IPsec tussen PIX en Cisco VPN-client met behulp van smartcard-certificaten

Inhoud

Inleiding

Dit document toont aan hoe u een IPSec VPN-tunnel tussen een PIX-firewall en een Cisco VPN-client 4.0.x kunt configureren. Het configuratievoorbeeld in dit document benadrukt ook de certificeringsinstantie (CA) inschrijvingsprocedure voor zowel de Cisco IOS® router en de Cisco VPN client, evenals het gebruik van een Smartcard als certificatenopslag.

Raadpleeg IPSec configureren tussen Cisco IOS-routers en Cisco VPN-client die vertrouwenscertificaten gebruikt om meer te weten te komen over het configureren van IPSec tussen Cisco IOS-routers en Cisco VPN-client die vertrouwenscertificaten gebruikt.

Raadpleeg de optie Meervoudige-Identity certificaatautoriteiten op Cisco IOS-routers configureren om meer te weten te komen over het configureren van Meervoudige-Identity certificaatautoriteiten op Cisco IOS-routers.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco PIX Firewall met softwareversie 6.3(3)
- Cisco VPN-client 4.0.3 op een pc met Windows XP
- Een Microsoft Windows 2000 CA-server wordt in dit document gebruikt als CA-server.
- Certificaten op de Cisco VPN-client worden opgeslagen met Aladdin e-Token Smartcard.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

PIX invoeren en configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Configuraties

Dit document gebruikt deze configuraties.

- certificaatinschrijving op PIX-firewall
- Configuratie PIX-firewall

certificaatinschrijving op 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
```

Configuratie PIX-firewall

```
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
```

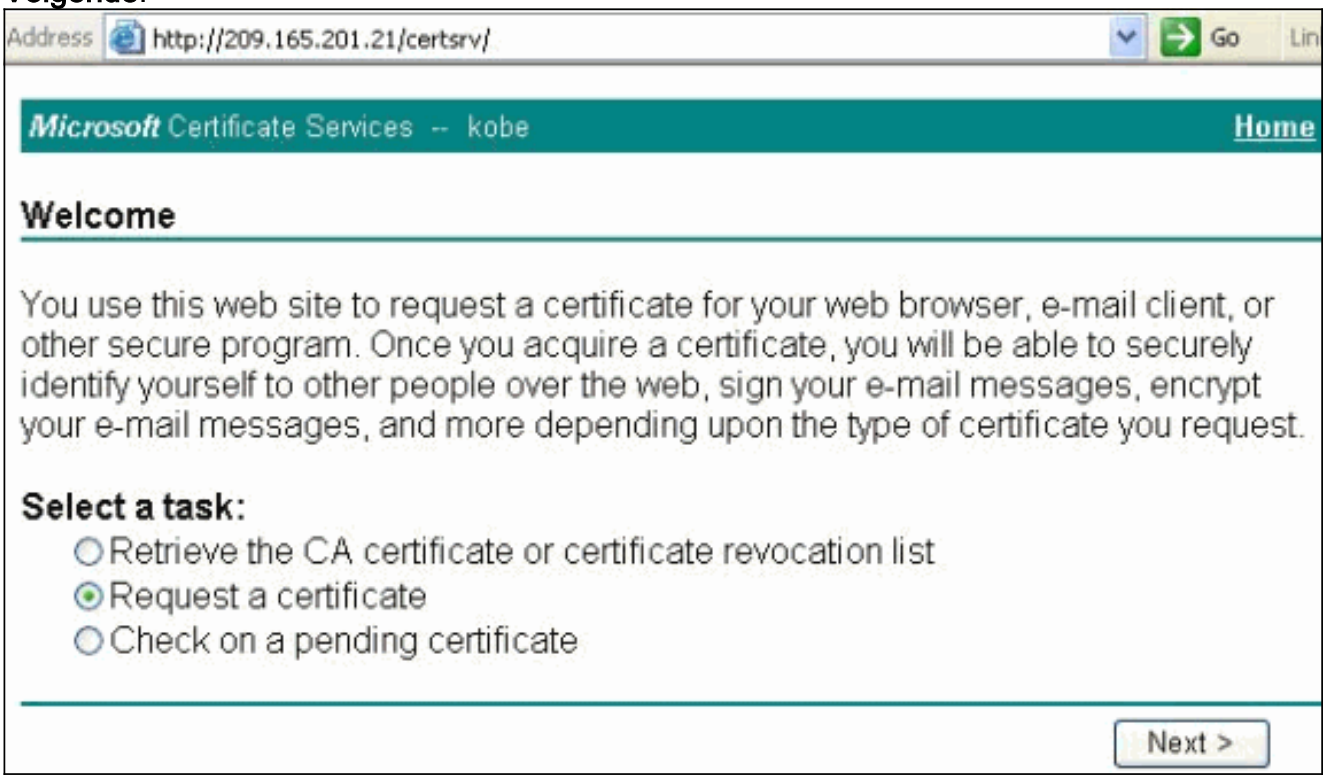
```
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 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)#
```

Cisco VPN-clientcertificaten invoeren

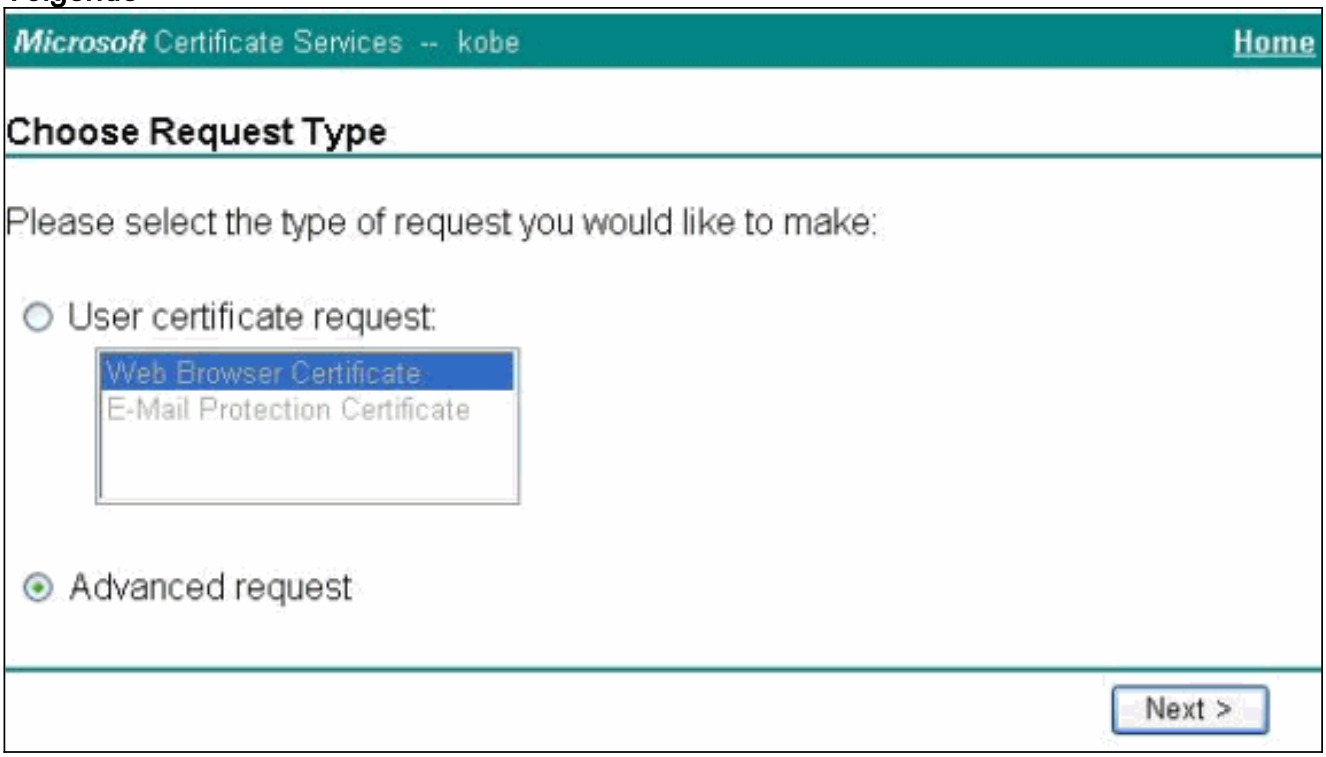
Vergeet niet alle benodigde stuurprogramma's en hulpprogramma's te installeren die met het Smartcard-apparaat op de pc worden gebruikt voor gebruik met de Cisco VPN-client.

Deze stappen tonen de procedures aan die worden gebruikt om de Cisco VPN-client voor MS-certificaten in te schrijven. Het certificaat is opgeslagen in de e-Token Smartcard winkel Aladdin .

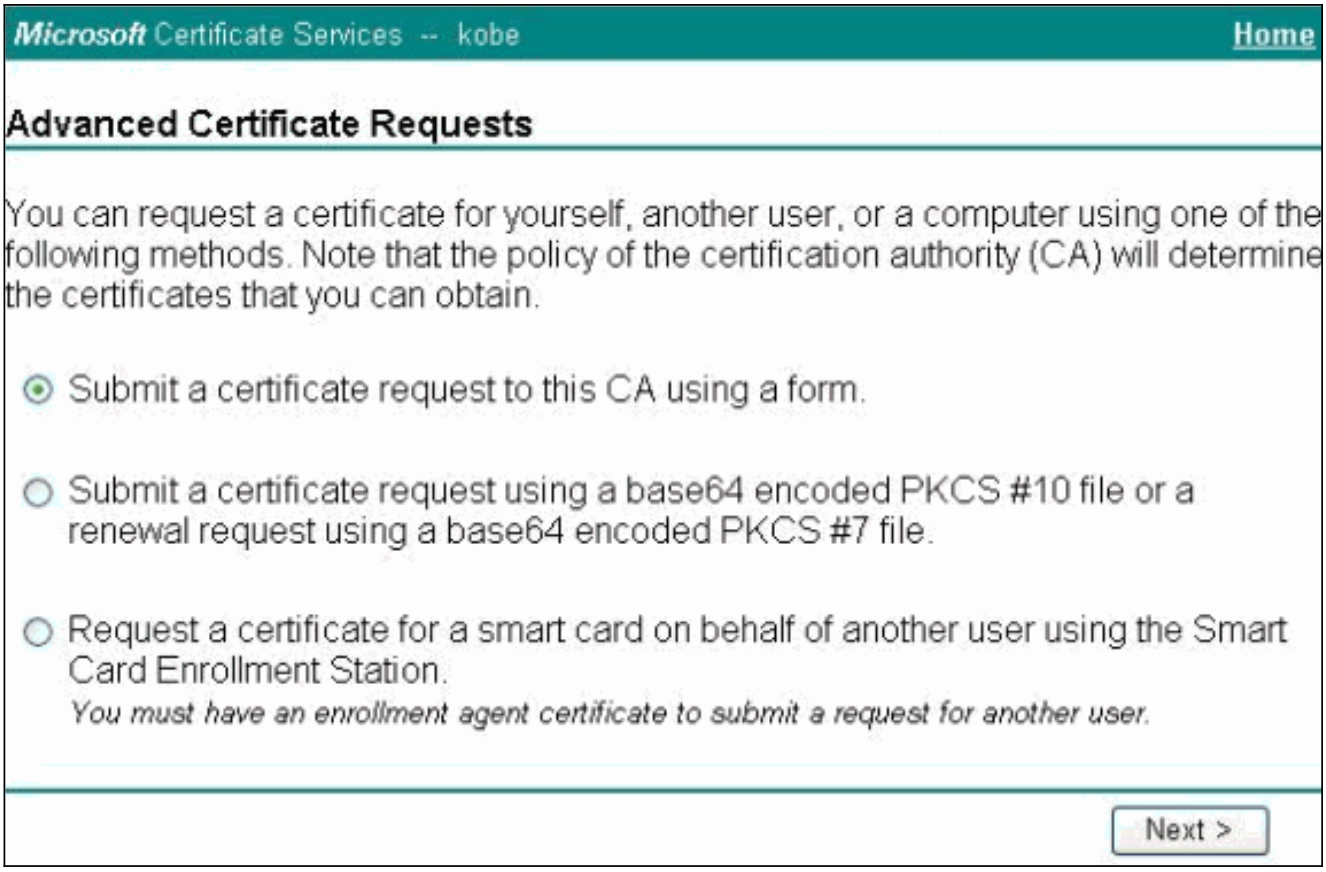
1. Start een browser en ga naar de pagina van de certificaatserver (http://CAServeraddress/certsrv/, in dit voorbeeld).
2. Selecteer **Een certificaat aanvragen** en klik op **Volgende**.



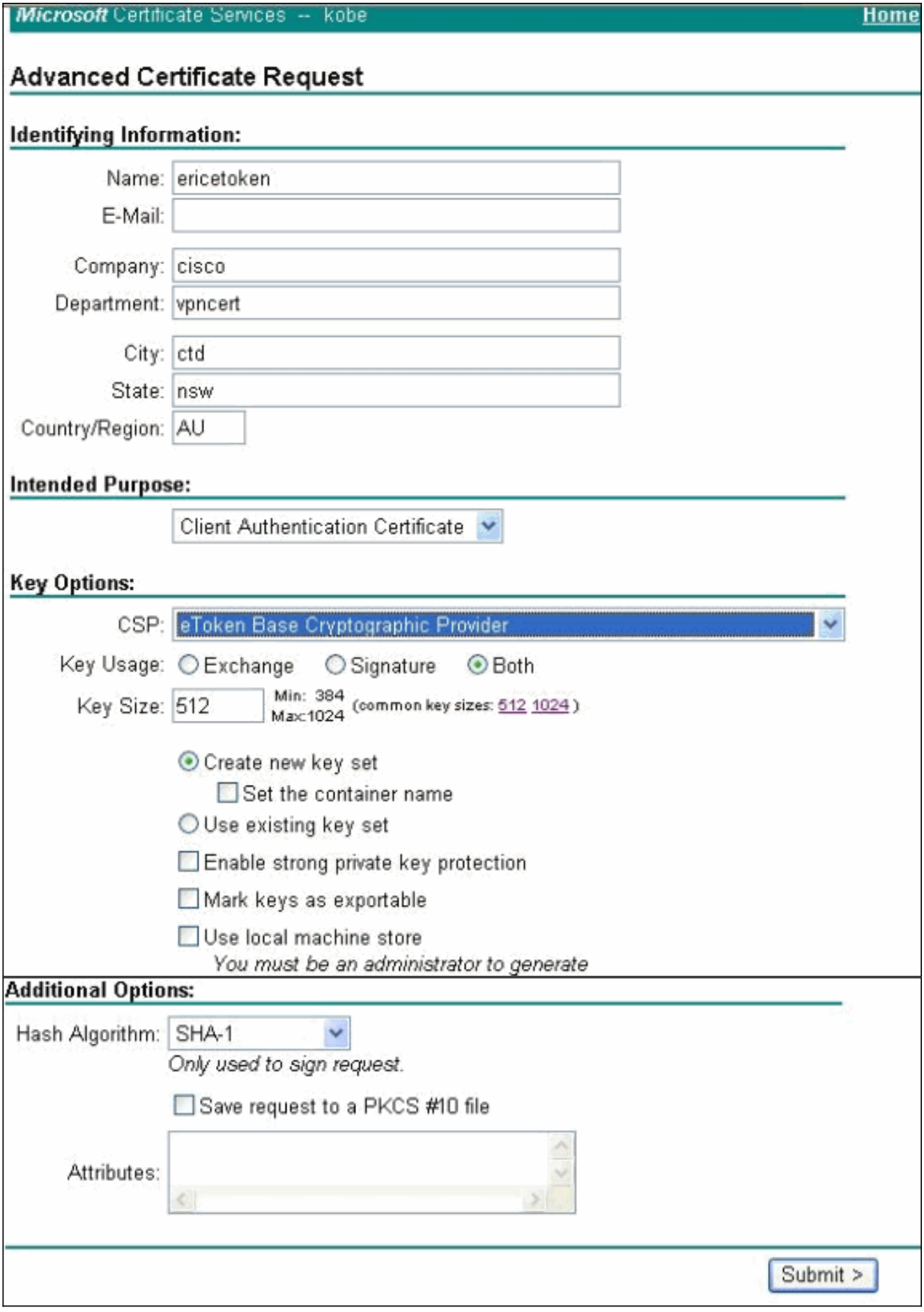
3. Selecteer in het venster Type aanvraag kiezen de optie **Geavanceerd** en klik op **Volgende**.



4. Selecteer **een certificaataanvraag bij deze CA indienen met behulp van een formulier** en klik op **Volgende**.



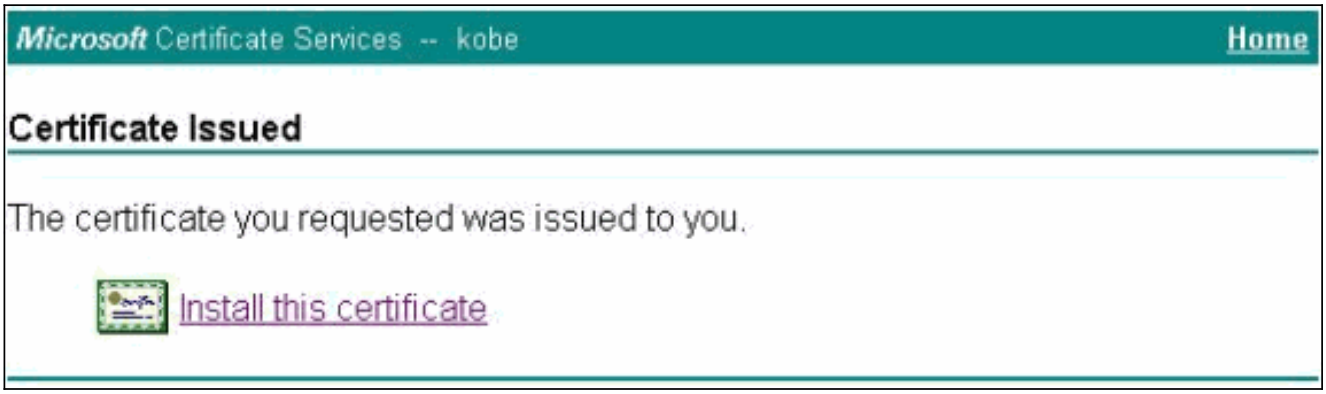
5. Vul alle items in op het formulier Geavanceerd certificaataanvraag.Zorg ervoor dat het departement of de organisatorische eenheid (OU) overeenkomt met de naam van de Cisco VPN-clientgroep, zoals ingesteld in de naam PIX-groep. Selecteer de juiste CSP-serviceprovider voor uw
instellingen.



6. Selecteer **Ja** om door te gaan met de installatie wanneer u de waarschuwing voor de potentiele Schrift Validering
krijgt.

7. Bij de certificaatinschrijving wordt gebruik gemaakt van de Token-winkel. Voer het wachtwoord in en klik op **OK**.

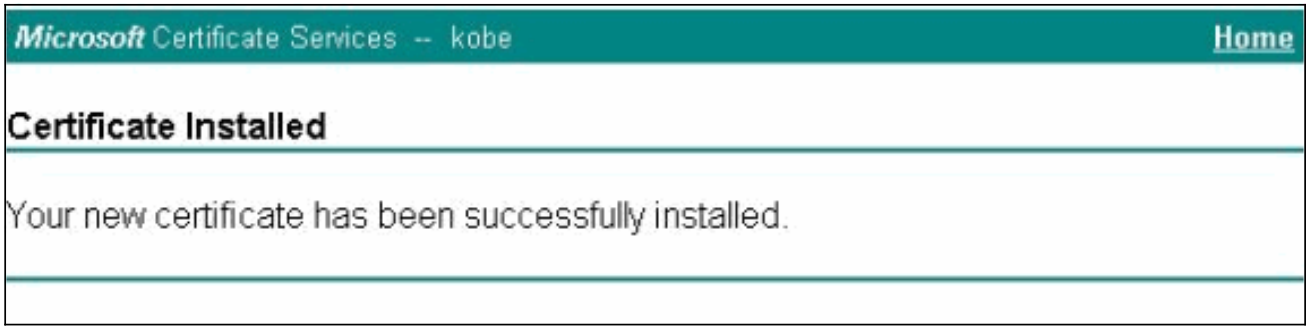
8. Klik op **Installeer dit certificaat**.



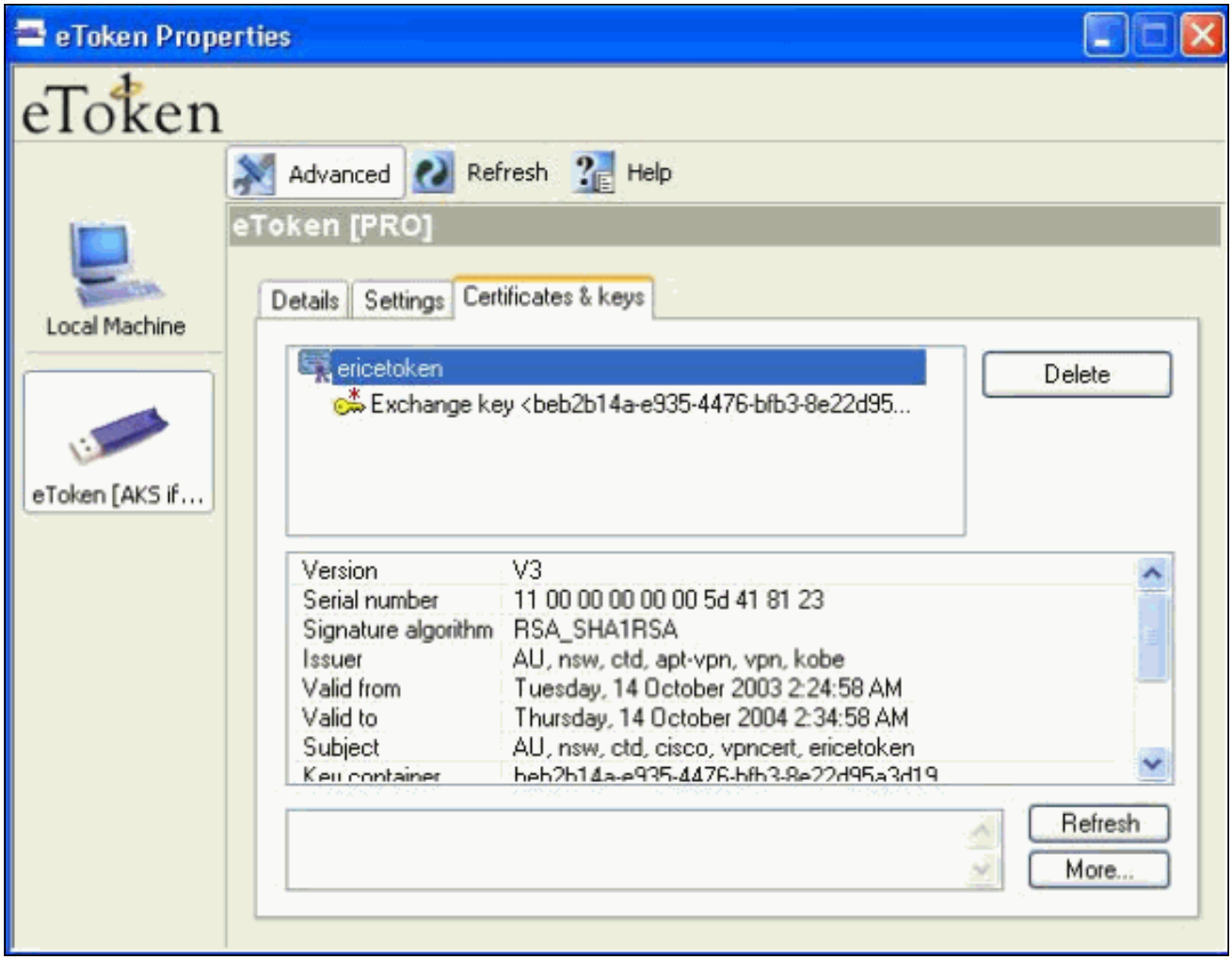
9. Selecteer **Ja** om door te gaan met de installatie wanneer u de waarschuwing voor de potentiele Schrift Validering krijgt.

10. Selecteer **Ja** om het basiscertificaat toe te voegen aan de Opslagwinkel.

11. Het venster Geïnstalleerd certificaat verschijnt en bevestigt de succesvolle installatie.



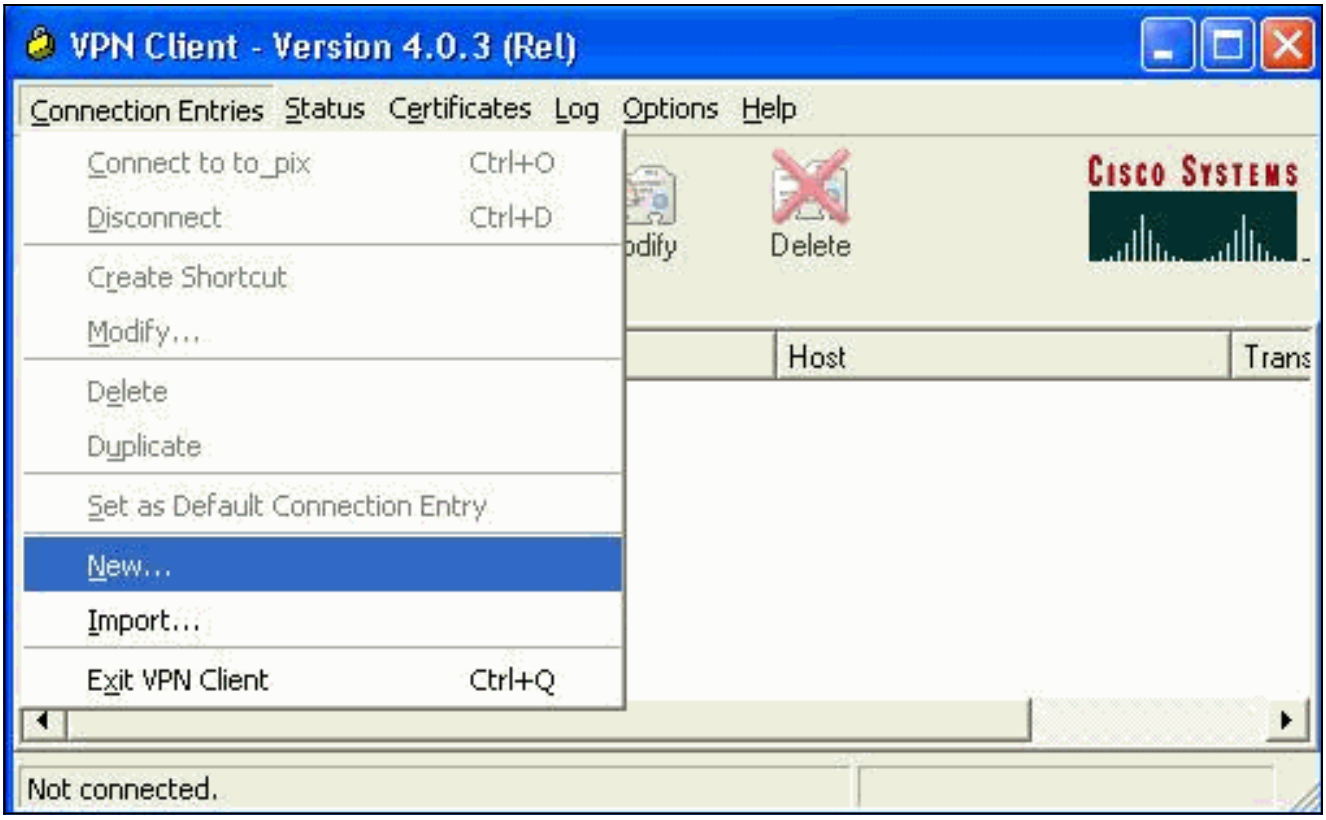
12. Gebruik het venster Token Application Viewer om het certificaat te bekijken dat is opgeslagen op de kaart.



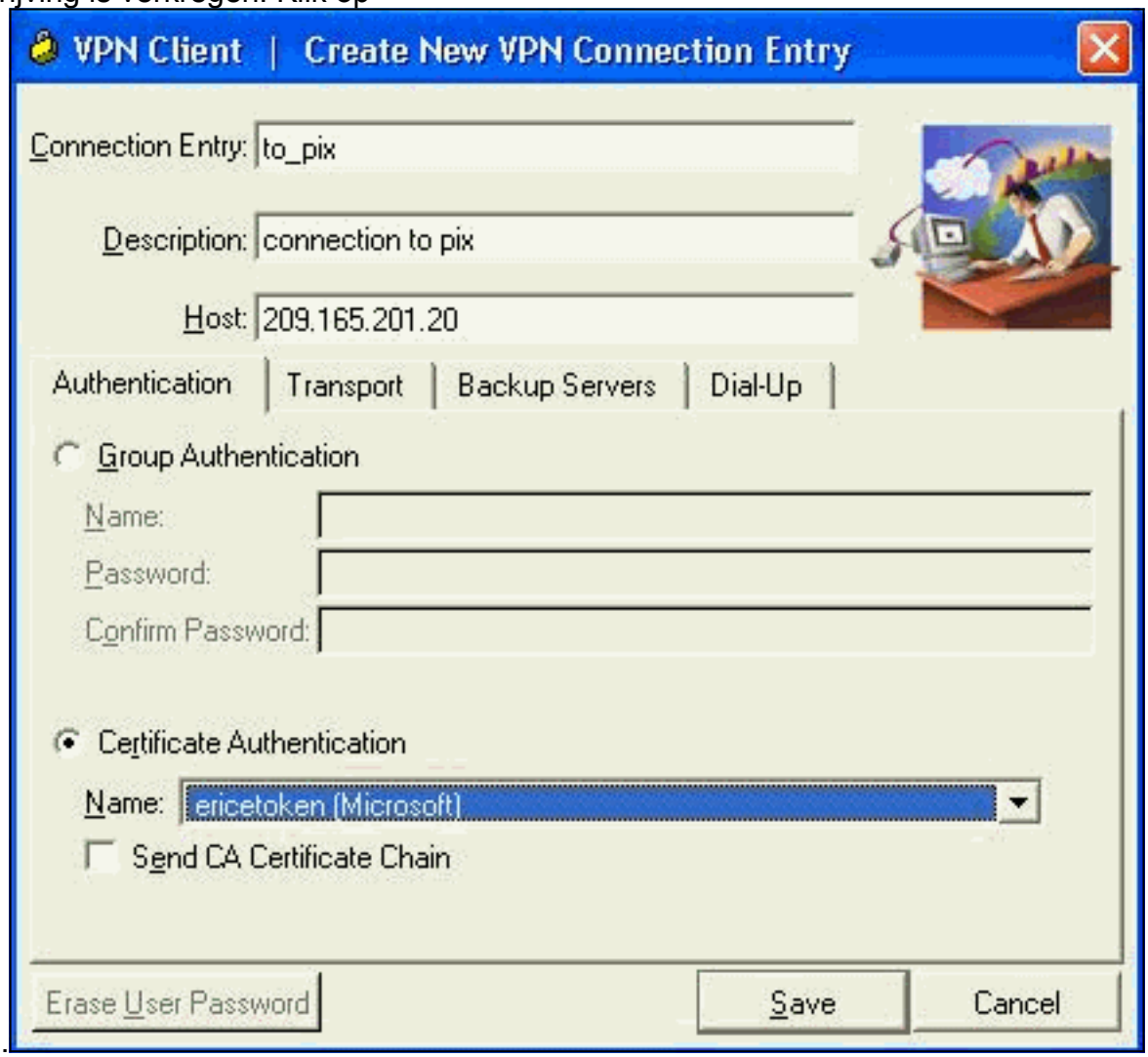
Configureer de Cisco VPN-client om het certificaat voor verbinding met de PIX te gebruiken

Deze stappen tonen de procedures aan die worden gebruikt om de Cisco VPN-client te configureren om het certificaat voor PIX-verbindingen te gebruiken.

1. Start de Cisco VPN-client. Onder Connection-ingangen klikt u op **Nieuw** om een nieuwe verbinding te
   maken.



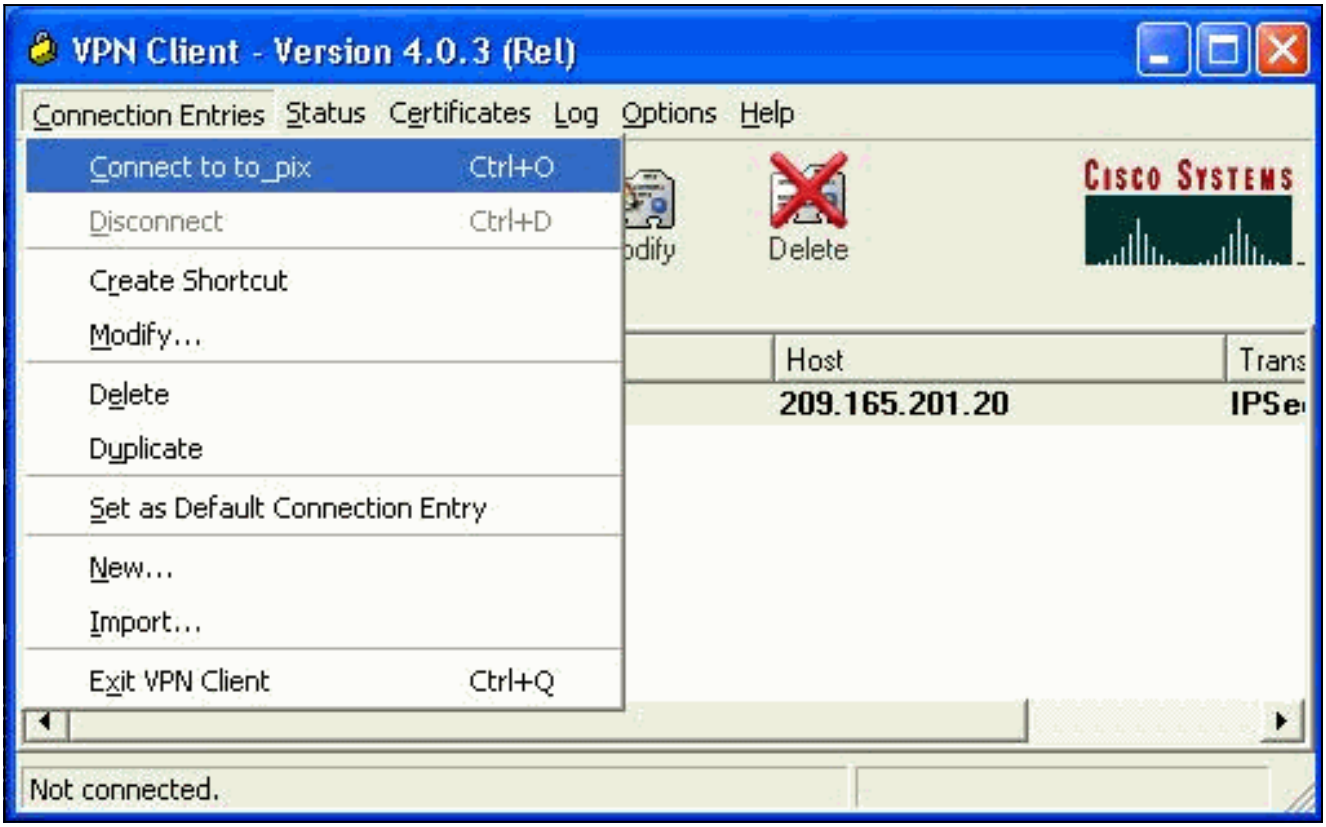
2. Specificeer de verbindingsdetails, specificeer certificaatverificatie, selecteer het certificaat dat uit inschrijving is verkregen. Klik op



Opslaan.

3. Als u de Cisco VPN-clientverbinding naar de PIX wilt starten, selecteert u de gewenste

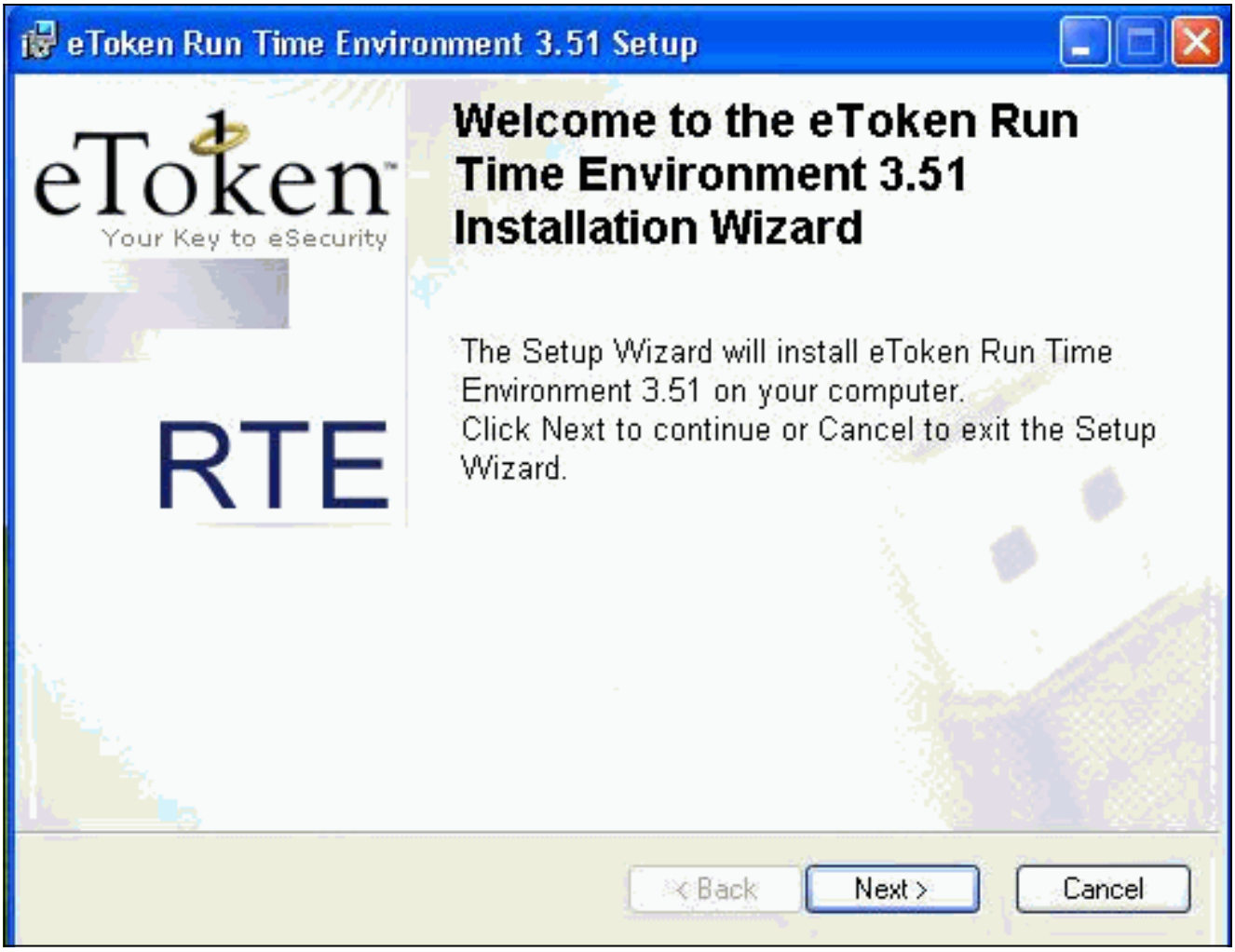
Connection-ingang en vervolgens klikt u op **Connect**.



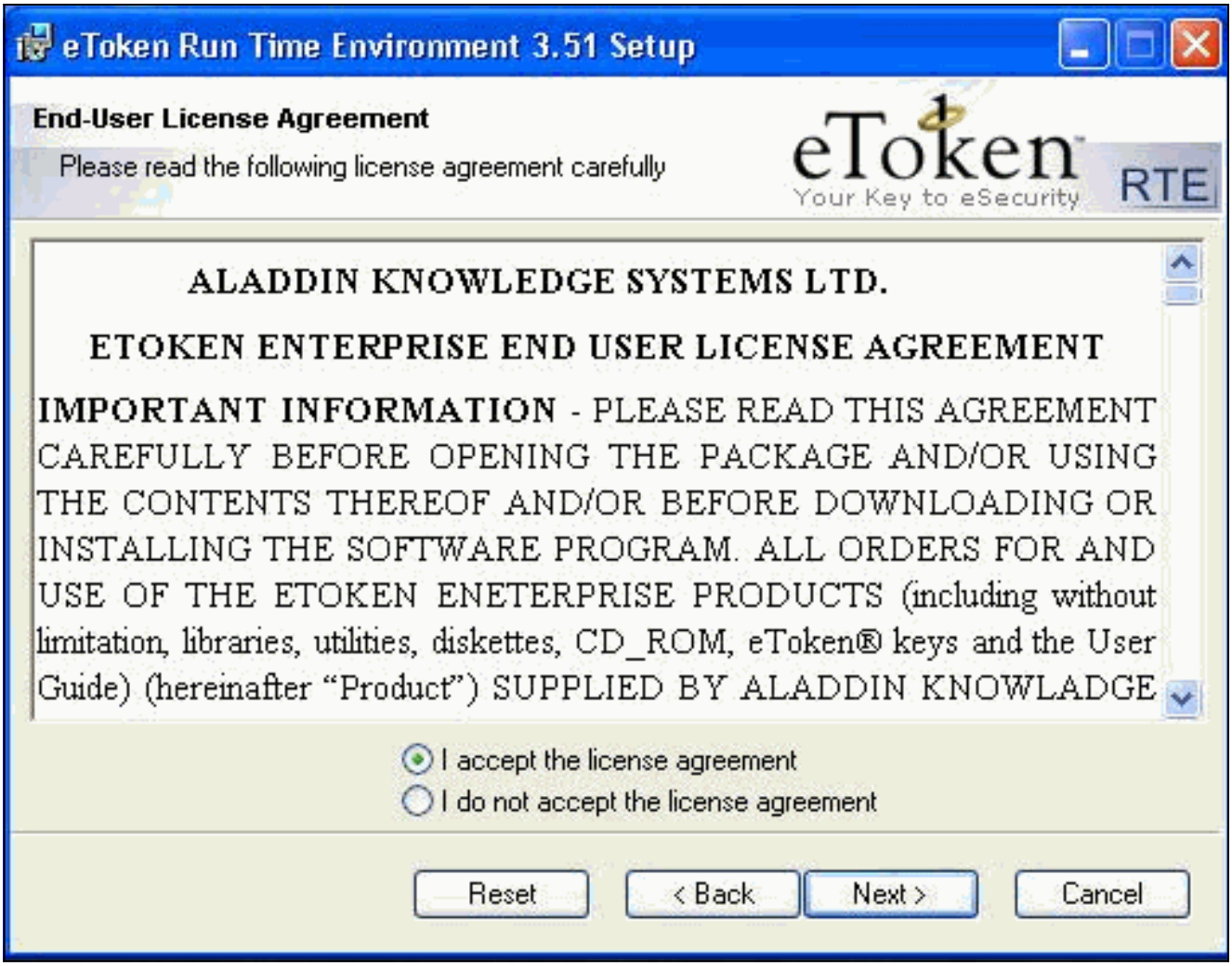
Installeer Token Smart-stuurprogramma's

Deze stappen tonen de installatie van de Aladdin-Smartcard-chauffeurs aan.

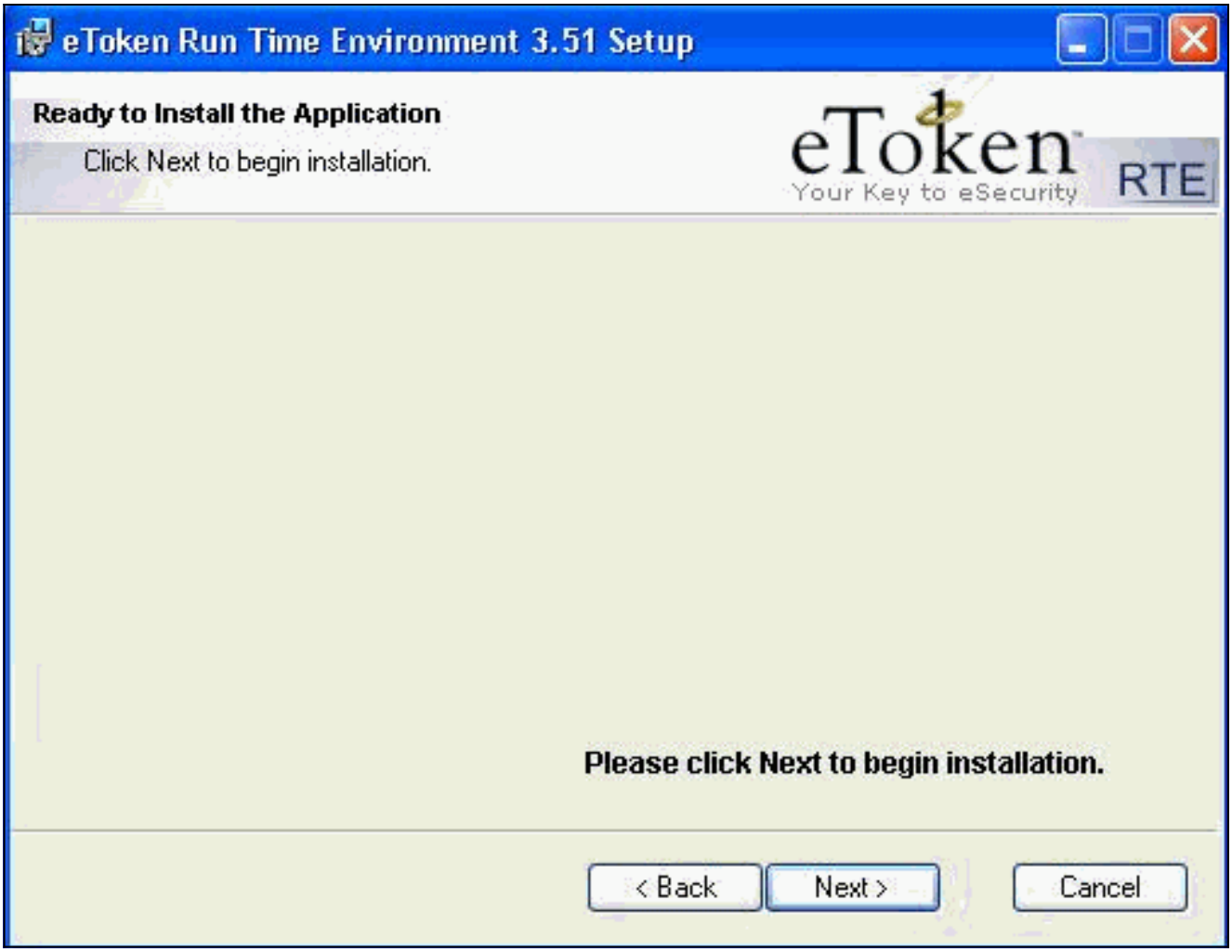
1. Open de wizard Token Run Time Environment 3.51 (Tijdmilieu).



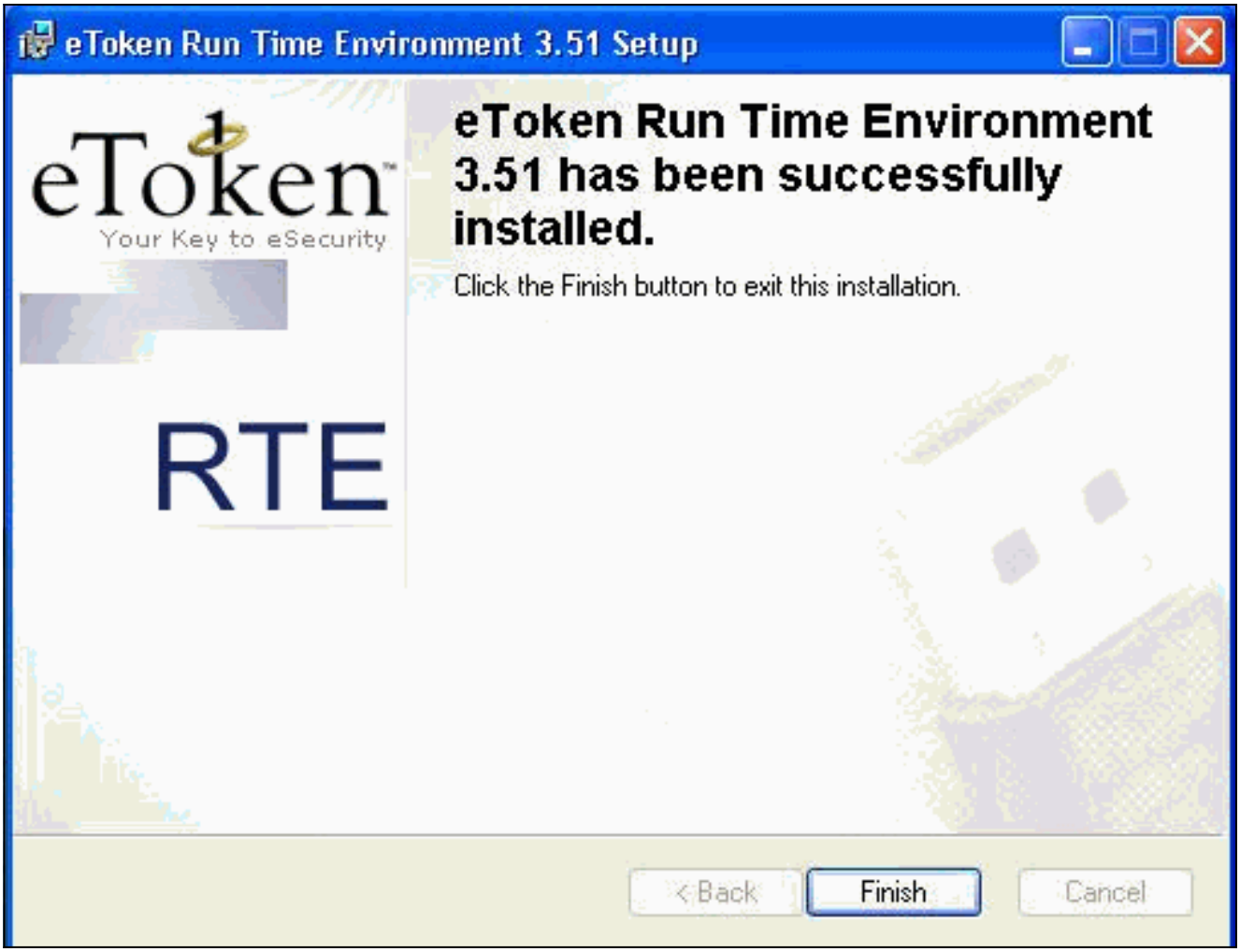
2. Accepteer de bepalingen van de Licentieovereenkomst en klik op **Volgende**.



3. Klik op **Install** (Installeren).



4. De Token Smartcard stuurprogramma's zijn nu geïnstalleerd. Klik op **Voltooien** om de wizard te
verlaten.



Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **toon crypto isakmp sa**-Toont alle huidige IKE (Internet Key Exchange) veiligheidsassociaties (SAs) bij een 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
```

- **Laat crypto ipsec sa**-displays de instellingen die worden gebruikt door de huidige beveiligingsassociaties.

```
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:
```

Problemen oplossen

Raadpleeg Problemen oplossen de PIX om gegevensverkeer via een vaste IPSec-tunnelbestand door te geven voor meer informatie over het oplossen van deze configuratie.

Gerelateerde informatie

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Ondersteuningspagina voor IPsec (IP security protocol)
- Cisco VPN-clientondersteuningspagina
- Ondersteuning van PIX 500 Series firewalls
- Technische ondersteuning - Cisco-systemen