Автоматическая регистрация PKI IOS, Auto-Rollover и таймеры

Содержание

Введение

Этот документ описывает, как Cisco, использование IOS® Public Key Infrastructure (PKI) автоматической подачи заявок и auto-rollover работает и как соответствующие таймеры PKI вычислены для этих операций.

Сертификаты исправили сроки службы и истекают в некоторый момент. Если сертификаты используются для целей аутентификации для решения для VPN (например), истечение этих сертификатов приводит к возможным ошибкам проверки подлинности, которые приводят к потере возможности VPN - подключения между оконечными точками. Во избежание этой проблемы эти два механизма доступны для автоматического обновления сертификата:

- Автоматическая подача заявок для клиента/маршрутизаторов на конце луча
- Auto-Rollover для сервера - маршрутизатора Центра сертификации (CA)

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- PKI и понятие доверия
- Базовая конфигурация CA на маршрутизаторах

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Терминология

автоматическая подача заявок

Когда сертификат на конечном устройстве собирается истечь, автоматическая подача заявок получает новый сертификат без разрушения. Когда автоматическая подача заявок настроена, клиент/маршрутизатор на конце луча может запросить новый сертификат в некоторое время, прежде чем истечет его собственный сертификат (известный как его идентичность или сертификат ID).

auto-rollover

Когда Сервер сертификатов (CS) генерирует свое одновременное нажатие клавиш (тень) сертификат, этот параметр решает; если команда введена под конфигурацией CS без какого-либо аргумента, время по умолчанию составляет 30 дней.

> **Примечание:** Для примеров в этом документе значение этого параметра составляет *10 минут*.

Когда сертификат на сервере CA собирается истечь, auto-rollover позволяет CA получить новый сертификат без разрушения. Когда auto-rollover настроен, маршрутизатор CA может генерировать новый сертификат в некоторое время, прежде чем истечет его собственный сертификат. Новый сертификат, который называют *тенью* или сертификатом *одновременного нажатия клавиш*, становится активным в точный момент, что истекает текущий сертификат CA.

С использованием двух функций, которые упомянуты в разделе Введения этого документа, развертывания PKI становятся автоматизированными и позволяют лучу или устройству клиента получать сертификат идентификации тени/одновременного нажатия клавиш и сертификат CA тени/одновременного нажатия клавиш до текущего истечения сертификата CA. Когда его текущий ID и сертификаты CA истекают, Таким образом, это может перейти без прерывания к новому ID и сертификатам CA.

пожизненный сертификат CA

Этот параметр задает срок действия сертификата CA. Значение этого параметра может быть задано в днях/часах/минутах.

> **Примечание:** Для примеров в этом документе значение этого параметра составляет *30 минут*.

пожизненный сертификат

Этот параметр задает срок действия сертификата идентификации, который выполнен маршрутизатором CA. Значение этого параметра может быть задано в днях/часах/минутах.

> **Примечание:** Для примеров в этом документе значение этого параметра составляет *20 минут*

Настройка

> **Примечание:** Меньшие значения таймера PKI для *срока действия*, *auto-rollover* и *автоматической регистрации* используются в этом документе для иллюстрирования ключевой автоматической регистрации и понятий auto-rollover. В среде действующей сети Cisco рекомендует использовать стандартные сроки действия для этих параметров.

> **Совет:** Весь PKI, на основанные на таймере события, такие как *одновременное нажатие клавиш* и *перерегистрация*, можно влиять, если нет никакого надежного источника времени. Поэтому Cisco рекомендует настроить сетевой Протокол времени (NTP) на всех маршрутизаторах, которые выполняют PKI.

Cisco IOS CA конфигурация сервера

Этот раздел предоставляет пример configuratinon для Cisco IOS CA сервер.

```
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
```

> **Примечание:** Значение, которое задано с **командой auto-rollover** , является количеством дней/часов/минут *, прежде чем* будет генерироваться *дата завершения текущего CA certificatethat* сертификат одновременного нажатия клавиш. Поэтому, если сертификат CA допустим от 12:00 до 12:30, то **auto-rollover 0 0 10** подразумевает, что сертификат CA одновременного нажатия клавиш генерируется вокруг 12:20.

Введите **показ крипто-**команда **сертификата pki** для проверки конфигурации на Cisco IOS CA сервер:

```
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
```

На основе этих выходных данных маршрутизатор включает сертификат CA, который допустим с 9:16 до 9:46 IST 25 ноября 2012. Так как auto-rollover настроен в течение 10 минут, сертификат тени/одновременного нажатия клавиш, как ожидают, будет генерироваться *к 9:36 IST* 25 ноября 2012.

Для подтверждения введите **показ крипто-команда timer pki**:

```
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
```

На основе этих выходных данных **показ крипто-команда timer pki** была выполнена в 9:19 IST, и сертификат тени/одновременного нажатия клавиш, как ожидают, будет генерироваться в течение 16.43 минут:

[9:19:22 + 0:16:43] = **9:36:05**, который является [конец-date_of_current_CA_cert - auto_rollover_timer]; т.е. [9:46:05 - 0:10:00] = **9:36:05**.

Конфигурация Клиента/Маршрутизатора на конце луча

Этот раздел предоставляет пример конфигурации для клиента/маршрутизатора на конце луча.

```
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
```

> **Примечание: Команда auto-enroll** активирует опцию автоматической подачи заявок на маршрутизаторе. Синтаксис команды: **автоматические регистрации** [*val %*] *[восстанавливают]*.

В предыдущих выходных данных функция автоматической регистрации задана как 70%; т.е. в 70% **[срок действия current_ID_cert]**, маршрутизатор автоматически повторно регистрируется с CA.

> **Совет:** Cisco рекомендует установить значение автоматической регистрации в 60% или больше чтобы гарантировать, что таймеры PKI работают должным образом.

Опция regenerate приводит к созданию нового ключа алгоритма цифровой подписи райвеста шамира адлемана (RSA) в целях перерегистрации/обновления сертификата. Если эта опция не задана, текущий ключ RSA используется.

Автоматическая подача заявок в действии

Выполните эти шаги для проверки функции автоматической подачи заявок:

1. Введите **команду crypto pki authenticate** для ручной аутентификации точки доверия на клиентском маршрутизаторе:

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

   Примечание: Для получения дополнительной информации об этой команде обратитесь к Справочнику по командам Безопасности Cisco IOS.
   Как только вы вводите команду, выходные данные, подобные этому, должны появиться:

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

2. Введите **да** для принятия сертификата CA на клиентском маршрутизаторе. Затем таймер **RENEW** начинается на маршрутизаторе:

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

3. Как только таймер **RENEW** достигает нуля, клиентский маршрутизатор автоматически регистрирует себя с CA для получения его сертификата идентификации. Как только сертификат получен, введите **показ крипто-** команда **сертификата pki** для просмотра его:

   ```
   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
```

Возобновить дата является **9:30:08** и вычислена как показано здесь:

start-time + (%renewal ID_cert_lifetime)

Или

9:16:57 + (70% * 20 минут) = **9:30:08**

Таймеры PKI отражают то же:

```
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. Как только таймер **RENEW** истекает, маршрутизатор повторно регистрируется с CA для получения нового сертификата идентификатора. После того, как обновление сертификата произошло, введите **команду show crypto pki cert** для просмотра нового сертификата идентификатора:

```
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
```

Заметьте, что больше нет *возобновить даты*; вместо этого, таймер SHADOW начинается:

```
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
```

Вот логика процесса:

- Если дата завершения сертификата ID не равна дате завершения сертификата CA, то вычислите возобновлять-дату на основе процента автоматической регистрации и запустите таймер RENEW.

- Если дата завершения сертификата ID равна дате завершения сертификата CA, то никакой процесс возобновления не необходим, так как текущий сертификат ID допустим только, пока текущий сертификат CA допустим. Вместо этого таймер SHADOW запущен.

Этот таймер также вычислен на основе процента, упомянутого в команде auto-enroll. Например, рассмотрите даты законности возобновленного сертификата ID, которые показывают в предыдущем примере:

```
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
```

Срок действия этого сертификата составляет 16 минут. Поэтому таймер одновременного нажатия клавиш (т.е. таймер SHADOW) составляют 70% 16 минут, которые равняются приблизительно 11 минутам. Это вычисление подразумевает, что маршрутизатор начинает запросы о своих сертификатах тени/одновременного нажатия клавиш в [9:30:09 + 0:11:00] = 9:41:09, который соответствует PKI таймер SHADOW, показанный ранее в этом документе:

```
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
```

Auto-Rollover в действии

В этом разделе описываются функцию auto-rollover в действии.

На Cisco IOS CA сервер

Когда таймер SHADOW истекает, сертификат одновременного нажатия клавиш появляется на маршрутизаторе CA:

```
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
```

В клиентском маршрутизаторе

Как описано ранее в этом документе, функция автоматической подачи заявок начала таймер SHADOW на клиентском маршрутизаторе. Когда таймер SHADOW истекает, функция автоматической подачи заявок позволяет маршрутизатору запросить сервер CA на *сертификат CA одновременного нажатия клавиш/тени*. После того, как полученный, это делает запрос для его сертификата *ID одновременного нажатия клавиш/тени* также. В результате маршрутизатор имеет двух пар сертификатов: одна пара, которая является текущей и другая пара, которая содержит сертификаты одновременного нажатия клавиш/тени:

```
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
```

Заметьте законность сертификата ID одновременного нажатия клавиш:

```
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
```

Срок действия сертификата является всего четырьмя минутами (вместо ожидаемых 20 минут, согласно конфигурации на Cisco IOS CA сервер). На Cisco IOS CA сервер, *абсолютный* срок действия сертификата ID должен составить 20 минут (что означает, для данного клиентского маршрутизатора, сумма сроков службы сертификатов ID (текущий + тень) выполненный к нему не должна быть больше, чем 20 минут).

Этот процесс далее описан здесь:

- Вот законность текущего сертификата ID на маршрутизаторе:

```
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
```

Поэтому *current_id_cert_lifetime* составляет 16 минут.

- Вот законность сертификата ID одновременного нажатия клавиш:

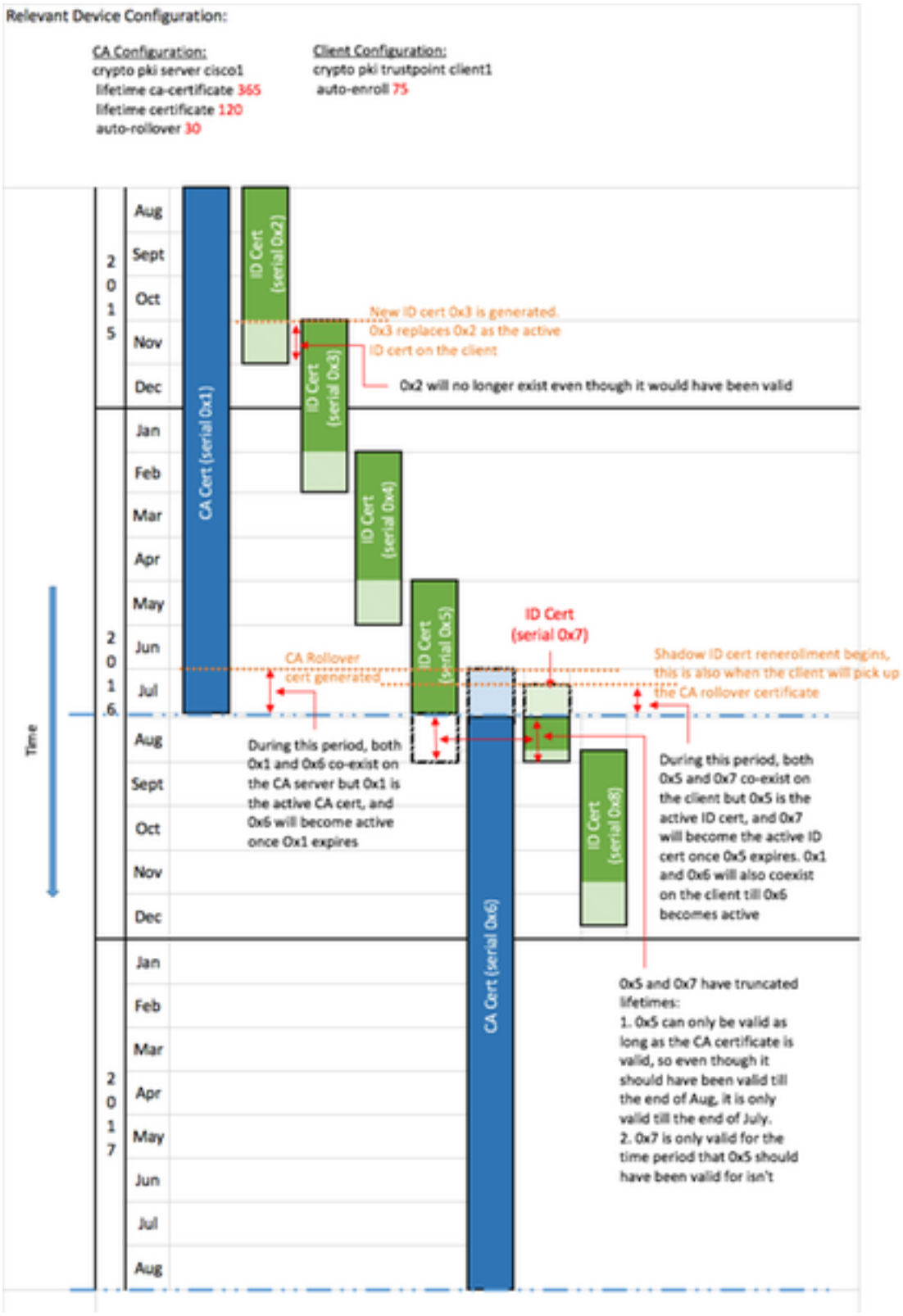
```
Client-1#show crypto pki certificate
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 09:41:42.983 IST Sun Nov 25 2012
Router Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 05
Certificate Usage: General Purpose
Issuer:
cn=Root-CA
ou=TAC
c=IN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

Поэтому *rollover_id_cert_lifetime* составляет четыре минуты.

- На Cisco IOS, когда [current_id_cert_lifetime] добавлен к [rollover_id_cert_lifetime], он должен равняться [total_id_cert_lifetime]. Это истинно в этом случае.

Типовая шкала времени PKI с одновременным нажатием клавиш и регистрацией



Важные замечания

- Таймеры PKI требуют авторитетных часов для функционирования должным образом. Cisco рекомендует использовать NTP для синхронизации часов между клиентскими маршрутизаторами и Cisco IOS CA маршрутизатор. В отсутствие NTP может использоваться система/аппаратные часы на маршрутизаторе. Для получения информации о том, как настроить аппаратные часы и сделать их авторитетными, обращается к Руководству по конфигурации Основ управления системой, Cisco IOS Release 12.4T.

- На повторную загрузку маршрутизатора синхронизация NTP часто занимает несколько минут. Однако таймеры PKI установлены почти сразу. С Версий 15.2 (3.8) T и 15.2 (4) S, автоматически переоценены таймеры PKI после того, как NTP синхронизируется.

- Таймеры PKI не являются абсолютными; они основываются *на остающемся времени* и, поэтому, повторно вычислены после перезагрузки. Например, предположите, что клиентский маршрутизатор имеет сертификат ID, который допустим в течение 100 дней, и функция автоматической регистрации установлена в 80%. Затем перерегистрация, как ожидают, произойдет после 80-го дня. Если маршрутизатор повторно загружен в 60-й день, он загружает и повторно вычисляет таймер PKI как показано здесь: (*остающееся время*), * *(%auto-регистрируются)* = (100-60) * 80% = 32 дня.

  Поэтому перерегистрация происходит на [60 + 32] = 92-й день.

- При настройке автоматической регистрации и auto-rollovertimers важно настроить их со значениями, которые позволяют доступность сертификата CA SHADOW на Сервере pki когда запросы клиента PKI один. Это помогает смягчать потенциальные сбои сервисов PKI в крупномасштабной среде.

Дополнительные сведения

- Развертывание безопасности Cisco IOS с отчетом инфраструктуры открытого ключа
- Инфраструктура открытых ключей: преимущества развертываний и отчет функций
- Руководство по конфигурации инфраструктуры открытых ключей
- Cisco Systems – техническая поддержка и документация