Guide de déploiement de PKI IOS : Renversement de certificat - Aperçu de configuration et d'exécution

Contenu

Introduction

Ce document décrit le renversement de certificat sur des serveurs et des clients d'Infrastructure à clés publiques (PKI) de Cisco IOS en détail.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Matériel

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

Logiciel

- IOS
  - Pour ISR-G1 – Le dernier 15.1(4)M*
  - Pour l'ISR G2 – Le plus tard 15.4(3)M
- IOS-XE
  - XE 3.15 ou 15.5(2)S

Remarque: La maintenance logicielle générale pour des périphériques ISR n'est plus en activité, tous les futurs correctifs de bogue ou caractéristique-améliorations exigeraient une mise à niveau matérielle aux routeurs de la gamme ISR-2 ou ISR-4xxx.

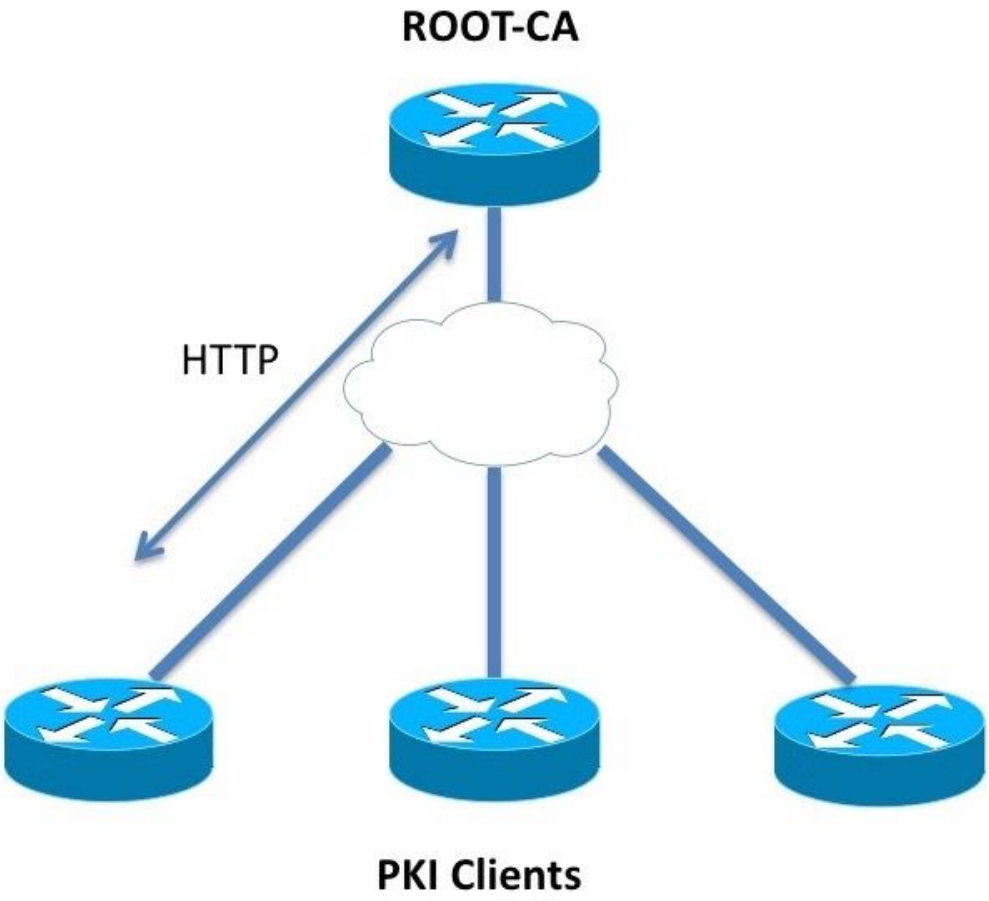
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Délivrez un certificat le renversement également connu sous le nom d'exécution de renouvellement s'assure que quand un certificat expire, un nouveau certificat est prêt à succéder. Du point de vue d'un serveur de PKI, cette exécution implique de générer le puits inversé de certificat de nouveau serveur à l'avance pour s'assurer que tous les clients de PKI ont reçu un certificat inversé de nouveau client signé par le certificat inversé de nouveau serveur avant que le

certificat valable expire. Du point de vue d'un client de PKI, si le certificat client expire mais le certificat de serveur d'Autorité de certification (CA) n'est pas, les demandes de client d'un nouveau certificat et remplace le certificat ancien dès que le nouveau certificat sera reçu, et si le certificat client expire en même temps que le certificat de serveur CA, le client veille à recevoir le certificat inversé du serveur CA d'abord, et alors il demande pour un certificat inversé signé par le certificat inversé de nouveau serveur CA, et chacun des deux seront lancés quand les vieux Certificats expirent.

Installation



PKI et condition préalable simple de Protocol d'inscription de Ceritificate (SCEP)

Source temporelle bien fondée

Dans l'IOS, par défaut le clock source est considéré non-bien fondé puisque l'horloge de matériel n'est pas la meilleure source de temps. PKI étant sensible au temps, il est important de configurer une source valide de temps utilisant le NTP. Dans un déploiement de PKI, il est recommandé pour faire synchroniser tous les clients et à serveur leur horloge à un serveur simple de NTP, par de

plusieurs serveurs de NTP s'il y a lieu. Plus sur ceci est expliqué du guide de déploiement de PKI IOS : Conception initiale et déploiement

L'IOS n'initialise pas des temporisateurs de PKI sans horloge bien fondée. Bien que le NTP soit fortement recommandé, comme mesure provisoire, l'administrateur puisse marquer l'horloge de matériel comme l'utilisation bien fondée :

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

Transmission de HTTP

Une condition requise pour un serveur actif de PKI IOS est le serveur HTTP, qui peut être activé utilisant cette commande niveau du config :

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

Ce serveur HTTP de commandes enables sur le port 80 par défaut, qui peut être changé comme affiché ci-dessus.

Les clients de PKI devraient pouvoir communiquer avec le serveur de PKI au-dessus du HTTP au port configuré.

Configuration de PKI

Serveur - Renversement

La configuration inversée automatique de serveur de PKI ressemble à :

```
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
```

Le paramètre d'auto-rollover est défini en quelques jours. À un niveau plus granulaire, la commande ressemble à :

```
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
```

Une valeur d'auto-rollover de 90 indique que l'IOS crée un certificat de serveur inversé pendant 90 jours avant l'échéance du certificat de serveur en cours, et la validité débuts inversés de ce de nouveaux certificat en même temps que l'échéance temps du certificat actif en cours.

L'auto-rollover devrait être configuré avec une telle valeur qui veille que le certificat de CA inversé est généré sur le puits de serveur de PKI à l'avance avant que n'importe quel client de PKI dans le

réseau exécute l'exécution de GetNextCACert comme décrit dans la vue d'ensemble d'**exécution de SHADOW** ci-dessous.

Client - Renouvellement

La configuration automatique de renouvellement de certificat de client de PKI ressemble à :

```
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
```

Ici, déclarer de commande **[régénérés] de <percentage> d'auto-enroll** que l'IOS devrait exécuter le renouvellement de certificat exactement à 80% de la vie du certificat valable.

Le régénéré de mot clé déclare que l'IOS devrait régénérer la paire de clés RSA connue sous le nom de paire de clés de shadow pendant chaque exécution de renouvellement de certificat.

Le soin devrait être pris tout en configurant le pourcentage d'auto-enroll. Sur n'importe quel client indiqué de PKI dans le déploiement, si une condition surgit où le certificat d'identité expire en même temps que le certificat de CA émettant, puis la valeur d'auto-enroll devrait toujours déclencher [l'exécution de renouvellement de shadow] après que le CA ait créé le certificat inversé. *Référez-vous à la* section de **dépendances de temporisateur de PKI** sous les exemples de déploiement.

Renouvellement de PKI/conditions préalables inversées

Ce document adresse des exécutions de renversement et de renouvellement de certificat en détail, et par conséquent ces événements sont considérés pour être terminés avec succès :

- Initialisation de serveur de PKI avec un certificat de CA valide.
- Des clients de PKI ont été inscrits avec succès avec le serveur de PKI. c.-à-d. Chaque client de PKI a le certificat de CA et un certificat de routeur de certificat d'identité aka.

L'inscription d'un client implique ces événements. Sans obtenir trop dans le détail :

- Authentification de point de confiance
- Inscription de point de confiance

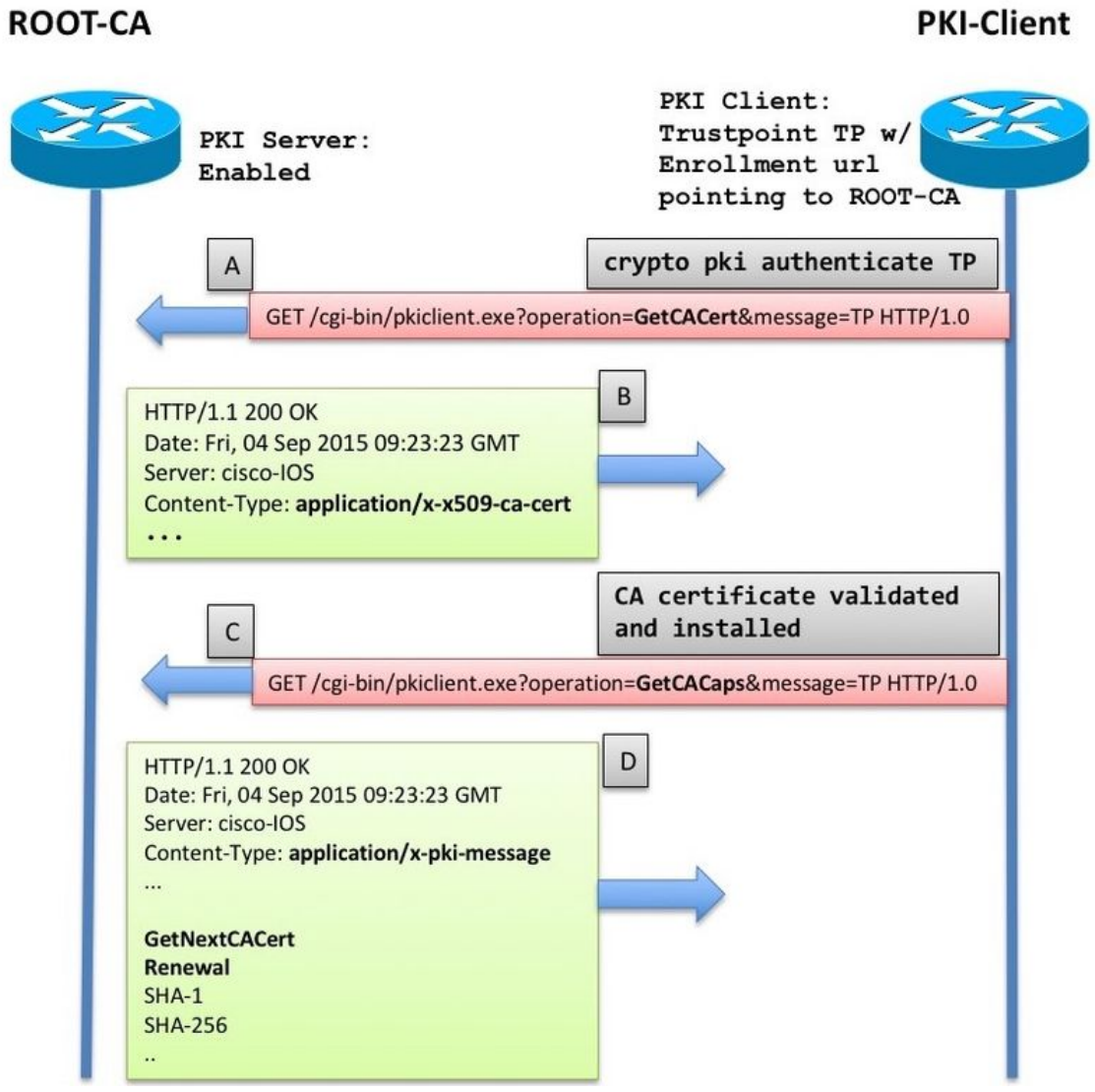
Dans l'IOS, un point de confiance est un conteneur pour des Certificats. N'importe quel point de confiance donné peut contenir un certificat d'identité actif et/ou un certificat de CA d'active. Un point de confiance est considéré authentifié s'il contient un ceryificate actif CA. Et il est considéré inscrit s'il contient un certificat d'identité. Un point de confiance doit être authentifié avant une inscription. La configuration de serveur et de client de PKI, avec l'authentification de point de confiance et l'inscription sont couvertes en détail du guide de déploiement de PKI IOS : Conception initiale et déploiement

Après la récupération/installation de certificat de CA, le client de PKI récupère les capacités de serveur de PKI avant d'exécuter une inscription. La récupération de capacités CA est expliquée dans cette section.

Capacités CA

Dans l'IOS, quand un client de PKI authentifie un CA, en d'autres termes, quand un administrateur crée un point de confiance sur un routeur IOS, et exécute le **<trustpoint-name> de crypto pki authenticate de** commande, ces événements ont lieu sur le routeur :

- L'IOS envoie une demande SCEP contenant le type d'exécution de GetCACert.
- La réponse prévue ici est un message de HTTP avec un type de contenu d'**application/x-x509-ca-cert** en cas de déploiement CA, ou **application/x-x509-ca-ra-cert** en cas de RA et de déploiement CA. Et le corps de HTTP contient le certificat de CA. [et un certificat de RA dans ce dernier cas,].
- Après la récupération et l'installation de certificat CA/RA, le client initie une demande automatique SCEP contenant l'exécution de GetCACaps.
- La réponse prévue ici est un message de HTTP avec un type de contenu d'**application/x-pki-message**, qui pourrait également être **texte/brute** et le corps de HTTP contient une gamme de capacités prises en charge par le CA, séparé par un caractère de retour à la ligne. Une réponse typique de serveur de PKI IOS est suivant les indications du diagramme ci-dessous.



La réponse est interprétée en tant que ceci par le client de PKI IOS :

```
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 ces capacités, ce document se concentre sur ces deux.

GetNextCACert

Quand cette capacité est retournée par le CA, l'IOS comprend que le CA prend en charge le renversement de certificat de CA. Cette capacité étant retourné, si la commande d'**auto-enroll** n'est pas configurée sous le point de confiance, l'IOS initialise un temporisateur de SHADOW réglé à 90% de la période de la validité de certificat CA.

Quand le temporisateur de SHADOW expire, l'IOS exécute l'exécution de GetNextCACert SCEP pour chercher le certificat de CA inversé.

> Remarque: Si la commande d'**auto-enroll** a été configurée sous le point de confiance avec un **URL d'inscription**, un temporisateur de RENOUVELER est initialisé même avant d'authentifier le point de confiance, et il essaye constamment de s'inscrire avec le CA situé à l'**URL d'inscription**, bien qu'aucun message réel d'inscription [CSR] ne soit envoyé jusqu'à ce que le point de confiance soit authentifié.

> Remarque: GetNextCACert est envoyé comme capacité par le serveur de PKI IOS même si l'**auto-rollover** n'est pas configuré au service

Renouvellement

Avec cette capacité, le serveur de PKI informe le client de PKI qu'elle peut employer un certificat actif d'ID pour signer une demande de signature de certificat de renouveler le certificat existant.

Plus sur ceci dans la section d'Automatique-**renouvellement de client de PKI**.

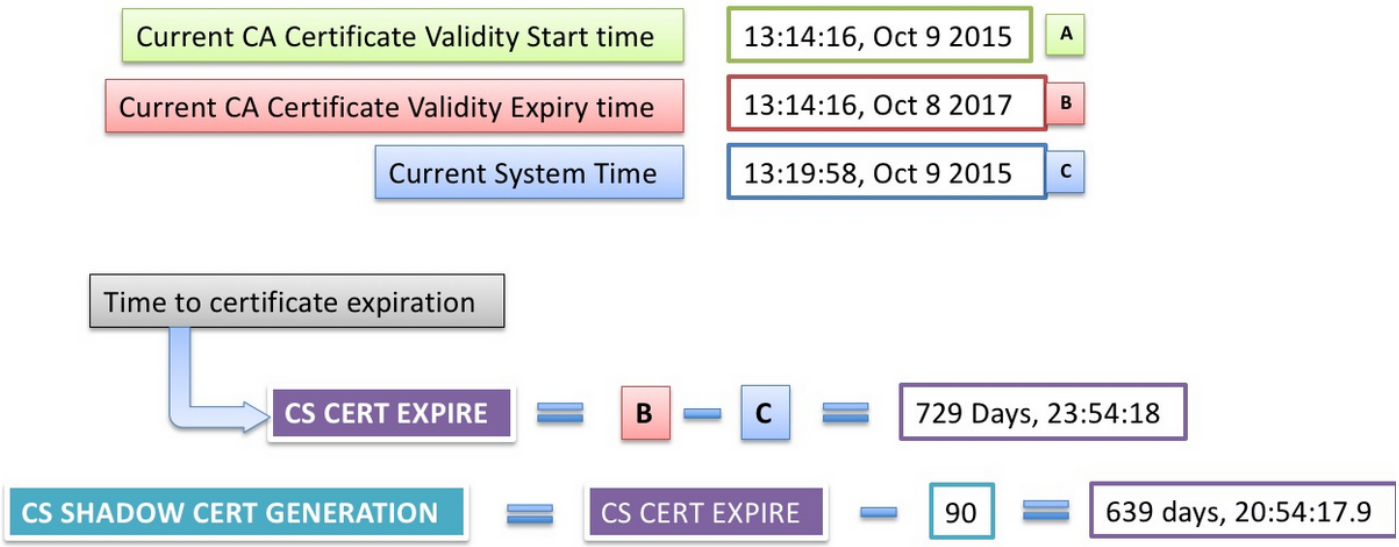
Auto-rollover de serveur de PKI

Avec la configuration ci-dessus sur le serveur CA, vous voyez :

```
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
```

Notez ceci :



Exécution inversée

Quand le temporisateur de **GÉNÉRATION de CERT de SHADOW de CS** expire :

- L'IOS génère une paire de clés inversée première – actuellement il a le même nom que la paire de clés active avec a # informations parasites ajoutées à lui.

```
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
```

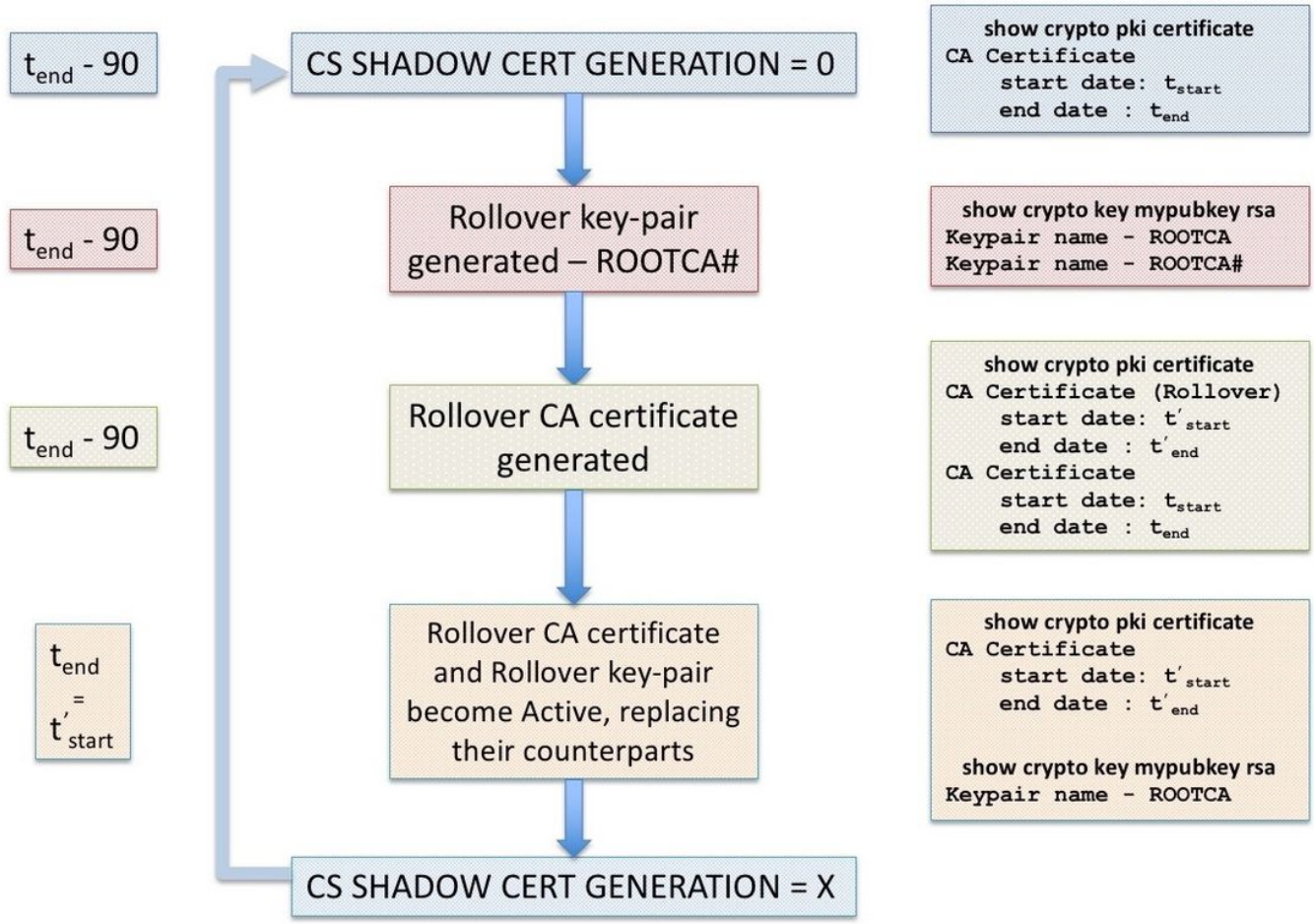
```
 F751D810 70CEA8C8 B0023B4B 0FB9A538 A1C118D3 5530D46D C4B4DC14 3BD1D231
 48B0C053 A781D0C7 86DEE9DE CCA58C18 B5804B29 911D1D57 76B3EC3F 42D38C3A
 1E0F8DD9 1DE228B9 95AC3C10 87C132FC 75956338 258727F6 1A1F0818 83020301 0001

% 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
```

- L'IOS génère alors le certificat de CA inversé, où la date de début de validité est identique que la date de fin de validité du certificat de CA actif en cours.

```
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
```



Manuel-renversement de serveur de PKI

Le serveur de PKI IOS prend en charge le renversement manuel du certificat de CA, c.-à-d. un administrateur peut déclencher la génération d'un certificat de CA inversé à l'avance sans devoir configurer l'auto-rollover **sous la** configuration du serveur de PKI. Il est fortement recommandé

pour configurer l'auto-rollover **si** on prévoit d'étendre la vie d'un serveur au commencement déployé CA pour être du côté plus sûr. PKICLIENTS **peut surcharger le CA sans certificat de CA inversé.** Référez-vous à l'exécution de SHADOW de client de Dependencyof sur le renversement de serveur de PKI.

Un renversement manuel peut être déclenché utilisant la commande de niveau de configuration :

```
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
```

Et aussi, un certificat de CA inversé peut être annulé pour générer frais manuellement, toutefois quelque chose un admin ne devrait pas faire dans un environnement de production, utilisation :

```
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
```

Ceci supprime la paire de clés de la RSA de renversement et le certificat de CA inversé. Ceci est informé contre parce que :

- Une fois que le CA génère le certificat inversé, les plusieurs clients peuvent télécharger le certificat de CA inversé aussi bien qu'un certificat client inversé signés par le certificat de CA inversé.
- Àce stade si le renversement est annulé, le client peut devoir re-être inscrit.

Automatique-renouvellement de client de PKI

Tape du renouvellement de certificat client - RENOUVELEZ et OMBRAGEZ

L'IOS sur le serveur de PKI veille toujours que l'échéance temps du certificat d'ID fourni au client ne dépasse jamais l'échéance temps du certificat de CA.

Sur un client de PKI, l'IOS prend en compte toujours les temporisateurs suivants avant de programmer l'exécution de renouvellement :

- Échéance temps du certificat d'identité étant renouvelé
- Échéance temps du certificat de l'émetteur (CA)

Si l'échéance temps du certificat d'identité n'est pas identique que l'échéance temps du certificat de CA, l'IOS exécute une exécution simple de renouvellement.

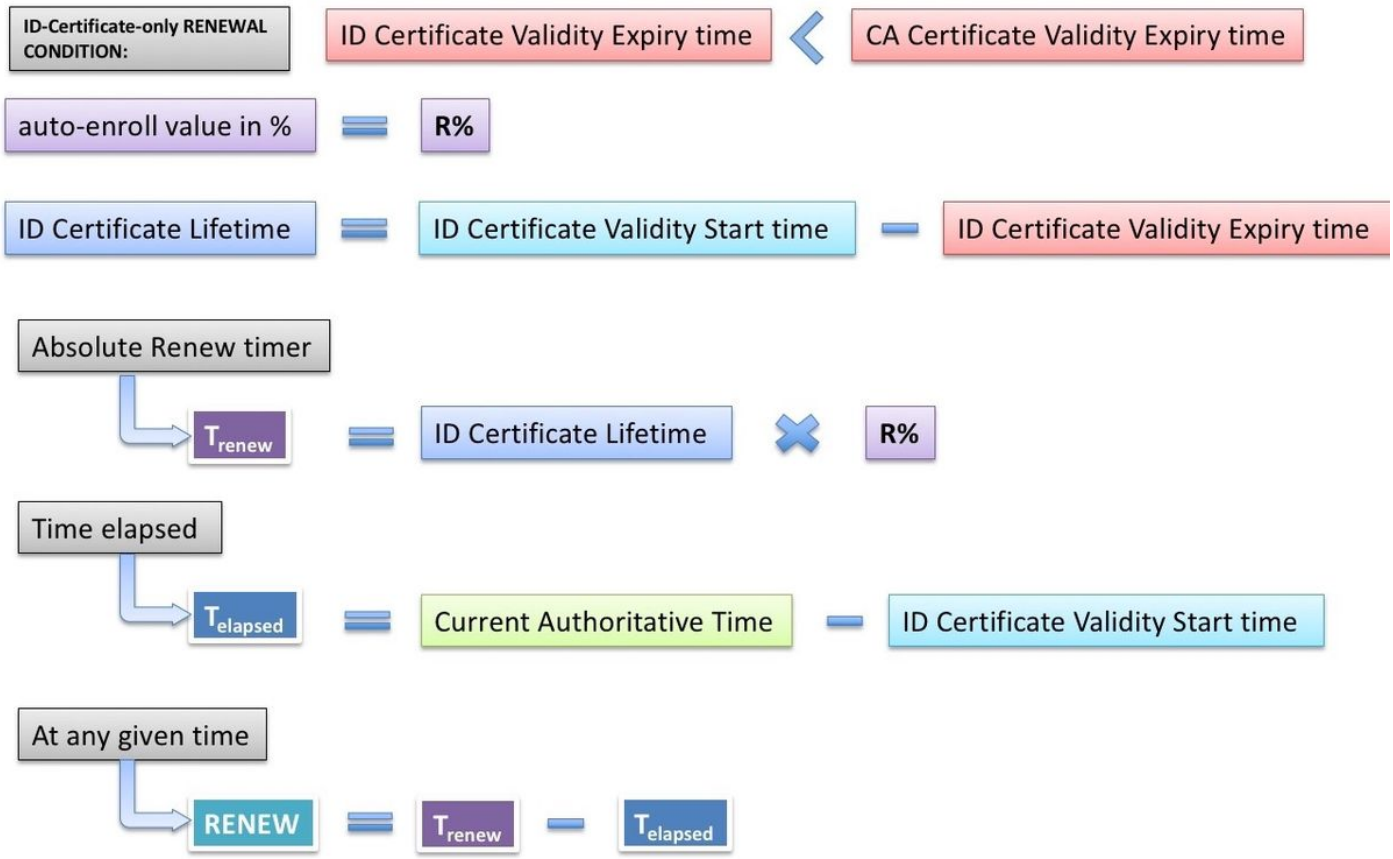
Si l'échéance temps du certificat d'identité est identique que l'échéance temps du certificat de CA,

l'IOS exécute une exécution de renouvellement de shadow.

RENOUVELEZ - Renouvellement de certificat d'identité de routeur

Comme indiqué précédemment, le client de PKI IOS exécute une exécution simple de renouvellement si l'échéance temps du certificat d'identité n'est pas identique que l'échéance temps du certificat de CA, en d'autres termes le certificat d'identité expirant avant que le certificat de l'émetteur déclenche un renouvellement simple du certificat d'identité.

Dès qu'un certificat d'identité sera installé, l'IOS calcule le temporisateur de RENOUVELER pour le confiance point spécifique comme affiché ci-dessous :

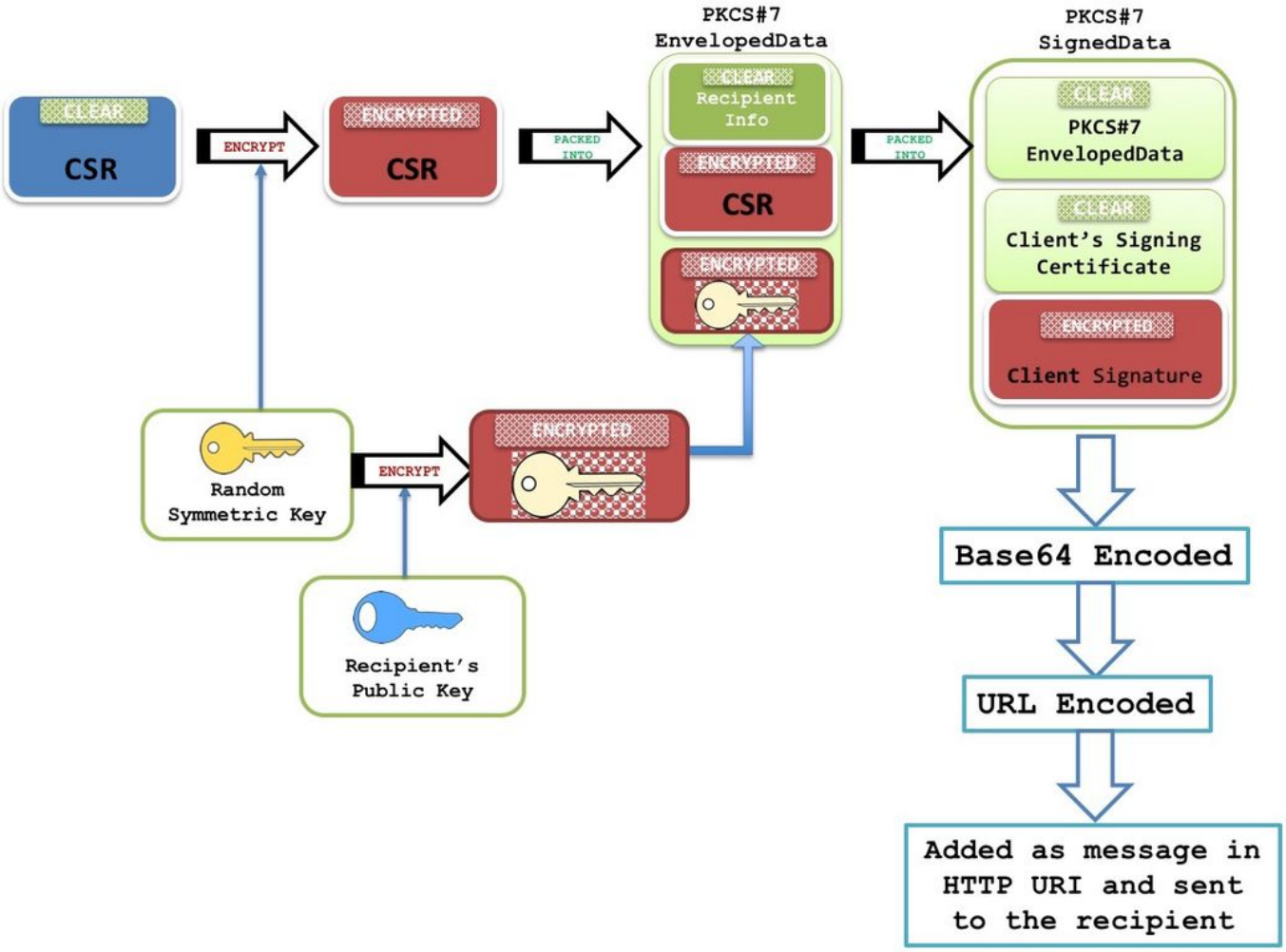


Le Courant-Bien fondé-Time signifie que l'horloge système doit être une source bien fondée de temps comme décrit ici. (lien à la section bien fondée de source temporelle) des temporisateurs de PKI ne seront pas initialisés sans source bien fondée de temps. Et par conséquent, l'exécution de renouvellement n'aura pas lieu.

Les événements suivants ont lieu quand RENOUVELEZ le temporisateur expire :

- L'IOS génère une paire de clés de shadow si le **régénéré** est configuré [exemple : régénéré de l'auto-enroll 80]. Sans **régénéré l'**IOS réutilise actuellement - la paire de clés RSA active.
- L'IOS crée une demande de certificat formatée par PKCS-10, qui est alors chiffrée dans une enveloppe PKCS-7. Cette enveloppe contient également le RecipientInfo, qui est le subject-name et le numéro de série du CA émettant. Ce PKCS7-envelope consécutivement est emballé dans des signer-données PKCS-7. Pendant l'inscription initiale, l'IOS emploie un certificat auto-signé pour signer ce message. Et pendant les inscriptions ultérieures, c.-à-d. les re-inscriptions, IOS emploie le certificat d'identité actif pour signer le message. Les

données signées par PKCS7 sont également incluses avec le certificat de signature, c.-à-d. l'un ou l'autre le certificat auto-signé ou le certificat d'identité.



Pour plus d'informations sur cette structure de paquet référez-vous au [document d'aperçu SCEP]

> Remarque: L'information principale ici est le RecipientInfo qui est le subject-name et le numéro de série du CA émettant, et la clé publique de ce CA est utilisée pour chiffrer la symétrique-clé. Le CSR dans l'enveloppe PKCS7 est chiffré utilisant cette symétrique-clé.

Cette symétrique-clé chiffrée est déchiffrée par le CA de réception utilisant sa clé privée, et cette symétrique-clé est utilisée pour déchiffrer l'enveloppe PKCS7 indiquant le CSR.

- Cette demande de signature de certificat (CSR) emballée dans le format PKCS7 est alors envoyée au CA avec un type de message SCEP de PKCSReq et une exécution SCEP appelée PKIOperation.
- Si le CA rejette la demande, l'IOS arrête le temporisateur de RENOUVELER. À partir de là, pour renouveler le certificat d'identité, l'administrateur doit exécuter un renouvellement manuel (le lien à la section de Manuel-**renouvellement de client de PKI**)
- Si le CA envoie un état SCEP comme **en suspens**, l'IOS sur le client de PKI met en marche un temporisateur de BALAYAGE démarrer à 60 secondes ou à 1 minute. Chaque fois qu'un temporisateur de BALAYAGE expire, l'IOS envoie le message de GetCertInitial SCEP par une exécution de PKIOperation. Quand le premier temporisateur de BALAYAGE expire, si le message de GetCertInitial est répondu à avec un état en attendant SCEP, un algorithme de

ré-émission temporisée exponentielle place le premier retry interval de temporisateur de BALAYAGE à 1 minute, le deuxième retry interval de temporisateur de BALAYAGE à 2 minutes, le troisième retry interval de temporisateur de BALAYAGE à 4 minutes et ainsi de suite pour les 999 prochaines relances par défaut ou jusqu'à ce que le certificat de CA émettant expire.

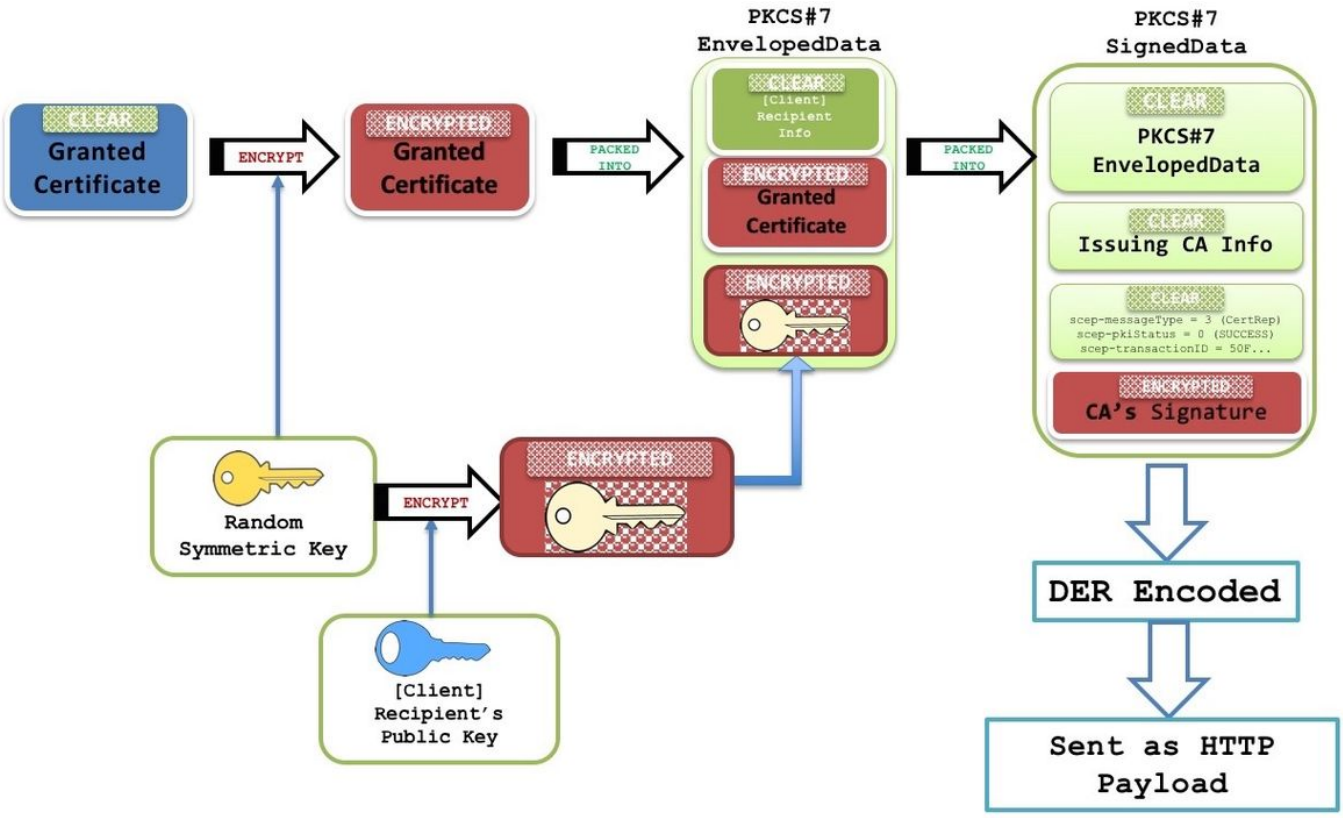
Le compte de balayage et la première période de relance peuvent être configurés utilisant :

```
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
```

- Quand on accorde le certificat sur le serveur de PKI, le prochain message de GetCertInitial SCEP est répondu à avec un message de HTTP du type satisfait **application/x-pki-message** et d'un corps contenant des données signées par PKCS#7 signées. Ces données signées par PKCS7 contiennent l'état SCEP sous forme d'**accordé**, et également un PKCS7 a enveloppé des données. Ces données enveloppées par PKCS contiennent le certificat accordé et le RecipientInfo, qui est le subject-name et le numéro de série du certificat auto-signé pendant l'inscription initiale et du certificat d'identité actif pendant les re-inscriptions.

  Les données enveloppées par PKCS7 contiennent également une clé symétrique chiffrée avec la clé publique du destinataire (pour ce que le nouveau certificat a été accordé). Le

routeur récepteur le déchiffre utilisant la clé privée. Cette clé symétrique claire est alors utilisée pour déchiffrer les données enveloppées par PKCS#7, indiquant le nouveau certificat d'identité.



- Àce stade, l'IOS remplace le certificat d'identité existant par le nouveau certificat immédiatement. Et si le **régénéré** était configuré, la paire de clés de shadow remplace la paire de clés active aussi bien.
- En outre, la date de fin du nouveau certificat est comparée à la date de fin du certificat de CA pour déterminer si RENOUVELEZ le temporisateur doit être initialisé ou un temporisateur de SHADOW doit être initialisé comme expliqué ici les **types de** <href de **renouvellement de certificat client - RENOUVELEZ et SHADOW>**