

Ejemplo de Configuración de IPSec entre PIX y Cisco VPN Client Usando Certificados Smartcard

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Inscripción y configuración de PIX](#)

[Configuraciones](#)

[Inscriba certificados de Cisco VPN Client](#)

[Configure Cisco VPN Client para Utilizar el Certificado para la Conexión con el PIX](#)

[Instalación de controladores de tarjeta inteligente eToken](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

[Introducción](#)

Este documento muestra cómo configurar un túnel IPSec VPN entre un Firewall PIX y un Cisco VPN Client 4.0.x. El ejemplo de configuración de este documento también resalta el procedimiento de inscripción de la entidad de certificación (CA) tanto para el router Cisco IOS® como para Cisco VPN Client, así como el uso de una Smartcard como almacenamiento de certificados.

Consulte [Configuración de IPSec entre Cisco IOS Routers y Cisco VPN Client Usando Certificados Entrust](#) para obtener más información sobre la Configuración de IPSec entre Cisco IOS Routers y Cisco VPN Client usando Certificados Entrust.

Consulte [Configuración de Autoridades de Certificados de Identidad Múltiple en Cisco IOS Routers](#) para obtener más información sobre la Configuración de Autoridades de Certificados de Identidad Múltiple en Cisco IOS Routers.

[Prerequisites](#)

[Requirements](#)

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco PIX Firewall que ejecuta la versión de software 6.3(3)
- Cisco VPN Client 4.0.3 en un PC con Windows XP
- En este documento se utiliza un servidor de CA de Microsoft Windows 2000 como servidor de CA.
- Los certificados en Cisco VPN Client se almacenan 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.

Convenciones

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Inscripción y configuración de PIX

En esta sección se ofrece información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

Configuraciones

Este documento usa estas configuraciones.

- [Inscripción de certificados en PIX Firewall](#)
- [Configuración de Firewall de PIX](#)

Inscripción de certificados en 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
```

Configuración de Firewall de 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)#

```

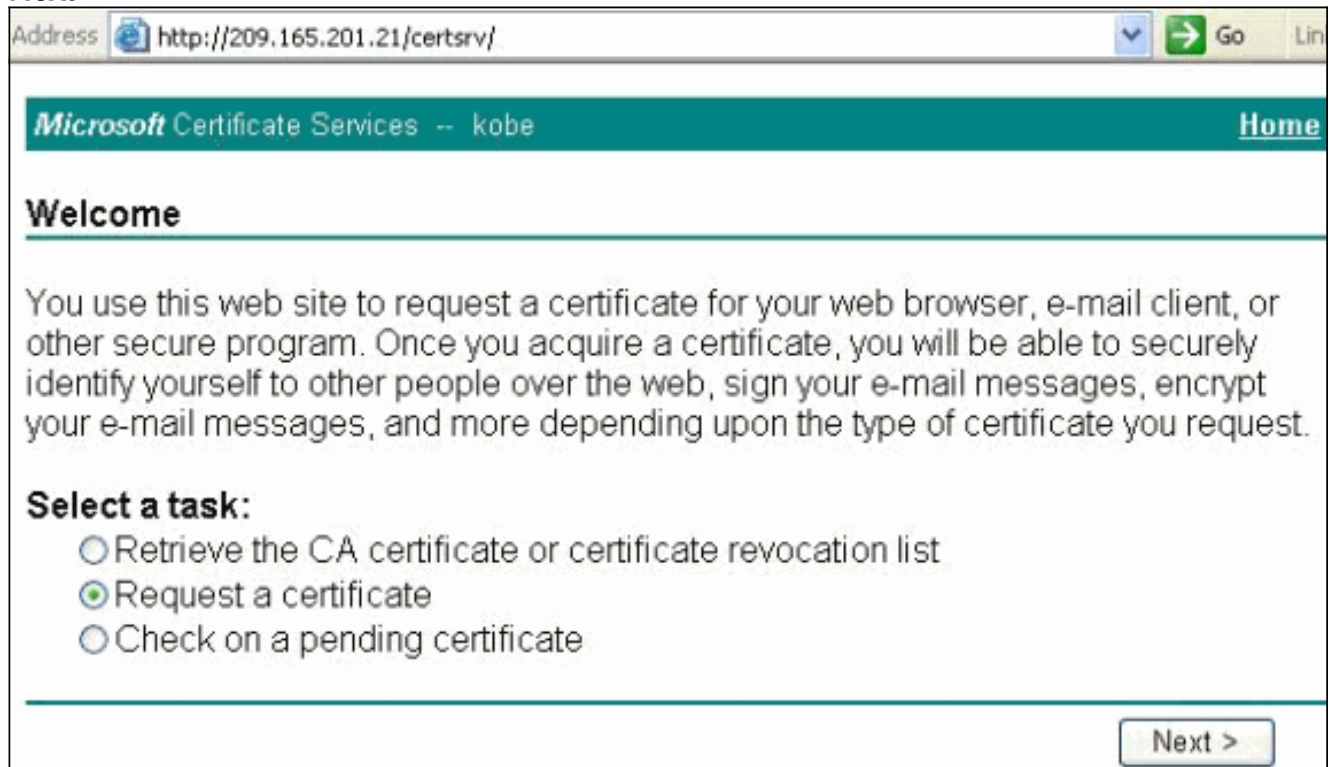
[Inscriba certificados de Cisco VPN Client](#)

Recuerde instalar todos los controladores y utilidades necesarios que vienen con el dispositivo Smartcard en el PC para ser usados con Cisco VPN Client.

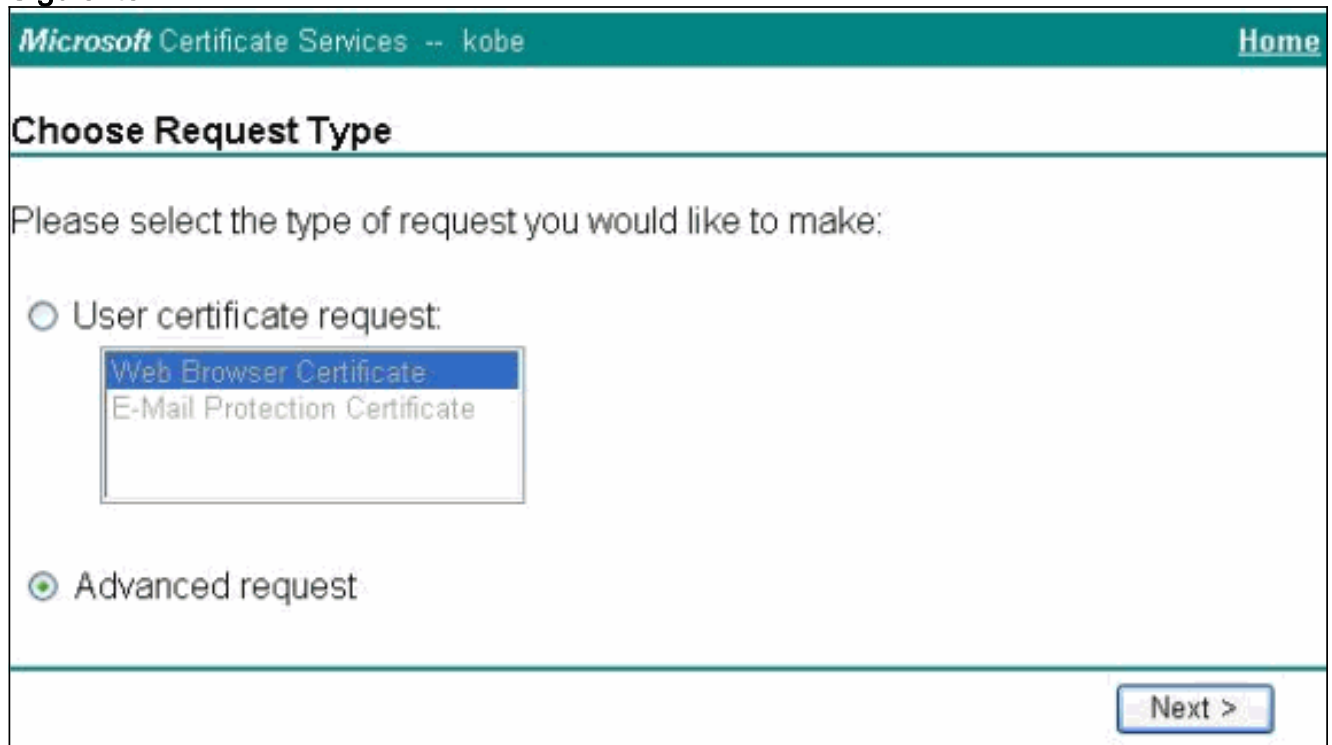
Estos pasos demuestran los procedimientos utilizados para inscribir Cisco VPN Client para

certificados MS. El certificado se almacena en la [tienda Aladdin](#) e-Token Smartcard.

1. Inicie un explorador y vaya a la página servidor de certificados (<http://CAServeraddress/certsrv/>, en este ejemplo).
2. Seleccione **Request a certificate** y haga clic en **Next**.



3. En la ventana Elegir tipo de solicitud, seleccione **Solicitud avanzada** y haga clic en **Siguiente**.



4. Seleccione **Submit a certificate request to this CA using a form** y haga clic en **Next**.

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. Rellene todos los elementos del formulario de solicitud de certificado avanzado. Asegúrese de que el Departamento o la unidad organizativa (OU) corresponda al nombre del grupo de Cisco VPN Client, tal como se configuró en el nombre del vpngroup PIX. Seleccione el proveedor de servicios de certificados (CSP) adecuado para la configuración.

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. Seleccione **Yes** para continuar con la instalación cuando reciba la advertencia Validación de scripts potencial.

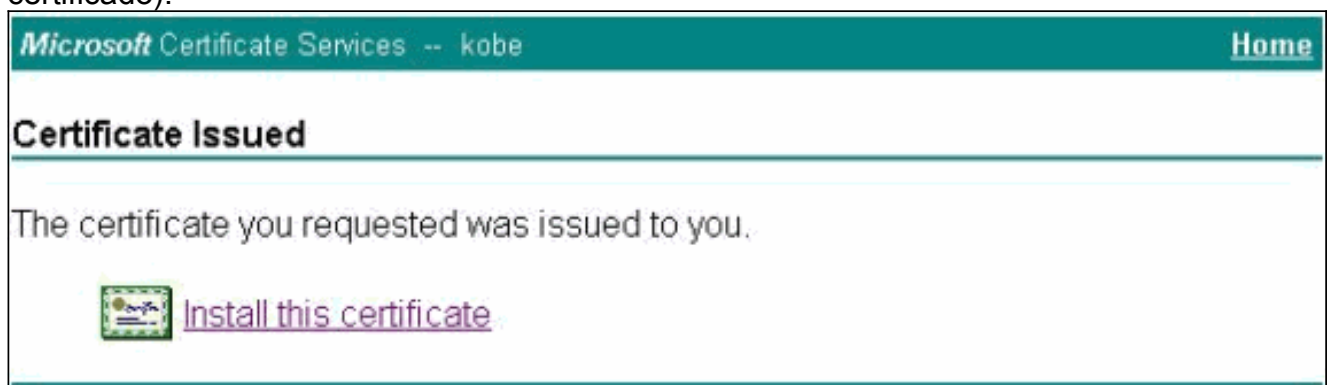


7. La inscripción de certificados invoca el almacén de eToken. Introduzca la contraseña y haga

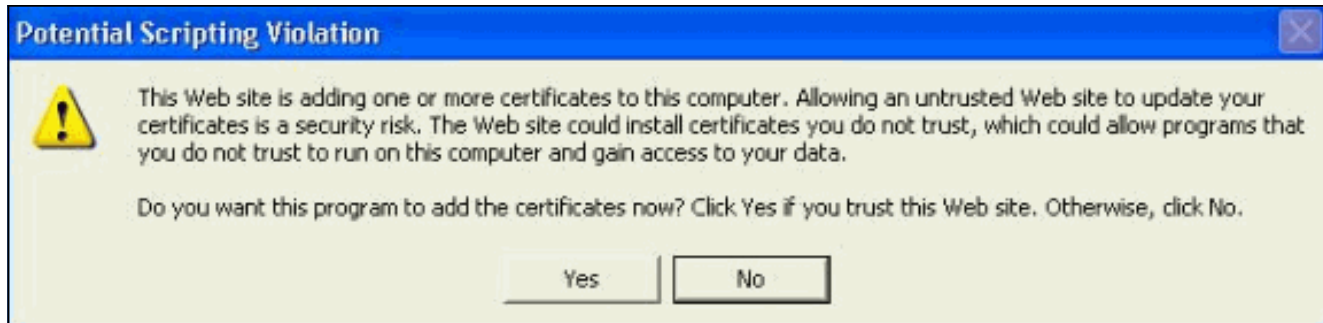


clic en **Aceptar**.

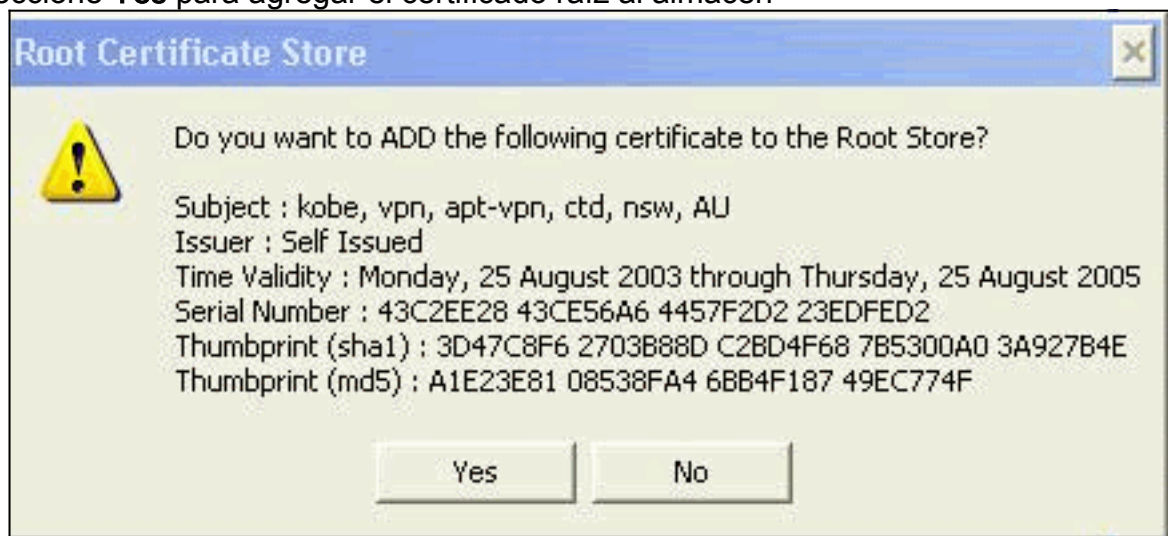
8. Haga clic en Install this certificate (Instalar este certificado).



9. Seleccione **Yes** para continuar con la instalación cuando reciba la advertencia Validación de scripts potencial.

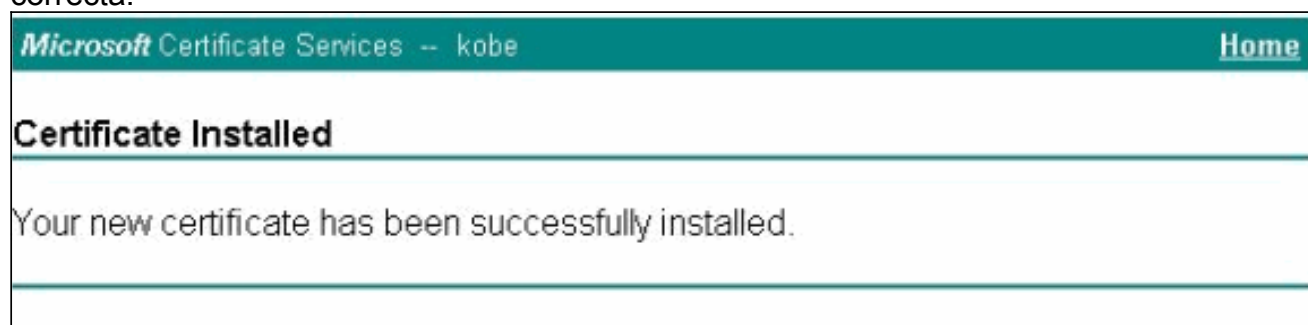


10. Seleccione **Yes** para agregar el certificado raíz al almacén

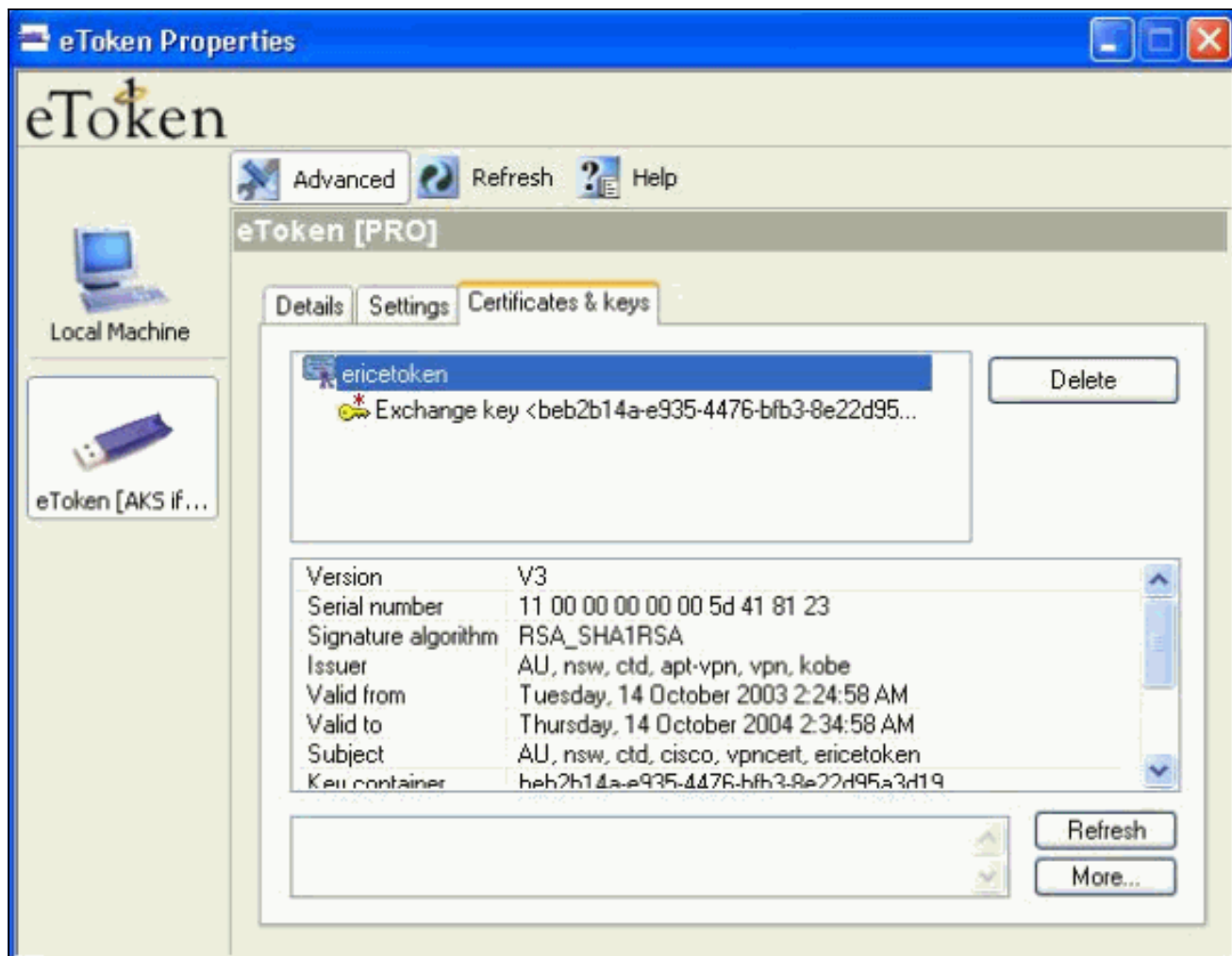


raíz.

11. Aparece la ventana Certificado instalado y confirma la instalación correcta.



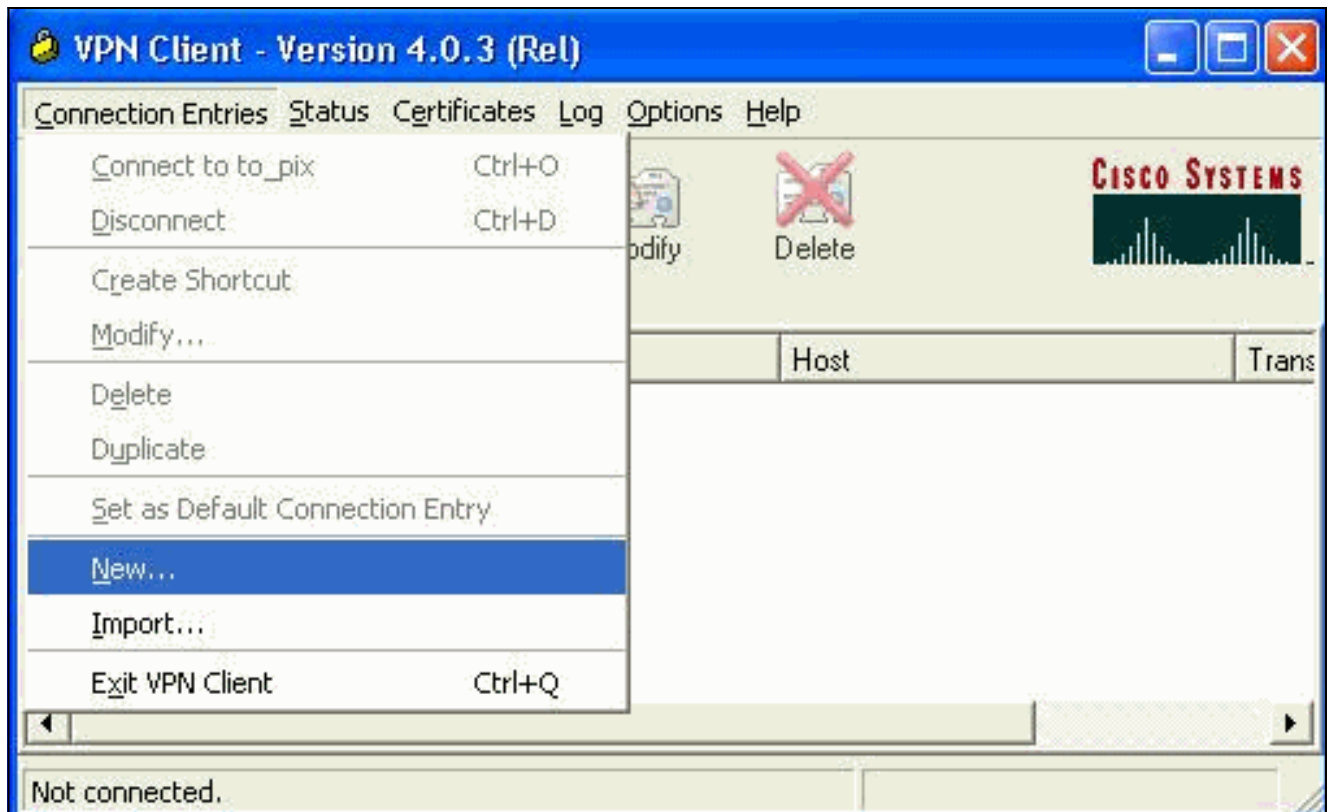
12. Utilice eToken Application Viewer para ver el certificado almacenado en la Smartcard.



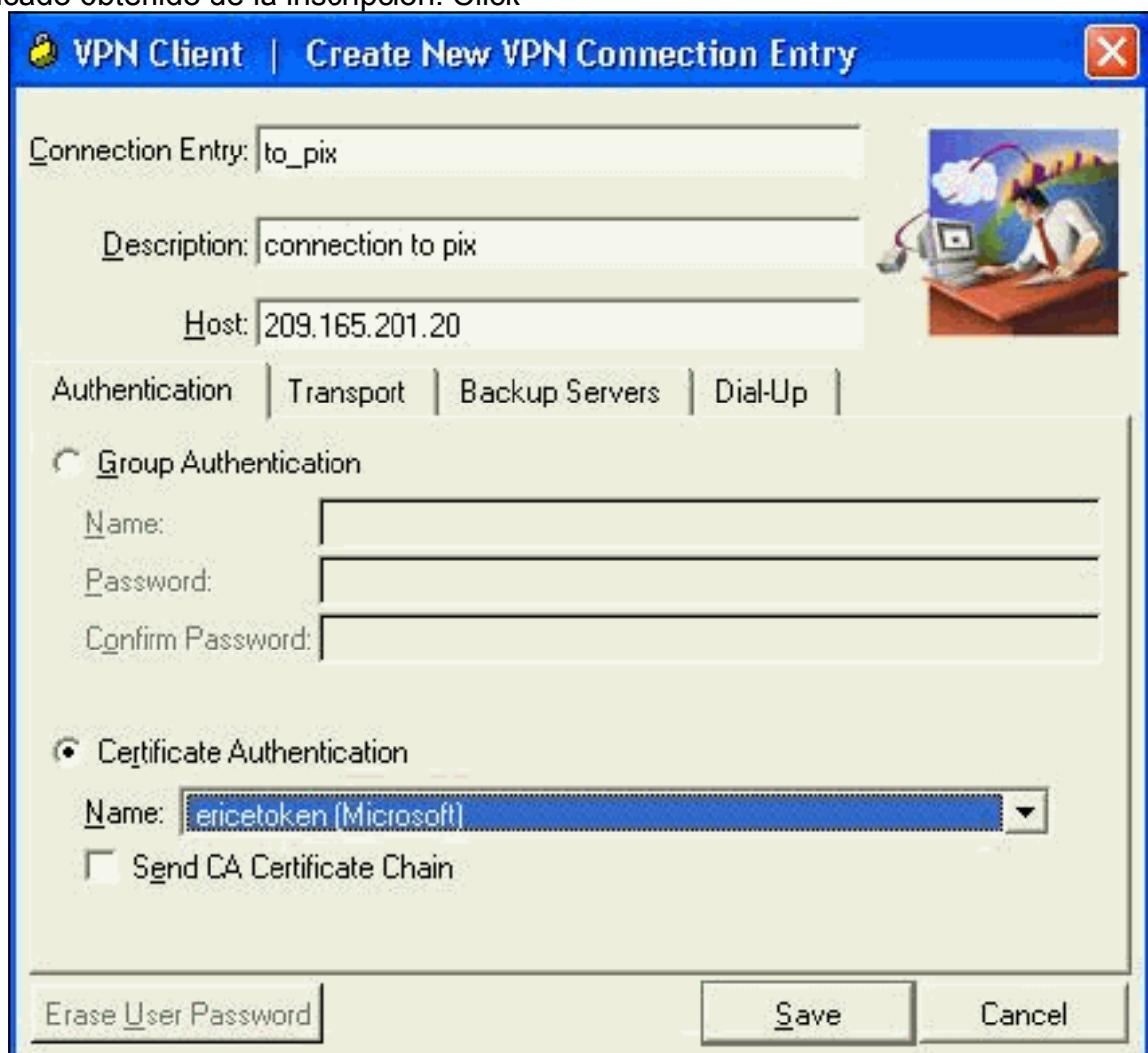
[Configure Cisco VPN Client para Utilizar el Certificado para la Conexión con el PIX](#)

Estos pasos demuestran los procedimientos utilizados para configurar Cisco VPN Client para utilizar el certificado para las conexiones PIX.

1. Inicie Cisco VPN Client. En Connection Entries (Entradas de conexión), haga clic en **New** para crear una nueva conexión.



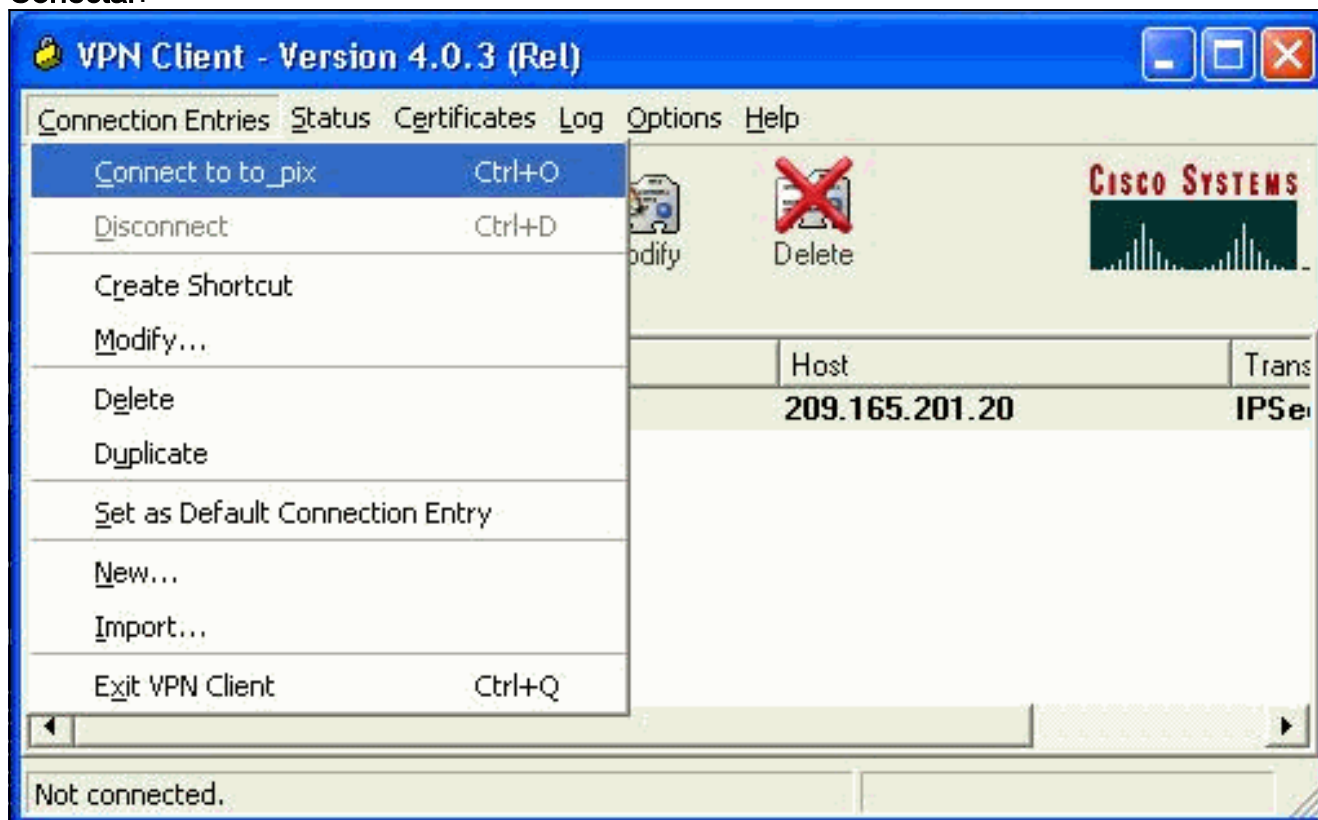
2. Complete el detalle de conexión, especifique la autenticación de certificado y seleccione el certificado obtenido de la inscripción. Click



Save.

3. Para iniciar la conexión de Cisco VPN Client con el PIX, seleccione la entrada de conexión

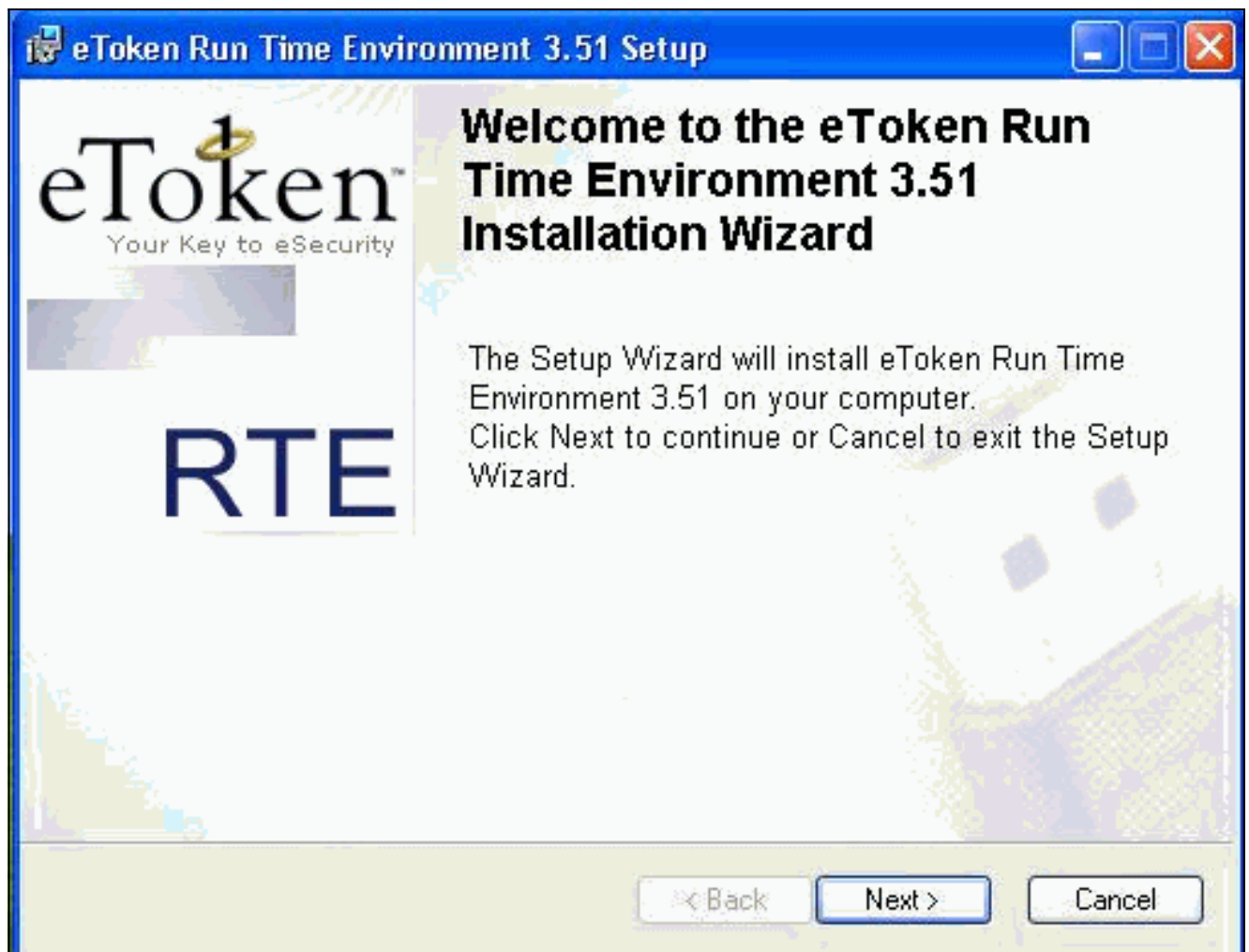
deseada y haga clic en **Conectar**.



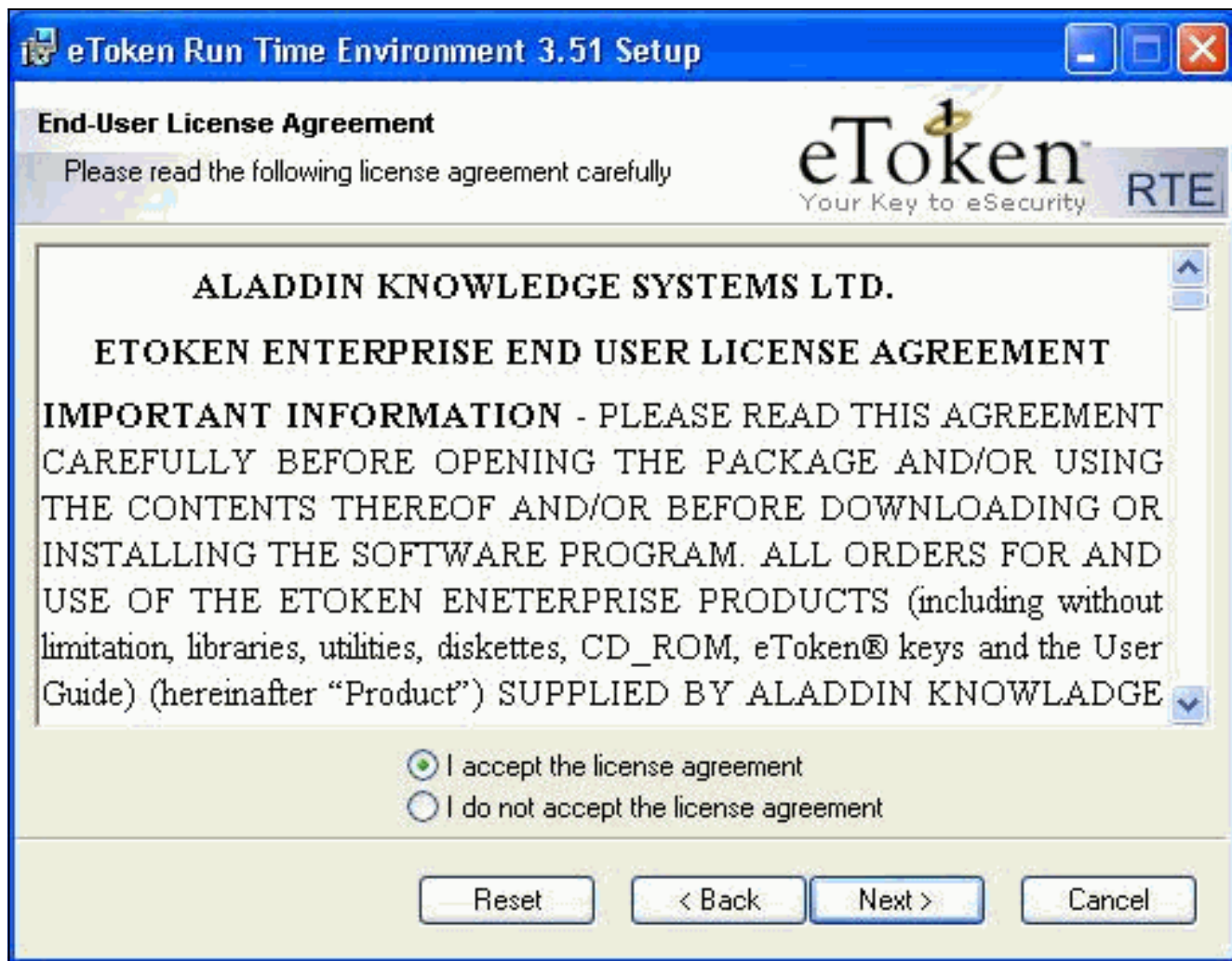
[Instalación de controladores de tarjeta inteligente eToken](#)

Estos pasos demuestran la instalación de los controladores [Aladdin](#) eToken Smartcard.

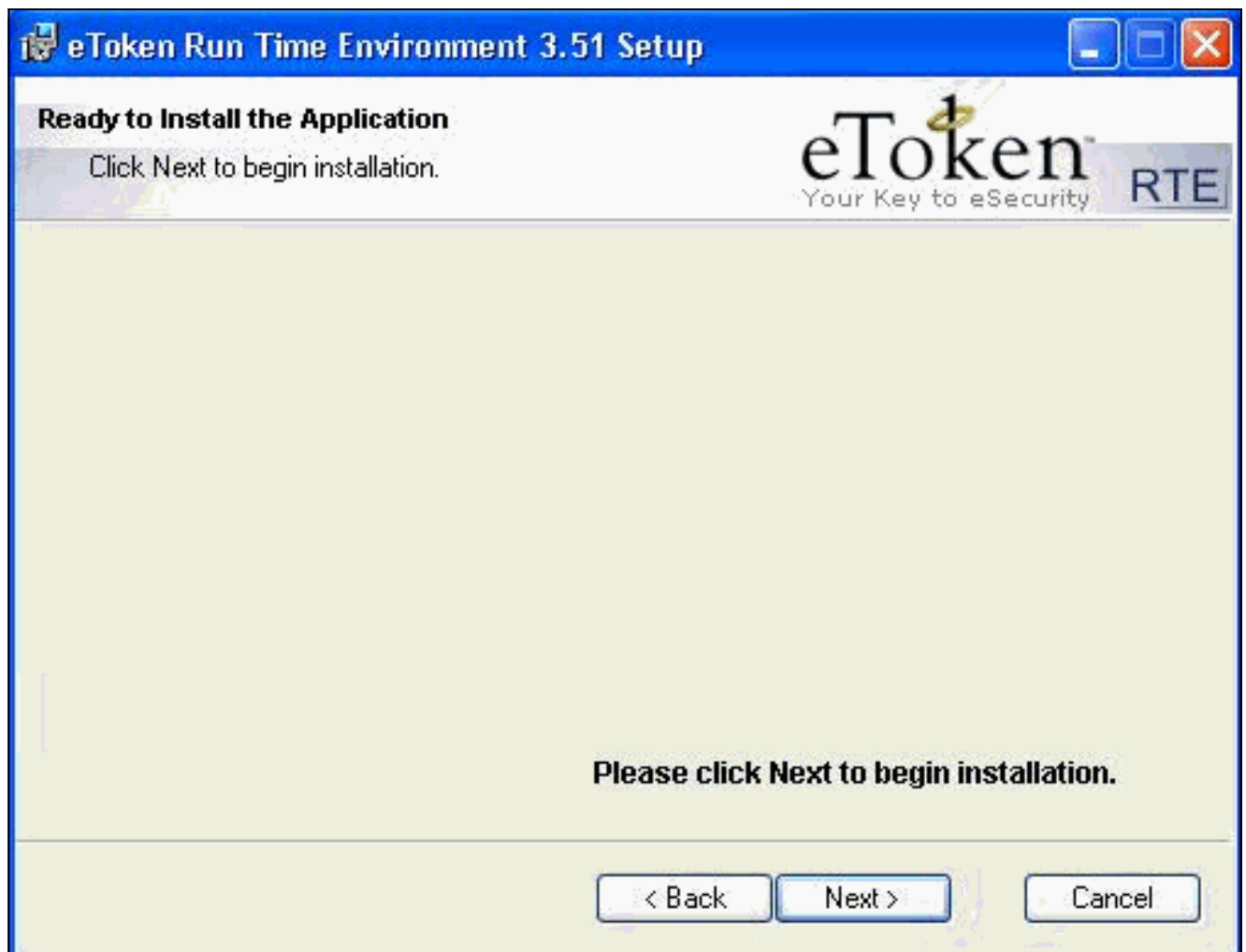
1. Abra el asistente de configuración de eToken Run time Environment 3.51.



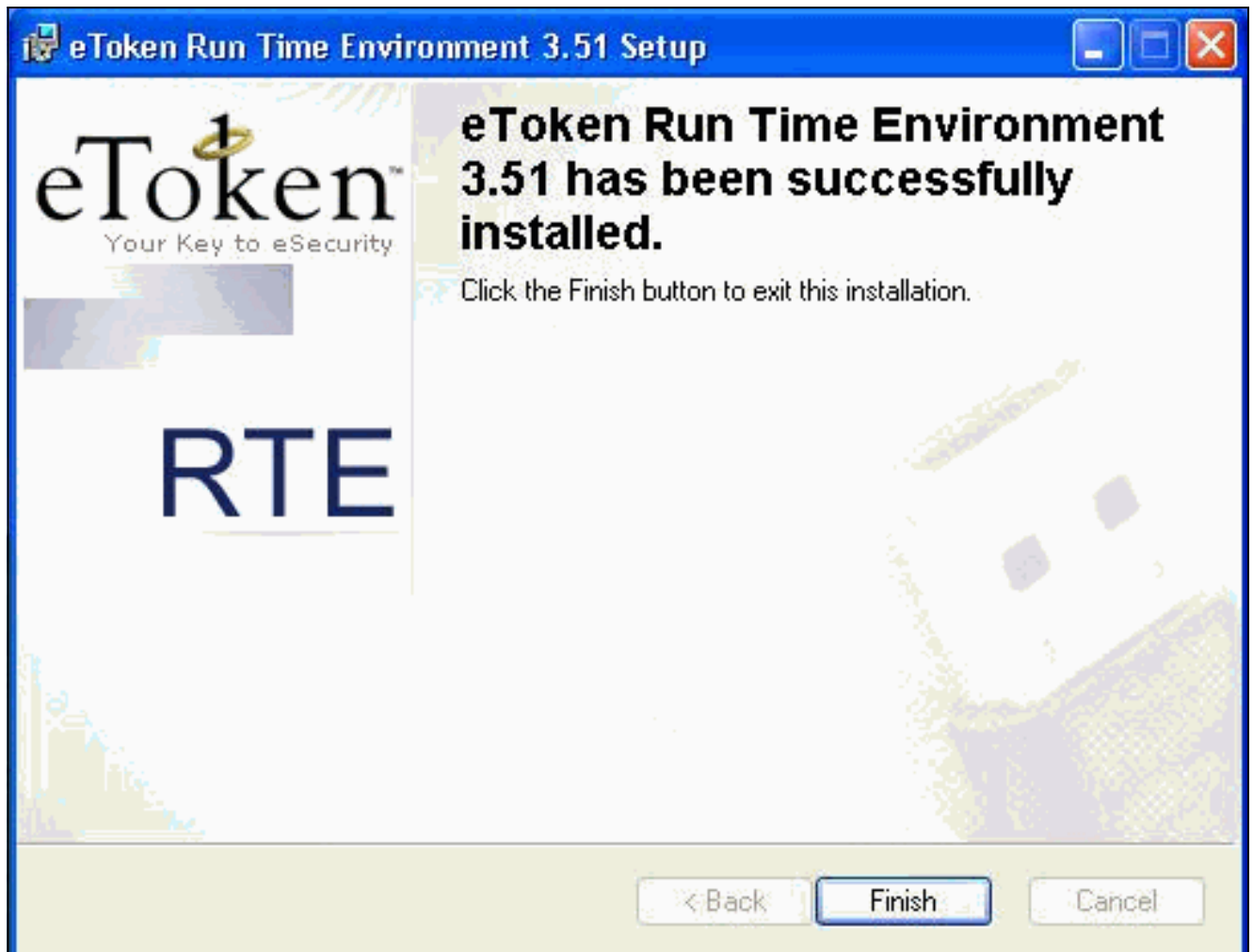
2. Acepte los términos del acuerdo de licencia y haga clic en **Next**.



3. Haga clic en **Install**.



4. Los controladores eToken Smartcard están instalados. Haga clic en **Finalizar** para salir del asistente de configuración.



Verificación

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto isakmp sa:** muestra todas las asociaciones de seguridad (SA) de Internet Key Exchange (IKE) actuales en un 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

- **show crypto ipsec sa:** muestra la configuración utilizada por las asociaciones de seguridad actuales.

```
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](#)

Refiérase a [Troubleshooting de PIX para Pasar el Tráfico de Datos en un Túnel IPSec Establecido](#) para obtener más información sobre la solución de problemas de esta configuración.

[Información Relacionada](#)

- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Página de Soporte de IPSec \(IP Security Protocol\)](#)
- [Página de soporte para cliente Cisco VPN](#)
- [Página de soporte técnico de Firewalls PIX serie 500](#)
- [Soporte Técnico - Cisco Systems](#)