IOS PKI自动注册、自动反转和计时器

目录

简介

本文描述自动注册和自动反转的Cisco IOS公共密钥基础设施(PKI)操作如何工作，并且各自PKI计时器如何为这些操作计算。

证书修复寿命并且超时。如果证书为认证的目的使用VPN解决方案(例如)，终止这些证书导致导致VPN连接损耗终端之间的可能的认证失败。为了避免此问题，这两机制为自动证书续订是可用的：

- 客户端/分支路由器的自动注册
- 认证机构(CA)服务器路由器的自动反转

先决条件

要求

Cisco 建议您了解以下主题：

- PKI和信任的概念
- CA基本配置在路由器的

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认

）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

术语

自动注册

当在终端设备的一证书将超时时，自动注册获取新证书，不用中断。当自动注册配置时，客户端/分支路由器能某时要求新证书，在其自己的证书(叫作其标识或ID证书)前超时。

自动反转

此参数决定，当证书服务器(CS)生成其反转(Shadow)证书;如果命令被输入在CS配置下，不用任何参数，默认时间是30天。

> **注意**：对于在本文的示例，值此参数是*10分钟*。

当在CA服务器的一证书将超时时，自动反转使CA获取新证书，不用中断。当自动反转配置时，CA路由器能某时生成新证书，在其自己的证书超时前。新证书，呼叫*Shadow*或*反转*证书，准时变得激活当前CA证书超时。

使用在本文的介绍部分被提及的使用两个功能， PKI部署变得自动化并且允许分支或客户端设备获得Shadow/反转身份证书和在当前CA证书终止之前遮蔽/反转CA证书。当其当前ID和CA证书超时时，这样，它能过渡，不用中断到新的ID和CA证书。

寿命CA证书

此参数指定CA证书的寿命。值此参数可以以几天/几小时/分钟指定。

> **注意**： 对于在本文的示例，值此参数是*30分钟*。

寿命证书

此参数指定由CA路由器发出身份证书的寿命。值此参数可以以几天/几小时/分钟指定。

> **注意**： 对于在本文的示例，值此参数是*20分钟*

配置

> **注意**： *寿命*、自动*反转*和*自动注册的更加*小的PKI计时器值用于本文为了说明关键自动注册和自动反转概念。在真实网络环境，思科建议您使用默认寿命这些参数。

> **提示**： 如果没有可信的时间源，所有PKI基于定时器的事件，例如*反转*和*重新注册*，可以受影响。为此，思科建议您配置在所有的网络时间协议(NTP)路由器该peform PKI。

Cisco IOS CA服务器配置

此部分为Cisco IOS CA服务器提供一示例configuratinon。

```
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
```

> **注意**： 用自动**反转**命令指定的值是几天/几小时/分钟数量*在*反转证书生成*当前CA certificatethat的结束日期前*。所以，如果CA证书从12:00是有效到12:30，然后自动**反转0 0 10**暗示反转CA证书在12:20附近生成。

输入**certificate命令显示crypto的pki**为了验证在Cisco IOS CA服务器的配置：

```
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
```

凭此输出，从9:16是有效到9:46 IST十一月25的路由器包括CA证书， 2012。因为自动反转配置在10分钟， Shadow/反转证书预计由*9.36 IST*十一月25生成， 2012。

为了确认，请输入**显示crypto pki计时器**命令：

```
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
```

凭此输出，**显示crypto pki计时器**命令发出在9.19 IST，并且Shadow/反转证书预计在16.43分钟内生成：

[09:19:22 + 00:16:43] = **09:36:05**，是[end-date_of_current_CA_cert - auto_rollover_timer];即[09:46:05 - 00:10:00] = **09:36:05**。

客户端/分支路由器配置

此部分为客户端/分支路由器提供一配置示例。

```
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
```

> **注意**： **auto-enroll命令**启用在路由器的自动注册功能。 命令语法为： **自动注册**[val%] [regenerate]。

在上一个输出中，自动注册功能指定作为70%;即在70% **[lifetime of current_ID_cert]**，路由器自动地重新登记与CA。

> **提示**： 思科建议您设置自动注册值到60%或更多为了保证PKI计时器正常运转。

*再生*选项导致一新的Rivest沙米尔Addleman (RSA)密钥的创建证书重新注册/续订目的。如果此选项没有指定，使用当前RSA密钥。

在操作的自动注册

完成这些步骤为了验证自动注册功能：

1. 输入**crypto pki验证**命令为了手工验证在客户端路由器的信任点：

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

   注意：关于此命令的更多信息，参考Cisco IOS安全命令参考。
   一旦输入命令，输出类似于此应该出现：

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

2. 键入**是**为了接受在客户端路由器的CA证书。然后，**更新**计时器在路由器开始：

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

3. 一旦**更新**计时器到达零，客户端路由器自动地登记以CA为了获取其身份证书。一旦证书接收，请输入**certificate命令显示crypto的pki**为了查看它：

   ```
   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
```

更新日期是09:30:08和计算如显示此处：

开始时间+ (ID_cert_lifetime %renewal)

或者

09:16:57 + (70% * 20分钟) = 09:30:08

PKI计时器反射同样：

```
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. 一旦**更新**计时器超时，路由器重新登记以CA为了获取一新的ID证书。在证书续订发生后，请输入**显示crypto pki cert**命令为了查看新的ID证书：

```
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
```

注意不再有*更新日期*;反而， SHADOW计时器开始：

```
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
```

这是进程逻辑：

- 如果ID证书的结束日期与CA证书的结束日期不是相等的，则请计算根据自动注册百分比的更新DATE并且启动更新计时器。
- 如果ID证书的结束日期与CA证书的结束日期是相等的，则更新过程不是必要的，因为当前ID证书有效，只有只要当前CA证书有效。反而， SHADOW计时器开始。

此计时器根据在auto-enroll命令提及的百分比也计算。例如，请考虑在前一个示例显示更新的ID证书的有效日期：

```
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
```

寿命此证书是16分钟。所以，反转计时器(即SHADOW计时器)是70% 16分钟，等于大约11分钟。此计算暗示路由器开始要求其Shadow/反转证书在[09:30:09 + 00:11:00] = 09:41:09，对应于在本文以前显示的PKI SHADOW计时器：

```
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
```

在操作的自动反转

此部分描述在操作的自动反转功能。

在Cisco IOS CA服务器上

当SHADOW计时器超时时，反转证书出现在CA路由器：

```
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
```

在客户端路由器

如以前描述在本文，自动注册功能开始在客户端路由器的一个SHADOW计时器。当SHADOW计时器超时时，自动注册功能使路由器请求*反转/Shadow CA证书的*CA服务器。一旦接收，它查询其*反转/Shadow ID*证书。结果，路由器有两个对证书：当前的一个对和包含反转/Shadow证书的另一个对：

```
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
```

注意反转ID证书的正确性：

```
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
```

证书寿命是四分钟(而不是预计20分钟，如配置在Cisco IOS CA服务器)。每个Cisco IOS CA服务器，*绝对*ID证书寿命应该是(为一个给的客户端路由器比20分钟含义， ID证书的20分钟(当前+ Shadow)寿命的总和发出对它不能极大)。

此进程进一步描述此处：

- 这是当前ID证书的正确性在路由器的：

```
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
```

所以， *current_id_cert_lifetime*是16分钟。

- 这是反转ID证书的正确性：

```
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

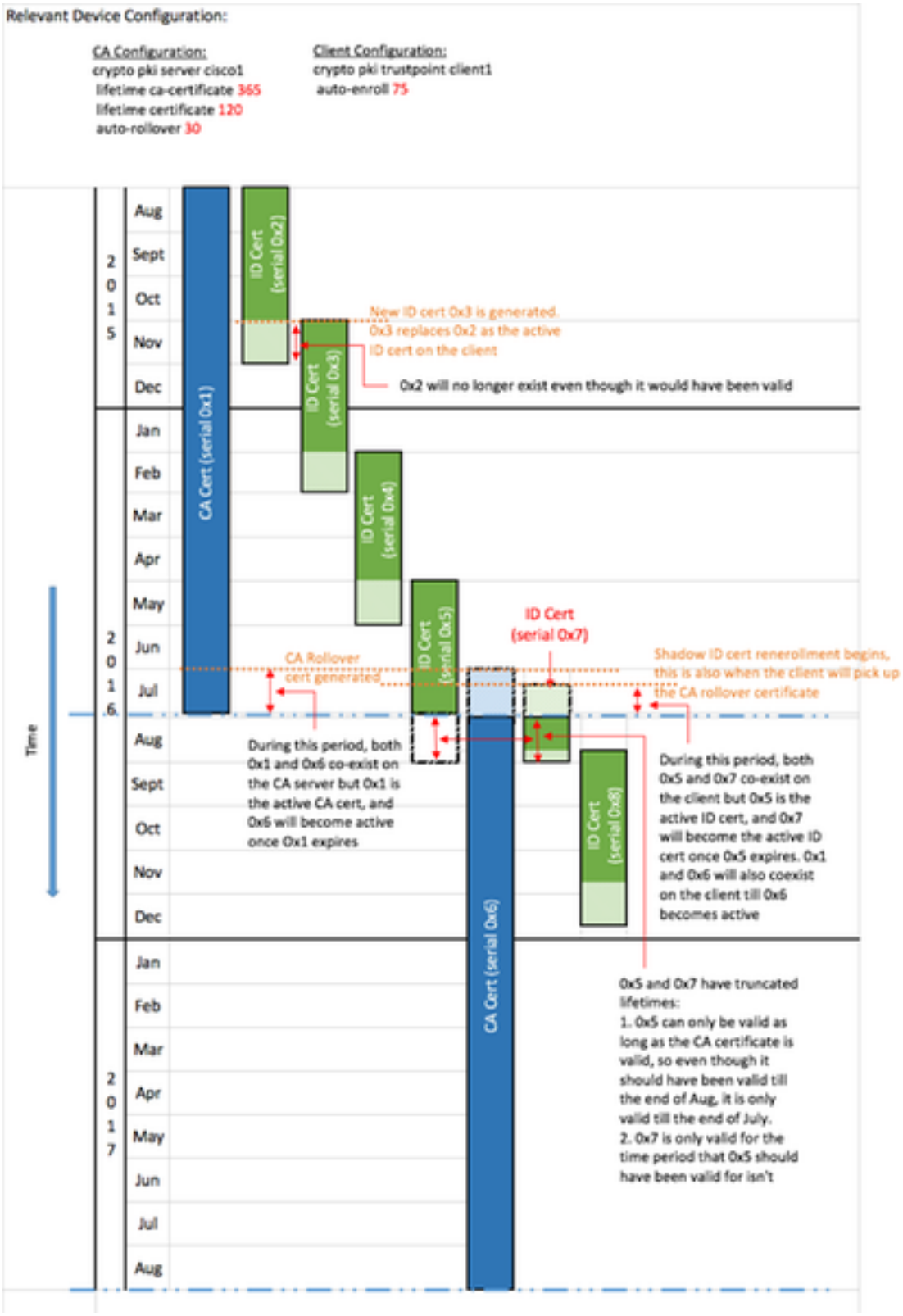
```
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=Root-CA
ou=TAC
c=IN
Subject:
cn=Root-CA
```

```
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
```

所以， *rollover_id_cert_lifetime*是四分钟。

- 每Cisco IOS，当[current_id_cert_lifetime]被添加到[rollover_id_cert_lifetime]时，它必须等于[total_id_cert_lifetime]。这在此实例中是真的。

与反转和登记的示例PKI时间安排



重要考虑事项

- PKI计时器要求一个授权时钟为了正常运行。思科建议您使用NTP为了同步在客户端路由器和Cisco IOS CA路由器之间的时钟。在没有NTP时，可以使用系统/硬件时钟在路由器。关于如何配置硬件时钟和使的信息授权，参考基本的系统管理配置指南， Cisco IOS版本12.4T。

- 在路由器的重新加载， NTP的同步经常花费几分钟。然而， PKI计时器几乎立即设立。自版本15.2(3.8)T和15.2(4)S，在NTP同步后， PKI计时器自动地被复评。

- PKI计时器不绝对;他们根据*剩余时间*和，因此，在重新启动以后重新计算。例如，假设客户端路由器有是有效在100天内，并且自动注册功能设置到80%的一ID证书。然后，重新注册预计在第80个天之后发生。如果路由器在第60个天重新加载，启动并且重新计算PKI计时器如显示此处： (*剩余时间*) * (请%auto*登记*) = (100-60) * 80% = 32天。

  所以，重新注册在发生[60 + 32] =第92个天。

- 当您配置自动注册和自动rollovertimers时，用允许SHADOW在PKI服务器的CA证书可用性的值配置他们是重要的，当PKI客户端要求一时。这帮助缓和一个大规模环境的潜在的PKI服务失败。

相关信息

- **部署与公钥基础架构Whitepaper的Cisco IOS安全**
- **公共钥匙结构：部署好处和功能Whitepaper**
- **公共钥匙结构配置指南**
- **技术支持和文档 - Cisco Systems**