IOS PKI 구축 설명서:인증서 롤오버 - 구성 및 작업 개요

목차

소개

이 문서에서는 Cisco IOS PKI(Public Key Infrastructure) 서버 및 클라이언트의 인증서 롤오버에 대해 자세히 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

하드웨어

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

소프트웨어

- IOS
  - ISR-G1 - 최신 15.1(4)M*
  - ISR-G2의 경우 - 최신 15.4(3)M
- IOS-XE
  - XE 3.15 또는 15.5(2)S

참고:ISR 장치에 대한 일반적인 소프트웨어 유지 관리가 더 이상 활성 상태가 아니며, 향후 버그 수정 또는 기능 개선 사항을 위해서는 ISR-2 또는 ISR-4xxx 시리즈 라우터로 하드웨어 업그레이드가 필요합니다.

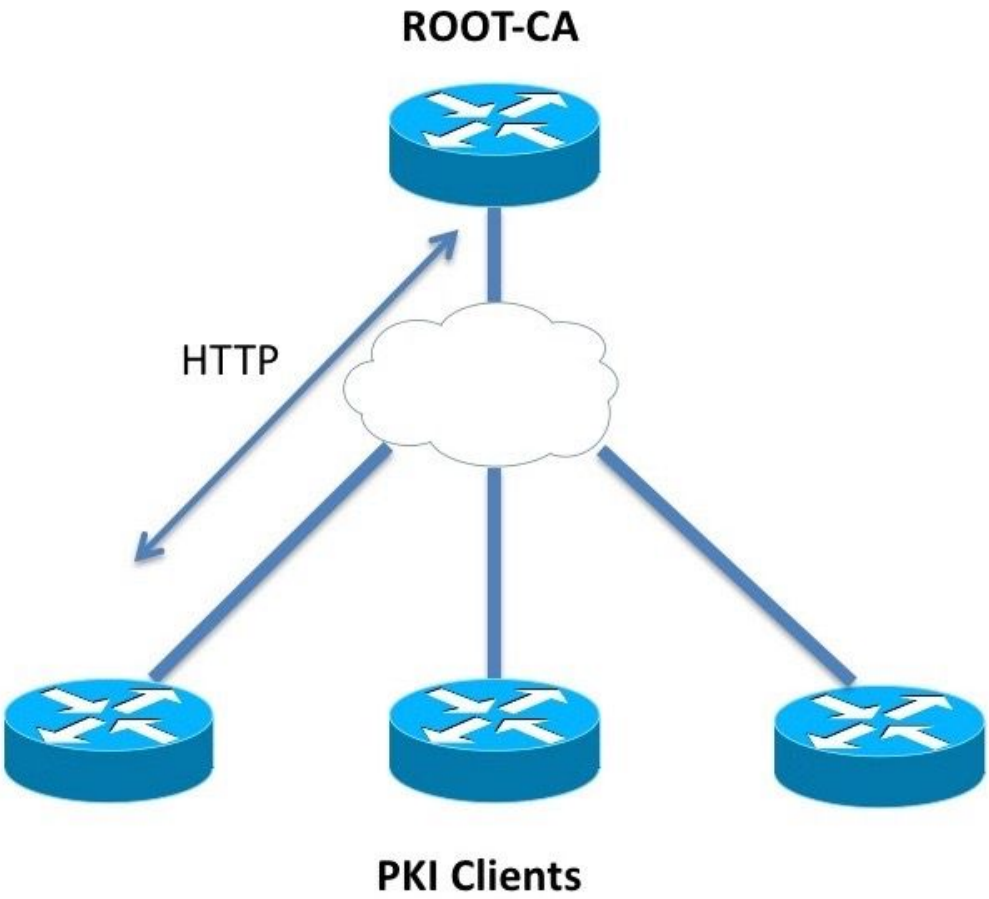
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

갱신 작업이라고도 하는 인증서 롤오버는 인증서가 만료될 때 새 인증서를 인계받을 준비가 된 것을 보장합니다.PKI 서버의 관점에서 이 작업은 모든 PKI 클라이언트가 현재 인증서가 만료되기 전에 새 서버 롤오버 인증서에서 서명한 새 클라이언트 롤오버 인증서를 받았는지 확인하기 위해 새 서버 롤오버 인증서를 미리 생성하는 작업을 포함합니다.PKI 클라이언트의 관점에서 클라이언트 인증서가 만료되지만 CA(Certificate Authority) 서버의 인증서가 만료되지 않은 경우 클라이언트는 새 인증서를 요청하고 새 인증서가 수신되는 즉시 이전 인증서를 대체하며, 클라이언트 인증서가 CA 서버의 인증서와 동시에 만료될 경우 클라이언트는 CA 서버의 롤오버 인증서를 먼저 수신하고

새 CA 서버에서 서명한 롤오버 인증서를 요청하게 되며, 두 인증서 모두 활성화될 때 활성화됩니다. 만료됩니다.

설정



PKI 및 SCEP(Simple Certificate Enrollment Protocol) 사전 요구 사항

신뢰할 수 있는 시간 소스

IOS에서는 하드웨어 클럭이 최상의 시간 소스가 아니므로 기본적으로 클럭 소스가 비권한 것으로 간주됩니다.PKI는 시간에 민감하므로 NTP를 사용하여 유효한 시간 소스를 구성하는 것이 중요합니다.PKI 구축에서는 필요한 경우 여러 NTP 서버를 통해 모든 클라이언트와 서버가 자신의 시계를 단일 NTP 서버에 동기화하도록 하는 것이 좋습니다.이에 대한 자세한 내용은 [IOS PKI 구축 설명서를 참조하십시오.초기 설계 및 구축]

IOS는 권한 클럭 없이 PKI 타이머를 초기화하지 않습니다.NTP는 매우 권장되지만, 임시 측정으로 관리자는 다음을 사용하여 하드웨어 시계를 신뢰할 수 있는 것으로 표시할 수 있습니다.

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

HTTP 통신

활성 IOS PKI 서버에 대한 요구 사항은 HTTP 서버이며, 이 config-level 명령을 사용하여 활성화할 수 있습니다.

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

이 명령은 기본적으로 포트 80에서 HTTP 서버를 활성화하며, 위와 같이 변경할 수 있습니다.

PKI 클라이언트는 HTTP를 통해 PKI 서버와 구성된 포트로 통신할 수 있어야 합니다.

PKI 컨피그레이션

서버 - 롤오버

PKI 서버 자동 롤오버 구성은 다음과 같습니다.

```
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
```

자동 롤오버 매개변수는 일 단위로 정의됩니다.보다 세분화된 레벨에서 명령은 다음과 같습니다.

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

자동 롤오버 값 90은 IOS가 현재 서버 인증서가 만료되기 90일 전에 롤오버 서버 인증서를 생성하며, 이 새 롤오버 인증서의 유효성이 현재 활성 인증서의 만료 시간과 동시에 시작됨을 나타냅니다.

자동 롤오버는 네트워크의 PKI 클라이언트가 아래 **SHADOW 작업 개요** 섹션에 설명된 대로 GetNextCACert 작업을 수행하기 전에 PKI 서버에서 롤오버 CA 인증서가 미리 생성되도록 하는 값으로 구성해야 합니다.

클라이언트 - 갱신

PKI 클라이언트 자동 인증서 갱신 구성은 다음과 같습니다.

```
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
```

여기서 **auto-enroll <percentage> [regenerate]** 명령은 IOS가 현재 인증서 수명의 정확히 80%에서 인증서 갱신을 수행해야 한다고 말합니다.

키워드 **regenerate는** IOS가 모든 인증서 갱신 작업 동안 shadow key-pair라고 하는 RSA 키 쌍을 재생성해야 한다고 나타냅니다.

자동 등록 비율을 구성하는 동안 주의해야 합니다.구축의 지정된 PKI 클라이언트에서 ID 인증서가 발급 CA 인증서와 동시에 만료되는 조건이 발생하면 자동 등록 값은 CA가 롤오버 인증서를 생성한 후 항상 [shadow] 갱신 작업을 트리거해야 합니다.구축 예제 아래의 **PKI 타이머 종속성** 섹션을 참조하십시오.

PKI 갱신/롤오버 사전 요구 사항

이 문서에서는 인증서 롤오버 및 갱신 작업을 자세히 다루므로 이러한 이벤트가 성공적으로 완료된 것으로 간주됩니다.

- 유효한 CA 인증서를 사용하는 PKI 서버 초기화
- PKI 클라이언트가 PKI 서버에 등록되었습니다.예: 각 PKI 클라이언트에는 CA 인증서와 라우터 인증서라는 ID 인증서가 있습니다.

클라이언트 등록에는 이러한 이벤트가 포함됩니다.자세한 내용은 다음을 참조하십시오.

- 신뢰 지점 인증
- 신뢰 지점 등록

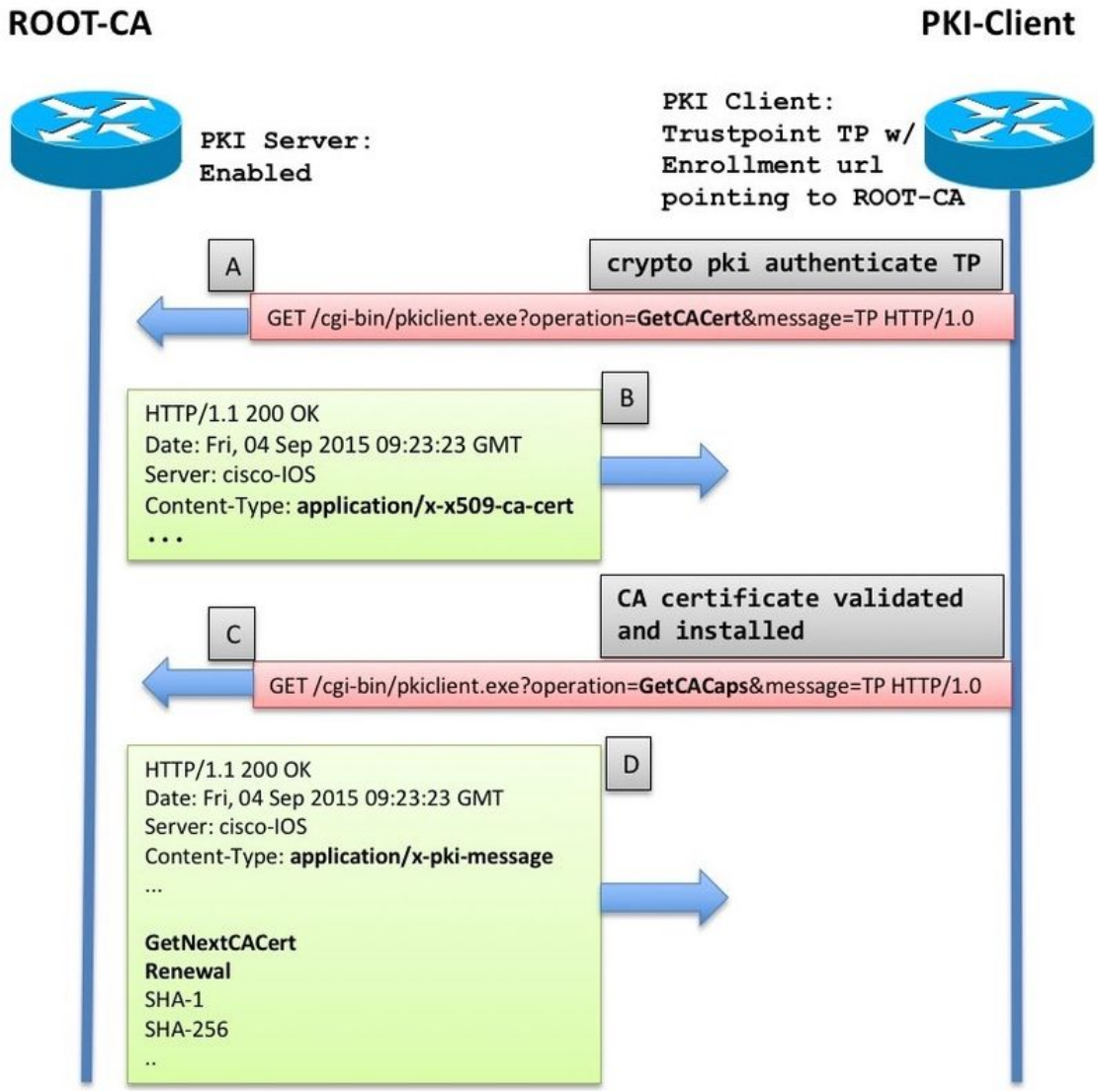
IOS에서 신뢰 지점은 인증서의 컨테이너입니다.지정된 신뢰 지점은 하나의 활성 ID 인증서 및/또는 하나의 활성 CA 인증서를 포함할 수 있습니다.신뢰 지점은 활성 CA 인증서를 포함하는 경우 인증된 것으로 간주됩니다.ID 인증서가 포함된 경우 등록된 것으로 간주됩니다.등록 전에 신뢰 지점을 인증해야 합니다.PKI 서버 및 클라이언트 컨피그레이션과 신뢰 지점 인증 및 등록은 IOS PKI 구축 가이드에서 자세히 다룹니다.초기 설계 및 구축

CA 인증서 검색/설치 후 PKI 클라이언트는 등록을 수행하기 전에 PKI 서버 기능을 검색합니다.CA 기능 검색에 대해서는 이 섹션에서 설명합니다.

CA 기능

IOS에서 PKI 클라이언트가 CA를 인증하는 경우, 즉 관리자가 IOS 라우터에서 신뢰 지점을 생성하고 crypto pki authenticate **<trustpoint-name>** 명령을 실행하면 다음 이벤트가 라우터에서 발생합니다.

- IOS는 GetCACert 작업 유형을 포함하는 SCEP 요청을 보냅니다.
- 여기서 예상되는 응답은 content-type of **application/x-x509-ca-cert**를 CA 구축의 경우, 또는 RA 및 CA 구축의 경우 **application/x-x509-ca-ra-cert**를 포함하는 HTTP 메시지입니다.HTTP 본문에는 CA 인증서가 포함되어 있습니다.[그리고 후자의 경우 RA 인증서]
- CA/RA 인증서 검색 및 설치에 따라 클라이언트는 GetCACaps 작업이 포함된 자동 SCEP 요청을 시작합니다.
- 여기에 예상 응답은 content-type of **application/x-pki-message**를 포함하는 HTTP 메시지입니다. 이 메시지는 **text/plain**일 수 있으며 HTTP 본문에는 CA에서 지원하는 일련의 기능이 포함되어 있으며, 이 기능은 줄-피드 문자로 구분됩니다.일반적인 IOS PKI 서버 응답은 아래 다이어그램에 나와 있습니다.



응답은 IOS PKI 클라이언트에서 다음과 같이 해석됩니다.

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

이 문서에서는 이 두 가지 기능에 초점을 두고 있습니다.

다음 CACert 가져오기

CA에서 이 기능을 반환하면 IOS는 CA가 CA-인증서 롤오버를 지원함을 인식합니다.이 기능을 반환하면 신뢰 지점 아래에서 **auto-enroll** 명령이 구성되지 않은 경우 IOS는 CA 인증서의 유효 기간의 90%로 설정된 SHADOW 타이머를 초기화합니다.

SHADOW 타이머가 만료되면 IOS는 GetNextCACert SCEP 작업을 수행하여 롤오버 CA 인증서를 가져옵니다.

> **참고**: **auto-enroll** 명령**이 등록 URL**과 함께 신뢰 지점에 구성된 경우, 신뢰 지점을 인증하기 전이라도 RENEW 타이머가 초기화되며, 신뢰 지점이 인증될 때까지 실제 등록 메시지 [CSR]이(가) 전송되지 않더라도 등록 url에 있는 CA에 등록하려고 **계속 시도합니다**.

참고: GetNextCACert는 IOS PKI 서버에서 **자동 롤오버가** 서버에 구성되지 않은 경우에도 기능으로 전송됩니다.

갱신

이 기능을 사용하여 PKI 서버는 PKI 클라이언트에 활성 ID 인증서를 사용하여 기존 인증서를 갱신하기 위해 인증서 서명 요청에 서명할 수 있음을 알립니다.

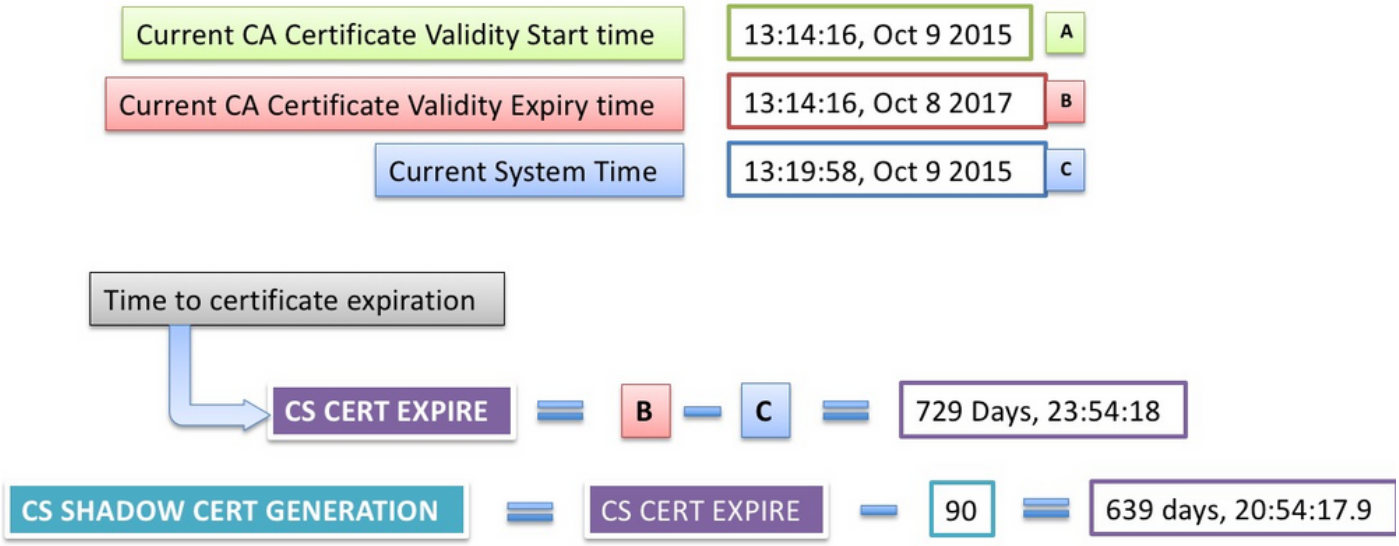
이에 대한 자세한 내용은 PKI **Client Auto-Renewal** 섹션을 참조하십시오.

PKI 서버 자동 롤오버

CA 서버에서 위의 컨피그레이션을 사용하면 다음을 볼 수 있습니다.

```
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
```

다음 사항에 유의하십시오.



롤오버 작업

CS **SHADOW CERT 생성** 타이머 만료 시:

- IOS는 먼저 롤오버 키 쌍을 생성합니다. 현재 활성 키 쌍과 이름이 같고 # 해시가 추가됩니다.

```
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
```

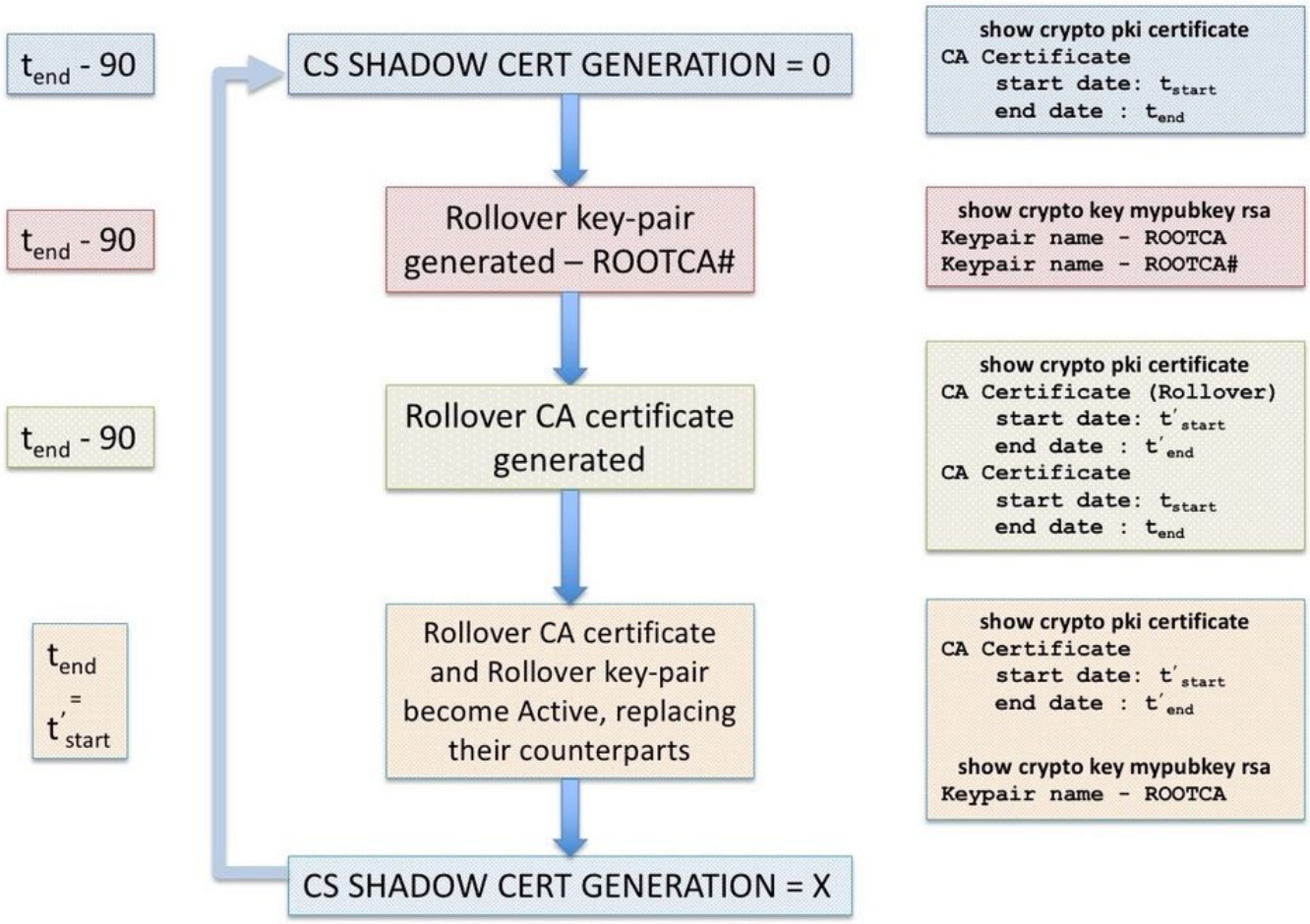
```
1818EA43 93C17CA1 C4917F43 C9199C9E F9F9C059 FDE11DA9 C7991826 43736FCE
A80D0CEE 2378F23B 6AC5FC3B 4A7A0120 D391BE8F A9AFD212 E05A2864 6610233C
E0E58D93 23AA0ED2 A5B1C140 122E6E3D 98A7D974 E2363902 70A89CE3 BF020301 0001
```

- 그런 다음 IOS에서 롤오버 CA 인증서를 생성합니다. 여기서 유효성 시작 날짜는 현재 활성 CA 인증서의 유효성 종료 날짜와 동일합니다.

```
Jul 10 13:14:18.326: CRYPTO_CS: shadow CA successfully created.
Jul 10 13:14:18.326: CRYPTO_CS: exporting shadow CA key and cert
Jul 10 13:14:18.327: CRYPTO_CS: file opened: ftp://10.1.1.1/DB/ROOTCA/ROOTCA_00001.p12
```

```
Root-CA# show crypto pki certificates
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 13:14:46.820 CET Mon Jul 10 2017

CA Certificate (Rollover)
 Status: Available
 Certificate Serial Number (hex): 03
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
   ou=TAC
   o=Cisco
 Subject:
   Name: RootCA
   cn=RootCA
   ou=TAC
   o=Cisco
 Validity Date:
   start date: 13:14:16 CET Oct 8 2017
   end   date: 13:14:16 CET Oct 8 2019
 Associated Trustpoints: ROOTCA

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=RootCA
   ou=TAC
   o=Cisco
 Subject:
   cn=RootCA
   ou=TAC
   o=Cisco
 Validity Date:
   start date: 13:14:16 CET Oct 9 2015
    end   date: 13:14:16 CET Oct 8 2017
 Associated Trustpoints: ROOTCA
 Storage: nvram:RootCA#1CA.cer

Root-CA# show crypto pki server
Certificate Server ROOTCA:
Status: enabled
State: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=RootCA,OU=TAC,O=Cisco
```

```
CA cert fingerprint: CC748544 A0AB7832 935D8CD0 214A152E
Granting mode is: manual
Last certificate issued serial number (hex): 6
CA certificate expiration timer: 13:14:16 CET Oct 8 2017
CRL NextUpdate timer: 19:11:54 CET Jul 10 2017
Current primary storage dir: unix:/iosca-root/
Database Level: Complete - all issued certs written as <serialnum>.cer
 Rollover status: available for rollover
Rollover CA certificate fingerprint: 031904DC F4FAD1FD 8A866373 C63CE20F
 Rollover CA certificate expiration time: 13:14:16 CET Oct 8 2019
Auto-Rollover configured, overlap period 90 days

Root-CA# show run | section chain ROOTCA
crypto pki certificate chain ROOTCA
 certificate ca rollover 03
 30820237 308201A0 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
 2F310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 0F300D06 03550403 1306526F 6F744341 301E170D 31373130 30383132 31343136
 5A170D31 39313030 38313231 3431365A 302F310E 300C0603 55040A13 05436973
 636F310C 300A0603 55040B13 03544143 310F300D 06035504 03130652 6F6F7443
 4130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100BF2A
 52687F11 2BC92635 41BB4029 399C66D2 708D3EAC ED4F63AA 509FB340 E838C8AC
 381818EA 4393C17C A1C4917F 43C9199C 9EF9F9C0 59FDE11D A9C79918 2643736F
 CEA80D0C EE2378F2 3B6AC5FC 3B4A7A01 20D391BE 8FA9AFD2 12E05A28 64661023
 3CE0E58D 9323AA0E D2A5B1C1 40122E6E 3D98A7D9 74E23639 0270A89C E3BF0203
 010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
 01FF0404 03020186 301F0603 551D2304 18301680 1419FCA4 DDE84233 F79C066F
 93CCF6B3 E14F8355 31301D06 03551D0E 04160414 19FCA4DD E84233F7 9C066F93
 CCF6B3E1 4F835531 300D0609 2A864886 F70D0101 04050003 81810065 AC780BB4
 2398D765 BE4C4C0A 0D0F16C0 82530D85 99933BDC 8388C46D 926145D8 B0BA275A
 93AAB497 FC876F6A E951C138 F5D652AE C0C25E2A FDD80BAA C6BD5A78 E439158F
 5544F30F 33C59E22 1994A8D3 AADC1287 BD15A104 55CB5DC3 49A9401A 8DB3940A
 5054EA21 99CCE4F3 40B471FE DEB4BB38 AC3ACD48 4CDDCBC9 9829D3
     quit
certificate ca 01
 30820237 308201A0 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 2F310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 0F300D06 03550403 1306526F 6F744341 301E170D 31353130 30393132 31343136
 5A170D31 37313030 38313231 3431365A 302F310E 300C0603 55040A13 05436973
 636F310C 300A0603 55040B13 03544143 310F300D 06035504 03130652 6F6F7443
 4130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100B071
 27360CF0 0613B259 CE7BB815 8DE6BC8A A48A763F 7350CE64 B071AC5D 93ED59C9
 36F751D8 1070CEA8 C8B0023B 4B0FB9A5 38A1C118 D35530D4 6DC4B4DC 143BD1D2
 3148B0C0 53A781D0 C786DEE9 DECCA58C 18B5804B 29911D1D 5776B3EC 3F42D38C
 3A1E0F8D D91DE228 B995AC3C 1087C132 FC759563 38258727 F61A1F08 18830203
 010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
 01FF0404 03020186 301F0603 551D2304 18301680 148D421A BED6DCAD B8CFE4B4
 1B2C7E41 C73428AC 9A301D06 03551D0E 04160414 8D421ABE D6DCADB8 CFE4B41B
 2C7E41C7 3428AC9A 300D0609 2A864886 F70D0101 04050003 8181008C 3495278E
 DA6C14B0 533E746D 8DA743AF 06BE4088 913BF9BC A94576FA BC86EFD1 1DFE6B9F
 0D244144 473C67AD 24414A20 84E9B083 D1720766 0A698C29 115482C6 2FB57E86
 95CDECF2 29662362 866CDC91 730ADBB3 BDBBDC3C EA5301B0 150658E7 AF722BD7
 6B5C2D6A 661A4FED CDA32DE5 D6C2CE7A 544086DC F957A87C 2C07FF
     quit
```



PKI 서버 수동 롤오버

IOS PKI Server는 CA 인증서의 수동 롤오버를 지원합니다. 즉, 관리자는 PKI 서버 컨피그레이션에서 **자동 롤오버를** 구성하지 않고도 롤오버 CA 인증서를 미리 생성할 수 있습니다.처음 구축된 CA 서버의 수명을 더 안전하게 확장할 계획이 있는지 여부에 관계없이 **자동 롤오버**를 구성하는 것이 좋습니다.**PKI 클라이언트는 롤오버 CA 인증서 없이 CA를 오버로드할 수 있습니다**.*PKI* 서버 롤오버에서 클라이언트 섀도우 작업의 종속성을 참조하십시오.

컨피그레이션 레벨 명령을 사용하여 수동 롤오버를 트리거할 수 있습니다.

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

또한 롤오버 CA 인증서는 수동으로 새로 생성하기 위해 취소할 수 있지만, 관리자는 다음을 사용하여 프로덕션 환경에서 해서는 안 되는 작업입니다.

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

이렇게 하면 롤오버 rsa 키 쌍 및 롤오버 CA 인증서가 삭제됩니다.다음과 같은 이유로 권장됩니다.

- CA가 롤오버 인증서를 생성한 후에는 여러 클라이언트가 롤오버 CA 인증서 및 롤오버 CA 인증서에서 서명한 롤오버 클라이언트 인증서를 다운로드할 수 있습니다.
- 이 단계에서 롤오버가 취소되면 클라이언트를 다시 등록해야 할 수 있습니다.

PKI 클라이언트 자동 갱신

클라이언트 인증서 갱신 유형 - 갱신 및 섀도우

PKI 서버의 IOS는 클라이언트에 발급된 ID 인증서의 만료 시간이 CA 인증서의 만료 시간을 초과하지 않도록 항상 보장합니다.

PKI 클라이언트에서 IOS는 갱신 작업을 예약하기 전에 항상 다음 타이머를 고려합니다.

- 갱신되는 ID 인증서의 만료 시간
- 발급자(CA) 인증서의 만료 시간

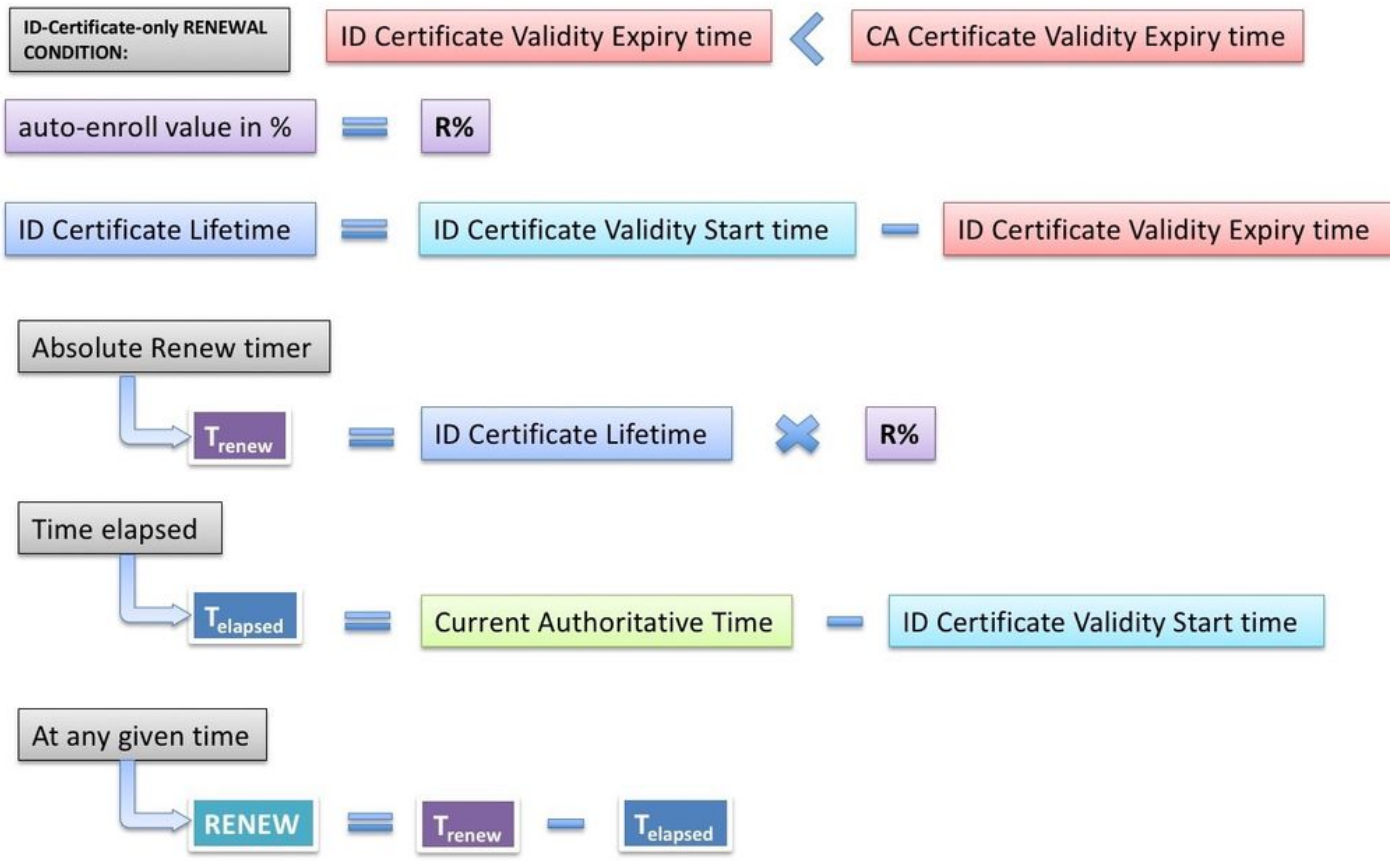
ID 인증서의 만료 시간이 CA 인증서의 만료 시간과 같지 않으면 IOS는 간단한 갱신 작업을 수행합니다.

ID 인증서의 만료 시간이 CA 인증서의 만료 시간과 같으면 IOS는 섀도우 갱신 작업을 수행합니다.

RENEW - 라우터 ID 인증서 갱신

앞에서 언급했듯이 IOS PKI 클라이언트는 ID 인증서의 만료 시간이 CA 인증서의 만료 시간과 동일하지 않을 경우 간단한 갱신 작업을 수행합니다. 즉, 발급자의 인증서가 ID 인증서의 단순 갱신을 트리거하기 전에 만료되는 ID 인증서가 만료됩니다.

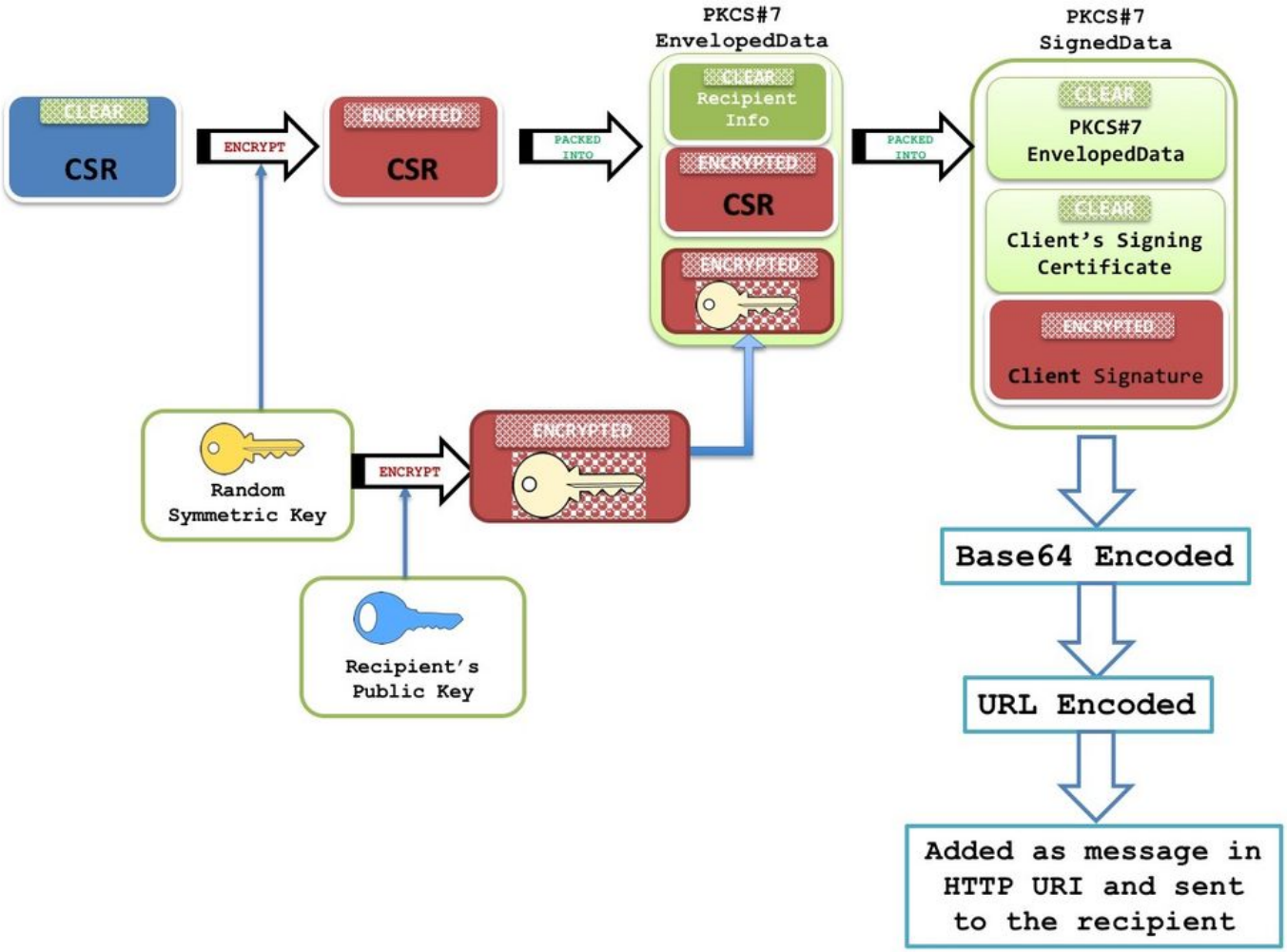
ID 인증서가 설치되면 IOS는 다음과 같이 특정 신뢰 지점에 대한 RENEW 타이머를 계산합니다.



Current-Authoritative-Time은 시스템 시계가 여기에 설명된 대로 신뢰할 수 있는 시간 소스가 되어야 함을 의미합니다.(신뢰할 수 있는 시간 소스 섹션에 대한 링크) PKI 타이머는 권한 있는 시간 소스가 없으면 초기화되지 않습니다.따라서 갱신 작업은 수행되지 않습니다.

RENEW 타이머가 만료될 때 다음 이벤트가 발생합니다.

- 재생성이 구성된 경우 IOS에서 섀도우 키 쌍을 생성합니다. [예:자동 등록 80 재생성]IOS를 **재생성하지** 않으면 현재 활성 RSA 키 쌍을 다시 사용합니다.
- IOS는 PKCS-10 형식의 인증서 요청을 생성합니다. 그러면 PKCS-7 포락으로 암호화됩니다.또한 이 봉투에는 발급 CA의 주체 이름과 일련 번호인 RecipientInfo도 포함되어 있습니다.이 PKCS7-envelope는 PKCS-7 서명 데이터로 채워집니다.초기 등록 중에 IOS는 자체 서명 인증서를 사용하여 이 메시지에 서명합니다.그리고 후속 등록 중에(다시 등록) IOS는 활성 ID 인증서를 사용하여 메시지에 서명합니다.PKCS7 서명 데이터도 서명 인증서(예: 자체 서명 인증서 또는 ID 인증서)와 함께 포함됩니다.



이 패킷 구조에 대한 자세한 내용은 SCEP 개요 문서를 참조하십시오.

참고:여기서 주요 정보는 발급 CA의 주체 이름과 일련 번호인 RecipientInfo이며, 이 CA의 공개 키는 대칭 키를 암호화하는 데 사용됩니다.PKCS7 봉투의 CSR은 이 대칭 키를 사용하여 암호화됩니다.

이 암호화된 대칭 키는 개인 키를 사용하여 수신 CA에 의해 해독되며, 이 대칭 키는 CSR을 나타내는 PKCS7 봉투를 해독하는 데 사용됩니다.

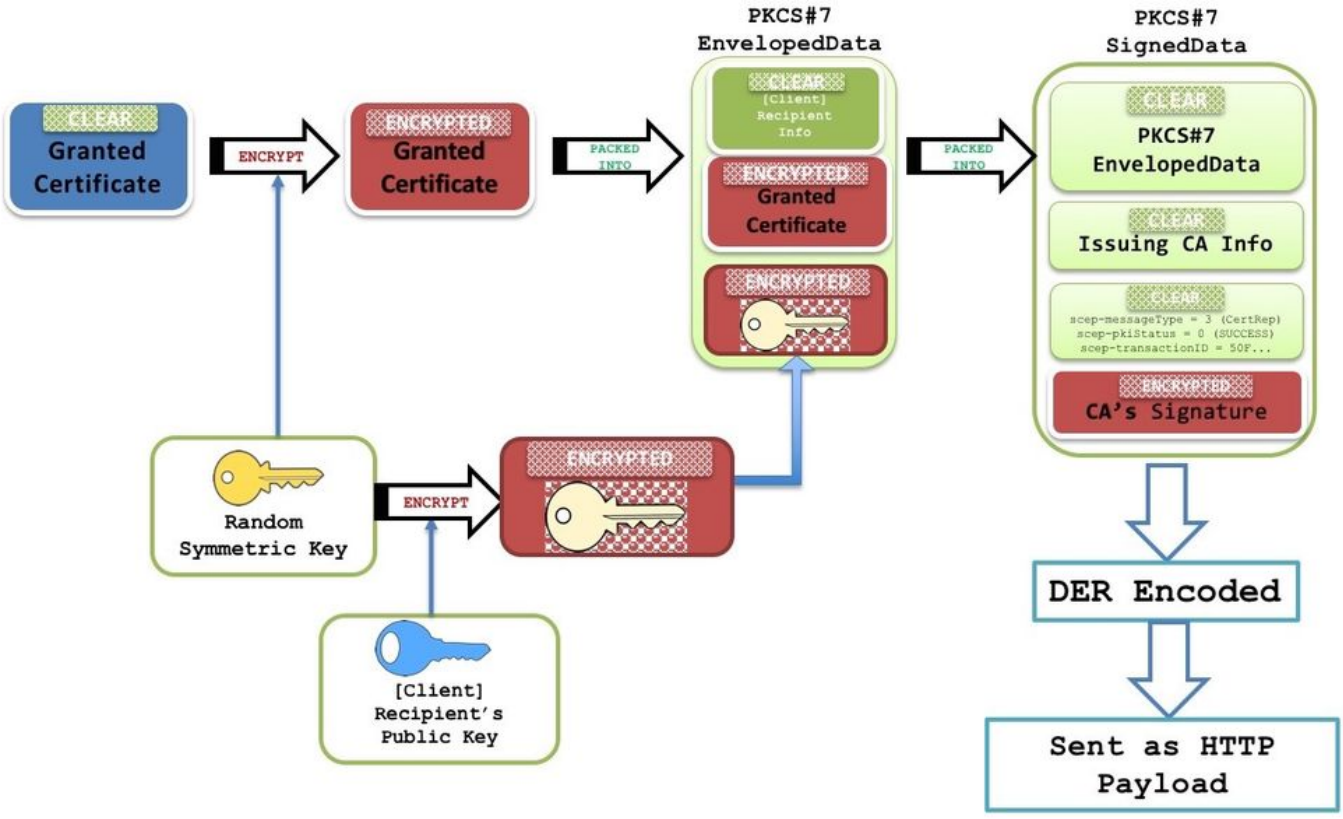
- 그런 다음 PKCS7 형식으로 패키지된 이 CSR(Certificate Signing Request)은 SCEP 메시지 유형 PKCSReq 및 PKIOperation이라는 SCEP 작업을 사용하여 CA로 전송됩니다.
- CA가 요청을 거부하면 IOS는 RENEW 타이머를 중지합니다.이 시점부터 ID 인증서를 갱신하려면 관리자가 수동 갱신을 수행해야 합니다(PKI **클라이언트 수동 갱신** 섹션 링크).
- CA가 SCEP 상태를 **pending**으로 전송하는 경우 PKI 클라이언트의 IOS는 60초 또는 1분에 시

작하여 POLL 타이머를 시작합니다.POLL 타이머가 만료될 때마다 IOS는 PKIOperation 작업을 통해 GetCertInitial SCEP 메시지를 보냅니다.첫 번째 POLL 타이머가 만료될 때 GetCertInitial 메시지가 SCEP Pending 상태로 응답될 경우, 지수 백오프 알고리즘은 첫 번째 POLL 타이머 재시도 간격을 1분, 두 번째 POLL 타이머 재시도 간격을 2분으로, 세 번째 POLL 재시도 타이머를 4분으로 설정합니다. 다음 99999 또는 Issuing CA 인증서가 만료될 때까지.
폴링 카운트 및 첫 번째 재시도 기간은 다음을 사용하여 구성할 수 있습니다.

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

- PKI 서버에 인증서가 부여되면 다음 GetCertInitial SCEP 메시지는 콘텐츠 유형 **application/x-pki-message**의 HTTP 메시지 및 서명된 PKCS#7 서명 데이터가 포함된 본문으로 응답됩니다.이 PKCS7 서명 데이터에는 SCEP 상태가 Granted로 포함되며 PKCS7 봉투 데이터도 포함됩니다.이 PKCS 봉투 데이터에는 허가된 인증서 및 RecipientInfo가 포함되어 있습니다. RecipientInfo는 초기 등록 중에 자체 서명된 인증서의 주체 이름과 일련 번호를 포함하고 재등록 중에 활성 ID 인증서를 포함합니다.

  PKCS7 봉투 데이터에는 수신자의 공개 키로 암호화된 대칭 키(새 인증서가 부여됨)도 포함되어 있습니다. 수신 라우터는 개인 키를 사용하여 암호를 해독합니다.그런 다음 이 일반 대칭 키를 사용하여 PKCS#7 봉투 데이터를 해독하고 새 ID 인증서를 표시합니다.



- 이 단계에서 IOS는 기존 ID 인증서를 즉시 새 인증서로 교체합니다.그리고 **재생성**이 구성된 경우 섀도우 키 쌍도 활성 키 쌍을 대체합니다.

- 또한 새 인증서의 종료 날짜를 CA 인증서의 종료 날짜와 비교하여 RENEW 타이머를 초기화해야 하는지 아니면 SHADOW 타이머를 초기화해야 하는지 확인합니다. 여기서 <href **Types of Client Certificate Renewal - RENEW and SHADOW>**