Esempio di configurazione di IPSec tra PIX e client VPN Cisco con certificati smart card

Sommario

Introduzione

In questo documento viene illustrato come configurare un tunnel VPN IPSec tra un firewall PIX e un client VPN Cisco 4.0.x. L'esempio di configurazione riportato in questo documento evidenzia anche la procedura di registrazione dell'Autorità di certificazione (CA) per i router Cisco IOS® e i client VPN Cisco, nonché l'utilizzo di una Smartcard per l'archiviazione dei certificati.

Per ulteriori informazioni sulla configurazione di IPSec tra router Cisco IOS e client VPN Cisco con certificati Entrust, consultare il documento sulla configurazione di IPSec tra router Cisco IOS e client VPN Cisco con certificati Entrust.

Per ulteriori informazioni sulla configurazione di più autorità di certificazione di identità sui router Cisco IOS, consultare il documento sulla configurazione di più autorità di certificazione di identità sui router Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco PIX Firewall con software versione 6.3(3)
- Cisco VPN Client 4.0.3 su un PC con Windows XP
- Nel presente documento, come server CA viene utilizzato un server CA Microsoft Windows 2000.
- I certificati sul client VPN Cisco vengono archiviati utilizzando la smart card Aladdin e-Token.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Registrare e configurare il PIX

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurazioni

Nel documento vengono usate queste configurazioni.

- Registrazione certificato su PIX Firewall
- Configurazione firewall PIX

Registrazione certificato su 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
```

Configurazione firewall 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)#
```

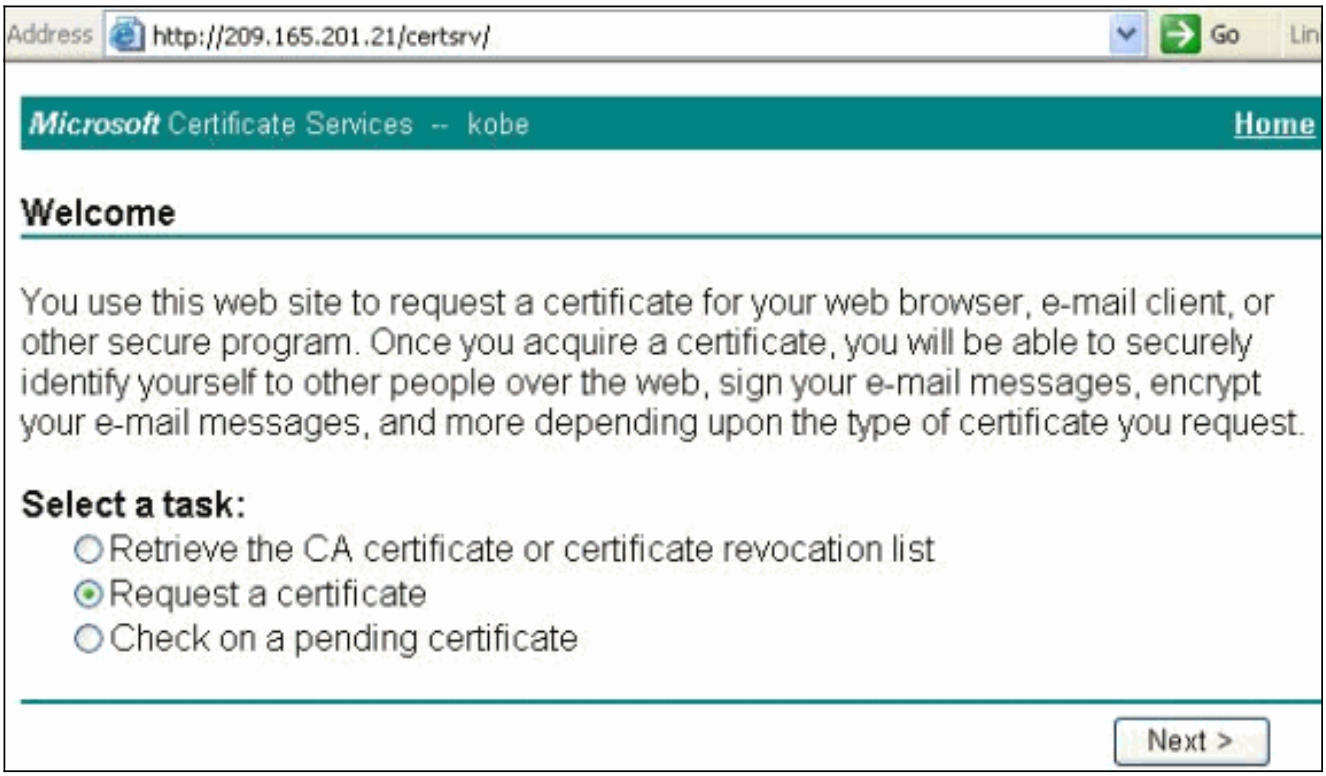
Registra certificati client VPN Cisco

Ricorda di installare tutti i driver e le utilità necessari forniti con il dispositivo Smartcard sul PC per poterlo usare con il client VPN Cisco.

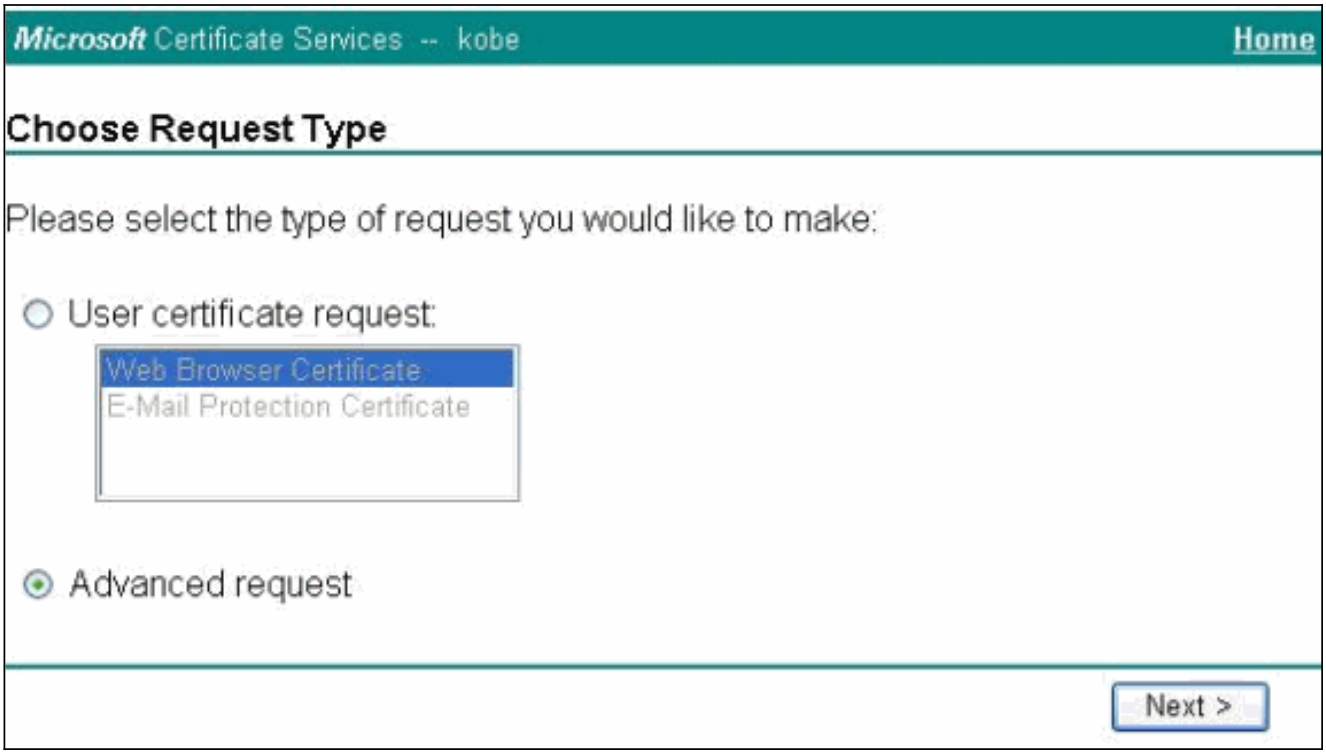
In questa procedura vengono illustrate le procedure utilizzate per registrare il client VPN Cisco per

i certificati MS. Il certificato è archiviato nell'archivio smart card Aladdin e-Token.

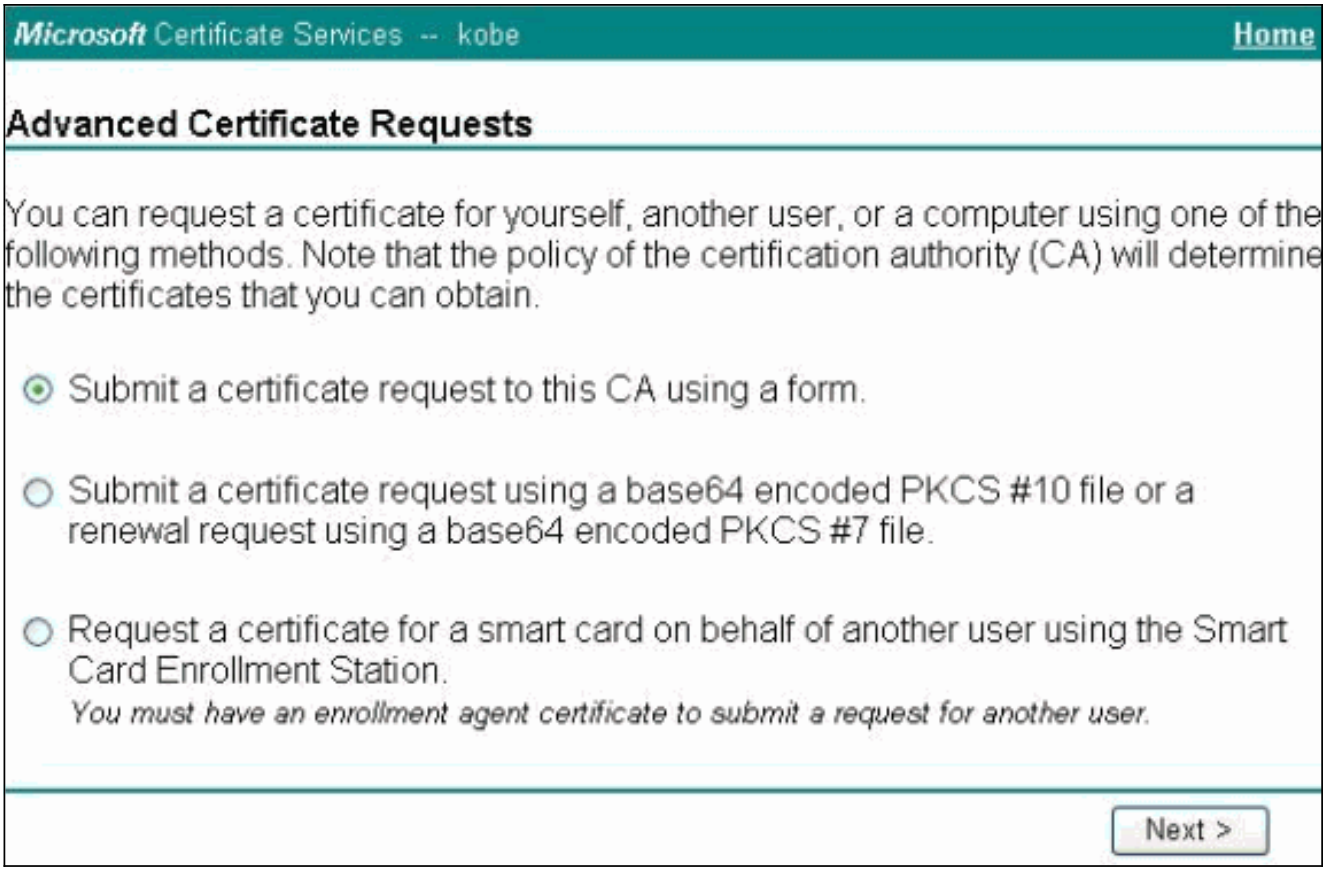
1. Avviare un browser e accedere alla pagina del server dei certificati (http://CAServeraddress/certsrv/, in questo esempio).
2. Selezionare **Richiedi certificato** e fare clic su **Avanti**.



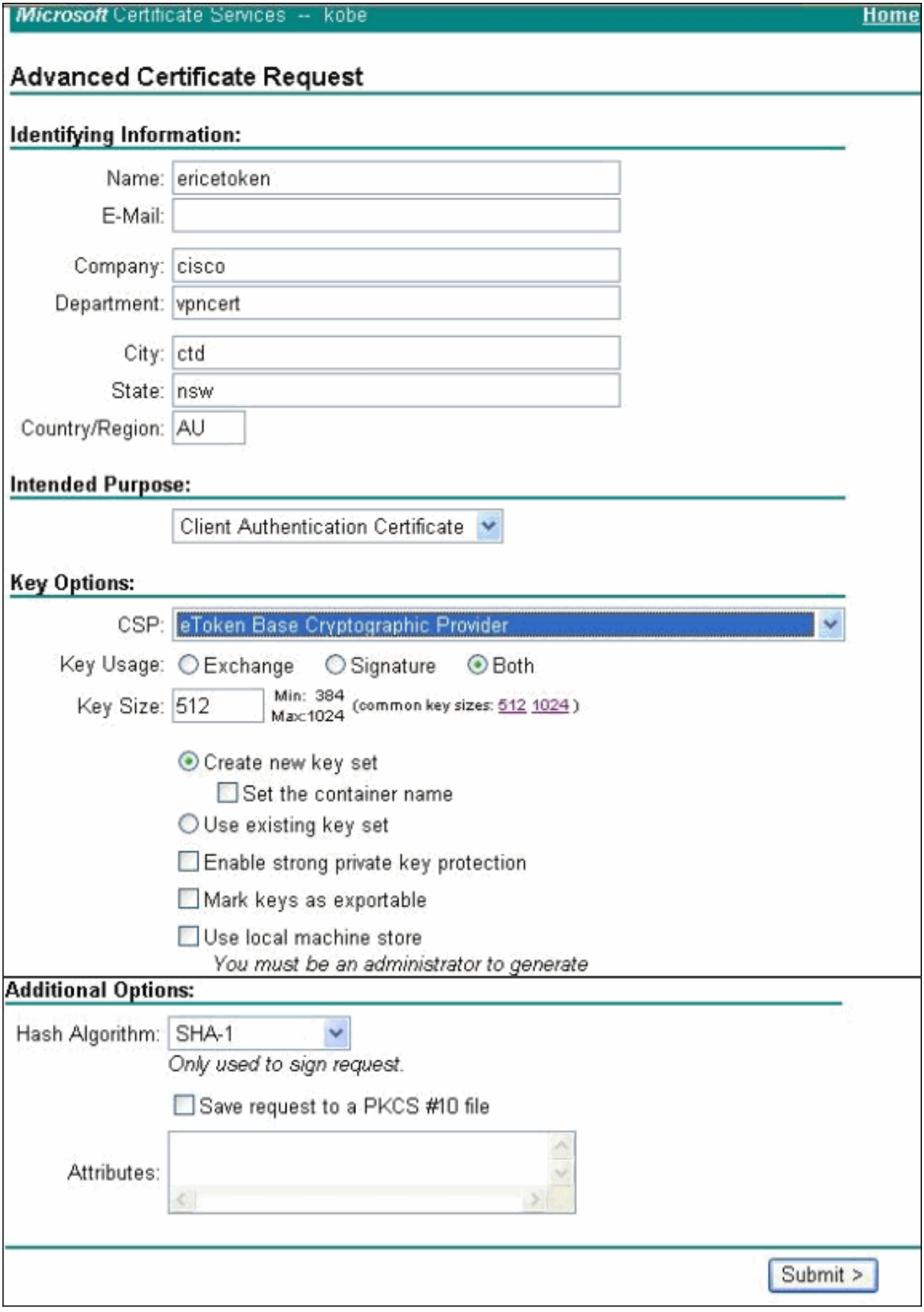
3. Nella finestra Scegli tipo di richiesta, selezionare **Richiesta avanzata** e fare clic su **Avanti**.



4. Selezionare **Invia una richiesta di certificato a questa CA utilizzando un modulo** e fare clic su **Avanti**.



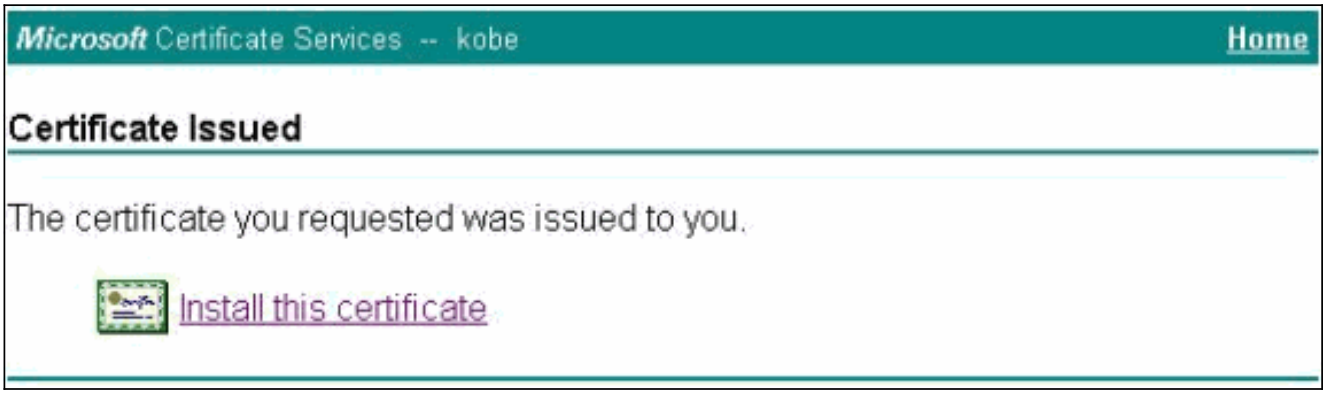
5. Compilare tutti gli elementi del modulo Richiesta avanzata di certificati.Accertarsi che il reparto o l'unità organizzativa corrisponda al nome del gruppo Cisco VPN Client, come configurato nel nome del gruppo VPN PIX. Selezionare il provider di servizi certificati (CSP) corretto per
l'installazione.



6. Selezionare **Sì** per continuare l'installazione quando viene visualizzato l'avviso Convalida script
potenziale.

7. La registrazione certificati richiama l'archivio eToken. Immettere la password e fare clic su OK.

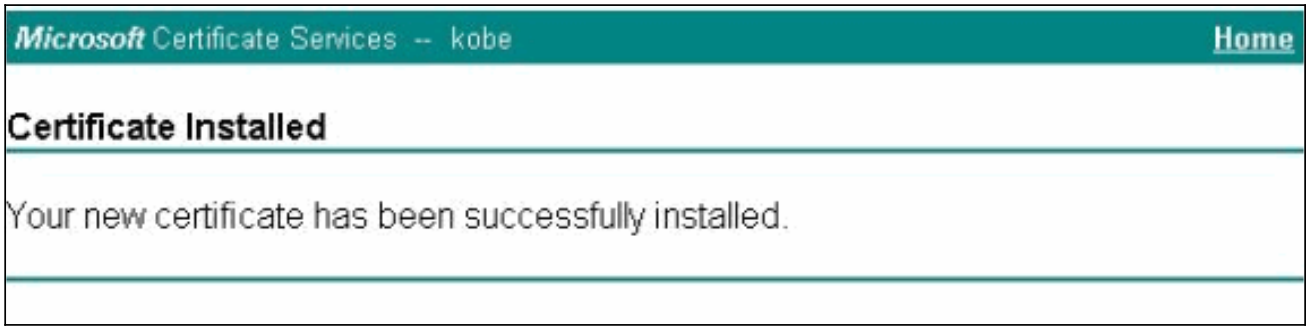
8. Fare clic su **Installa il certificato**.



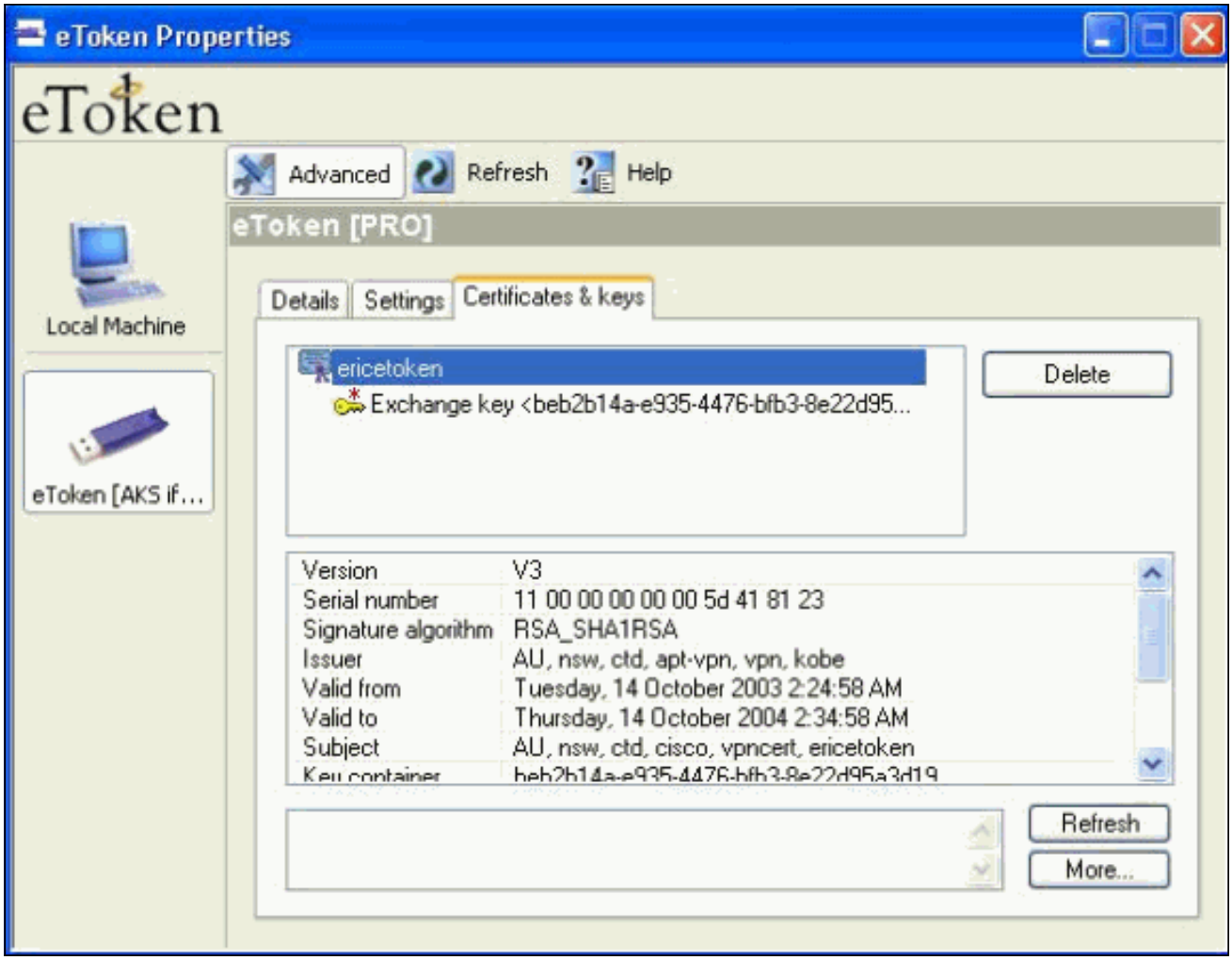
9. Selezionare **Sì** per continuare l'installazione quando viene visualizzato l'avviso Convalida script
potenziale.

10. Selezionare **Sì** per aggiungere il certificato radice all'archivio radice.

11. Viene visualizzata la finestra Certificato installato che conferma l'installazione.



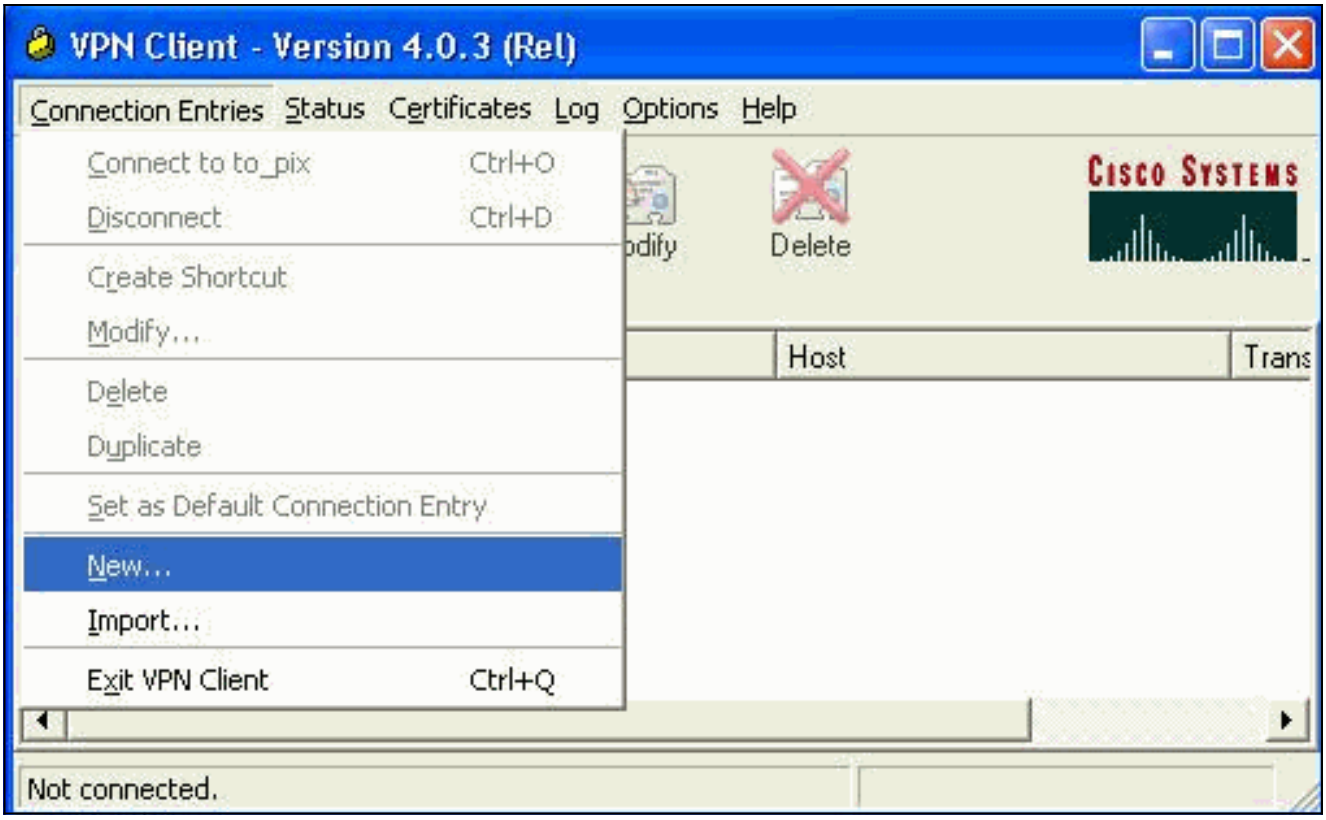
12. Per visualizzare il certificato archiviato nella smart card, utilizzare il visualizzatore applicazioni eToken.



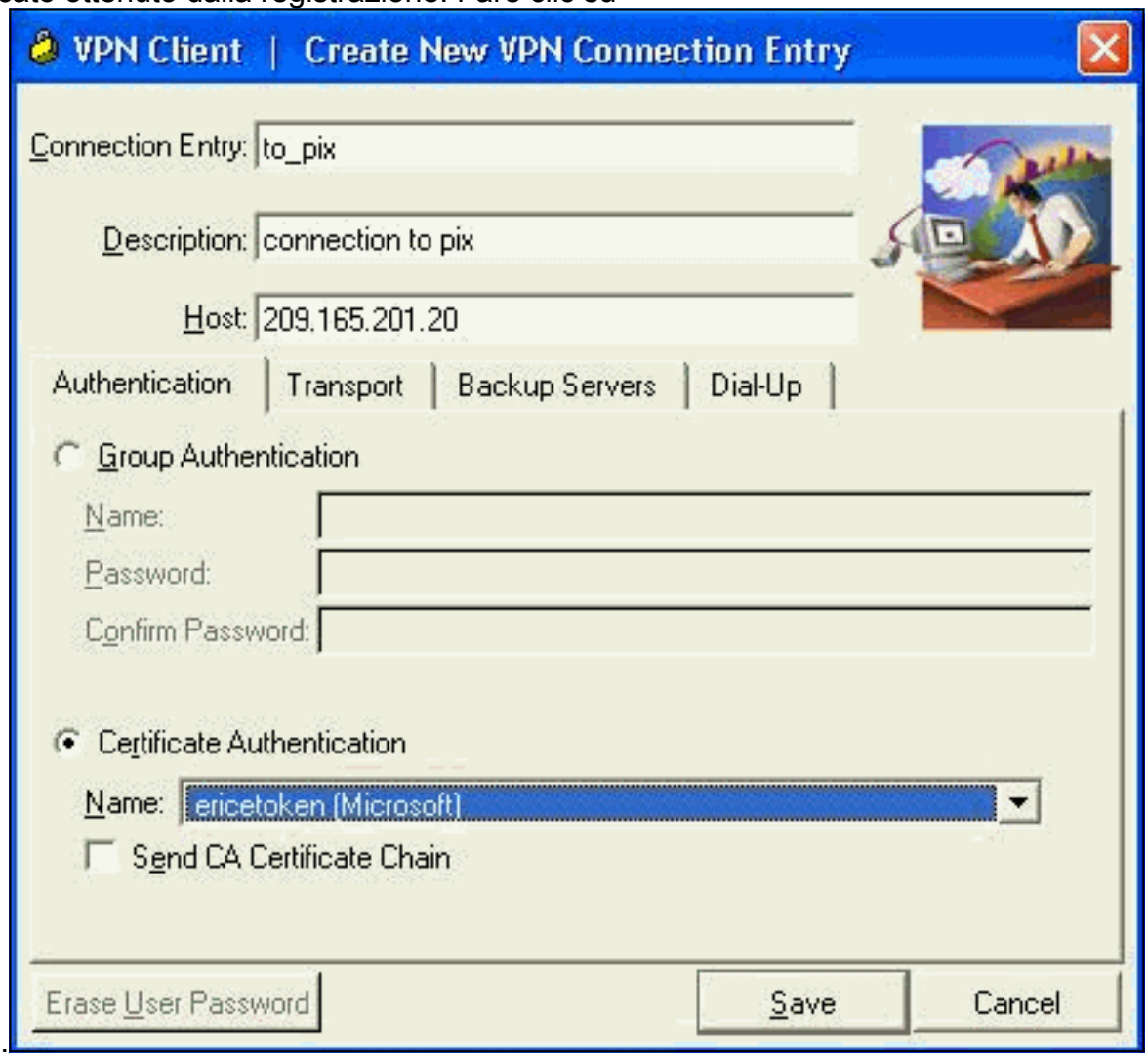
Configurare il client VPN Cisco per utilizzare il certificato per la connessione al PIX

In questa procedura vengono illustrate le procedure utilizzate per configurare il client VPN Cisco in modo che utilizzi il certificato per le connessioni PIX.

1. Avviare il client VPN Cisco. In Voci di connessione fare clic su **Nuovo** per creare una nuova connessione.



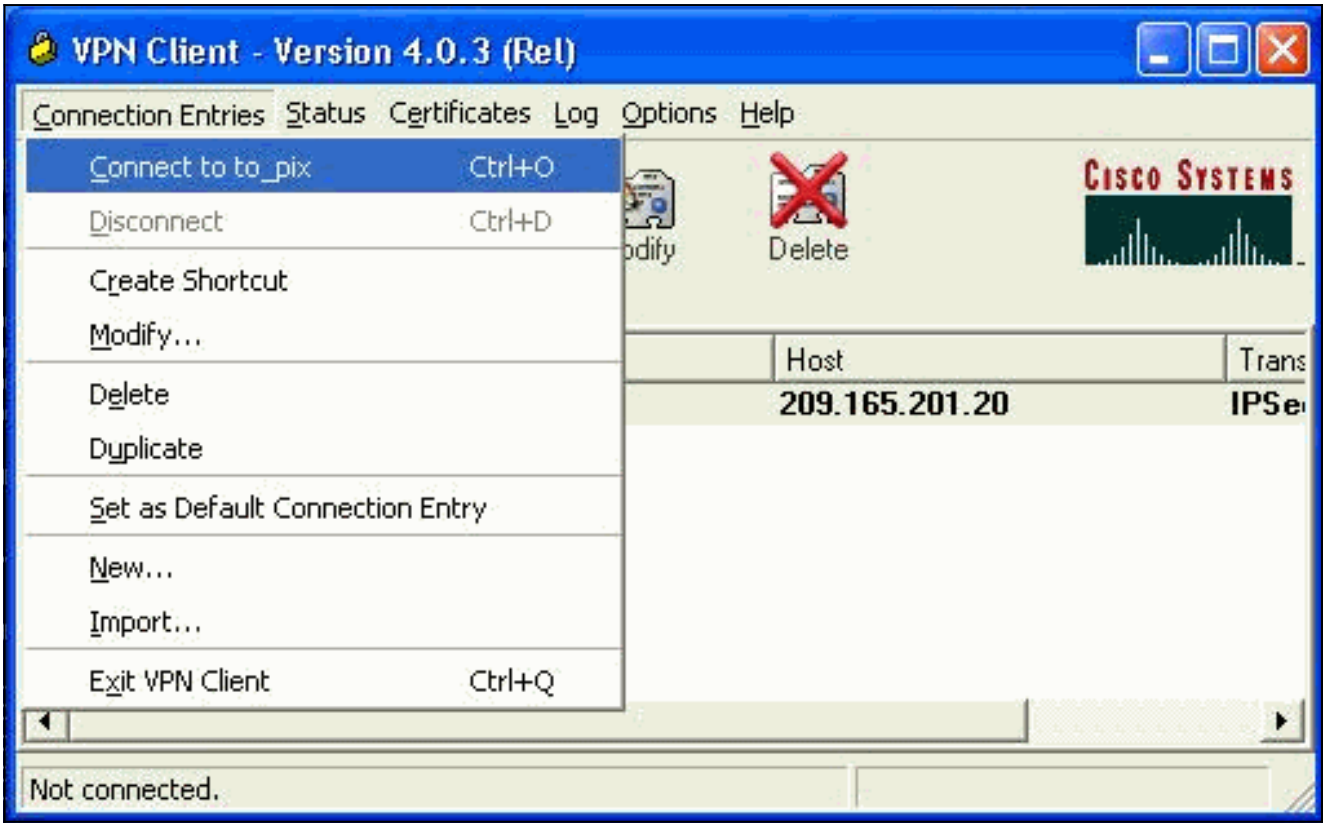
2. Completare i dettagli di connessione, specificare l'autenticazione certificato, selezionare il certificato ottenuto dalla registrazione. Fare clic su



Salva.

3. Per avviare la connessione del client VPN Cisco al PIX, selezionare la voce di connessione

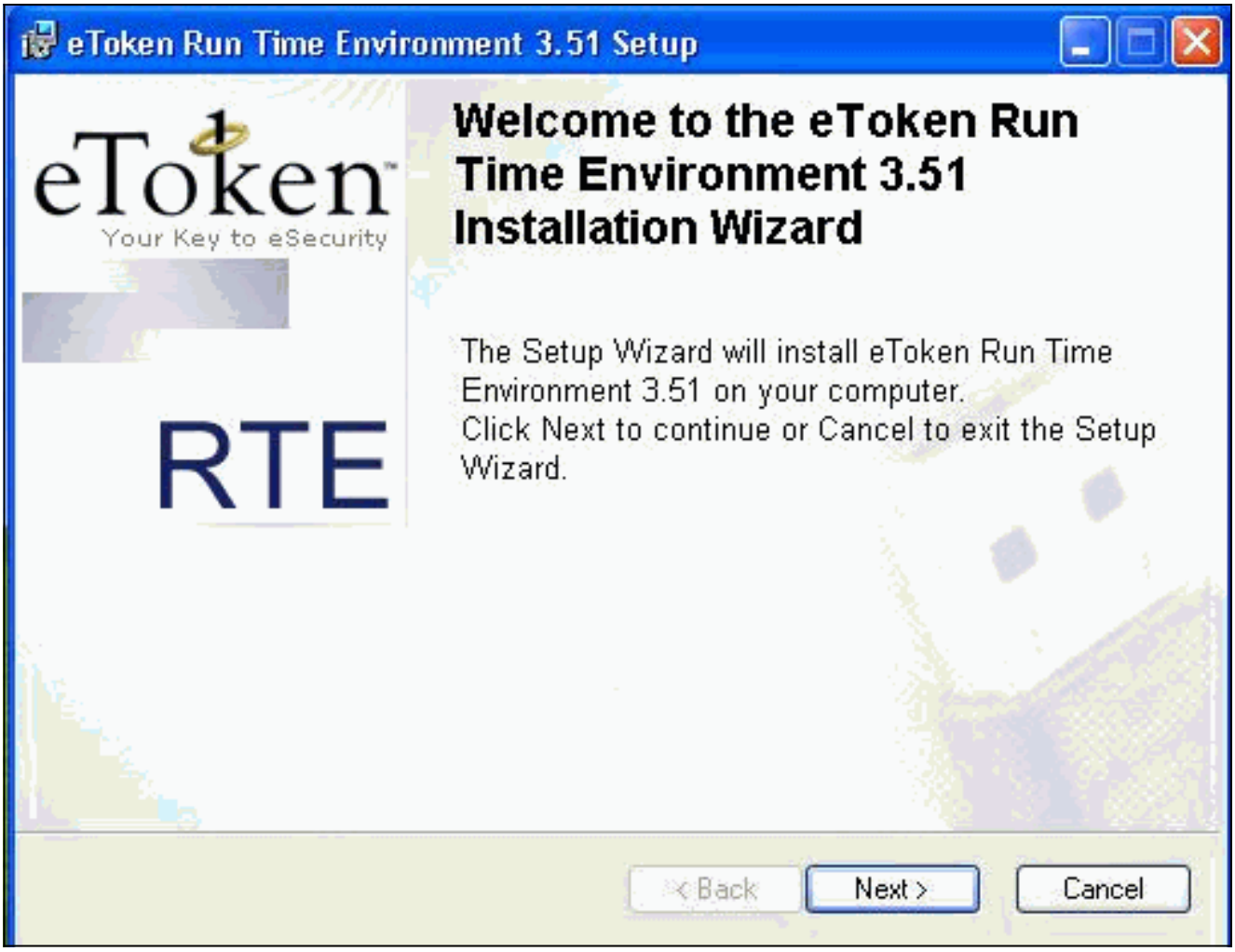
desiderata e fare clic su
Connetti.



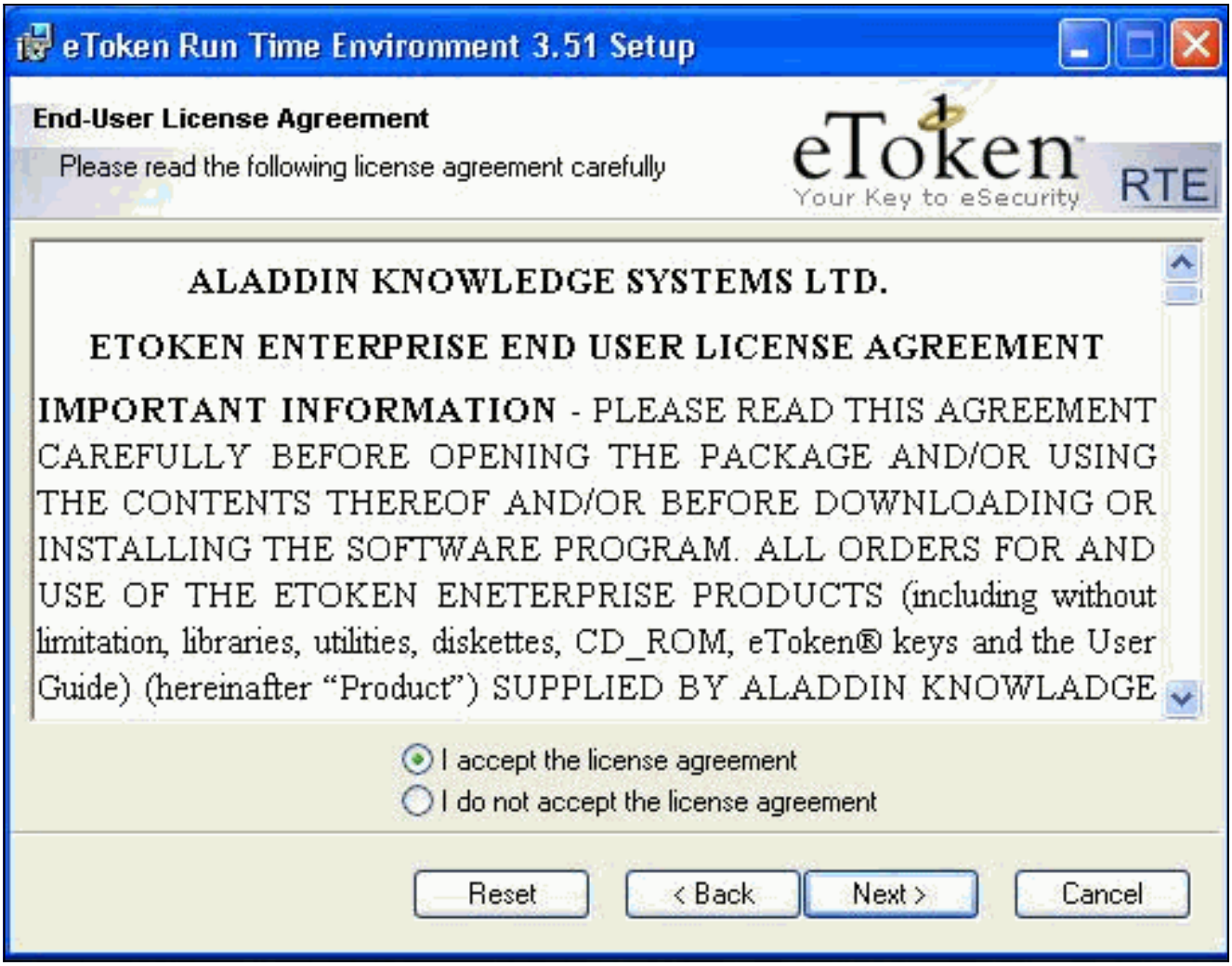
Installa driver per smart card eToken

In questa procedura viene illustrata l'installazione dei driver per smart card Aladdin eToken.

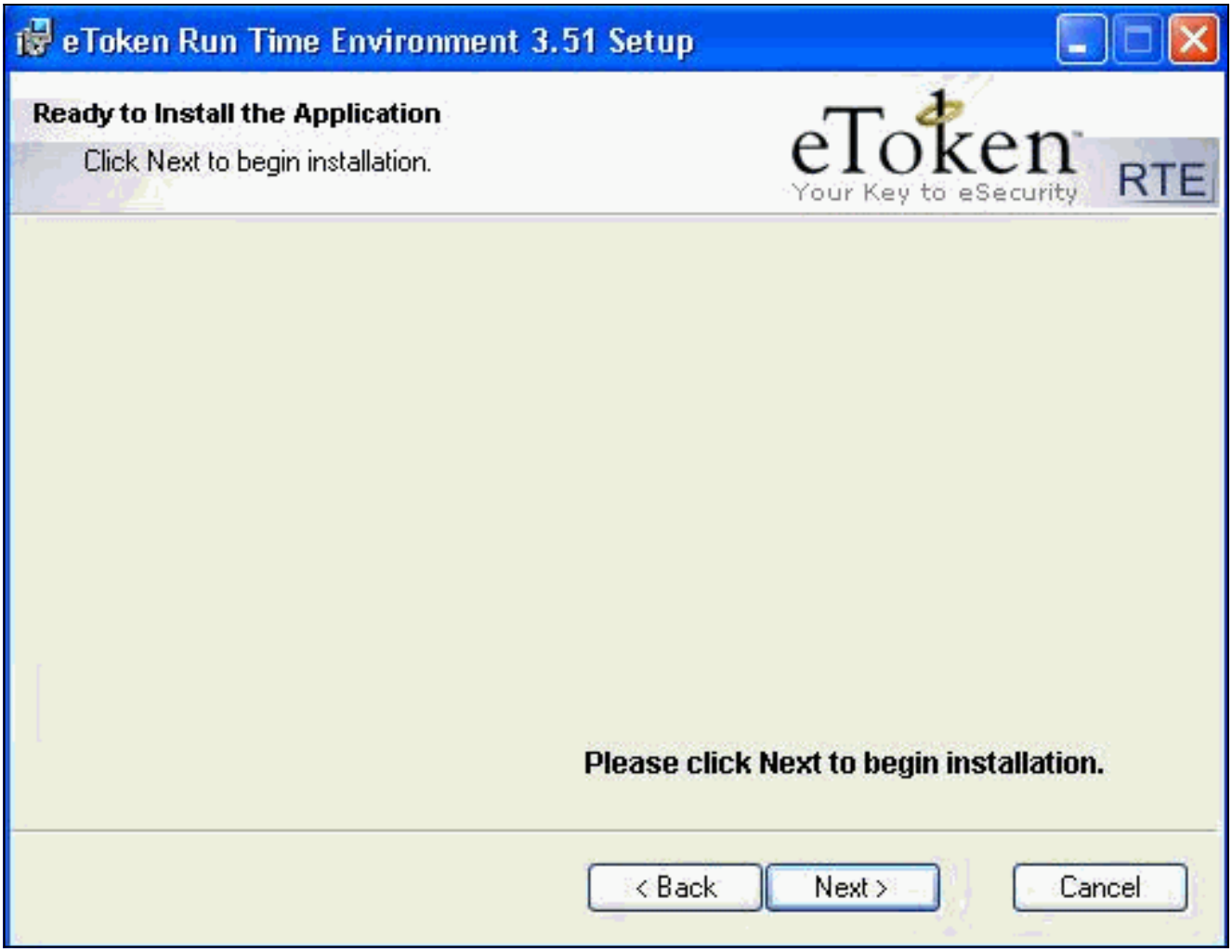
1. Aprire l'installazione guidata di eToken Run Time Environment 3.51.



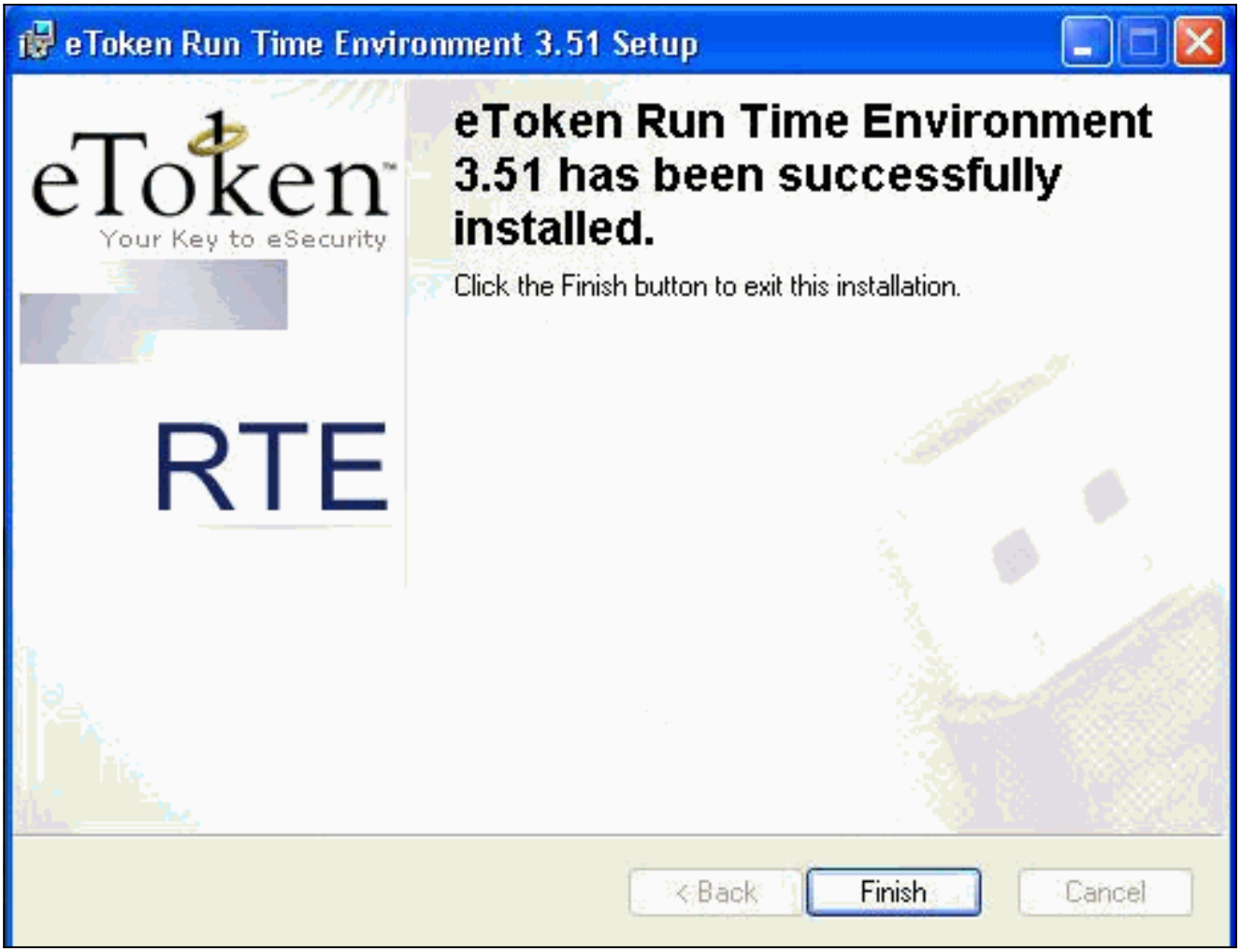
2. Accettare i termini del Contratto di Licenza e fare clic su **Avanti**.



3. Fare clic su **Installa**.



4. I driver eToken Smartcard sono stati installati. Per uscire dall'installazione guidata, fare clic su
Fine.



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza (SA) IKE (Internet Key Exchange) correnti in un 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
```

- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.

```
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:
```

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi di configurazione, consultare il documento sulla risoluzione dei problemi relativi al PIX per il passaggio del traffico di dati su un tunnel IPSec stabilito.

Informazioni correlate

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- RFC (Requests for Comments)
- Pagina di supporto per IPSec (IP Security Protocol)
- Pagina di supporto per Cisco VPN Client
- Pagina di supporto per i firewall PIX serie 500
- Supporto tecnico – Cisco Systems