Exemplo de configuração de IPSec entre PIX e Cisco VPN Client usando certificados Smartcard

Contents

Introduction

Este documento demonstra como configurar um túnel VPN IPSec entre um PIX Firewall e um Cisco VPN Client 4.0.x. O exemplo de configuração neste documento também destaca o procedimento de inscrição da autoridade de certificação (CA) para o roteador Cisco IOS® e o Cisco VPN Client, assim como o uso de um Smartcard como um armazenamento de certificado.

Consulte Configuração de IPSec entre Cisco IOS Routers e Cisco VPN Client Usando Certificados Entrust para saber mais sobre Configuração de IPSec entre Cisco IOS Routers e Cisco VPN Client usando Certificados Entrust.

Consulte Configurando Autoridades de Certificados de Várias Identidades em Cisco IOS Routers para saber mais sobre a Configuração de Autoridades de Certificados de Várias Identidades em Cisco IOS Routers.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco PIX Firewall executando o software versão 6.3(3)
- Cisco VPN Client 4.0.3 em um PC com Windows XP
- Um servidor de AC do Microsoft Windows 2000 é usado neste documento como o servidor de CA.
- Os certificados no Cisco VPN Client são armazenados usando Aladdin e-Token Smartcard.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Inscrever e configurar o PIX

Nesta seção, você verá informações sobre a configuração dos recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados) .

Configurações

Este documento utiliza estas configurações.

- Inscrição de certificado no PIX Firewall
- Configuração de firewall PIX

Inscrição de certificado no PIX Firewall

```
!--- 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




!--- 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
```

Configuração de firewall PIX

```
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
```

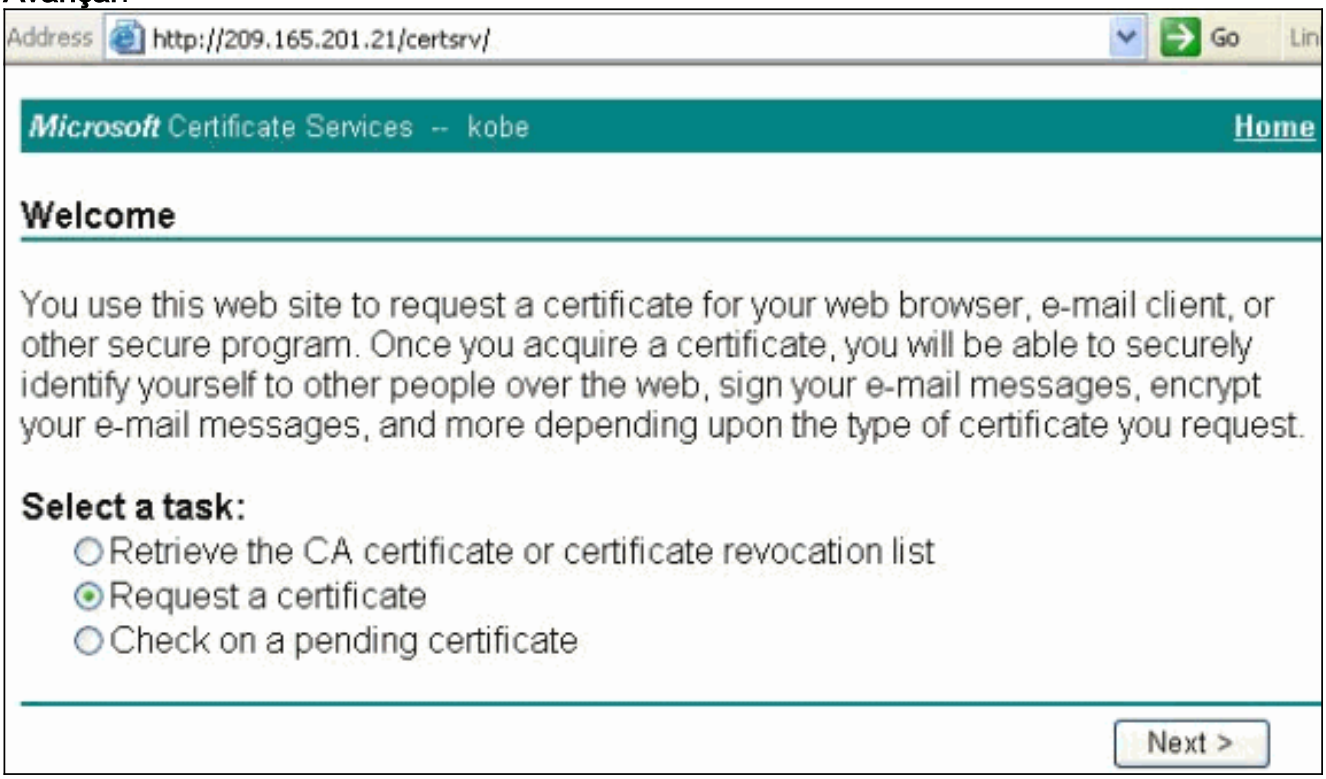
```
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask
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)#
```

Inscrever certificados do Cisco VPN Client

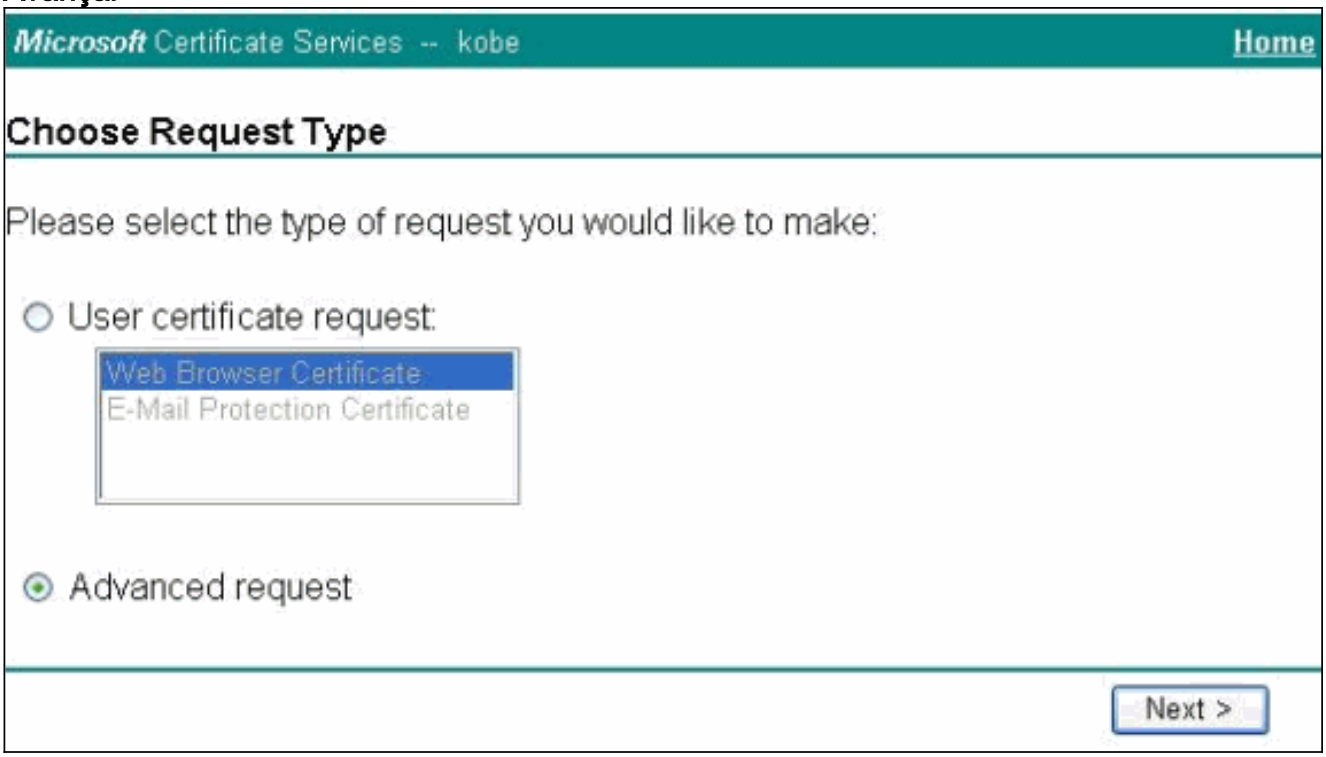
Lembre-se de instalar todos os drivers e utilitários necessários que acompanham o dispositivo Smartcard no PC para serem usados com o Cisco VPN Client.

Estas etapas demonstram os procedimentos usados para inscrever o Cisco VPN Client para certificados MS. O certificado é armazenado no arquivo de cartões eletrônicos Aladdin .

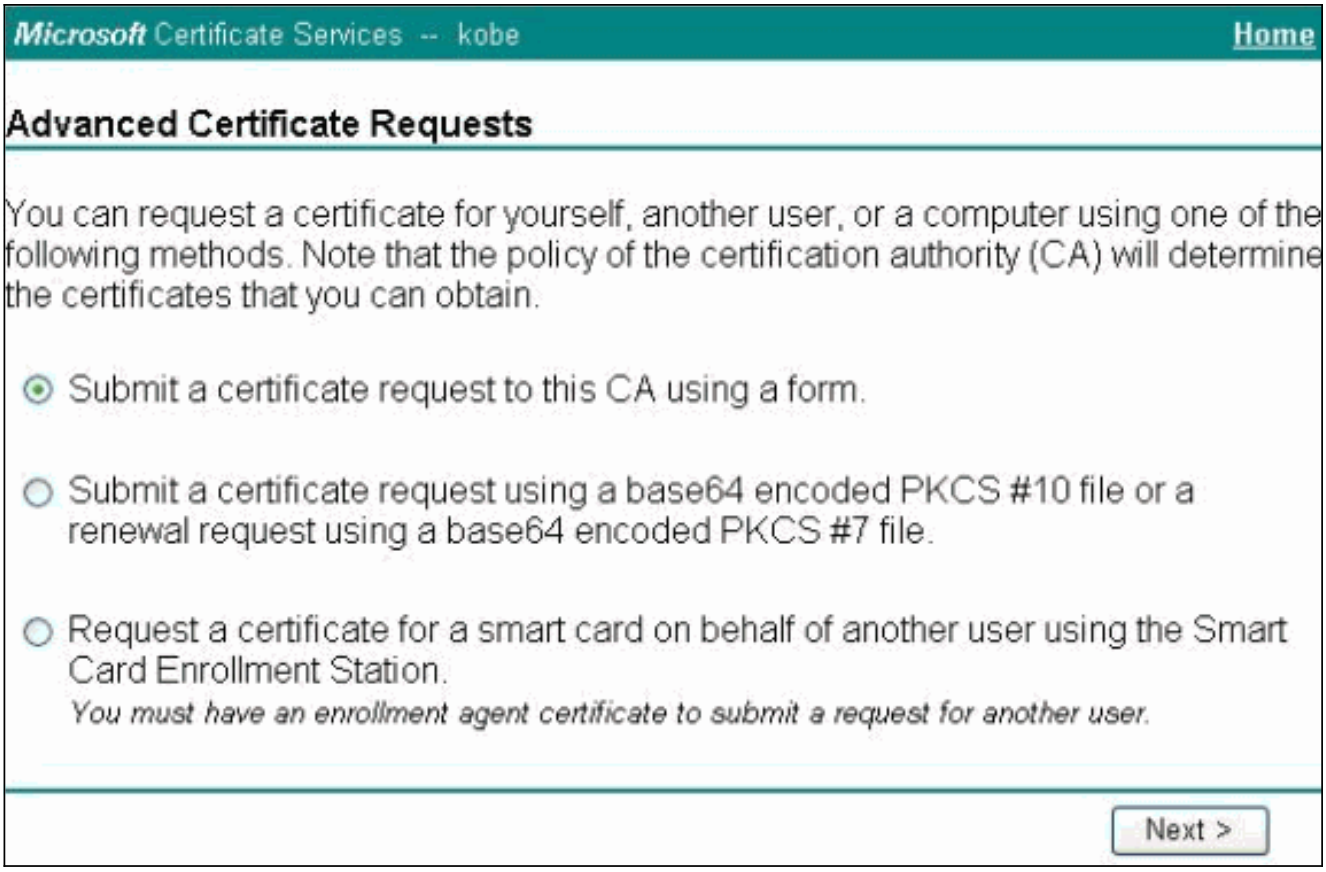
1. Inicie um navegador e vá para a página do servidor de certificados (http://CAServeraddress/certsrv/, neste exemplo).
2. Selecione **Solicitar um certificado** e clique em **Avançar**.



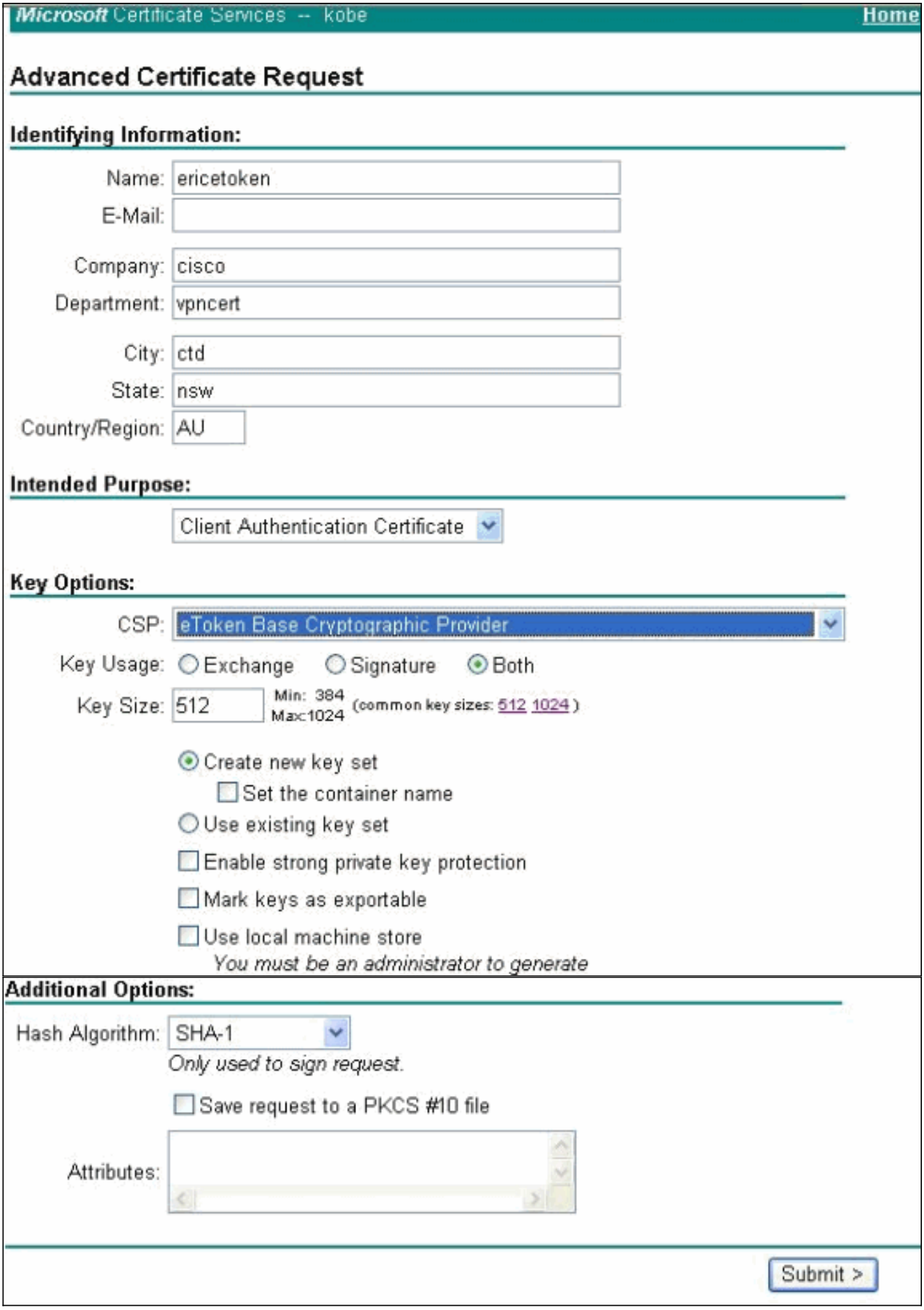
3. Na janela Escolher tipo de solicitação, selecione **Solicitação avançada** e clique em **Avançar**.



4. Selecione **Enviar uma solicitação de certificado para esta CA usando um formulário** e clique em **Avançar**.



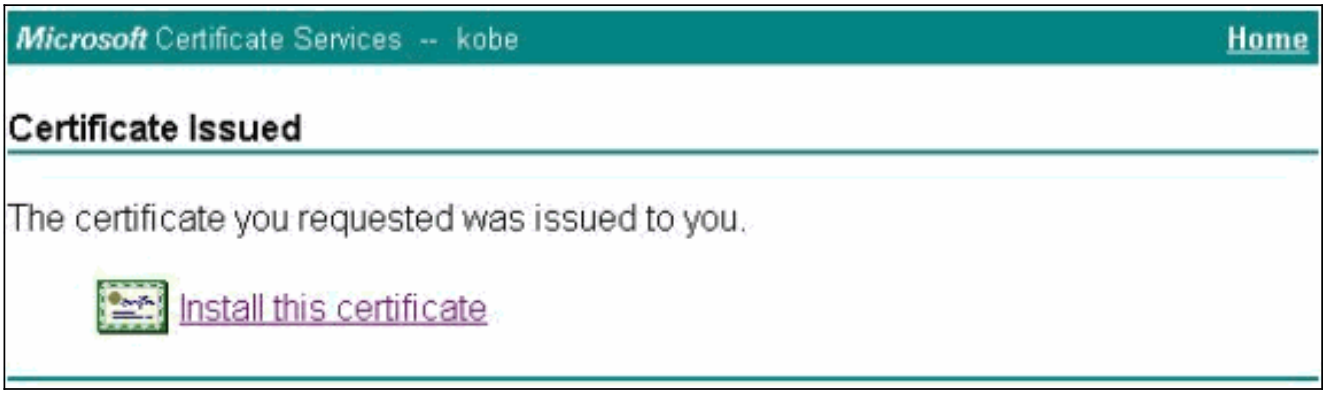
5. Preencha todos os itens no formulário Solicitação de certificado avançado.Certifique-se de que o departamento ou a unidade organizacional (OU) corresponde ao nome do grupo do Cisco VPN Client, conforme configurado no nome do grupo de VPN PIX. Selecione o provedor de serviços de certificado (CSP) correto para sua configuração.



6. Selecione **Sim** para continuar a instalação quando receber o aviso Validação de script potencial.

7. A inscrição de certificado chama o repositório eToken. Digite a senha e clique em OK.

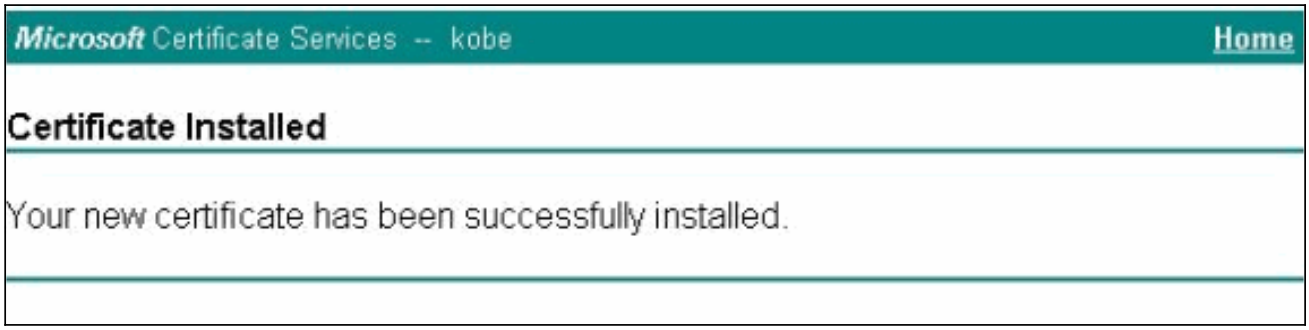
8. Clique em Instalar este certificado.



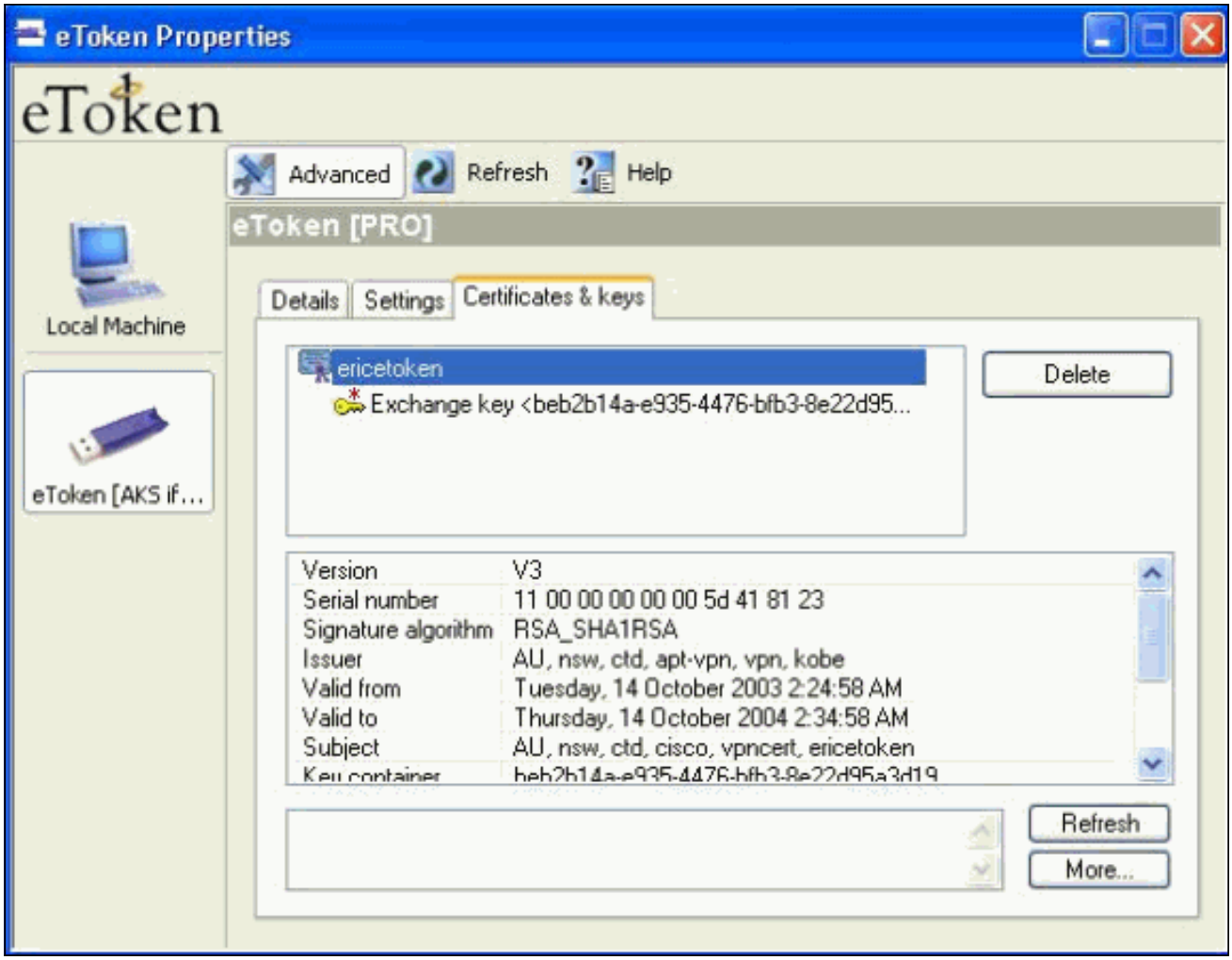
9. Selecione **Sim** para continuar a instalação quando receber o aviso Validação de script potencial.

10. Selecione **Yes** para adicionar o certificado raiz ao Root Store.

11. A janela Certificado instalado é exibida e confirma a instalação bem-sucedida.



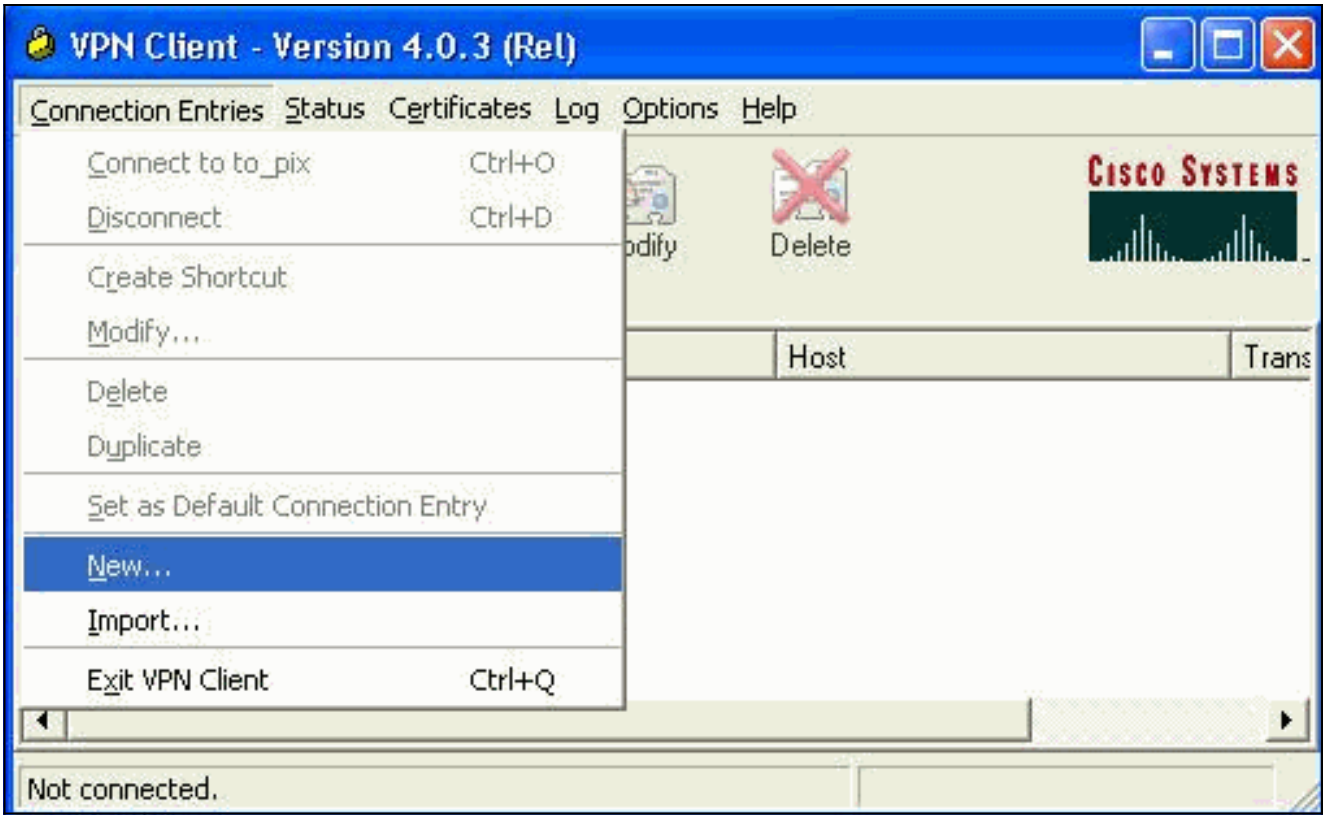
12. Use o eToken Application Viewer para exibir o certificado armazenado no Smartcard.



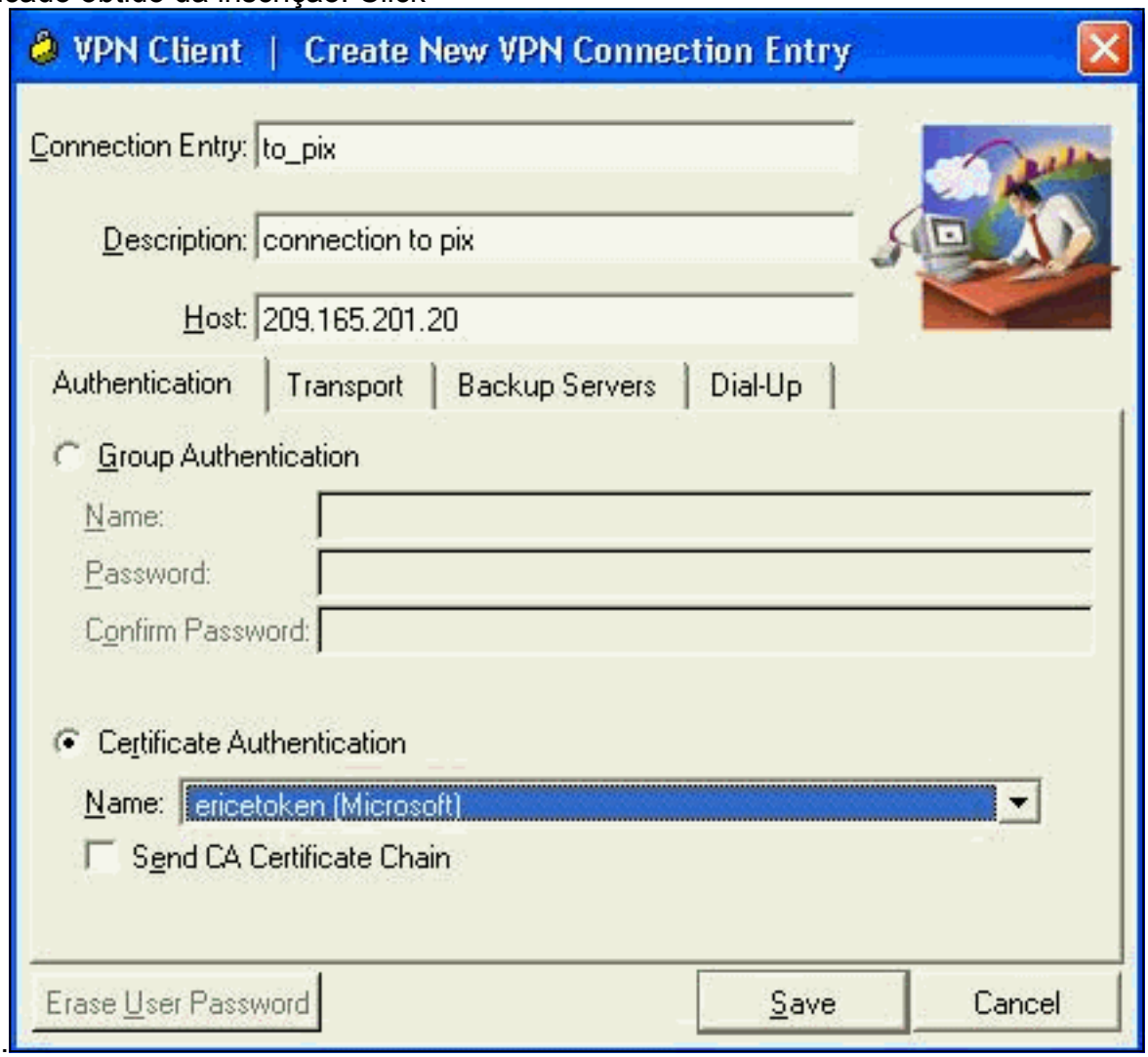
Configure o Cisco VPN Client para usar o certificado para conexão com o PIX

Estas etapas demonstram os procedimentos usados para configurar o Cisco VPN Client para usar o certificado para conexões PIX.

1. Inicie o Cisco VPN Client. Em Connection Entries (Entradas de conexão), clique em **New** para criar uma nova
   conexão.



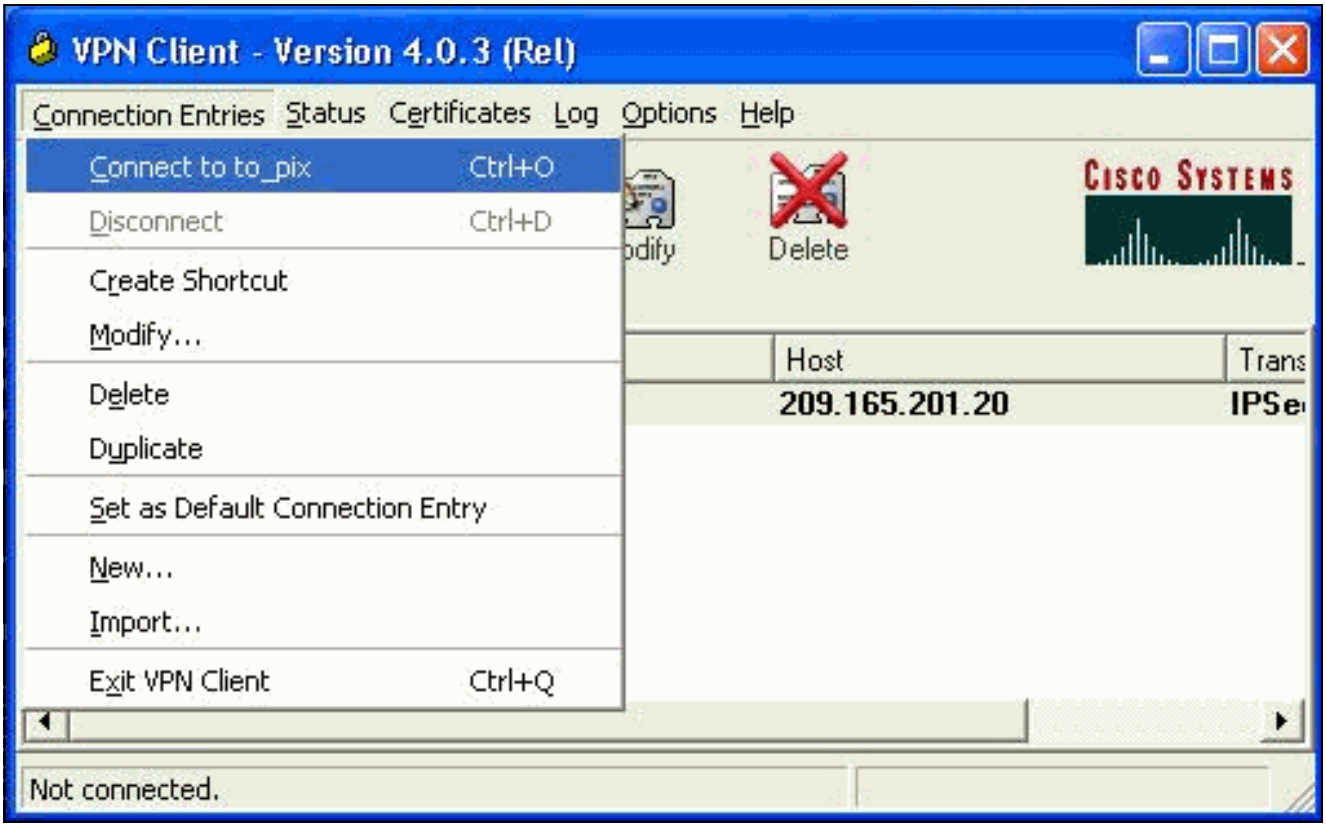
2. Preencha o detalhe da conexão, especifique a Autenticação do certificado, selecione o certificado obtido da inscrição. Click



Save.

3. Para iniciar a conexão do Cisco VPN Client com o PIX, selecione a Entrada de conexão

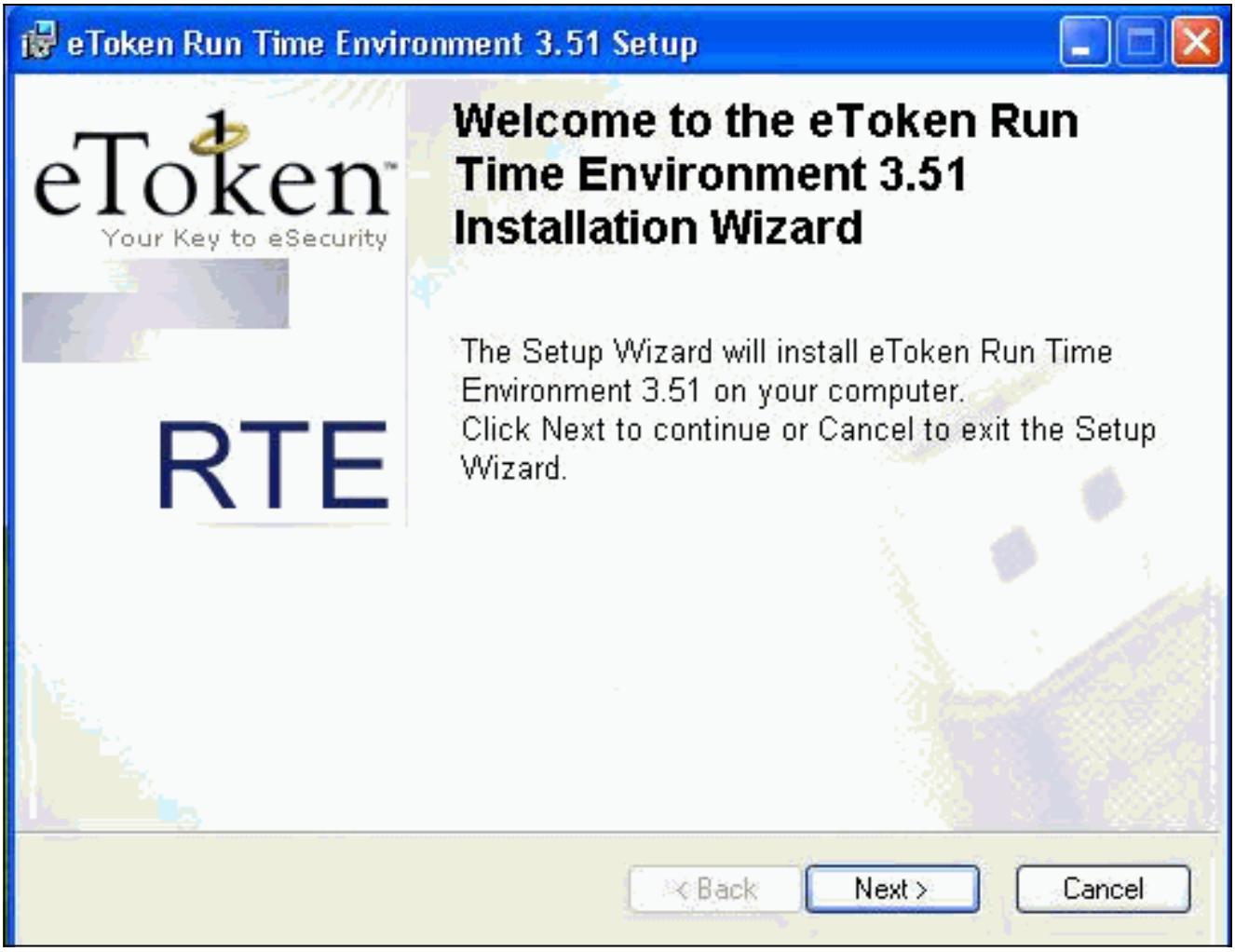
desejada e clique em
Conectar.



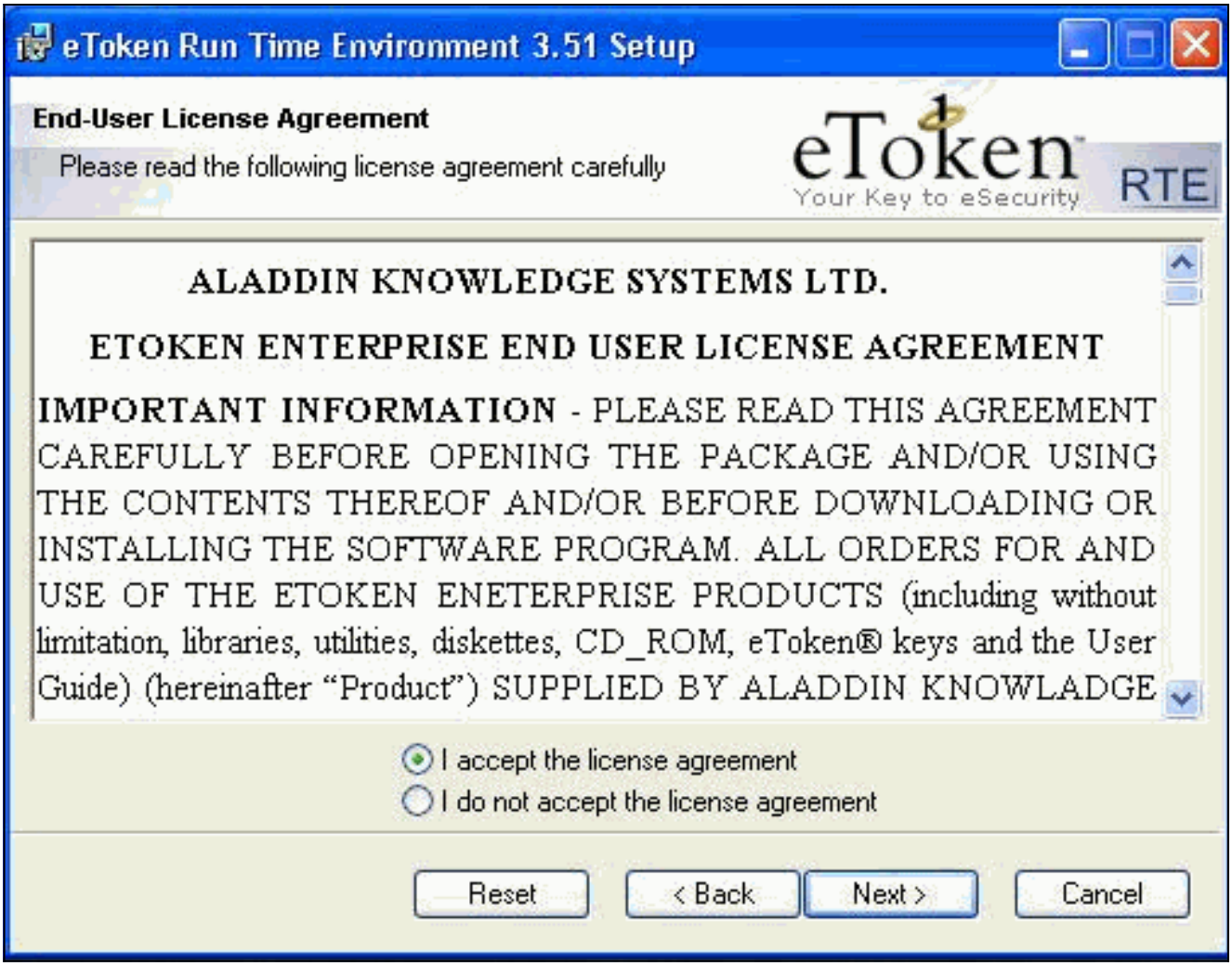
Instalar drivers eToken Smartcard

Estas etapas demonstram a instalação dos drivers Aladdin eToken Smartcard.

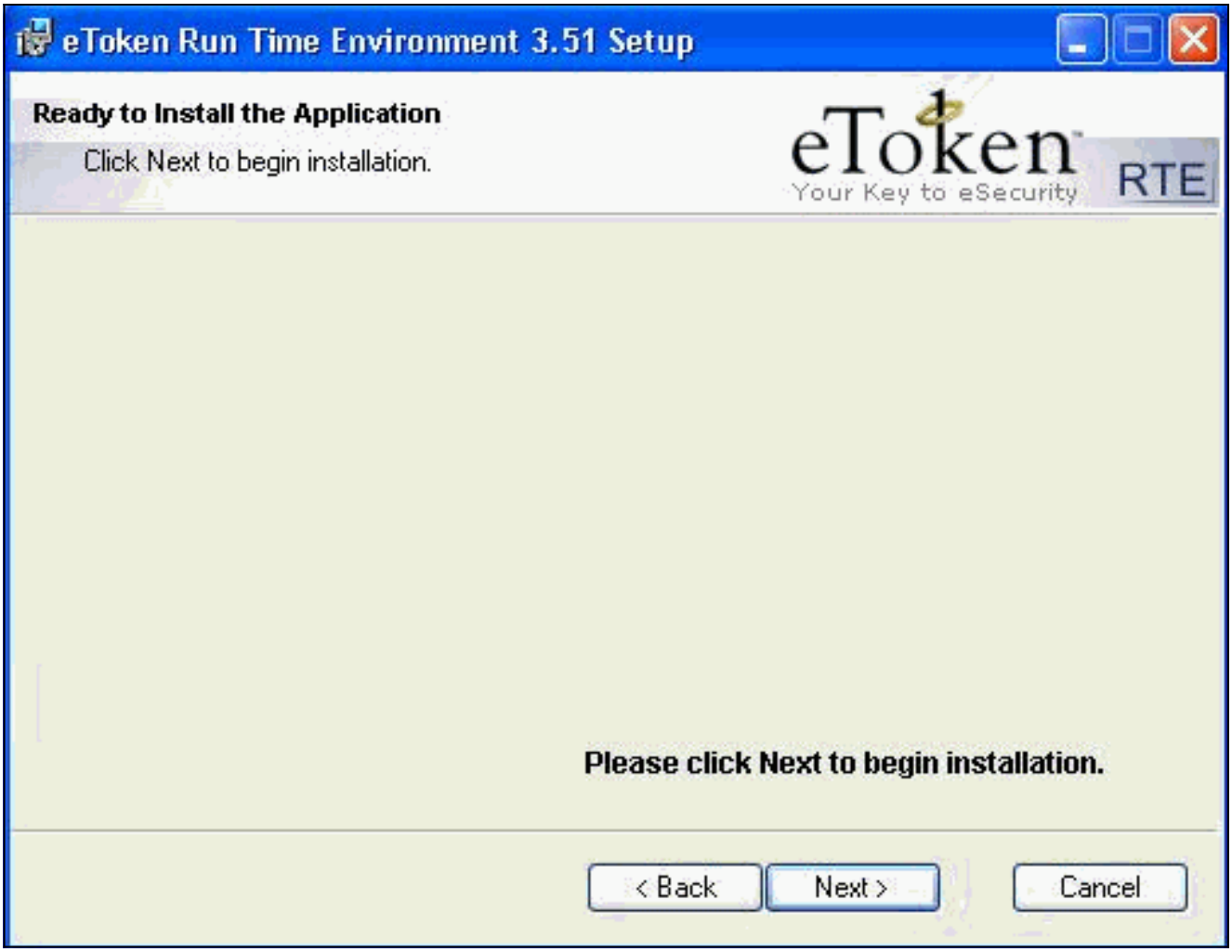
1. Abra o assistente de configuração eToken Run time Environment 3.51.



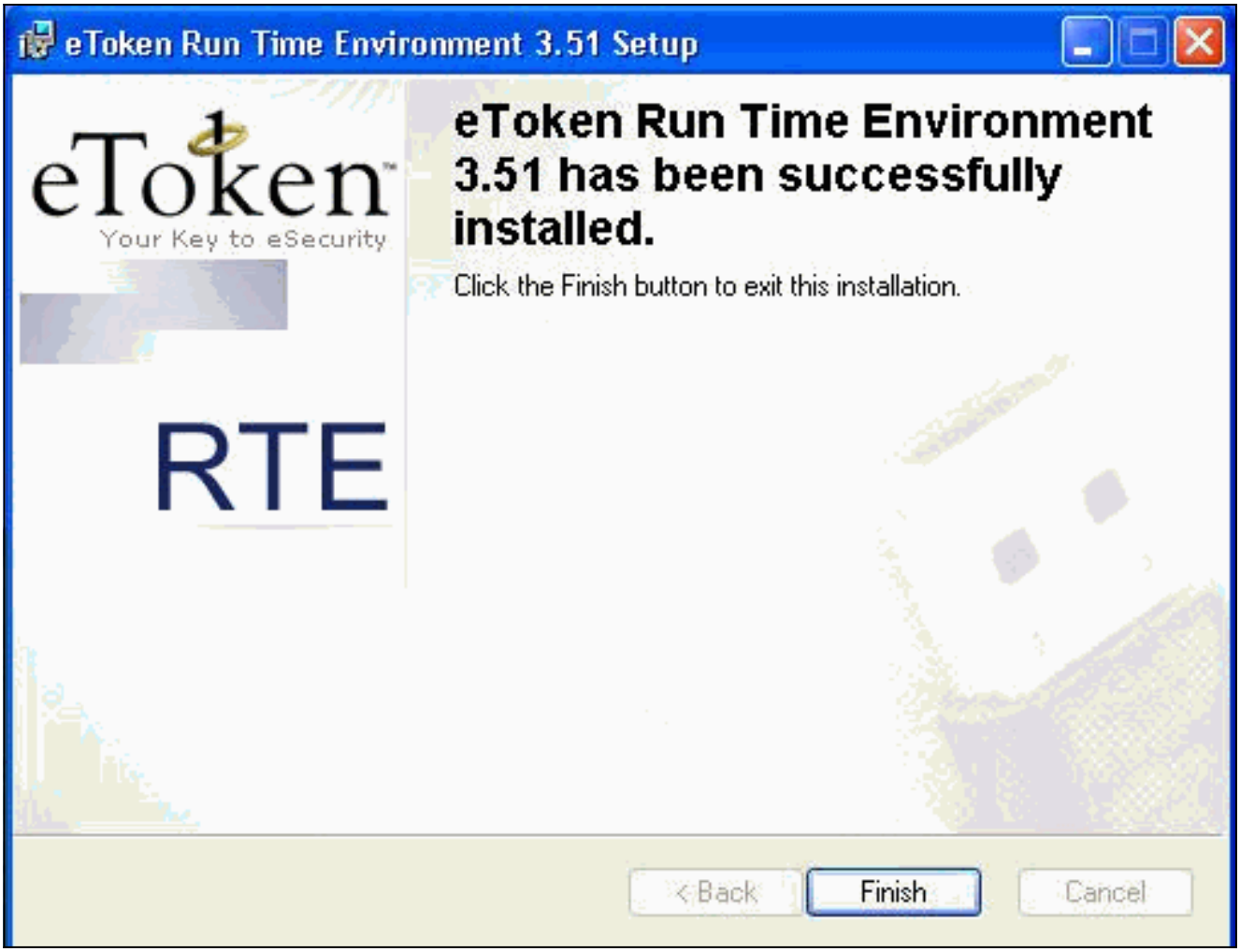
2. Aceite os termos do Contrato de Licença e clique em **Avançar**.



3. Clique em Instalar.



4. Os drivers do eToken Smartcard estão agora instalados. Clique em **Finish** para sair do assistente de
configuração.



Verificar

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto isakmp sa** — Exibe todas as associações de segurança (SAs) atuais do Internet Key Exchange (IKE) em um peer.

```
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** — Exibe as configurações usadas pelas associações de segurança atuais.

```
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:
```

Troubleshoot

Consulte Troubleshooting do PIX para Passar o Tráfego de Dados em um Túnel IPSec Estabelecido para obter mais informações sobre como solucionar problemas dessa configuração.

Informações Relacionadas

- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Página de suporte do IPSec (protocolo de segurança IP)
- Página de Suporte do Cisco VPN Client
- Página de suporte de PIX 500 Series Firewalls
- Suporte Técnico - Cisco Systems