiente**, el IOS en el cliente PKI comienza un temporizador de la ENCUESTA a comenzar en 60 segundos o 1 minuto. Un temporizador de

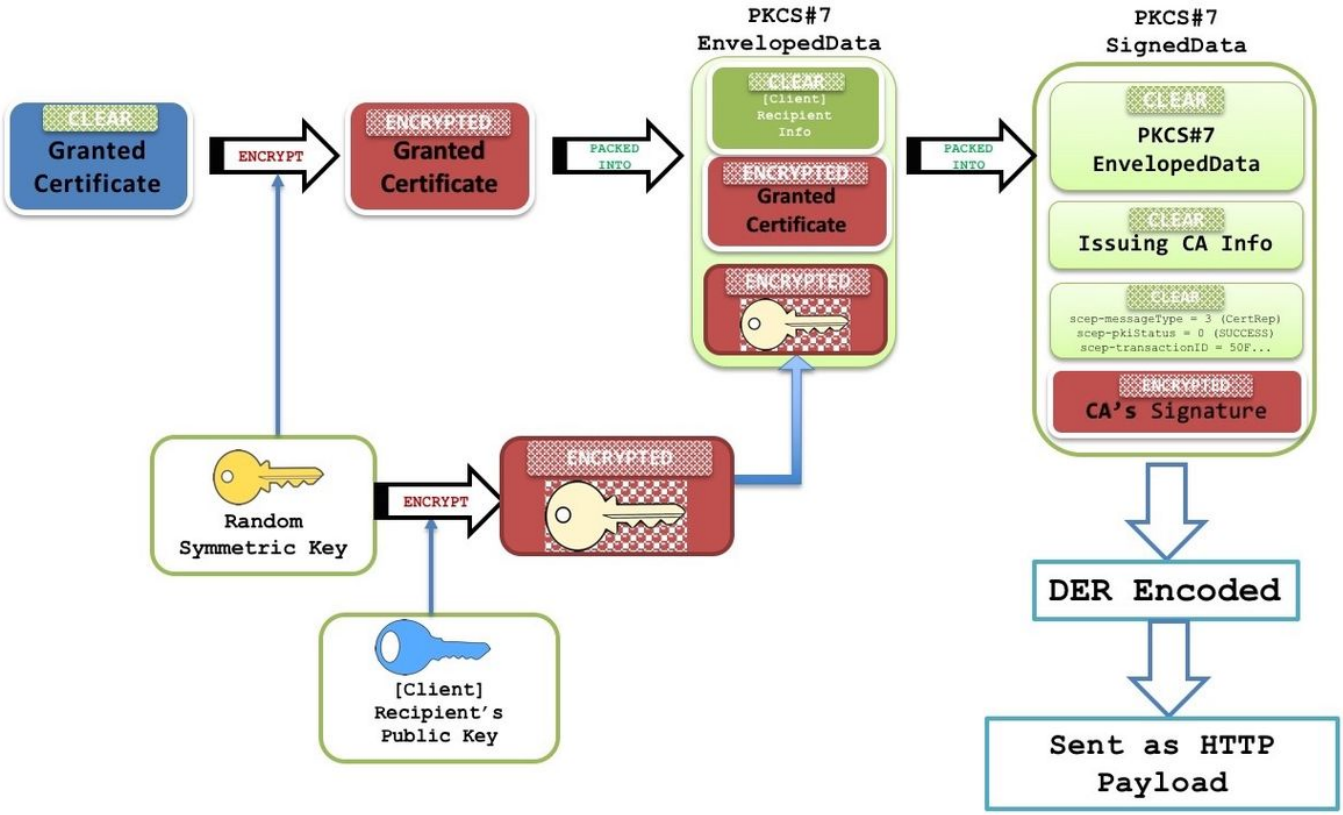
la ENCUESTA expira cada vez, IOS envía el mensaje de GetCertInitial SCEP con una operación de PKIOperation. Cuando expira el primer temporizador de la ENCUESTA, si el mensaje de GetCertInitial se responde con a un estado pendiente SCEP, un algoritmo del retroceso exponencial fija el primer intervalo entre reintentos del temporizador de la ENCUESTA a 1 minuto, segundo intervalo entre reintentos del temporizador de la ENCUESTA a 2 minutos, tercer intervalo entre reintentos del temporizador de la ENCUESTA a 4 minutos y así sucesivamente para las 999 recomprobaciones siguientes por abandono o hasta que expira el certificado de CA de publicación.
La cuenta de la encuesta y el primer período de la recomprobación se pueden configurar usando:

```
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
```

- Cuando el certificado se concede en el servidor pki, el mensaje siguiente de GetCertInitial SCEP se responde con a un mensaje HTTP del tipo de contenido **application/x-pki-message** y a un cuerpo que contiene los datos PKCS-7 firmados firmados. Estos datos firmados PKCS7 contienen el estado SCEP según lo **concedido**, y también un PKCS7 envolvió los datos. Estos datos envueltos PKCS contienen el certificado concedido y el RecipientInfo, que es el tema-

nombre y el número de serie del certificado autofirmado durante la inscripción inicial y del certificado de identidad activo durante las reinscripciones.

Los datos envueltos PKCS7 también contienen una clave simétrica cifrada con la clave pública del beneficiario (para cuál fue concedido el nuevo certificado). La recepción del router los desencripta usando la clave privada. Esta clave simétrica clara entonces se utiliza para desencriptar los datos PKCS-7 envueltos, revelando el nuevo certificado de identidad.



- En esta etapa, el IOS substituye el certificado de identidad existente por el nuevo certificado inmediatamente. Y si el **regenerado** fue configurado, el par clave de la sombra substituye el par clave activo también.

- También, la fecha de finalización del nuevo certificado se compara con la fecha de finalización del certificado de CA para determinar si RENUEVE el temporizador tiene que ser inicializado o un temporizador de la SOMBRA tiene que ser inicializado como aquí explicados **tipos del** <href de **renovación del certificado del cliente - RENUEVE y SHADOW>**