Пример конфигурации IPSec между PIX и Cisco VPN Client, использующего сертификаты смарт-карт

Содержание

Введение

Этот документ демонстрирует, как настроить VPN-туннель IPSec между Межсетевым экраном PIX и Cisco VPN Client 4.0. x. Пример конфигурации в этом документе также выделяет процедуру регистрации центра сертификации (CA) и для маршрутизатора Cisco IOS® и для Cisco VPN Client, а также использования смарт-карты как хранилище сертификата.

См. IPSec Настройки Между маршрутизаторами Cisco IOS и Cisco VPN Client Использование Доверенных сертификатов для узнавания больше о IPSec Настройки между маршрутизаторами Cisco IOS и Cisco VPN Client с помощью Доверенных сертификатов.

См. Центры сертификации со множественной идентификацией Настройки на маршрутизаторах Cisco IOS для узнавания больше о Центрах сертификации со множественной идентификацией Настройки на маршрутизаторах Cisco IOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Межсетевой экран Cisco PIX, работающий под управлением ПО версии 6.3 (3)
- Cisco VPN Client 4.0.3 на ПК, выполняющем Windows XP
- Microsoft Windows 2000 CA сервер используется в этом документе в качестве сервера CA.
- Сертификаты на Cisco VPN Client сохранены с помощью смарт-карты e-Token Аладдина.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Зарегистрируйте и настройте PIX

В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Примечание: Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд (только для зарегистрированных клиентов).

Конфигурации

Эти конфигурации используются в данном документе.

- Хранилище сертификатов на межсетевом экране PIX
- Конфигурация межсетевого экрана PIX

Хранилище сертификатов на межсетевом экране 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
```

Конфигурация межсетевого экрана 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)#
```

Зарегистрируйте сертификаты клиента Cisco VPN

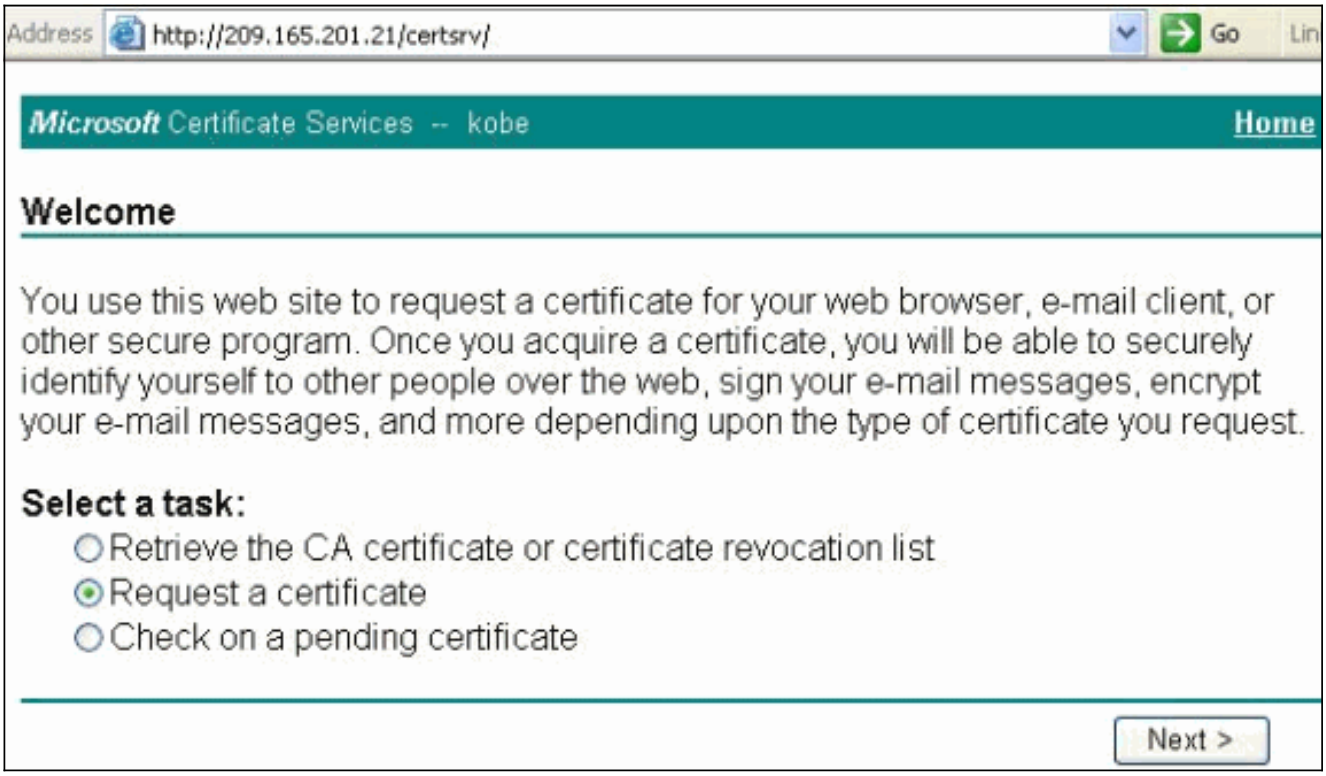
Не забудьте устанавливать все необходимые драйверы и утилиты, которые идут с Устройством смарт-карты на ПК, который будет использоваться с Cisco VPN Client.

Эти шаги демонстрируют, что процедуры использовали регистрировать Cisco VPN Client на сертификаты MS. Сертификат сохранен на хранилище смарт-карты e-Token Аладдина.

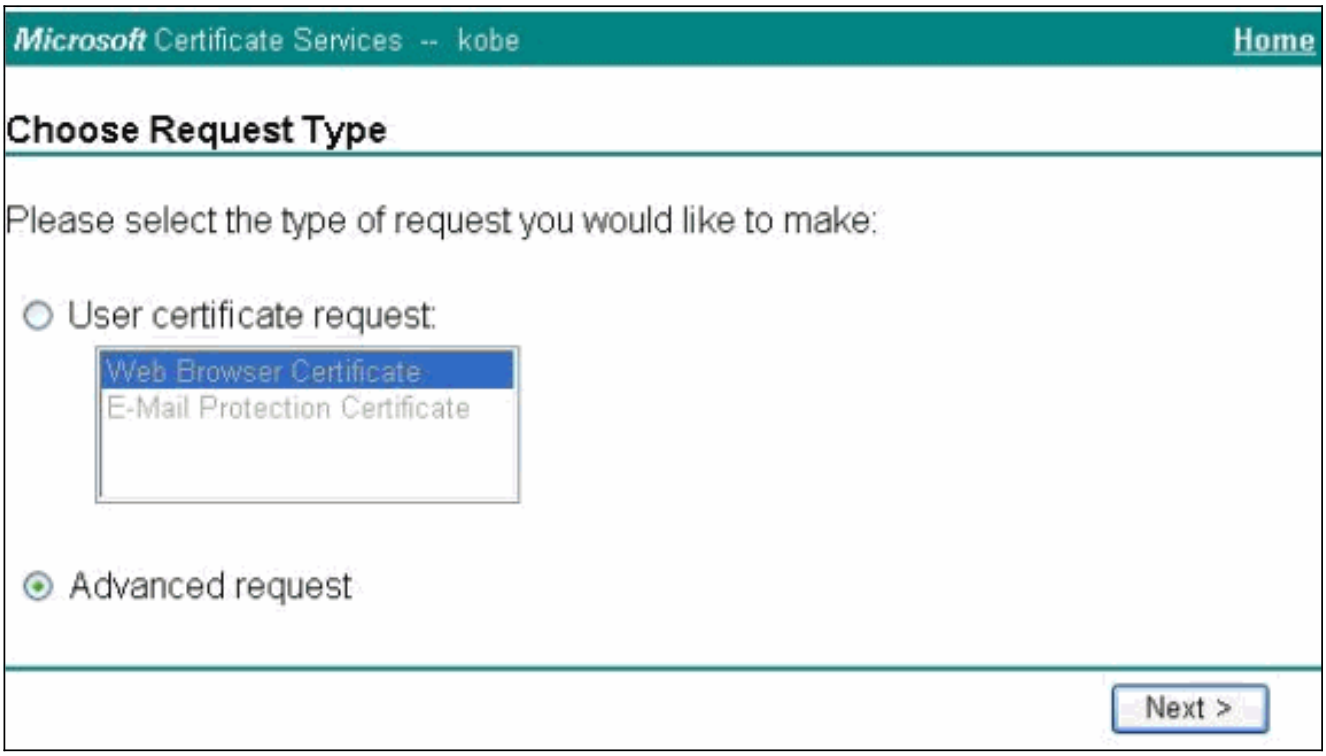
1. Запустите браузер и перейдите к странице сервера сертификатов

(http://CAServeraddress/certsrv / в данном примере).

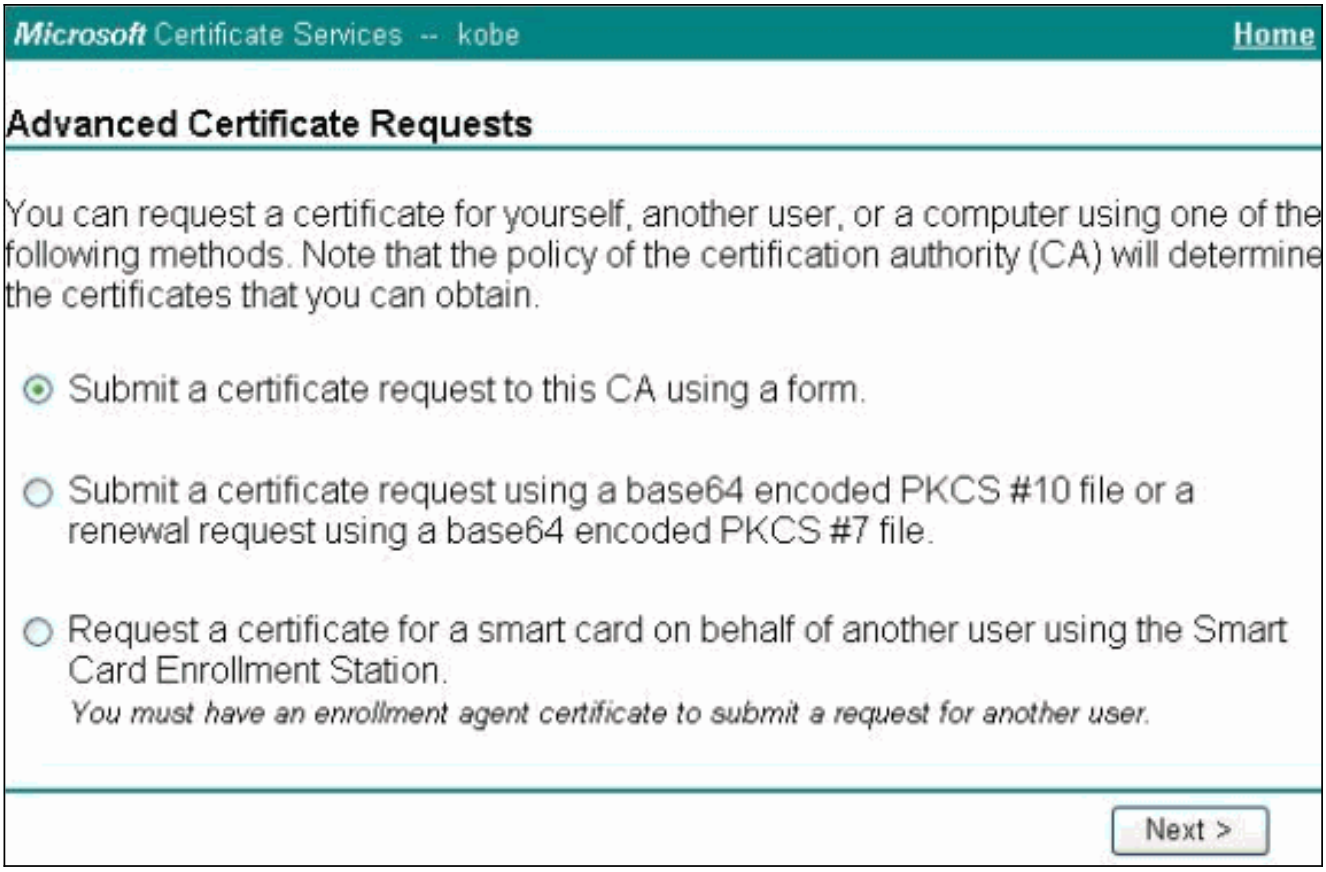
2. Выберите **Request сертификат** и нажмите **Next**.



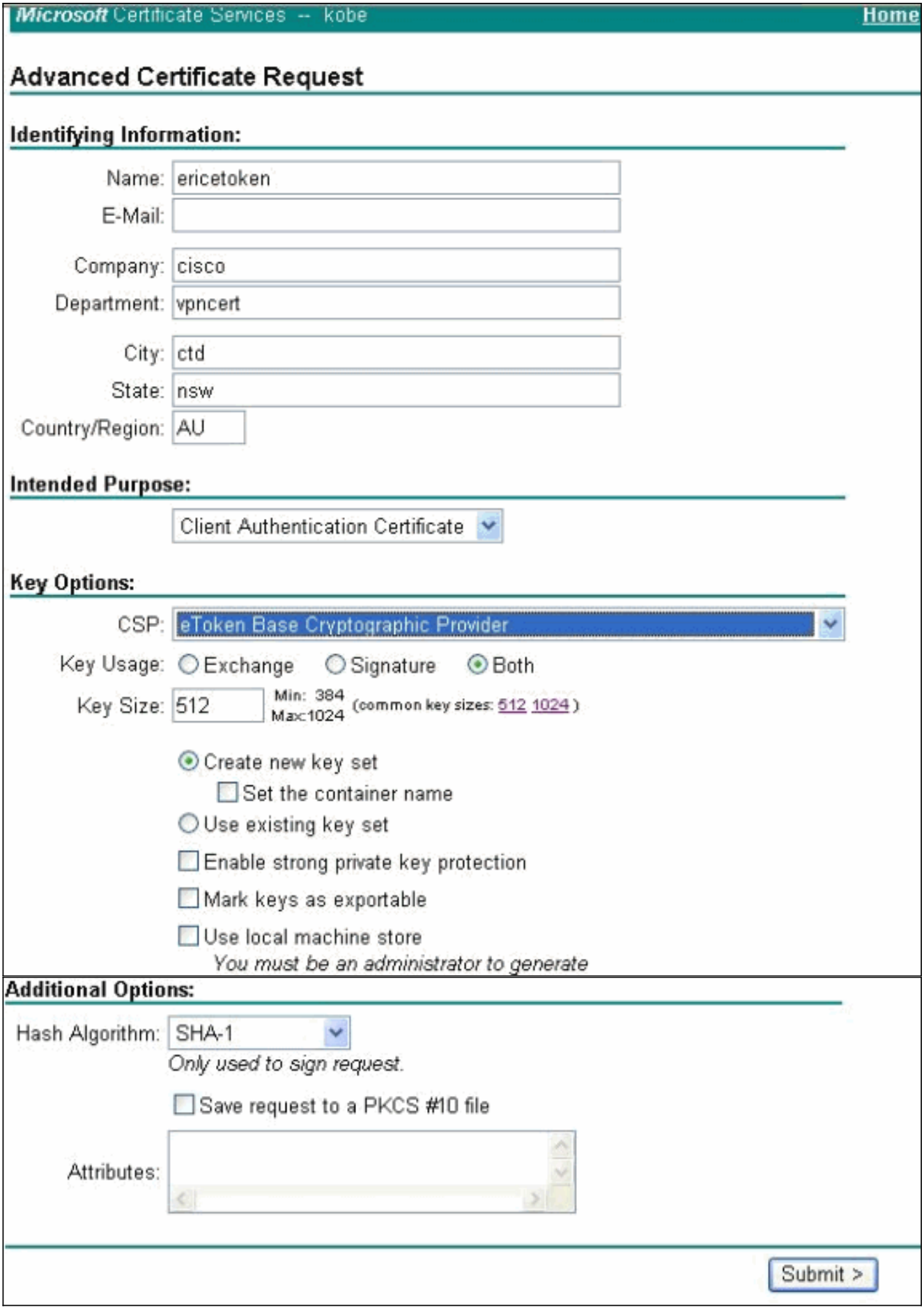
3. В окне Choose Request Type выберите **Расширенный запрос** и нажмите **Next**.



4. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы** и нажмите **Next**.



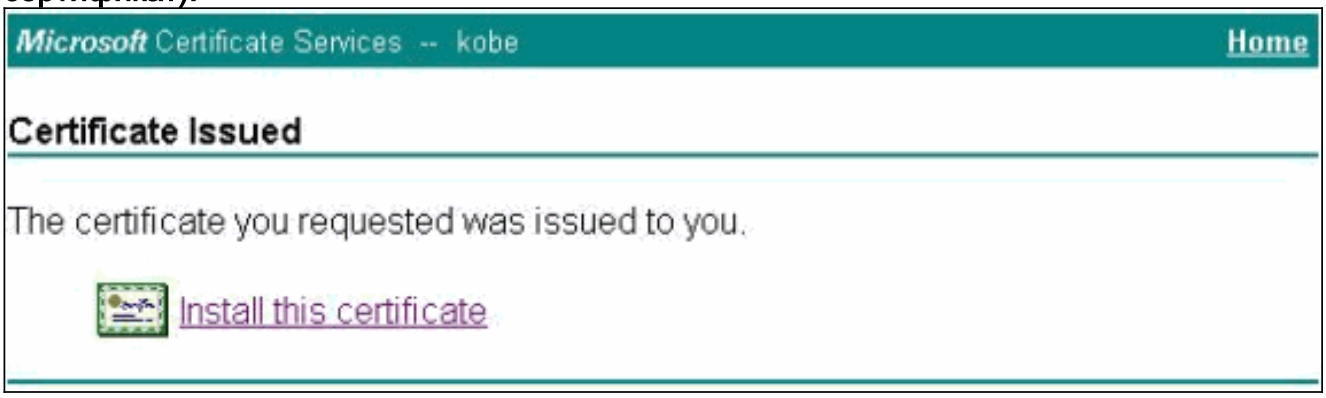
5. Заполните все элементы на Усовершенствованной Форме запроса сертификата.Убедитесь, что Отдел или подразделение (OU) соответствуют имени группы Cisco VPN Client, согласно конфигурации в PIX vpngroup название. Выберите корректный Certificate Service Provider (CSP), соответствующий вашей настройке.



6. Выберите **Yes** для продолжения установки, когда вы получаете Потенциальное предупреждение Проверки
Сценариев.

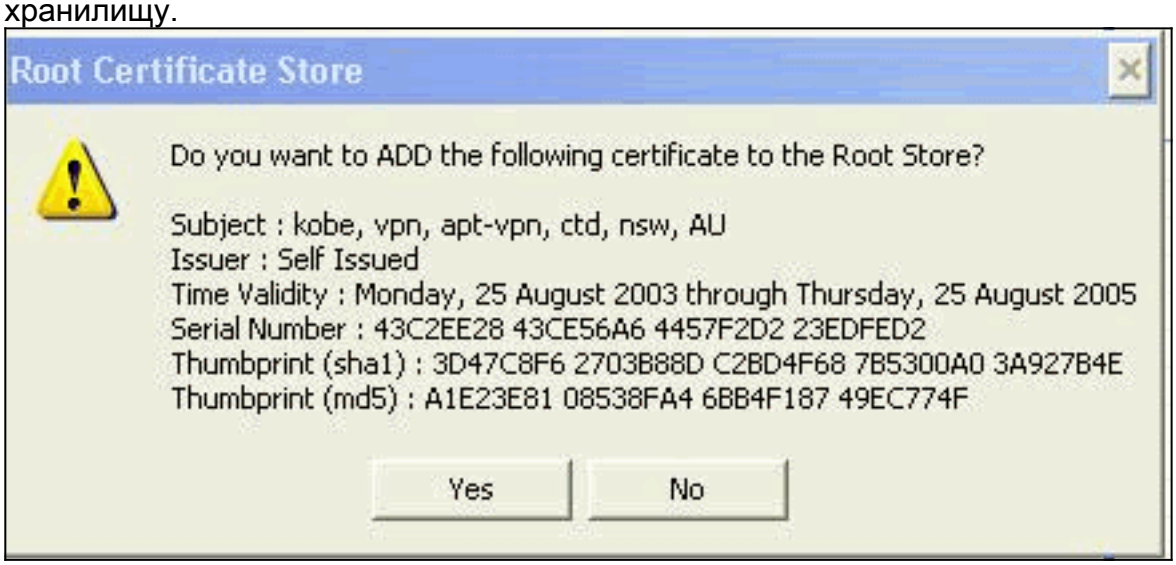
7. Хранилище сертификатов вызывает хранилище eToken. Введите пароль и нажмите OK.

8. **Нажмите кнопку Install this certificate (Установить этот сертификат).**

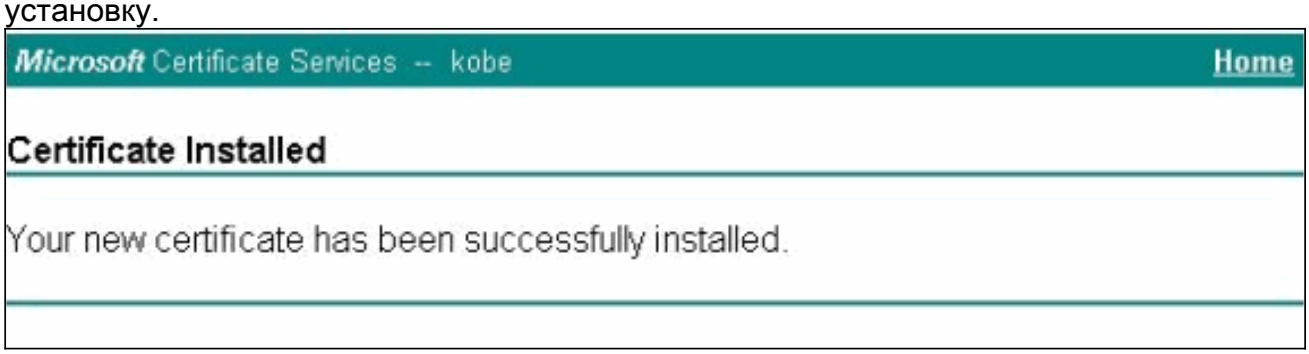


9. Выберите **Yes** для продолжения установки, когда вы получаете Потенциальное предупреждение Проверки
Сценариев.

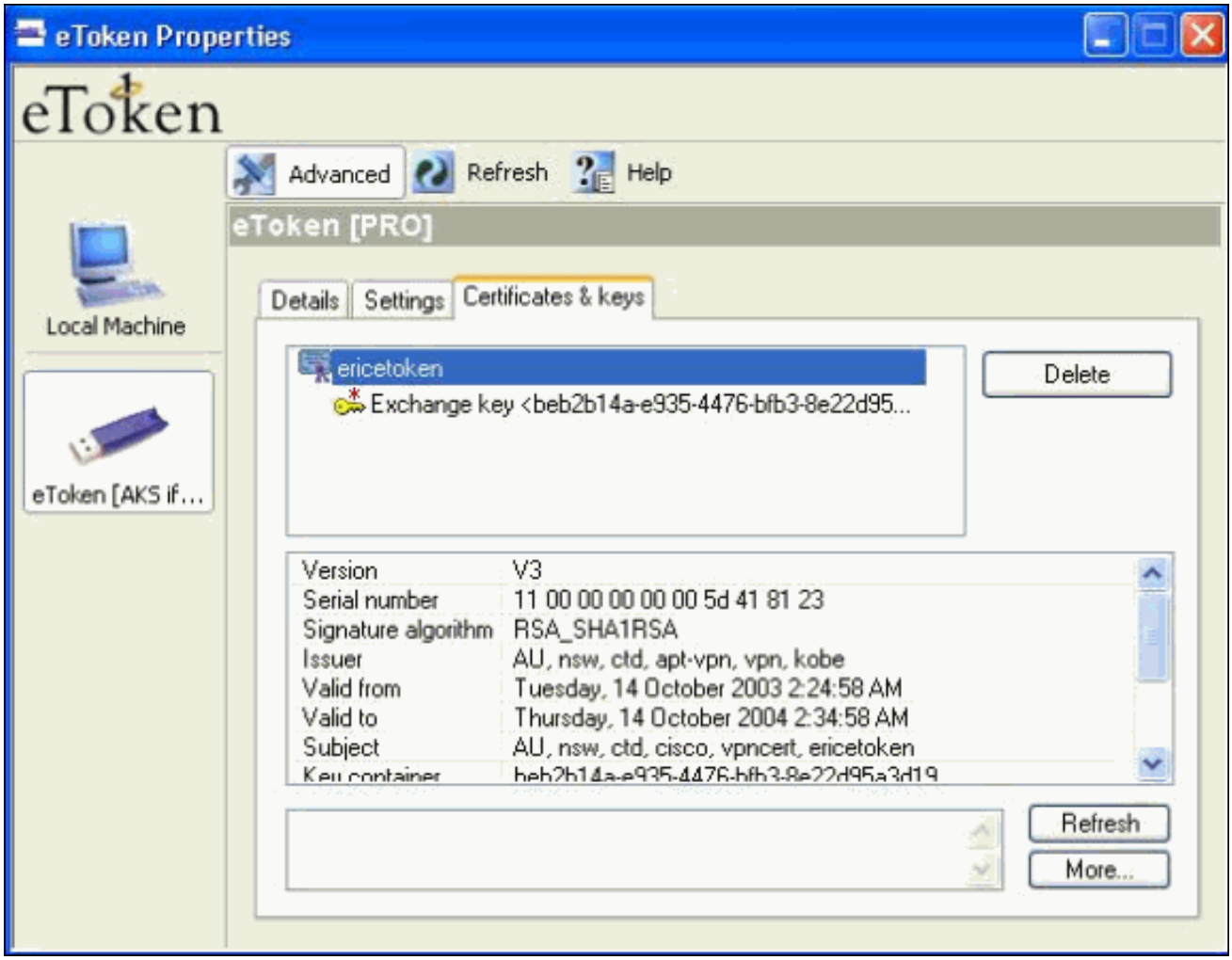
10. Выберите **Yes** для добавления корневого сертификата к Корневому хранилищу.



11. Окно Certificate Installed появляется и подтверждает успешную установку.



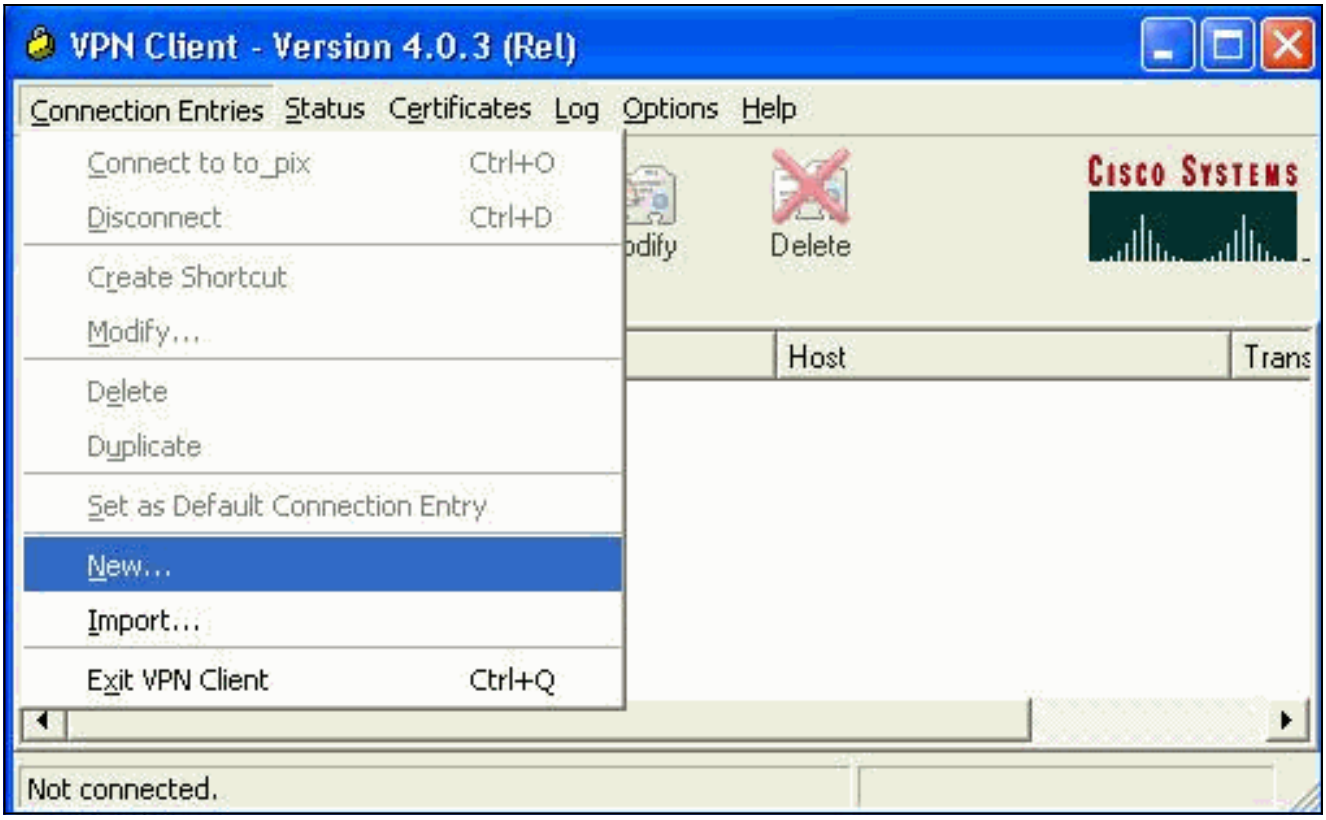
12. Используйте средство просмотра для приложения eToken для просмотра сертификата, сохраненного на смарт-карте.



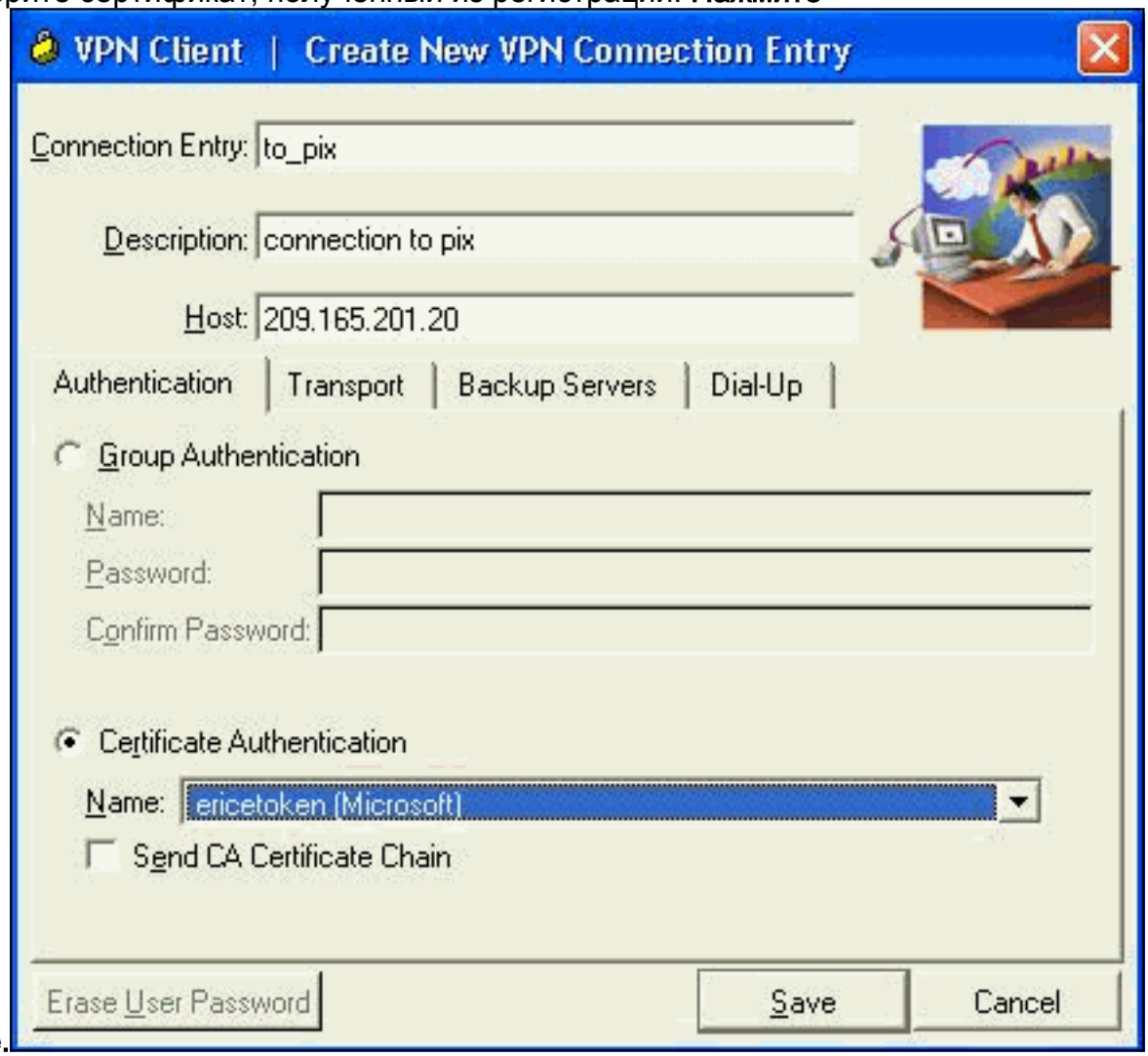
Настройте Cisco VPN Client для Использования Сертификата для Соединения с PIX

Эти шаги демонстрируют, что процедуры использовали настраивать Cisco VPN Client для использования сертификата для соединений PIX.

1. Запустите Cisco VPN Client. При Соединениях нажимают **New** для создания нового соединения.



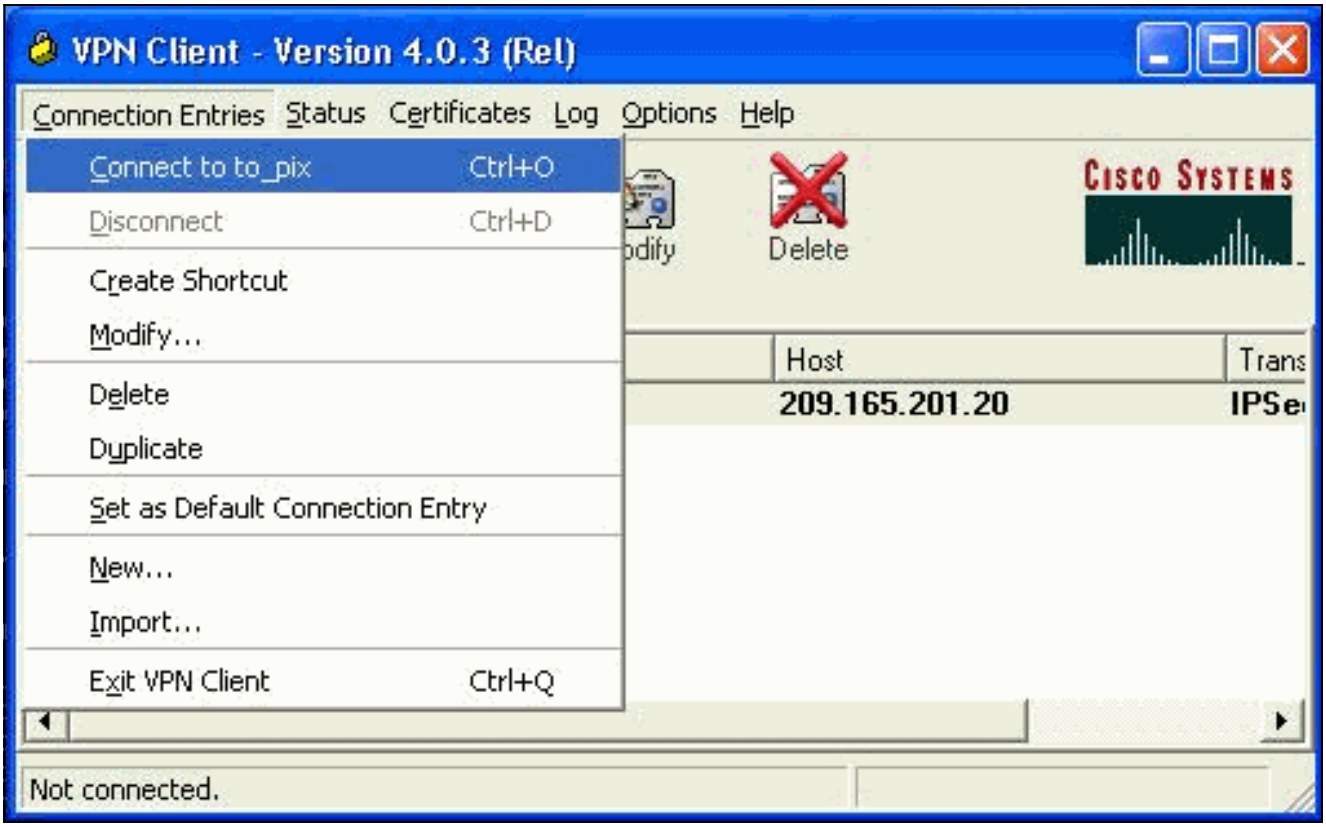
2. Завершите подробность соединения, задайте Проверку подлинности сертификата, выберите сертификат, полученный из регистрации. **Нажмите**



Save.

3. Для начала соединения Cisco VPN Client с PIX выберите желаемое Соединение и

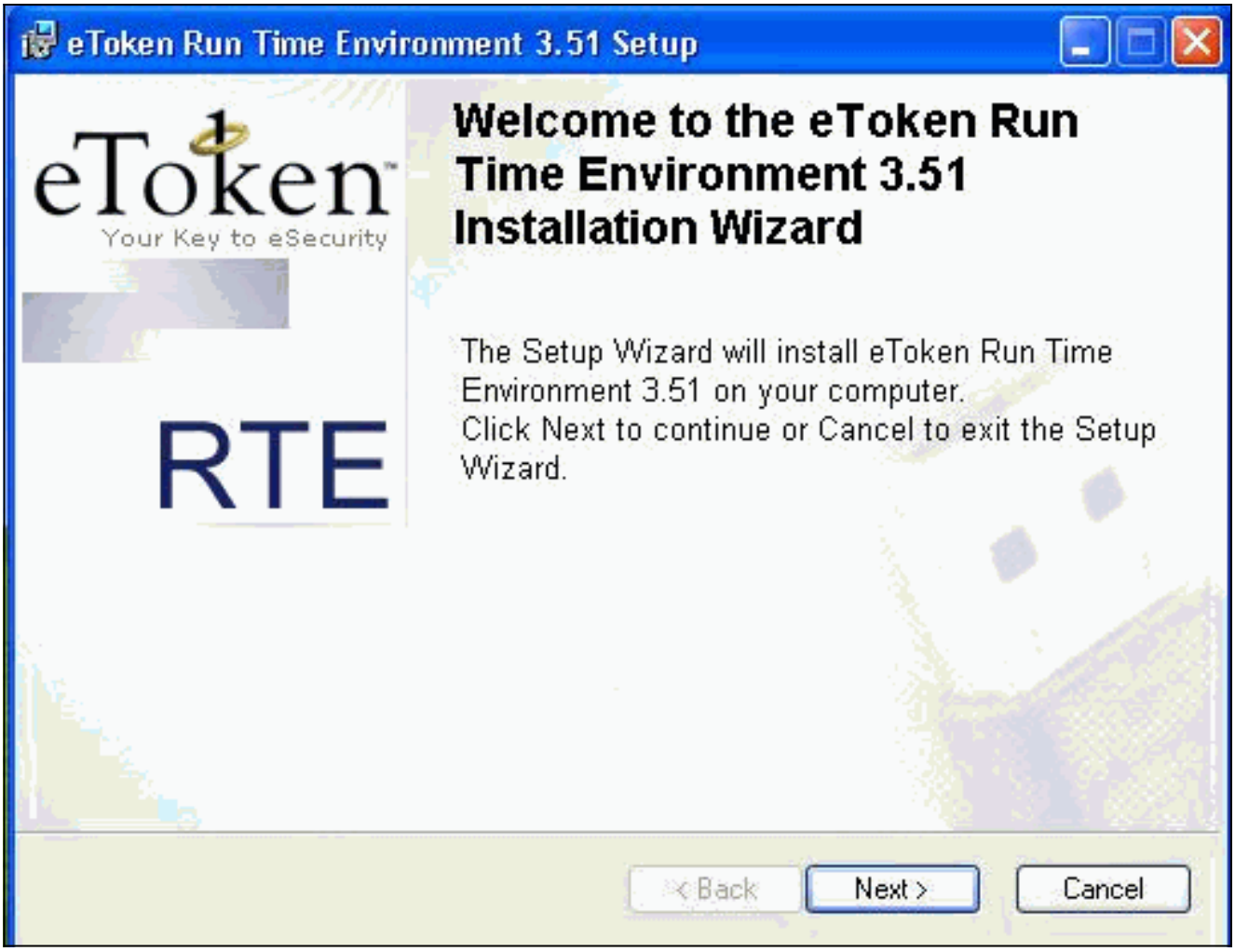
нажмите
Connect.



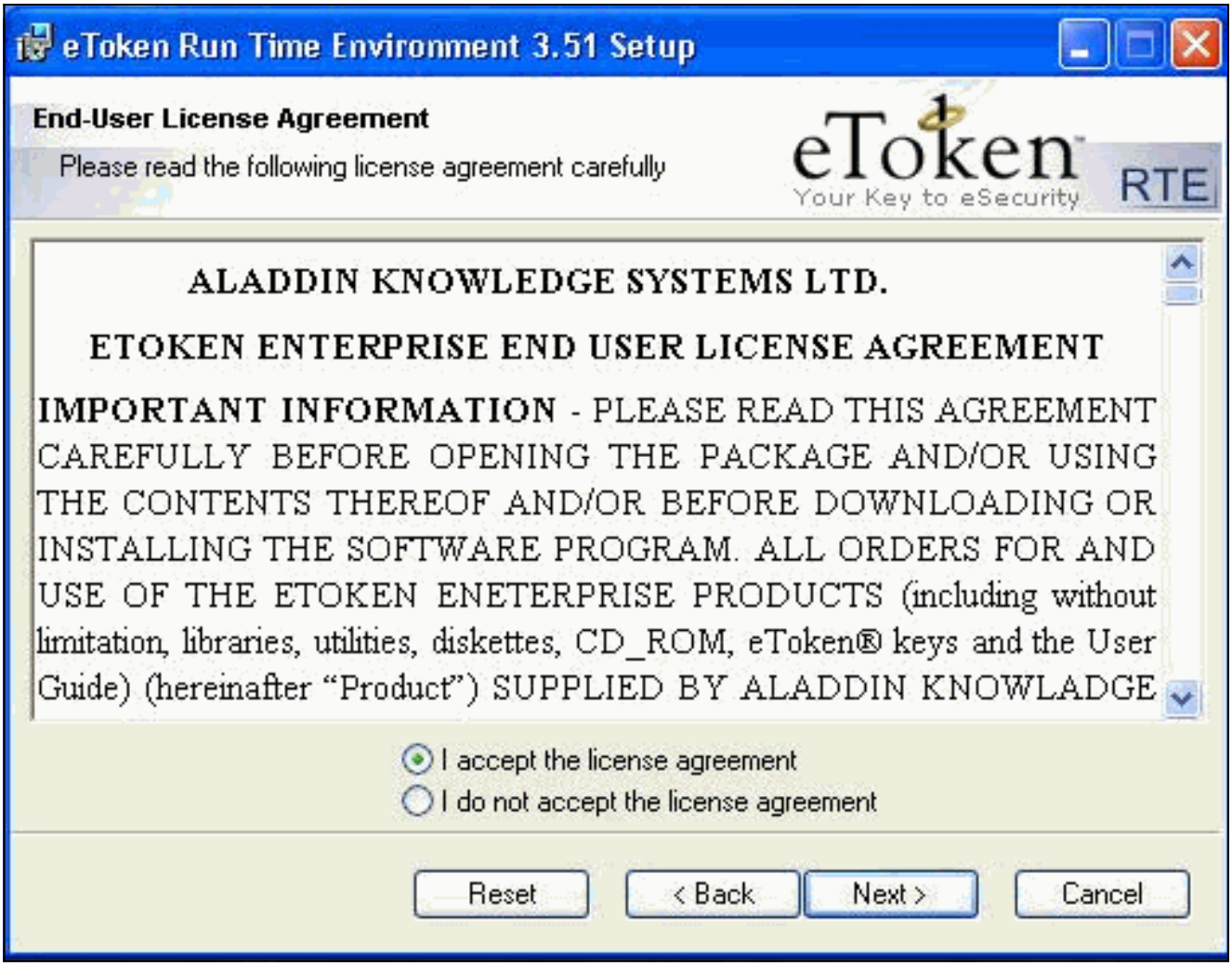
Установите драйверы смарт-карты etoken

Эти шаги демонстрируют установку Драйверов Aladdin eToken Smartcard.

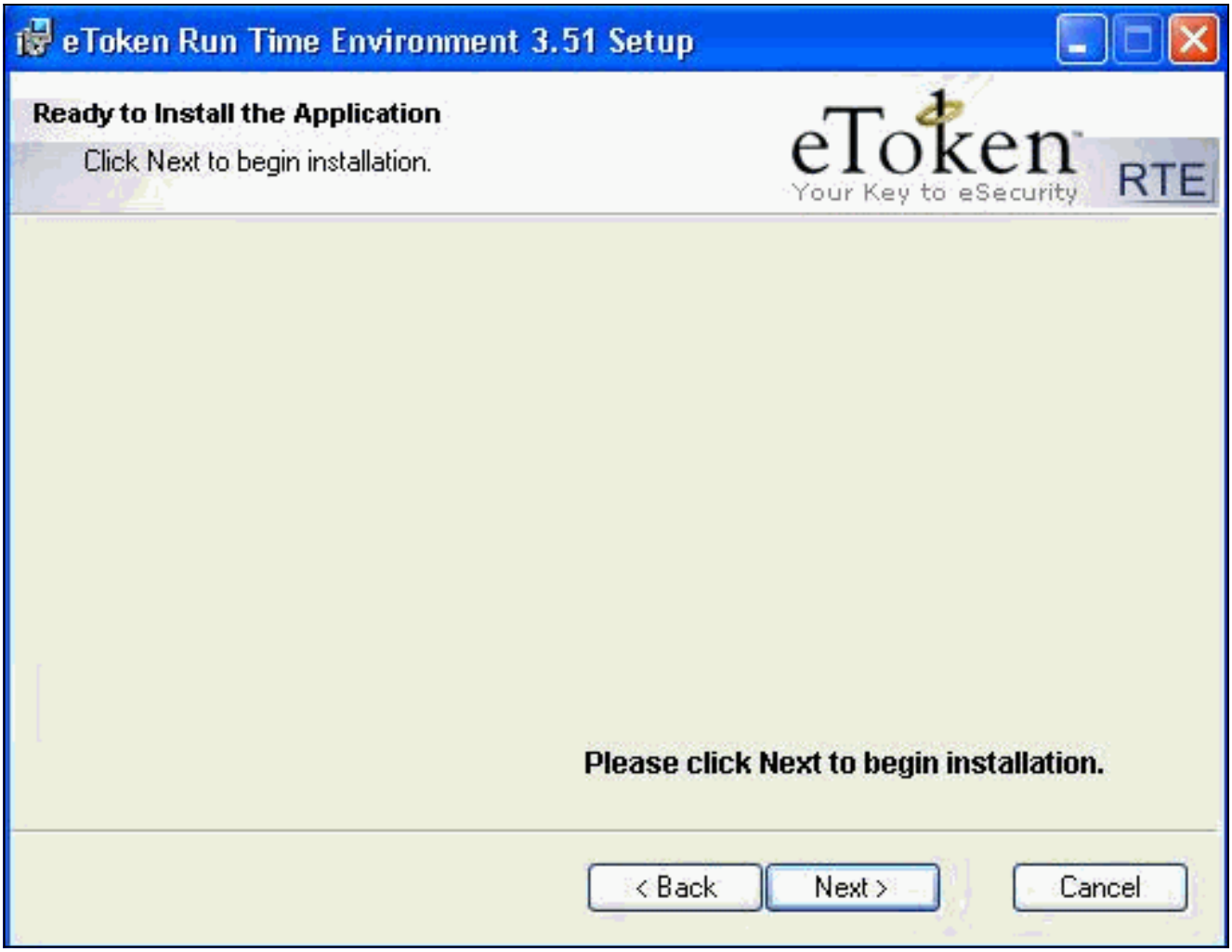
1. Откройте Среду выполнения eToken 3.51 мастера настройки.



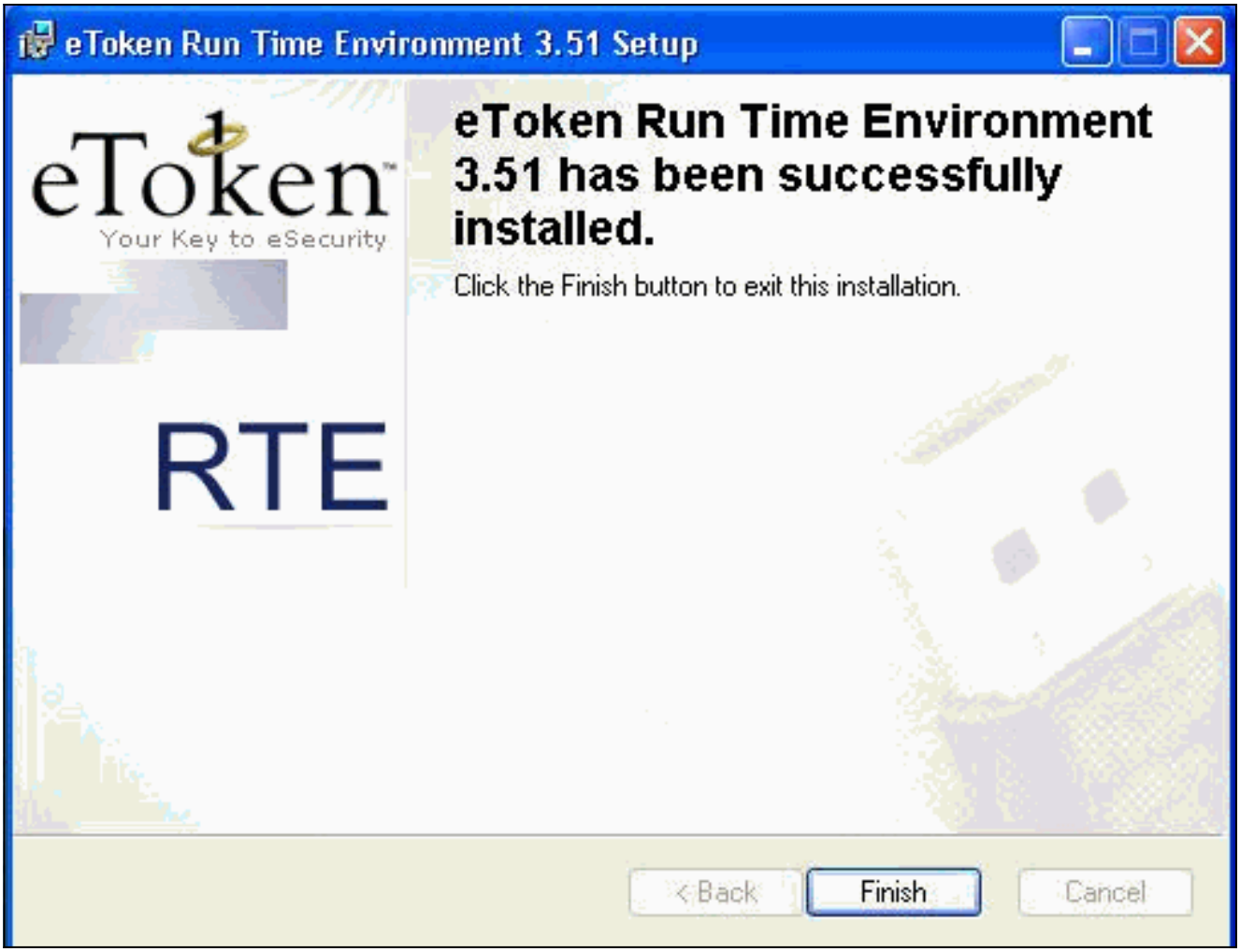
2. Примите сроки Лицензионного соглашения и нажмите **Next**.



3. Нажмите кнопку Install (Установить).



4. Драйверы смарт-карты etoken теперь установлены. Нажмите **Finish** для выхода из мастера
настройки.



Проверка

В данном разделе содержатся сведения для проверки правильности конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show crypto isakmp sa — показывает все текущие ассоциации безопасности протокола IKE (Internet Key Exchange, обмен ключами в Интернете) на одноранговом узле.**
```
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** параметры настройки, используемые текущими сопоставлениями безопасности.
```
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:
```

Устранение неполадок

См. Устранение проблем PIX для Передачи Трафика данных Установке туннеля IPSec для получения дополнительной информации об устранении проблем этой конфигурации.

Дополнительные сведения

- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Запросы комментариев (RFC)
- Страница поддержки IPSec (протокола IP-безопасности)
- Страница поддержки Cisco VPN Client
- Страница поддержки межсетевых экранов PIX серии 500
- Техническая поддержка - Cisco Systems