# Guia de implantação de PKI do IOS: Sobreposição de certificado - Visão geral da configuração e da operação

## Contents

# Introduction

Este documento descreve a rollover de certificado em servidores e clientes da infraestrutura de chave pública (PKI) do Cisco IOS em detalhes.

# Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

### Hardware

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

### Software

- IOS
  - Para ISR-G1 - 15.1(4)M* mais recente
  - Para ISR-G2 - Último 15.4(3)M
- IOS-XE
  - XE 3.15 ou 15.5(2)S

**Note**: A manutenção geral de software para dispositivos ISR não está mais ativa, quaisquer correções futuras de bugs ou aprimoramentos de recursos exigiriam uma atualização de hardware para os roteadores das séries ISR-2 ou ISR-4xxx.

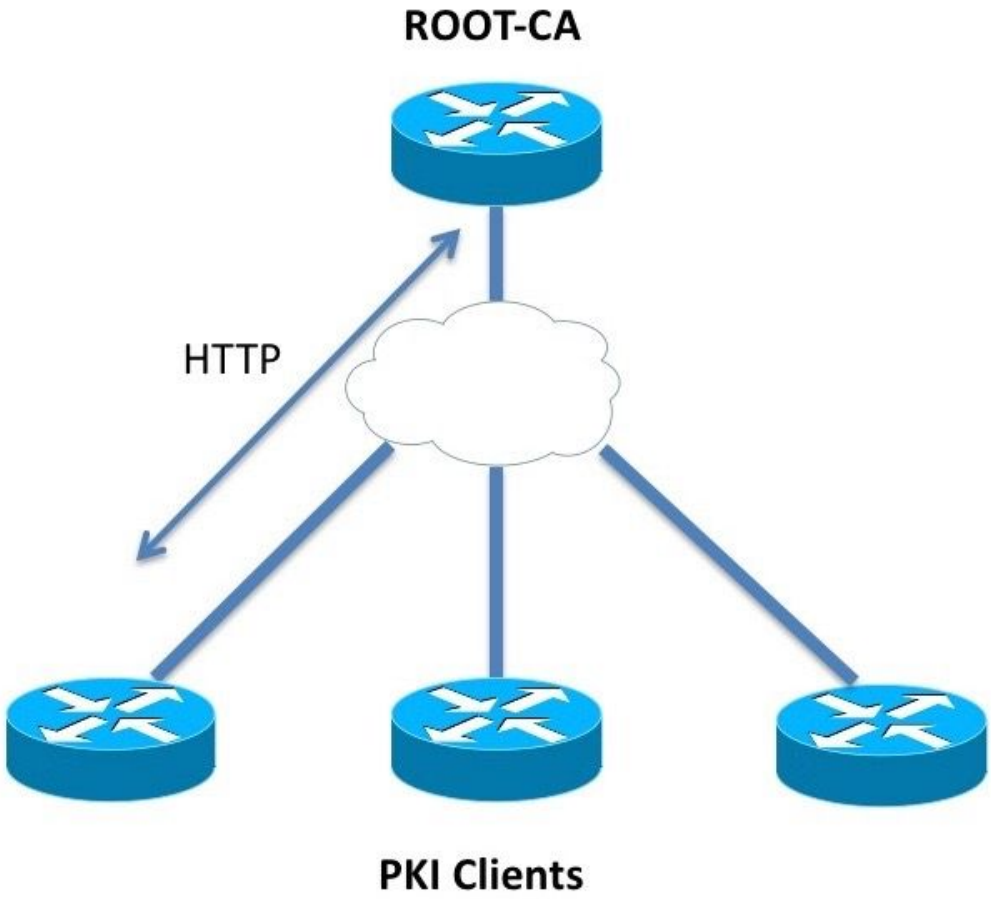
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Informações de Apoio

A transferência de certificado também conhecida como operação de renovação garante que, quando um certificado expira, um novo certificado esteja pronto para assumir o controle. Do ponto de vista de um servidor PKI, esta operação envolve a geração do novo certificado de transferência do servidor com bastante antecedência para garantir que todos os clientes PKI

tenham recebido um novo certificado de transferência do cliente assinado pelo novo certificado de transferência do servidor antes de o certificado atual expirar. Do ponto de vista de um cliente PKI, se o certificado do cliente está expirando, mas o certificado do Servidor da Autoridade de Certificação (AC) não está, o cliente solicita um novo certificado e substitui o certificado antigo assim que o novo certificado é recebido, e se o certificado do cliente está expirando ao mesmo tempo que o certificado do servidor da AC, o cliente garante primeiro a recepção do certificado de transferência do servidor da AC e solicita um certificado de transferência assinado pelo novo certificado de transferência do servidor CA e ambos serão ativados quando os certificados antigos expirarem.

# Instalação




# Pré-requisito de PKI e Protocolo de Inscrição de Certificado Simples (SCEP - Simple Certificate Enrollment Protocol)

## Origem de Tempo Autoritativa

No IOS, por padrão, a origem do relógio é considerada não autoritativa, pois o relógio do hardware não é a melhor fonte de tempo. Sendo o PKI sensível ao tempo, é importante configurar

uma fonte de tempo válida usando o NTP. Em uma implantação de PKI, recomenda-se que todos os clientes e o Servidor sincronizem seu relógio para um único servidor NTP, por meio de vários servidores NTP, se necessário. Mais detalhes sobre isso estão explicados no Guia de implantação de PKI do IOS: Projeto e implantação iniciais

O IOS não inicializa temporizadores PKI sem um relógio autoritativo. Embora o NTP seja altamente recomendado, como medida temporária, o administrador pode marcar o relógio do hardware como autoritativo usando:

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

### Comunicação HTTP

Um requisito para um servidor PKI IOS ativo é o servidor HTTP, que pode ser ativado usando este comando config-level:

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

Esse comando ativa o servidor HTTP na porta 80 por padrão, que pode ser alterado conforme mostrado acima.

Os clientes PKI devem ser capazes de se comunicar com o servidor PKI via HTTP com a porta configurada.

## Configuração de PKI

### Servidor - Sobreposição

A configuração de sobreposição automática do servidor PKI é semelhante 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
```

O parâmetro de substituição automática é definido em dias. Em um nível mais granular, o comando se parece com:

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

Um valor de substituição automática de 90 indica que o IOS cria um certificado de servidor de sobreposição 90 dias antes da expiração do certificado de servidor atual, e a validade desse novo certificado de sobreposição começa ao mesmo tempo que o tempo de expiração do certificado ativo atual.

A rollover automático deve ser configurada com um valor que assegure que o certificado CA de rollover seja gerado no servidor PKI com bastante antecedência antes que qualquer cliente PKI

na rede execute a operação GetNextCACert, conforme descrito na seção **de visão geral da operação SHADOW** abaixo.

### Cliente - Renovação

A configuração de renovação automática de certificado do PKI Client tem a seguinte aparência:

```
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
```

Aqui, o **comando autoenroll <percentual> [regenerar]** afirma que o IOS deve executar a renovação de certificado exatamente em 80% do tempo de vida do certificado atual.

A palavra-chave **regenerate** afirma que o IOS deve regenerar o par de chaves RSA conhecido como par de chaves de sombra durante cada operação de renovação de certificado.

Deve-se tomar cuidado ao configurar o percentual de inscrição automática. Em qualquer cliente PKI na implantação, se surgir uma condição em que o certificado de identidade expire ao mesmo tempo que o certificado CA emissor, o valor da inscrição automática sempre acionará a operação de renovação [sombra] depois que a CA tiver criado o certificado de transferência. *Consulte a* seção **dependências do temporizador PKI** nos exemplos de implantação.

## Pré-requisitos de renovação/rollover de PKI

Este documento aborda detalhadamente as operações de renovação e substituição de certificados e, portanto, considera-se que estes eventos foram concluídos com êxito:

- Inicialização do servidor PKI com um certificado CA válido.
- Os clientes PKI foram inscritos com êxito com o servidor PKI. Ou seja, cada cliente PKI tem o certificado CA e um certificado de identidade também conhecido como certificado de roteador.

A inscrição de um cliente envolve esses eventos. Sem entrar em detalhes demais:

- Autenticação de ponto de confiança
- Inscrição de ponto de confiança

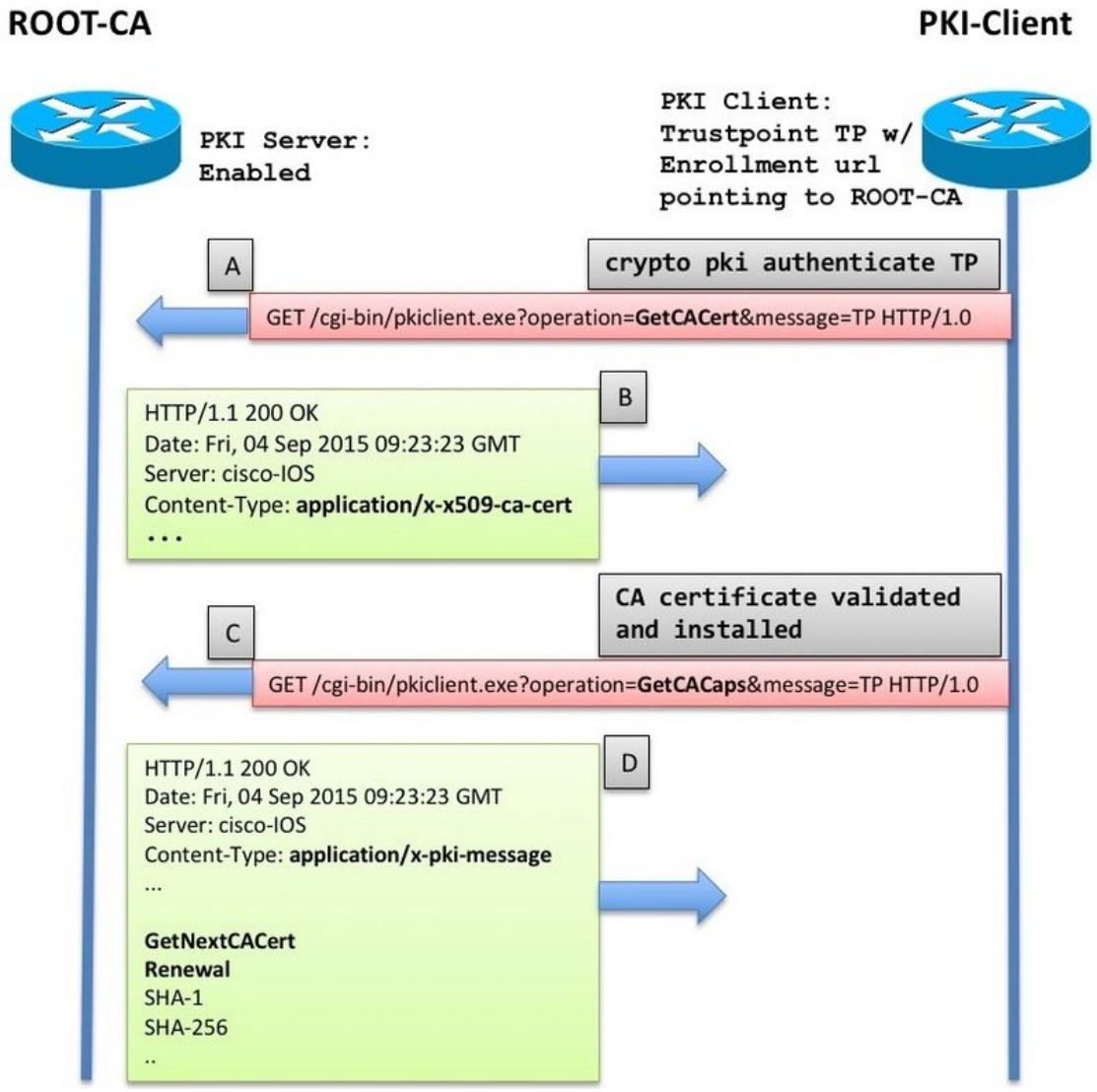
No IOS, um ponto de confiança é um contêiner de certificados. Qualquer ponto confiável fornecido pode conter um certificado de identidade ativo e/ou um certificado de CA ativo. Um ponto confiável é considerado autenticado se contiver um certificado CA ativo. E é considerado inscrito se contiver um certificado de identidade. Um ponto confiável deve ser autenticado antes de uma inscrição. A configuração do cliente e do servidor PKI, juntamente com a autenticação de ponto de confiança e a inscrição, são abordadas em detalhes no Guia de implantação de PKI do IOS: Projeto e implantação iniciais

Após a recuperação/instalação do certificado CA, o cliente PKI recupera os recursos do servidor PKI antes de executar uma inscrição. A recuperação de recursos de CA é explicada nesta seção.

## Recursos de CA

No IOS, quando um cliente PKI autentica uma CA, em outras palavras, quando um administrador cria um ponto de confiança em um roteador IOS e executa o comando **crypto pki authenticate <trustpoint-name>**, esses eventos acontecem no roteador:

- O IOS envia uma solicitação SCEP contendo o tipo de operação GetCACert.
- A resposta esperada aqui é uma mensagem HTTP com um tipo de conteúdo de **application/x-x509-ca-cert** em caso de implantação de CA ou **application/x-x509-ca-ra-cert** em caso de implantação de RA e CA. E o corpo HTTP contém o certificado CA. [e um certificado de RA no último caso].
- Após a recuperação e instalação do certificado CA/RA, o cliente inicia uma solicitação SCEP automática contendo a operação GetCACaps.
- A resposta esperada aqui é uma mensagem HTTP com um tipo de conteúdo de **aplicativo/x-pki-message**, que também pode ser **texto/simples** e o corpo HTTP contém uma série de recursos suportados pela CA, separados por um caractere de feed de linha. Uma resposta típica do IOS PKI Server é mostrada no diagrama abaixo.




A resposta é interpretada como esta pelo IOS PKI Client:

```
CA_CAP_GET_NEXT_CA_CERT
```

```
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

Desses recursos, este documento se concentra nesses dois recursos.

### GetNextCACert

Quando esse recurso é retornado pela CA, o IOS entende que a CA suporta o CA-Certificate Rollover. Com esse recurso retornado, se o comando **autoenroll** não estiver configurado no ponto de confiança, o IOS inicializa um temporizador SHADOW definido como 90% do período de validade do certificado CA.

Quando o temporizador SHADOW expira, o IOS executa a operação GetNextCACert SCEP para buscar o certificado Rollover CA.

> **Observação**: se o comando **autoenroll** tiver sido configurado no ponto de confiança junto com uma **url de inscrição**, um temporizador RENOVAR será inicializado mesmo antes de autenticar o ponto de confiança e tentará constantemente se inscrever com a CA localizada na **url de inscrição**, embora nenhuma mensagem de inscrição real [CSR] seja enviada até que o ponto de confiança seja autenticado.

> **Note**: GetNextCACert é enviado como um recurso pelo servidor PKI do IOS, mesmo que a **rollover automático** não esteja configurada no servidor

### Renovação

Com esse recurso, o servidor PKI informa ao cliente PKI que ele pode usar um certificado de ID ativo para assinar uma solicitação de assinatura de certificado para renovar o certificado existente.

Mais sobre isso na seção **Renovação automática de cliente PKI**.

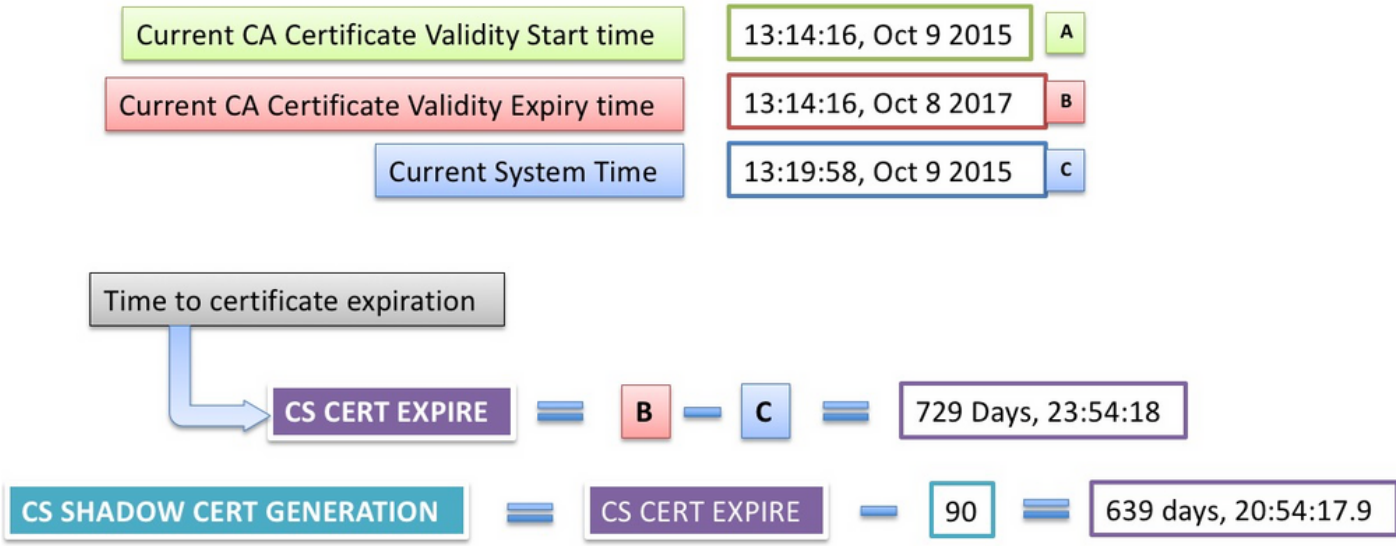
## Substituição automática do servidor PKI

Com a configuração acima no CA Server, você vê:

```
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 o seguinte:




## Operação Rollover

Quando o temporizador **CS SHADOW CERT GENERATION** expira:

- O IOS gera um par de chaves rollover primeiro - atualmente ele tem o mesmo nome do par de chaves ativo com um # hash anexado a ele.

```
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
```

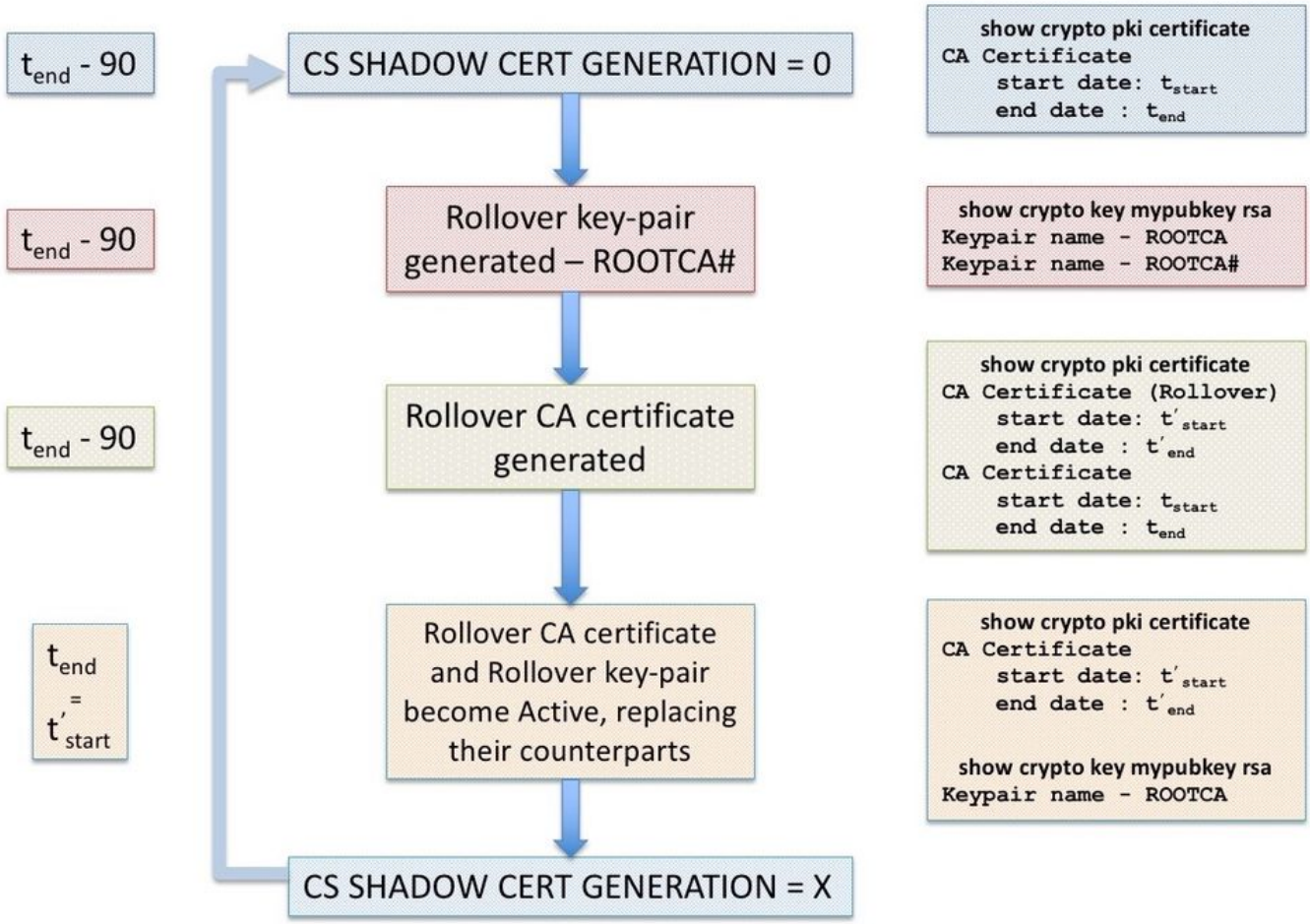
- Em seguida, o IOS gera o certificado CA de transferência, em que a data de início da validade é igual à data de término da validade do certificado CA ativo atual.

```
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 Server Manual-Rollover

O IOS PKI Server suporta a transferência manual do certificado CA, ou seja, um administrador pode acionar a geração de um certificado CA de transferência com antecedência sem precisar configurar a **transferência automática** na configuração do servidor PKI. É altamente recomendável configurar a **transferência automática**, independentemente de se planejar ou não estender a vida útil de um servidor CA inicialmente implantado para estar no lado mais seguro. **Os clientes PKI podem sobrecarregar a CA sem um certificado CA rollover**. *Consulte* Dependência da operação SHADOW do cliente na transferência do servidor PKI.

Uma sobreposição manual pode ser acionada usando o comando configuration level:

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

Além disso, um certificado CA rollover pode ser cancelado para gerar um novo manualmente, no

entanto, algo que um administrador não deve fazer em um ambiente de produção, usando:

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

Isso exclui o par de chaves rsa rollover e o certificado CA rollover. Este fato é aconselhado contra porque:

- Quando a CA gera o certificado de transferência, vários clientes podem baixar o certificado de CA de transferência e também um certificado de cliente de transferência assinado pelo certificado de CA de transferência.
- Nesse estágio, se a transferência for cancelada, o cliente poderá ter que ser reinscrito.

# Renovação automática de cliente PKI

## Tipos de renovação de certificado do cliente - RENOVAR e SOMBRA

O IOS no servidor PKI sempre garante que o tempo de expiração do certificado de ID emitido ao cliente nunca vá além do tempo de expiração do certificado CA.

Em um cliente PKI, o IOS sempre leva em consideração os seguintes temporizadores antes de programar a operação de renovação:

- Prazo de validade do certificado de identidade que está a ser renovado
- Prazo de validade do certificado do emitente (AC)

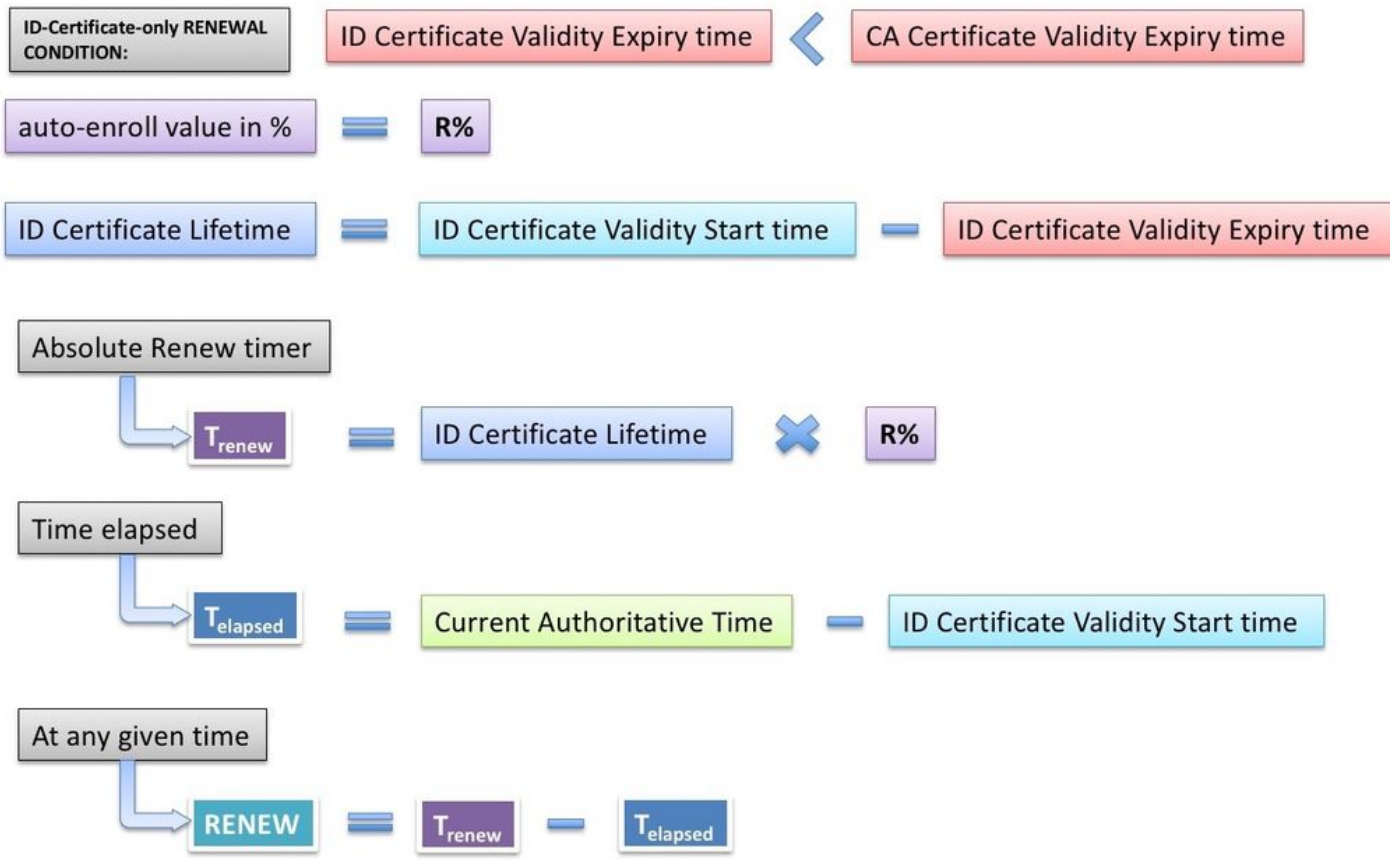
Se o tempo de validade do certificado de identidade não for o mesmo que o tempo de expiração do certificado CA, o IOS executa uma operação de renovação simples.

Se o tempo de expiração do certificado de identidade for o mesmo que o tempo de expiração do certificado CA, o IOS executará uma operação de renovação de sombra.

## RENOVAÇÃO - Renovação do certificado de identidade do roteador

Como mencionado anteriormente, o cliente PKI IOS executa uma operação de renovação simples se o tempo de expiração do certificado de identidade não for o mesmo que o tempo de expiração do certificado CA, em outras palavras, o certificado de identidade que expira antes do certificado do emitente aciona uma renovação simples do certificado de identidade.

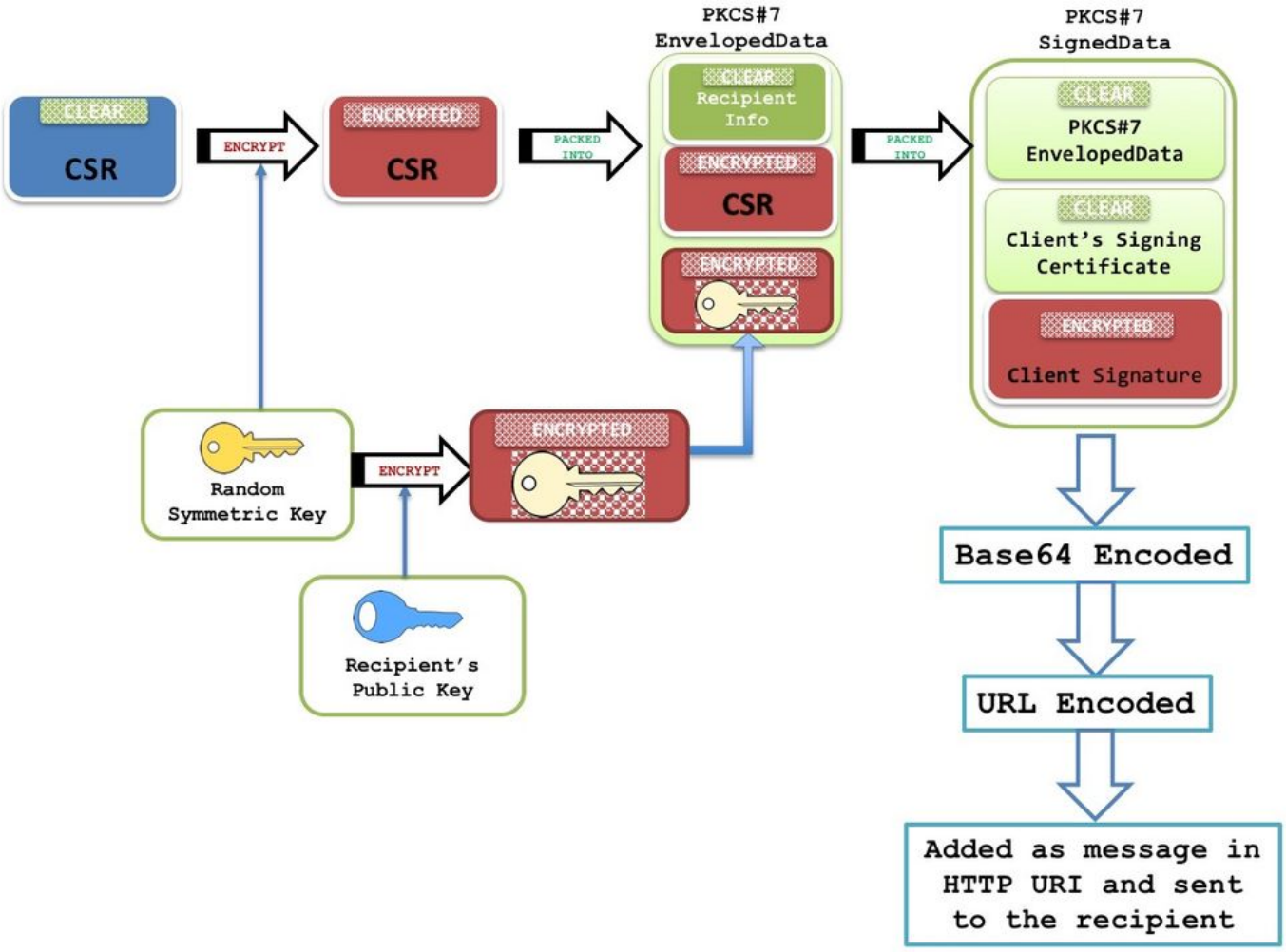
Assim que um certificado de identidade é instalado, o IOS calcula o temporizador RENOVAR para o ponto de confiança específico, como mostrado abaixo:




Current-Authitative-Time significa que o relógio do sistema deve ser uma fonte de tempo autoritativa, como descrito aqui. (link para a seção de fonte de tempo autoritativa) Os temporizadores PKI não serão inicializados sem uma fonte de tempo autoritativa. Como consequência, não haverá renovação.

Os eventos a seguir ocorrem quando o temporizador de RENOVAÇÃO expira:

- O IOS gera um par de chaves sombra se **regenerar** estiver configurado [exemplo: autorregistrar 80 regenerar]. Sem **regenerar** o IOS reutiliza o par de chaves RSA atualmente ativo.
- O IOS cria uma solicitação de certificado formatado PKCS-10, que é criptografada em um envelope PKCS-7. Este envelope também contém RecipientInfo, que é o nome do assunto e o número de série da AC emissora. Este envelope PKCS7 é, por sua vez, compactado em dados assinados PKCS-7. Durante a inscrição inicial, o IOS usa um certificado autoassinado para assinar essa mensagem. E durante as inscrições subsequentes, ou seja, as reinscrições, o IOS usa o certificado de identidade ativo para assinar a mensagem. Os dados assinados PKCS7 também estão incorporados no certificado de assinatura, ou seja, no certificado autoassinado ou no certificado de identidade.




Para obter mais informações sobre esta estrutura de pacotes, consulte o Documento de Visão Geral do SCEP

> **Note**: As principais informações aqui são RecipientInfo, que é o nome do assunto e o número de série da AC emissora, e a chave pública desta AC é usada para criptografar a chave simétrica. O CSR no envelope PKCS7 é criptografado usando essa chave simétrica.

Essa chave simétrica criptografada é descriptografada pela CA receptora usando sua chave privada, e essa chave simétrica é usada para descriptografar o envelope PKCS7 que revela o CSR.

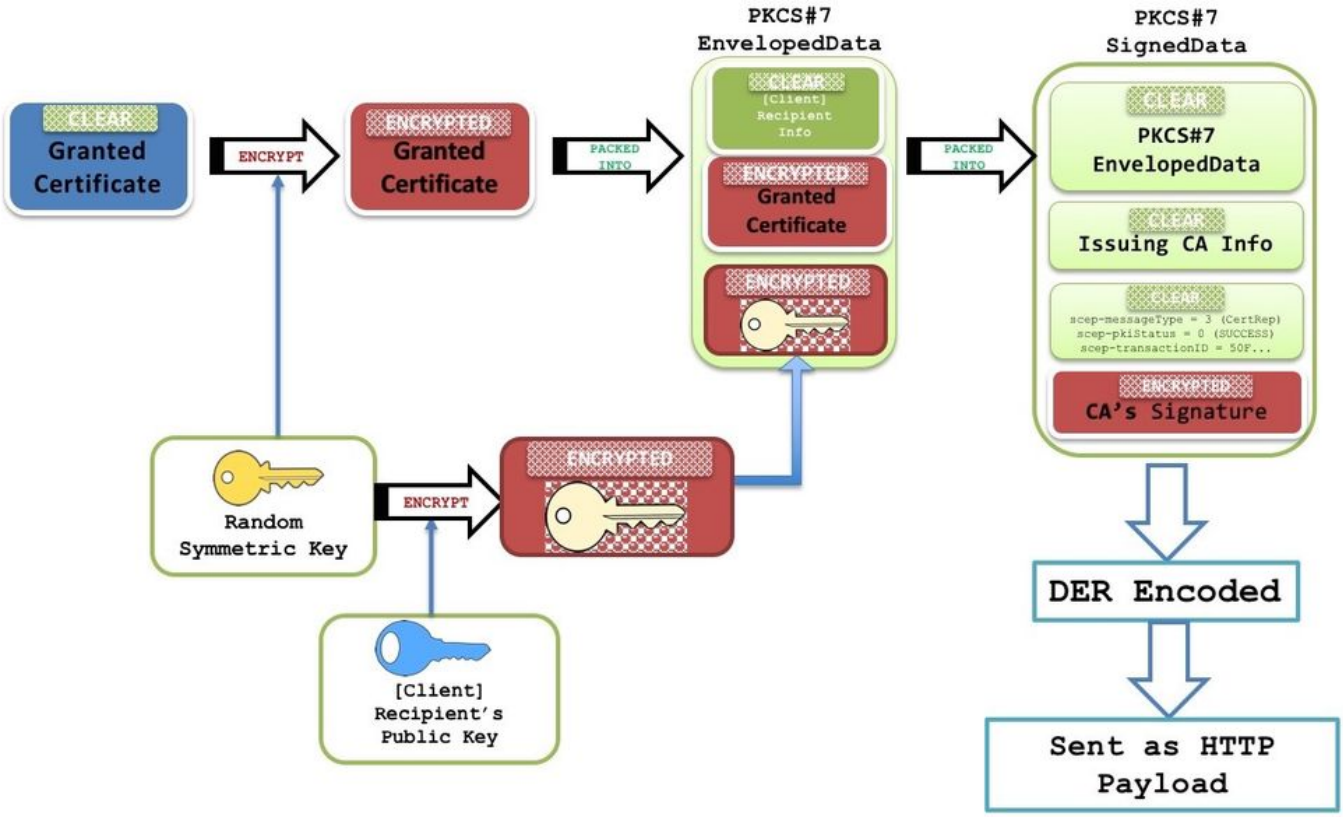
- Esta Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) empacotada no formato PKCS7 é então enviada para a CA com um tipo de mensagem SCEP de PKCSReq e uma operação SCEP chamada PKIOperation.
- Se a CA rejeitar a solicitação, o IOS interrompe o temporizador RENOVAR. A partir deste ponto, para renovar o certificado de identidade, o administrador deve executar uma renovação manual (link para a seção **Manual-Renovação do cliente PKI**)
- Se a CA enviar um status SCEP como **pendente**, o IOS no cliente PKI inicia um temporizador de POLL iniciando em 60 segundos ou 1 minuto. Sempre que um temporizador de POLL expira, o IOS envia a mensagem GetCertInitial SCEP através de uma operação PKIOperation.Quando o primeiro temporizador de POLL expira, se a mensagem GetCertInitial for respondida com um status SCEP Pending, um algoritmo de recuo exponencial configurará o primeiro intervalo de repetição do temporizador de POLL para 1 minuto, segundo intervalo

de tentativa de POLL intervalo de nova tentativa do mer para 4 minutos e assim por diante para as próximas 999 novas tentativas por padrão ou até que o certificado CA de emissão expire.
A contagem de votações e o primeiro período de repetição podem ser configurados usando:

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

- Quando o certificado é concedido no servidor PKI, a próxima mensagem SCEP GetCertInitial é respondida com uma mensagem HTTP de tipo de conteúdo **application/x-pki-message** e um corpo contendo dados assinados PKCS#7. Esses dados assinados do PKCS7 contêm o status SCEP como **Concedido**, e também um PKCS7 com dados encapsulados. Estes dados com PKCS contêm o certificado concedido e o RecipientInfo, que é o nome do assunto e o número de série do certificado autoassinado durante a inscrição inicial e do certificado de identidade ativo durante as reinscrições.

  Os dados com envelope PKCS7 também contêm uma chave simétrica criptografada com a chave pública do destinatário (para a qual o novo certificado foi concedido). O roteador receptor descriptografa-o usando a chave privada. Essa chave simétrica clara é então usada para descriptografar os dados com envelope PKCS#7, revelando o novo certificado de identidade.




- Neste estágio, o IOS substitui imediatamente o certificado de identidade existente pelo novo certificado. E se **regenerar** foi configurado, o par de chaves sombra substitui o par de chaves ativo também.

- Além disso, a data de término do novo certificado é comparada com a data de término do certificado CA para determinar se o temporizador de RENOVAÇÃO deve ser inicializado ou

se um temporizador de SHADOW deve ser inicializado conforme explicado aqui <href **Types of Client Certificate Renewal - RENEW and SHADOW>**