IPSec entre el PIX y el Cliente Cisco VPN que usa el ejemplo de configuración de los Certificados de Smartcard

Contenido

Introducción

Este documento demuestra cómo configurar un túnel del IPSec VPN entre un firewall PIX y un Cliente Cisco VPN 4.0.x. El ejemplo de configuración en este documento también resalta el procedimiento de la inscripción del Certification Authority (CA) para el router de Cisco IOS® y el Cliente Cisco VPN, así como el uso de un Smartcard como almacenamiento del certificado.

Refiera a configurar el IPSec entre el Routers del Cisco IOS y el Cliente Cisco VPN que usa los certificados encomendados para aprender más sobre configurar el IPSec entre el Routers del Cisco IOS y el Cliente Cisco VPN que usa los certificados encomendados.

Refiera a configurar las Autoridades de certificación de múltiple identidad en el Routers del Cisco IOS para aprender más sobre configurar las Autoridades de certificación de múltiple identidad en el Routers del Cisco IOS.

prerrequisitos

Requisitos

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 funciona con la versión de software 6.3(3)
- Cliente Cisco VPN 4.0.3 en un PC que ejecuta Windows XP
- Un servidor de CA del Microsoft Windows 2000 se utiliza en este documento como el servidor de CA.
- Los Certificados en el Cliente Cisco VPN se salvan usando el e-Token Smartcard de Aladdin.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Aliste y configure el PIX

En esta sección, le presentan con la información para configurar las características descritas en este documento.

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

Configuraciones

Este documento usa estas configuraciones.

- Inscripción del certificado en el firewall PIX
- Configuración de Firewall de PIX

Inscripción del certificado en el firewall PIX

```
!--- 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
```

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)#
```

Aliste los Certificados de Cliente Cisco VPN

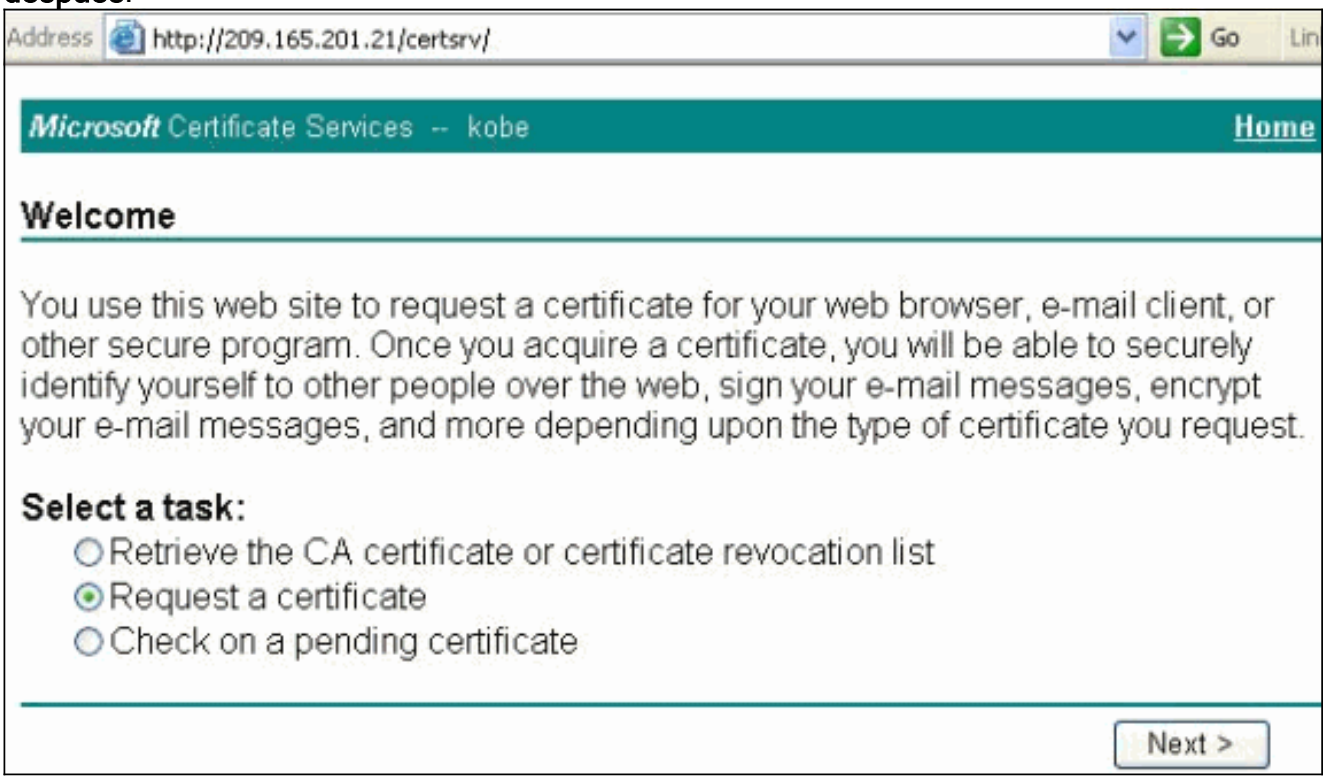
Recuerde instalar todos los driveres necesarios y utilidades que vienen con el dispositivo Smartcard en el PC que se utilizará con el Cliente Cisco VPN.

Estos pasos demuestran los procedimientos usados para alistar al Cliente Cisco VPN para los Certificados MS. El certificado se salva en el almacén del e-Token Smartcard de Aladdin.

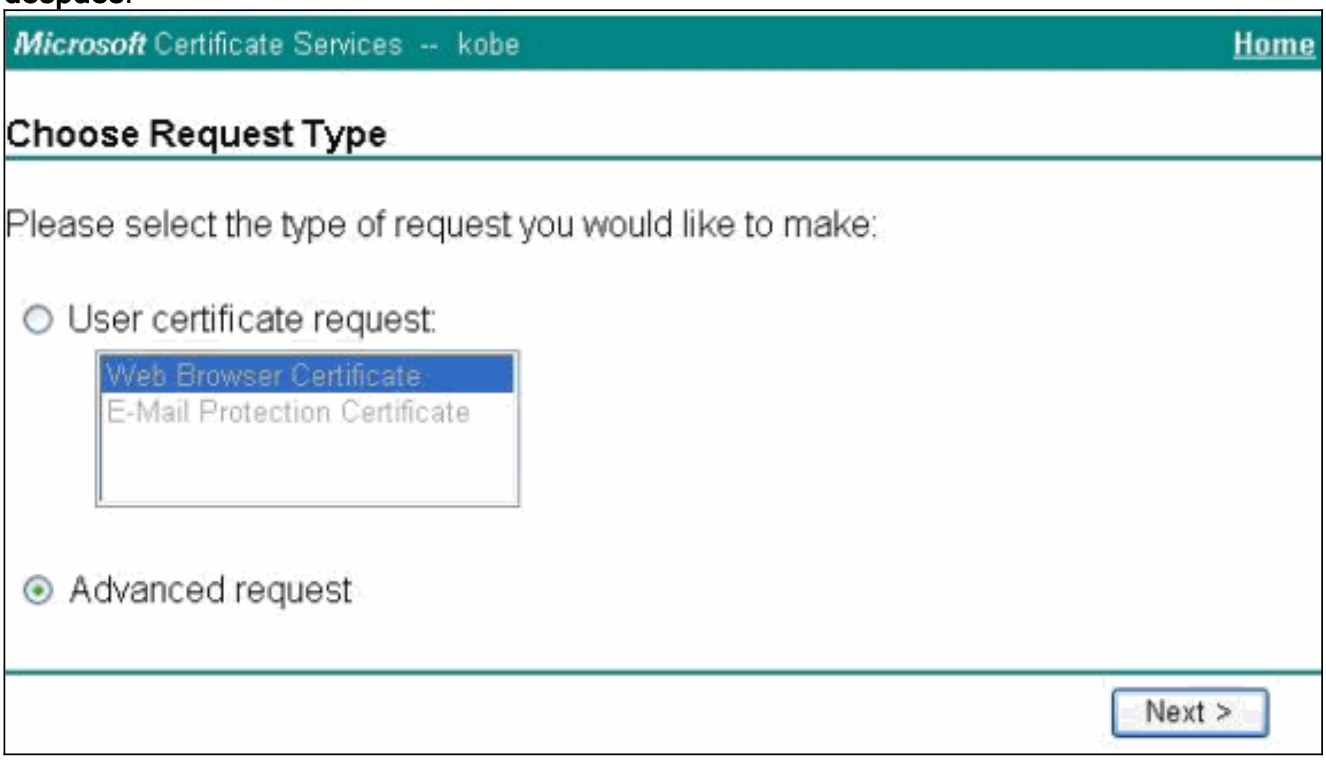
1. Ponga en marcha a un navegador y vaya a la página del servidor de certificados

(http://CAServeraddress/certsrv/, en este ejemplo).

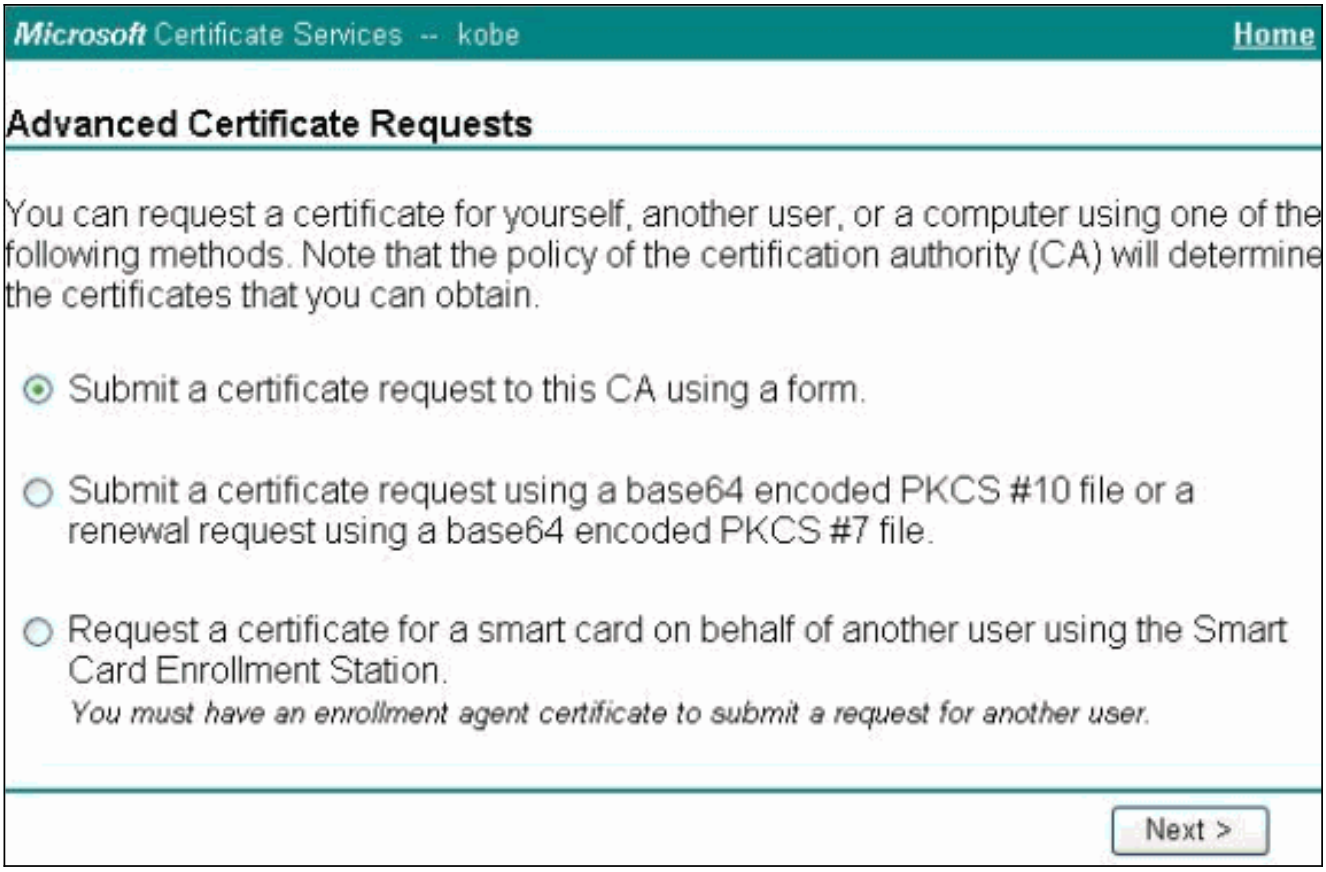
2. Seleccione la **petición un certificado** y haga clic **después**.



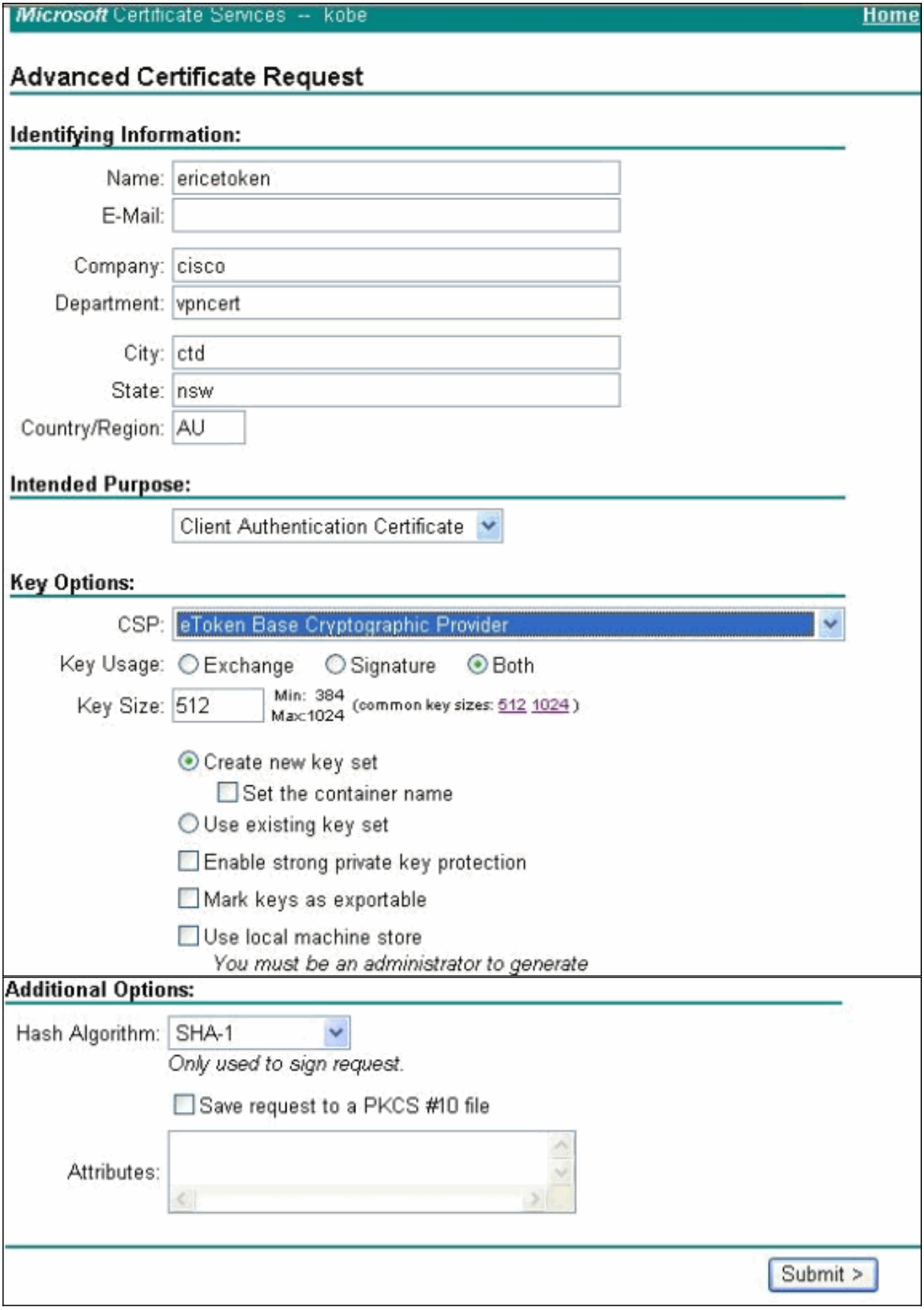
3. En la ventana del tipo de la petición del elegir, el **pedido avanzado** selecto y el tecleo **después**.



4. Selecto **presente un pedido de certificado a este CA usando una forma** y haga clic **después**.



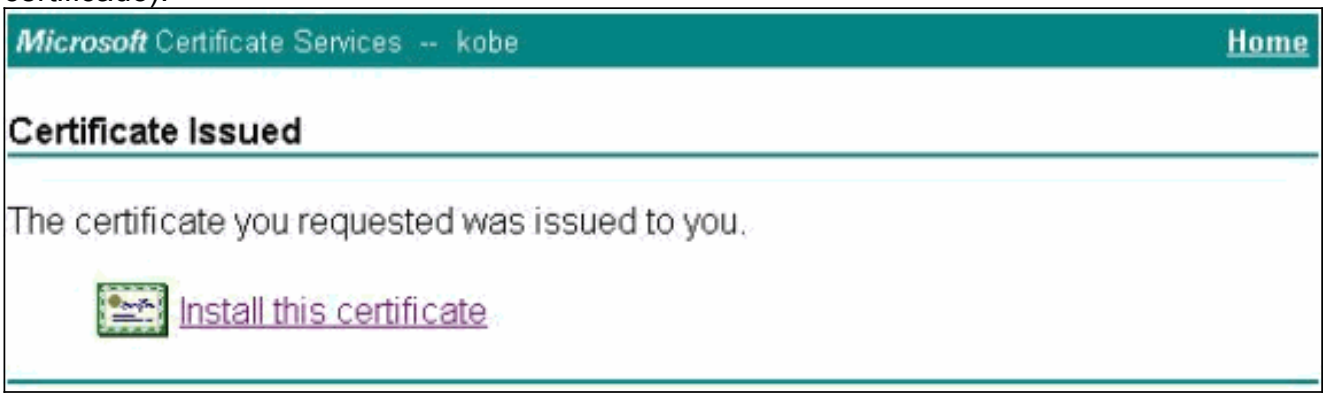
5. Complete todos los elementos en el formulario de solicitud de certificado avanzado.Esté seguro que el departamento o la unidad organizativa (OU) corresponde al nombre del grupo del Cliente Cisco VPN, como está configurado en el nombre del vpngroup PIX. Seleccione el Certificate Service Provider correcto (CSP) se apropian para su configuración.



6. Seleccione **sí** para continuar la instalación cuando usted consigue la advertencia potencial de la validación del
scripting.

7. La inscripción del certificado invoca el almacén del eToken. Ingrese la contraseña y haga clic la **AUTORIZACIÓN**.

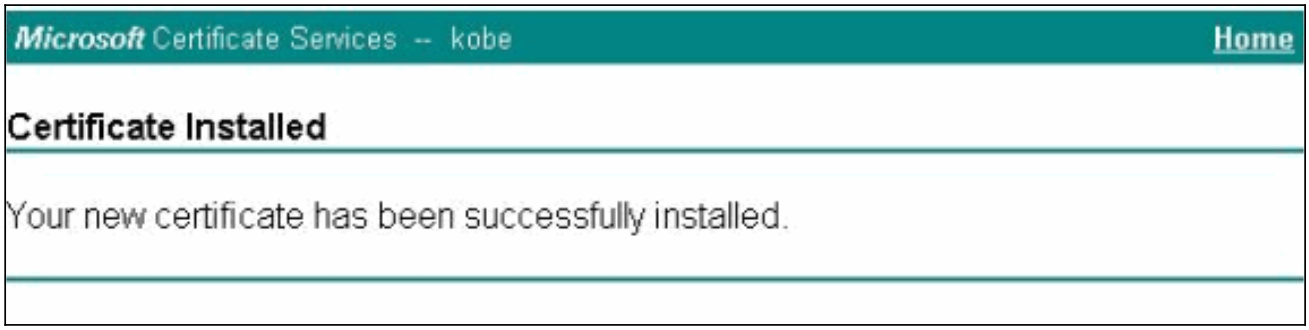
8. Haga clic en Install this certificate (Instalar este certificado).



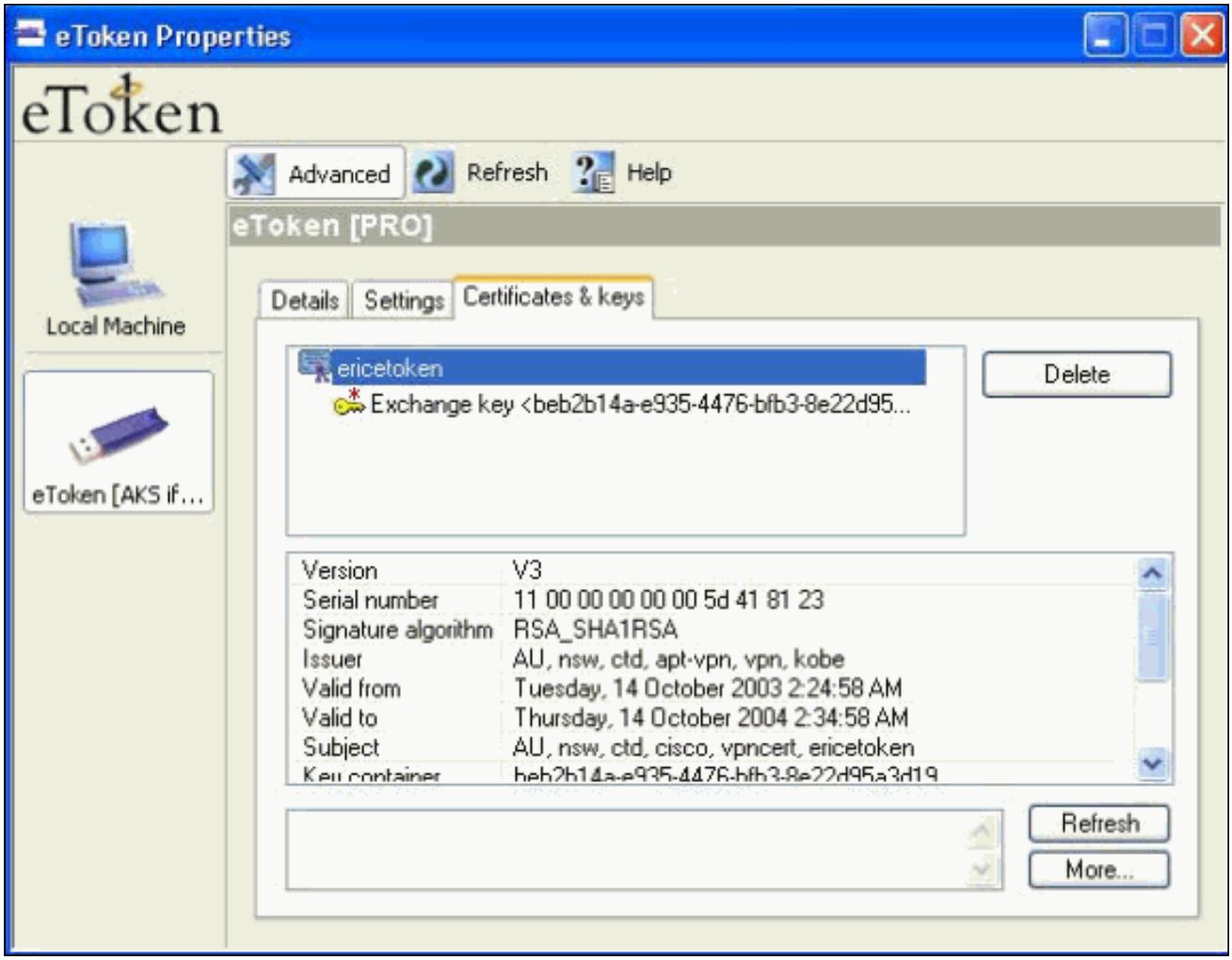
9. Seleccione **sí** para continuar la instalación cuando usted consigue la advertencia potencial de la validación del scripting.

10. Seleccione **sí** para agregar el certificado raíz al Almacén raíz.

11. La ventana instalada certificado aparece y confirma la instalación exitosa.



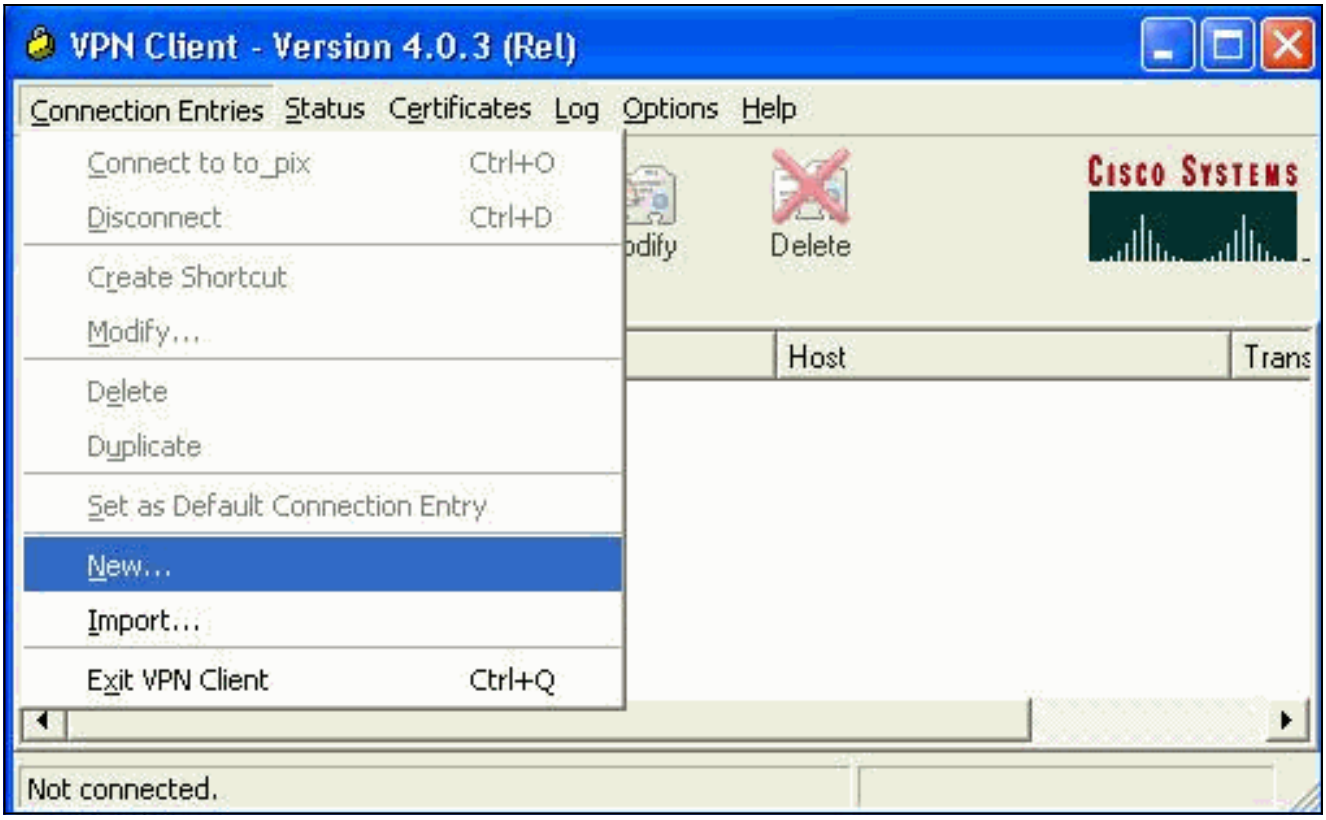
12. Utilice el visor de la aplicación eToken para ver el certificado salvado en el Smartcard.



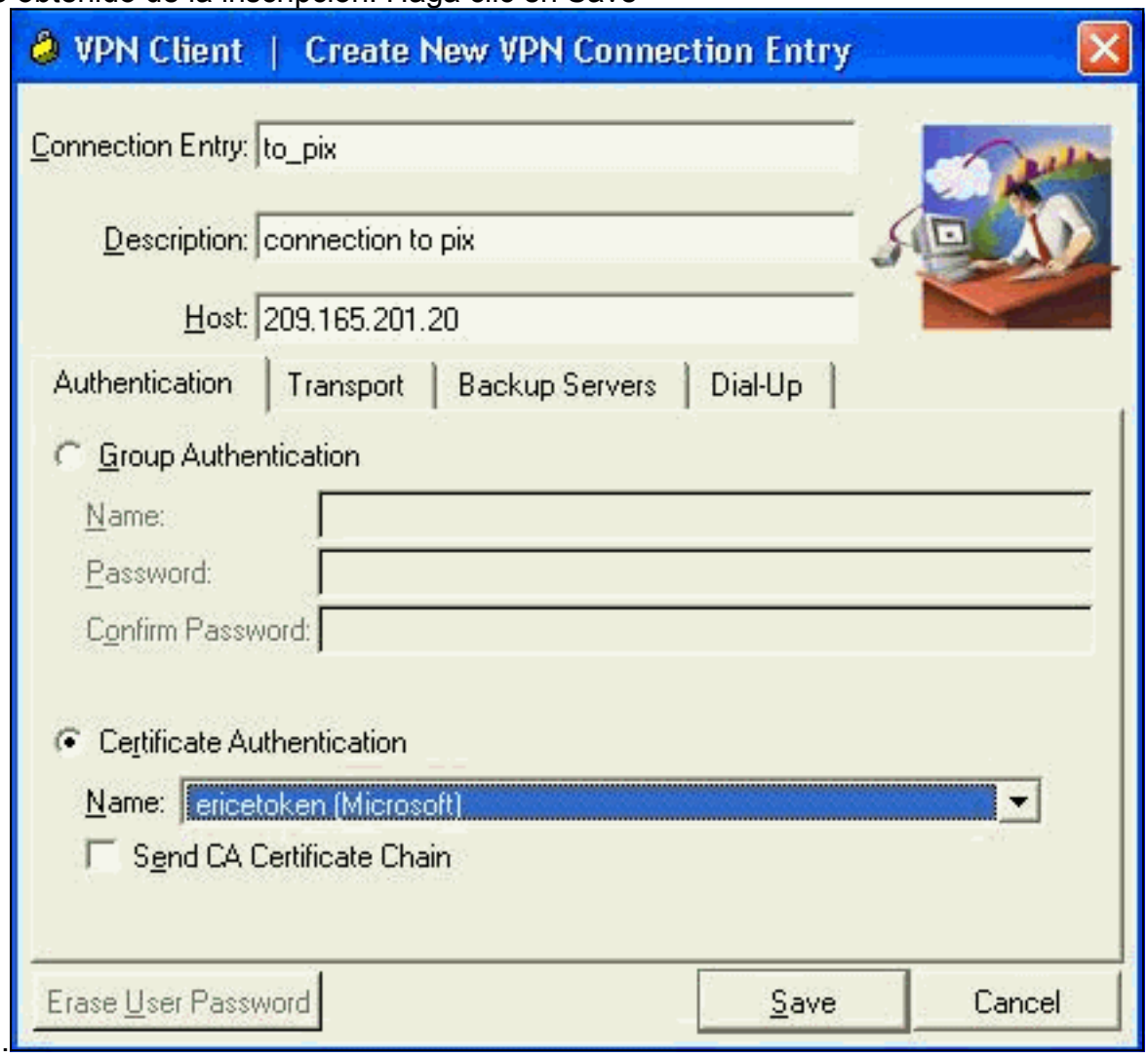
Configure al Cliente Cisco VPN para utilizar el certificado para la conexión al PIX

Estos pasos demuestran los procedimientos usados para configurar al Cliente Cisco VPN para utilizar el certificado para las conexiones PIX.

1. Inicie al Cliente Cisco VPN. Bajo conexión las entradas hacen clic **nuevo** para crear una nueva
   conexión.



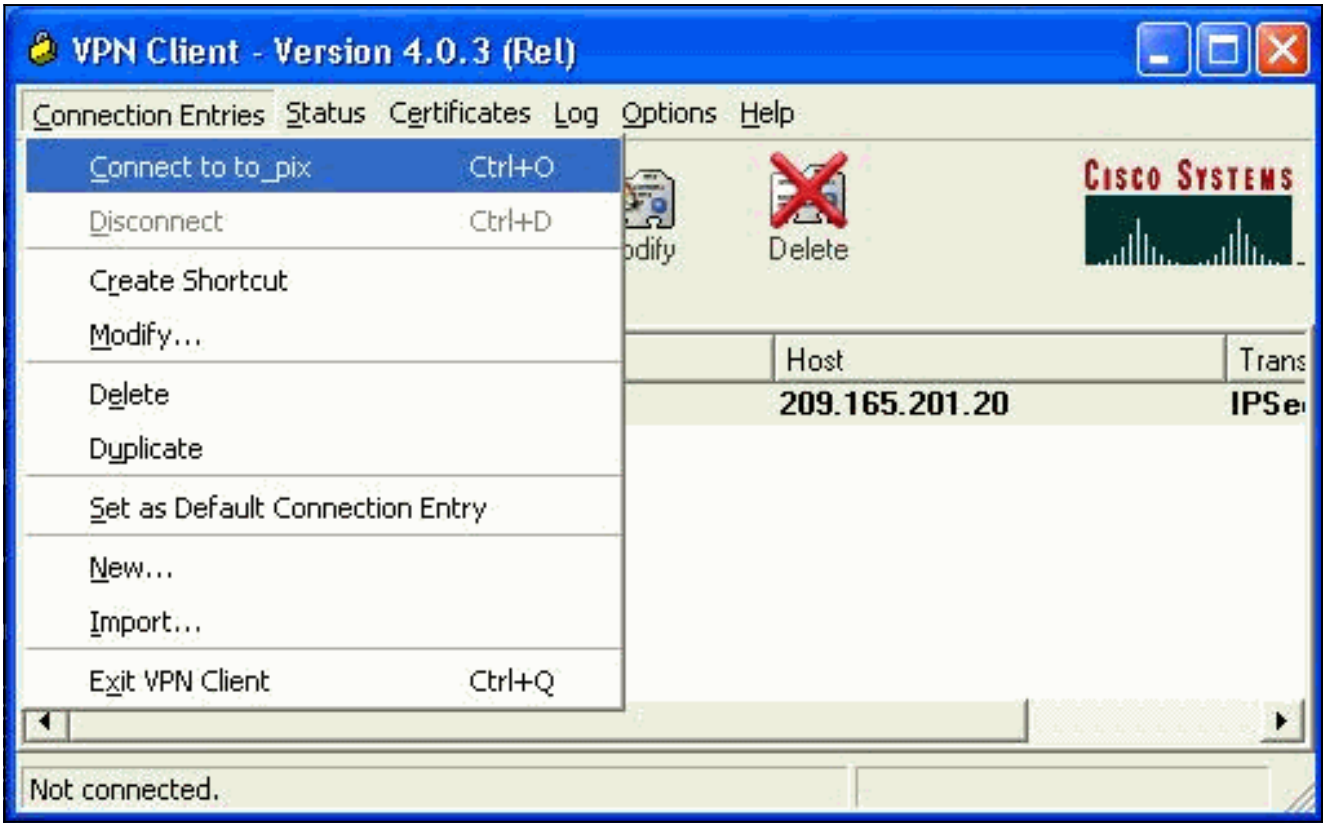
2. Complete el detalle de la conexión, especifique la autenticación certificada, seleccione el certificado obtenido de la inscripción. Haga clic en Save



(Guardar).

3. Para comenzar la conexión del Cliente Cisco VPN al PIX, seleccionar deseado Entrada de

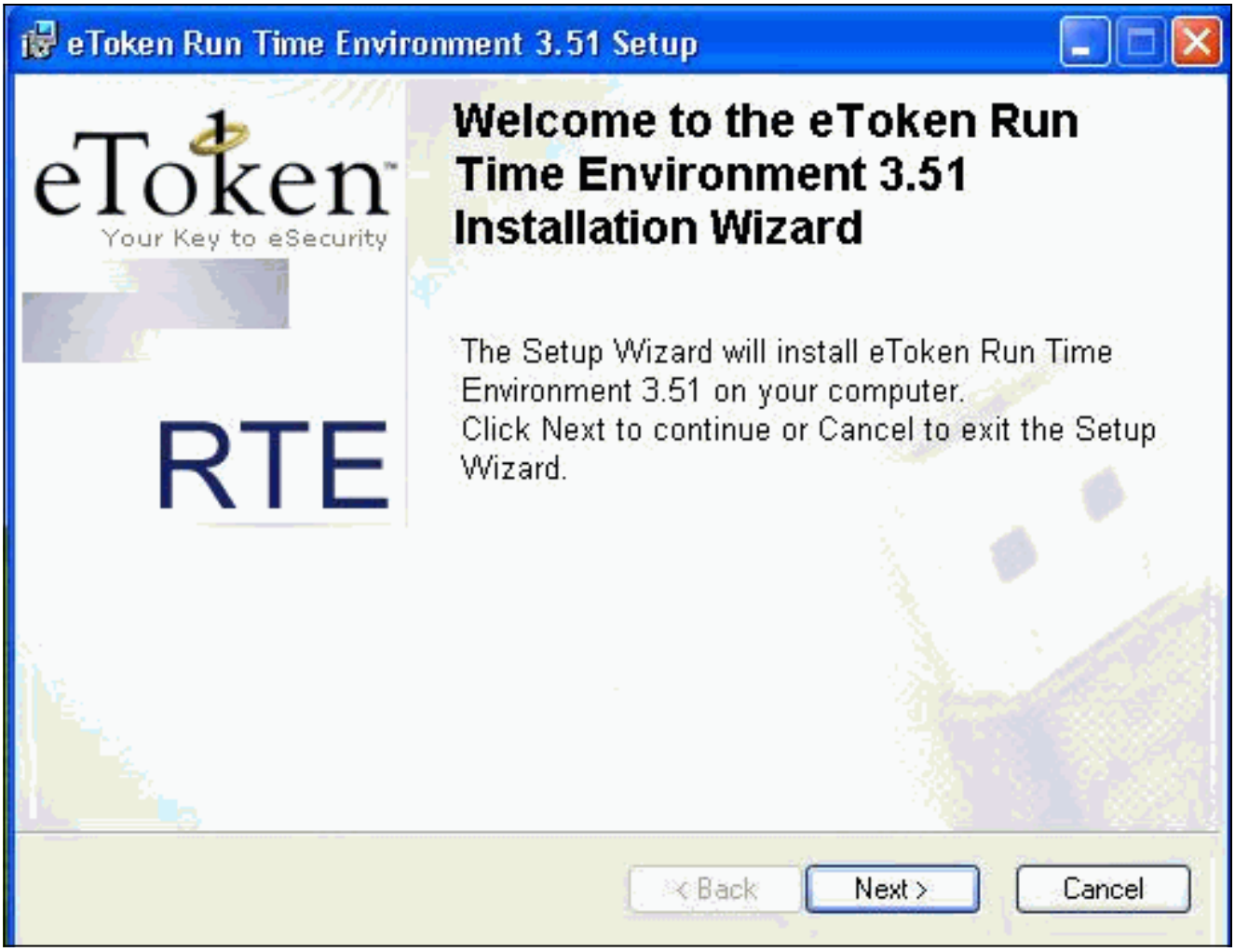
conexión y el tecleo
conecta.



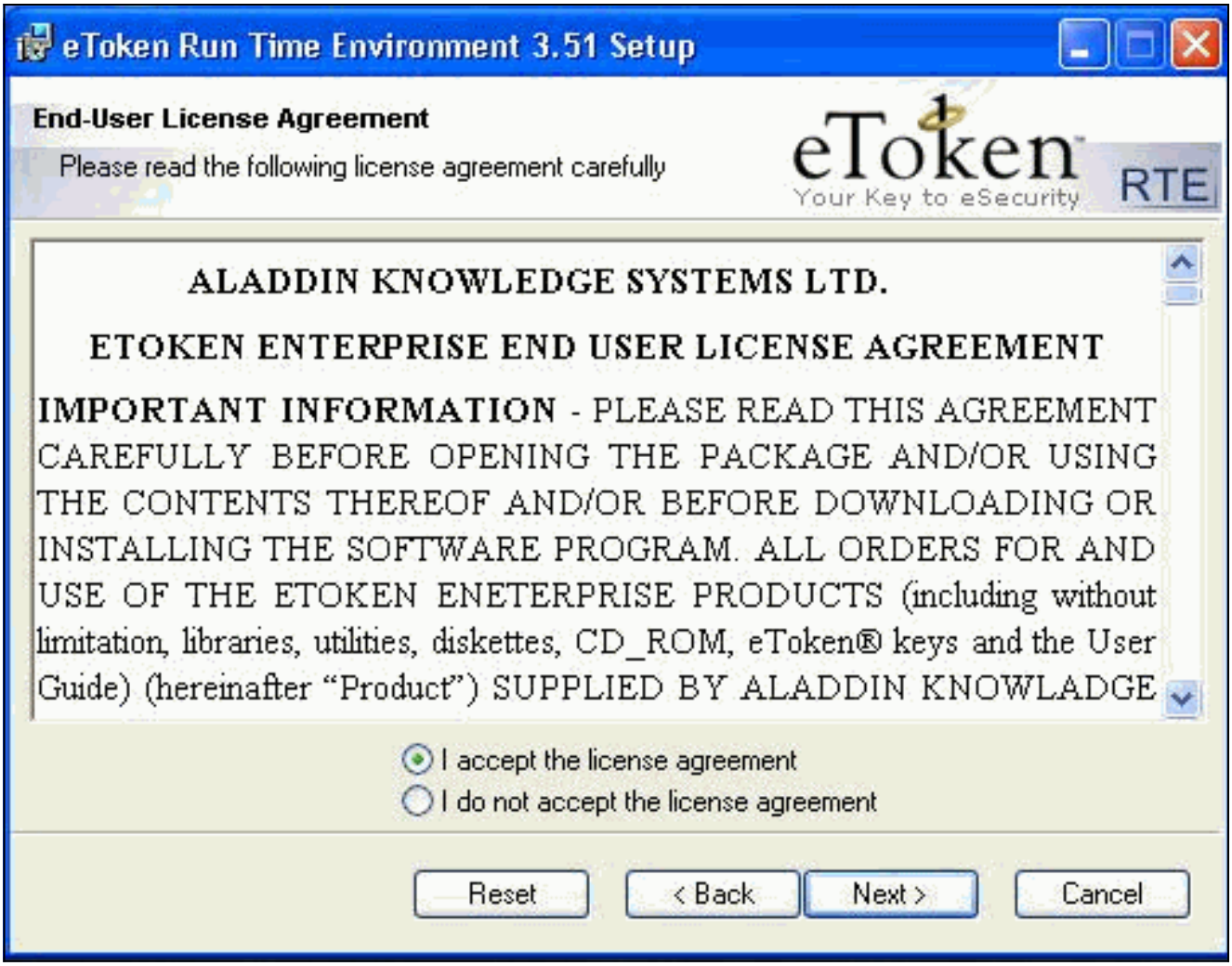
Instale los driveres Smartcard eToken

Estos pasos demuestran la instalación de los driveres Aladdin eToken Smartcard .

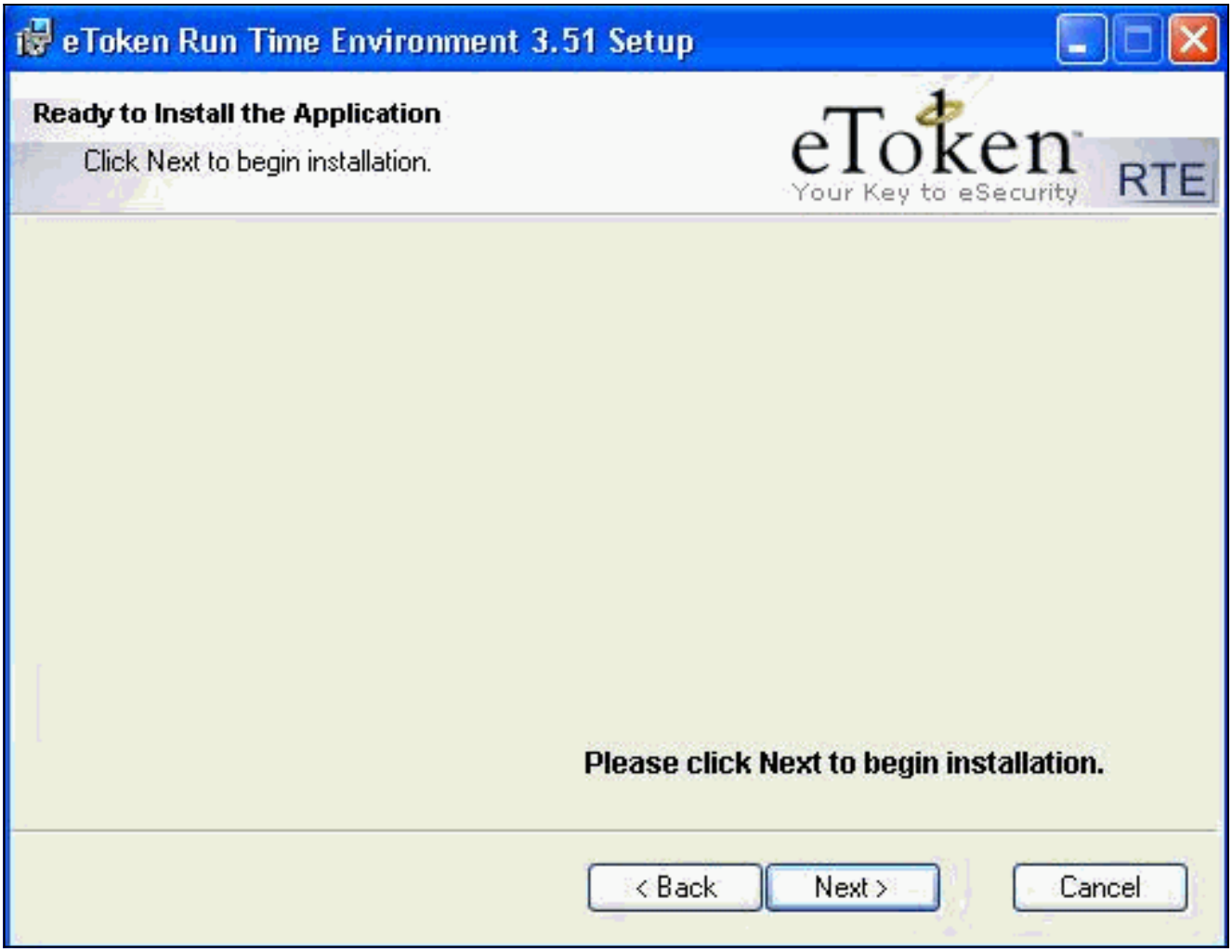
1. Abra al asistente para la configuración del entorno de tiempo de ejecución 3.51 del eToken.



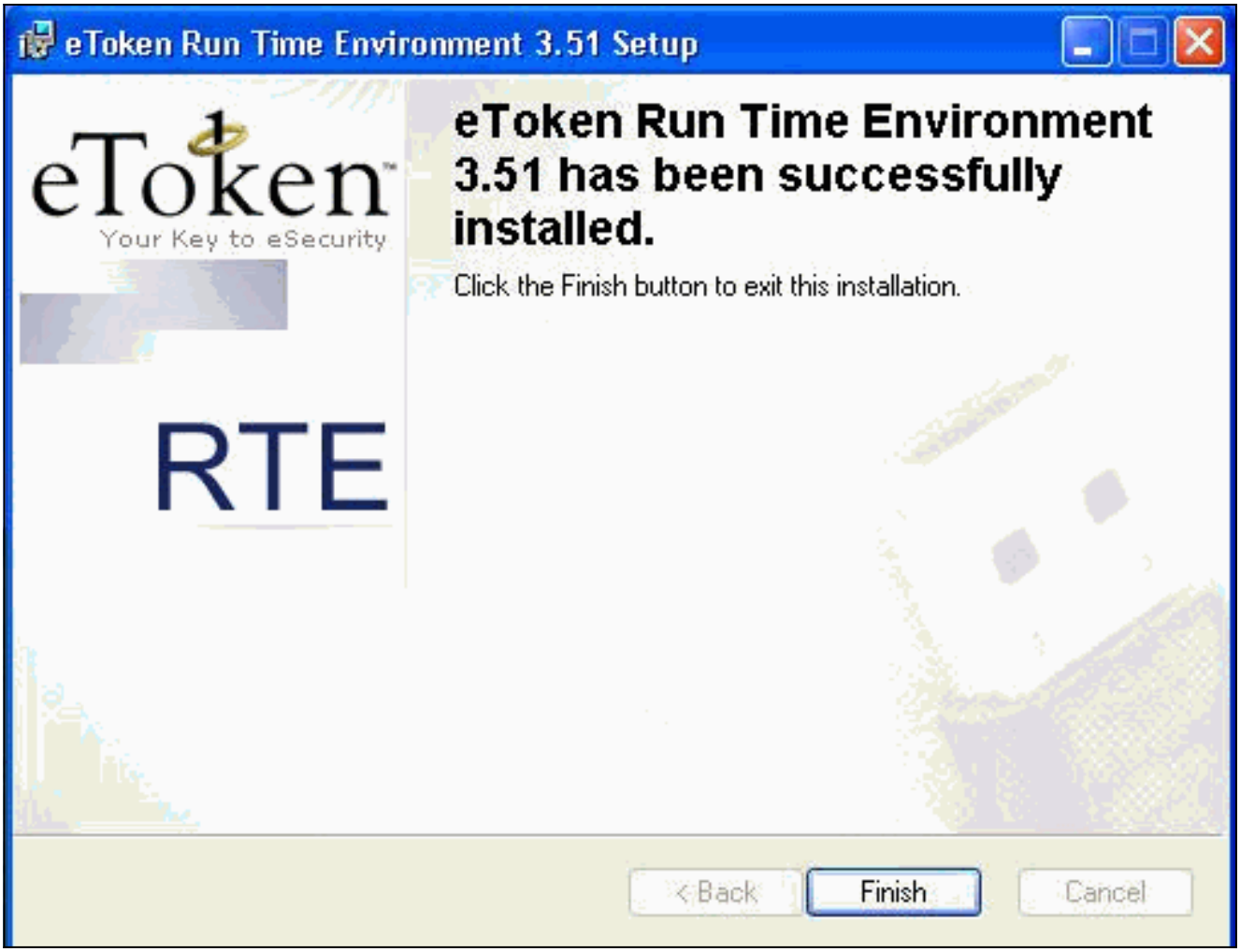
2. Valide los términos del acuerdo de licencia y haga clic **después**.



3. El tecleo **instala**.



4. Los driveres Smartcard eToken ahora están instalados. Clic en Finalizar para salir al asistente para la
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.

- **muestre isakmp crypto sa** — Visualiza todas las asociaciones de seguridad actuales del Internet Key Exchange (IKE) (SA) 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
```

- **muestre IPSec crypto sa** — Visualiza las configuraciones usadas por las asociaciones de seguridad vigente.`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

Refiera a resolver problemas el PIX para pasar el tráfico de datos en un túnel de IPSec establecido para más información sobre resolver problemas esta configuración.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Página de Soporte de IPSec (Protocolo de Seguridad IP)
- Página de soporte para cliente Cisco VPN
- Página de soporte de los PIX 500 Series Firewall
- Soporte Técnico - Cisco Systems