在PIX和使用智能卡证书的Cisco VPN客户端之间的IPSec配置示例

目录

简介

本文展示了如何配置PIX防火墙和Cisco VPN客户端4.0.x之间的IPSec VPN隧道。本文的配置示例还突出强调了Cisco IOS®路由器和Cisco VPN客户端的证书机构(CA)登记程序，并且将Smartcard用作证书存贮。

参考配置在使用委托认证的Cisco IOS路由器和Cisco VPN Client之间的IPSec为了得知更多配置在使用委托认证的Cisco IOS路由器和Cisco VPN Client之间的IPSec。

参考配置Cisco IOS路由器的多重身份CA为了得知更多配置Cisco IOS路由器的多重身份CA。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本的Cisco PIX防火墙6.3(3)
- 运行Windows XP的PC的Cisco VPN Client 4.0.3

- Microsoft Windows 2000 CA服务器用于本文作为CA服务器。
- 使用Aladdin eToken智能卡，在Cisco VPN Client的证书 存储。

本文档中的信息都是基于特定实验室环境中的设备编写的。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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

登记并且配置PIX

本部分提供有关如何配置本文档中所述功能的信息。

注意： 要查找有关本文档中所使用的命令的详细信息，请使用命令查找工具（仅限注册用户）。

配置

本文档使用以下配置。

- 在PIX防火墙的证书登记
- PIX 防火墙配置

在PIX防火墙的证书登记

```
!--- Define a hostname and domain name for the router.
!--- The fully qualified domain name (FQDN) is used !---
as the identity of the router during certificate
enrollment. pix(config)#hostname sv2-11
sv2-11(config)#domain-name cisco.com
!--- Confirm that you have the correct time set on the
PIX. show clock
clock set <hh:mm:ss> {<day> <month> | <month> <day>}
<year>
!--- This command clears the PIX RSA keys. ca zeroize
rsa
!--- Generate RSA (encryption and authentication) keys.
ca gen rsa key
!--- Select the modulus size (512 or 1024). !--- Confirm
the keys generated. show ca mypub rsa
!--- Define the CA identity. ca ident kobe
10.1.1.2:/certsrv/mscep/mscep.dll
ca conf kobe ra 1 20 crlopt
ca auth kobe
ca enroll kobe [ipaddress]
!--- Confirm the certificate and validity. show ca cert
```

PIX 防火墙配置

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-11
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit tcp any host 209.165.201.21 eq
www
access-list 120 permit ip 10.1.1.0 255.255.255.0
10.0.0.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 209.165.201.20 255.255.255.224
ip address inside 10.1.1.10 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 10.0.0.10-10.0.0.100
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask
255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
```

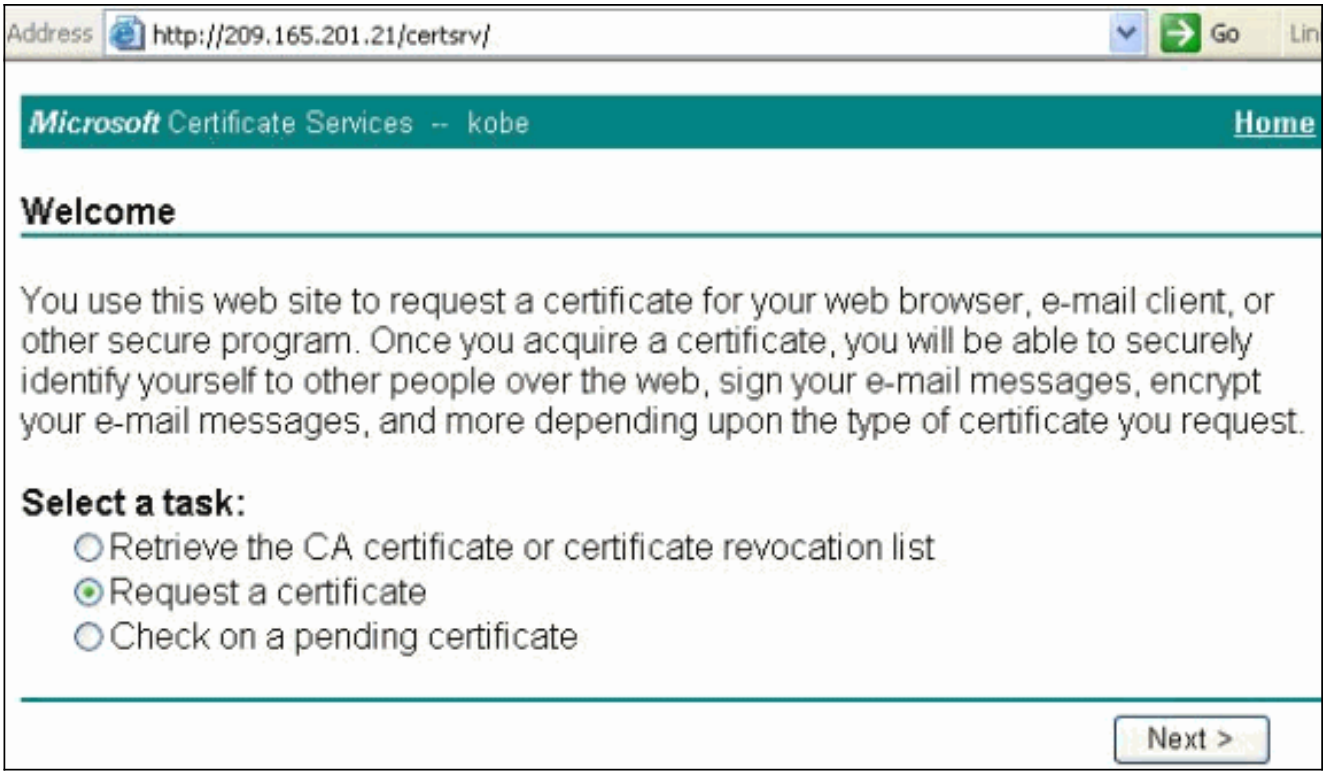
```
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpncert address-pool vpnpool
vpngroup vpncert idle-time 1800
vpngroup vpncert password ********
ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca configure kobe ra 1 20 crloptional
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:2ae252ac69e5218d13d35acdf1f30e55
: end
[OK]
sv2-11(config)#
```

登记Cisco VPN客户端证书

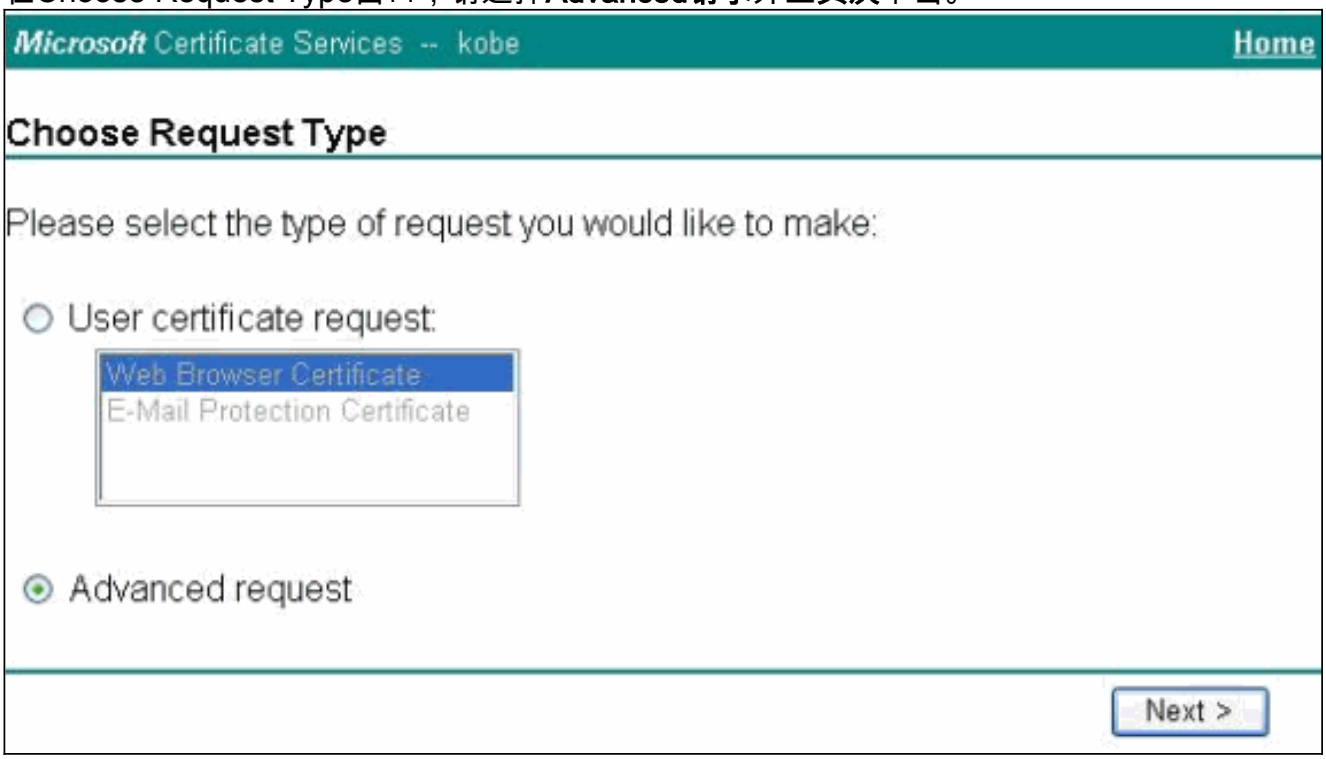
记住安装所有必要的驱动程序光盘和PC上的智能卡设备，将它们与Cisco VPN客户端同时使用。

这些步骤展示使用的步骤登记MS证书的Cisco VPN Client。证书在Aladdin eToken智能卡 存储存储。

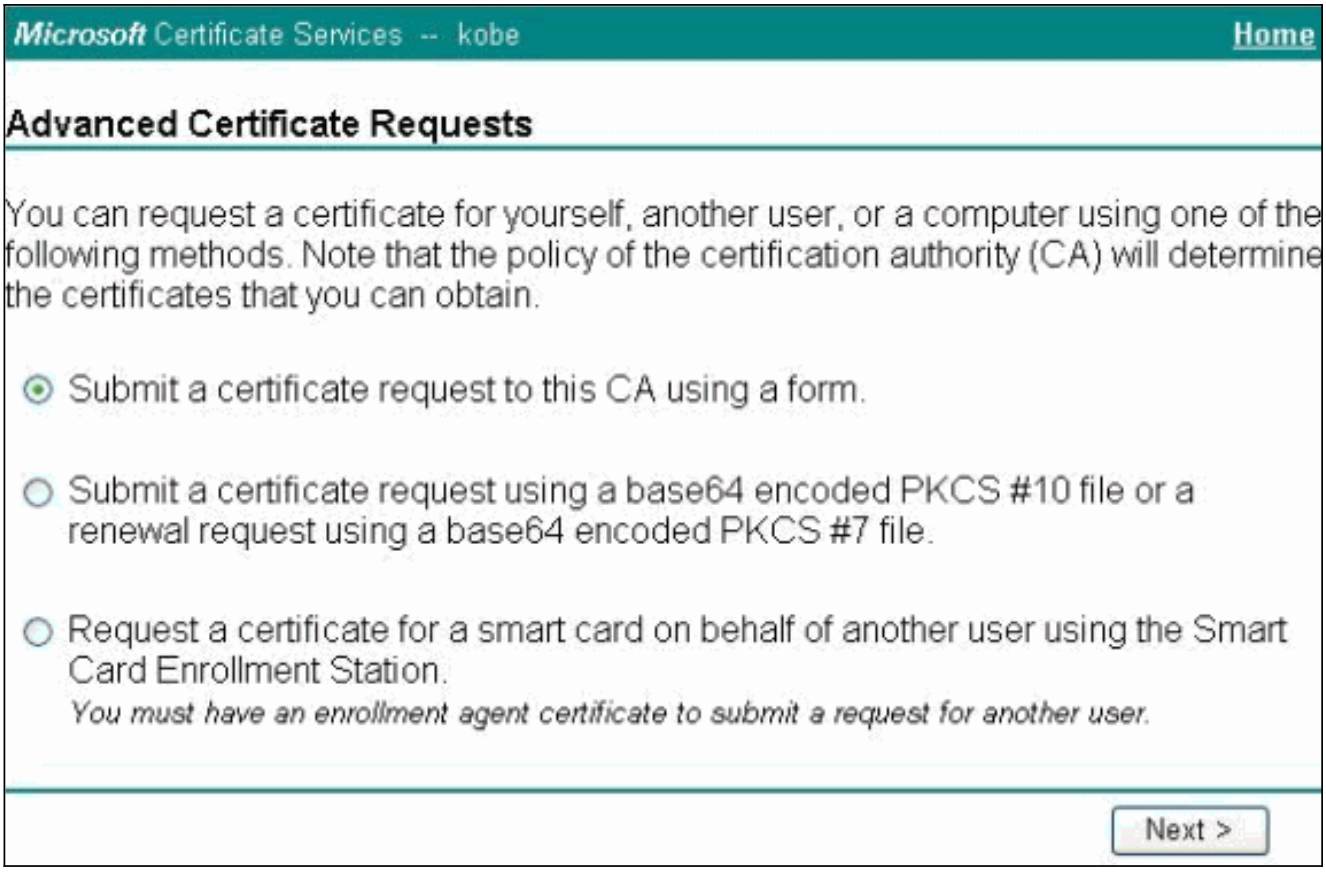
1. 启动浏览器并且去证书服务器页(http://CAServeraddress/certsrv/，在本例中)。
2. Select请求**证书**和**其次**单击。



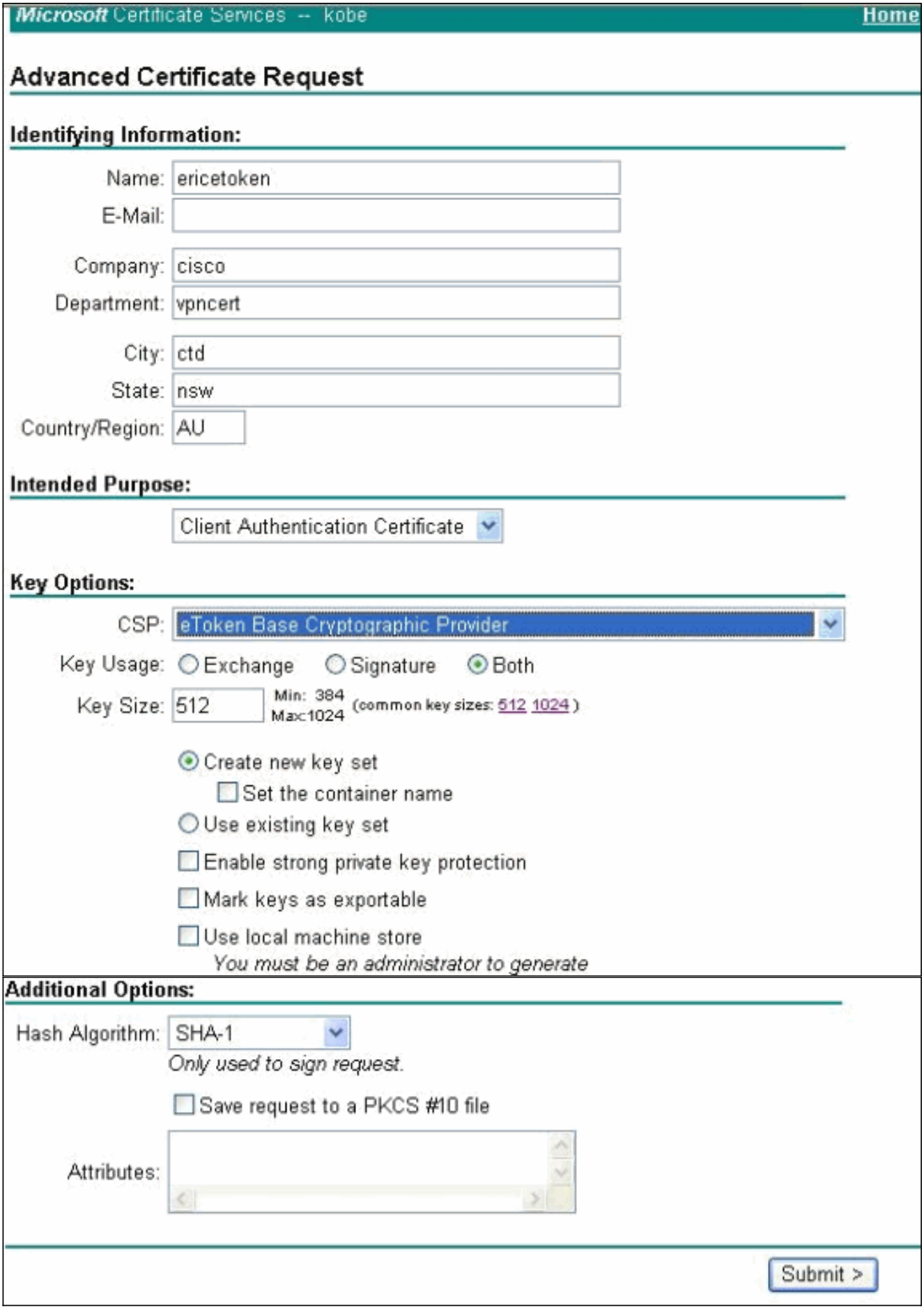
3. 在Choose Request Type窗口，请选择**Advanced请求**并且**其次**单击。



4. 选择**提交证书请求对此CA使用表**并且**其次**单击。



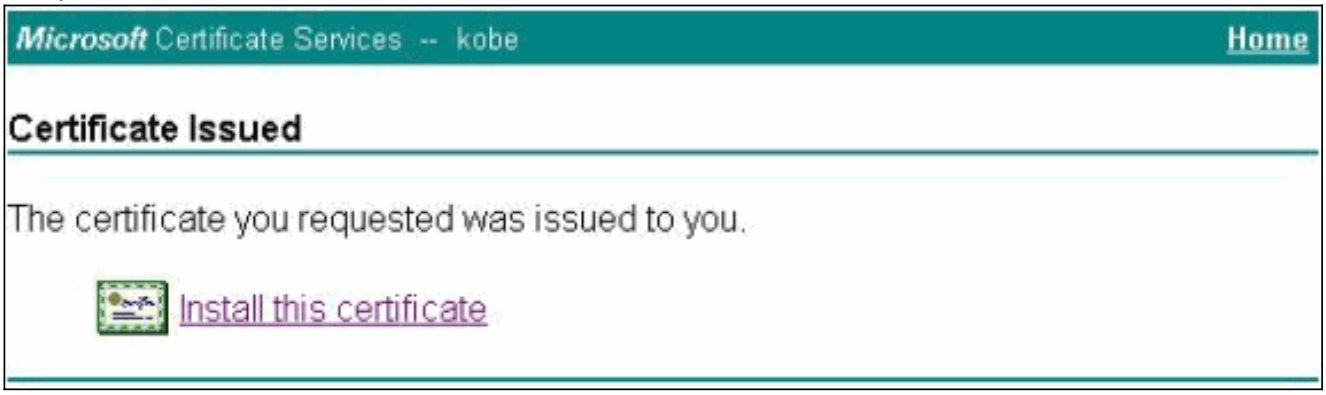
5. 填写在Advanced Certificate请求表的所有项目。确保部门或组织单位(OU)与Cisco VPN客户端组名对应（如PIX vpngroup名字所配置的名字一样）。选择正确证书服务提供商(CSP)适当为您的设置。



6. 当您获得潜在的执行脚本验证警告时，请选择**是**为了继续安装。

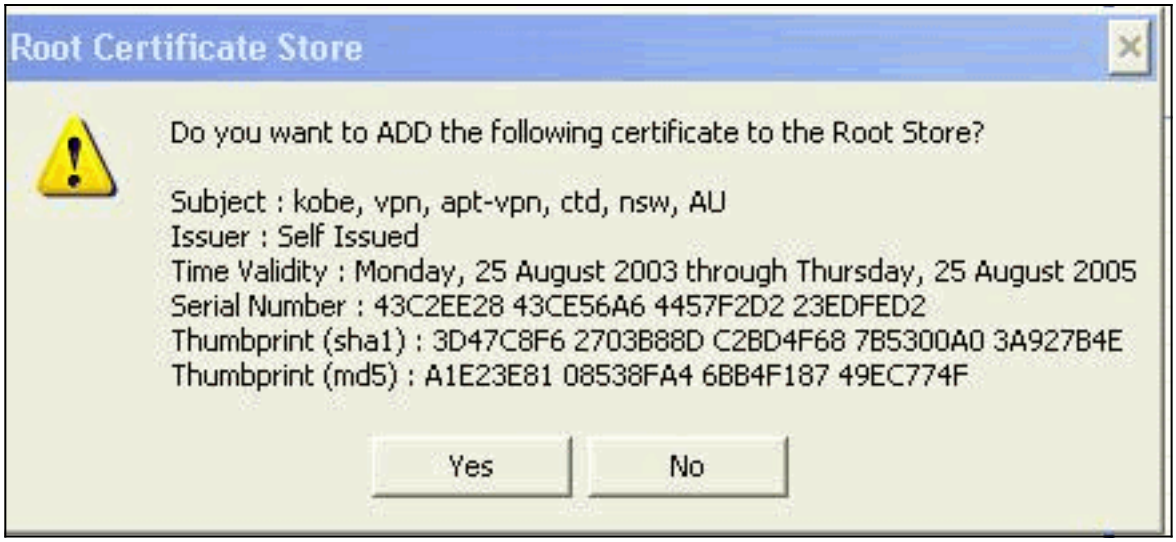
7. 证书登记调用eToken存储。输入密码并且点击OK键。

8. 单击 **Install this certificate**。

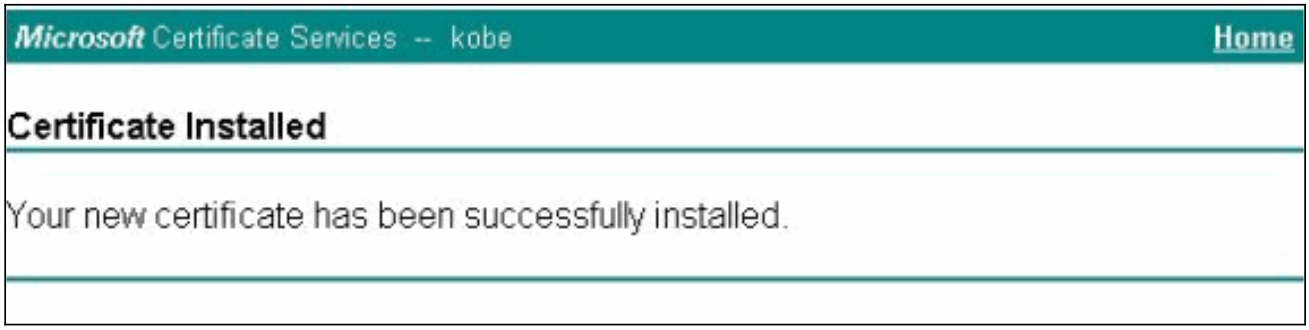


9. 当您获得潜在的执行脚本验证警告时，请选择**是**为了继续安装。

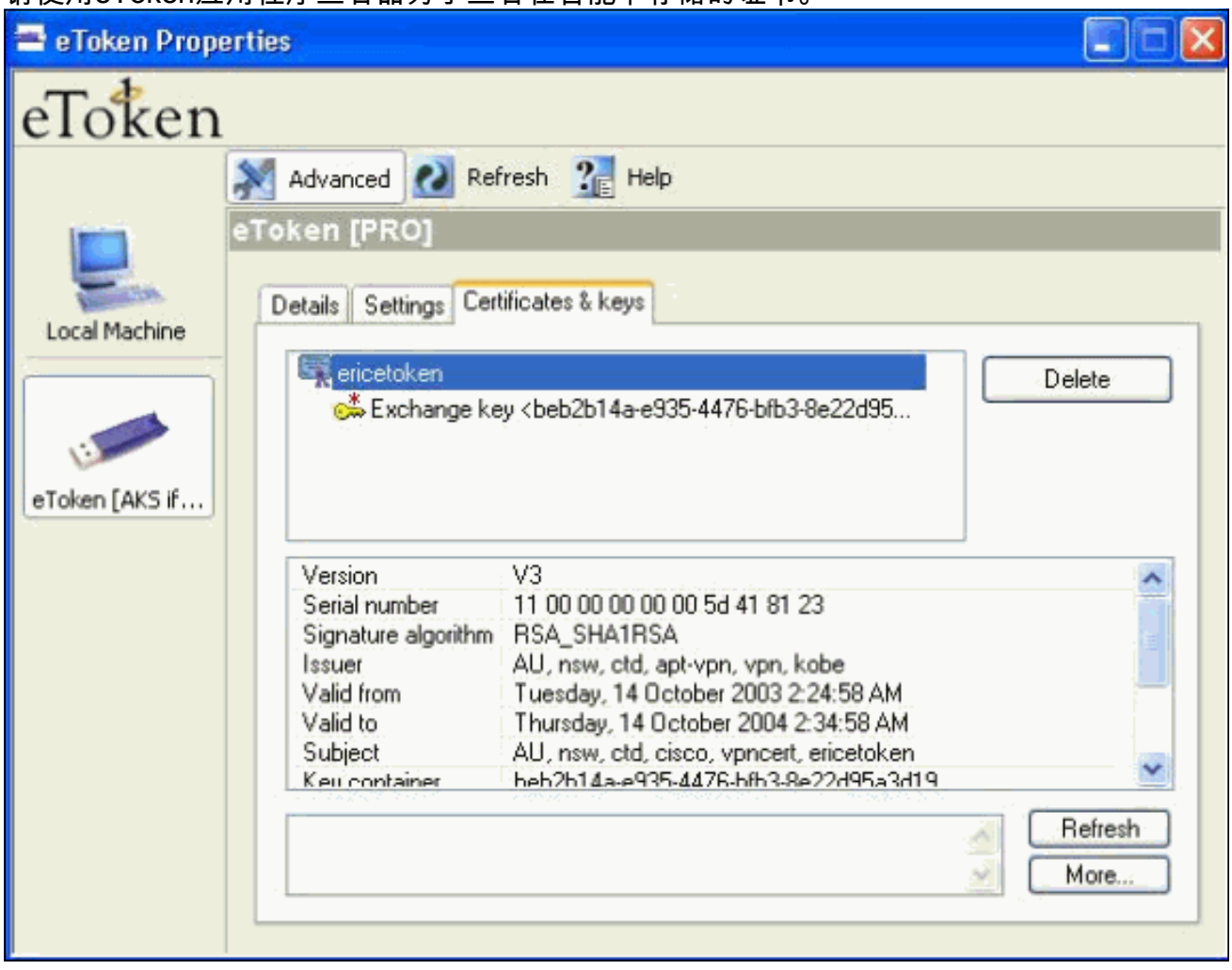
10. 选择**是**为了添加根证明到根存储。



11. Certificate Installed窗口出现并且确认成功的安装。



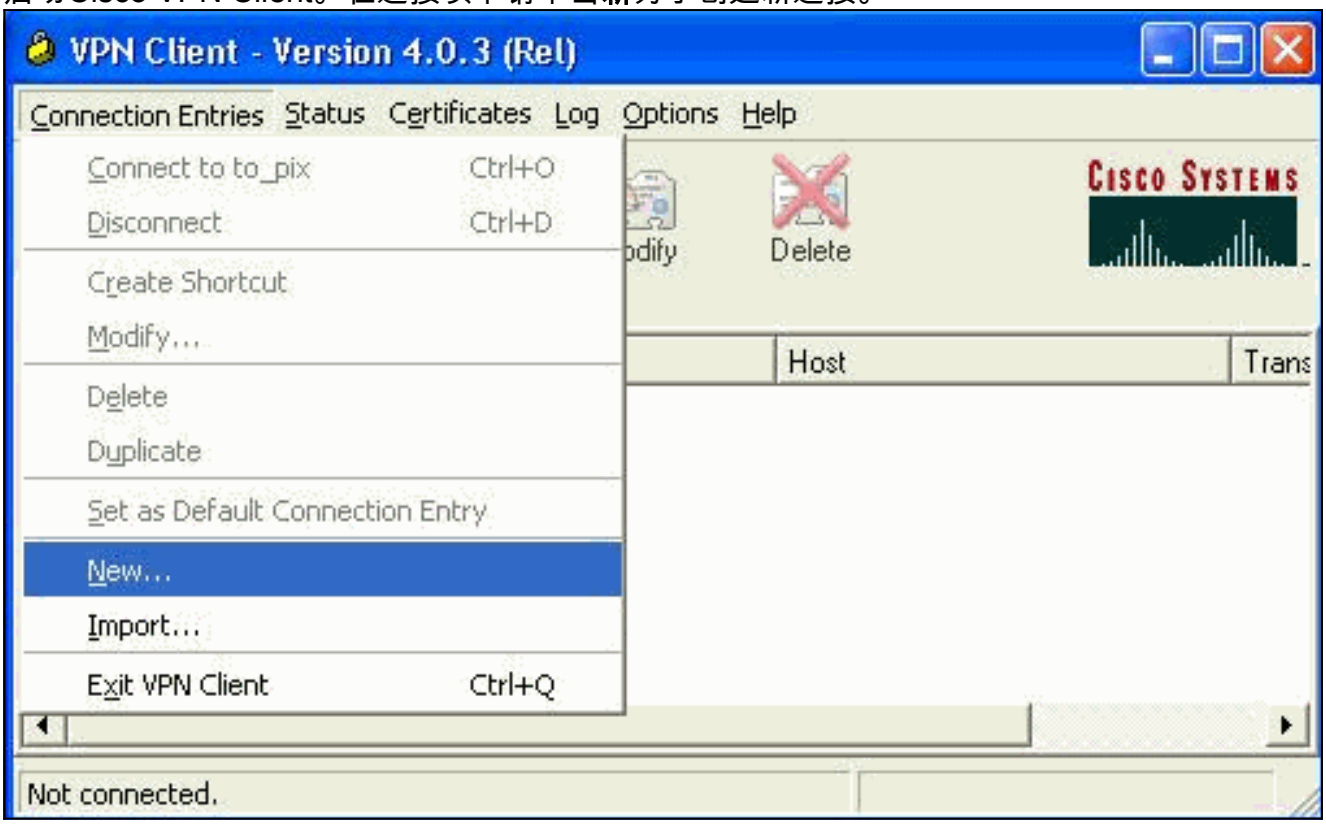
12. 请使用eToken应用程序查看器为了查看在智能卡存储的证书。



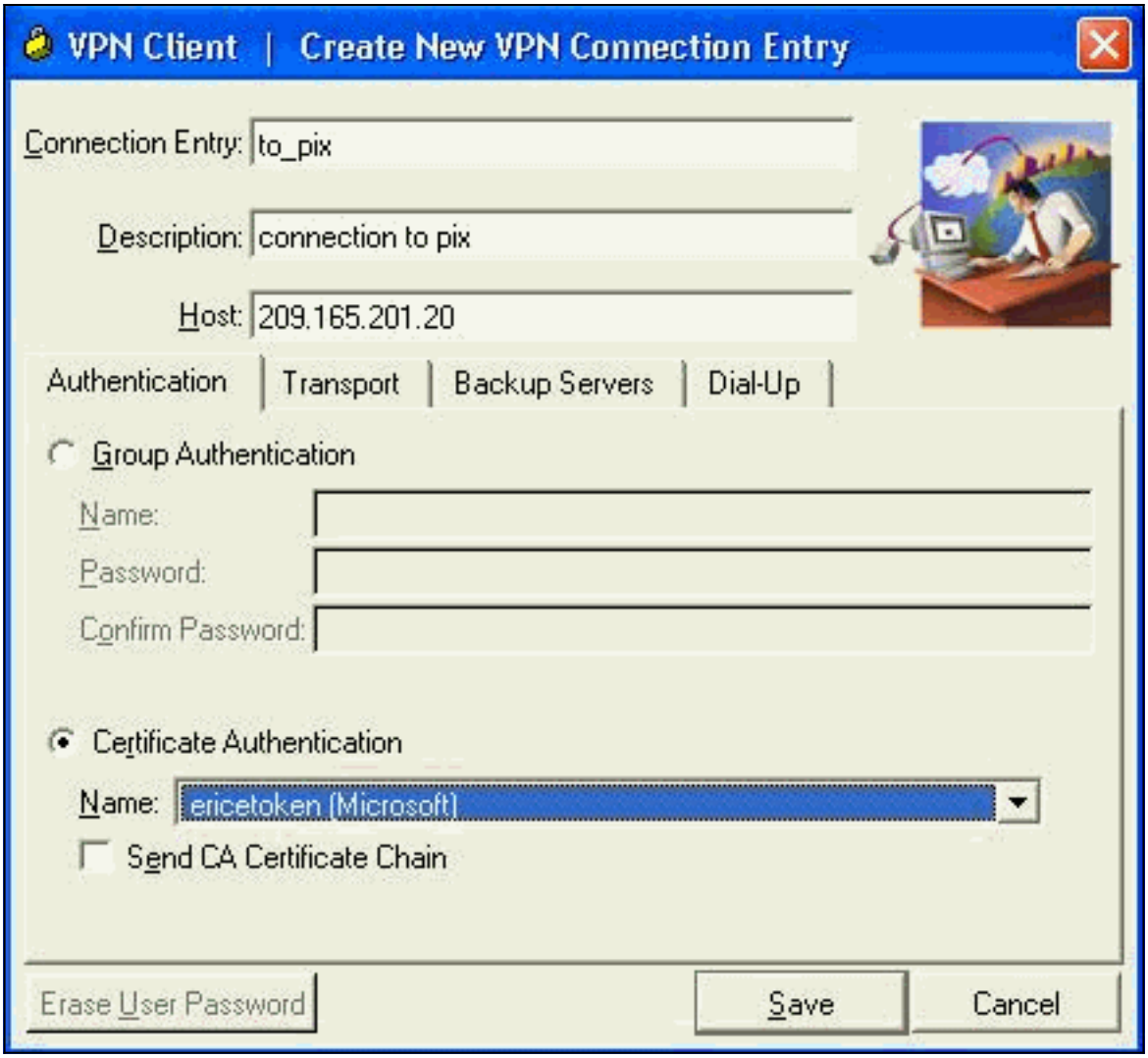
配置Cisco VPN Client为了使用证书对PIX的连接

这些步骤展示使用的步骤配置Cisco VPN Client使用证书PIX连接。

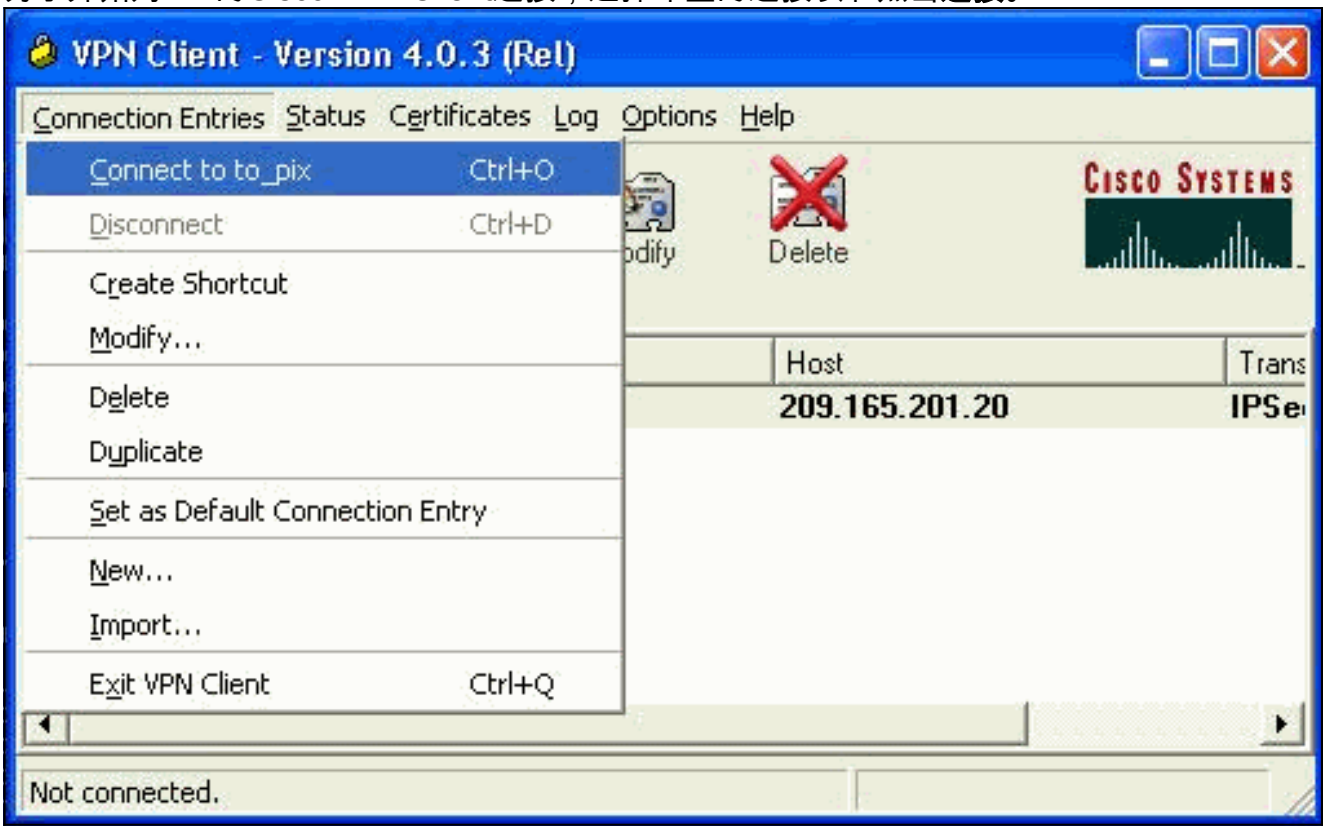
1. 启动Cisco VPN Client。在连接项下请单击**新**为了创建新连接。



2. 完成连接详细信息，指定证书验证，选择从登记获取的证书。单击 **Save**。



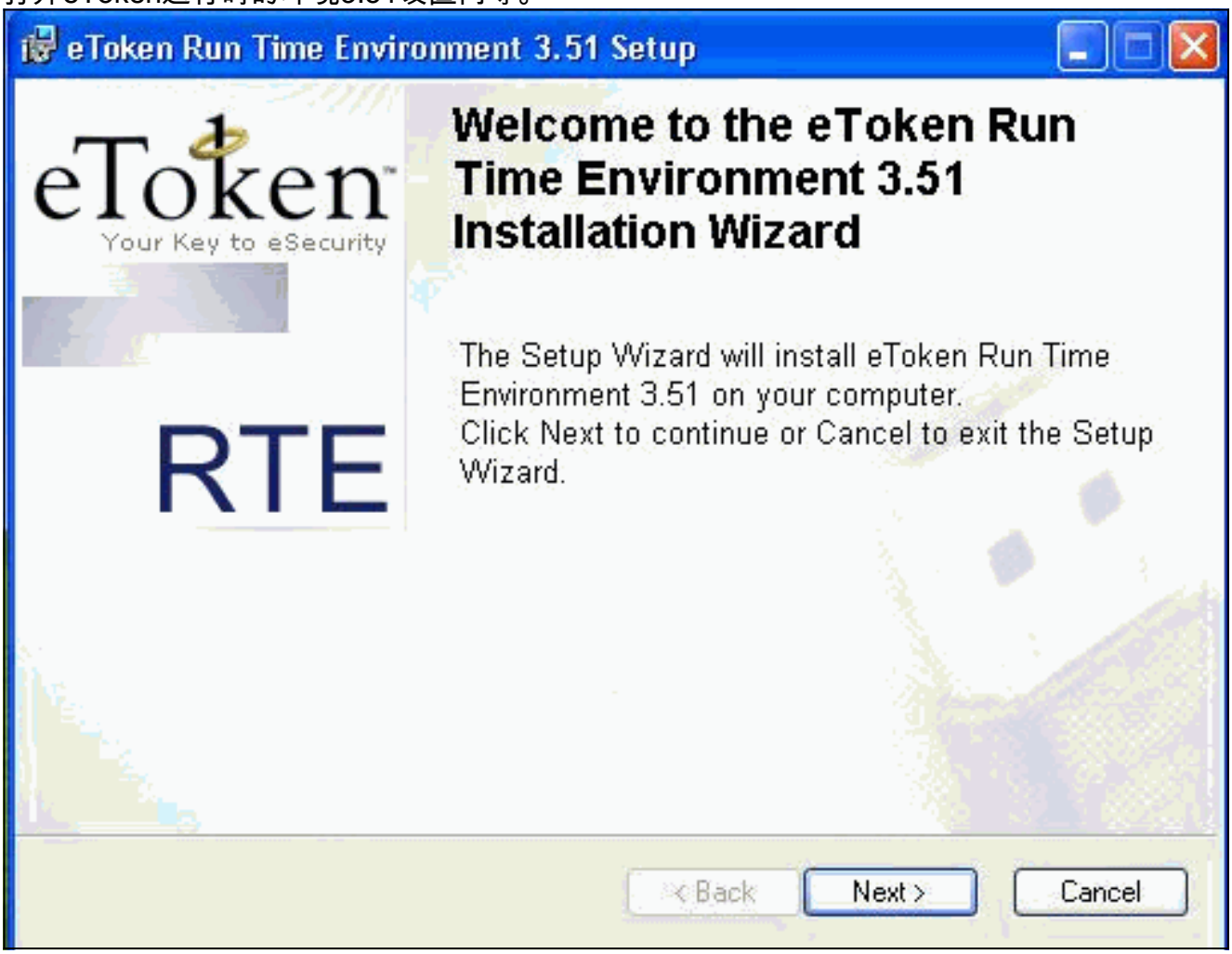
3. 为了开始对PIX的Cisco VPN Client连接，选择希望的连接项和点击**连接**。



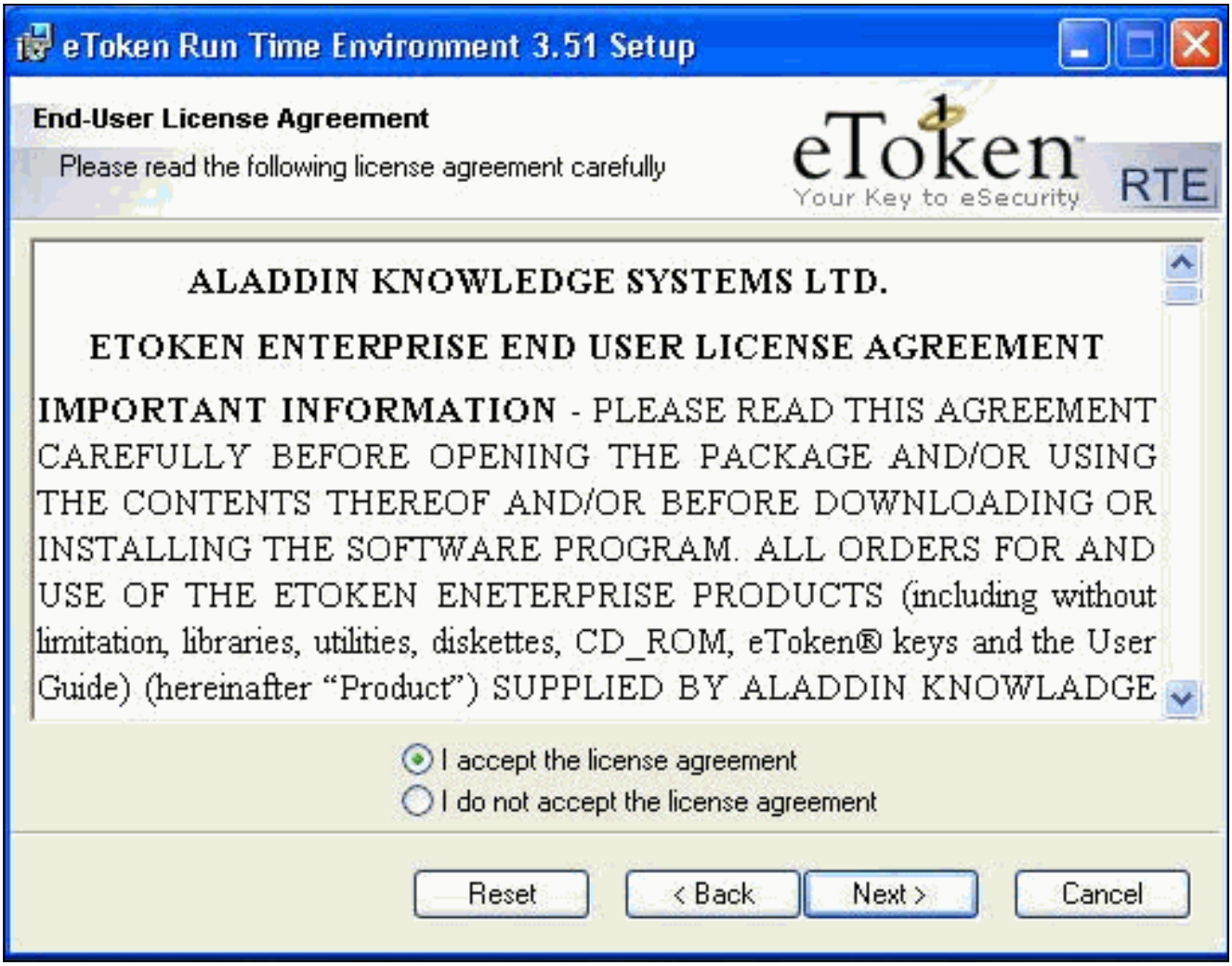
安装Etoken智能卡驱动器

这些步骤展示Aladdin Etoken智能卡驱动程序的安装 。

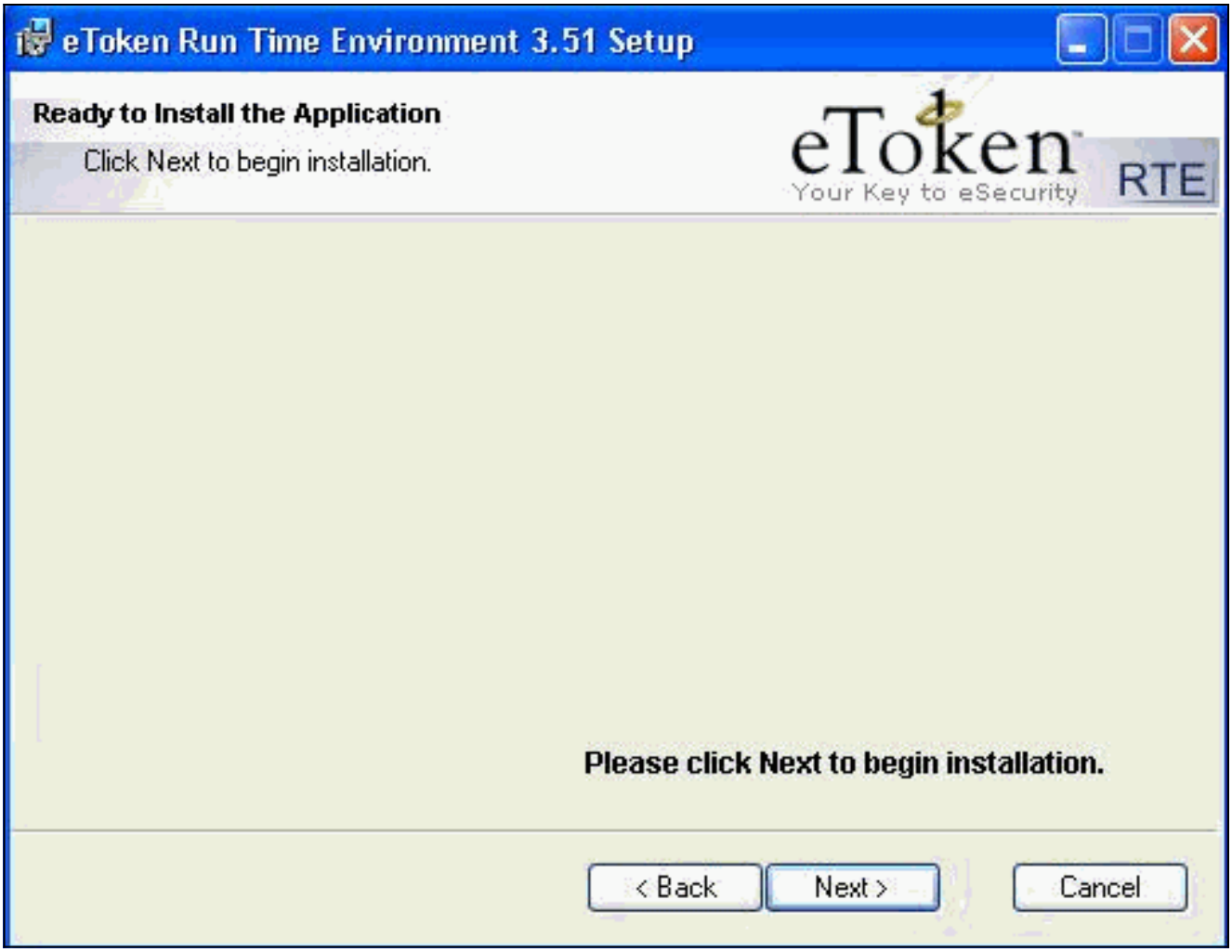
1. 打开eToken运行时的环境3.51设置向导。



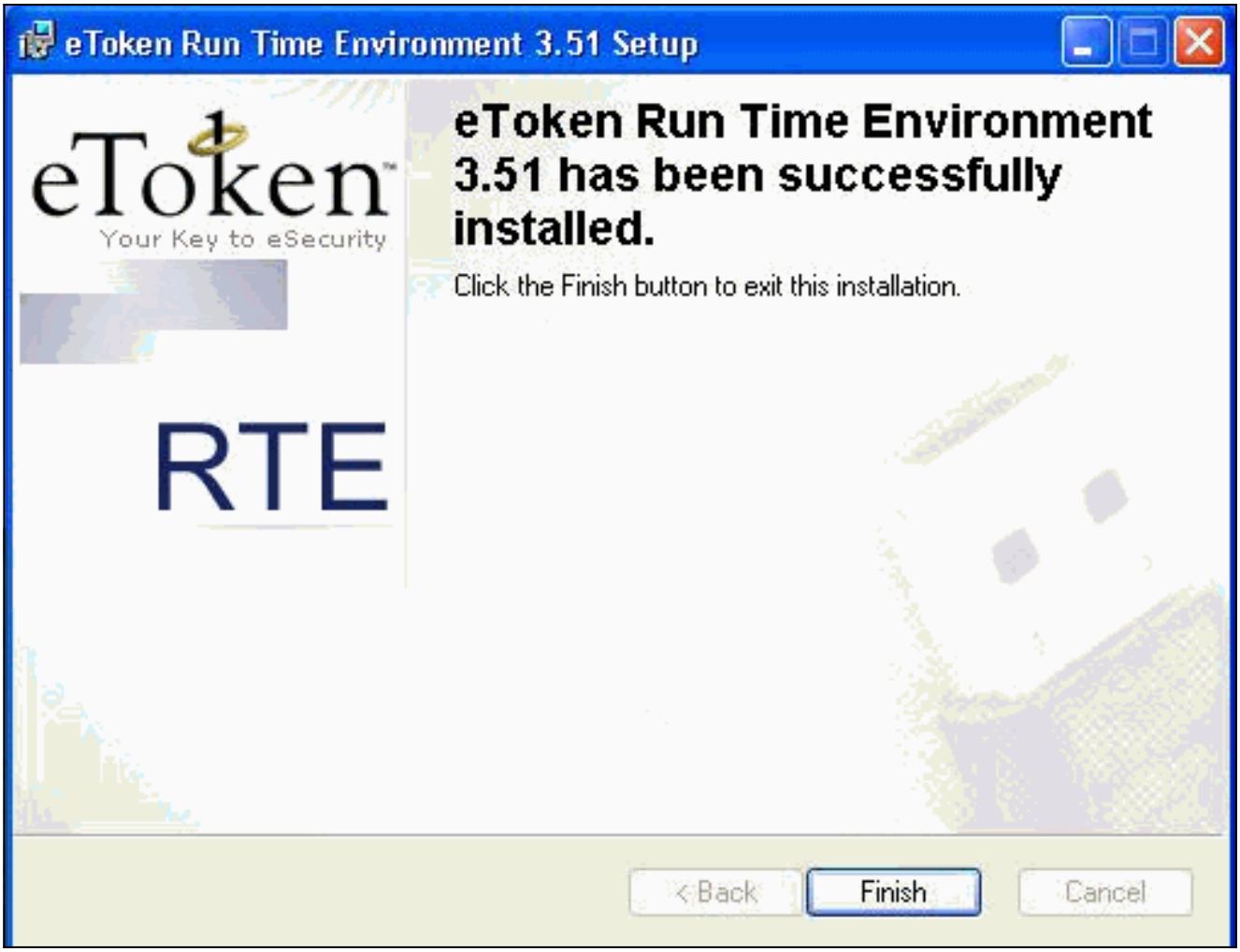
2. 接受许可证协议条件并且**其次**单击。


eToken Run Time Environment 3.51 Setup
End-User License Agreement
Please read the following license agreement carefully
eToken
Your Key to eSecurity
RTE
ALADDIN KNOWLEDGE SYSTEMS LTD.
ETOKEN ENTERPRISE END USER LICENSE AGREEMENT
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE AND/OR USING THE CONTENTS THEREOF AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF THE ETOKEN ENETERPRISE PRODUCTS (including without limitation, libraries, utilities, diskettes, CD_ROM, eToken® keys and the User Guide) (hereinafter "Product") SUPPLIED BY ALADDIN KNOWLADGE
I accept the license agreement
I do not accept the license agreement
Reset
< Back
Next >
Cancel

3. 单击 **Install**。



4. Etoken智能卡驱动器当前安装。点击**芬通社**为了退出设置向导。



验证

本部分提供了可用于确认您的配置是否正常运行的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto isakmp sa** -显示所有当前在对等端的互联网密钥交换(IKE)安全关联(SAs)。
```
SV2-11(config)#show crypto isa sa
Total     : 1
Embryonic : 0
        dst               src        state     pending     created
  209.165.201.20   209.165.201.19    QM_IDLE         0           1
```
- **show crypto ipsec sa** —显示当前安全关联使用的设置。
```
SV1-11(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, local addr. 209.165.201.20
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0)
current_peer: 209.165.201.19:500
dynamic allocated peer ip: 10.0.0.10
PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.19
     path mtu 1500, ipsec overhead 56, media mtu 1500
```

```
     current outbound spi: c9a9220e
inbound esp sas:
spi: 0xa9857984(2844096900)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607996/28746)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xc9a9220e(3383304718)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28748)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

故障排除

欲知关于排除故障此配置的详情，参考排除故障PIX通过在已建立的IPSec隧道的数据流。

相关信息

- Cisco Secure PIX 防火墙命令参考
- 请求注解 (RFC)
- IPSec（IP 安全协议）支持页
- Cisco VPN 客户端支持页
- PIX 500 系列防火墙支持页
- 技术支持 - Cisco Systems