Guía de implementación de PKI de IOS: Renovación de certificados - Descripción general de la configuración y el funcionamiento

Contenido

Introducción

Este documento describe la renovación de certificados en los servidores y clientes de la infraestructura de clave pública (PKI) de Cisco IOS en detalle.

Prerequisites

Requirements

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 - Última versión 15.1(4)M*
  - Para ISR-G2 - Última versión 15.4(3)M
- IOS-XE
  - XE 3.15 o 15.5(2)S

Nota: El mantenimiento general del software para los dispositivos ISR ya no está activo, cualquier corrección de errores o mejora de funciones futuras requeriría una actualización del hardware a los routers ISR-2 o ISR-4xxx series.

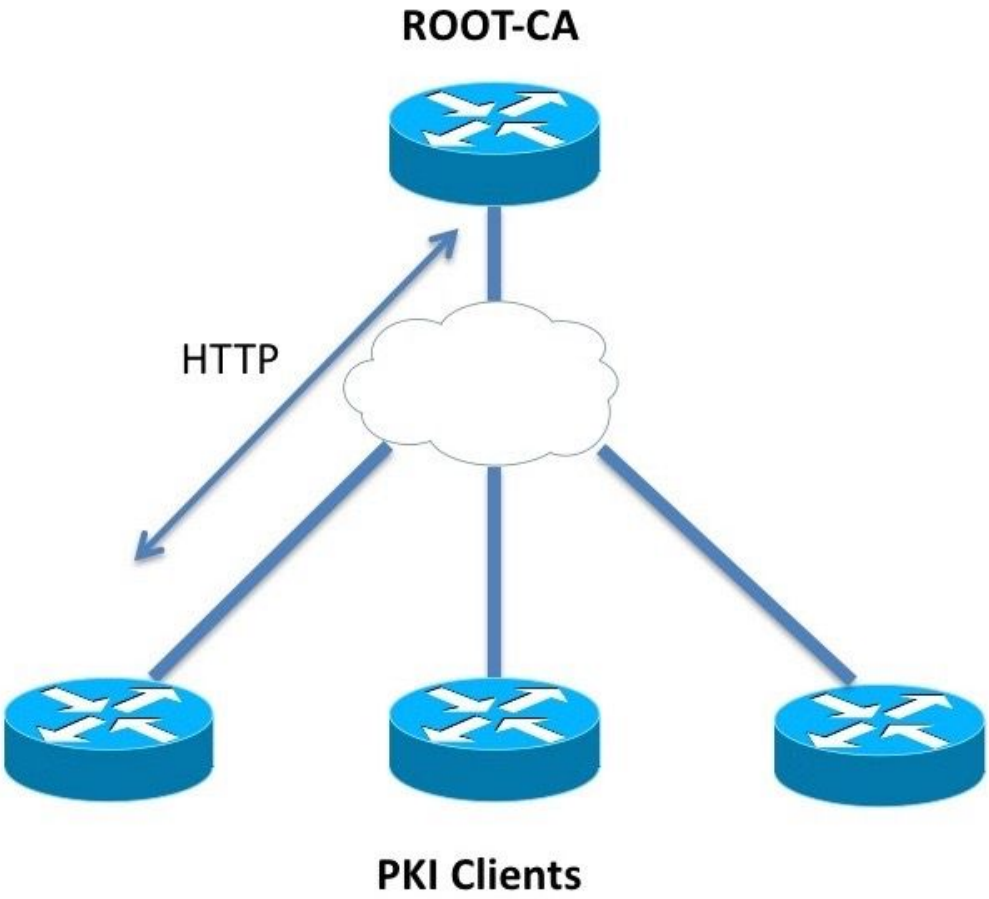
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

La renovación de certificados también conocida como operación de renovación garantiza que cuando caduque un certificado, un nuevo certificado estará listo para asumir el control. Desde el punto de vista de un servidor PKI, esta operación implica generar el nuevo certificado de renovación del servidor con mucha antelación para asegurarse de que todos los clientes PKI

hayan recibido un nuevo certificado de renovación del cliente firmado por el nuevo certificado de renovación del servidor antes de que venza el certificado actual. Desde el punto de vista de un cliente PKI, si el certificado del cliente caduca pero el certificado del servidor de la autoridad certificadora (CA) no, el cliente solicita un nuevo certificado y reemplaza el certificado antiguo tan pronto como se recibe el nuevo certificado, y si el certificado del cliente caduca al mismo tiempo que el certificado del servidor de la CA, el cliente se asegura de recibir primero el certificado de renovación del servidor de la CA y luego solicita un certificado de renovación firmado por el nuevo certificado de renovación del servidor de la CA y ambos se activarán cuando venzan los certificados antiguos.

Configuración



Requisito previo de PKI y protocolo simple de inscripción de certificados (SCEP)

Origen de tiempo autorizado

En IOS, de forma predeterminada, el origen del reloj se considera no autorizado, ya que el reloj de hardware no es la mejor fuente de tiempo. Si la PKI distingue el tiempo, es importante

configurar un origen de tiempo válido mediante NTP. En una implementación de PKI, se recomienda que todos los clientes y el servidor sincronicen su reloj con un único servidor NTP, a través de varios servidores NTP si es necesario. Se explica más sobre esto en la Guía de Implementación de PKI de IOS: Diseño e implementación iniciales

IOS no inicializa los temporizadores PKI sin un reloj autorizado. Aunque se recomienda encarecidamente NTP, como medida temporal, el administrador puede marcar el reloj de hardware como autoritativo usando:

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

Comunicación HTTP

Un requisito para un servidor PKI de IOS activo es el servidor HTTP, que se puede habilitar usando este comando config-level:

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

Este comando habilita el servidor HTTP en el puerto 80 de forma predeterminada, que se puede cambiar como se muestra arriba.

Los clientes PKI deberían poder comunicarse con el servidor PKI a través de HTTP al puerto configurado.

Configuración PKI

Servidor - Renovación

La configuración de renovación automática del servidor PKI es similar a:

```
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 renovación automática se define en días. A un nivel más granular, el comando tiene el siguiente aspecto:

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

Un valor de renovación automática de 90 indica que el IOS crea un certificado de servidor de sustitución incremental 90 días antes de la expiración del certificado de servidor actual, y la validez de este nuevo certificado de renovación comienza al mismo tiempo que la hora de vencimiento del certificado activo actual.

La renovación automática debe configurarse con tal valor que se asegure de que el certificado de CA de sustitución incremental se genere en el servidor PKI con mucha antelación antes de que

cualquier cliente PKI en la red realice la operación GetNextCACert como se describe en la sección **Descripción general de la operación SHADOW** a continuación.

Cliente - Renovación

La configuración de renovación automática de certificados del cliente PKI es similar a:

```
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, el comando **auto-enroll <porcentaje> [regenerate]** establece que el IOS debe realizar la renovación del certificado exactamente al 80% de la vida útil del certificado actual.

La palabra clave **regenerate** establece que el IOS debe regenerar el par de llaves RSA conocido como par de llaves centrales sombra durante cada operación de renovación de certificados.

Se debe tener cuidado al configurar el porcentaje de inscripción automática. En cualquier cliente PKI dado en la implementación, si surge una condición en la que el certificado de identidad caduca al mismo tiempo que el certificado CA emisor, el valor auto-enroll siempre debe activar la operación de renovación [Shadow] después de que la CA haya creado el certificado de renovación. *Consulte la* sección **Dependencias del Temporizador PKI** en los ejemplos de Implementación.

Prerrequisitos de Renovación/Renovación de PKI

Este documento aborda detalladamente las operaciones de renovación y renovación de certificados y, por lo tanto, se considera que estos eventos se han completado correctamente:

- Inicialización del servidor PKI con un certificado CA válido.
- Los clientes PKI se han registrado correctamente con el servidor PKI. Es decir, cada cliente PKI tiene el certificado de CA y un certificado de identidad denominado certificado de router.

La inscripción de un cliente implica estos eventos. Sin entrar en detalles:

- autenticación de punto de confianza
- Inscripción en Trustpoint

En IOS, un punto de confianza es un contenedor para certificados. Cualquier punto de confianza determinado puede contener un certificado de identidad activo y/o un certificado de CA activo. Un punto de confianza se considera autenticado si contiene un certificado de CA activo. Y se considera inscrito si contiene un certificado de identidad. Se debe autenticar un punto de confianza antes de una inscripción. La configuración del servidor PKI y del cliente, junto con la autenticación y la inscripción en el punto de confianza, se tratan detalladamente en la Guía de implementación de PKI de IOS: Diseño e implementación iniciales

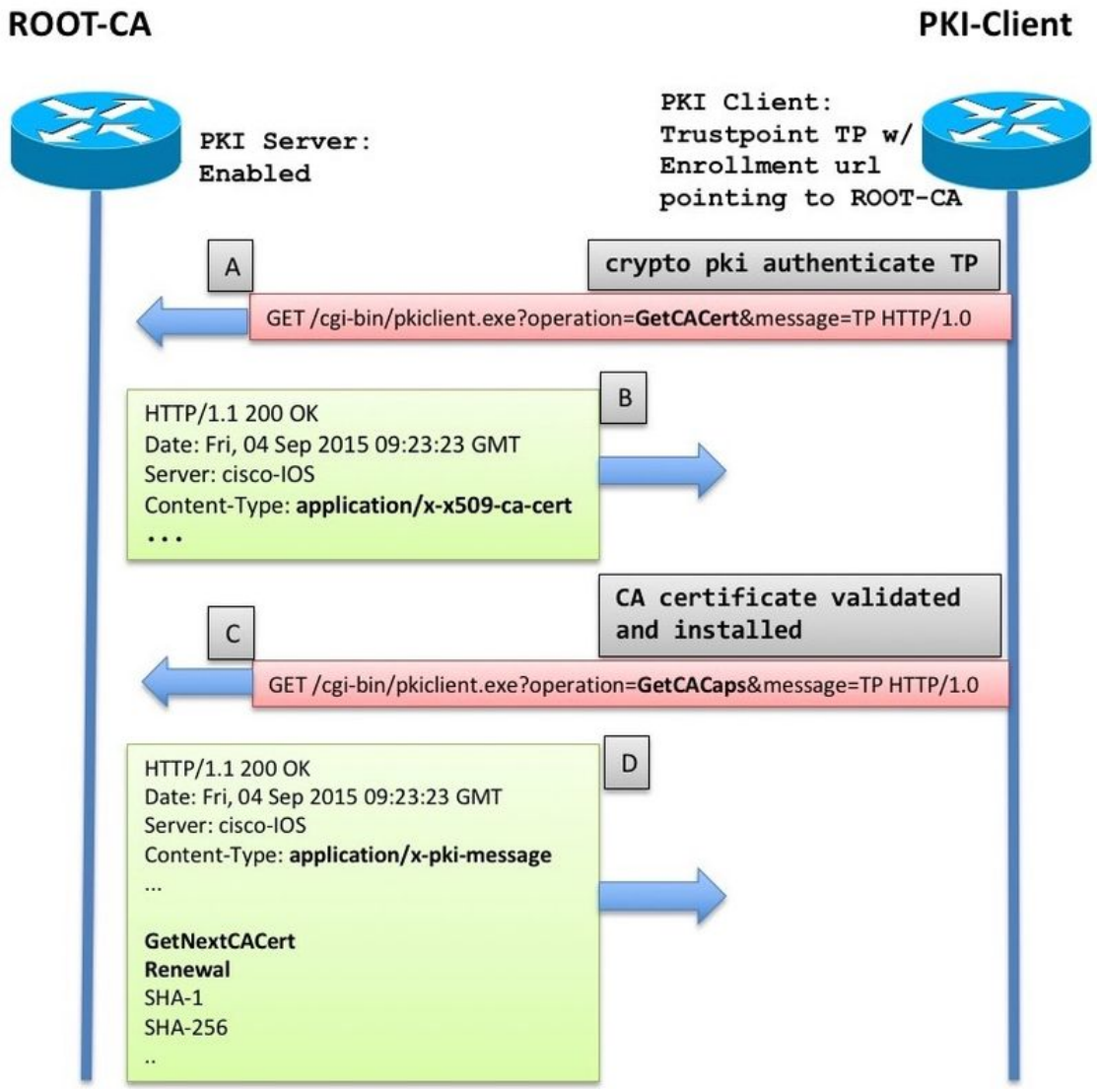
Después de la recuperación/instalación del certificado de CA, el cliente PKI recupera las capacidades del servidor PKI antes de realizar una inscripción. La recuperación de capacidades

de CA se explica en esta sección.

Capacidades de CA

En IOS, cuando un cliente PKI autentica una CA, en otras palabras, cuando un administrador crea un punto de confianza en un router IOS y ejecuta el comando **crypto pki authenticate <trustpoint-name>**, estos eventos se producen en el router:

- IOS envía una solicitud SCEP que contiene el tipo de operación GetCACert.
- La respuesta esperada aquí es un mensaje HTTP con un tipo de contenido de **application/x-x509-ca-cert** en caso de una implementación de CA, o **application/x-x509-ca-ra-cert** en caso de una implementación de RA y CA. Y el cuerpo HTTP contiene el certificado CA. [y un certificado RA en este último caso].
- Después de la recuperación e instalación del certificado CA/RA, el cliente inicia una solicitud SCEP automática que contiene la operación GetCACaps.
- La respuesta esperada aquí es un mensaje HTTP con un tipo de contenido de **aplicación/x-pki-message**, que también podría ser **text/plain** y el cuerpo HTTP contiene una serie de capacidades soportadas por la CA, separadas por un carácter de fuente de línea. Una respuesta típica del servidor PKI de IOS es como se muestra en el diagrama siguiente.



El cliente PKI del IOS interpreta la respuesta como esta:

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

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

GetNextCACert

Cuando la CA devuelve esta capacidad, el IOS entiende que la CA soporta la Renovación de Certificados de CA. Con esta capacidad devuelta, si el comando **auto-enroll** no se configura bajo el punto de confianza, IOS inicializa un temporizador SHADOW establecido en el 90% del período de validez del certificado CA.

Cuando caduca el temporizador SHADOW, IOS realiza la operación GetNextCACert SCEP para obtener el certificado Rollover CA.

> **Nota**: Si el comando **auto-enroll** se ha configurado en el punto de confianza junto con un **url de inscripción**, se inicializa un temporizador RENEW incluso antes de autenticar el punto de confianza y constantemente intenta inscribirse en la CA ubicada en el URL de inscripción, aunque no se envía ningún mensaje de inscripción real [CSR] hasta que se autentica el punto de confianza.

> **Nota:** GetNextCACert es enviado como una capacidad por el servidor IOS PKI incluso si **auto-rollover** no está configurado en el servidor

Renovación

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

Más información sobre esto en la sección **Renovación automática de cliente PKI**.

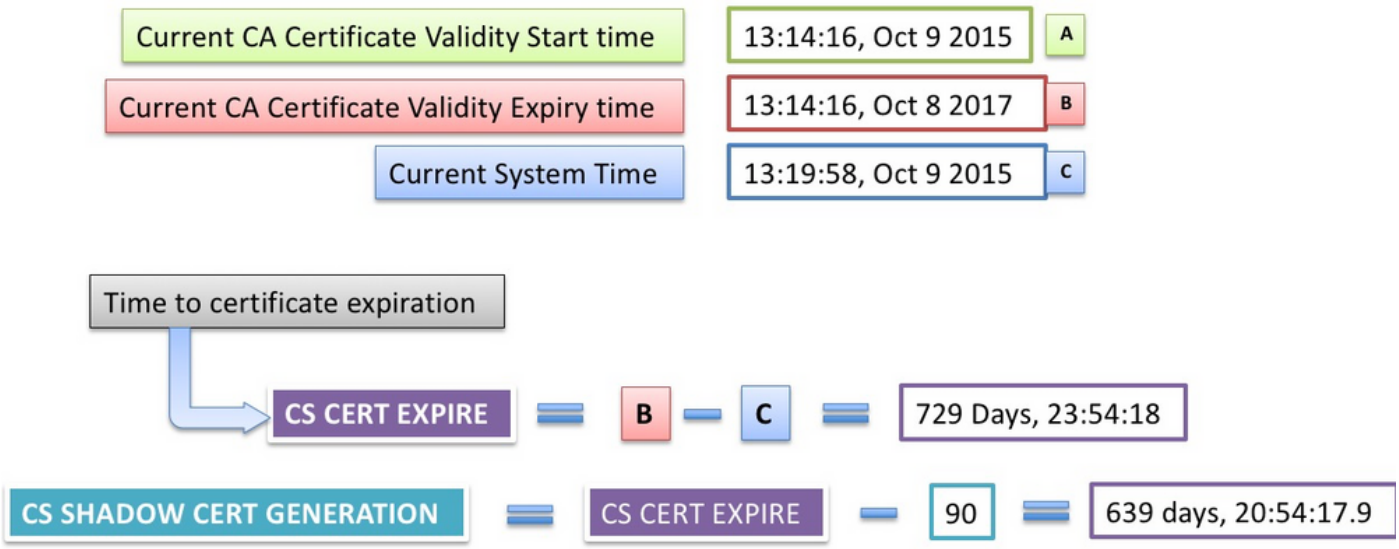
Renovación automática del servidor PKI

Con la configuración anterior en el servidor de la CA, verá:

```
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
```

Observe lo siguiente:



Operación de Renovación

Cuando caduca el temporizador **CS SHADOW CERT GENERATION**:

- IOS genera primero un par de llaves de reversión - actualmente tiene el mismo nombre que el par de llaves activo con un hash # agregado 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
```

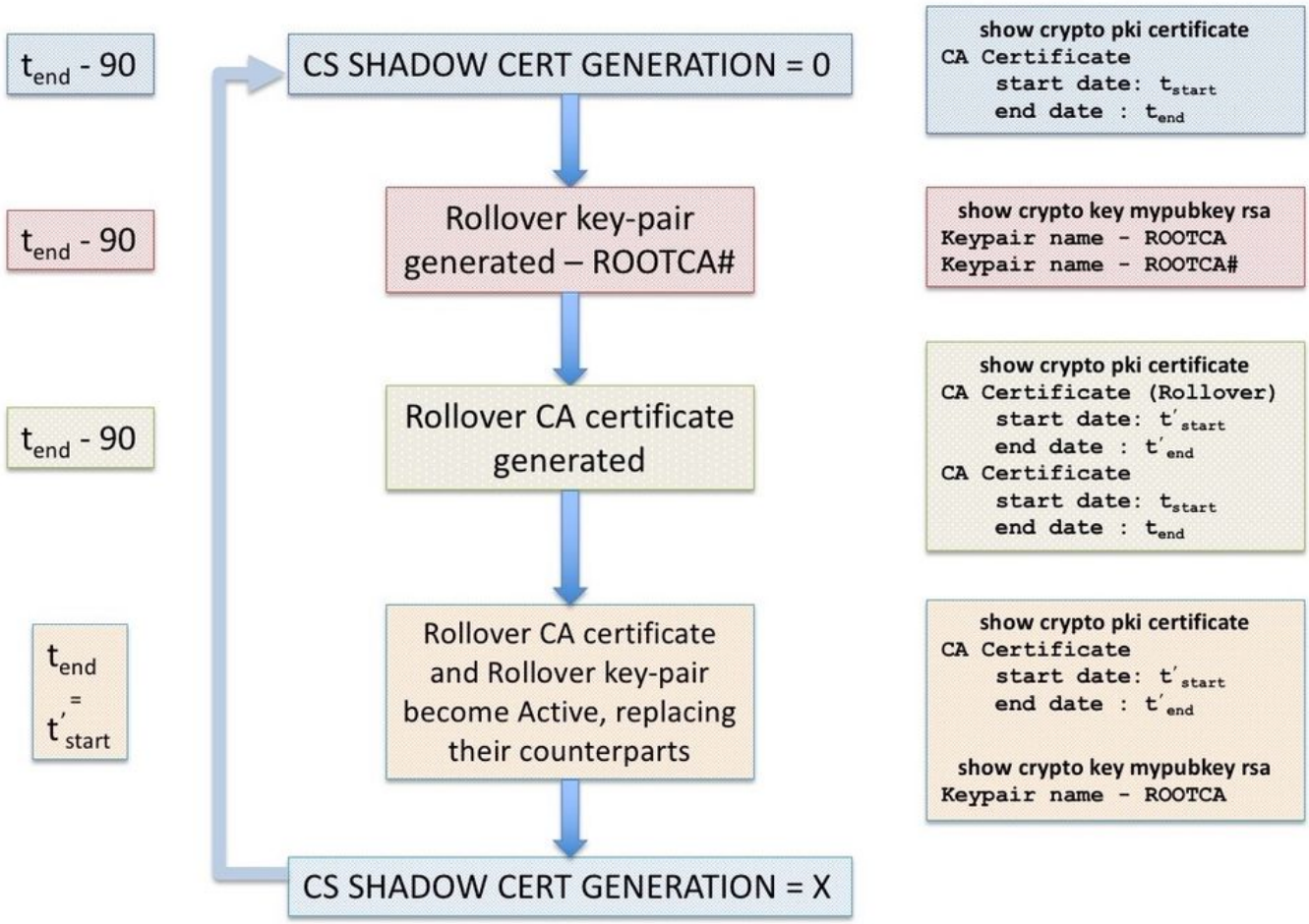
- A continuación, IOS genera el certificado de CA de renovación, donde la fecha de inicio de validez es la misma que la fecha de finalización de validez del certificado de CA activo actual.

```
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
```



Renovación manual del servidor PKI

El servidor PKI de IOS admite la renovación manual del certificado de CA, es decir, un administrador puede activar la generación de un certificado de CA de sustitución incremental de antemano sin necesidad de configurar la **renovación automática** en la configuración del servidor PKI. Se recomienda configurar la renovación **automática** si se planea ampliar o no la duración de un servidor de CA implementado inicialmente para estar en el lado más seguro. **Los clientes PKI pueden sobrecargar la CA sin un certificado de CA de sustitución incremental**. *Refiérase a* Dependencia de la Operación SHADOW del Cliente en la Renovación del Servidor PKI.

Se puede activar una renovación manual mediante el comando configuration level:

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

Además, se puede cancelar un certificado CA de sustitución incremental para generar uno nuevo manualmente, sin embargo, algo que un administrador no debería hacer en un entorno de producción, utilizando:

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

Esto elimina el par de claves rsa de renovación y el certificado de CA de renovación. Esto se aconseja en contra porque:

- Una vez que la CA genera el certificado de renovación, varios clientes pueden descargar el certificado de la CA de sustitución incremental así como un certificado de cliente de renovación firmado por el certificado de CA de sustitución incremental.
- En esta etapa, si se cancela la renovación, es posible que el cliente tenga que volver a inscribirse.

Renovación automática de cliente PKI

Tipos de renovación de certificados de cliente: RENEW y SHADOW

El IOS en el servidor PKI siempre se asegura de que la hora de vencimiento del certificado de ID emitido al cliente nunca exceda la hora de vencimiento del certificado de CA.

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

- Hora de expiración del certificado de identidad que se renueva
- Hora de vencimiento del certificado (CA) del emisor

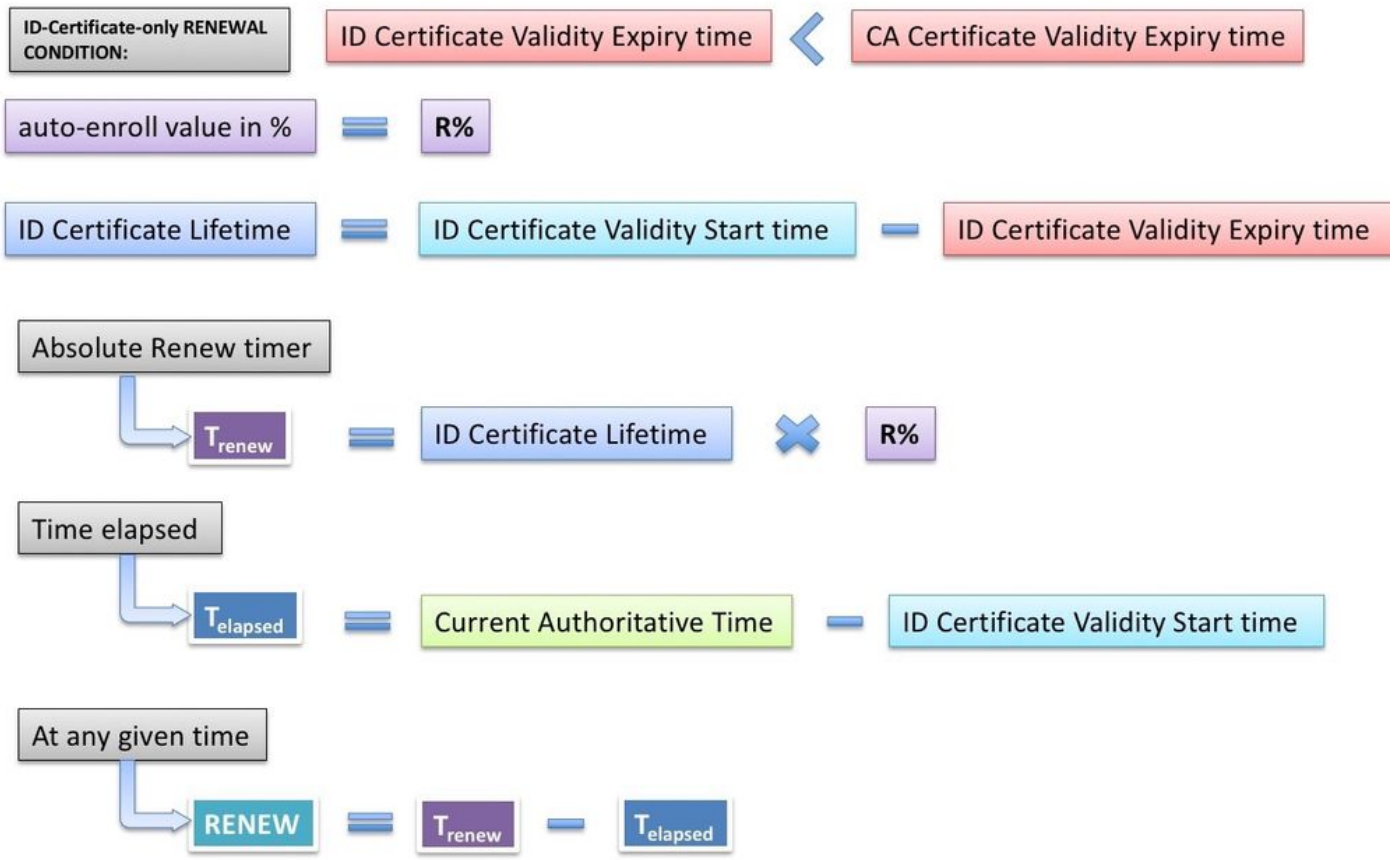
Si la hora de vencimiento del certificado de identidad no es la misma que la hora de vencimiento del certificado de CA, IOS realiza una simple operación de renovación.

Si la hora de vencimiento del certificado de identidad es la misma que la hora de vencimiento del certificado de CA, IOS realiza una operación de renovación de sombra.

RENOVACIÓN - Renovación de certificado de identidad del router

Como se mencionó anteriormente, el cliente PKI de IOS realiza una simple operación de renovación si la hora de vencimiento del certificado de identidad no es la misma que la hora de vencimiento del certificado de CA, es decir, el certificado de identidad que caduca antes de que el certificado del emisor active una simple renovación del certificado de identidad.

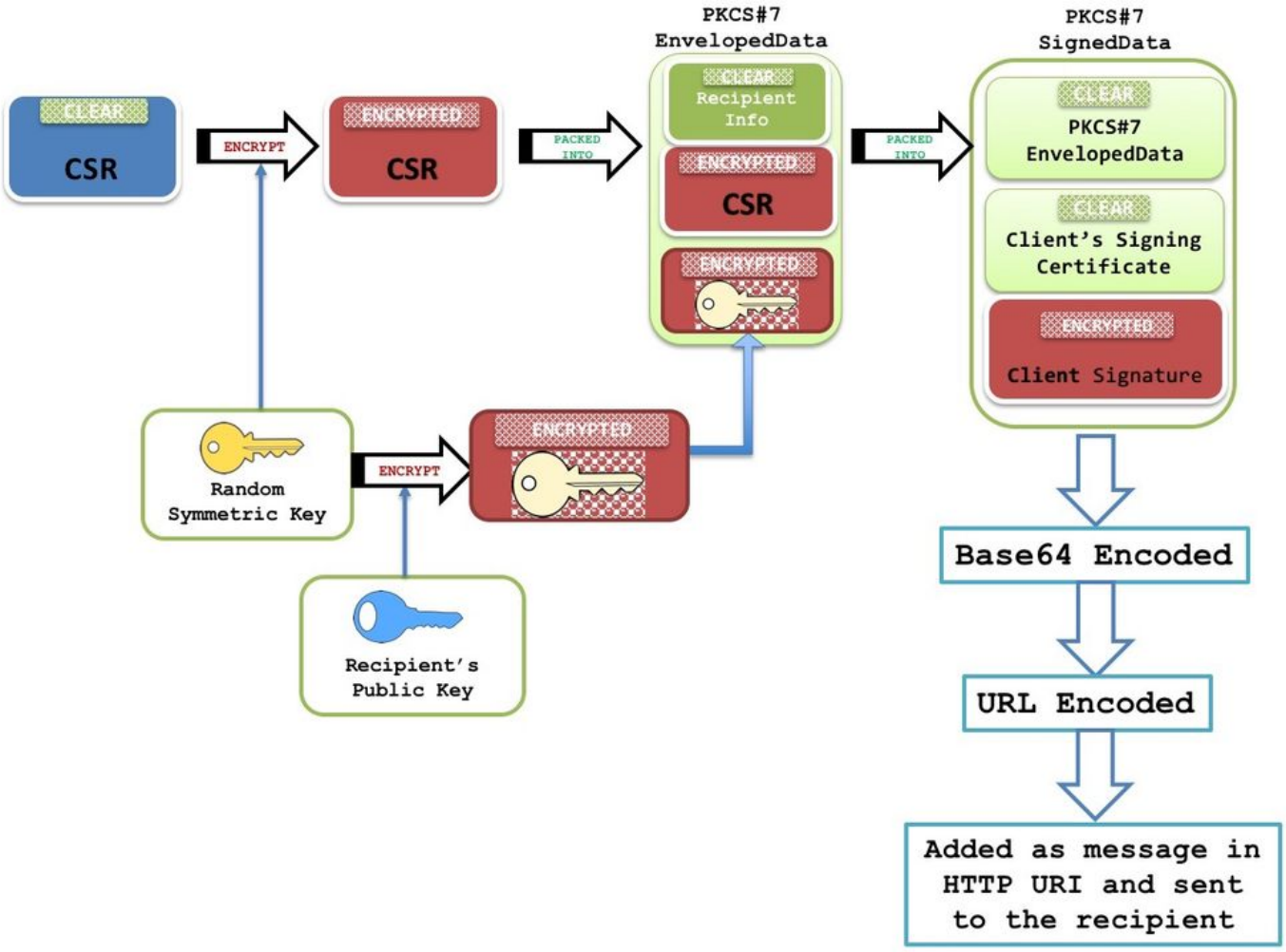
Tan pronto como se instala un certificado de identidad, IOS calcula el temporizador RENEW para el punto de confianza específico como se muestra a continuación:



Current-Authoritative-Time significa que el reloj del sistema debe ser una fuente autorizada de tiempo, como se describe aquí. (enlace a la sección de origen de tiempo autorizado) Los temporizadores PKI no se inicializarán sin una fuente de tiempo autorizada. Y, como consecuencia, no se llevará a cabo la operación de renovación.

Los siguientes eventos tienen lugar cuando caduca el temporizador RENEW:

- IOS genera un par de llaves centrales sombra si **se configura la regeneración** [ejemplo: auto-enroll 80 regenerate]. Sin **regenerar** IOS, se reutiliza el par de llaves RSA activo actualmente.
- IOS crea una solicitud de certificado con formato PKCS-10, que luego se cifra en un sobre PKCS-7. Este sobre también contiene RecipientInfo, que es el nombre del asunto y el número de serie de la CA emisora. Este sobre PKCS7, a su vez, se empaqueta en datos firmados PKCS-7. Durante la inscripción inicial, IOS utiliza un certificado autofirmado para firmar este mensaje. Y durante las inscripciones posteriores, es decir, las rematrículas, IOS utiliza el certificado de identidad activo para firmar el mensaje. Los datos firmados por PKCS7 también están integrados con el certificado de firma, es decir, el certificado autofirmado o el certificado de identidad.



Para obtener más información sobre esta estructura de paquetes, consulte el Documento de descripción general de SCEP

> **Nota:** La información clave aquí es RecipientInfo, que es el nombre del asunto y el número de serie de la CA emisora, y la clave pública de esta CA se utiliza para cifrar la clave simétrica. La CSR del sobre PKCS7 se cifra utilizando esta clave simétrica.

La CA receptora descifra esta clave simétrica cifrada mediante su clave privada y esta clave simétrica se utiliza para descifrar el sobre PKCS7 que revela el CSR.

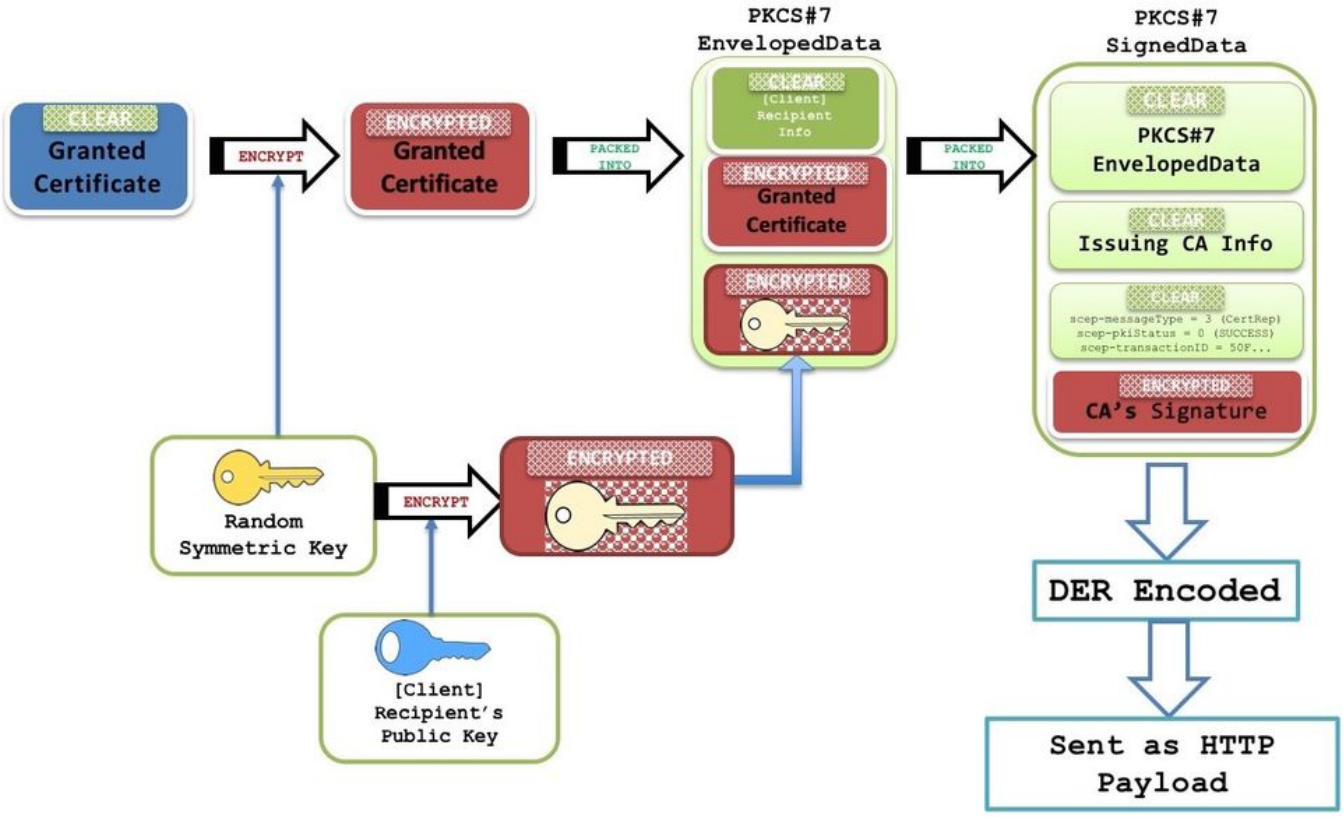
- Esta solicitud de firma de certificado (CSR) empaquetada en formato PKCS7 se envía a la CA con un tipo de mensaje SCEP PKCSReq y una operación SCEP llamada PKIOperation.
- Si la CA rechaza la solicitud, el IOS detiene el temporizador RENEW. A partir de este punto, para renovar el certificado de identidad, el administrador debe realizar una renovación manual (enlace a la sección **Renovación manual-cliente PKI**)
- Si la CA envía un estado SCEP como **pendiente**, el IOS en el cliente PKI inicia un temporizador POLL a partir de 60 segundos o 1 minuto. Cada vez que caduca un temporizador POLL, IOS envía el mensaje GetCertInicial SCEP a través de una operación PKIOperation.Cuando caduca el primer temporizador POLL, si el mensaje GetCertInicial se responde con un estado SCEP Pendiente, un algoritmo de retroceso exponencial establece el primer intervalo de reintento del temporizador POLL en 1 minuto, el segundo intervalo de reintento del temporizador POLL en 2 minutos, y así después en 4 minutos el siguiente 999

se reintenta de forma predeterminada o hasta que caduque el certificado de CA emisor. El recuento de sondeos y el primer período de reintento se pueden configurar utilizando:

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

- Cuando el certificado se concede en el servidor PKI, se responde al siguiente mensaje GetCertinitial SCEP con un mensaje HTTP de tipo de contenido **application/x-pki-message** y un cuerpo que contiene datos firmados PKCS#7. Estos datos PKCS7 firmados contienen el estado SCEP como **Otorgado**, y también datos PKCS7 envueltos. Estos datos envueltos de PKCS contienen el certificado concedido y RecipientInfo, que es el nombre del sujeto y el número de serie del certificado autofirmado durante la inscripción inicial y del certificado de identidad activo durante las rematrículas.

  Los datos envueltos PKCS7 también contienen una clave simétrica cifrada con la clave pública del destinatario (para la que se concedió el nuevo certificado). La recepción del router lo descifra usando la clave privada. Esta clave simétrica clara se utiliza luego para descifrar los datos envueltos PKCS#7, revelando el nuevo certificado de identidad.



- En esta etapa, IOS reemplaza el certificado de identidad existente con el nuevo certificado inmediatamente. Y si se configuró **regenerar**, el par de llaves centrales sombra reemplaza también al par de llaves activo.

- Además, la fecha de finalización del nuevo certificado se compara con la fecha de finalización del certificado de CA para determinar si se debe inicializar el temporizador RENEW o se debe inicializar un temporizador SHADOW como se explica aquí <href **Types of Client Certificate Renewal - RENEW and SHADOW>**