Guide de déploiement de l'ICP IOS : Transfert de certificat - Vue d'ensemble de la configuration et de l'opération

Contenu

Introduction

Ce document décrit en détail le transfert de certificat sur les serveurs et les clients de l'infrastructure à clé publique (PKI) de Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

le logiciel Cisco IOS

- IOS
  - Pour ISR-G1 - Dernière version 15.1(4)M*
  - Pour ISR-G2 - Dernière version 15.4(3)M
- IOS-XE
  - XE 3.15 ou 15.5(2)S

Note: La maintenance logicielle générale des périphériques ISR n'est plus active, les correctifs de bogues ou les améliorations de fonctionnalités futurs nécessiteront une mise à niveau matérielle vers les routeurs de la gamme ISR-2 ou ISR-4xxx.

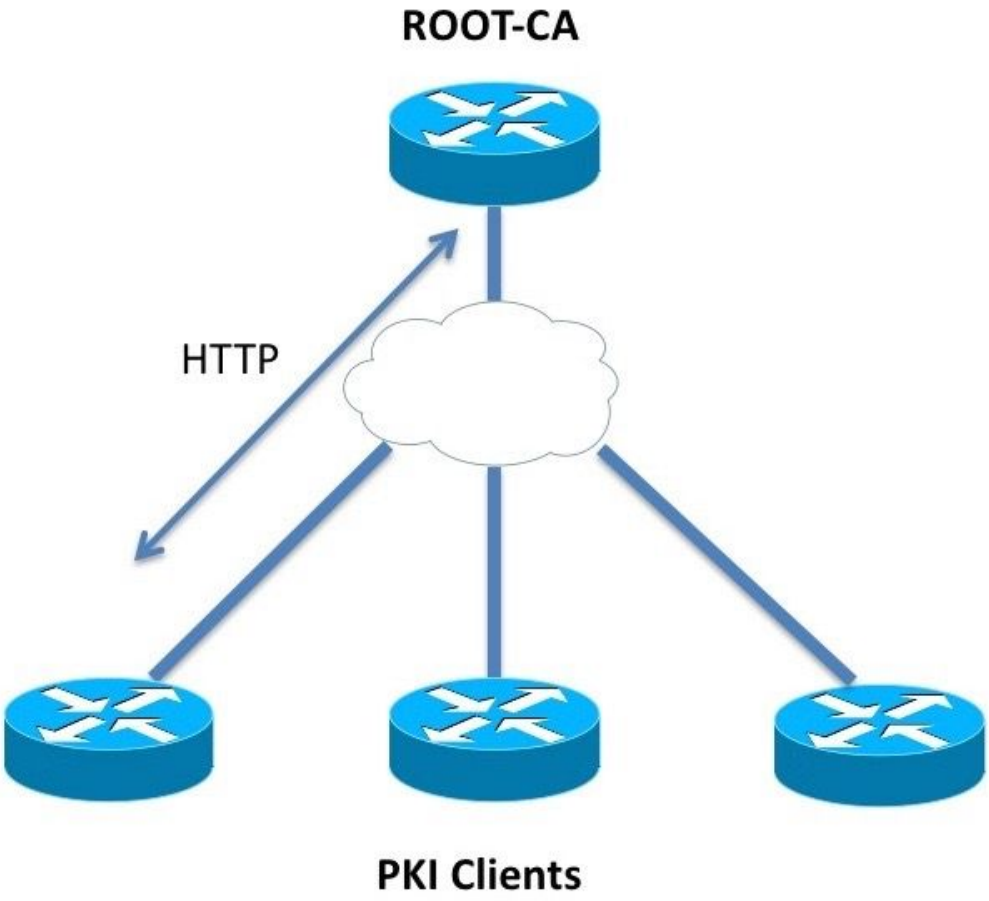
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le transfert de certificat, également appelé opération de renouvellement, garantit que lorsqu'un certificat expire, un nouveau certificat est prêt à prendre le relais. Du point de vue d'un serveur PKI, cette opération implique la génération du nouveau certificat de renversement de serveur bien

à l'avance pour s'assurer que tous les clients PKI ont reçu un nouveau certificat de renversement de client signé par le nouveau certificat de renversement de serveur avant l'expiration du certificat actuel. Du point de vue d'un client PKI, si le certificat client expire mais que le certificat du serveur de l'autorité de certification (AC) ne l'est pas, le client demande un nouveau certificat et remplace l'ancien certificat dès la réception du nouveau certificat, et si le certificat client expire en même temps que le certificat du serveur AC, le client s'assure de recevoir d'abord le certificat de substitution du serveur AC, puis il demande un transfert certificat signé par le nouveau certificat de substitution de serveur AC, et les deux seront activés lorsque les anciens certificats expireront.

Configuration



Configuration requise pour l'ICP et le protocole SCEP (Simple Ceritificate Enrollment Protocol)

Source temporelle autorisée

Dans IOS, par défaut, la source d'horloge est considérée comme non autorisée, car l'horloge matérielle n'est pas la meilleure source de temps. PKI étant sensible au temps, il est important de configurer une source de temps valide à l'aide de NTP. Dans un déploiement PKI, il est

recommandé que tous les clients et le serveur synchronisent leur horloge sur un seul serveur NTP, via plusieurs serveurs NTP si nécessaire. Plus d'informations à ce sujet sont expliquées dans le Guide de déploiement de l'ICP IOS : Conception et déploiement initiaux

IOS n'initialise pas les compteurs PKI sans horloge faisant autorité. Bien que NTP soit fortement recommandé, à titre de mesure temporaire, l'administrateur peut marquer l'horloge matérielle comme faisant autorité en utilisant :

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

Communication HTTP

Un serveur ICP IOS actif est requis par le serveur HTTP, qui peut être activé à l'aide de cette commande de niveau de configuration :

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

Cette commande active le serveur HTTP sur le port 80 par défaut, qui peut être modifié comme indiqué ci-dessus.

Les clients PKI doivent pouvoir communiquer avec le serveur PKI via HTTP au port configuré.

Configuration PKI

Serveur - Renvoi

La configuration automatique de transfert du serveur 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 de substitution automatique est défini en jours. À un niveau plus précis, la commande ressemble à :

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

Une valeur de substitution automatique de 90 indique que l'IOS crée un certificat de serveur de substitution 90 jours avant l'expiration du certificat de serveur actuel et que la validité de ce nouveau certificat de substitution commence en même temps que l'expiration du certificat actif actuel.

Le transfert automatique doit être configuré avec une valeur telle que le certificat d'autorité de certification de transfert soit généré bien à l'avance sur le serveur PKI avant que n'importe quel client PKI du réseau n'effectue l'opération GetNextCACert comme décrit dans la section **Vue d'ensemble de l'opération SHADOW** ci-dessous.

Client - Renouvellement

La configuration de renouvellement automatique de certificat du client 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, la commande **auto-enroll <pourcentage> [régénération]** indique que IOS doit effectuer le renouvellement du certificat à 80 % exactement de la durée de vie du certificat actuel.

Le mot clé **régénération** indique qu'IOS doit régénérer la paire de clés RSA connue sous le nom de paire de clés cachées lors de chaque opération de renouvellement de certificat.

Soyez prudent lors de la configuration du pourcentage d'inscription automatique. Sur un client PKI donné dans le déploiement, si une condition se produit lorsque le certificat d'identité expire en même temps que le certificat d'autorité de certification émetteur, la valeur d'inscription automatique doit toujours déclencher l'opération de renouvellement [shadow] après que l'autorité de certification a créé le certificat de substitution. *Reportez-vous à la* section **Dépendances du temporisateur PKI** dans les exemples de déploiement.

Conditions préalables au renouvellement/transfert de l'ICP

Ce document traite en détail des opérations de transfert et de renouvellement de certificat et, par conséquent, ces événements sont considérés comme ayant réussi :

- Initialisation du serveur PKI avec un certificat CA valide.
- Les clients PKI ont été correctement inscrits au serveur PKI. Par exemple, chaque client PKI possède le certificat CA et un certificat d'identité, c'est-à-dire le certificat de routeur.

L'inscription d'un client implique ces événements. Sans trop entrer dans les détails :

- Authentification Trustpoint
- Inscription à Trustpoint

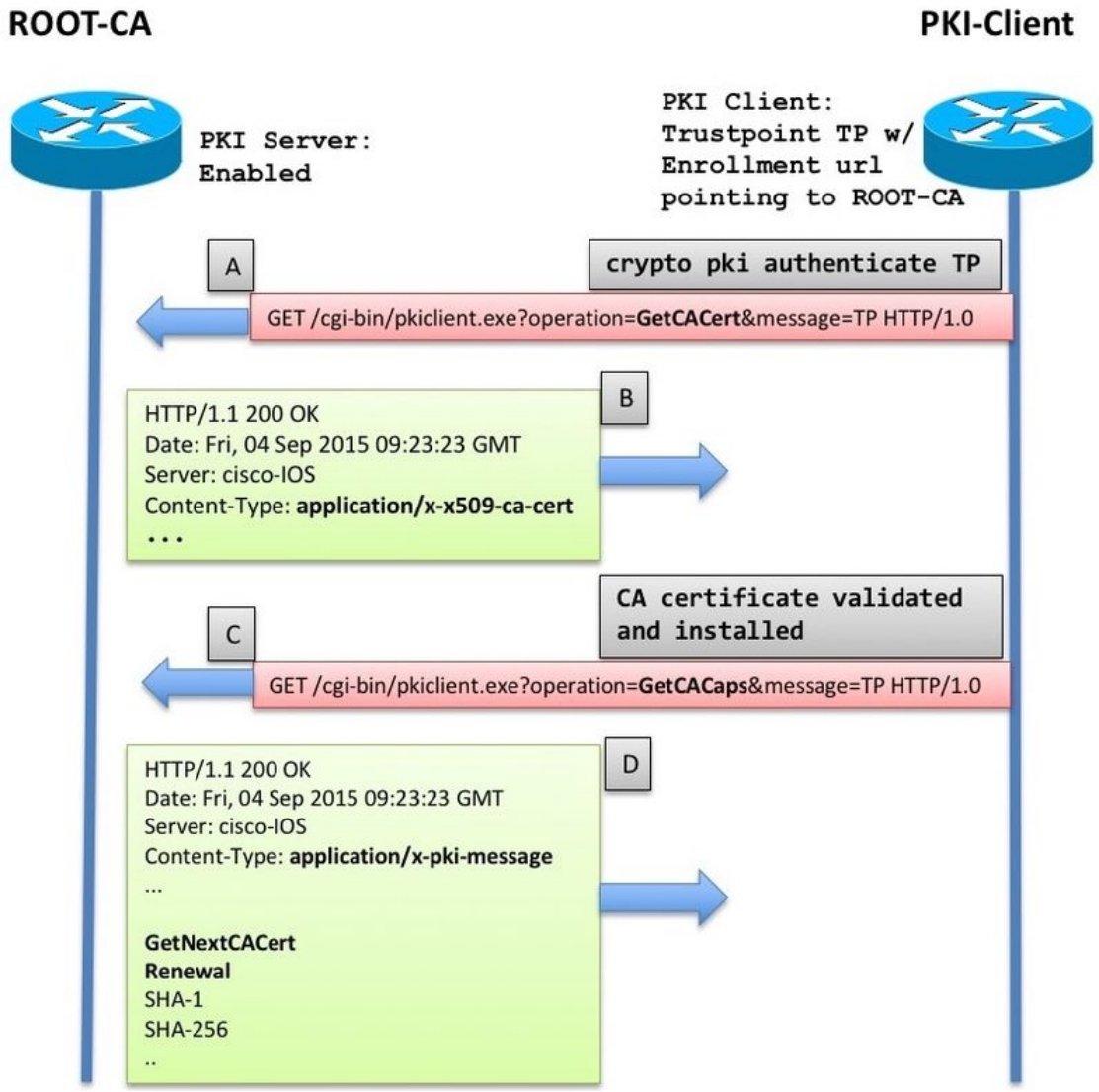
Dans IOS, un point de confiance est un conteneur de certificats. Tout point de confiance donné peut contenir un certificat d'identité actif et/ou un certificat d'autorité de certification actif. Un point de confiance est considéré comme authentifié s'il contient un certificat CA actif. Et il est considéré comme inscrit s'il contient un certificat d'identité. Un point de confiance doit être authentifié avant une inscription. La configuration du serveur et du client PKI, ainsi que l'authentification et l'inscription des points de confiance sont traitées en détail dans le Guide de déploiement de l'ICP IOS : Conception et déploiement initiaux

Après avoir récupéré/installé le certificat de l'autorité de certification, le client PKI récupère les capacités du serveur PKI avant d'effectuer une inscription. La récupération des capacités de l'autorité de certification est expliquée dans cette section.

Capacités CA

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

- IOS envoie une requête SCEP contenant le type d'opération GetCACert.
- La réponse attendue ici est un message HTTP avec un type de contenu d'**application/x-x509-ca-cert** en cas de déploiement d'autorité de certification, ou **application/x-x509-ca-ra-cert** en cas de déploiement d'autorité de certification et d'autorité de certification. Et le corps HTTP contient le certificat CA. [et un certificat RA dans ce dernier cas].
- Après la récupération et l'installation du certificat CA/RA, le client lance une demande SCEP automatique contenant l'opération GetCACaps.
- La réponse attendue ici est un message HTTP avec un type de contenu d'**application/x-pki-message**, qui peut également être **texte/clair** et le corps HTTP contient une série de fonctionnalités prises en charge par l'autorité de certification, séparées par un caractère de flux de ligne. Une réponse typique du serveur ICP IOS est présentée dans le schéma ci-dessous.



La réponse est interprétée comme ceci par le client ICP IOS :

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
```

```
CA_CAP_SHA_1
CA_CAP_SHA_256
```

Parmi ces capacités, le présent document porte sur ces deux aspects.

GetNextCACert

Lorsque cette fonctionnalité est renvoyée par l'autorité de certification, IOS comprend que l'autorité de certification prend en charge le transfert de certificat CA. Avec cette fonctionnalité retournée, si la commande **auto-enroll** n'est pas configurée sous le point de confiance, IOS initialise un temporisateur SHADOW défini à 90 % de la période de validité du certificat CA.

Lorsque le minuteur SHADOW expire, IOS exécute l'opération GetNextCACert SCEP pour récupérer le certificat de l'autorité de certification de renversement.

> **Remarque** : si la commande **auto-enroll** a été configurée sous le trustpoint avec une **url d'inscription**, un minuteur RENEW est initialisé avant même d'authentifier le trustpoint, et il tente constamment de s'inscrire auprès de l'autorité de certification située à l'**url d'inscription**, bien qu'aucun message d'inscription réel [truR] ne soit envoyé jusqu'authentification.

> **Note**: GetNextCACert est envoyé en tant que fonctionnalité par le serveur ICP IOS même si le **basculement automatique** n'est pas configuré sur le serveur

Renouvellement

Grâce à cette fonctionnalité, le serveur PKI informe le client PKI qu'il peut utiliser un certificat d'ID actif pour signer une demande de signature de certificat pour renouveler le certificat existant.

Pour en savoir plus, consultez la section **Renouvellement automatique du client PKI** .

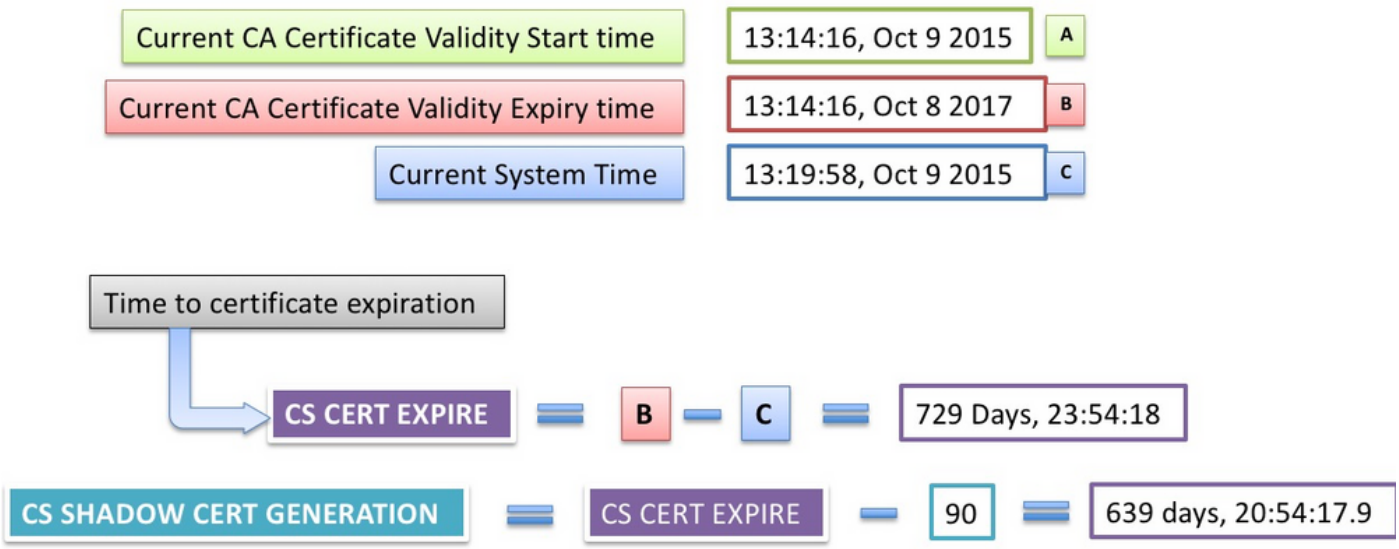
Transfert automatique du serveur PKI

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

```
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
```

Notez ceci :



Opération de substitution

Lorsque le minuteur **CS SHADOW CERT GENERATION** expire :

- IOS génère d'abord une paire de clés à paires inversées. Actuellement, elle porte le même nom que la paire de clés active à laquelle un hachage # est ajouté.

```
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
```

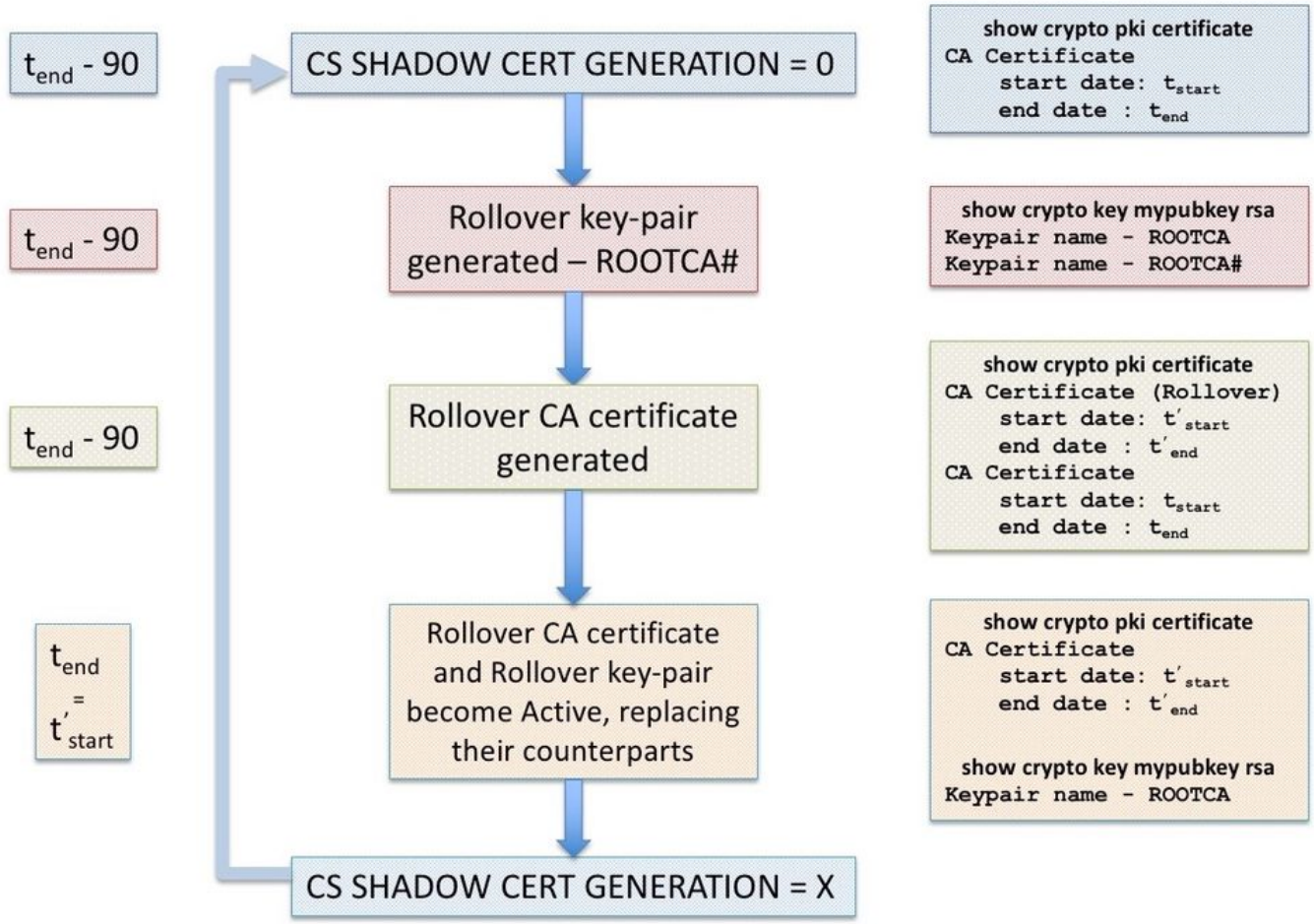
- IOS génère ensuite le certificat d'autorité de certification de substitution, où la date de début de validité est identique à la date de fin de validité du certificat d'autorité de certification actif actuel.

```
    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
```



Transfert manuel du serveur PKI

IOS PKI Server prend en charge le renversement manuel du certificat d'autorité de certification, c'est-à-dire qu'un administrateur peut déclencher la génération d'un certificat d'autorité de certification de renversement à l'avance sans avoir à configurer le **renversement automatique** sous la configuration du serveur PKI. Il est fortement recommandé de configurer le **transfert automatique**, que l'on envisage ou non de prolonger la durée de vie d'un serveur AC initialement déployé pour qu'il soit plus sûr. **Les clients PKI peuvent surcharger l'autorité de certification sans certificat d'autorité de certification inversé**. *Référez-vous à* Dépendance de l'opération SHADOW du client sur le basculement du serveur PKI.

Un basculement manuel peut être déclenché à l'aide de la commande configuration level :

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

De plus, un certificat CA à paires inversées peut être annulé pour en générer un nouveau

manuellement. Toutefois, un administrateur ne doit pas faire quelque chose dans un environnement de production, en utilisant :

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

Cette opération supprime la paire de clés rsa inversée et le certificat CA inversé. Il est déconseillé de le faire car :

- Une fois que l'autorité de certification génère le certificat de substitution, plusieurs clients peuvent télécharger le certificat d'autorité de certification de substitution ainsi qu'un certificat de client de substitution signé par le certificat d'autorité de certification de substitution.
- Àce stade, si le transfert est annulé, le client devra peut-être être réinscrit.

Renouvellement automatique du client PKI

Types de renouvellement de certificat client - RENOUVEAU et SHADOW

IOS sur le serveur PKI s'assure toujours que le délai d'expiration du certificat d'ID émis au client ne dépasse jamais le délai d'expiration du certificat d'autorité de certification.

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

- Heure d'expiration du renouvellement du certificat d'identité
- Heure d'expiration du certificat de l'émetteur (CA)

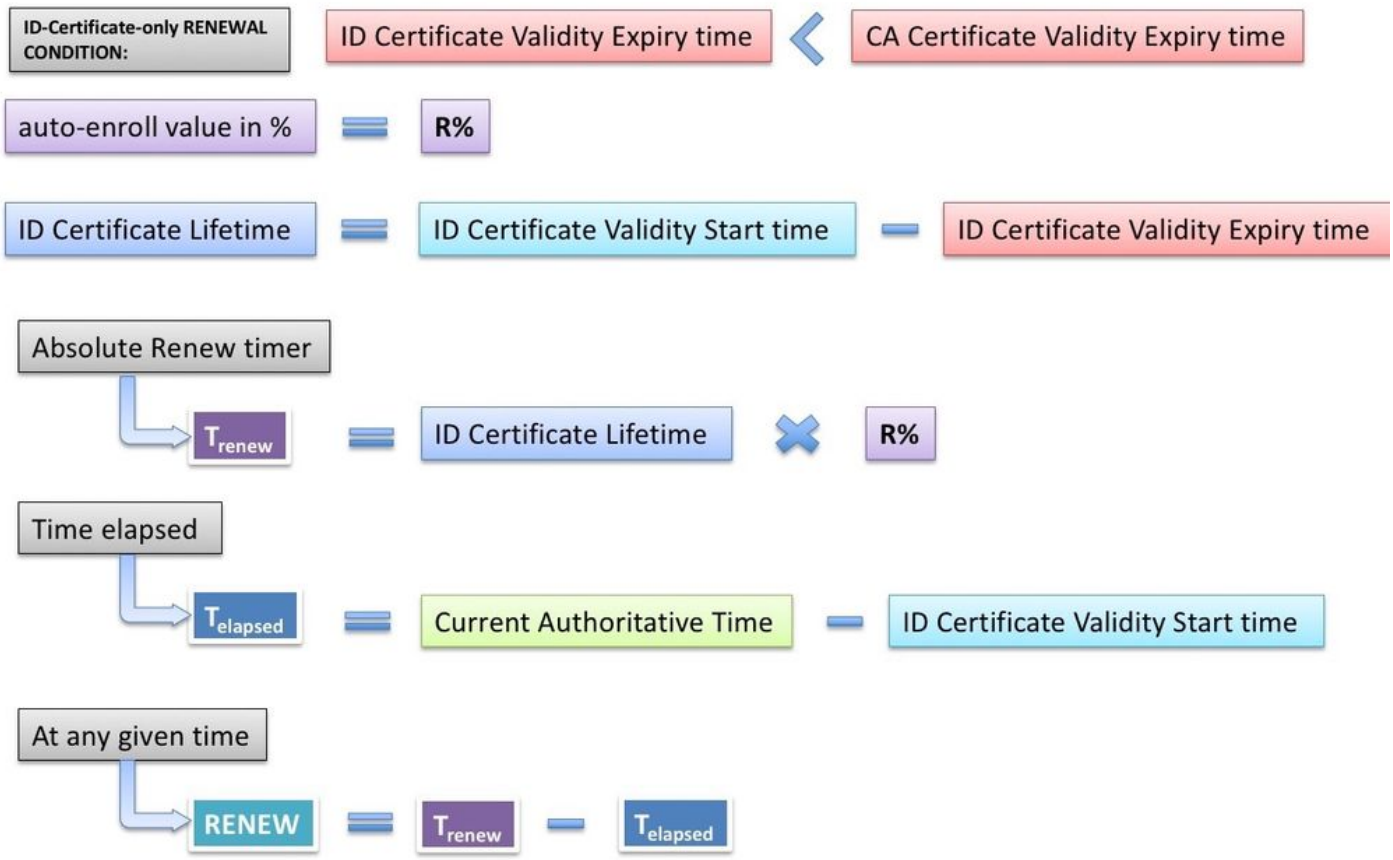
Si le délai d'expiration du certificat d'identité n'est pas le même que le délai d'expiration du certificat d'autorité de certification, IOS effectue une opération de renouvellement simple.

Si le délai d'expiration du certificat d'identité est le même que le délai d'expiration du certificat d'autorité de certification, IOS effectue une opération de renouvellement instantané.

RENOUVEAU - Renouvellement du certificat d'identité du routeur

Comme mentionné précédemment, le client ICP IOS effectue une opération de renouvellement simple si le délai d’expiration du certificat d’identité n’est pas le même que le délai d’expiration du certificat d’AC, c’est-à-dire que le certificat d’identité expirant avant que le certificat de l’émetteur ne déclenche un renouvellement simple du certificat d’identité.

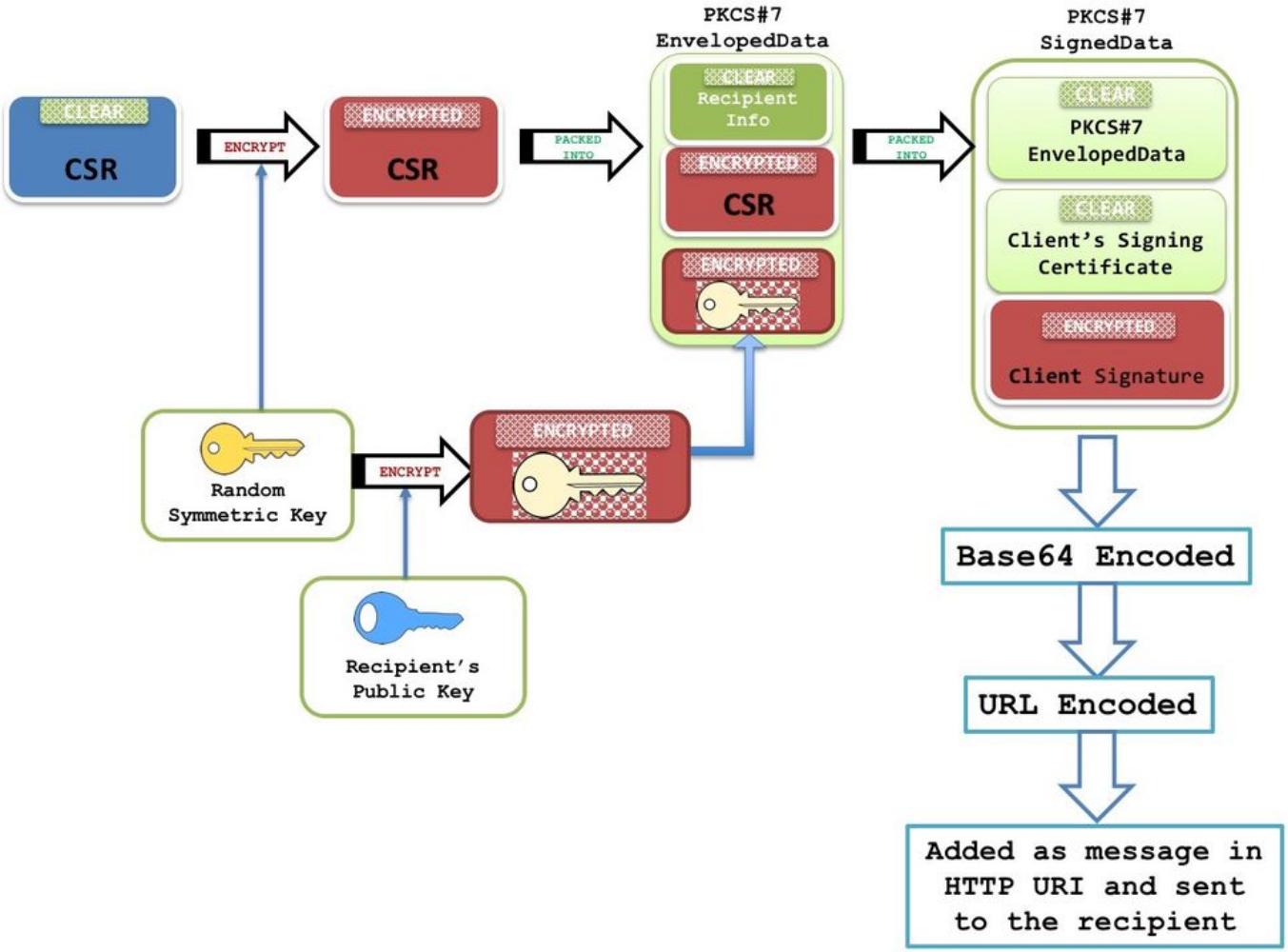
Dès qu'un certificat d'identité est installé, IOS calcule le compteur RENEW pour le point d'approbation spécifique comme indiqué ci-dessous :



Current-Authoritative-Time signifie que l'horloge système doit être une source de temps faisant autorité, comme décrit ici. (lien vers la section source temporelle faisant autorité) Les temporisateurs PKI ne seront pas initialisés sans une source temporelle faisant autorité. Et par conséquent, l'opération de renouvellement n'aura pas lieu.

Les événements suivants se produisent à l'expiration du compteur RENEW :

- IOS génère une paire de clés cachées si **la régénération** est configurée [exemple : auto-enroll 80 regénérer]. Sans **régénérer** IOS, il réutilise la paire de clés RSA active.
- IOS crée une demande de certificat formatée PKCS-10, qui est ensuite cryptée dans une enveloppe PKCS-7. Cette enveloppe contient également les informations sur le destinataire, qui sont le nom du sujet et le numéro de série de l'autorité de certification émettrice. Cette enveloppe PKCS7 est à son tour conditionnée en données signées PKCS-7. Au cours de l'inscription initiale, IOS utilise un certificat auto-signé pour signer ce message. Et lors des inscriptions suivantes, c'est-à-dire des réinscriptions, IOS utilise le certificat d'identité actif pour signer le message. Les données signées PKCS7 sont également intégrées au certificat de signature, c'est-à-dire au certificat auto-signé ou au certificat d'identité.



Pour plus d'informations sur cette structure de paquets, reportez-vous au [document de présentation SCEP]

> **Note**: Les informations de clé ici sont le RecipientInfo qui est le nom du sujet et le numéro de série de l'autorité de certification émettrice, et la clé publique de cette autorité de certification est utilisée pour chiffrer la clé symétrique. Le CSR de l'enveloppe PKCS7 est chiffré à l'aide de cette clé symétrique.

Cette clé symétrique cryptée est déchiffrée par l'autorité de certification réceptrice à l'aide de sa clé privée, et cette clé symétrique est utilisée pour déchiffrer l'enveloppe PKCS7 révélant la CSR.

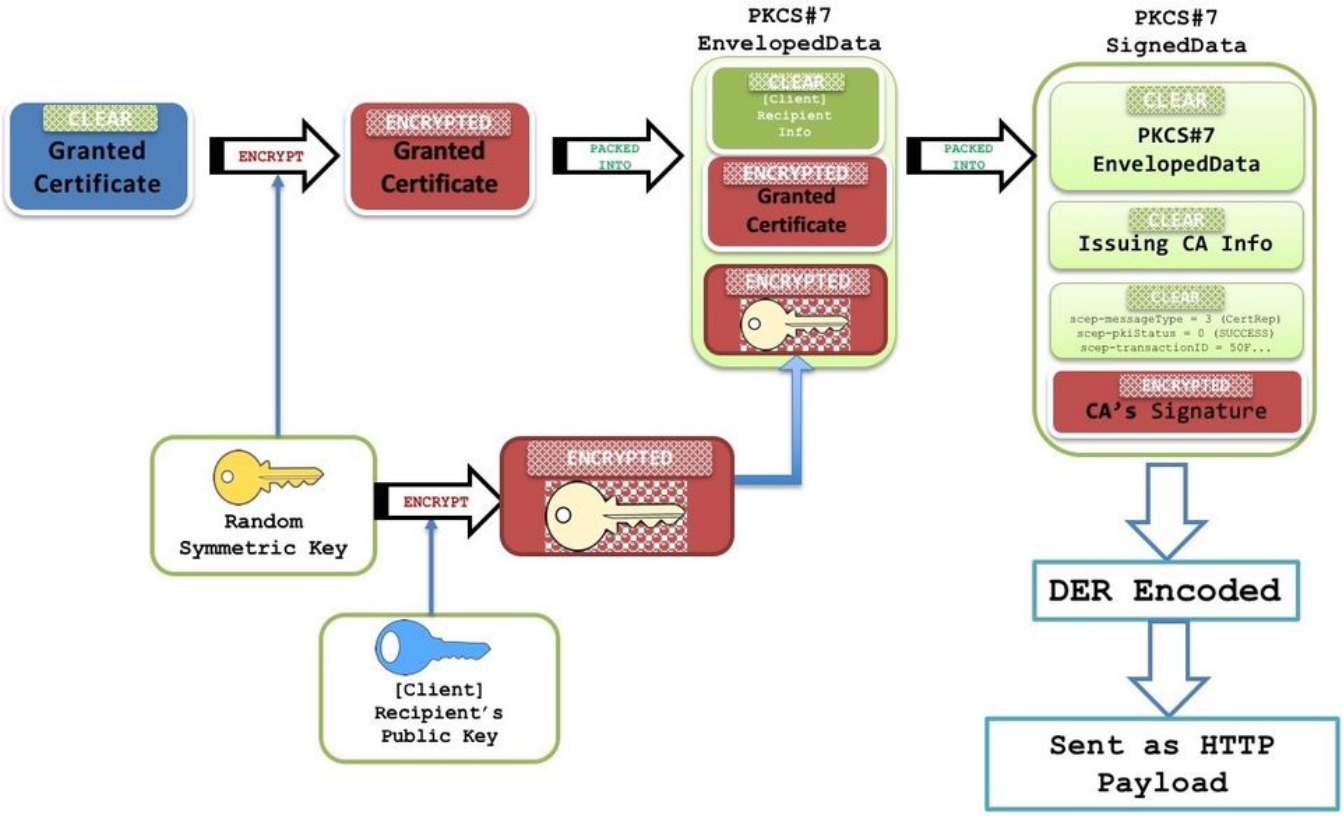
- Cette demande de signature de certificat (CSR) emballée au format PKCS7 est ensuite envoyée à l'AC avec un type de message SCEP de PKCSReq et une opération SCEP appelée PKIOperation.
- Si l'autorité de certification rejette la demande, IOS arrête le compteur RENEW. À partir de ce moment, pour renouveler le certificat d'identité, l'administrateur doit effectuer un renouvellement manuel (lien vers la section **Renouvellement manuel du client PKI**)
- Si l'autorité de certification envoie un état SCEP comme **en attente**, IOS sur le client PKI démarre un compteur de POLL à partir de 60 secondes ou 1 minute. Chaque fois qu'un minuteur de POLL expire, IOS envoie un message GetCertInitial SCEP via une opération PKIOperation.Lorsque le premier minuteur de POLL expire, si le message GetCertInitial reçoit une réponse avec un état SCEP En attente, un algorithme de désactivation exponentiel définit le premier intervalle de temporisation de POLL à 1 minute, le deuxième intervalle de

temporisation à 2 minutes, le troisième. intervalle de nouvelle tentative du temporisateur à 4 minutes, etc., pour les 999 prochaines tentatives par défaut ou jusqu'à l'expiration du certificat de l'autorité de certification émettrice.
Le nombre d'interrogations et la première période de nouvelle tentative peuvent être configurés à l'aide des éléments suivants :

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

- Lorsque le certificat est accordé sur le serveur PKI, le prochain message GetCertInitial SCEP reçoit une réponse avec un message HTTP de type **application/x-pki-message** et un corps contenant des données signées PKCS#7. Ces données signées PKCS7 contiennent l'état SCEP comme **Granted**, ainsi qu'une donnée enveloppée PKCS7. Ces données enveloppées PKCS contiennent le certificat accordé et les informations sur le destinataire, qui sont le nom du sujet et le numéro de série du certificat auto-signé lors de l'inscription initiale et du certificat d'identité actif lors des réinscriptions.

  Les données enveloppées PKCS7 contiennent également une clé symétrique chiffrée avec la clé publique du destinataire (pour laquelle le nouveau certificat a été accordé). La réception du routeur le déchiffre à l'aide de la clé privée. Cette clé symétrique claire est ensuite utilisée pour déchiffrer les données enveloppées PKCS#7, révélant le nouveau certificat d'identité.



- Àce stade, IOS remplace immédiatement le certificat d'identité existant par le nouveau certificat. Et si **la régénération** a été configurée, la paire de clés cachées remplace également la paire de clés active.

- En outre, la date de fin du nouveau certificat est comparée à la date de fin du certificat CA

pour déterminer si le compteur RENEW doit être initialisé ou si un compteur SHADOW doit être initialisé comme expliqué ici <href **Types de renouvellement de certificat client - RENEW et SHADOW>**