IOS PKI の自動登録、自動ロールオーバー、およびタイマー

目次

概要

自動登録および自動ロールオーバーの Cisco IOS ® 公開鍵インフラストラクチャ（PKI）オペレーションがどのようにはたらく、そしてどのようにそれぞれ PKI タイマーがこれらのオペレーションのために計算されるかこの資料に記述されています。

認証はライフタイムを固定し、ある時点で切れます。 認証が VPN ソリューションのために（たとえば）認証の目的で使用されれば、これらの認証の終止はエンドポイント間の VPN 接続の損失という結果に終る可能性のある 認証失敗の原因となります。 この問題を避けるために、これら二つのメカニズムは自動認証 更新に利用できます:

- クライアント/スポークルータのための自動登録
- Certification Authority（CA）サーバ ルータのための自動ロールオーバー

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 信頼の PKI および概念
- ルータの CA の基本設定

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

用語

自動登録

エンド デバイスの認証が約切れるとき自動登録は中断なしで新しい認証を得ます。 自動登録が設定されるとき、自身の認証が（アイデンティティか ID 認証として知られている）切れる前にクライアント/スポークルータは新しい認証をある時点で要求できます。

自動ロールオーバー

このパラメータは認証サーバ（CS）がロールオーバー（シャドウ）認証を生成すると決定します; コマンドが引数なしで CS 設定の下で入力される場合、既定の時刻は 30 日です。

> **注:** この資料の例に関しては、このパラメータの値は *10 分*です。

CA サーバの認証が約切れるとき自動ロールオーバーは中断なしで新しい認証を得ることを CA が可能にします。 自動ロールオーバーが設定されるとき、CA ルータは自身の認証が切れる前に新しい認証をある時点で生成できます。 *シャドウかロールオーバー* 認証呼ばれる新しい認証は現在の CA 認証が切れること精密な時点にアクティブになります。

この資料の概要 セクションで述べられる 2 つの機能の使用によって、PKI 配備は自動化されるようになり、スポークかクライアントデバイスがシャドウ/ロールオーバー ID証明得、現在の CA 認証終止前に/ロールオーバー CA 認証をシャドウイングするようにします。 こうすれば、それは新しい ID および CA証明に割り込みなしで電流 ID および CA証明が切れるとき移行できます。

ライフタイム CA 認証

このパラメータは CA 認証のライフタイムを規定 します。 このパラメータの値は幾日/時間/分に規定 することができます。

> **注:** この資料の例に関しては、このパラメータの値は *30 分*です。

ライフタイム 認証

このパラメータは CA ルータによって発行される ID証明のライフタイムを規定 します。 このパラメータの値は幾日/時間/分に規定 することができます。

> **注:** この資料の例に関しては、このパラメータの値は *20 分*です

設定

注: *ライフタイム*のより小さい PKI タイマー値は、自動*ロールオーバー*、この資料で使用されますキー自動登録しますおよび自動ロールオーバー概念を説明するために*自動登録し*。 実稼働中 の ネットワーク 環境では、Cisco はこれらのパラメータのためにデフォルトのライフタイムを使用することを推奨します。

ヒント： PKI タイマー ベース イベントすべては、*ロールオーバー*および*再登録*のような、信頼できる時刻ソースがない場合影響を受けます。 従って、Cisco はルータ全員の Network Time Protocol （ NTP ）をその peform PKI 設定することを推奨します。

Cisco IOS CA サーバコンフィギュレーション

このセクションは Cisco IOS CA サーバに configuratinon 例を提供します。

```
RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up RootCA#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 10.1.1.1 YES manual up up
```

注: 自動ロールオーバー コマンドで規定 される値はロールオーバー 認証が生成される*電流 CA certificatethat の終了日の前に*日数/時間/分です。 従って CA 認証が 12:00 から 12:30 まで有効なら、ロールオーバー CA 認証が 12:20 のまわりで生成されることをそして自動**ロールオーバー 0 は 0 10** 意味します。

Cisco IOS CA サーバの設定を確認するために**提示暗号 PKI certificate コマンドを**入力して下さい:

```
RootCA#show crypto pki certificate
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

この出力に基づいて、9:16 から 9:46 IST 2012 年 11 月 25 日であるルータは CA 認証がに有効含まれています。 自動ロールオーバーが 10 分の間設定されるので、シャドウ/ロールオーバー 認証は *9.36 IST* 2012 年 11 月 25 日によって生成されると期待されます。

確認するために、**提示暗号 PKI タイマー** コマンドを入力して下さい:

```
RootCA#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:22.283 IST Sun Nov 25 2012
```

```
PKI Timers
| 12:50.930
| 12:50.930 SESSION CLEANUP
CS Timers
| 16:43.558
| 16:43.558  CS SHADOW CERT GENERATION
| 26:43.532 CS CERT EXPIRE
| 26:43.558 CS CRL UPDATE
```

この出力に基づいて、**提示暗号 PKI タイマー** コマンドは 9.19 IST で発行され、シャドウ/ロールオーバー 認証は 16.43 分以内に生成されると期待されます:

[09:19:22 + 00:16:43] = である **09:36:05**、[end-date_of_current_CA_cert - auto_rollover_timer]; すなわち、[09:46:05 - 00:10:00] = **09:36:05**。

クライアント/スポークルータ 設定

このセクションはクライアント/スポークルータに設定例を提供します。

```
Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up Client-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0/0 172.16.1.1 YES manual up up
```

> **注: auto-enroll コマンドは**ルータの自動登録 機能を有効に します。 コマンドの構文は次のとおりです。 **自動登録して下さい**[*val%*] [*再生*]。

前の出力では、自動登録機能は 70% として規定 されます; すなわち、の 70% で**[current_ID_cert のライフタイム]**、ルータは CA と自動的に再登録します。

> **ヒント**： Cisco は PKI タイマーがきちんとはたらくようにするために 60% に自動登録値または多くを設定 したことを推奨します。

*再生*オプションは認証 再登録/更新目的で Rivest シャミールAddleman 新しい（ RSA ）キーの作成の原因となります。 このオプションが規定 されない場合、電流 RSA キーは使用されます。

処理の自動登録

自動登録 機能を確認するためにこれらのステップを完了して下さい:

1. 手動で クライアントルータのトラストポイントを認証するために**暗号 PKI 認証する** コマンドを入力して下さい:

   ```
   Client-1(config)#crypto pki authenticate client1
   ```

   注: このコマンドに関する詳細については、Cisco IOSセキュリティ コマンドレファレンスを参照して下さい。
   コマンドを入力すれば、これと同じような出力は現われる必要があります:

   ```
   Client-1(config)#crypto pki authenticate client1
   ```

2. **はい**型クライアントルータの CA 認証を受け入れるため。 それから、**更新**タイマーはルータで始まります:

```
Client-1#show crypto pki timer
PKI Timers
| 0.086
| 0.086 RENEW cvo-pki
| 9:51.366 SESSION CLEANUP
```

3. **更新**タイマーがゼロに達すれば、クライアントルータは CA と自動的に ID証明を得るためにそれ自身を登録します。 認証が受け取られたら、それを表示するために**提示暗号 PKI certificate コマンドを**入力して下さい:

```
Client-1#show crypto pki certificate
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:16:57 IST Nov 25 2012
end date: 09:36:57 IST Nov 25 2012
renew date: 09:30:08 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

更新日付は 09:30:08、ここに示されているように計算されます:

開始時刻 + （ ID_cert_lifetime の %renewal ）

または

09:16:57 + （ 70% * 20 分 ） = 09:30:08

PKI タイマーは同じを反映します:

```
Client-1#show crypto pki timer
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:19:01.714 IST Sun Nov 25 2012
PKI Timers
| 1:21.790
| 1:21.790 SESSION CLEANUP
| 11:06.894  RENEW client1
```

4. **更新**タイマーが切れれば新しい ID 認証を得るために、ルータは CA と再登録します。 認証更新が発生した後、新しい ID 認証を表示するために**提示暗号 PKI 証明書**コマンドを入力して下さい:

```
Client-1#show crypto pki cert
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:55.063 IST Sun Nov 25 2012
Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

もはや*更新日付が*ないことに注意して下さい; その代り、**シャドウ** タイマーは始まります:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

プロセス ロジックはここにあります:

- ID 認証の終了日が **CA 認証**の終了日と**等しくない**場合、自動登録パーセントに基づいて更新日付を計算し、**更新**タイマーを開始して下さい。

- ID 認証の終了日が **CA 認証**の終了日と**等しい**場合、再生過程は現在の CA 認証が有効である限りだけ電流 ID 認証が有効であるので必要ではないです。 その代り、**シャドウ** タイマーは開始します。

このタイマーはまた **auto-enroll コマンド**で述べられるパーセントに基づいて計算されます。 たとえば、前例で表示される更新された ID 認証の有効 日付を考慮して下さい:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618 SHADOW client1
```

この認証のライフタイムは 16 分です。 従って、ロールオーバー タイマー (すなわち、シャドウ タイマー) はおよそ 11 分に匹敵する 16 分の 70% です。 この計算はルータがシャドウ/ロールオーバー 認証のための要求をで [09:30:09 + 00:11:00] = この資料で以前に示されている PKI シャドウ タイマーに対応する 09:41:09 始めることを意味します、:

```
Client-1#show crypto pki timer
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:34:57.922 IST Sun Nov 25 2012
PKI Timers
| 25.582
| 25.582 SESSION CLEANUP
| 6:20.618  SHADOW client1
```

処理の自動ロールオーバー

このセクションは操作で自動ロールオーバー 機能を説明しています。

Cisco IOS CA サーバ

シャドウ タイマーが切れるとき、ロールオーバー 認証は CA ルータで現われます:

```
RootCA#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:36:28.184 IST Sun Nov 25 2012
CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
 start date: 09:46:05 IST Nov 25 2012
end   date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

```
CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: ios-ca
```

クライアントルータ

この資料に以前に説明があられるように、自動登録 機能はクライアントルータのシャドウ タイマーを始めました。 シャドウ タイマーが切れるとき、自動登録 機能は*ロールオーバー/シャドウ CA 認証*のために CA サーバを要求することをルータが可能にします。 受け取られて、それは*ロールオーバー/シャドウ ID* 認証のために同様に問い合わせます。 その結果、ルータに認証の 2 つのペアがあります: 現在であるおよびロールオーバー/シャドウ 認証が含まれている他のペア 1 つのペア:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
```

```
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

ロールオーバー ID 認証の有効性に注意して下さい:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
```

```
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

認証 ライフタイムはちょうど 4 分です（Cisco IOS CA サーバで設定される期待された 20 分の代りに、）。 Cisco IOS CA サーバごとに、*絶対* ID 認証 ライフタイムはであるそれに発行される

ID 認証（電流 + シャドウ）のライフタイムの合計を 20 分より大きくなければならない意味する）20 分（、ある特定のクライアントルータのために、はずです。

このプロセスは更にここに説明されます:

- ルータの電流 ID 認証の有効性はここにあります:

```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
```

```
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

従って、*current_id_cert_lifetime は* 16 分です。

- ロールオーバー ID 認証の有効性はここにあります:

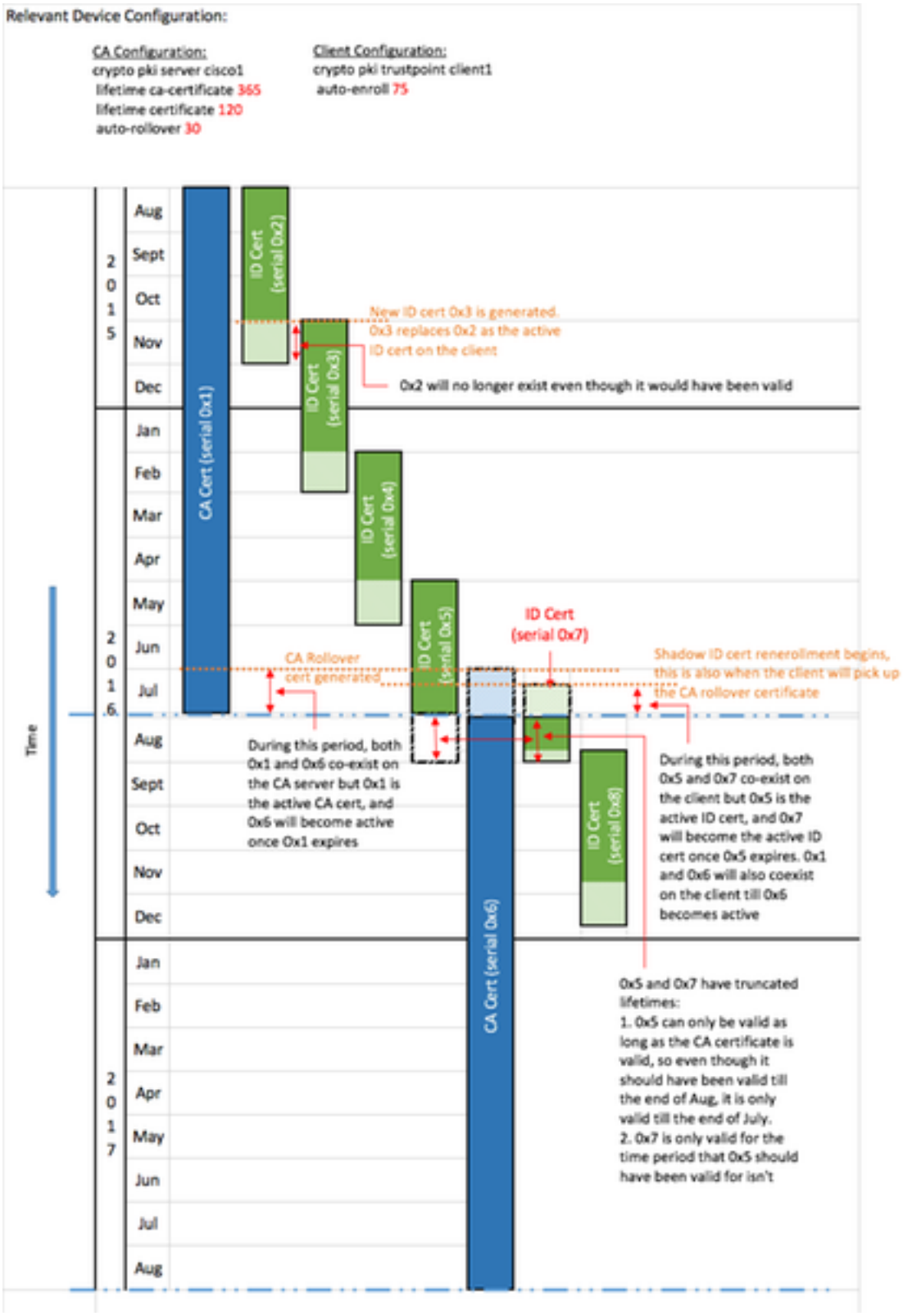
```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 09:50:09 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Root-CA
cn=Root-CA
ou=TAC
```

```
c=IN
Validity Date:
start date: 09:46:05 IST Nov 25 2012
end date: 10:16:05 IST Nov 25 2012
Associated Trustpoints: client1

Certificate
Status: Available
Certificate Serial Number (hex): 03
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
Name: Client-1
hostname=Client-1
cn=Client-1
ou=TAC
c=IN
CRL Distribution Points:
http://10.1.1.1/cgi-bin/pkiclient.exe?operation=GetCRL
Validity Date:
start date: 09:30:09 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1

CA Certificate
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
ou=TAC
c=IN
Validity Date:
start date: 09:16:05 IST Nov 25 2012
end date: 09:46:05 IST Nov 25 2012
Associated Trustpoints: client1
```

従って、*rollover_id_cert_lifetime は* 4 分です。

- Cisco IOS ごとに、[current_id_cert_lifetime]に[rollover_id_cert_lifetime]追加される時、それは匹敵する必要があります[total_id_cert_lifetime]。 これはこの場合本当です。

ロールオーバーおよび登録を用いるサンプル PKI タイムライン



重要な考慮事項

- PKI タイマーは適切に機能するために保証された クロックが要求します。 Cisco はクライアントルータと Cisco IOS CA ルータ間のクロックを同期化するために NTP を使用することを推奨します。 NTP がない時、ルータのシステム/ハードウェア クロックは使用することができます。 ハードウェア クロックを設定し保証されたようにする方法の情報に関しては基本システム管理 コンフィギュレーション ガイドを、Cisco IOS Release 12.4T 参照して下さい。

- ルータのリロードに、NTP の同期は頻繁に数分かかります。 ただし、PKI タイマーはほとん

どすぐに確立されます。 バージョン 15.2(3.8)T および 15.2(4)S 現在で、PKI タイマーは自動的に NTP が同期された後再評価されます。

- PKI タイマーは絶対ではないです; 従ってそれらは再度ブートするの後で*残りの時間*に計算し直されます基づき。 たとえばクライアントルータが 100 日間有効であり、自動登録機能が 80% に設定 される ID 認証を備えていることを、仮定して下さい。 それから、再登録は第 80 日以降に発生すると期待されます。 ルータが第 60 日にリロードされる場合、起動し、ここに示されているように PKI タイマーを計算し直します: （*残りの時間*）* （%auto *登録して下さい*）=（100-60）* 80% の = 32 日。

  従って、再登録はに [60 + 32] = 第 92 日発生します。

- 自動登録および自動rollovertimers を設定するとき、PKI サーバのシャドウ CA 認証 アベイラビリティをとき PKI Client 要求 1 可能にする値でそれらを設定することは重要です。 これは大規模 な 環境の潜在的な PKI サービス失敗の軽減を助けます。

関連情報

- Public-Key Infrastructure Whitepaper の Cisco IOSセキュリティの展開
- 公開鍵インフラストラクチャ: 配備ベネフィットおよび機能 Whitepaper
- 公開キー インフラストラクチャ構成ガイド
- テクニカルサポートとドキュメント - Cisco Systems