Guia de distribuição IO PKI: Derrubamento do certificado - Configuração e visão geral de operação

Índice

Introdução

Este documento descreve o derrubamento do certificado em server e em clientes do Public Key Infrastructure (PKI) do Cisco IOS em detalhe.

Pré-requisitos

Requisitos

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 – O 15.1(4)M* o mais atrasado
  - Para ISR-G2 – O mais tarde 15.4(3)M
- IOS-XE
  - XE 3.15 ou 15.5(2)S

Nota: A manutenção de software geral para dispositivos ISR é já não ativa, todas as correções de bug ou aprimoramentos de recursos futuros exigiriam uma upgrade de hardware aos Series Router ISR-2 ou de ISR-4xxx.

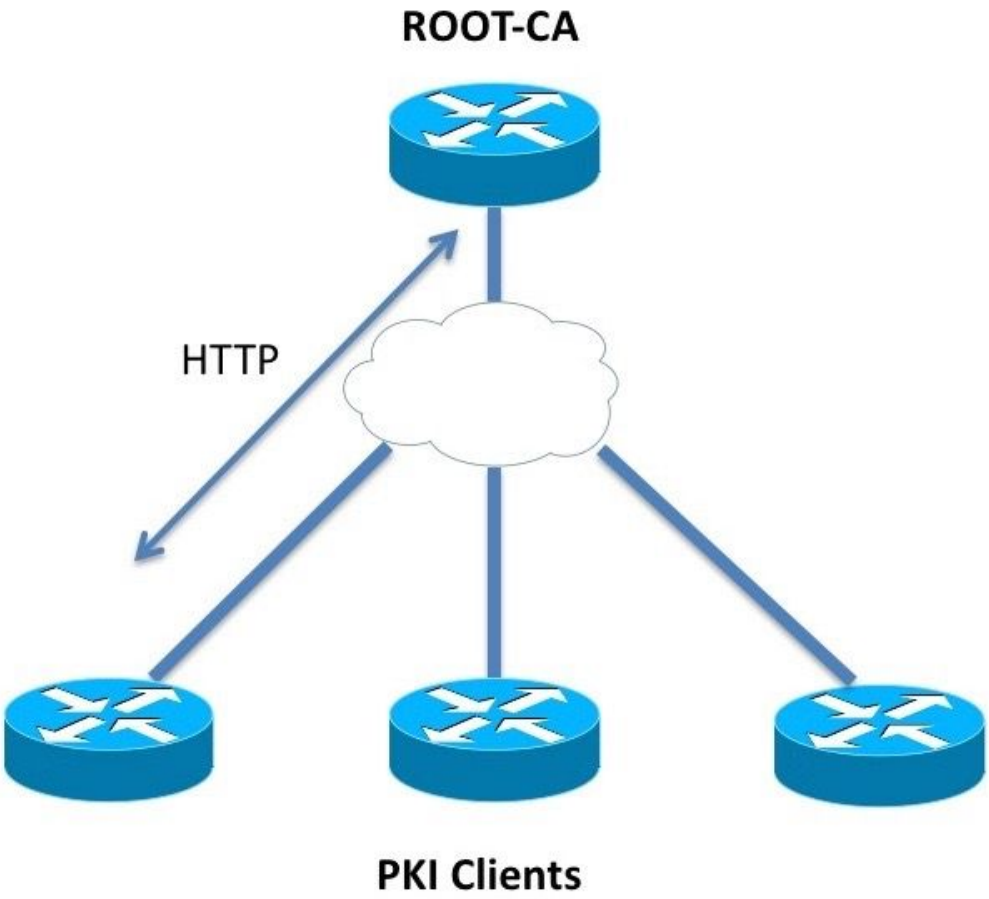
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O derrubamento do certificado igualmente conhecido como a operação da renovação assegura-se de que quando um certificado expira, um certificado novo esteja pronto para tomar sobre. Do ponto de vista de um servidor PKI, esta operação envolve gerar o poço novo do certificado do derrubamento do server adiantado para certificar-se de que todos os clientes PKI receberam um certificado novo do derrubamento do cliente assinado pelo certificado novo do derrubamento do server antes que o certificado atual expire. Do ponto de vista de um cliente PKI, se o certificado

de cliente está expirando mas o certificado de server do Certificate Authority (CA) não é, os pedidos do cliente para um certificado novo e substituem o certificado velho assim que o certificado novo for recebido, e se o certificado de cliente está expirando ao mesmo tempo que o certificado de server de CA, o cliente certifica-se receber primeiramente o certificado do derrubamento do server de CA, e então pede para um certificado do derrubamento assinado pelo certificado novo do derrubamento do server de CA, e ambos serão ativados quando os Certificados velhos expiram.

Instalação



PKI e condição prévia simples do protocolo do registro de Ceritificate (SCEP)

Fonte de tempo autoritária

Nos IO, o origem do relógio é considerado à revelia ser NON-competente desde que o relógio de hardware não é a melhor fonte de tempo. PKI que é sensível ao tempo, é importante configurar um origem válida do tempo usando o NTP. Em um desenvolvimento PKI, recomenda-se mandar todos os clientes e server sincronizar se for necessário seu pulso de disparo a um único servidor

de NTP, através dos servidores de NTP múltiplos. Mais neste é explicado no guia de distribuição IO PKI: Projeto inicial e desenvolvimento

Os IO não inicializam temporizadores PKI sem um pulso de disparo competente. Embora o NTP seja altamente recomendado, como uma medição temporária, o administrador possa marcar o relógio de hardware como a utilização competente:

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

Uma comunicação HTTP

Uma exigência para um servidor PKI ativo IO é o Server do HTTP, que pode ser permitido usando este comando do configuração-nível:

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

Este comando permite o Server do HTTP na porta 80 à revelia, que pode ser mudada como mostrado acima.

Os clientes PKI devem poder comunicar-se com o servidor PKI sobre o HTTP à porta configurada.

Configuração PKI

Server - Derrubamento

A configuração automática do derrubamento do servidor PKI olha como:

```
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 do auto-derrubamento é definido nos dias. A nível mais granulado, o comando olha como:

```
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
```

Um valor do auto-derrubamento de 90 indica que os IO criam um certificado de servidor do derrubamento 90 dias antes da expiração do certificado de servidor atual, e a validez deste certificado novo do derrubamento começa ao mesmo tempo que a época da expiração do certificado ativo atual.

o Auto-derrubamento deve ser configurado com tal valor que se certifica de que o certificado de

CA do derrubamento está gerado no poço do servidor PKI adiantado antes que todo o cliente PKI na rede execute a operação de GetNextCACert como descrito na seção de **visão geral de operação da SOMBRA** abaixo.

Cliente - Renovação

A configuração automática da renovação do certificado do cliente PKI olha como:

```
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, auto-**registre** estados do comando do **[regenerate] do <percentage>** que os IO devem executar a renovação do certificado em exatamente 80% da vida do certificado atual.

O regenerado da palavra-chave indica que os IO devem regenerar o par de chaves RSA conhecido como o par de chaves da sombra durante cada operação da renovação do certificado.

Deve ser tomado ao configurar auto-registre a porcentagem. Em todo o cliente dado PKI no desenvolvimento, se uma circunstância elevara onde o certificado de identidade expira ao mesmo tempo que o certificado de CA de emissão, a seguir o valor auto-registrar-se deve sempre provocar a operação da renovação do [shadow] depois que CA criou o certificado do derrubamento. *Refira a* seção das **dependências do temporizador PKI** sob os exemplos de distribuição.

Condições prévias da renovação/derrubamento PKI

Este documento endereça operações do derrubamento e da renovação do certificado em detalhe, e daqui estes eventos são considerados ser terminados com sucesso:

- Iniciação do servidor PKI com um certificado de CA válido.
- Os clientes PKI foram registrados com sucesso com o servidor PKI. isto é. Cada cliente PKI tem o certificado de CA e um certificado de roteador do certificado de identidade aka.

Registrar um cliente envolve estes eventos. Sem obter demasiado no detalhe:

- Autenticação do ponto confiável
- Registro do ponto confiável

Nos IO, um ponto confiável é um recipiente para Certificados. Todo o ponto confiável dado pode conter um certificado de identidade ativo e/ou um certificado de CA ativo. Um ponto confiável está considerado autenticado se contém um ceryificate ativo de CA. E considera-se registrado se contém um certificado de identidade. Um ponto confiável deve ser autenticado antes de um registro. O servidor PKI e a configuração de cliente, junto com a autenticação do ponto confiável e o registro são cobertos em detalhe no guia de distribuição IO PKI: Projeto inicial e desenvolvimento

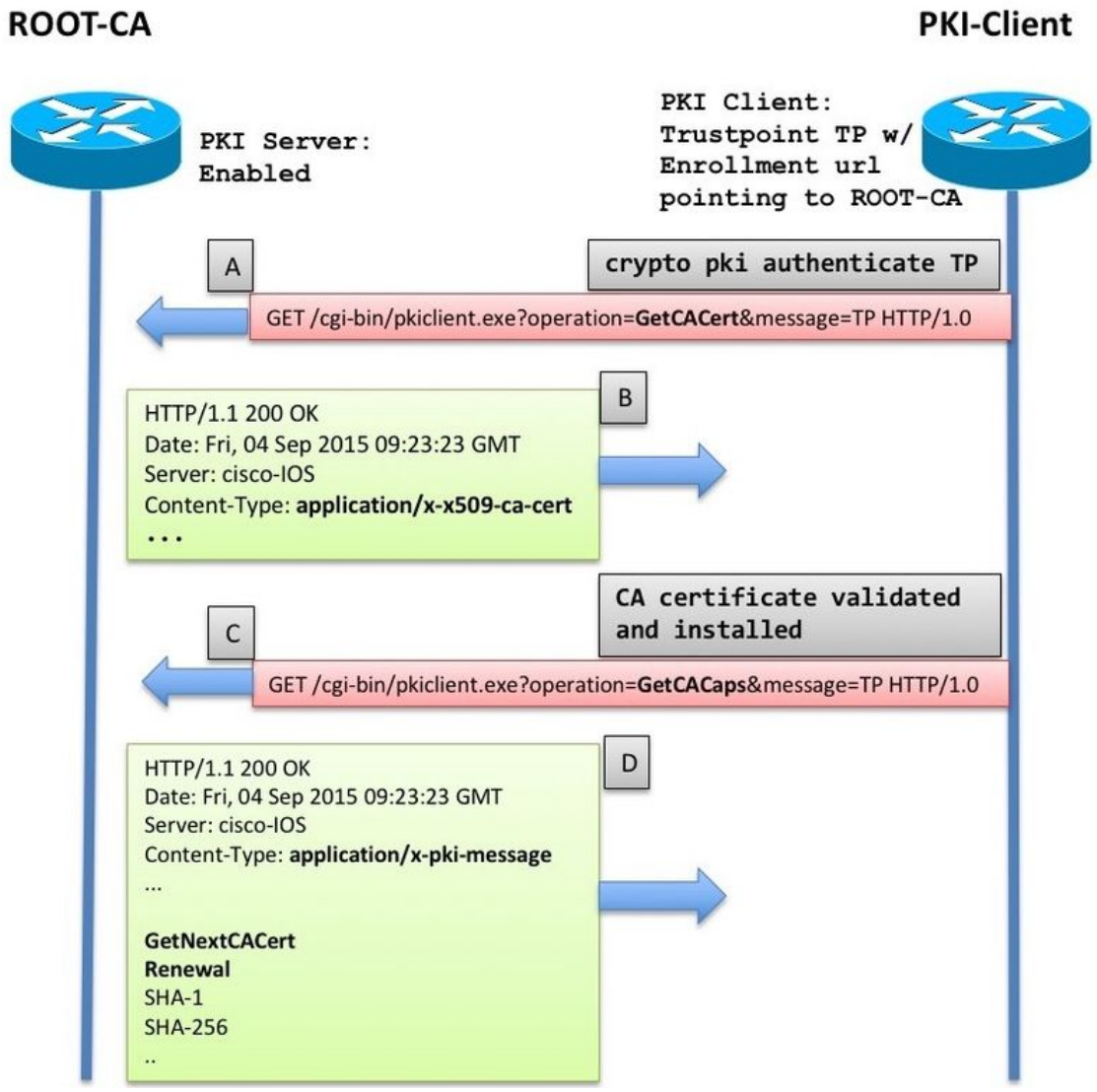
Depois da recuperação/instalação do certificado de CA, o cliente PKI recupera as capacidades do servidor PKI antes de executar um registro. A recuperação das capacidades de CA é explicada

nesta seção.

Capacidades de CA

Nos IO, quando um cliente PKI autenticar CA, ou seja quando um administrador criar um ponto confiável em um IOS Router, e executa o comando crypto que o **pki autentica o <trustpoint-name>**, estes eventos ocorrem no roteador:

- Os IO enviam um pedido SCEP que contém o tipo de operação de GetCACert.
- A resposta esperada aqui é uma mensagem HTTP com um tipo de conteúdo de **application/x-x509-ca-cert** em caso de um desenvolvimento de CA, ou **application/x-x509-ca-ra-cert** em caso de um RA e de um desenvolvimento de CA. E o corpo HTTP contém o certificado de CA. [and an RA certificate in the latter case].
- Depois da recuperação de certificado e da instalação CA/RA, o cliente inicia um pedido automático SCEP que contém a operação de GetCACaps.
- A resposta esperada aqui é uma mensagem HTTP com um tipo de conteúdo de **application/x-pki-message**, que poderia igualmente ser **texto/liso** e o corpo HTTP contém uma série de capacidades apoiadas por CA, separado por um caráter da LINE FEED. Uma resposta típica do servidor PKI IO é segundo as indicações do diagrama abaixo.



A resposta é interpretada como esta pelo cliente IO 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
```

Destas capacidades, este documento focaliza nestes dois.

GetNextCACert

Quando esta capacidade é retornada por CA, os IO compreendem que CA apoia o derrubamento do certificado de CA. Com esta capacidade retornada, se o **comando auto-enroll** não é configurado sob o ponto confiável, os IO inicializam um temporizador da SOMBRA ajustado a 90% do período de validade do certificado de CA.

Quando o temporizador da SOMBRA expira, os IO executam a operação de GetNextCACert SCEP para buscar o certificado de CA do derrubamento.

> Nota: Se o **comando auto-enroll** foi configurado sob o ponto confiável junto com um **registro URL**, um temporizador da RENOVAÇÃO está inicializado mesmo antes de autenticar o ponto confiável, e tenta constantemente registrar-se com CA situado no **registro URL**, embora nenhum [CSR] real da mensagem da matrícula seja enviado até que o ponto confiável esteja autenticado.

> Nota: GetNextCACert é enviado como uma capacidade pelo servidor PKI IO mesmo se o auto-**derrubamento** não é configurado no serviço

Renovação

Com esta capacidade, o servidor PKI informa o cliente PKI que pode usar um certificado ativo ID para assinar uma solicitação de assinatura de certificado renovar o certificado existente.

Mais nisto na seção da Auto-**renovação do cliente PKI**.

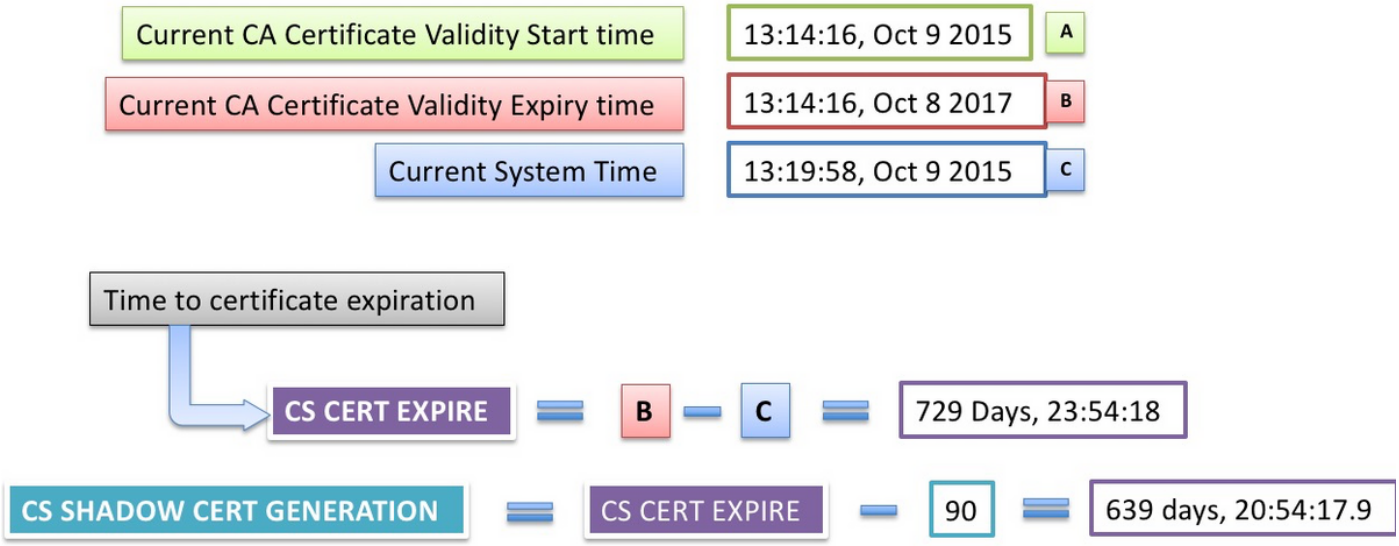
Auto-derrubamento do servidor PKI

Com a configuração acima no server de CA, você vê:

```
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
```

Observe isto:



Operação do derrubamento

Quando o temporizador da **GERAÇÃO da SOMBRA CERT CS** expirar:

- Os IO gerenciem um par de chaves do derrubamento primeiramente – atualmente tem o mesmo nome que o par de chaves ativo com a # mistura adicionado 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
```

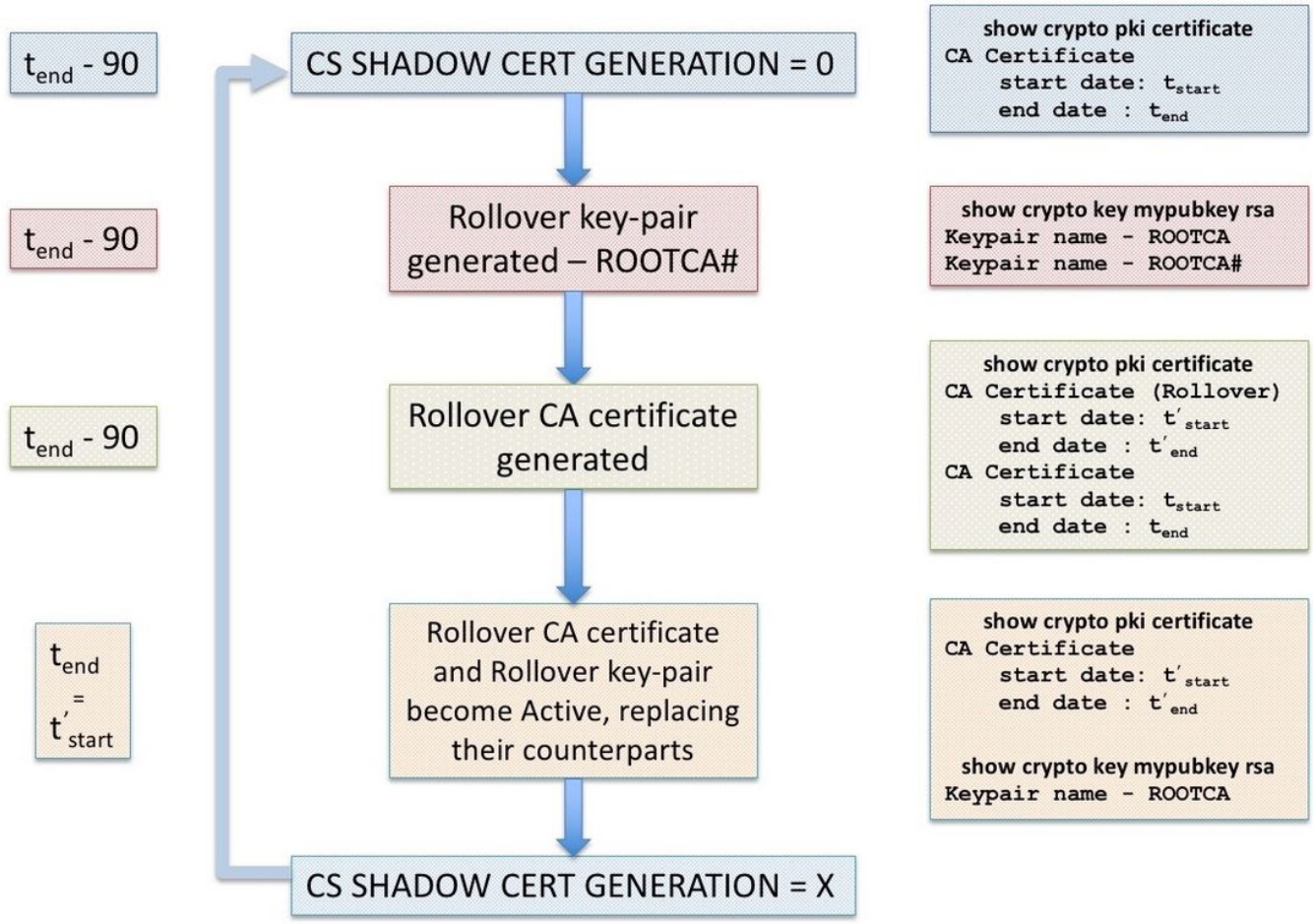
- Os IO gerenciem então o certificado de CA do derrubamento, onde a data de início da validez é a mesma que a data final da validez do certificado de CA ativo atual.

```
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-derrubamento do servidor PKI

O servidor PKI IO apoia o derrubamento manual do certificado de CA, isto é um administrador

pode provocar a geração de um certificado de CA do derrubamento adiantado sem precisar de configurar o auto-derrubamento **sob a** configuração de servidor PKI. É altamente recomendado configurar o auto-derrubamento **mesmo se** um planeia estender a vida de um server inicialmente distribuído de CA para estar no lado mais seguro. PKICLIENTS **pode sobrecarregar CA sem um certificado de CA do derrubamento.** Operação da SOMBRA do cliente de Referto Dependencyof no derrubamento do servidor PKI.

Um derrubamento manual pode ser provocado usando o comando do nível da configuração:

```
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
```

E também, um certificado de CA do derrubamento pode ser cancelado para gerar manualmente fresco, porém algo um admin não deve fazer em um ambiente de produção, usar-se:

```
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
```

Isto suprime do par de chaves dos rsa do derrubamento e do certificado de CA do derrubamento. Isto é recomendado contra porque:

- Uma vez que CA gerencie o certificado do derrubamento, os clientes múltiplos podem transferir o certificado de CA do derrubamento assim como um certificado de cliente do derrubamento assinados pelo certificado de CA do derrubamento.
- Nesta fase se o derrubamento é cancelado, o cliente pode ter que re-ser registrado.

Auto-renovação do cliente PKI

Tipos de renovação do certificado de cliente - RENOVE e SOMBREIE

Os IO no servidor PKI certificam-se sempre de que a época da expiração do certificado ID emitido ao cliente nunca vai além da época da expiração do certificado de CA.

Em um cliente PKI, os IO tomam sempre os seguintes temporizadores na consideração antes de programar a operação da renovação:

- Tempo da expiração do certificado de identidade que está sendo renovado
- Tempo da expiração do certificado do expedidor (CA)

Se a época da expiração do certificado de identidade não é a mesma que a época da expiração

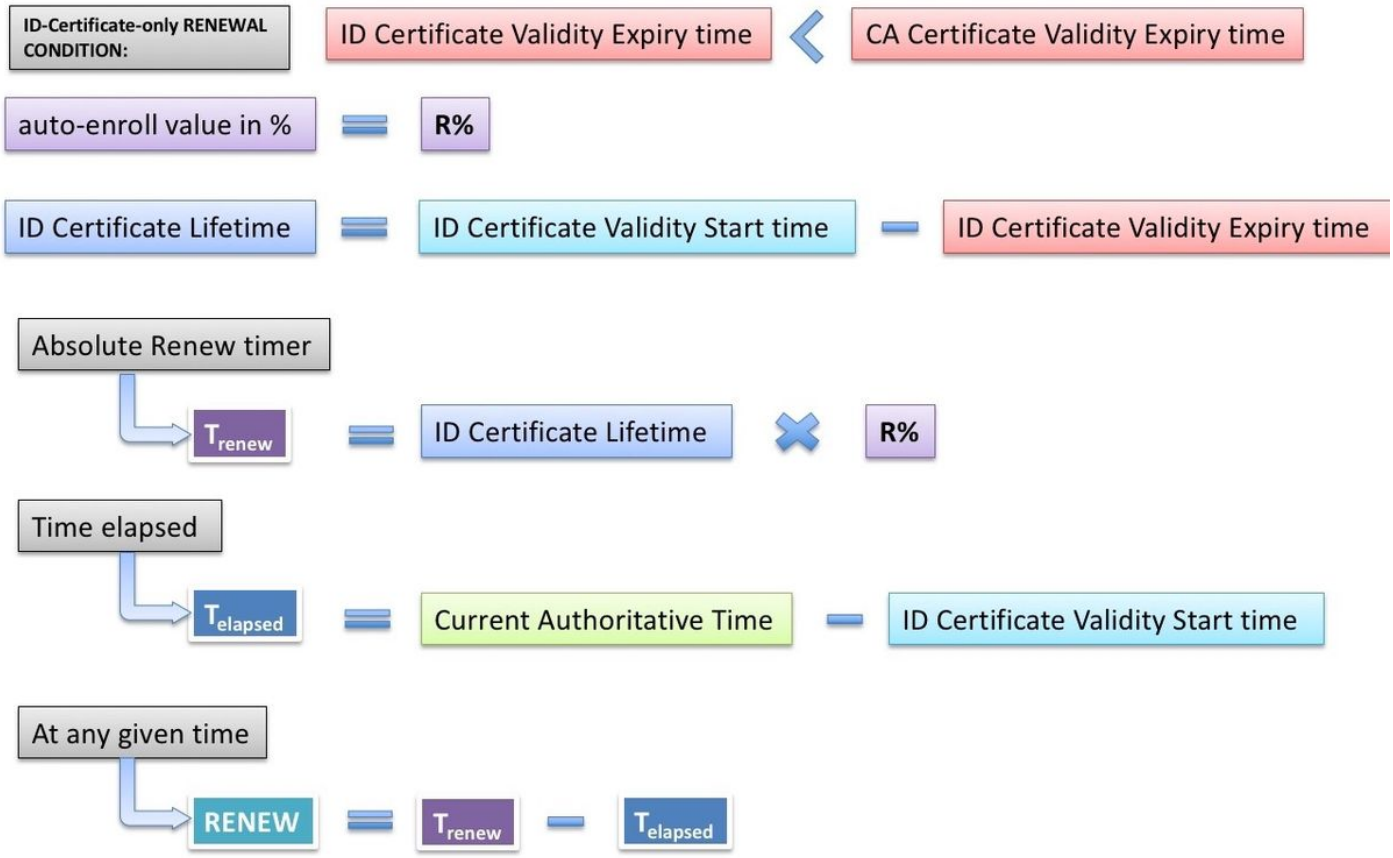
do certificado de CA, os IO executam uma operação simples da renovação.

Se a época da expiração do certificado de identidade é a mesma que a época da expiração do certificado de CA, os IO executam uma operação da renovação da sombra.

RENOVE - Renovação do certificado de identidade do roteador

Como mencionado antes, o cliente IO PKI executa uma operação simples da renovação se a época da expiração do certificado de identidade não é a mesma que a época da expiração do certificado de CA, em outras palavras o certificado de identidade que expira antes do certificado do expedidor provoca uma renovação simples do certificado de identidade.

Assim que um certificado de identidade for instalado, os IO calculam o temporizador da RENOVAÇÃO para o confiança-ponto específico como mostrado abaixo:

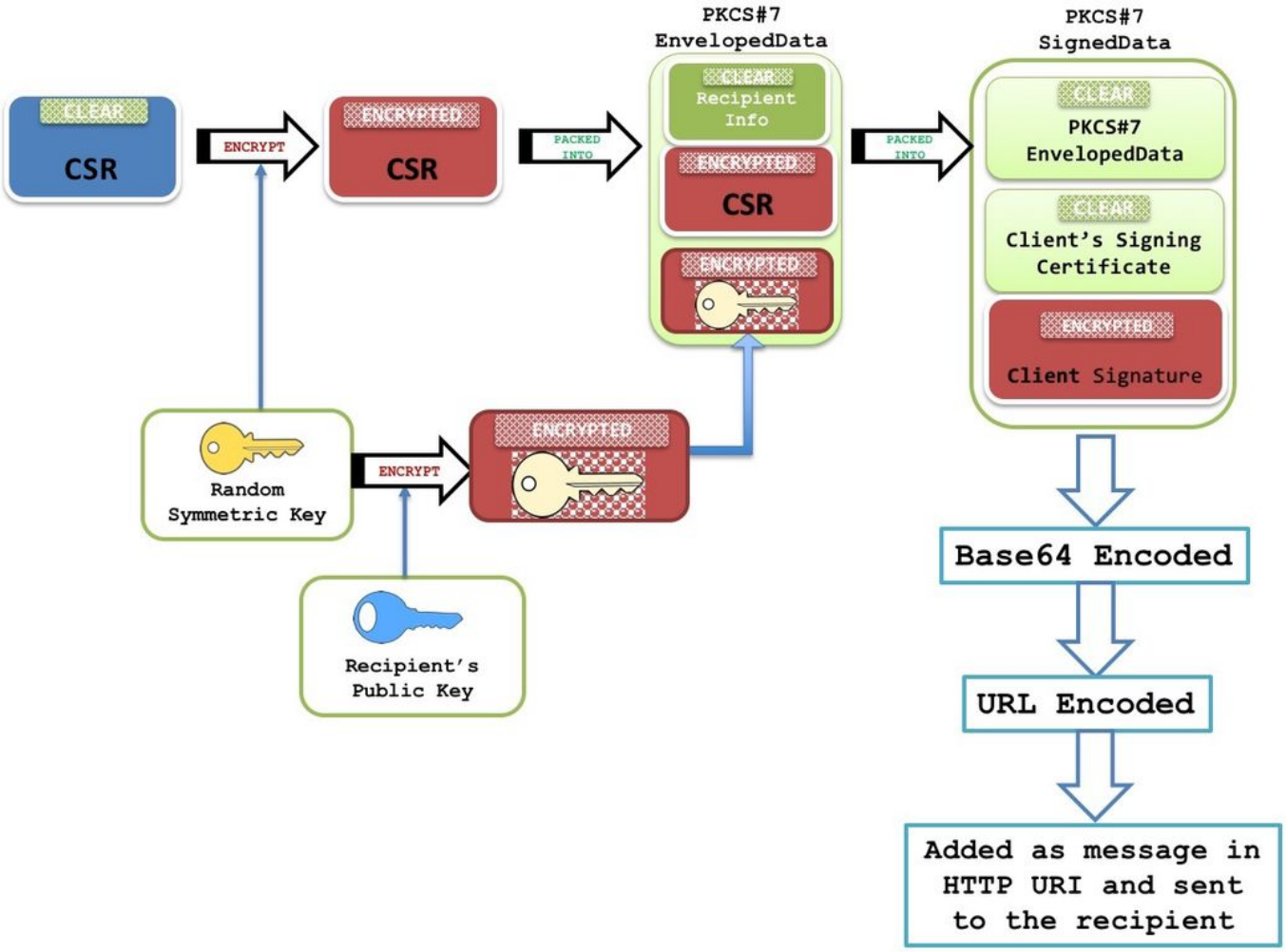


O Atual-Competente-tempo significa que o relógio de sistema tem que ser uma fonte competente de tempo como descrito aqui. (link à seção da fonte de tempo autoritária) os temporizadores PKI não serão inicializados sem uma fonte competente de tempo. E consequentemente, a operação da renovação não ocorrerá.

Os seguintes eventos ocorrem quando RENOVE o temporizador expira:

- Os IO gerenciem um par de chaves da sombra se o **regenerado** é configurado [exemplo: auto-registre o regenerado 80]. Sem IO **regenerados** reutiliza o par de chaves atualmente ativo RSA.
- Os IO criam um pedido do certificado formatado PKCS-10, que seja cifrado então em um envelope PKCS-7. Este envelope igualmente contém o RecipientInfo, que é o assunto-nome e o número de série de CA de emissão. Este PKCS7-envelope por sua vez é embalado em

um PKCS-7 assinar-DATA. Durante o registro inicial, os IO usam um certificado auto-assinado para assinar esta mensagem. E durante os registros subsequentes, isto é as novas inscrições, IO usam o certificado de identidade ativo para assinar a mensagem. Os dados assinados PKCS7 são encaixados igualmente com o certificado de assinatura, isto é o certificado auto-assinado ou o certificado de identidade.



Para obter mais informações sobre desta estrutura de pacote refira a documentação de visão geral SCEP

Nota: A informação chave aqui é o RecipientInfo que é o assunto-nome e o número de série de CA de emissão, e a chave pública deste CA é usada para cifrar a chave simétrica. O CSR no envelope PKCS7 é cifrado usando esta chave simétrica.

Esta chave simétrica cifrada é decifrada por CA de recepção usando sua chave privada, e esta chave simétrica é usada para decifrar o envelope PKCS7 que revela o CSR.

- Esta solicitação de assinatura de certificado (CSR) empacotada no formato PKCS7 é enviada então a CA com um tipo de mensagem SCEP de PKCSReq e uma operação SCEP chamada PKIOperation.
- Se CA rejeita o pedido, os IO param o temporizador da RENOVAÇÃO. A partir daqui, para renovar o certificado de identidade, o administrador deve executar uma renovação manual (o link à seção da Manual-**renovação do cliente PKI**)
- Se CA envia um status de SCEP como **pendente**, os IO no cliente PKI começam um

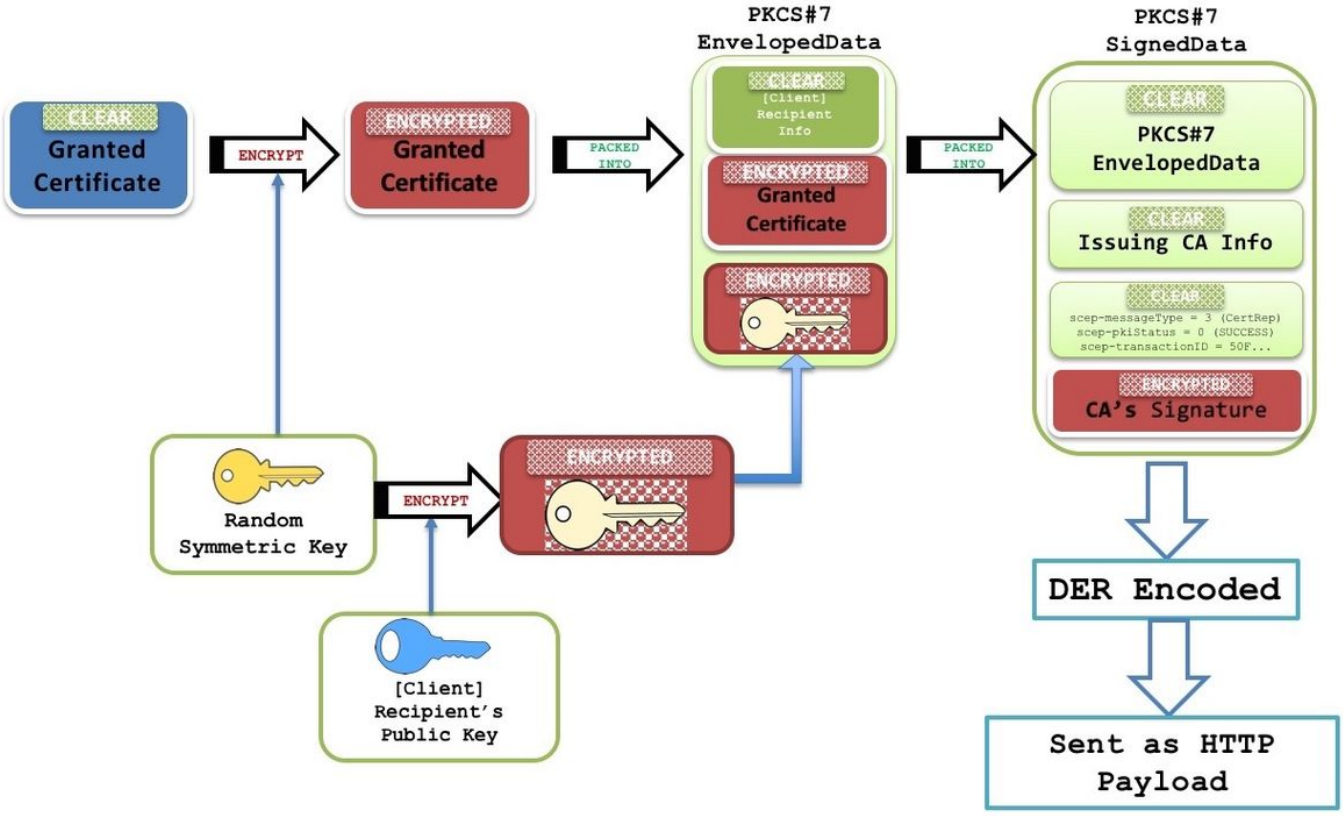
temporizador da VOTAÇÃO começar em 60 segundos ou em 1 minuto. Cada vez que um temporizador da VOTAÇÃO expira, os IO enviam a mensagem de GetCertInitial SCEP com uma operação de PKIOperation. Quando o primeiro temporizador da VOTAÇÃO expira, se a mensagem de GetCertInitial está respondida com a um status pendente SCEP, um algoritmo de retrocesso exponencial ajusta o primeiro intervalo de nova tentativa do temporizador da VOTAÇÃO a 1 minuto, segundo intervalo de nova tentativa do temporizador da VOTAÇÃO a 2 minutos, terceiro intervalo de nova tentativa do temporizador da VOTAÇÃO a 4 minutos e assim por diante para as 999 novas tentativas seguintes à revelia ou até que o certificado de CA de emissão expirar.
A contagem da votação e o primeiro período da nova tentativa podem ser utilização configurada:

```
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
```

- Quando o certificado é concedido no servidor PKI, a mensagem seguinte de GetCertInitial SCEP está respondida com a uma mensagem HTTP do tipo de conteúdo **application/x-pki-message** e a um corpo que contém uns dados assinados PKCS#7 assinados. Estes dados assinados PKCS7 contêm o status de SCEP como **concedido**, e igualmente um PKCS7

envolveu dados. Estes dados envolvidos PKCS contêm o certificado concedido e o RecipientInfo, que é o assunto-nome e o número de série do certificado auto-assinado durante o registro inicial e do certificado de identidade ativo durante novas inscrições.

Os dados envolvidos PKCS7 igualmente contêm uma chave simétrica cifrada com a chave pública do receptor (para qual o certificado novo foi concedido). Receber o roteador decifra-os que usam a chave privada. Esta chave simétrica clara é usada então para decifrar os dados envolvidos PKCS#7, revelando o certificado de identidade novo.



- Nesta fase, os IO substituem o certificado de identidade existente com o certificado novo imediatamente. E se o **regenerado** foi configurado, o par de chaves da sombra substitui o par de chaves ativo também.

- Também, a data final do certificado novo está comparada com a data final do certificado de CA para determinar se RENOVE o temporizador tem que ser inicializado ou um temporizador da SOMBRA tem que ser inicializado como **tipos** aqui explicados do <href de **renovação do certificado de cliente - RENOVE e SHADOW>**