

Konfigurationsbeispiel für IPSec zwischen PIX und Cisco VPN Client mithilfe von Smartcard-Zertifikaten

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Registrieren und Konfigurieren des PIX](#)

[Konfigurationen](#)

[Registrieren von Cisco VPN Client-Zertifikaten](#)

[Konfigurieren Sie den Cisco VPN-Client, um das Zertifikat für die Verbindung zum PIX zu verwenden.](#)

[eToken Smartcard-Treiber installieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument zeigt, wie ein IPSec-VPN-Tunnel zwischen einer PIX-Firewall und einem Cisco VPN-Client 4.0.x konfiguriert wird. Im Konfigurationsbeispiel in diesem Dokument wird auch das Anmeldeverfahren der Zertifizierungsstelle (CA) für den Cisco IOS® Router und den Cisco VPN Client sowie die Verwendung einer Smartcard als Zertifikatsspeicher hervorgehoben.

Unter [Konfigurieren von IPSec zwischen Cisco IOS-Routern und dem Cisco VPN-Client mithilfe von Vertrauenszertifikaten](#) finden Sie weitere Informationen zur Konfiguration von IPSec zwischen Cisco IOS-Routern und dem Cisco VPN-Client mithilfe von Vertrauenszertifikaten.

Unter [Konfigurieren von Zertifizierungsstellen für mehrere Identitäten auf Cisco IOS-Routern](#) finden Sie weitere Informationen zum Konfigurieren von Zertifizierungsstellen für mehrere Identitäten auf Cisco IOS-Routern.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco PIX Firewall mit Softwareversion 6.3(3)
- Cisco VPN Client 4.0.3 auf einem PC mit Windows XP
- Ein CA-Server für Microsoft Windows 2000 wird in diesem Dokument als CA-Server verwendet.
- Zertifikate auf dem Cisco VPN Client werden mit der [Aladdin](#) e-Token Smartcard gespeichert.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

Registrieren und Konfigurieren des PIX

In diesem Abschnitt werden die Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen angezeigt.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- [Zertifikatsregistrierung für PIX-Firewall](#)
- [PIX-Firewall-Konfiguration](#)

Zertifikatsregistrierung für 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
```

PIX-Firewall-Konfiguration

```
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)#

```

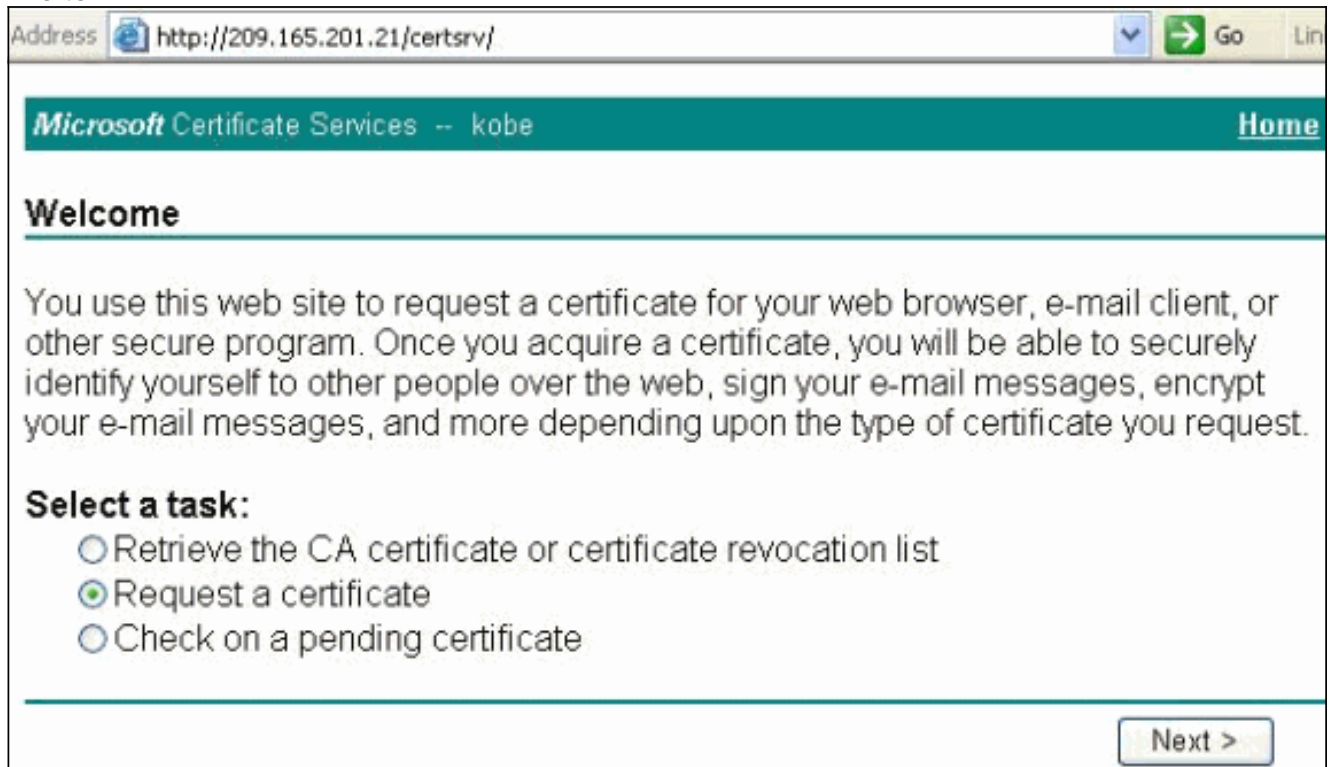
[Registrieren von Cisco VPN Client-Zertifikaten](#)

Denken Sie daran, alle notwendigen Treiber und Dienstprogramme zu installieren, die mit dem

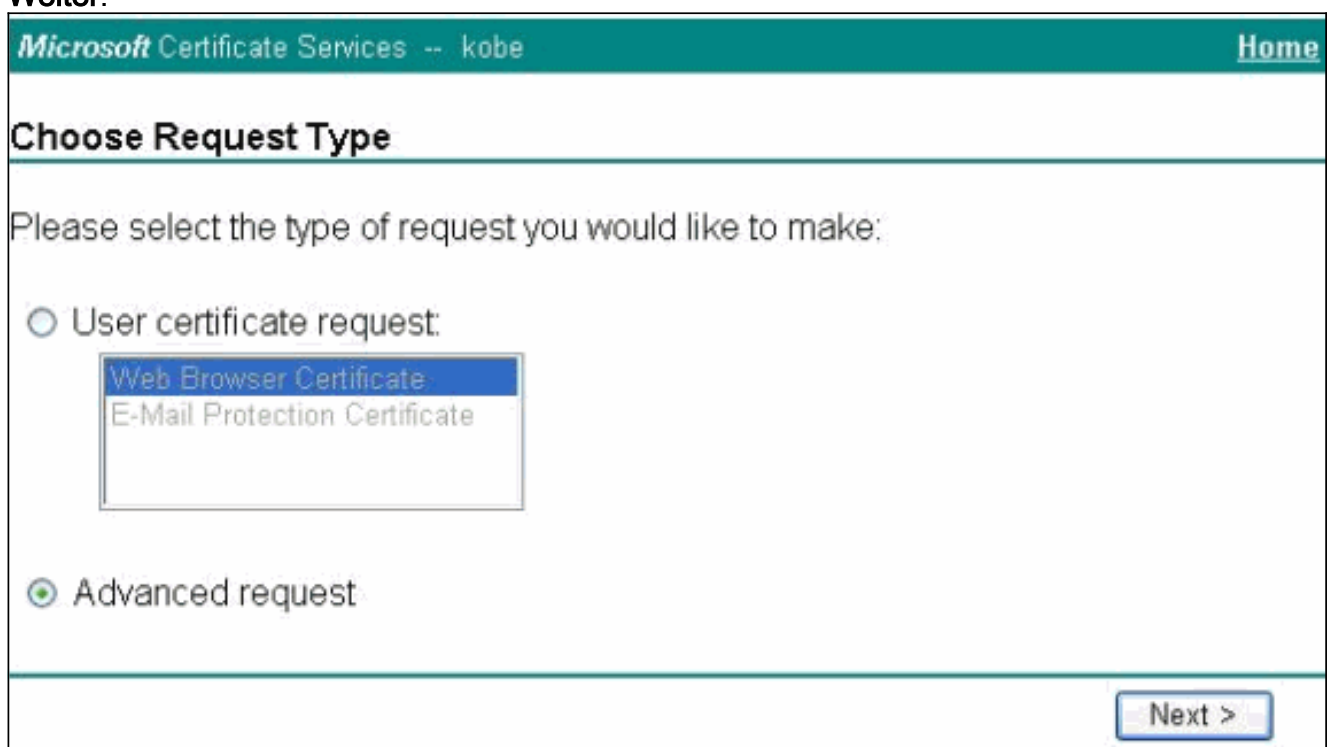
Smartcard-Gerät auf dem PC für die Verwendung mit dem Cisco VPN-Client ausgeliefert werden.

In diesen Schritten werden die Verfahren zur Registrierung des Cisco VPN Client für MS-Zertifikate veranschaulicht. Das Zertifikat wird im [Aladdin](#) e-Token Smartcard Store gespeichert.

1. Starten Sie einen Browser, und wechseln Sie zur Zertifikatserversseite (in diesem Beispiel <http://CAServeraddress/certsrv/>).
2. Wählen Sie **Zertifikat anfordern aus**, und klicken Sie auf **Weiter**.



3. Wählen Sie im Fenster Anfragetyp auswählen die Option **Erweiterte Anforderung aus**, und klicken Sie auf **Weiter**.



4. Wählen Sie eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus, und klicken Sie auf Weiter.

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. Füllen Sie alle Felder im Formular für erweiterte Zertifikatsanforderung aus. Stellen Sie sicher, dass die Abteilung oder Organisationseinheit (OU) dem im PIX-vpngroup-Namen konfigurierten Cisco VPN Client-Gruppenamen entspricht. Wählen Sie den für Ihre Einrichtung geeigneten Zertifikatsdiensteanbieter (Certificate Service Provider, CSP) aus.

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. Wählen Sie **Yes (Ja)** aus, um die Installation fortzusetzen, wenn Sie die Warnung zur Prüfung potenzieller Skripte erhalten.

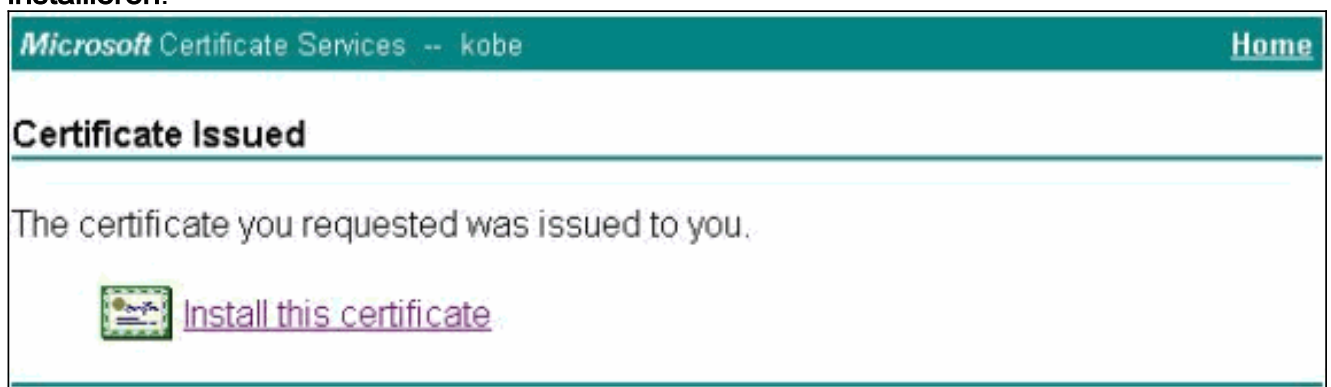


7. Die Zertifikatregistrierung ruft den eToken-Speicher auf. Geben Sie das Kennwort ein, und



klicken Sie auf **OK**.

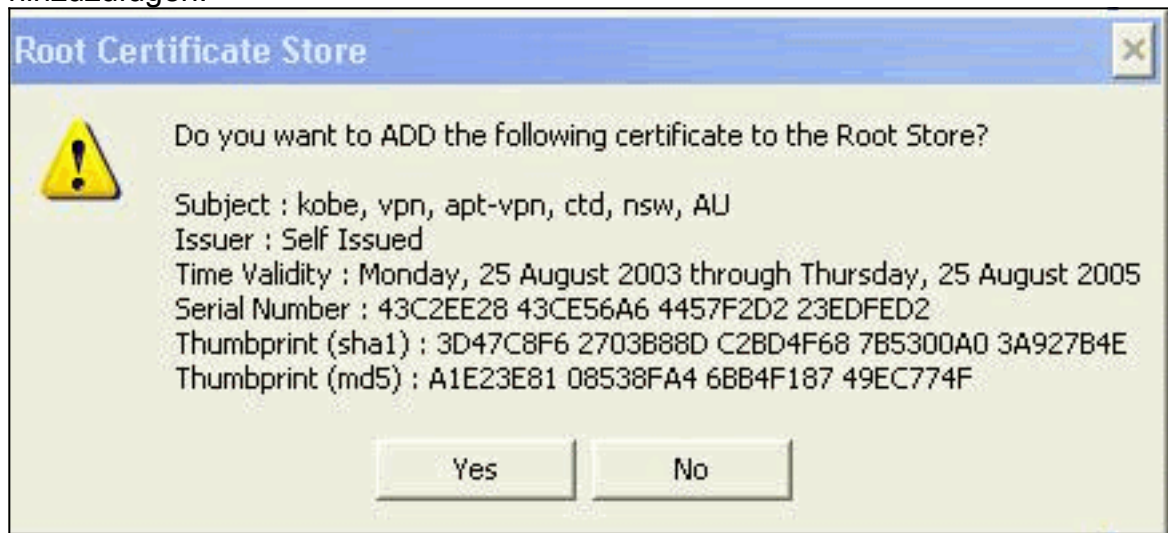
8. Klicken Sie auf **Zertifikat installieren**.



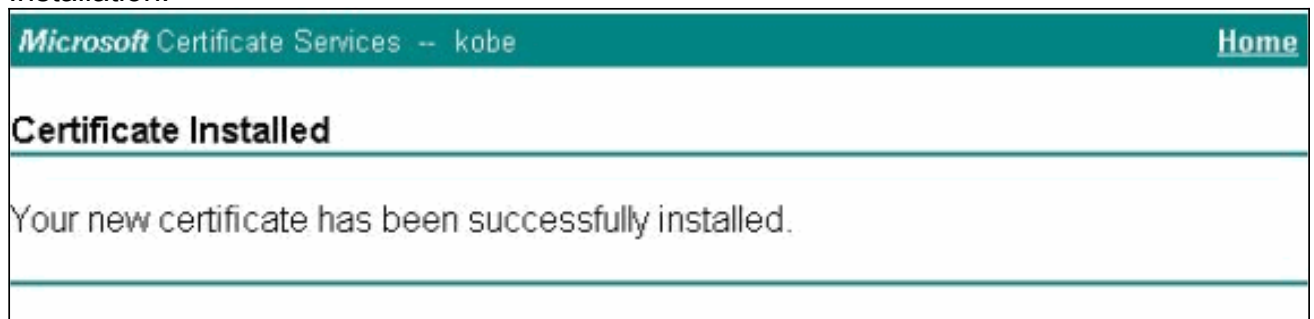
9. Wählen Sie **Yes (Ja)** aus, um die Installation fortzusetzen, wenn Sie die Warnung zur Prüfung potenzieller Skripte erhalten.



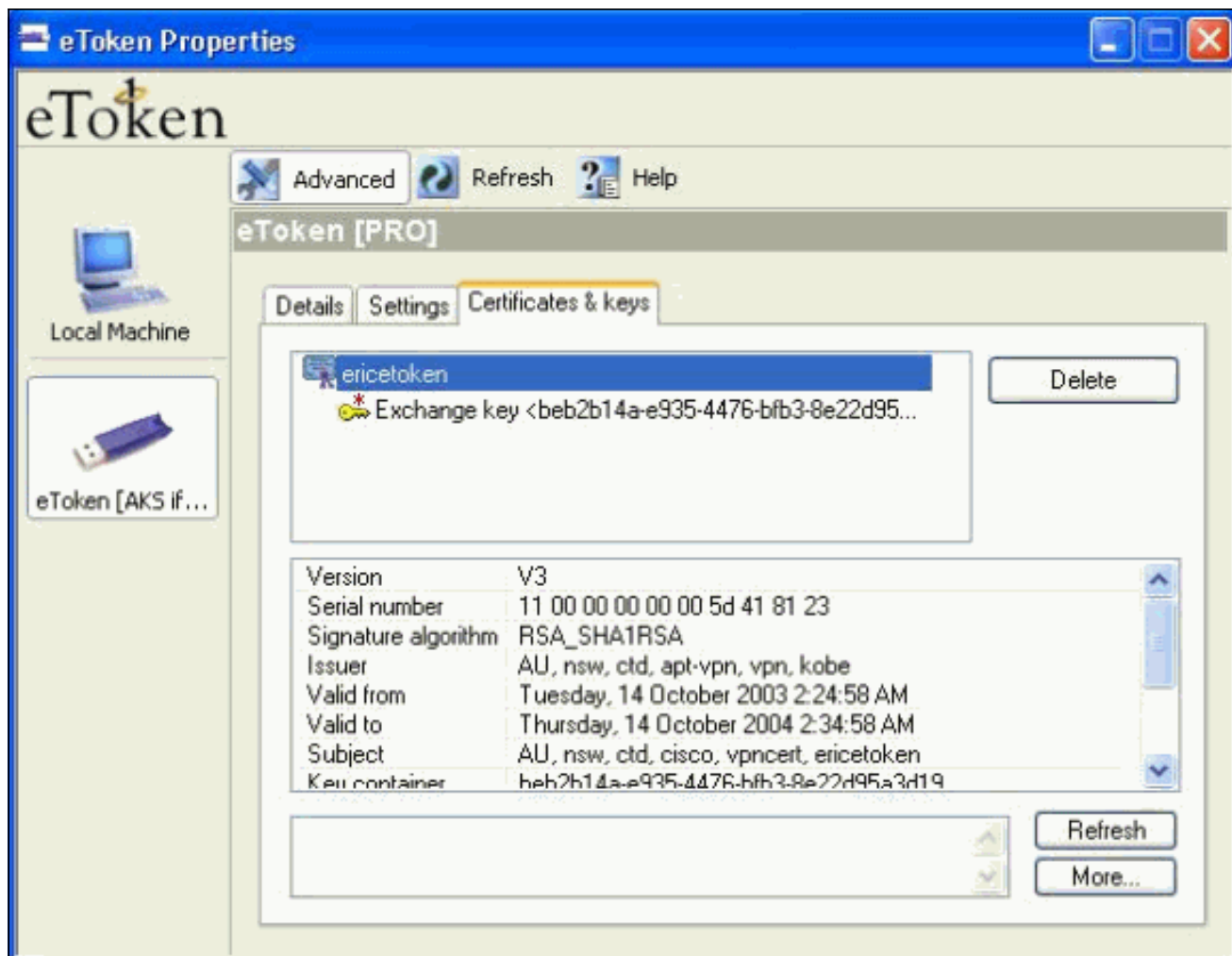
10. Wählen Sie **Yes (Ja)** aus, um das Stammzertifikat dem Root Store hinzuzufügen.



11. Das Fenster Zertifikat installiert wird angezeigt und bestätigt die erfolgreiche Installation.



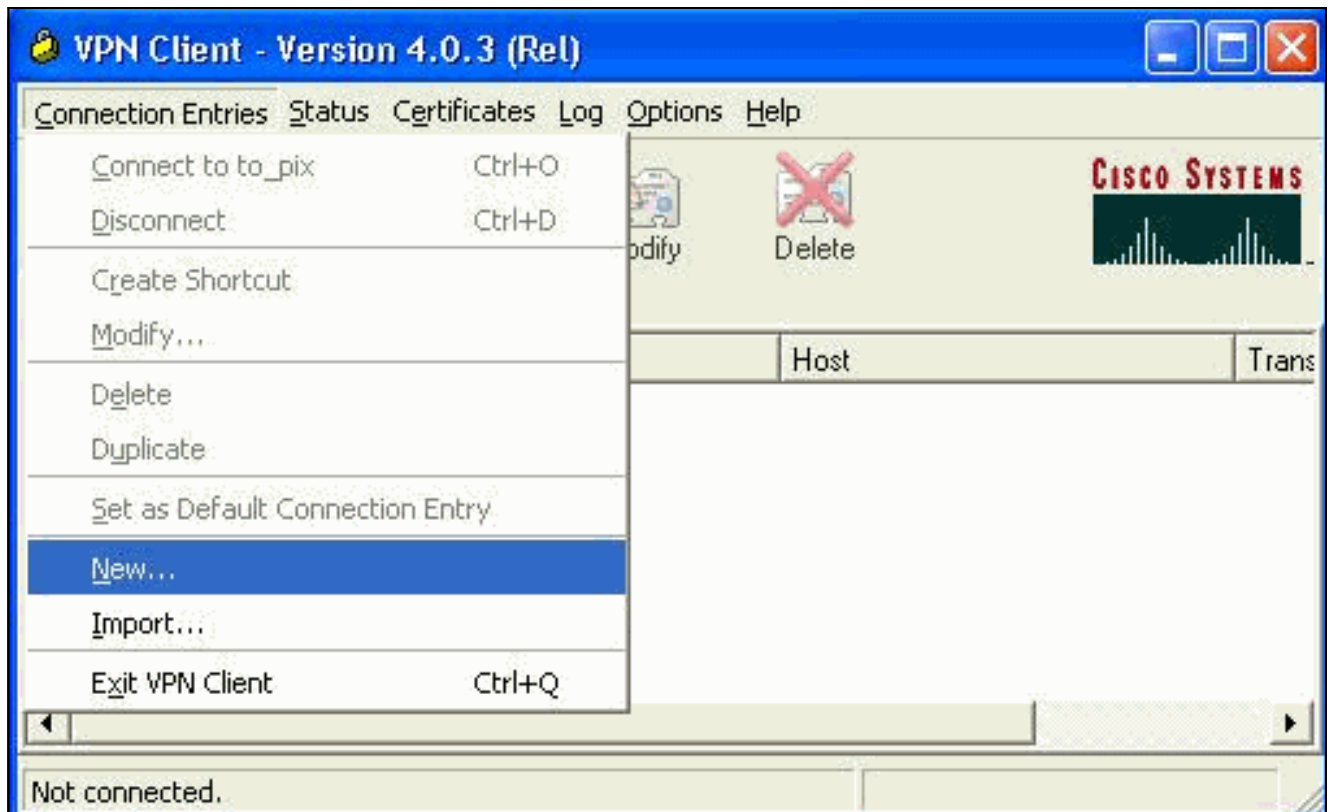
12. Verwenden Sie den eToken-Anwendungs-Viewer, um das auf der Smartcard gespeicherte Zertifikat anzuzeigen.



Konfigurieren Sie den Cisco VPN-Client, um das Zertifikat für die Verbindung zum PIX zu verwenden.

In diesen Schritten werden die Verfahren veranschaulicht, mit denen der Cisco VPN Client für die Verwendung des Zertifikats für PIX-Verbindungen konfiguriert wird.

1. Starten Sie den Cisco VPN Client. Klicken Sie unter Verbindungseinträge auf **Neu**, um eine neue Verbindung zu erstellen.



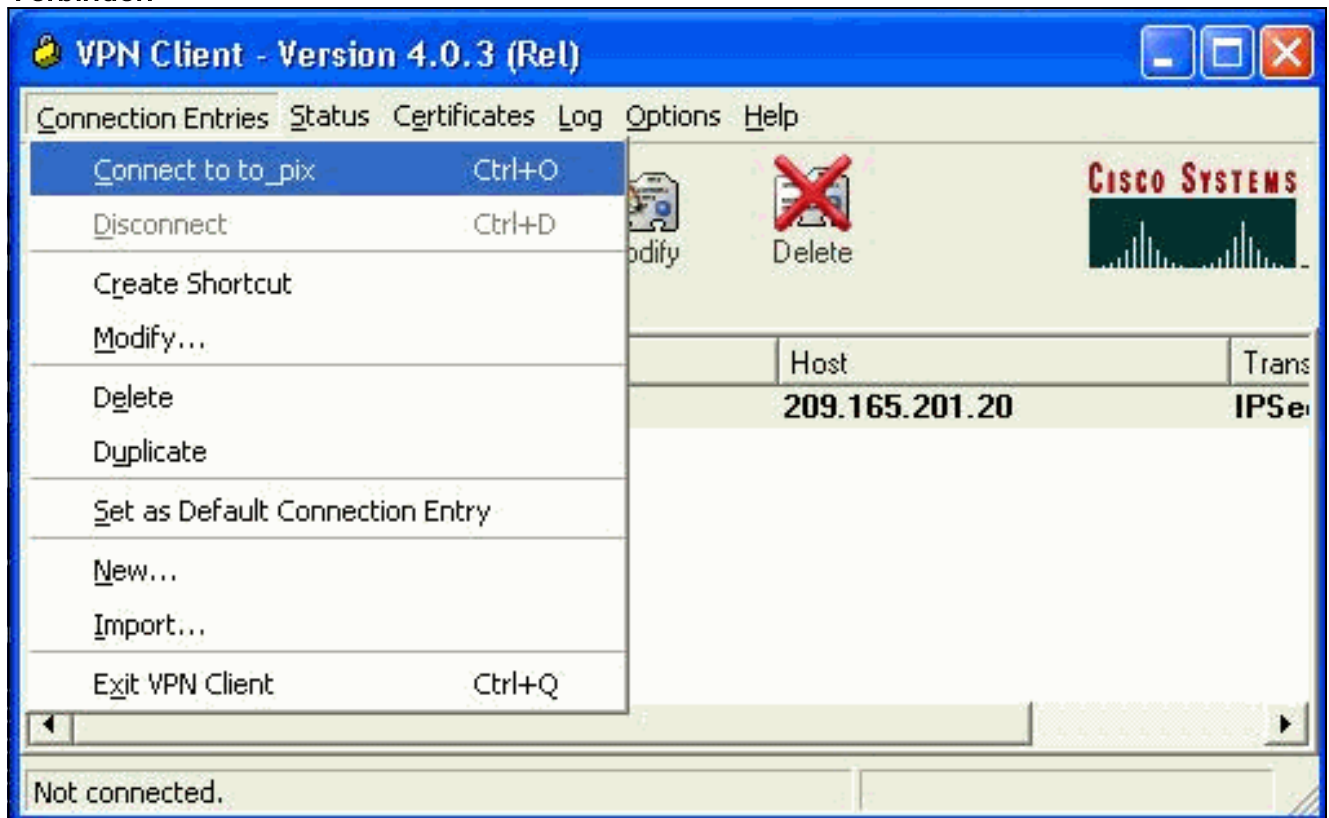
2. Füllen Sie die Verbindungsdetails aus, geben Sie die Zertifikatauthentifizierung an, und wählen Sie das Zertifikat aus, das Sie bei der Registrierung erhalten haben. Klicken Sie auf



Speichern.

3. Um die Verbindung des Cisco VPN-Clients mit dem PIX zu starten, wählen Sie den

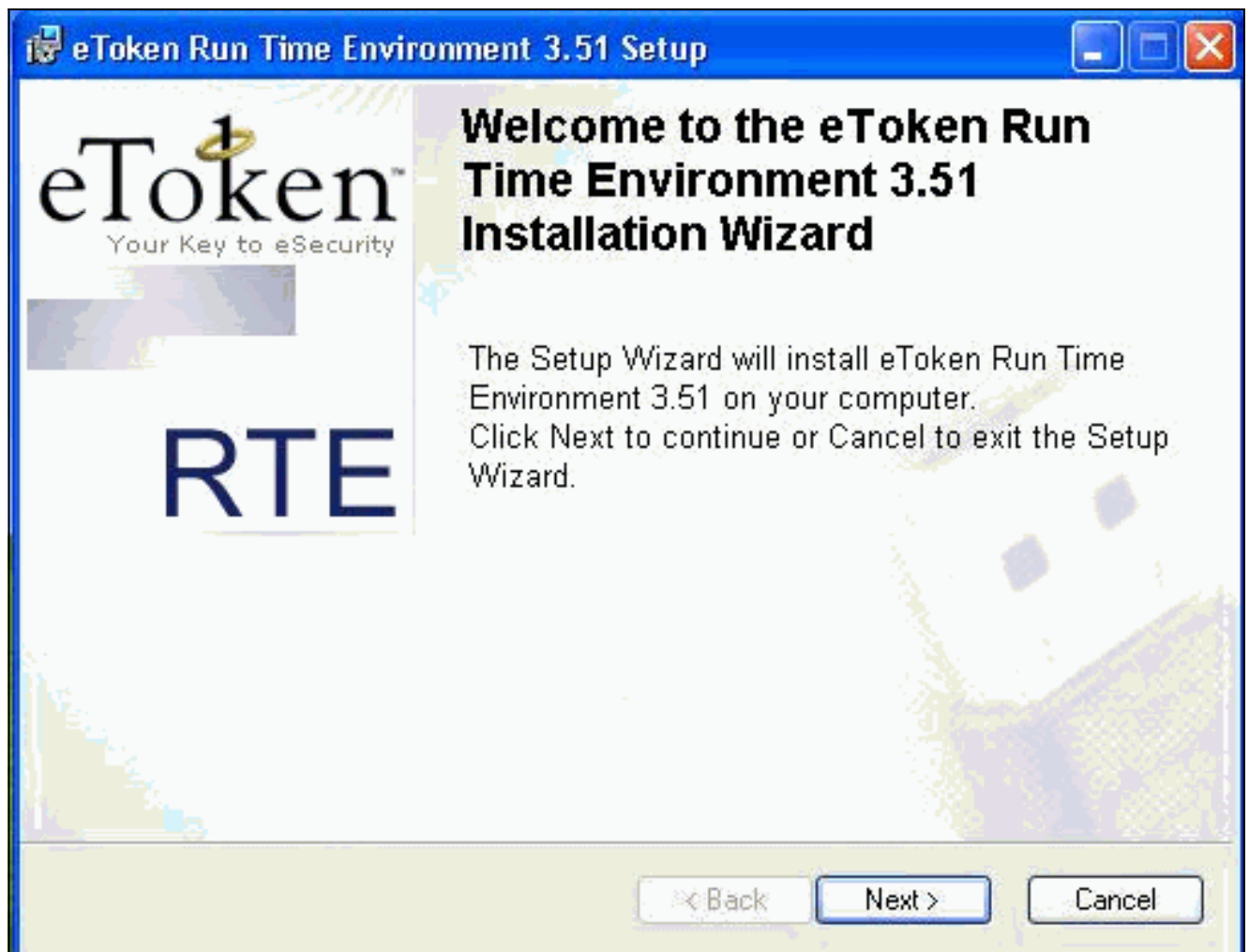
gewünschten Verbindungseintrag aus, und klicken Sie auf **Verbinden**.



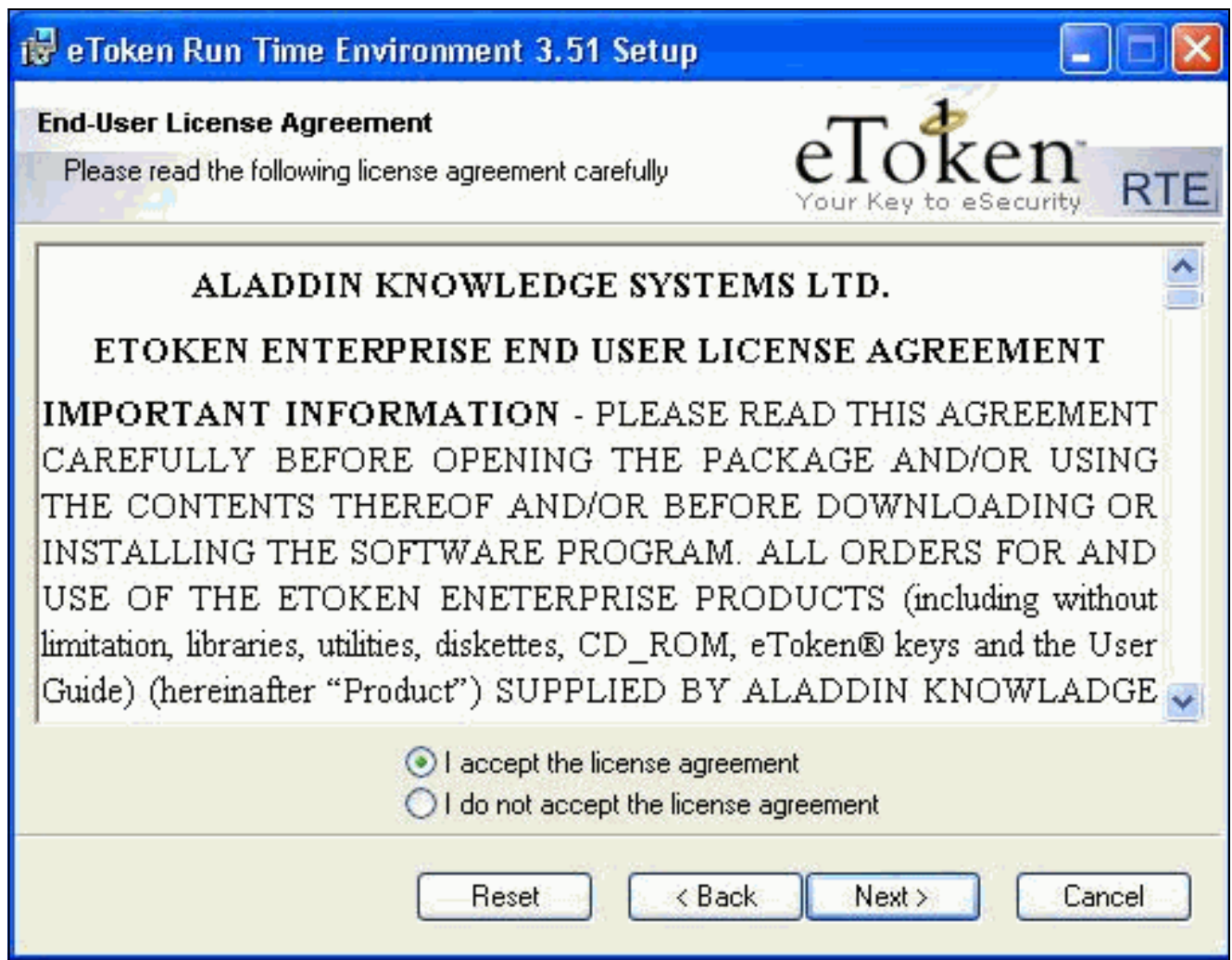
[eToken Smartcard-Treiber installieren](#)

Diese Schritte veranschaulichen die Installation der [Aladdin](#) eToken Smartcard-Treiber.

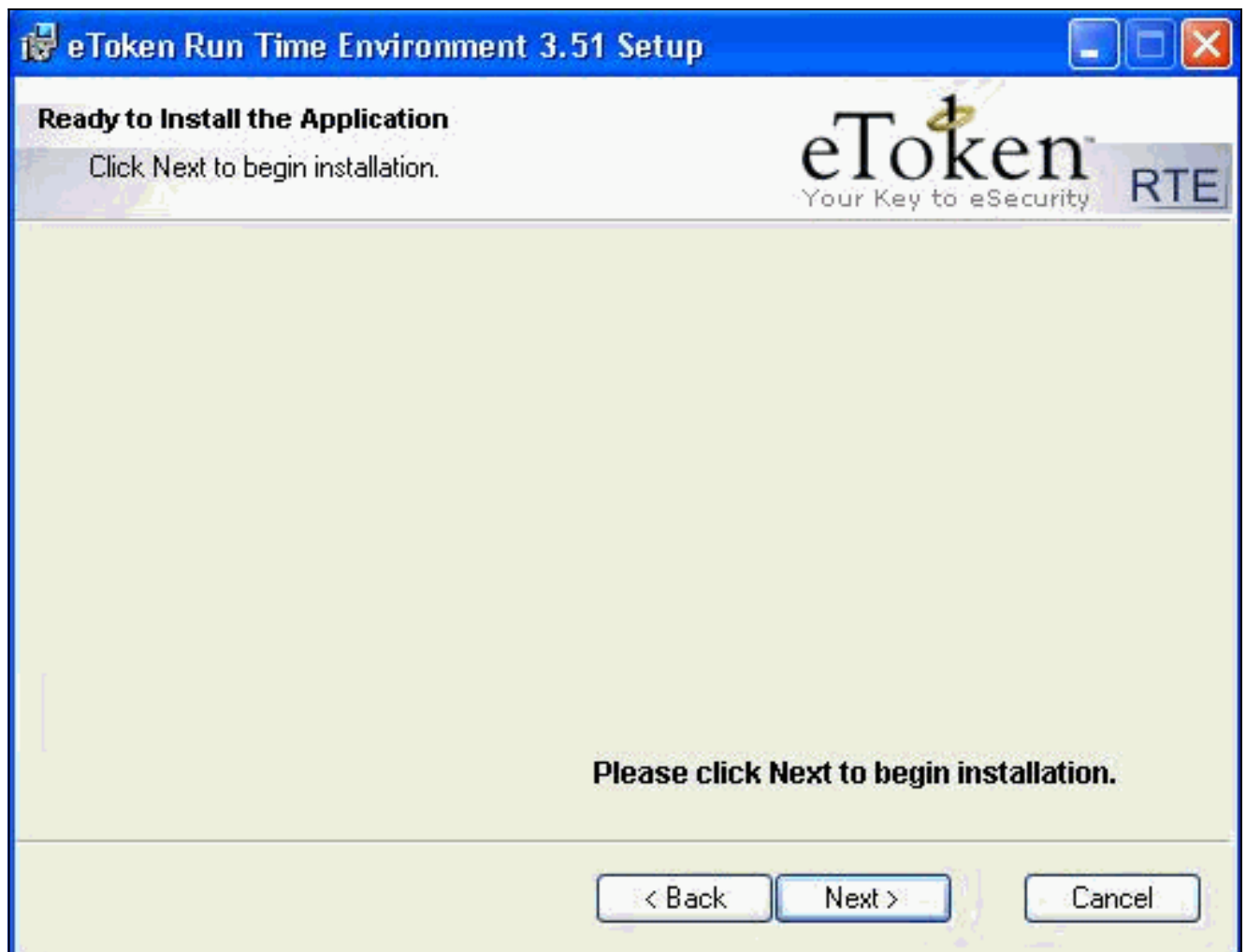
1. Öffnen Sie den eToken Run Time Environment 3.51 Setup-Assistenten.



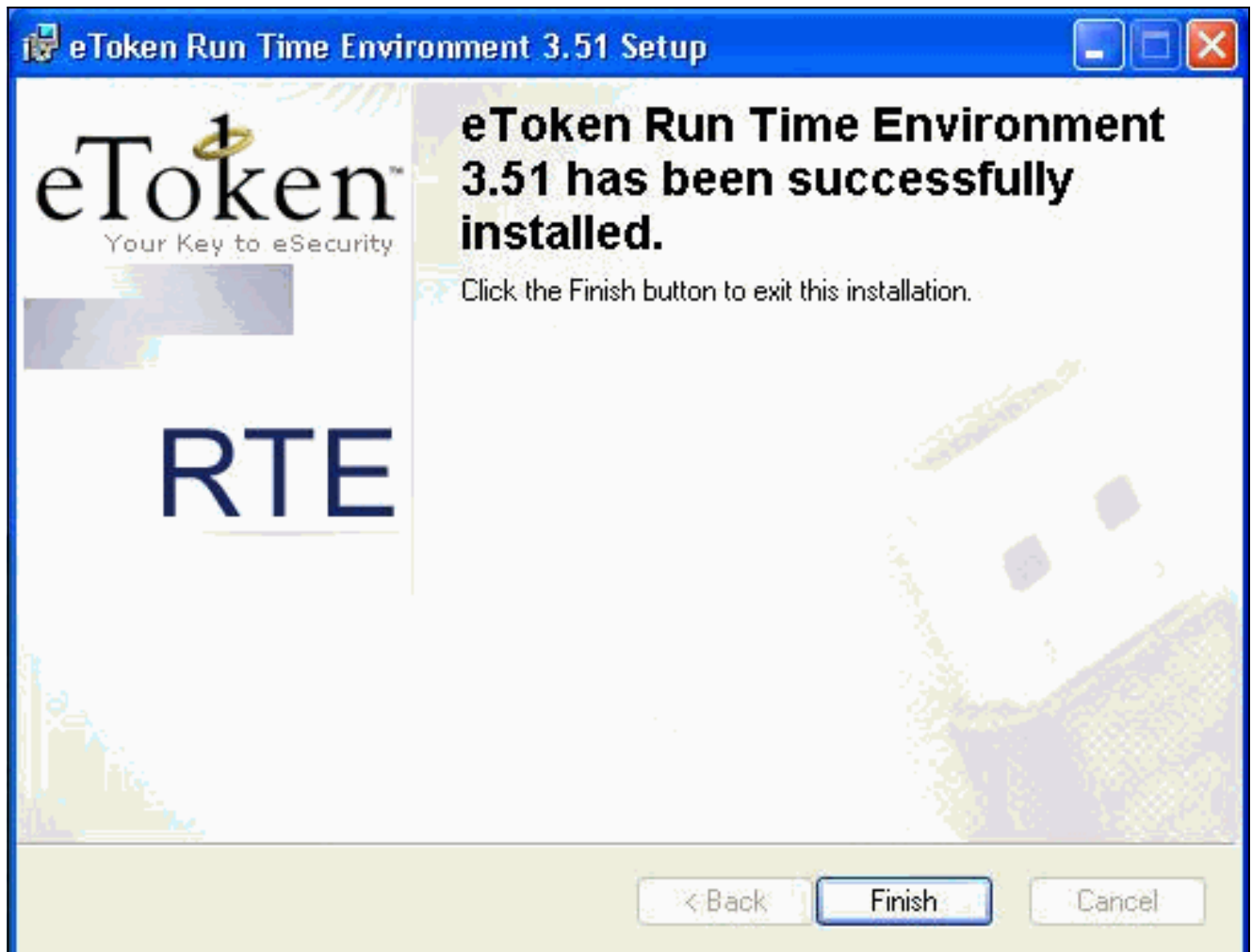
2. Akzeptieren Sie die Lizenzvertragsbedingungen, und klicken Sie auf **Weiter**.



3. Klicken Sie auf **Installieren**.



4. Die eToken Smartcard-Treiber sind jetzt installiert. Klicken Sie auf **Fertig stellen**, um den Installationsassistenten zu beenden.



Überprüfen

Dieser Abschnitt enthält Informationen, die Sie verwenden können, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto isakmp sa:** Zeigt alle aktuellen Sicherheitszuordnungen (SAs) für Internet Key Exchange (IKE) auf einem Peer an.

```
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:** Zeigt die von aktuellen Sicherheitszuordnungen verwendeten Einstellungen an.

```
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:
```

Fehlerbehebung

Weitere Informationen zur [Fehlerbehebung bei PIX zur Weiterleitung des Datenverkehrs an einen etablierten IPSec-Tunnel](#) finden Sie unter [Problembehandlung für diesen Datenverkehr](#).

Zugehörige Informationen

- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Support-Seite für IPSec \(IP Security Protocol\)](#)
- [Support-Seite für Cisco VPN-Clients](#)
- [Support-Seite für Firewalls der Serie PIX 500](#)
- [Technischer Support - Cisco Systems](#)