IOS PKI 導入ガイド：証明書のロールオーバー：構成と動作の概要

内容

概要

このドキュメントでは、Cisco IOS Public Key Infrastructure（PKI）サーバおよびクライアントの証明書ロールオーバーについて詳しく説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

ハードウェア

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

[ソフトウェア（Software）]

- IOS
  - ISR-G1：最新15.1(4)M*
  - ISR-G2：最新15.4(3)M
- IOS-XE
  - XE 3.15 または 15.5(2)S

注：ISR デバイスの一般的なソフトウェア メンテナンスは使用できなくなりました。今後のバグ修正または機能強化には、ISR-2 または ISR-4xxx シリーズ ルータにハードウェアをアップグレードする必要があります。

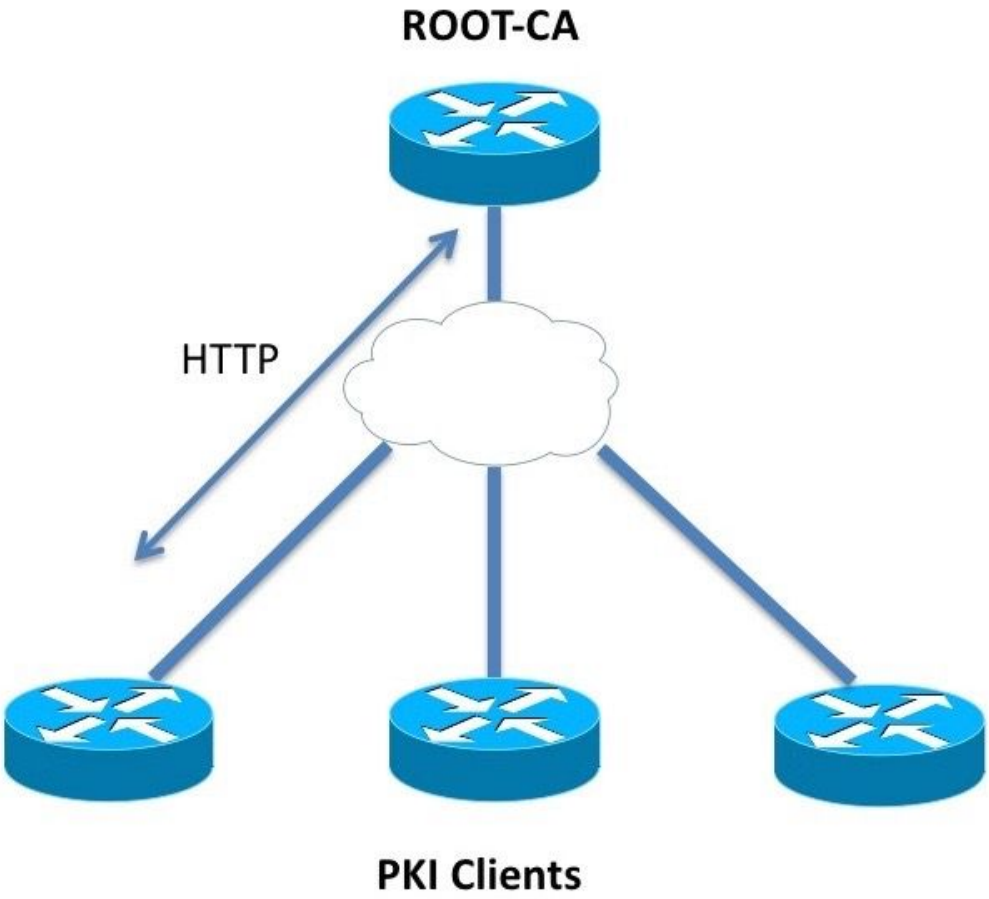
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

証明書ロールオーバー（更新操作とも呼ばれます）を使用することによって、証明書が期限切れになる時点で、確実に新しい証明書に引き継げる状態にしておくことができます。PKI サーバの側では、この操作には、現在の証明書が期限切れになる前に、すべての PKI クライアントが新しいサーバのロールオーバー証明書によって署名された新しいクライアント ロールオーバー証明書を受け取ることができるように、新しいサーバのロールオーバー証明書を十分前もって生成しておくことが含まれます。PKI クライアントの側では、クライアント証明書が期限切れになっても

、認証局（CA）サーバの証明書が期限切れにならなければ、クライアントは新しい証明書を要求し、新しい証明書を受け取ったらすぐに古い証明書と交換します。クライアント証明書が CA サーバの証明書と同時に期限切れになる場合、クライアントは、必ず CA サーバのロールオーバー証明書を最初に受け取り、その後新しい CA サーバのロールオーバー証明書によって署名されたロールオーバー証明書を要求します。このようにすると、古い証明書の期限が切れたときに、両方がアクティブになります。

セットアップ



PKI と Simple Ceritificate Enrollment Protocol（SCEP）の前提条件

正規の時刻源

ハードウェア クロックは最適な時刻源とはならないため、IOS ではデフォルトのクロック ソースは信頼できないと見なされます。PKI は時間が正確であることが求められるため、NTP を使用して有効な時間源を設定することが重要になります。PKI の導入では、すべてのクライアントとサーバで、単一の NTP サーバとクロックを同期させることが推奨されています。しかし、必要な場合は、複数の NTP サーバも使用できます。この詳細については、『IOS PKI 導入ガイド：初期設

計と展開』を参照してください。

IOS は、正規のクロックがないと PKI タイマーを初期化しません。NTP を使用することが強く推奨されますが、一時的な手段として、管理者は次のコマンドを使用して、ハードウェア クロックに正規としてマークを付けることができます。

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

HTTP 通信

アクティブ IOS PKI サーバの要件は、次の config レベルのコマンドを使用して有効にすることができる HTTP サーバです。

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

このコマンドは、ポート 80 で HTTP サーバをデフォルトで有効にします。これは、上記のように変更することができます。

PKI クライアントは、設定されたポートを使用して HTTP で PKI サーバと通信できる必要があります。

PKI 設定

サーバ：ロールオーバー

PKI サーバの自動ロールオーバー設定は、次のようになります。

```
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
```

auto-rollover のパラメータは日単位で定義されます。さらに細かいレベルで定義するには、次のようにコマンドを指定します。

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

auto-rollover の値「90」は、IOS が現在のサーバ証明書の期限が切れる 90 日前に、ロールオーバー サーバ証明書を作成することを意味します。この新しいロールオーバー証明書は、現在のアクティブな証明書の失効と同時に有効になります。

auto-rollover は、ネットワーク内の PKI クライアントが後続の「SHADOW 操作の概要」セクションで説明されているように GetNextCACert 操作を実行するよりも十分前もってロールオーバー CA 証明書を PKI サーバで生成できるような値に設定する必要があります。

クライアント：更新

PKI クライアントの自動証明書更新の設定は、次のようになります。

```
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
```

ここで、auto-enroll <percentage> [regenerate] コマンドは、IOS が現在の証明書の有効期間のちょうど 80 % で証明書の更新を実行する必要があることを示しています。

キーワード regenerate は、毎回の証明書更新操作中に IOS がシャドウ キー ペアと呼ばれる RSA キー ペアを再生成する必要があることを示しています。

auto-enroll のパーセンテージを設定する際は、細心の注意を払う必要があります。展開内の特定の PKI クライアントで、発行側 CA 証明書と同時に ID 証明書が期限切れになる状況が発生した場合、CA がロールオーバー証明書を作成した後に、auto-enroll 値によって常に [shadow] 更新操作がトリガーされる必要があります。*導入例の下にある*「**PKI タイマーの依存関係」セクションを参照してください。**

PKI の更新/ロールオーバーの前提条件

ここでは、証明書ロールオーバーおよび更新操作について詳しく説明します。そのため、以下のイベントは正常に完了したものと見なします。

- 有効な CA 証明書を用いた PKI サーバの初期化。
- PKI サーバでの PKI クライアントの登録。つまり、各PKIクライアントにはCA証明書とID証明書（ルータ証明書）があります。

クライアントの登録には、以下のイベントが含まれます（詳細については扱いません）。

- トラストポイント認証
- トラストポイント登録

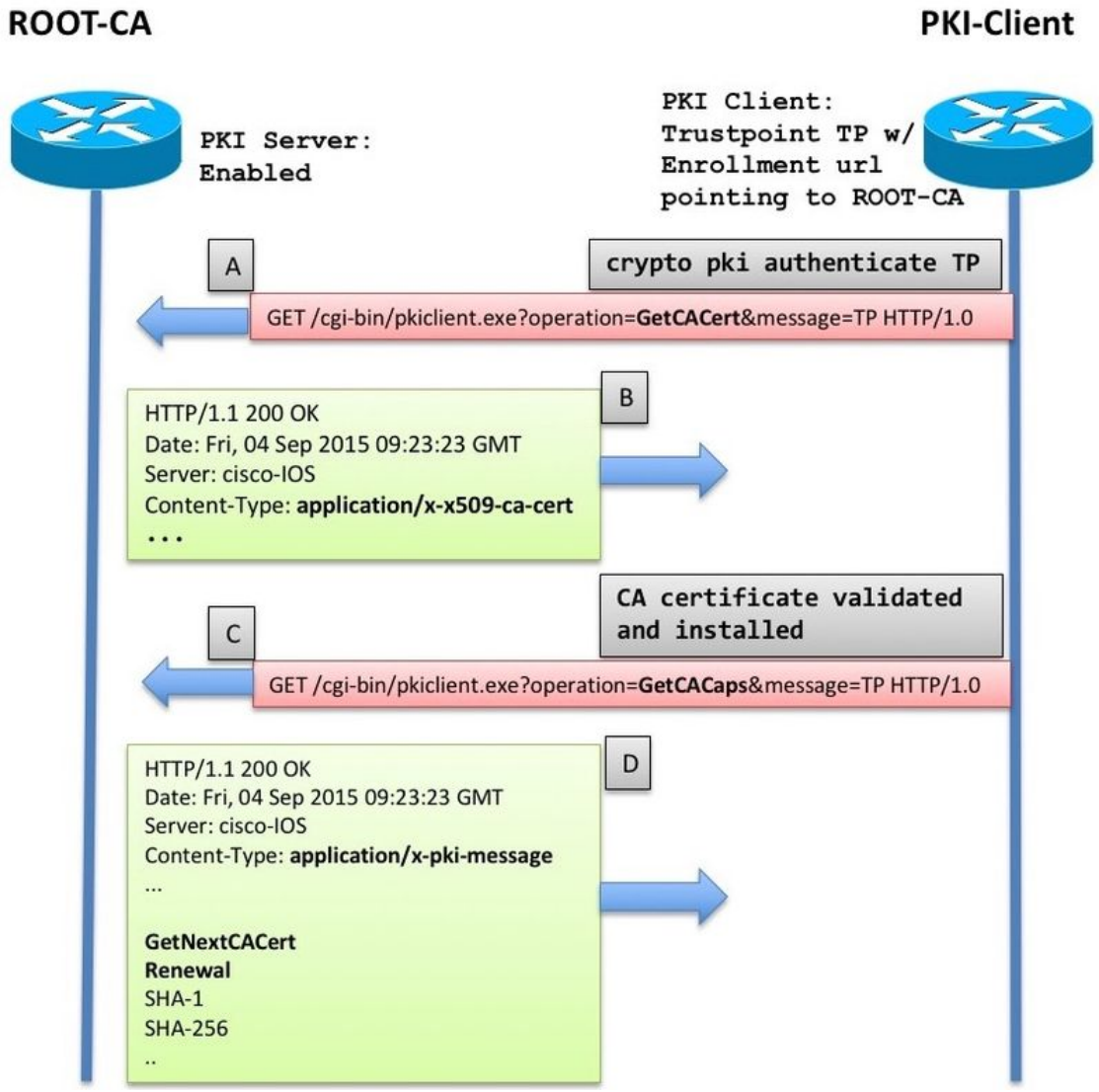
IOS では、トラストポイントは証明書のコンテナになります。1 つのトラストポイントには、1 つのアクティブな ID 証明書および/または 1 つのアクティブな CA 証明書を含めることができます。アクティブな CA 証明書が含まれている場合、トラストポイントは認証されていると見なされます。また、ID 証明書が含まれていると、登録されていると見なされます。登録前に、トラストポイントを認証する必要があります。トラストポイントの認証および登録とともに行う PKI サーバとクライアントの設定について詳しくは、『IOS PKI 導入ガイド：初期設計と展開』を参照してください。

CA 証明書の取得/インストールに続いて、PKI クライアントは登録を行う前に、PKI サーバ機能を取得します。CA の検索機能については、次のセクションで説明します。

CA 機能

IOS では、PKI クライアントが CA を認証すると、つまり管理者が IOS ルータにトラストポイントを作成してコマンド **crypto pki authenticate <trustpoint-name>** を実行すると、以下のイベントがルータで発生します。

- IOS は GetCACert 操作タイプを含む SCEP 要求を送信します。
- ここで期待される応答は、コンテンツ タイプが **application/x-x509-ca-cert（CA の導入の場合）、または application/x-x509-ca-ra-cert（RA および CA の導入の場合）である HTTP メッセージです。**また HTTP 本文には CA 証明書が含まれます（後者の場合、RA 証明書も含まれます）。
- CA/RA 証明書の取得とインストールに続いて、クライアントは GetCACaps 操作を含む自動 SCEP 要求を開始します。
- ここで期待される応答は、コンテンツ タイプが **application/x-pki-message** である HTTP メッセージです。また、タイプが **text/plain で、HTTP 本文に CA によってサポートされる一連の機能（ラインフィード文字で区切られます）が含まれるものも可能です。**一般的な IOS PKI サーバの応答は、次の図のようになります。



応答は、IOS PKI クライアントによって、次のように解釈されます。

```
CA_CAP_GET_NEXT_CA_CERT
CA_CAP_RENEWAL
CA_CAP_SHA_1
CA_CAP_SHA_256
```

このドキュメントでは、これらの機能のうち以下の 2 つに焦点を合わせます。

GetNextCACert

この機能が CA によって返されると、IOS は、CA がサポートする CA 証明書ロールオーバーを把握します。この機能が返されるときに、**auto-enroll コマンドがトラストポイントで設定されていない場合、IOS は CA 証明書の有効期間の 90 % に設定されている SHADOW タイマーを初期化します。**

SHADOW タイマーが期限切れになると、IOS は GetNextCACert SCEP 操作を実行して、ロールオーバー CA 証明書をフェッチします。

> 注**意**:**auto-enrollコマンドがトラストポイントの下にenrollment urlと共に設定されている場合**は、トラストポイントの認証前にRENEWタイマーが初期化され、トラストポイントが認証されるまで実際の登録メッセージ[CSR]は送信されません。

> **注：サーバで auto-rollover が設定されていない場合、GetNextCACert は IOS PKI サーバによって、機能として送信されます。**

更新

この機能により、PKI サーバは、既存の証明書を更新するために、アクティブな ID 証明書を使用して証明書署名要求に署名できることを PKI クライアントに通知します。

詳細については、**「PKI クライアントの自動更新」セクションを参照してください。**

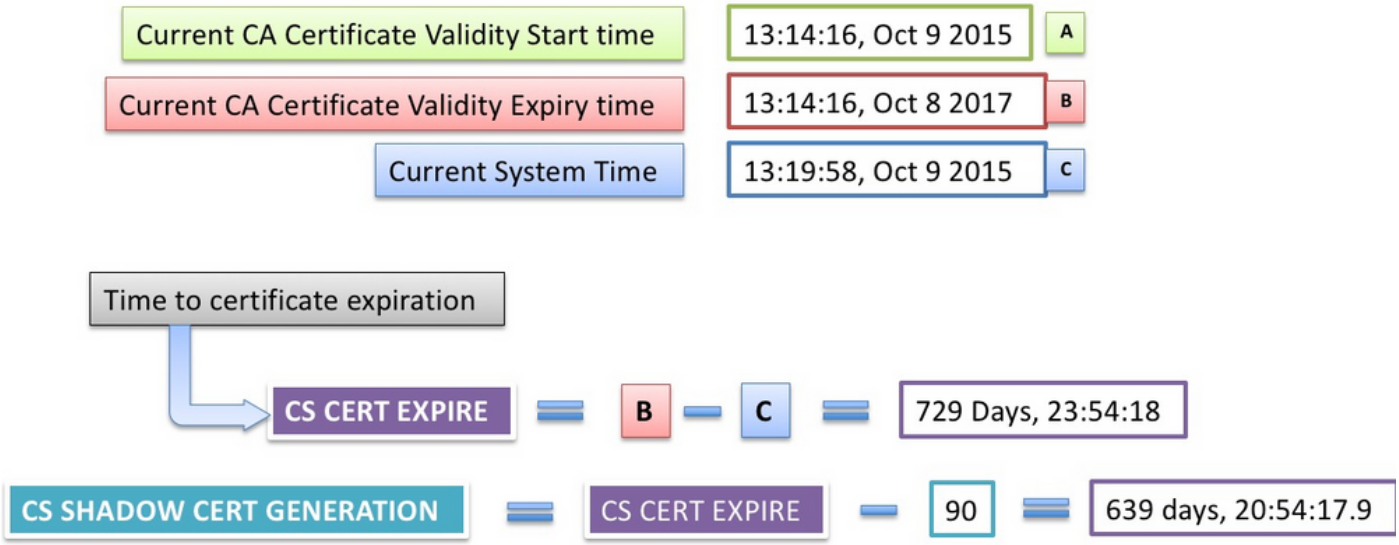
PKI サーバの自動ロールオーバー

上記の CA サーバの設定は、次のようになります。

```
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
```

以下に注目してください。



ロールオーバー オプション

CS SHADOW CERT GENERATION タイマーが期限切れになる場合：

- 最初に IOS はロールオーバーのキー ペアを生成します。この時点では、アクティブなキー ペアと同じ名前に # (ハッシュ) が付けられています。

```
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
```

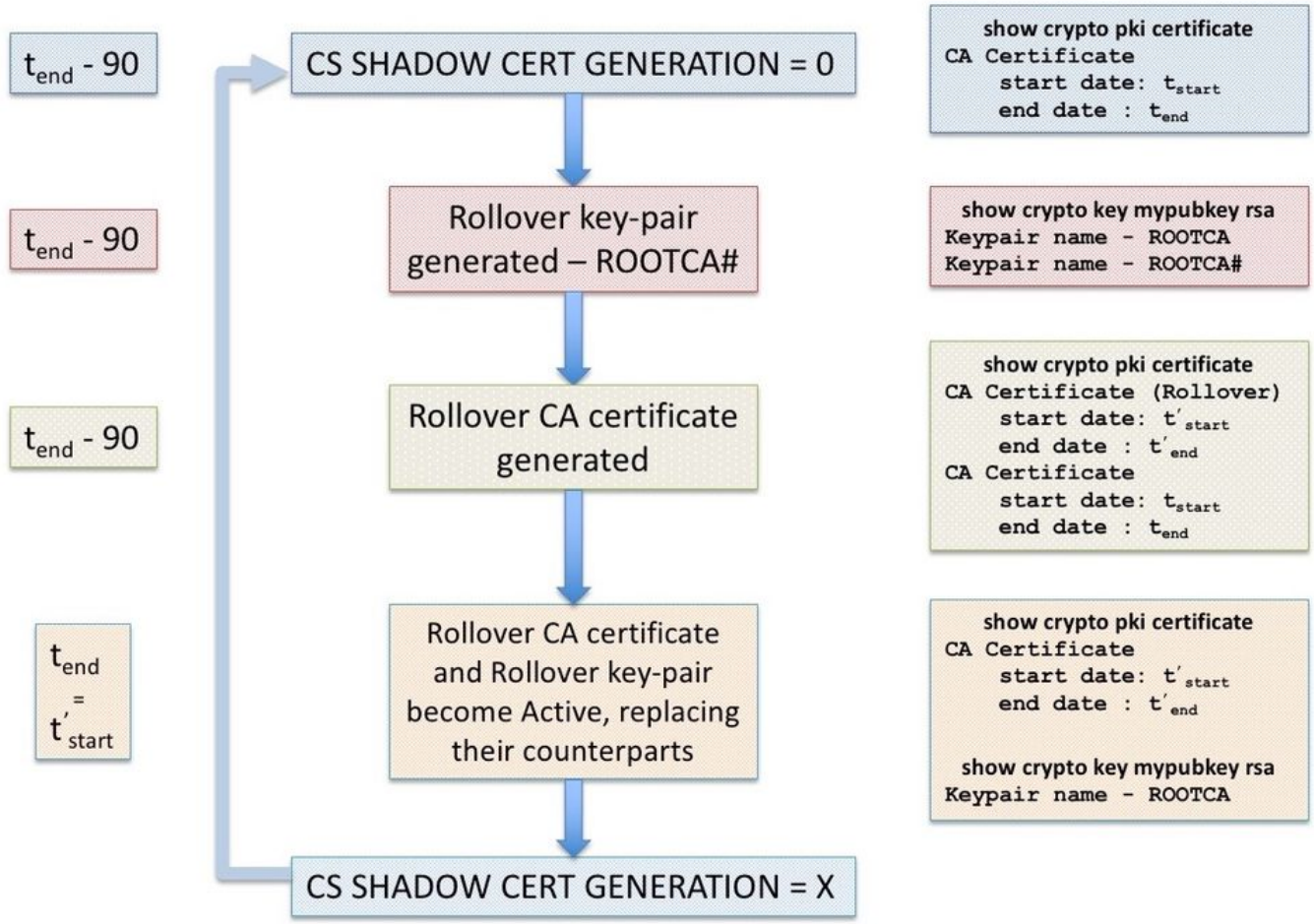
- 有効期間の開始日が現在のアクティブな CA 証明書の有効期間の終了日と同じである場合、次に IOS はロールオーバー CA 証明書を生成します。

```
    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 サーバの手動ロールオーバー

IOS PKI サーバは CA 証明書の手動ロールオーバーをサポートします。つまり、管理者は、事前に PKI サーバ設定で自動ロールオーバーを設定せずに、ロールオーバー CA 証明書の生成をトリガーできます。最初に導入した CA サーバの有効期間を拡張する予定があるかどうかに関わらず、万が一に備えて自動ロールオーバーを設定することを強くお勧めします。**PKIクライアントは、ロールオーバーCA証明書なしでCAをオーバーロードできます。***PKIサーバのロールオ*[ーバーにおけるクライアントSHADOW操作の依存関係を参照してください](#)。

次の設定レベルのコマンドを使用して、手動ロールオーバーをトリガーできます。

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

また、次のコマンドを使用して、新たに手動で作成するために、ロールオーバー CA 証明書をキャンセルすることもできます。ただし、実稼働環境では実行すべきではありません。

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

これにより、ロールオーバー RSA キー ペアとロールオーバー CA 証明書が削除されます。これは次の理由で推奨されます。

- CA がロールオーバー証明書を生成すると、複数のクライアントがロールオーバー CA 証明書と、ロールオーバー CA 証明書によって署名されたロールオーバー クライアント証明書をダウンロードすることができます。

- この段階でロールオーバーをキャンセルした場合、クライアントの再登録が必要になる場合があります。

PKI クライアントの自動更新

クライアント証明書更新のタイプ：RENEW と SHADOW

PKI サーバの IOS は、クライアントに発行された ID 証明書の有効期限が CA 証明書の有効期限を超えないようにします。

PKI クライアントで、IOS は更新操作をスケジュールする前に、必ず次のタイマーを考慮に入れます。

- 更新される ID 証明書の有効期限
- 発行者の（CA）証明書の有効期限

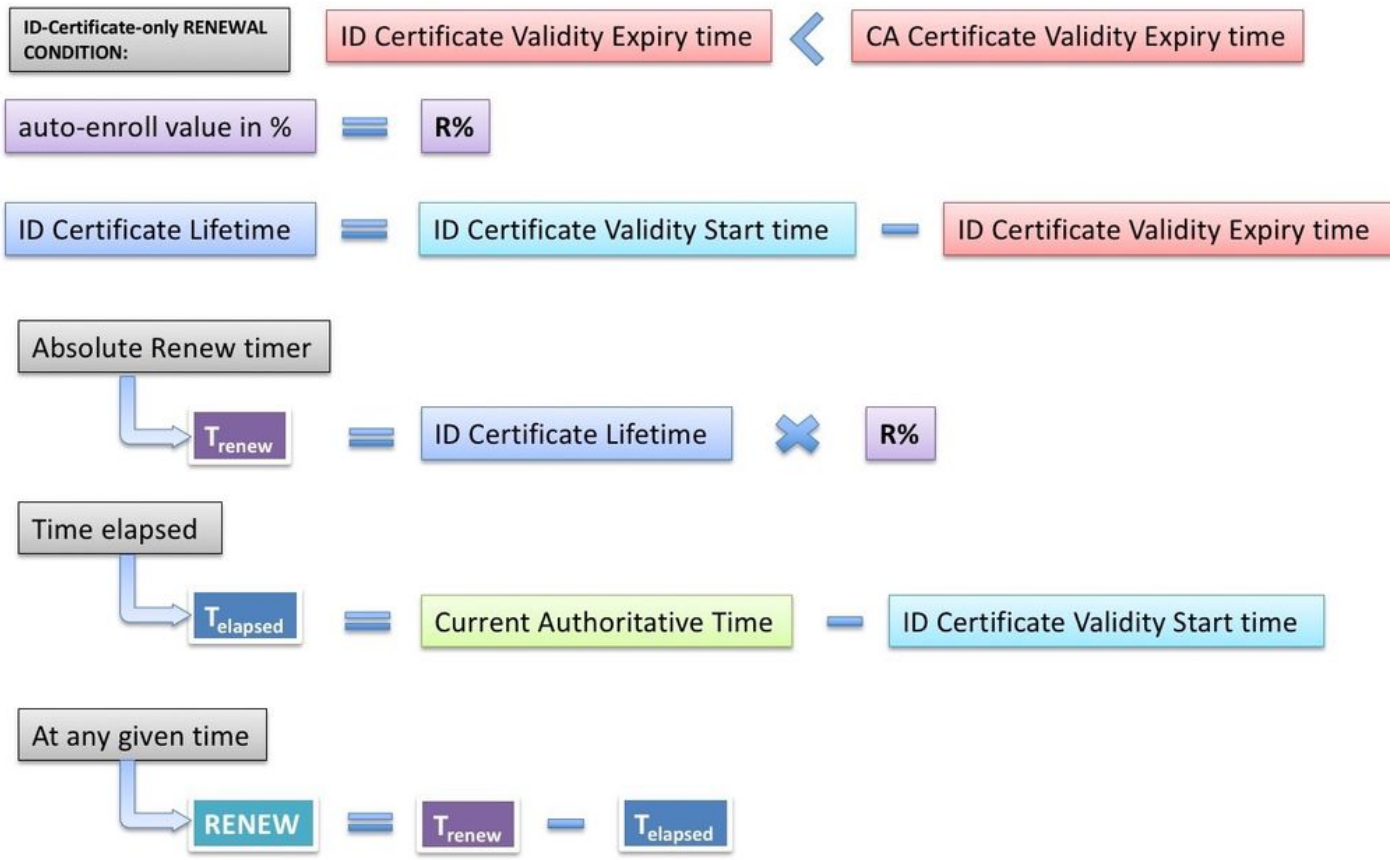
ID 証明書の有効期限が CA 証明書の有効期限と同じでない場合、IOS は簡単な更新操作を行います。

ID 証明書の有効期限が CA 証明書の有効期限と同じ場合、IOS はシャドウ更新操作を行います。

RENEW – ルータID証明書の更新

前述のとおり、ID 証明書の有効期限が CA 証明書の有効期限と同じでない場合、IOS PKI クライアントは簡単な更新操作を実行します。つまり発行者の証明書の前に失効する ID 証明書は、ID 証明書の簡単な更新をトリガーします。

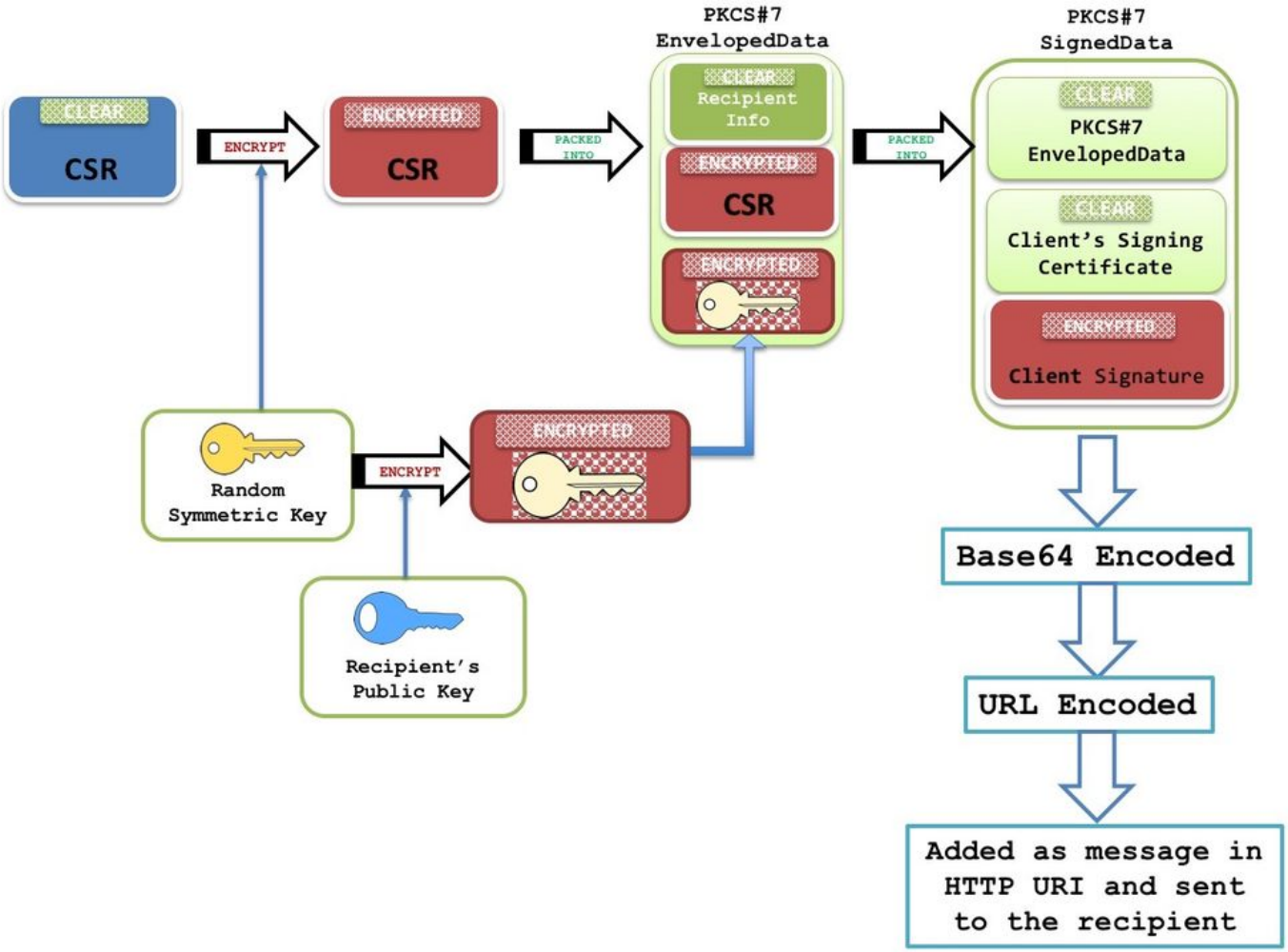
ID 証明書がインストールされるとすぐに、IOS は以下に示すように特定のトラストポイントの RENEW タイマーを計算します。



現在の正規の時刻（Current-Authoritative-Time）は、ここで示されているように、システム クロックが正規の時刻源となる必要があることを意味します（「正規の時刻源」セクションを参照）。PKI タイマーは正規の時刻源なしには初期化されません。そのため、更新操作は行われません。

次のイベントは、RENEW タイマーが期限切れになると発生します。

- IOS は、**regenerate が設定されている場合に、シャドウ キー ペアを生成します（例**：auto-enroll 80 regenerate）。**regenerate が設定されない場合、IOS は現在アクティブな RSA キー ペアを再利用します。**
- IOS は PKCS-7 エンベロープに暗号化される PKCS-10 形式の証明書要求を作成します。このエンベロープには、RecipientInfo（発行側 CA のサブジェクト名とシリアル番号）が含まれます。この PKCS7 エンベロープは、PKCS-7 署名済みデータに格納されます。最初の登録時に、IOS は、自己署名証明書を使用して、このメッセージに署名します。後続の登録（つまり再登録）中、IOS はアクティブな ID 証明書を使用してメッセージに署名します。PKCS7 署名済みデータは、署名する証明書（つまり、自己署名証明書または ID 証明書のいずれか）に組み込まれます。



このパケット構造の詳細については、SCEP の概要ドキュメントを参照してください。

注：ここでの重要な情報は、RecipientInfo（発行側 CA のサブジェクト名とシリアル番号）です。また、この CA の公開キーは対称キーの暗号化に使用されます。PKCS7 エンベロープの CSR は、この対称キーを使用して暗号化されます。

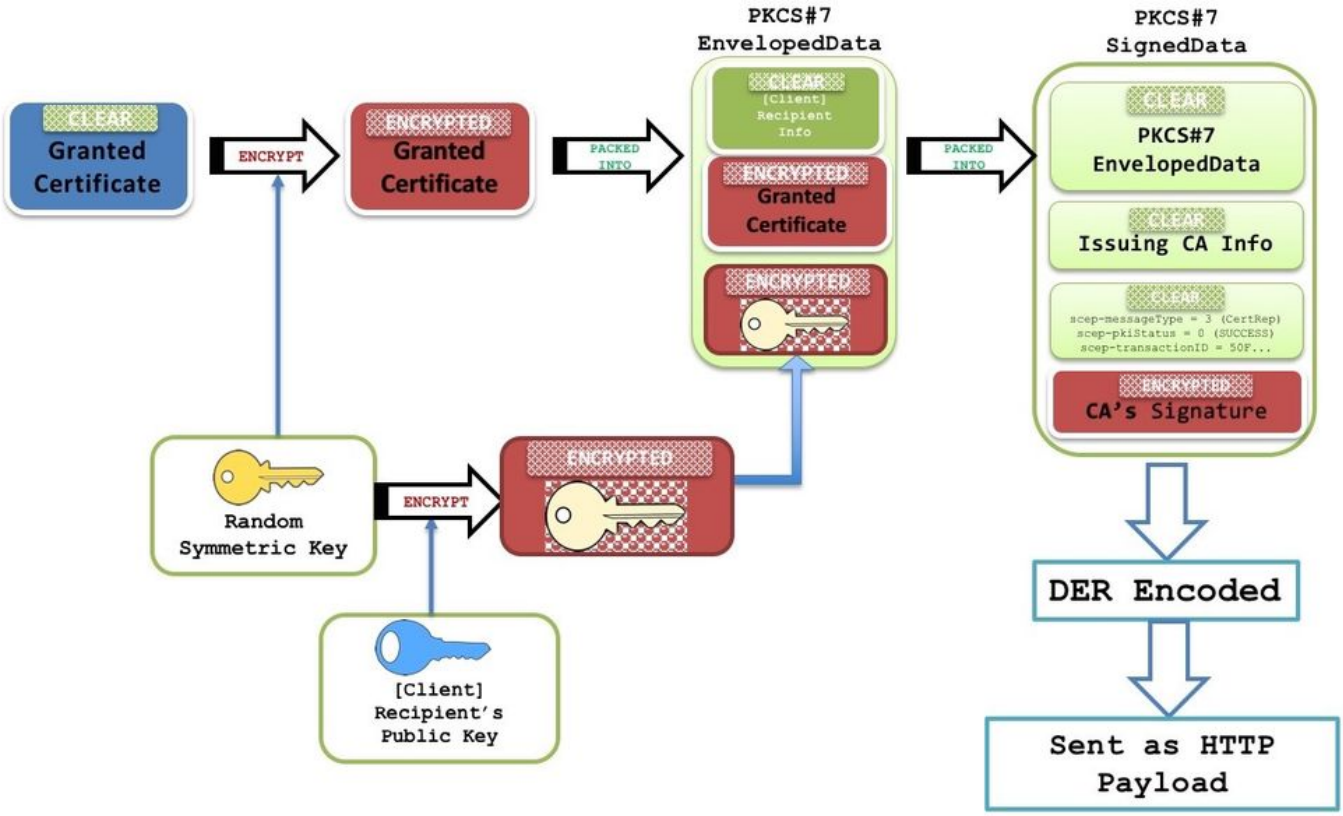
この暗号化された対称キーは、受信側 CA によって、秘密キーを使用して復号されます。この対称キーは CSR を公開する PKCS7 エンベロープを復号するために使用されます。

- PKCS7 形式でパッケージされたこの証明書署名要求（CSR）は、SCEP メッセージ タイプの PKCSReq および PKIOperation と呼ばれる SCEP 操作と一緒に CA に送信されます。
- CA が要求を拒否すると、IOS は RENEW タイマーを停止します。この時点で、ID 証明書を更新するために、管理者は手動更新を実行する必要があります（**「PKI クライアントの手動更新」セクションを参照）。**
- CA が SCEP ステータスを **pending** として送信する場合、PKI クライアントの IOS は POLL タイマーを 60 秒または 1 分から開始します。POLLタイマーが期限切れになるたびに、IOSはPKIOperation操作でGetCertInitial SCEPメッセージを送信します。最初のPOLLタイマーが期限切れになると、SCEP PendingステータスでGetCertInitialメッセージに応答すると、指数バックオフアルゴリズムは1分、再試行間隔2ですminutes、3番目のPOLLタイマーの再試行間隔は4分に続き、デフォルトでは次の999回の再試行、または発行CA証明書が期限切れになるまで続きます。
  以下を使用して、ポーリング カウントと最初の再試行期間を設定できます。

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

- 証明書が PKI サーバで許可されると、次の GetCertInitial SCEP メッセージに、コンテンツ タイプ **application/x-pki-message の HTTP メッセージと PKCS#7 署名データを含む本文で応答します。**この PKCS7 署名データには、**Granted** の SCEP ステータスと PKCS7 エンベロープ データが含まれます。この PKCS エンベロープ データには、許可された証明書と RecipientInfo が含まれます。この情報は、初回登録時の自己署名証明書と再登録時のアクティブな ID 証明書のサブジェクト名とシリアル番号です。

  PKCS7 エンベロープ データには、受信者の公開キー（新しい証明書が許可されたキー）で暗号化された対称キーが含まれています。 受信側のルータは、秘密キーを使って復号化します。この暗号化されていない対称キーが、新しい ID 証明書を公開する PKCS#7 エンベロープ データを復号するために使用されます。



- この段階で、IOS はすぐに既存の ID 証明書を新しい証明書と交換します。**regenerate が設定されている場合、シャドウ キー ペアもアクティブなキー ペアと交換されます。**

- また、<href **クライアント証明書更新のタイプ：RENEW と SHADOW> で説明されているように、RENEW タイマーまたは SHADOW タイマーのいずれを初期化する必要があるかを判断するために、新しい証明書の終了日が CA 証明書の終了日と比較されます。**