دليل نشر IOS PKI: إعادة توجيه الشهادة - نظرة عامة على التكوين والتشغيل

المحتويات

المقدمة

يصف هذا المستند تمرير الشهادة على خوادم وعملاء Cisco IOS للبنية الأساسية للمفاتح العام (PKI) بالتفصيل.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

الأجهزة

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

البرنامج

- IOS
  - ل ISR-G1 - الأحدث 15.1(4)M*
  - ل ISR-G2 - الأحدث 15.4(3)M
- IOS-XE
  - XE 3.15 وأ 15.5(2)S

ملاحظة: لم تعد صيانة البرامج العامة لأجهزة ISR نشطة، سيتطلب أي عمليات إصلاح للأخطاء وأ تحسينات للميزات في المستقبل ترقية الأجهزة إلى موجهات سلسلة ISR-2 وأ ISR-4xxx.

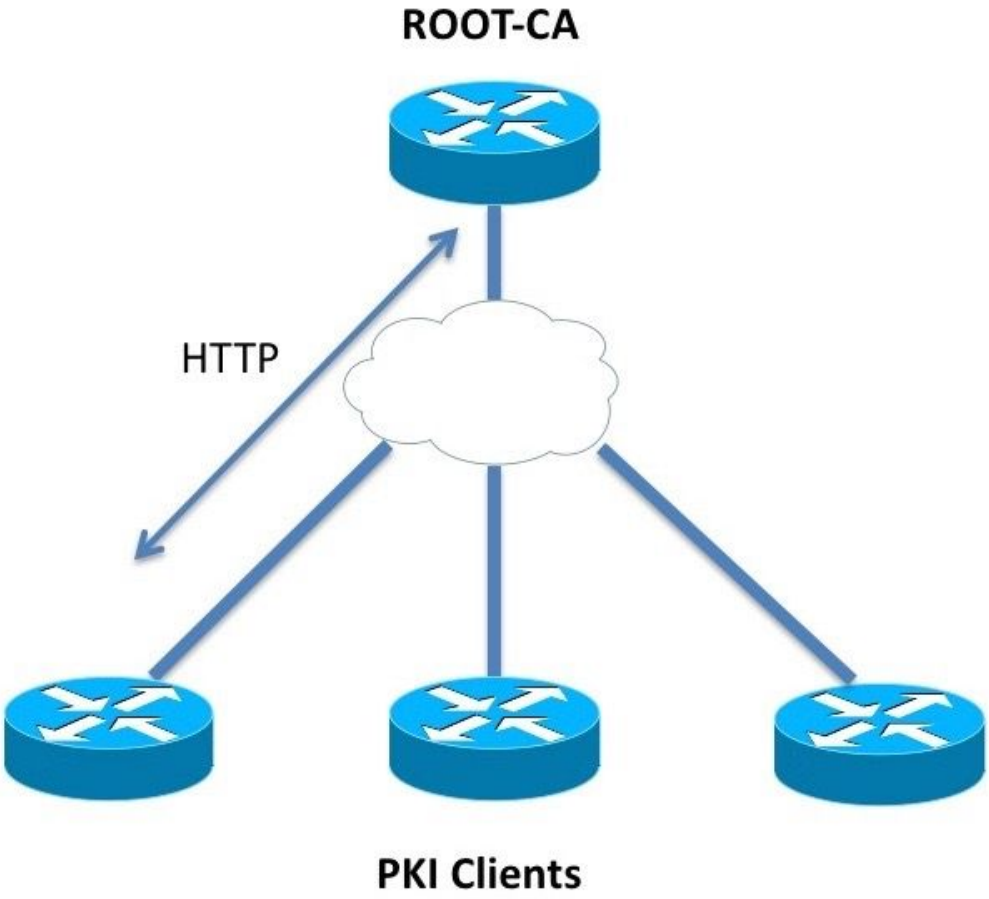
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتضمن عملية إعادة توجيه الشهادة المعروفة أيضا بعملية التجديد أنه عندما تنتهي صلاحية الشهادة، تكون الشهادة الجديدة جاهزة لتولي المهمة. من وجهة نظر خادم PKI، تتضمن هذه العملية إنشاء شهادة إعادة توجيه الخادم الجديدة بشكل مسبق للتأكد من أن جميع عملاء PKI قد تلقوا شهادة إعادة توجيه جديدة موقعة من قبل شهادة إعادة توجيه عميل جديدة قبل انتهاء صلاحية الشهادة الحالية. من وجهة نظر عميل PKI، إذا كانت شهادة الخادم الجديدة غير موجودة، يطلب العميل شهادة جديدة ولكن شهادة خادم مرجع الشهادات (CA) تبقى كما هي، وإذا كانت شهادة العميل الجديدة مطلوبة، يستبدل الشهادة القديمة بمجرد إستلام الشهادة الجديدة،

تنتهي في نفس وقت شهادة خادم CA، يتأكد العميل من تلقي شهادة إعادة توجيه خادم CA أولا، ثم يطلب شهادة إعادة توجيه موقعة بشهادة إعادة توجيه خادم CA الجديدة، وسيتم تنشيط كليهما عند انتهاء صلاحية الشهادات القديمة.

إعداد



متطلبات بروتوكول التسجيل البسيط (SCEP) ل PKI

مصدر الوقت المخول

في IOS، يعتبر مصدر الساعة غير موثوق به بشكل افتراضي نظرا لأن ساعة الأجهزة ليست أفضل مصدر للوقت. بما أن PKI حساس للوقت، فمن المهم تكوين مصدر وقت صالح باستخدام NTP. في نشر PKI، من المستحسن أن يقوم جميع العملاء والخادم بمزامنة الساعة مع خادم NTP واحد، من خلال خوادم NTP المتعددة إذا لزم الأمر. ويشرح المزيد حول هذا الأمر في دليل نشر IOS PKI: التصميم الأولي والنشر

ال يقوم IOS بتهيئة وحدات توقيت PKI بدون ساعة موثوق بها. على الرغم من أنه يوصى بشدة باستخدام بروتوكول وقت الشبكة (NTP)، إلا أنه يمكن للمسؤول وضع علامة على ساعة الأجهزة كموثوق بها باستخدام:

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

اتصال HTTP

متطلب لخادم IOS PKI نشط وهو خادم HTTP، والذي يمكن تمكينه باستخدام الأمر config-level هذا:

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

يقوم هذا الأمر بتمكين خادم HTTP على المنفذ 80 بشكل افتراضي، والذي يمكن تغييره أعلاه. كما هو موضح

يجب أن يكون عميل PKI قادرين على الاتصال بخادم PKI عبر HTTP إلى المنفذ الذي تم تكوينه.

تكوين PKI

الخادم - المرور

يجب تكوين المرور التلقائي لخادم PKI كما يلي:

```
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
```

يتم تحديد معلمة المرور التلقائي بالأيام. وعلى مستوى أكثر دقة، يجب الأمر كما يلي:

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

تشير قيمة التمرير التلقائي التي تبلغ 90 إلى أن IOS يقوم بإنشاء شهادة خادم تمرير جديدة قبل 90 يوما من انتهاء صلاحية شهادة الخادم الحالية، وتبدأ صلاحية شهادة التمرير الجديدة هذه في نفس وقت انتهاء صلاحية الشهادة النشطة الحالية.

يجب تكوين التمرير التلقائي باستخدام قيمة تضمن إنشاء شهادة مرجع مصدق المرور عملية PKI في الشبكة بتنفيذ عملية PKI بشكل مسبق قبل أن يقوم أي عميل PKI بطلب خادم PKI. راجع قسم **الظل عملية على عامة نظرة** أدناه. كما هو موضح في GetNextCACert

العميل - التجديد

يجب تكوين تجديد الشهادة التلقائي لعميل PKI كما يلي:

```
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
```

هنا، ينص **الأمر** <percentage> **[regenerate]** للتسجيل التلقائي على أن يقوم IOS بتجديد الشهادة بنسبة 80٪ تمامًا من العمر الافتراضي للشهادة الحالية.

تذكر الكلمة الأساسية **regenerate** أنه يجب على IOS إعادة إنشاء زوج مفاتيح RSA المعروف باسم زوج مفاتيح الظل أثناء كل عملية لتجديد الشهادة.

يجب توخي الحذر أثناء تكوين النسبة المئوية للتسجيل التلقائي. في أي عميل PKI محدد في النشر، إذا نشأت حالة تنتهي فيها شهادة الهوية في نفس الوقت الذي تنتهي فيه صلاحية شهادة CA المصدرة، فيجب أن تقوم قيمة التسجيل التلقائي دائمًا بتشغيل عملية تجديد [الظل] بعد أن يقوم CA بإنشاء شهادة إعادة توجيه. ارجع إلى قسم **تباعيات تقويم PKI** *ضمن أمثلة النشر.*

متطلبات تجديد/إعادة توجيه PKI

يتناول هذا المستند عمليات إعادة توجيه الشهادة وتجديدها بالتفصيل، وبالتالي تعتبر هذه الأحداث مكتملة بنجاح:

- تهيئة خادم PKI بشهادة CA صالحة.
- تم تسجيل عملاء PKI بنجاح مع خادم PKI، أي أن كل عميل PKI لديه شهادة CA وشهادة هوية مع شهادة موجه.

يتضمن تسجيل عميل هذه الأحداث. دون الخوض في تفاصيل كثيرة:

- مصادقة TrustPoint
- تسجيل TrustPoint

في IOS، تعد TrustPoint حاوية للشهادات. يمكن أن تحتوي أي نقطة ثقة محددة على شهادة هوية نشطة و/أو شهادة مرجع مصدق نشط. تعتبر نقطة الثقة مصدق عليها إذا كانت تحتوي على مصنف CA نشط. وهو يعتبر مسجلاً إذا احتوى على شهادة هوية. يجب مصادقة نقطة ثقة قبل التسجيل. تتم تغطية تكوين خادم PKI والعميل، بالإضافة إلى مصادقة TrustPoint والتسجيل بالتفصيل في [دليل النشر عبر IOS PKI: التصميم والنشر الأوليين]

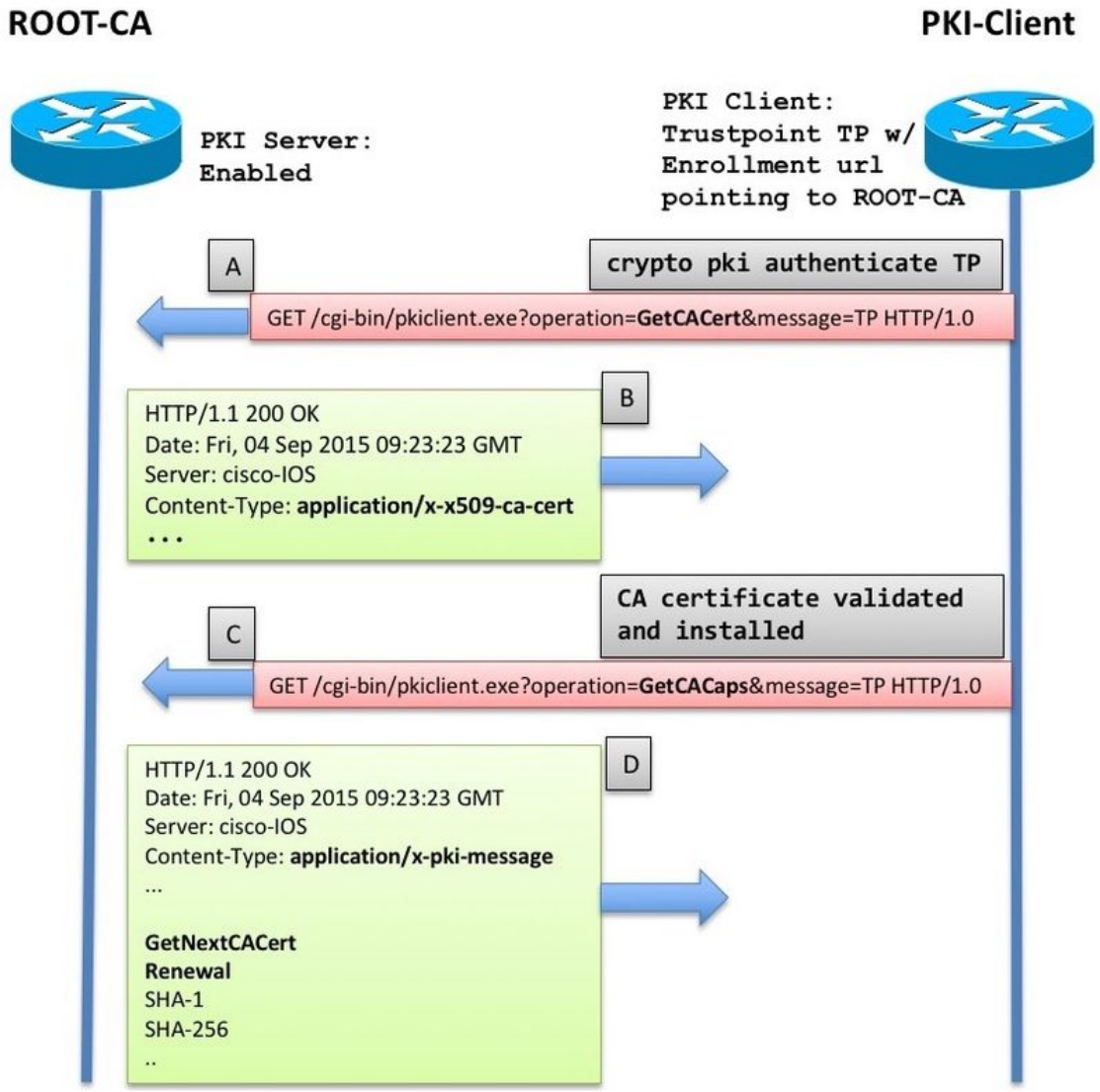
بعد إسترداد/تثبيت شهادة CA، يسترجع عميل PKI إمكانيات خادم PKI قبل تنفيذ التسجيل. يتم شرح إسترداد قدرات CA في هذا القسم.

قدرات CA

في IOS، عندما يقوم عميل PKI بمصادقة CA، بمعنى آخر، عندما يقوم المسؤول بإنشاء نقطة ثقة على موجه IOS وتنفيذ الأمر **crypto pki authenticate <trustPoint-name>**، تحدث هذه الأحداث على الموجه:

- يرسل IOS طلب SCEP يحتوي على نوع عملية GetCACert.
- الاستجابة المتوقعة هنا هي رسالة HTTP مع نوع محتوى **تطبيق/x-x509-ca-cert** في حالة نشر CA، أو **تطبيق/x-x509-ca-ra-cert** في حالة نشر RA و CA. يحتوي نص HTTP على شهادة CA. [وشهادة تقدير المخاطر في الحالة الأخيرة].
- بعد إسترداد وتثبيت شهادة CA/RA، يبدأ العميل طلب SCEP تلقائي يحتوي على عملية GetCACaps.

- الاستجابة الموقوعة هنا هي رسالة HTTP بنوع محتوى **التطبيق/x-pki-message**، والتي يمكن أن تكون أيضا **نص/عادي** ويحتوي نص HTTP على سلسلة من القدرات المدعومة من قبل CA، مفصولة بحرف تغذية خط. تظهر إستجابة نموذجية لخادم IOS PKI كما هو موضح في الرسم التخطيطي أدناه.



ويفسر عميل IOS PKI الاستجابة على أنها:

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

يركز هذا المستند على هاتين المميزتين.

GetNextCACert

عندما يتم إرجاع هذه الإمكانية من قبل المرجع المصدق (CA)، يدرك IOS أن المرجع المصدق يدعم إعادة تمرير شهادة المرجع المصدق. مع هذه الإمكانية التي تم إرجاعها، إذا لم يتم تكوين أمر **التسجيل التلقائي** ضمن TrustPoint، يقوم IOS بتهيئة مؤقت ظل معين إلى 90٪ من فترة صلاحية شهادة CA.

عند انتهاء صلاحية مؤقت الظل، يقوم IOS بتنفيذ عملية GetNextCacErt SCEP لجلب شهادة المرجع المصدق (CA) العابرة.

ملاحظة: إذا تم تكوين أمر **التسجيل التلقائي** ضمن TrustPoint مع عنوان URL لواجهة TrustPoint، فسيتم تهيئة مؤقت RENEW حتى قبل مصادقة TrustPoint **للتسجيل**، بغض النظر عن عدم إرسال عنوان URL **للتسجيل** في الموجود CA بشكل مستمر التسجيل حتى يتم مصادقة TrustPoint [CSR] على تسجيل فعلية رسالة.

ملاحظة: يتم إرسال GetNextCACert كإمكانية بوابة خادم IOS PKI إذا لم يتم تكوين **إعادة التوجيه التلقائي** على SERV

تجديد

بهذه الإمكانية، يقوم خادم PKI بإعلام عميل PKI أنه يمكنه إستخدام شهادة معرف نشطة لتوقيع طلب توقيع شهادة لتجديد الشهادة الموجودة.

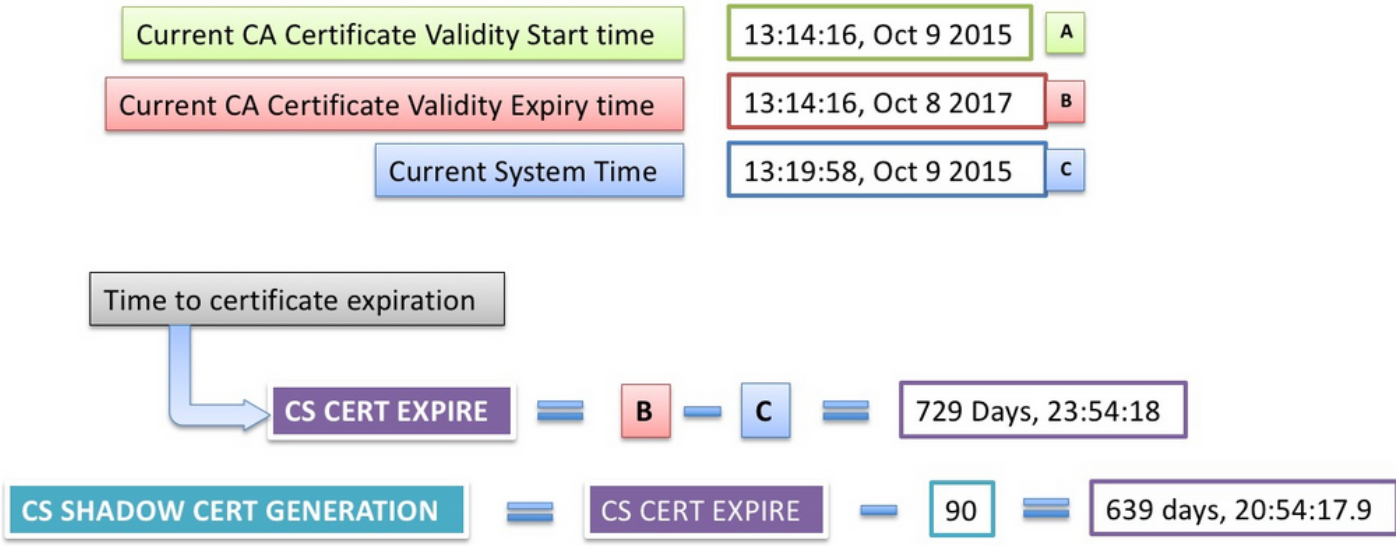
المزيد حول هذا الأمر في قسم **التجديد التلقائي لعميل PKI**.

النقل التلقائي لخادم PKI

مع التكوين المذكور أعلاه على خادم CA، يمكنك الاطلاع على:

```
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
```

الحظ هذا:



عملية التمرير

عند انتهاء صلاحية المؤقت **لإنشاء شهادة ظل CS**:

- يقوم IOS بإنشاء زوج مفاتيح إعادة توجيه أولا - وهو يحمل حاليا نفس اسم زوج المفاتيح النشط مع # تجزئة ملحقة به.

```
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
```

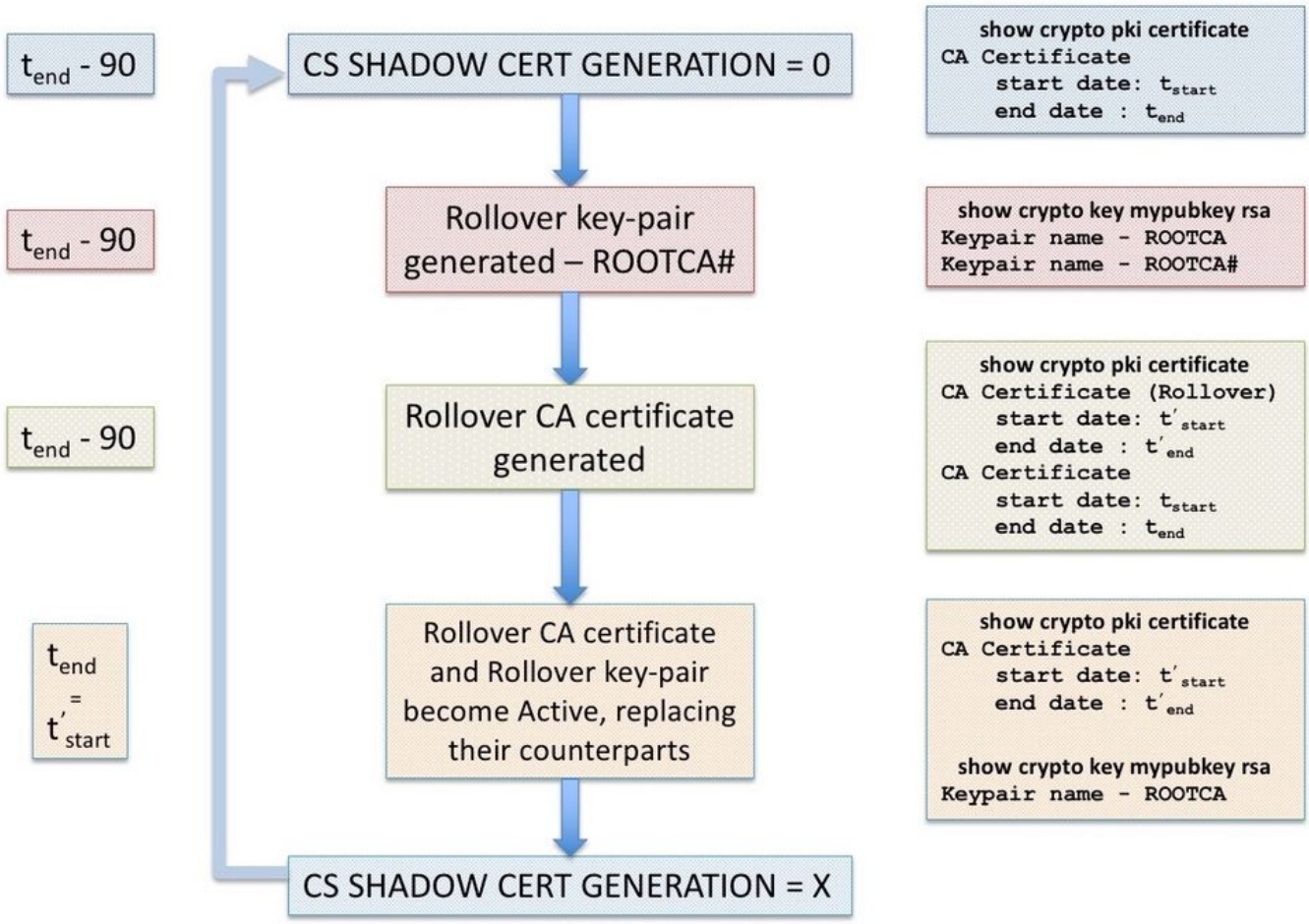
```
687F112B C9263541 BB402939 9C66D270 8D3EACED 4F63AA50 9FB340E8 38C8AC38
1818EA43 93C17CA1 C4917F43 C9199C9E F9F9C059 FDE11DA9 C7991826 43736FCE
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

- يقوم IOS بعد ذلك بإنشاء شهادة مرجع مصدق المرور، حيث يكون تاريخ بدء الصلاحية هو نفس تاريخ انتهاء صلاحية شهادة المرجع المصدق النشطة الحالية.

```
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
```



النقل اليدوي لخادم PKI

يدعم خادم IOS PKI التمرير اليدوي لشهادة CA، أي يمكن للمسؤول تشغيل إنشاء شهادة CA التمرير المسبق دون الحاجة إلى تكوين **التمرير التلقائي** ضمن تكوين خادم PKI. يوصى بشدة بتكوين **إعادة التوجيه التلقائي** سواء كان الشخص يخطط لتمديد فترة عمل خادم CA الذي تم نشره في البداية ليكون على الجانب الأكثر أمانا أم لا. **يمكن لعملاء PKI التحميل الزائد على المرجع المصدق بدون شهادة مرجع مصدق مرور**. ارجع إلى [تبعية عملية ظل العميل على إعادة توجيه خادم PKI](#).

يمكن تشغيل تمرير يدوي باستخدام الأمر مستوى التكوين:

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

وأيضا، يمكن إلغاء شهادة مرجع مصدق المرور لإنشاء شهادة جديدة يدويا، على أي حال، شيء ال يجب على المسؤول القيام به في بيئة الإنتاج، باستخدام:

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

يؤدي ذلك إلى حذف زوج مفاتيح RSA الذي يتم المرور فوقه وشهادة CA التي يتم إرسالها. ينصح بعدم القيام بذلك لأن:

- بمجرد أن يقوم المرجع المصدق بإنشاء شهادة المرور، قد يقوم العديد من العملاء بتنزيل شهادة مرجع مصدق المرور بالإضافة إلى شهادة تمرير عميل موقعة من خلال شهادة مرجع مصدق المرور.
- في هذه المرحلة، إذا تم إلغاء إعادة توجيه الملف، فقد يتعين إعادة تسجيل العميل.

التجديد التلقائي لعميل PKI

أنواع تجديد شهادات العميل - التجديد والظل

يتأكد IOS على خادم PKI دائما من أن وقت انتهاء صلاحية شهادة المعرف الصادرة للعميل لا يتجاوز وقت انتهاء صلاحية شهادة CA.

على عميل PKI، يأخذ IOS دائما وحدات التوقيت التالية في الاعتبار قبل جدولة عملية التجديد:

- وقت انتهاء صلاحية شهادة الهوية التي يتم تجديدها
- وقت انتهاء صلاحية شهادة المصدر (CA)

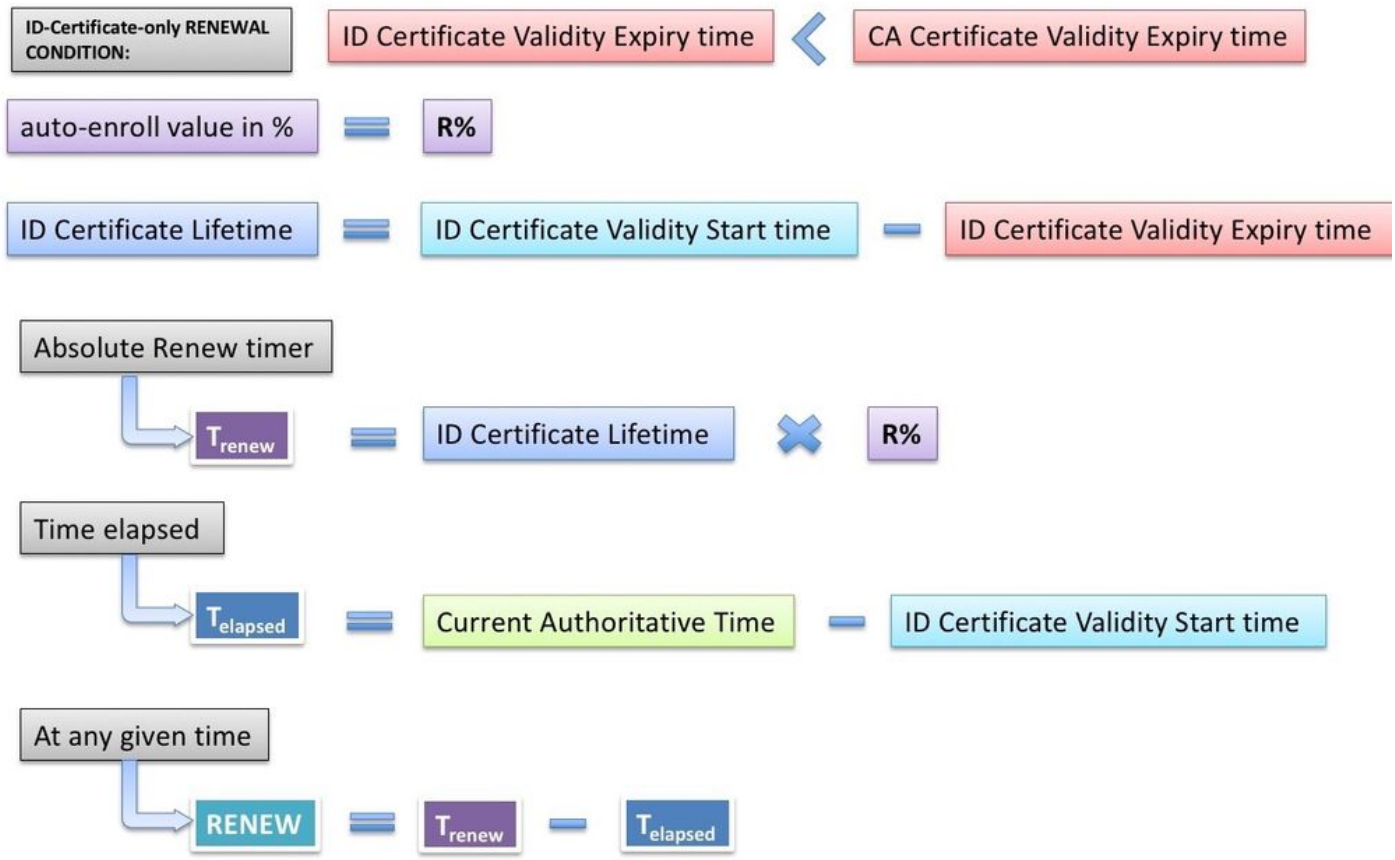
إذا لم يكن وقت انتهاء صلاحية شهادة الهوية هو نفسه وقت انتهاء صلاحية شهادة CA، فإن IOS يجري عملية تجديد بسيطة.

إذا كان وقت انتهاء صلاحية شهادة الهوية هو نفسه وقت انتهاء صلاحية شهادة CA، فإن IOS يجري عملية تجديد ظل.

تجديد - تجديد شهادة هوية الموجه

وكما تمت الإشارة سابقا، يقوم عميل IOS PKI بعملية تجديد بسيطة إذا لم يكن وقت انتهاء صلاحية شهادة الهوية مماثل لوقت انتهاء صلاحية شهادة CA، أو بعبارة أخرى، شهادة الهوية التي تنتهي قبل أن تقوم شهادة المصدر بتشغيل تجديد بسيط لشهادة الهوية.

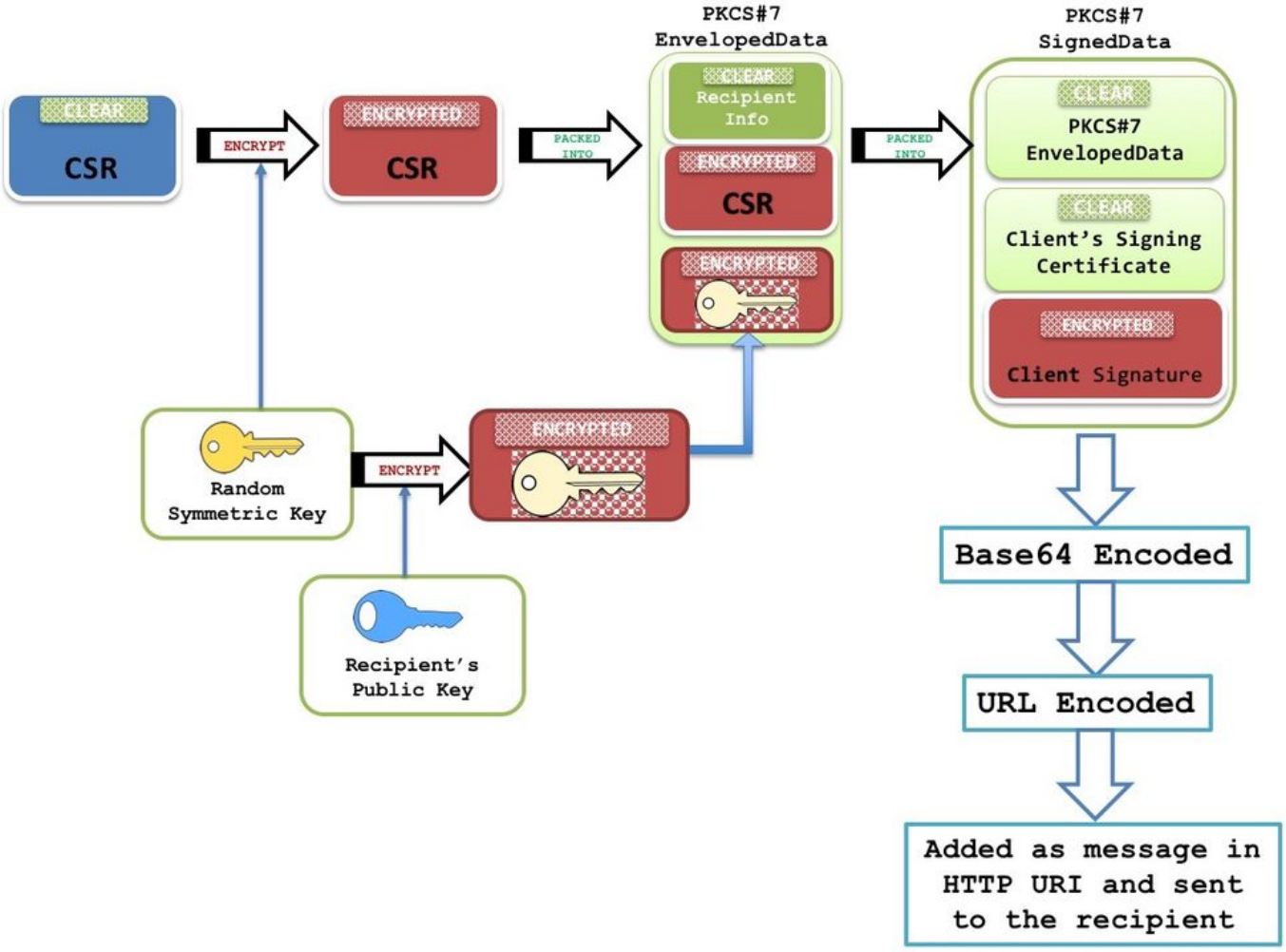
بمجرد تثبيت شهادة هوية، يقوم IOS بحساب مؤقت التجديد لنقطة الثقة المحددة كما هو موضح أدناه:



يعني "الوقت الحالي - الموثوق به" أنه يجب أن تكون ساعة النظام مصدرا موثوقا للوقت كما هو موضح هنا. (بالإضافة إلى قسم مصدر الوقت المخول) لن تتم تهيئة وحدات توقيت PKI دون مصدر وقت موثوق. وكنتيجة لذلك، لن تجري عملية التجديد.

تحدث الأحداث التالية عند انتهاء صلاحية مؤقت التجديد:

- يقوم IOS بإنشاء زوج مفاتيح ظل إذا تم تكوين **إعادة** الإنشاء [مثال: إعادة إنشاء التسجيل التلقائي 80]. دون **إعادة** إنشاء IOS، قم بإعادة إستخدام زوج مفاتيح RSA النشط حاليا.
- يقوم IOS بإنشاء طلب شهادة بتنسيق PKCS-10، والذي يتم تشفيره بعد ذلك في مظروف PKCS-7. يحتوي هذا المغلف أيضا على RecipientInfo، وهو اسم الموضوع والرقم التسلسلي الخاص بإصدار المرجع المصدق. هذا PKCS7-envelope بدوره تم حزمه إلى PKCS-7 بيانات موقعة. أثناء التسجيل الأولي، يستخدم IOS شهادة موقعة ذاتيا لتوقيع هذه الرسالة. وأثناء عمليات التسجيل اللاحقة، أي عمليات إعادة التسجيل، يستخدم IOS شهادة الهوية النشطة لتوقيع الرسالة. كما يتم تضمين بيانات PKCS7 الموقعة مع شهادة التوقيع، أي إما شهادة التوقيع الذاتي أو شهادة الهوية.



لمزيد من المعلومات حول بنية الحزمة هذه، ارجع إلى مستند نظرة عامة على SCEP

ملاحظة: المعلومات الأساسية هنا هي RecipientInfo وهو اسم الموضوع والرقم التسلسلي الخاص ب CA الإصدار، ويتم إستخدام المفتاح العام لهذا CA لتشفير المفتاح المتماثل. يتم تشفير CSR في مظروف PKCS7 باستخدام هذا المفتاح المتماثل.

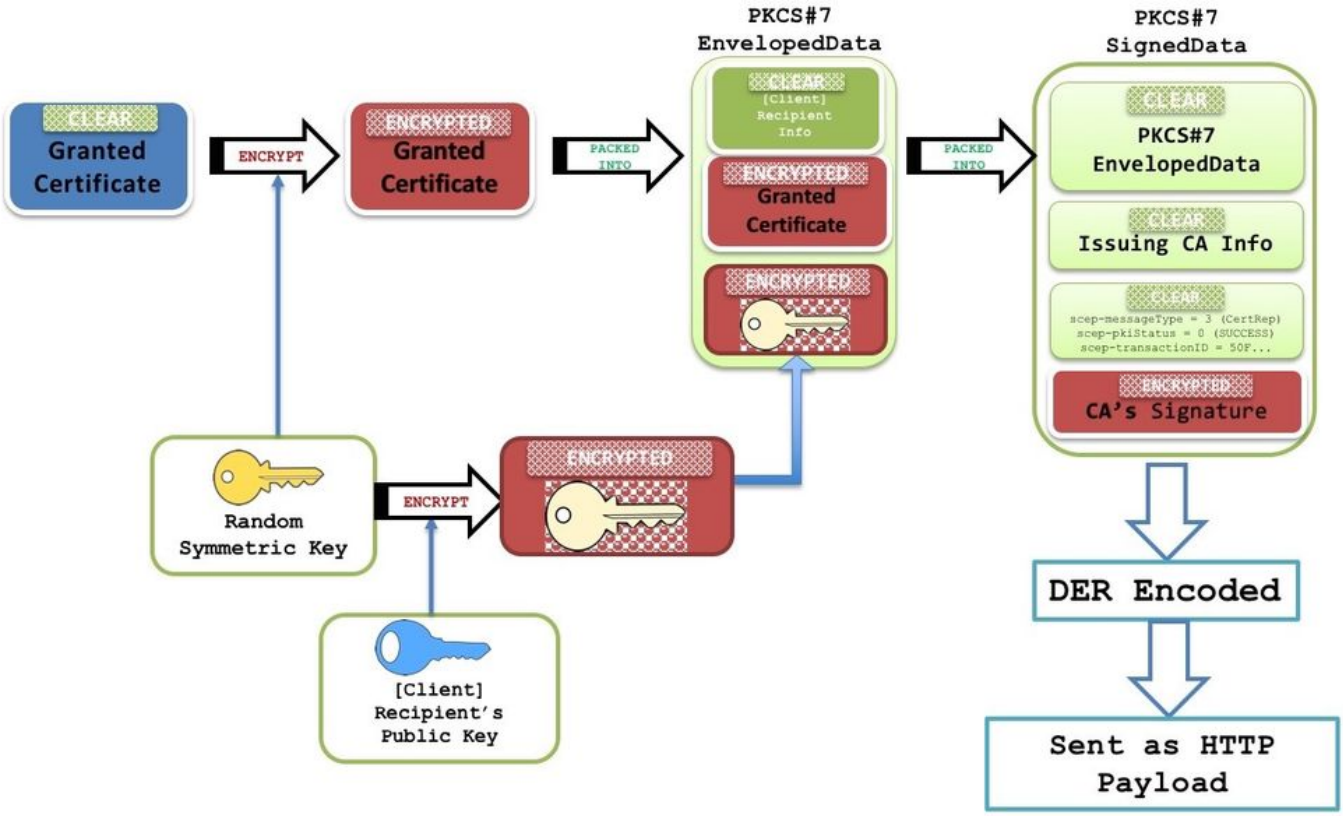
يتم فك تشفير هذه المفاتيح المتماثلة المشفرة بواسطة المرجع المصدق المتلقي باستخدام مفتاحه الخاص، ويتم إستخدام هذه المفاتيح المتماثلة لفك تشفير مظروف PKCS7 الذي يكشف CSR.

- يتم بعد ذلك إرسال طلب توقيع الشهادة (CSR) هذا المجهز بتنسيق PKCS7 إلى CA عن طريق عملية SCEP تسمى PKIOperation. وهو نوع رسالة SCEP من PKCSReq.
- إذا رفض المرجع المصدق الطلب، يقوم IOS بإيقاف مؤقت التجديد. من هذه النقطة فصاعدا، لتجديد شهادة الهوية، يجب على المسؤول إجراء تجديد يدوي (إرتباط بقسم **التجديد اليدوي لعميل PKI**)
- إذا قام المرجع المصدق بإرسال حالة SCEP **معلقة**، فإن IOS الموجود على عميل PKI يبدأ تشغيل مؤقت الاستطلاع في 60 ثانية وأدقيقة واحدة. في كل مرة تنتهي فيها صلاحية مؤقت للاستطلاع، يرسل IOS رسالة GetCertInitial SCEP من خلال عملية PKIOperation.عندما تنتهي صلاحية المؤقت الأول للاستطلاع، إذا تم الاستجابة برسالة GetCertInitial بحالة SCEP معلق، تقوم خوارزمية التراجع الأسي بتعيين الفاصل الزمني الأول لإعادة محاولة إجراء الاستطلاع إلى دقيقة واحدة، والفاصل الزمني الثالث لإعادة الثاني لإعادة محاولة إجراء الاستطلاع إلى دقيقتين، والفاصل الزمني لإعادة محاولة إجراء الاستطلاع إلى 4 دقائق، وهكذا لإعادة المحاولة التالية ل 999 مرة بشكل افتراضي أو حتى انتهاء صلاحية شهادة CA الإصدار.
  يمكن تكوين عدد الاستقصاءات وفترة إعادة المحاولة الأولى باستخدام:

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

- عندما يتم منح الشهادة على خادم PKI، فإن رسالة GetCertInitial SCEP التالية يتم الرد عليها باستخدام رسالة HTTP من نوع المحتوى application/x-pki-message ونص يحتوي على بيانات موقعة من PKCS#7. تحتوي هذه البيانات الموقعة على PKCS7 حالة SCEP عليها. تحتوي بيانات PKCS المغلفة هذه على بيانات PKCS7 المظلة. تحتوي أيضا على **مفوض**، وهي كما الشهادة المميزة و RecipientInfo، وهو اسم الموضوع والرقم التسلسلي للشهادة الموقعة ذاتيا أثناء التسجيل الأولي وشهادة الهوية النشطة أثناء عمليات إعادة التسجيل.

  تحتوي أيضا بيانات PKCS7 المغلفة على مفتاح متماثل مشفر باستخدام المفاتيح العام الخاص بالمستلم (والذي تم منح الشهادة الجديدة له). يؤدي إستلام الموجه إلى إستخدام المفاتيح المتناظرة الخاص. ثم يتم إستخدام هذا المفتاح المتماثل لفك تشفير بيانات PKCS#7 المضمنة، كاشفا شهادة الهوية الجديدة.



- في هذه المرحلة، يستبدل IOS شهادة الهوية الحالية بالشهادة الجديدة فورا. وإذا تم تكوين **إعادة** الإنشاء، فإن زوج مفاتيح الظل يحل محل زوج المفاتيح النشط كذلك.

- كما تتم مقارنة تاريخ انتهاء الشهادة الجديدة بتاريخ انتهاء شهادة CA لتحديد ما إذا كان يجب تهيئة مؤقت "التجديد" أو أنه يجب تهيئة مؤقت "الظل" كما هو موضح هنا <**أوناوع** href **و تجديد - "تجديد شهادة العميل" من** SHADOW>

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).