Exemple de configuration IPSec entre PIX et le client VPN Cisco à l'aide de certificats Smartcard

Contenu

Introduction

Ce document explique comment configurer un tunnel VPN IPSec entre un pare-feu PIX et un client VPN Cisco 4.0.x. L'exemple de configuration de ce document met également en évidence la procédure d'inscription de l'autorité de certification (CA) pour le routeur Cisco IOS® et le client VPN Cisco, ainsi que l'utilisation d'une carte à puce comme stockage de certificats.

Référez-vous à Configuration d'IPSec entre les routeurs Cisco IOS et le client VPN Cisco à l'aide de certificats Entrust afin d'en savoir plus sur Configuration d'IPSec entre les routeurs Cisco IOS et le client VPN Cisco à l'aide de certificats Entrust.

Référez-vous à Configuration d'autorités de certificats à identité multiple sur les routeurs Cisco IOS afin d'en savoir plus sur la configuration d'autorités de certificats à identité multiple sur les routeurs Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu Cisco PIX version 6.3(3)
- Client VPN Cisco 4.0.3 sur un PC exécutant Windows XP
- Un serveur AC Microsoft Windows 2000 est utilisé dans ce document en tant que serveur AC.
- Les certificats du client VPN Cisco sont stockés à l'aide de la carte à puce Aladdin e-Token.

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Inscrire et configurer le PIX

Cette section vous fournit des informations utilisées pour configurer les fonctionnalités décrites dans ce document.

Remarque : Afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commandes (clients enregistrés uniquement).

Configurations

Ce document utilise les configurations suivantes.

- Inscription de certificat sur PIX Firewall
- Configuration du pare-feu PIX

Inscription de certificat sur 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
```

Configuration du pare-feu 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
```

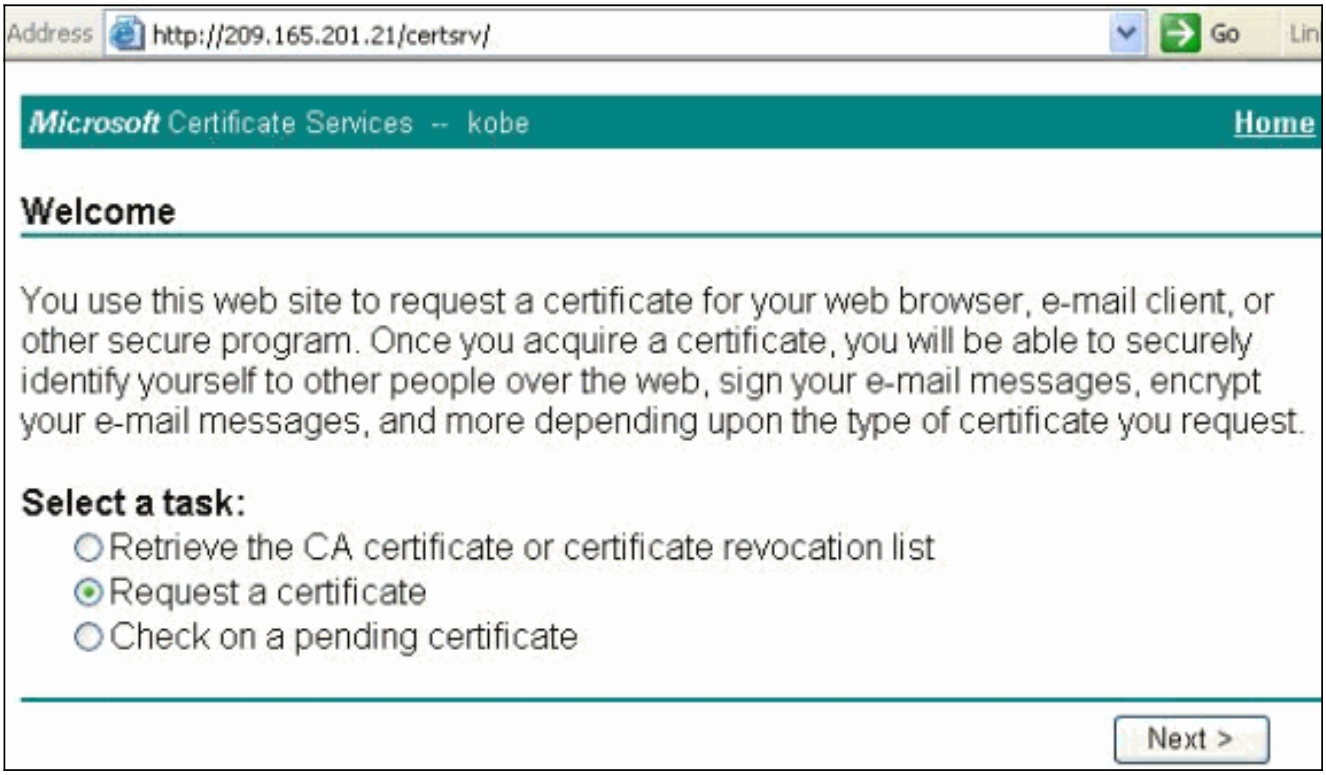
```
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask
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)#
```

Inscription des certificats client VPN Cisco

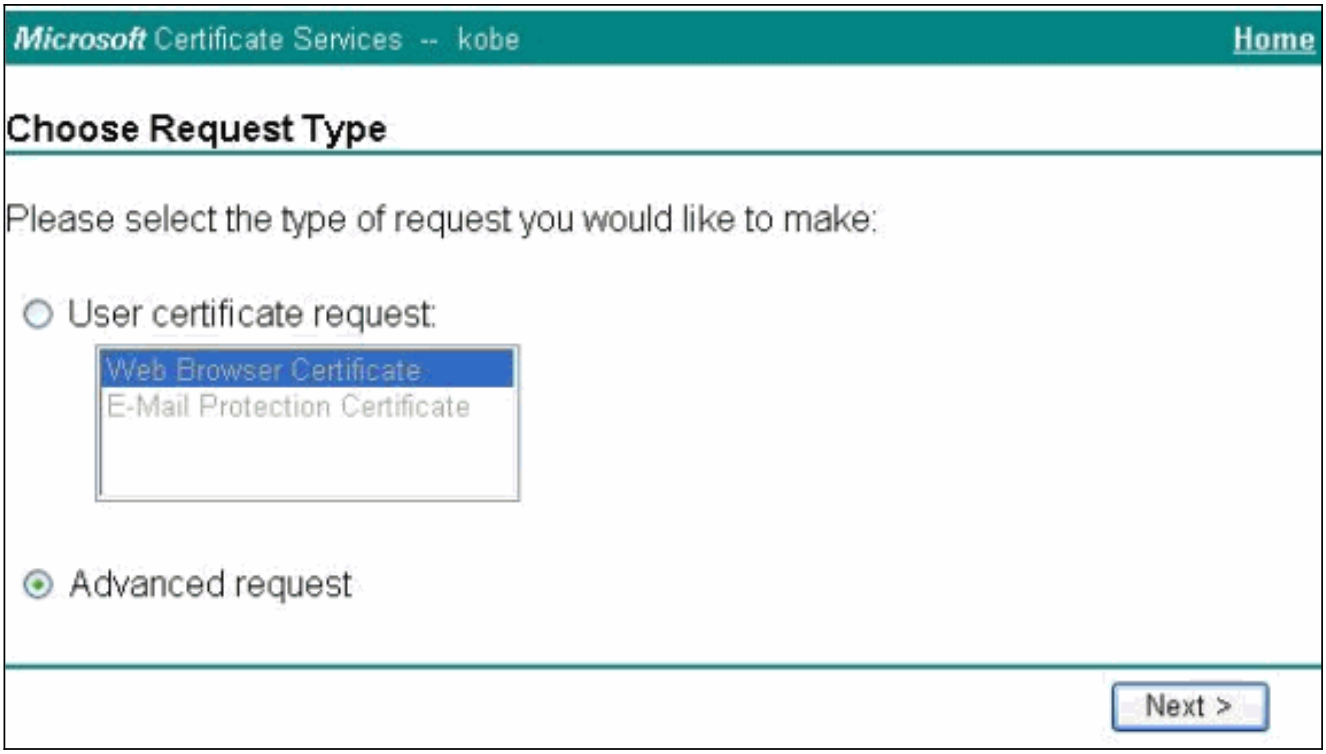
N'oubliez pas d'installer tous les pilotes et utilitaires nécessaires fournis avec le périphérique Smartcard sur le PC à utiliser avec le client VPN Cisco.

Ces étapes illustrent les procédures utilisées pour inscrire les certificats MS au client VPN Cisco. Le certificat est stocké dans le magasin Aladdin e-Token Smartcard.

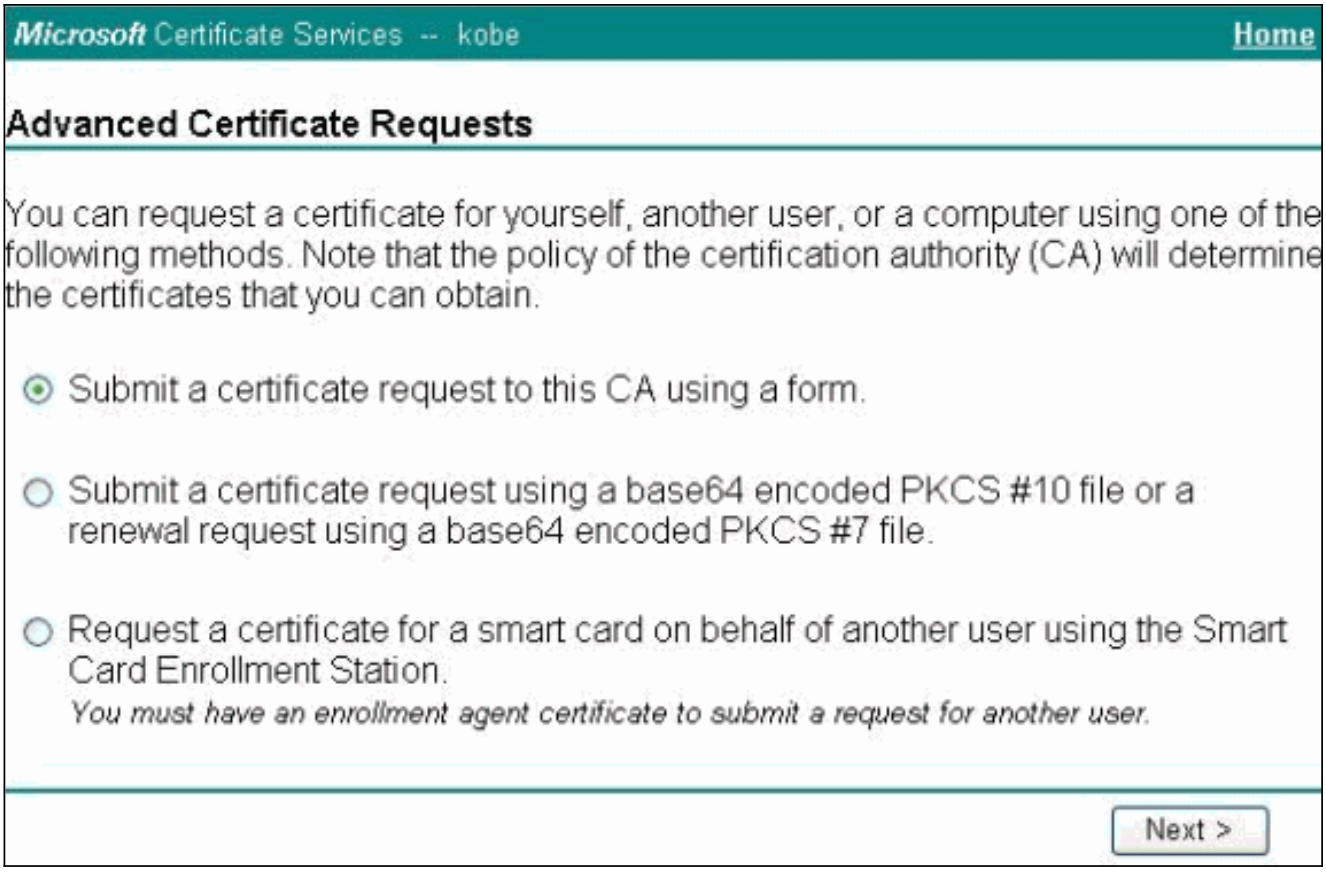
1. Lancez un navigateur et accédez à la page du serveur de certificats (http://CAServeraddress/certsrv/, dans cet exemple).
2. Sélectionnez **Demander un certificat** et cliquez sur **Suivant**.



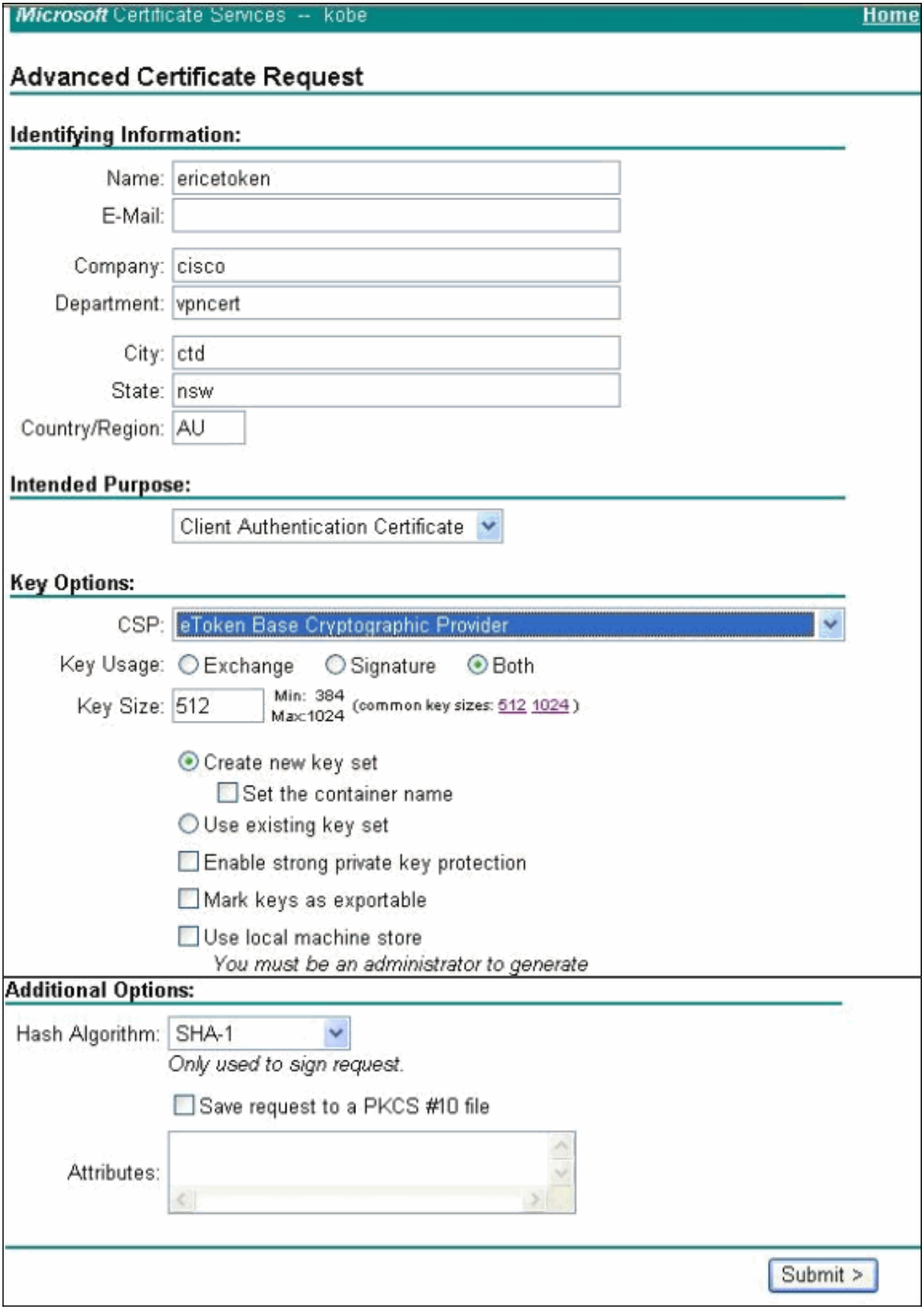
3. Dans la fenêtre Choisir un type de demande, sélectionnez **Demande avancée** et cliquez sur **Suivant**.



4. Sélectionnez **Soumettre une demande de certificat à cette autorité de certification à l'aide d'un formulaire** et cliquez sur **Suivant**.



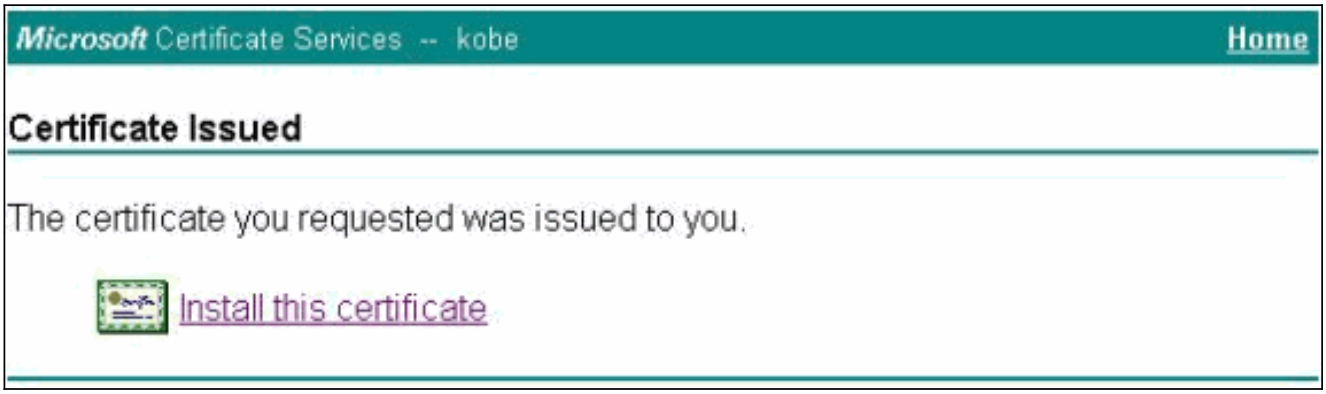
5. Complétez tous les éléments du formulaire de demande de certificat avancée.Assurez-vous que le département ou l'unité d'organisation correspond au nom du groupe Client VPN Cisco, tel que configuré dans le nom du groupe vpngroup PIX. Sélectionnez le fournisseur de services de certificats (CSP) approprié à votre configuration.



6. Sélectionnez **Oui** afin de poursuivre l'installation lorsque vous recevez l'avertissement de validation de script
potentiel.

7. L'inscription au certificat appelle le magasin eToken. Entrez le mot de passe et cliquez sur **OK**.

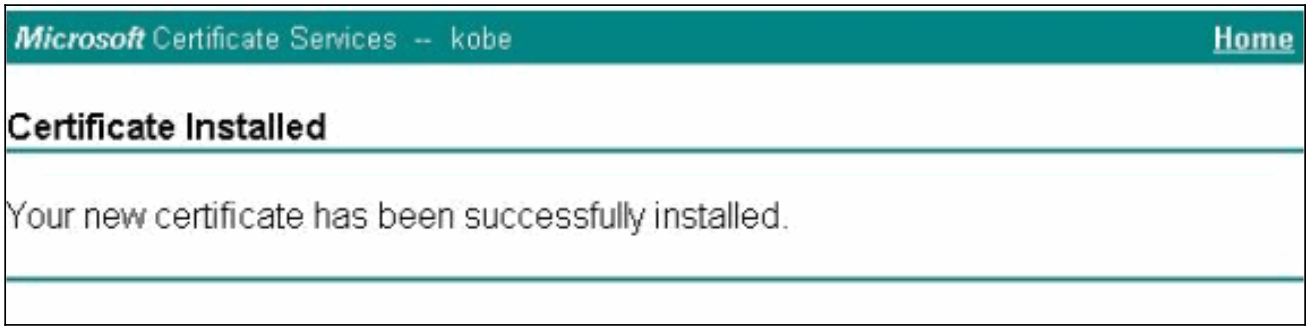
8. Cliquez sur **Installer ce certificat**.



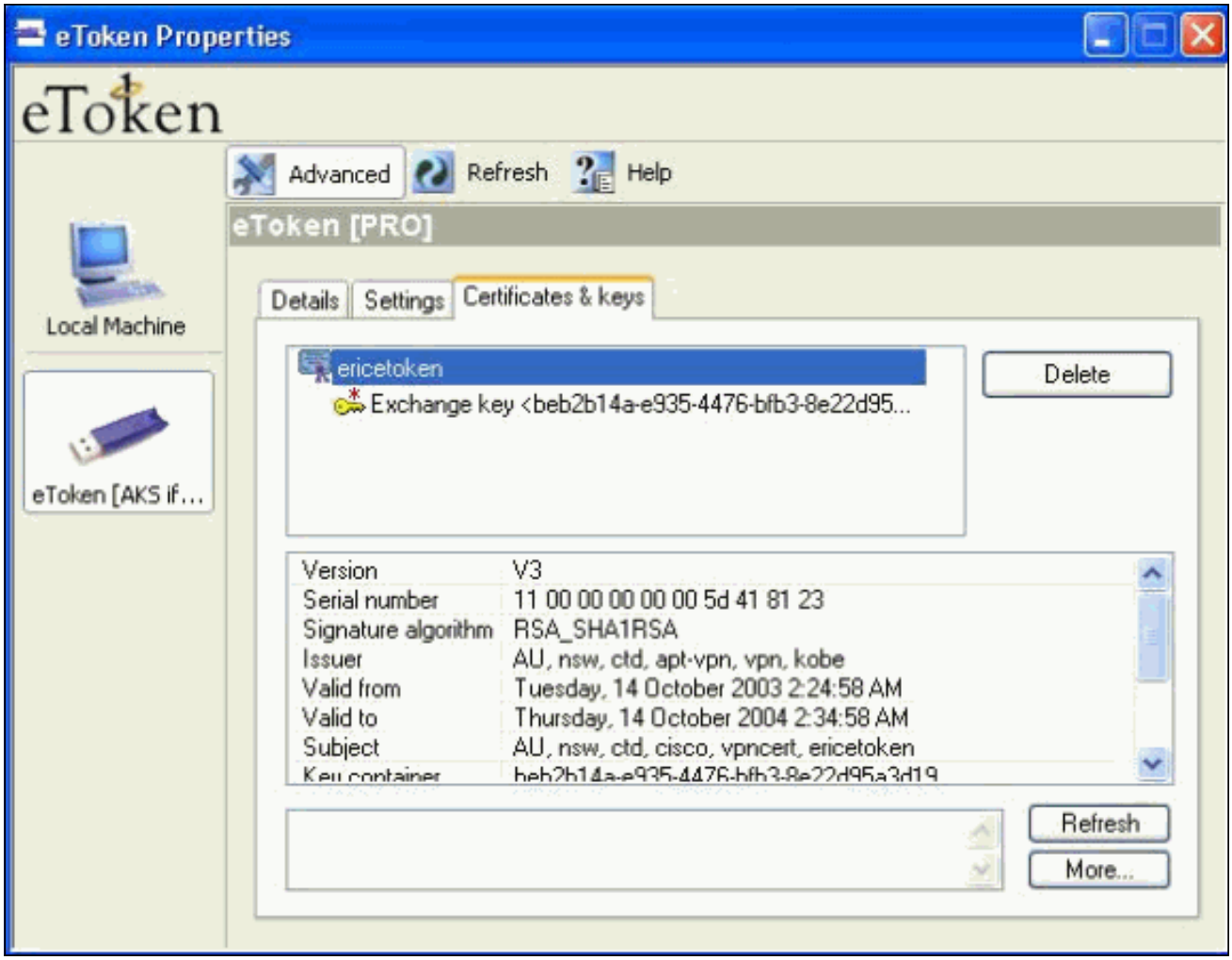
9. Sélectionnez **Oui** afin de poursuivre l'installation lorsque vous recevez l'avertissement de validation de script potentiel.

10. Sélectionnez **Oui** afin d'ajouter le certificat racine au magasin racine.

11. La fenêtre Certificat installé s'affiche et confirme l'installation réussie.



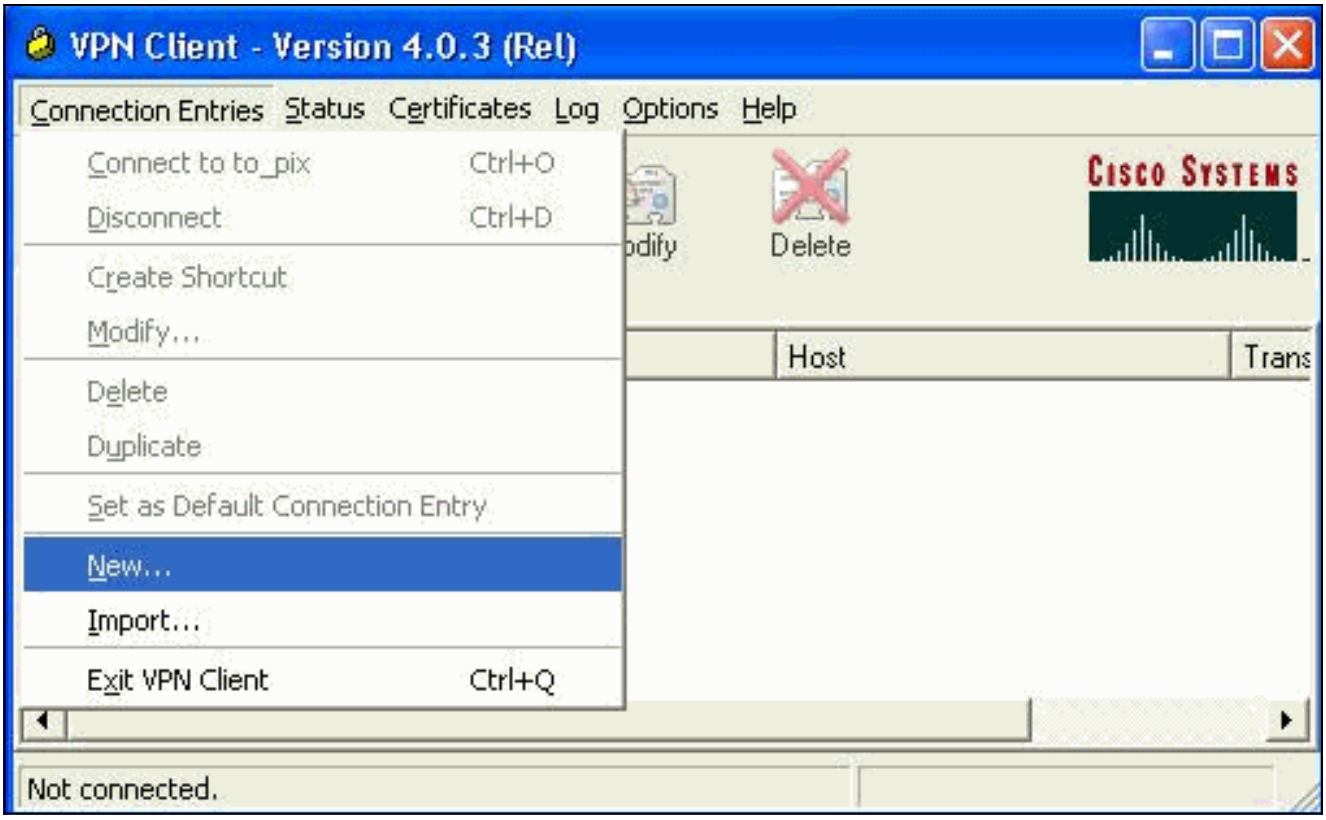
12. Utilisez le visualiseur d'applications eToken afin d'afficher le certificat stocké sur la carte à puce.



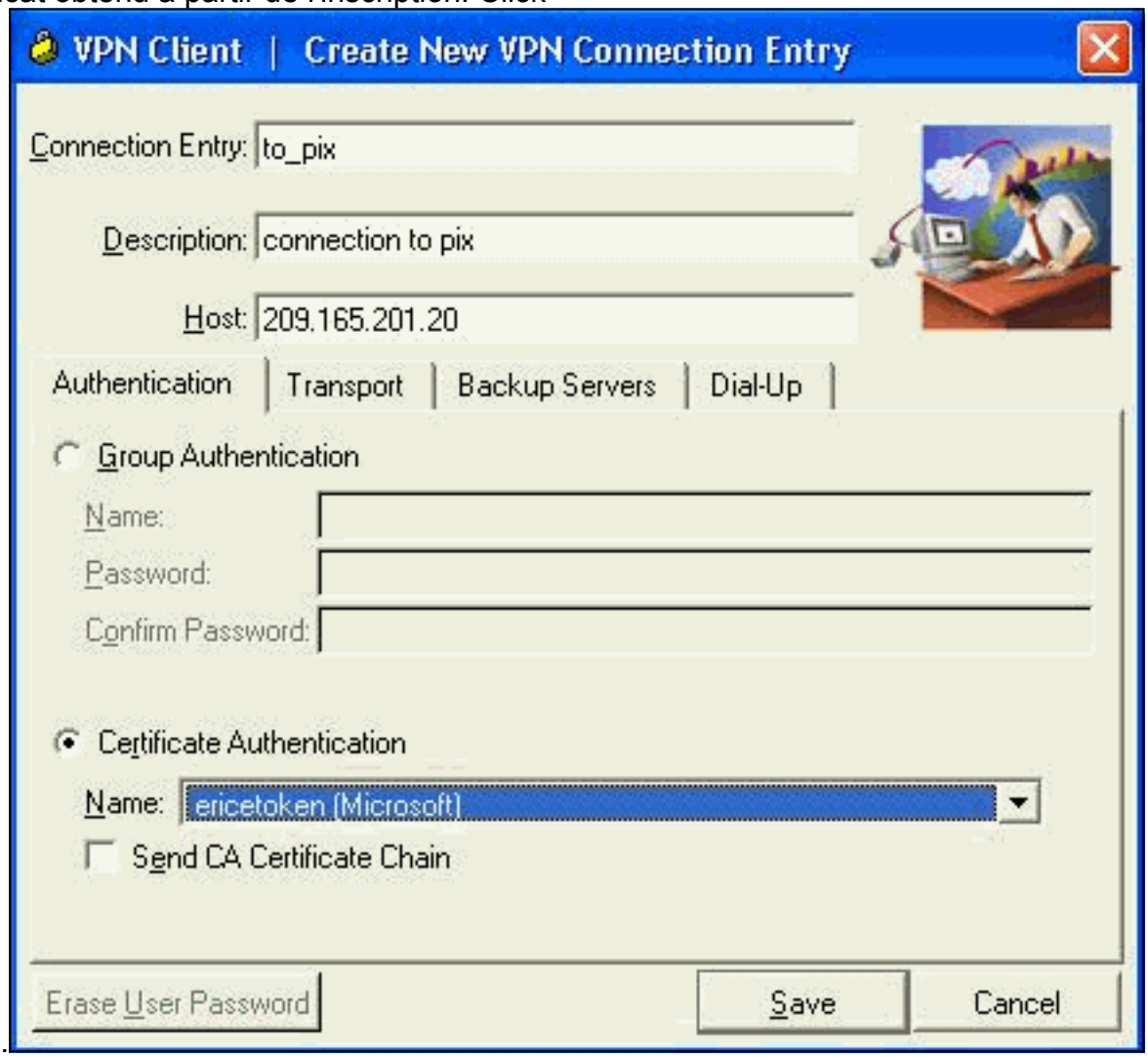
Configurer le client VPN Cisco afin d'utiliser le certificat de connexion au PIX

Ces étapes montrent les procédures utilisées pour configurer le client VPN Cisco afin qu'il utilise le certificat pour les connexions PIX.

1. Lancez le client VPN Cisco. Sous Entrées de connexion, cliquez sur **Nouveau** afin de créer une nouvelle
   connexion.



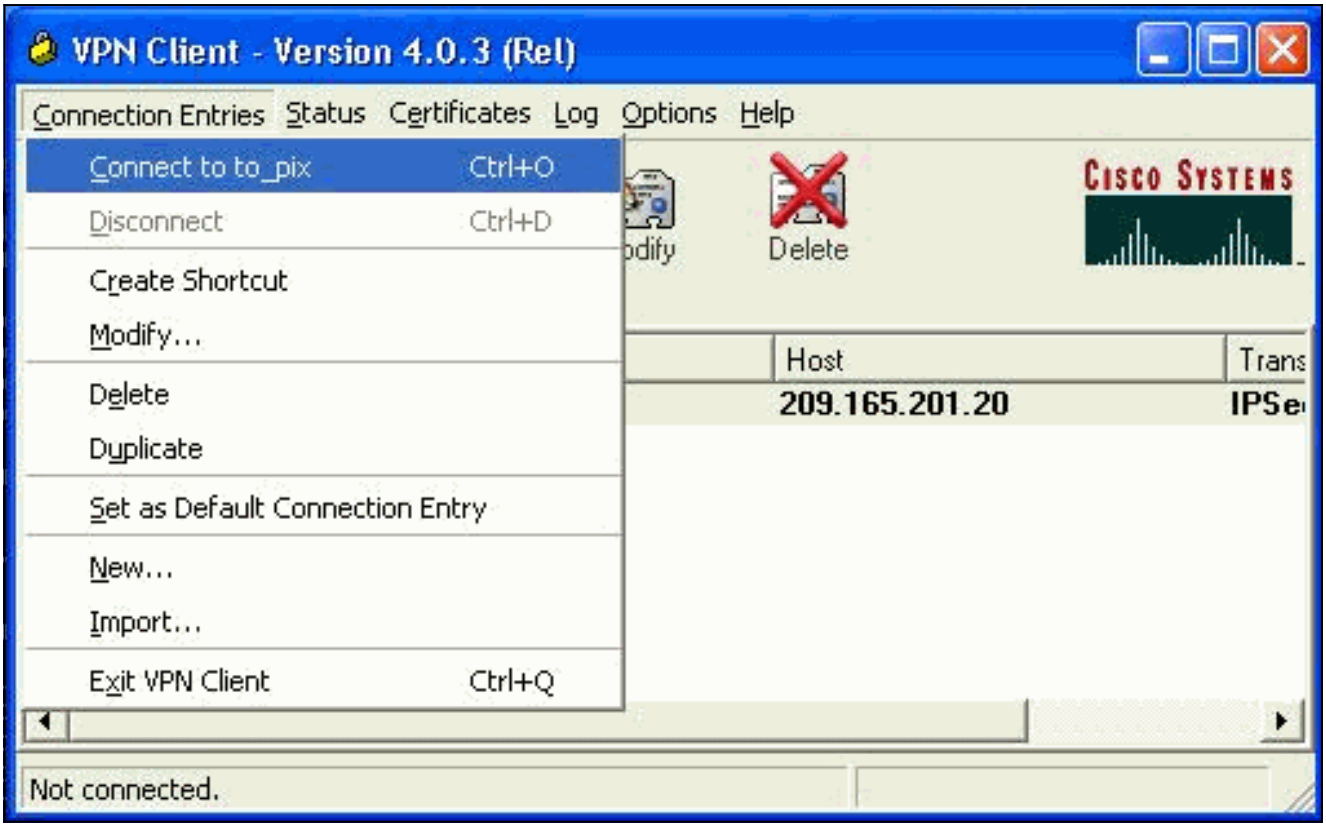
2. Complétez les détails de la connexion, spécifiez Certificate Authentication, sélectionnez le certificat obtenu à partir de l'inscription. Click



Save.

3. Afin de démarrer la connexion du client VPN Cisco au PIX, sélectionnez l'entrée de

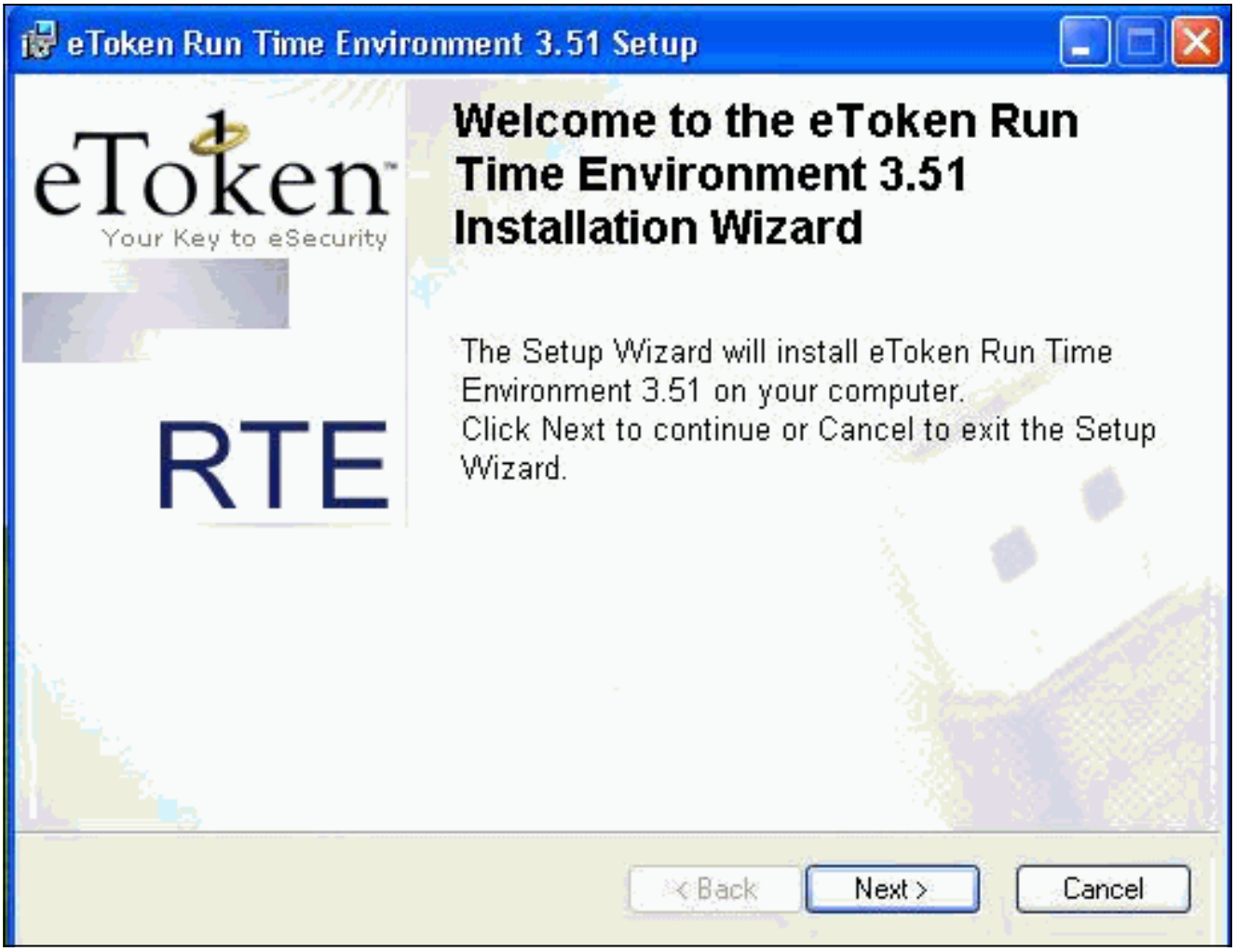
connexion souhaitée et cliquez sur **Connect**.



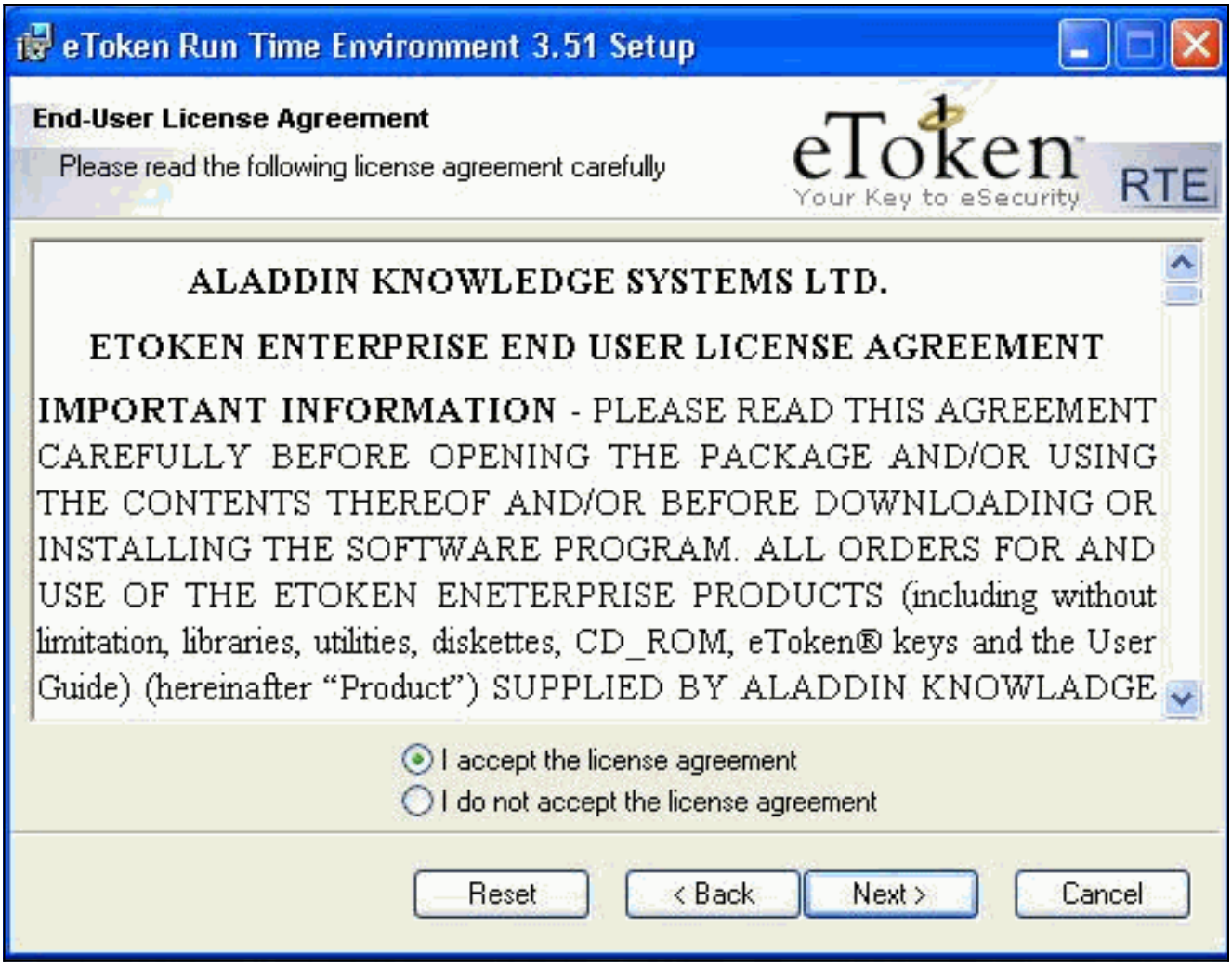
Installer les pilotes eToken Smartcard

Ces étapes illustrent l'installation des pilotes de carte à puce Aladdin eToken.

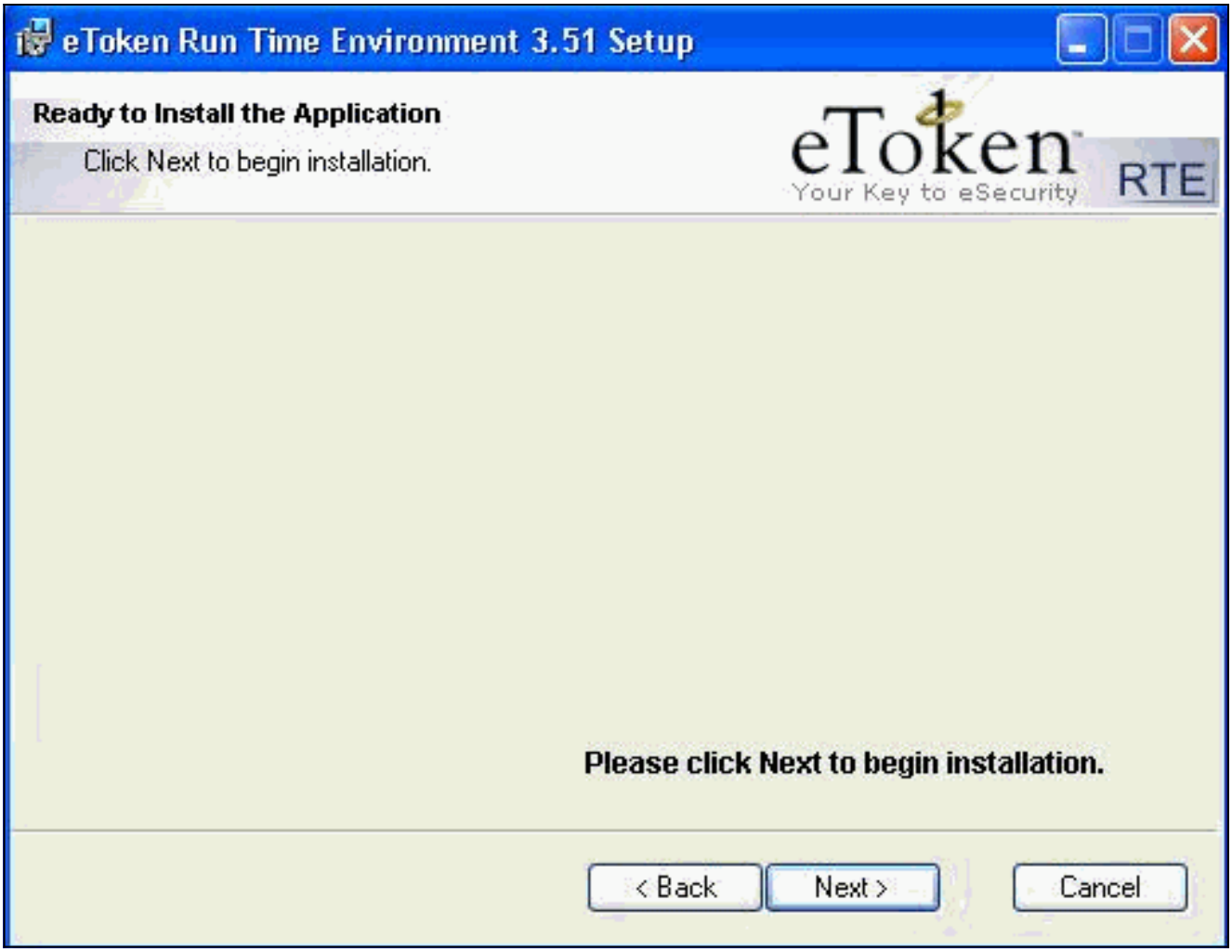
1. Ouvrez l'assistant de configuration de eToken Run Time Environment 3.51.



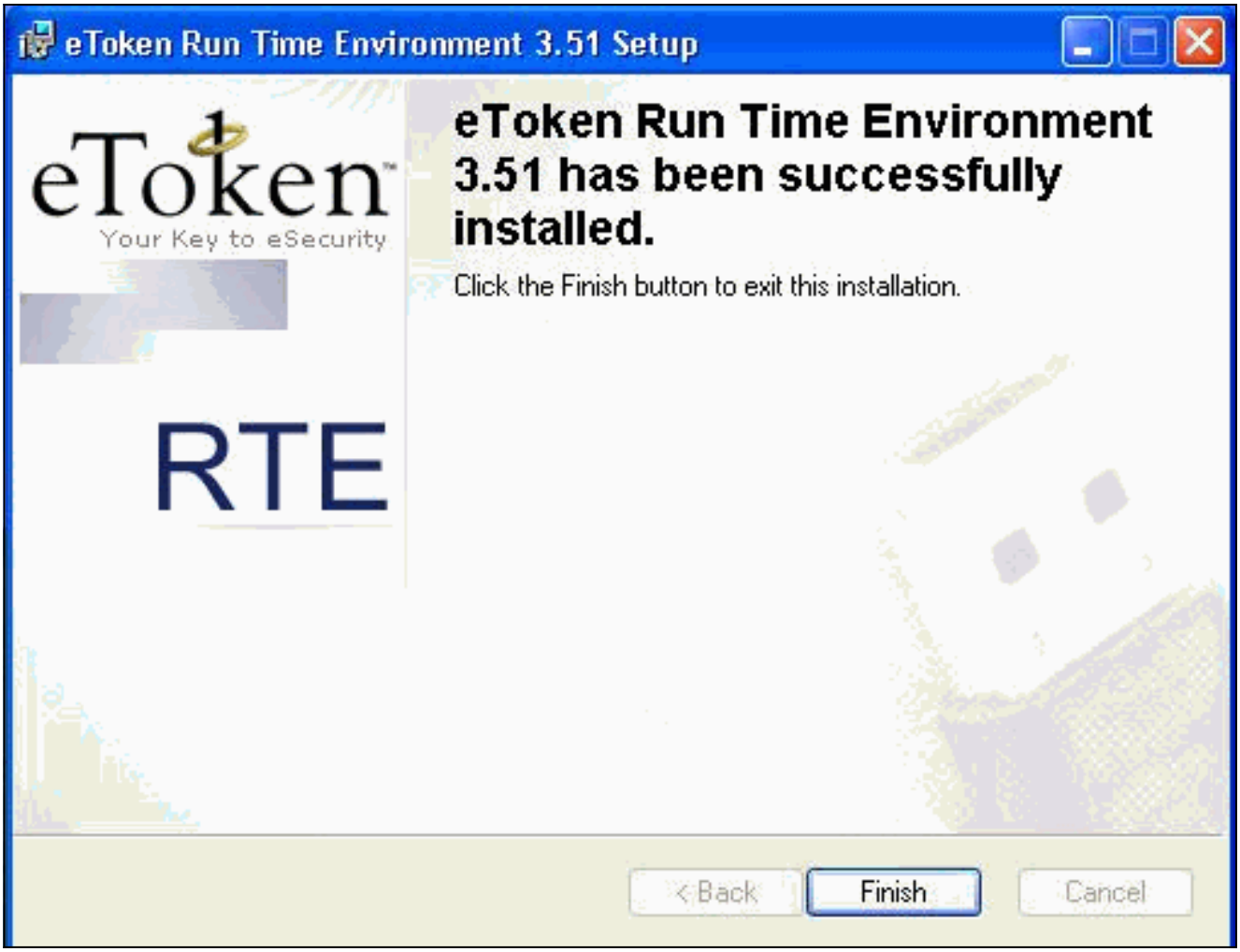
2. Acceptez les termes du contrat de licence et cliquez sur **Suivant**.



3. Cliquez sur **Install**.



4. Les pilotes eToken Smartcard sont maintenant installés. Cliquez sur **Terminer** afin de quitter l'assistant de
configuration.



Vérification

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité (SA) IKE (Internet Key Exchange) actuelles sur un homologue.

```
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** - Affiche les paramètres utilisés par les associations de sécurité actuelles.

```
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:
```

Dépannage

Référez-vous à Dépannage du PIX pour passer le trafic de données sur un tunnel IPSec établi pour plus d'informations sur le dépannage de cette configuration.

Informations connexes

- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Page d'assistance d'IPSec (protocole de sécurité IP)
- Cisco VPN Client Support Page
- Page d'assistance de pare-feu PIX 500 Series
- Support technique - Cisco Systems