

# IPsec entre o PIX e o Cisco VPN Client que usa o exemplo de configuração dos certificados smartcard

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Registre e configurar o PIX](#)

[Configurações](#)

[Registre certificados clientes Cisco VPN](#)

[Configurar o Cisco VPN Client a fim usar o certificado para a conexão ao PIX](#)

[Instale driveres etoken smartcard](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento demonstra como configurar um túnel do IPsec VPN entre um PIX Firewall e um Cisco VPN Client 4.0.x. O exemplo de configuração neste documento igualmente destaca o procedimento do registro do Certification Authority (CA) para o roteador de Cisco IOS® e o Cisco VPN Client, assim como o uso de Smartcard como um armazenamento do certificado.

Refira [configurar o IPsec entre o Roteadores do Cisco IOS e o Cisco VPN Client que usa certificados do entrust](#) a fim aprender mais sobre configurar o IPsec entre o Roteadores do Cisco IOS e o Cisco VPN Client que usa certificados do entrust.

Refira [configurar autoridades de certificado de identidade múltipla no Roteadores do Cisco IOS](#) a fim aprender mais sobre configurar autoridades de certificado de identidade múltipla no Roteadores do Cisco IOS.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

## Componentes Utilizados

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

- Cisco PIX Firewall que executa a versão de software 6.3(3)
- Cisco VPN Client 4.0.3 em um PC que executa Windows XP
- Um server de CA do Microsoft Windows 2000 é usado neste documento como o server de CA.
- Os Certificados no Cisco VPN Client são armazenados usando o e-token smartcard de [Aladdin](#).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## Registre e configurar o PIX

Nesta seção, você é apresentado com a informação a fim configurar as características descritas neste documento.

**Nota:** Para encontrar informações adicionais sobre os comandos usados neste documento, use a [Command Lookup Tool](#) ([somente clientes registrados](#)).

## Configurações

Este documento utiliza estas configurações.

- [Certificado de registro no PIX Firewall](#)
- [Configuração de firewall PIX](#)

### **Certificado de registro 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 <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
```

## Configuração de firewall PIX

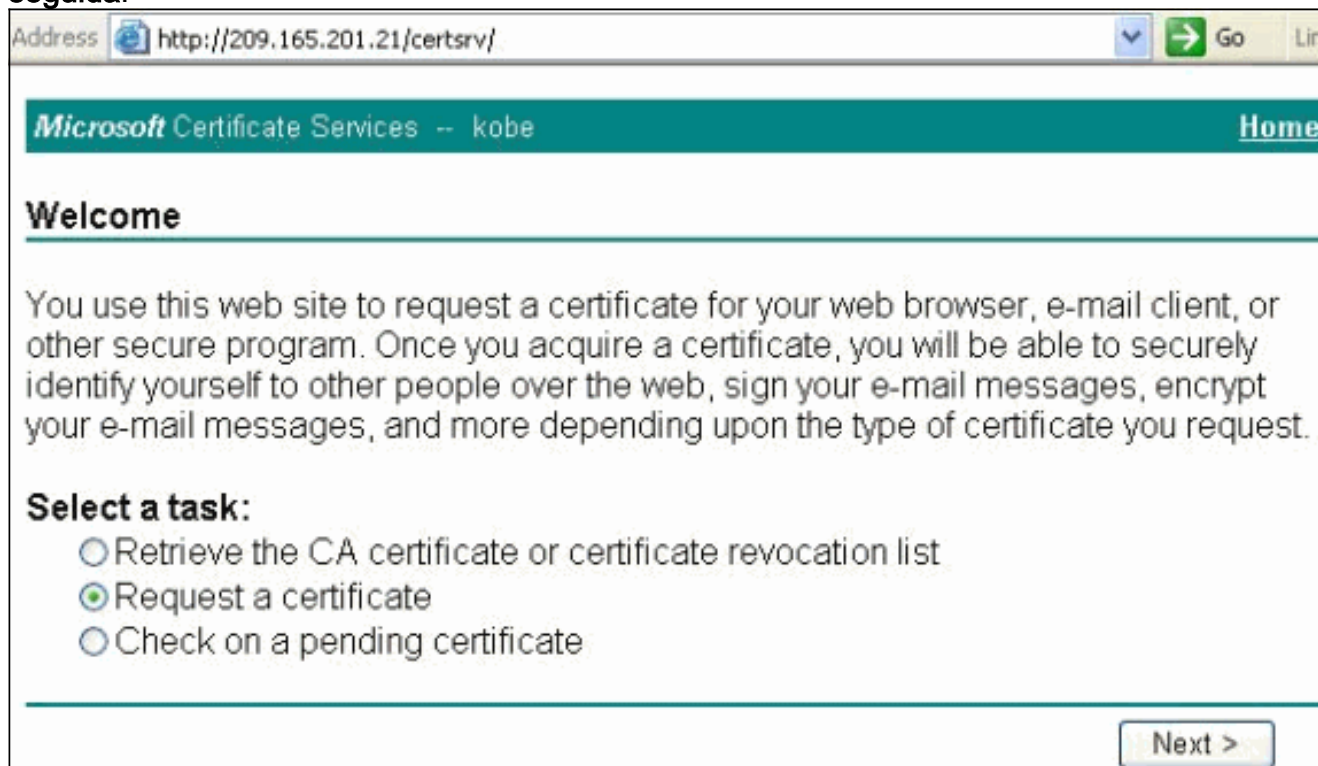
```
PIX Version 6.3(3) interface ethernet0 auto interface
ethernet1 auto interface ethernet2 auto shutdown
interface ethernet3 auto shutdown interface ethernet4
auto shutdown interface ethernet5 auto shutdown nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 nameif ethernet2 intf2 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)#
```

[Registre certificados clientes Cisco VPN](#)

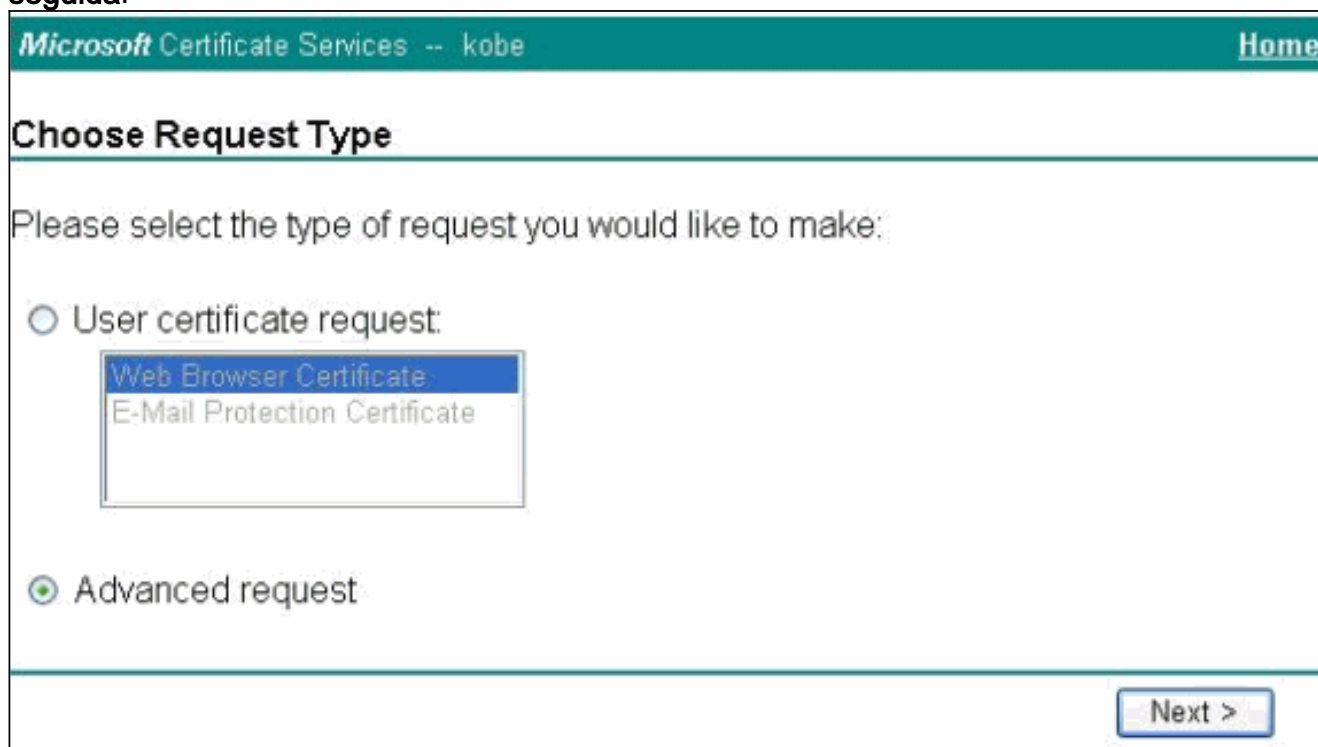
Recorde instalar todos os driveres necessários e utilidades que vêm com o dispositivo de Smartcard no PC a ser usado com o Cisco VPN Client.

Estas etapas demonstram os procedimentos usados para registrar o Cisco VPN Client para Certificados MS. O certificado é armazenado na loja do e-token smartcard de [Aladdin](#).

1. Lance um navegador e vá à página do servidor certificado (<http://CAServeraddress/certsrv/>, neste exemplo).
2. Selecione o **pedido um certificado** e clique-o em **seguida**.



3. No tipo indicador, **pedido avançado** selete e clique do pedido da escolha em **seguida**.



4. Seletor submeta um pedido de certificado para este CA usando um formulário e clique-o em seguida.

Microsoft Certificate Services -- kobe [Home](#)

### Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.  
*You must have an enrollment agent certificate to submit a request for another user.*

[Next >](#)

5. Preencha todos os artigos no formulário de requisição de certificado avançado. Seja certo que o departamento ou a unidade organizacional (OU) correspondem ao nome do grupo do Cisco VPN Client, como configurado no nome do vpngroup PIX. Selecione o Certificate Service Provider correto (CSP) apropriado para sua instalação.

## Advanced Certificate Request

### Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

### Intended Purpose:

### Key Options:

CSP:

Key Usage:  Exchange  Signature  Both

Key Size:  Min: 384  
Max: 1024 (common key sizes: [512](#) [1024](#))

Create new key set  
 Set the container name

Use existing key set

Enable strong private key protection

Mark keys as exportable

Use local machine store

*You must be an administrator to generate*

### Additional Options:

Hash Algorithm:    
*Only used to sign request.*

Save request to a PKCS #10 file

Attributes:

6. Selecione **sim** a fim continuar a instalação quando você obtém o aviso potencial da validação do script.

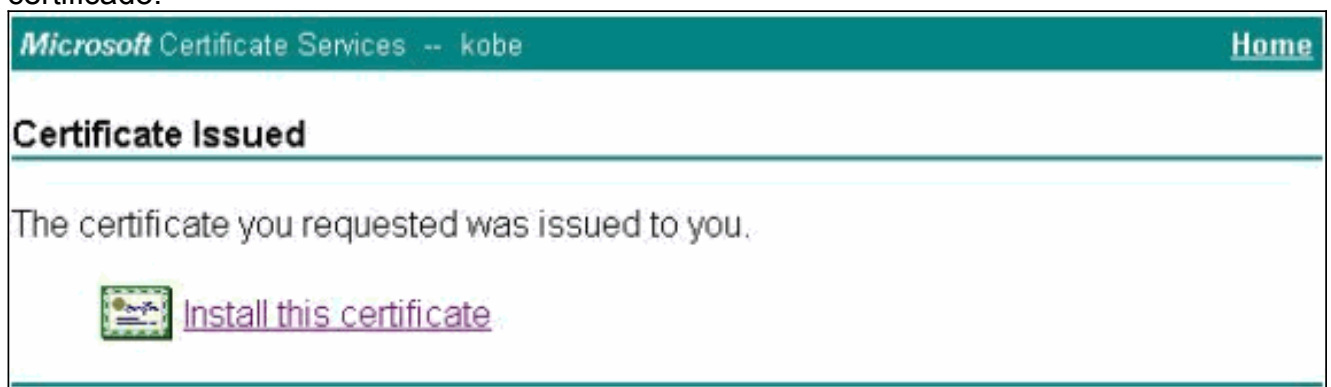


7. O certificado de registro invoca a loja do eToken. Incorpore a senha e clique a



**APROVAÇÃO.**

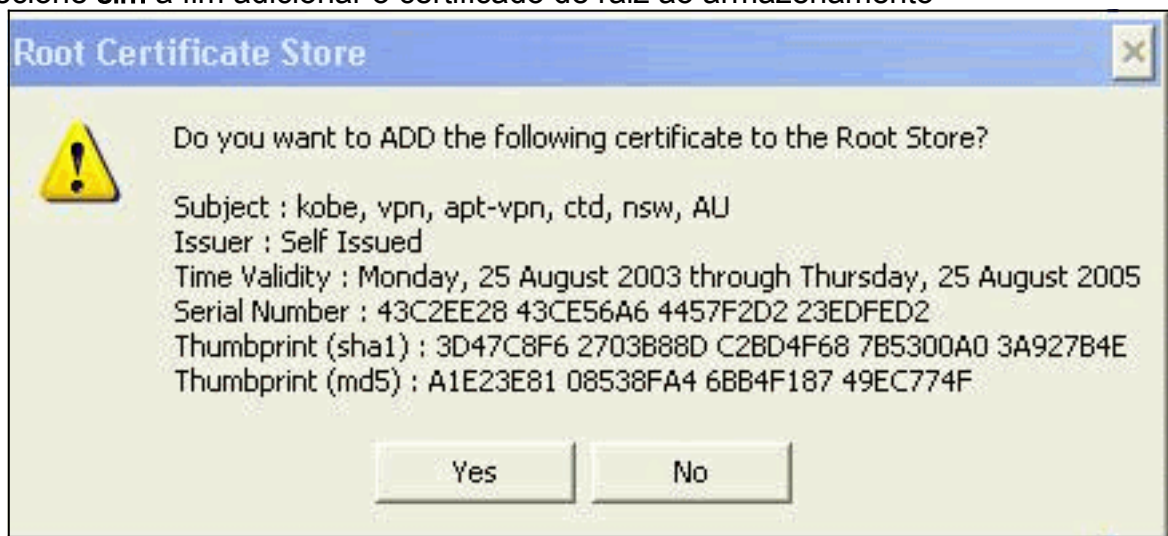
8. Clique em Instalar este certificado.



9. Selecione **sim** a fim continuar a instalação quando você obtém o aviso potencial da validação do script.

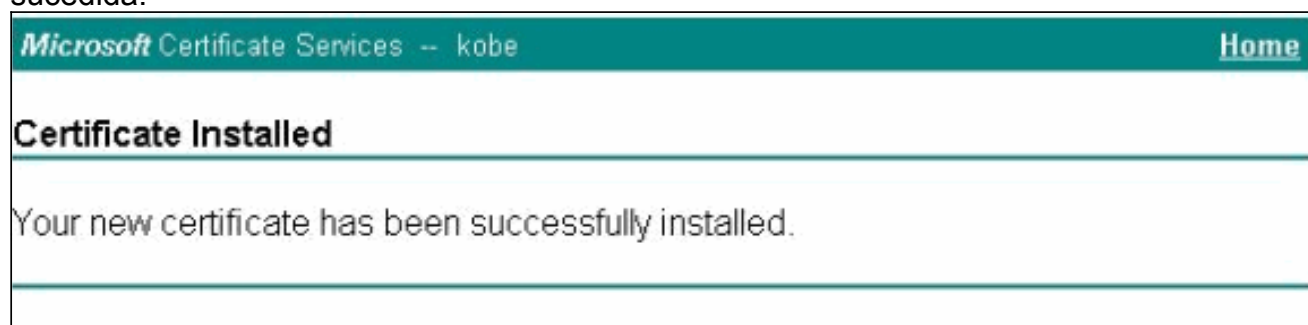


10. Selecione **sim** a fim adicionar o certificado de raiz ao armazenamento



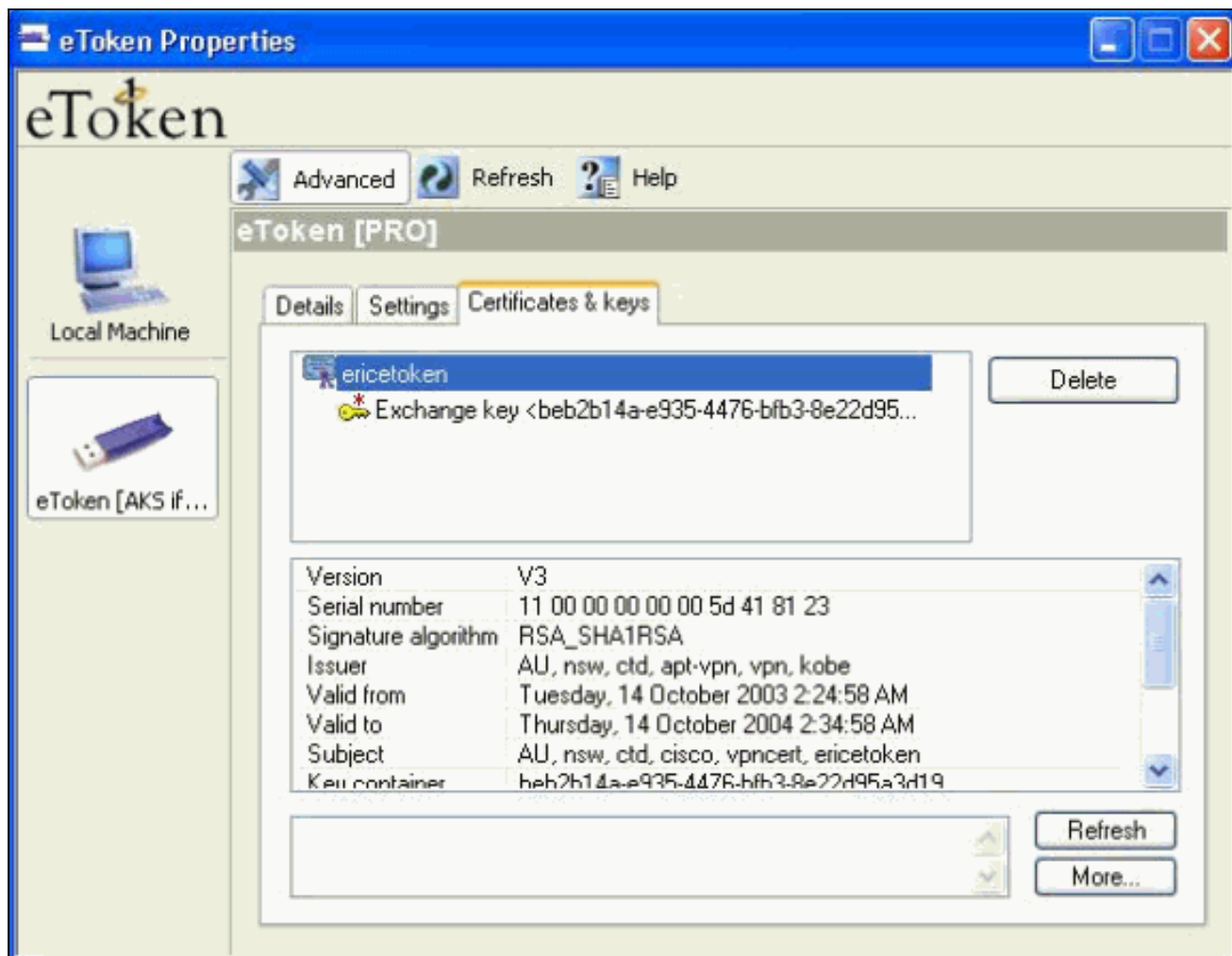
raiz.

11. O indicador instalado certificado aparece e confirma a instalação bem-sucedida.



12. Use o eToken Application Viewer a fim ver o certificado armazenado em Smartcard.

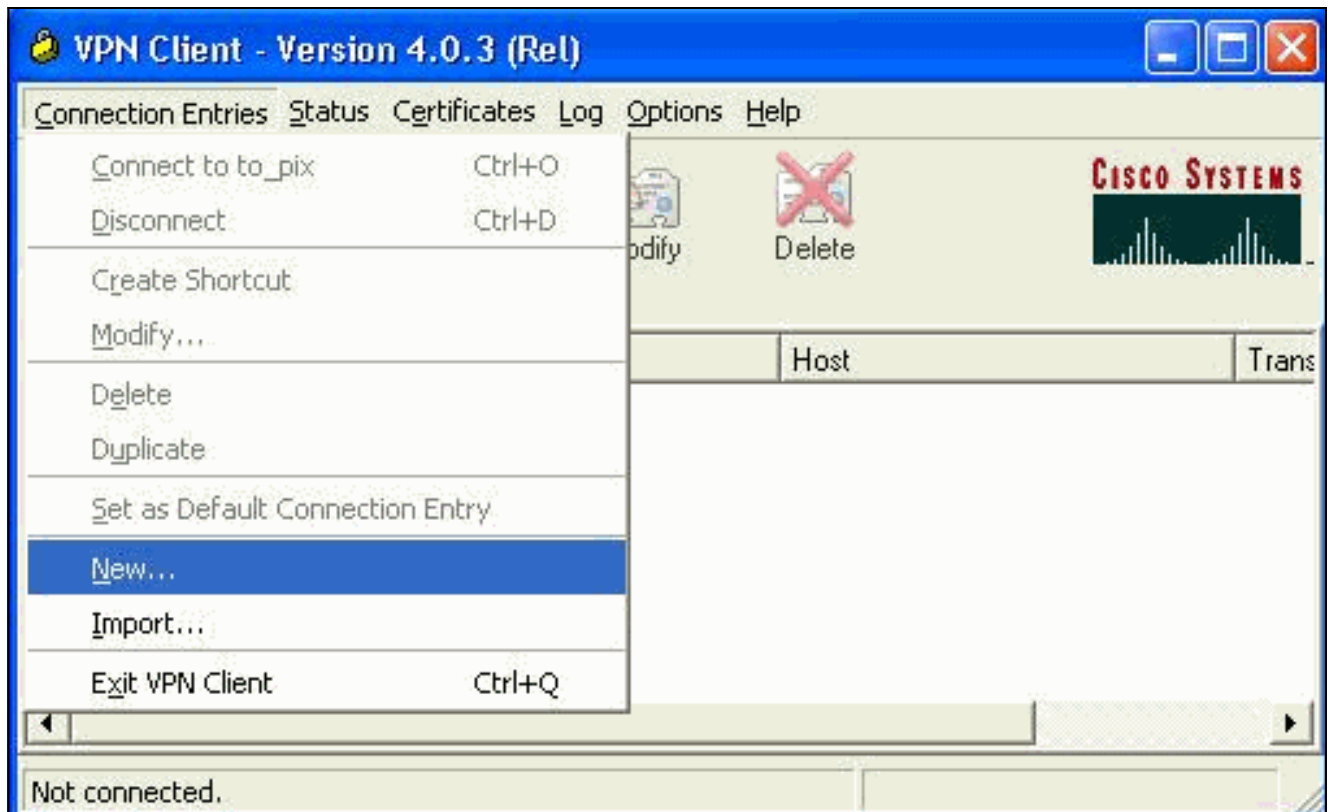




## [Configurar o Cisco VPN Client a fim usar o certificado para a conexão ao PIX](#)

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

1. Lance o Cisco VPN Client. Sob entradas de conexão clique **novo** a fim criar uma nova conexão.



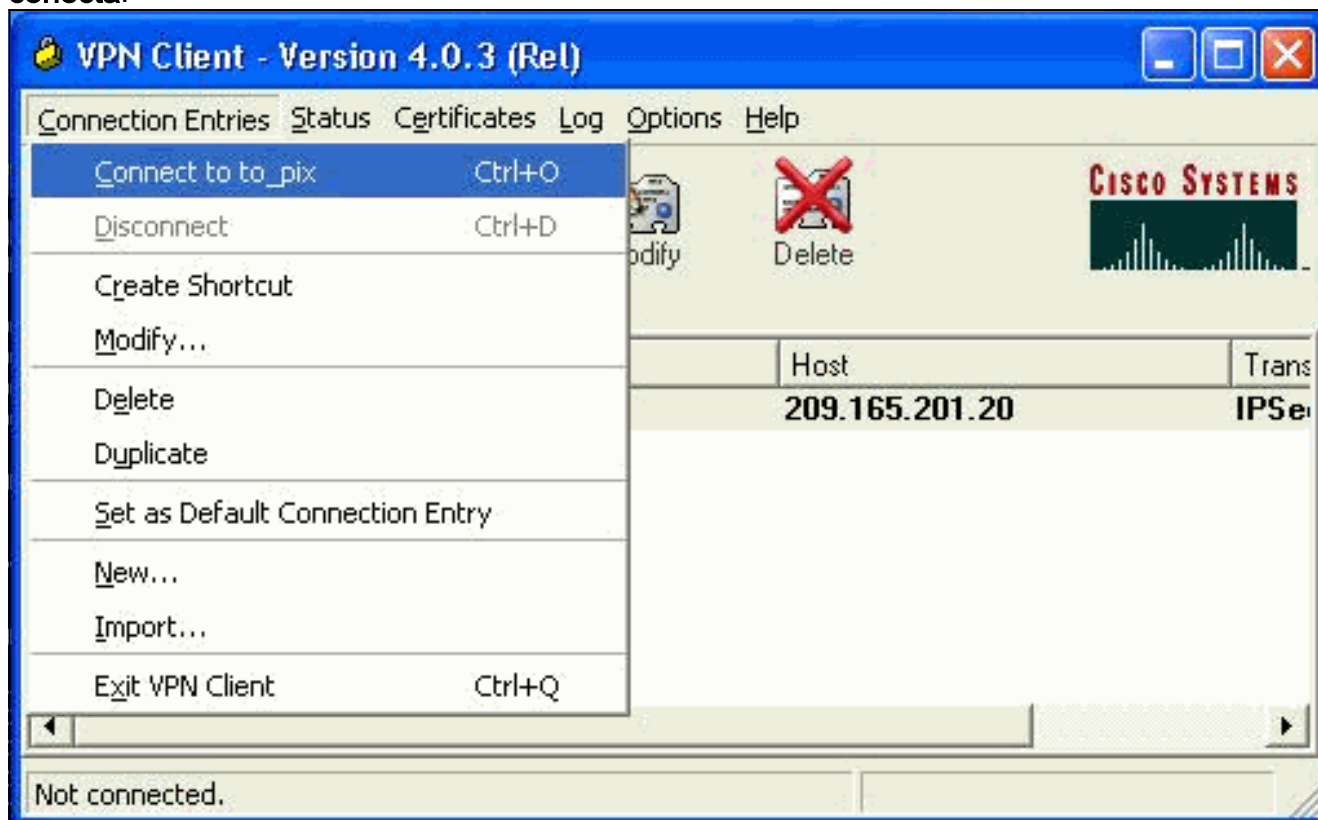
2. Termine o detalhe da conexão, especifique o certificado de autenticação, selecione o certificado obtido do registro. Clique em



Salvar.

3. A fim começar a conexão do Cisco VPN Client ao PIX, para selecionar a entrada de conexão

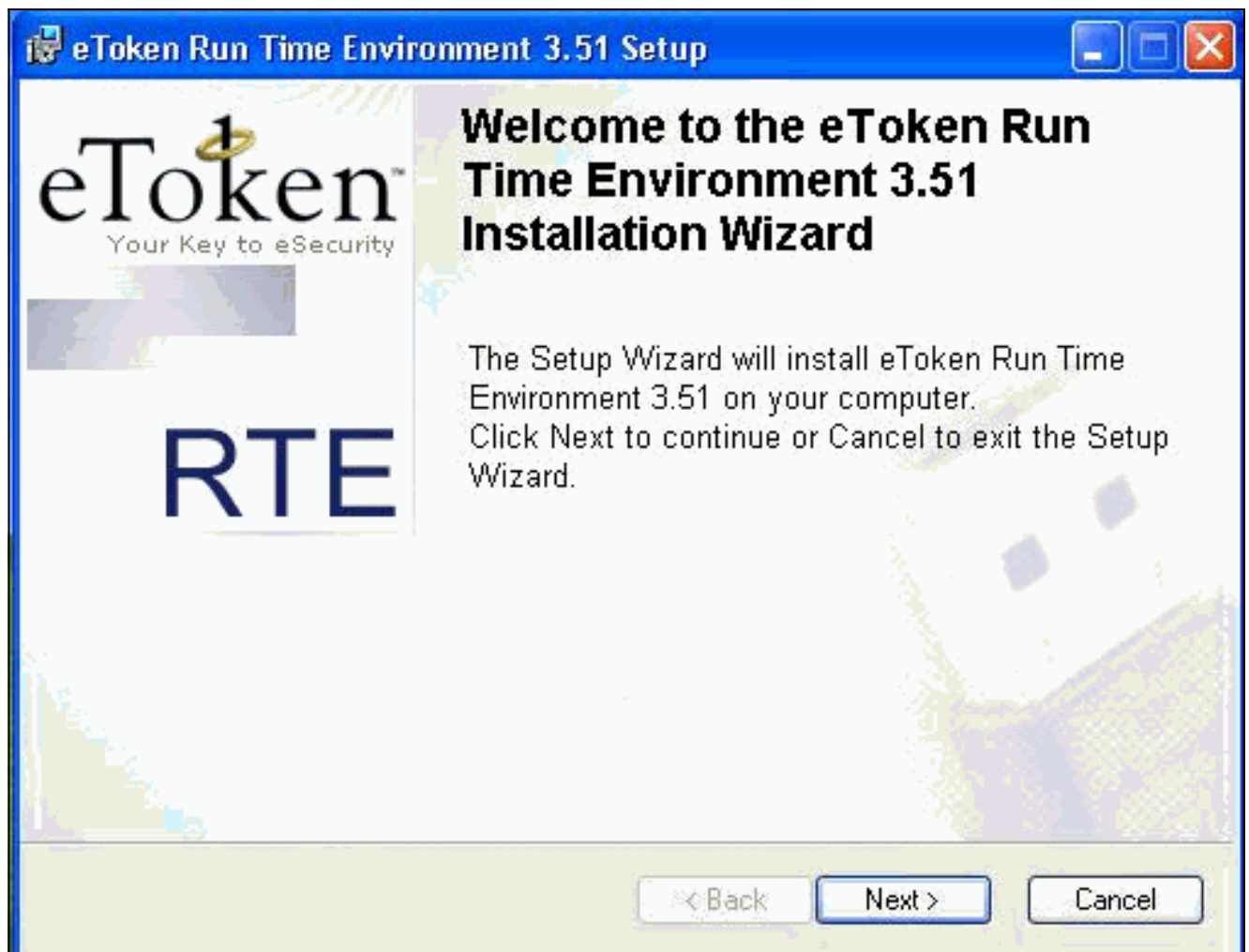
e o clique desejados  
conecta.



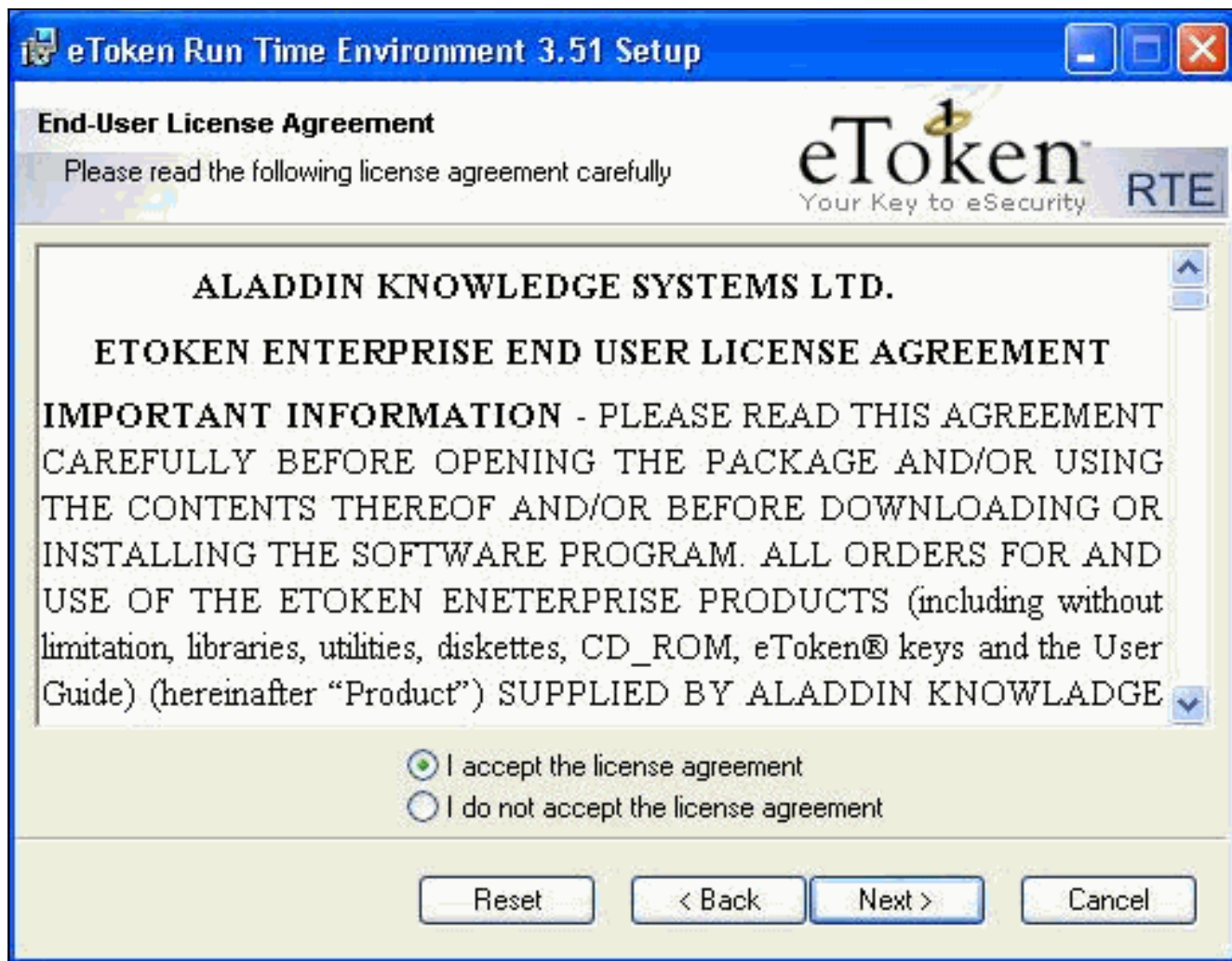
## Instale driveres etoken smartcard

Estas etapas demonstram a instalação dos [driveres aladdin etoken smartcard](#) .

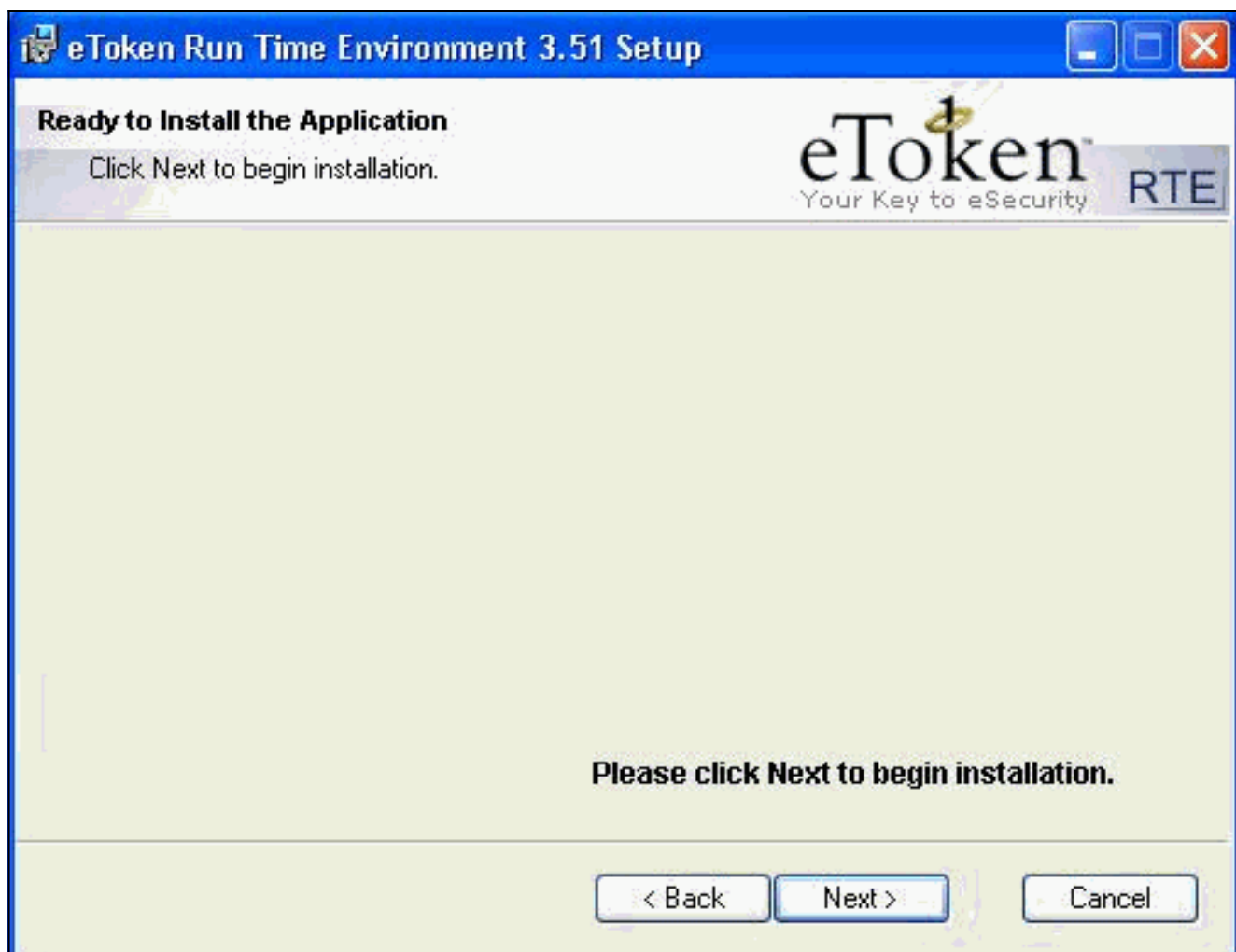
1. Abra o assistente de configuração do ambiente de tempo de corrida 3.51 do eToken.



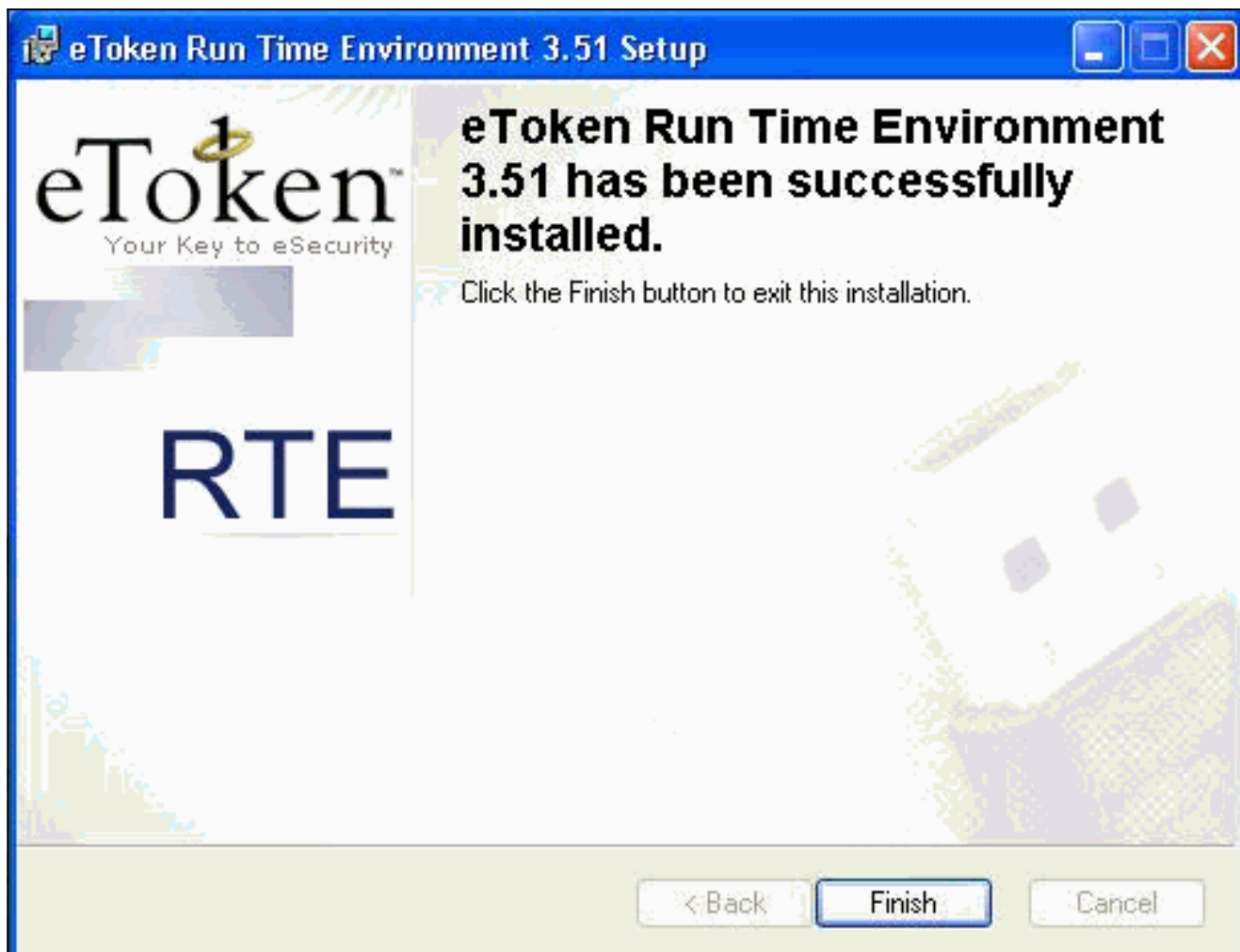
2. Aceite os termos do contrato de licença e clique-os **em seguida**.



3. O clique instala.



4. Os driveres etoken smartcard são instalados agora. **Revestimento do clique a fim retirar o 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.

- **mostre isakmp cripto sa** — Indica todas as associações de segurança atuais do Internet Key Exchange (IKE) (SA) em um par. `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
- **mostre IPsec cripto sa** — Indica os ajustes usados por associações de segurança atual. `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:

## Troubleshooting

Refira a [pesquisa de defeitos do PIX para passar o tráfego de dados em um túnel IPSec estabelecido](#) para mais informações sobre de pesquisar defeitos esta 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 dos Firewall da série PIX 500](#)
- [Suporte Técnico - Cisco Systems](#)