

スマート カード証明書を使用した PIX と Cisco VPN クライアント間の IPSec 設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[PIX を登録し、設定して下さい](#)

[設定](#)

[Cisco VPN クライアント 認証を登録して下さい](#)

[PIX への接続のために認証を使用するために Cisco VPN Client を設定して下さい](#)

[eToken Smartcard ドライバーをインストールして下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料に PIX ファイアウォールと Cisco VPN Client 4.0.x 間の IPSec VPN トンネルを設定する方法を示されています。この資料の設定例はまた認証 ストレージとして Cisco IOS® ルータおよび Cisco VPN Client 両方のための Certification Authority (CA) 登録プロシージャ、またスマートカードの使用を強調表示します。

委託認証を使用して Cisco IOS ルータと Cisco VPN Client 間の IPSec の設定について詳細を学ぶために [Entrust 証明書を使用する Cisco IOS ルータと Cisco VPN クライアント間の IPSec の設定を参照して下さい](#)。

複数ID認証権限 IOS ルータを on Cisco 設定することについて詳細を学ぶために [Cisco IOS ルータでの複数 ID 認証局の設定を参照して下さい](#)。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェアバージョンを実行する Cisco PIX Firewall 6.3(3)
- Windows XP を実行する PC の Cisco VPN Client 4.0.3
- Microsoft Windows 2000 CA サーバは CA サーバとしてこの資料で使用されます。
- Cisco VPN Client の認証は [Aladdin eToken](#)スマートカードを使用して保存されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

PIX を登録し、設定して下さい

このセクションでは、このドキュメントで説明されている機能を設定するための情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

設定

このドキュメントでは、次の設定を使用します。

- [PIXファイアウォールの証明書登録](#)
- [PIX Firewall の設定](#)

PIXファイアウォールの証明書登録

```
!--- 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
```

PIX ファイアウォールの設定

```
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
```

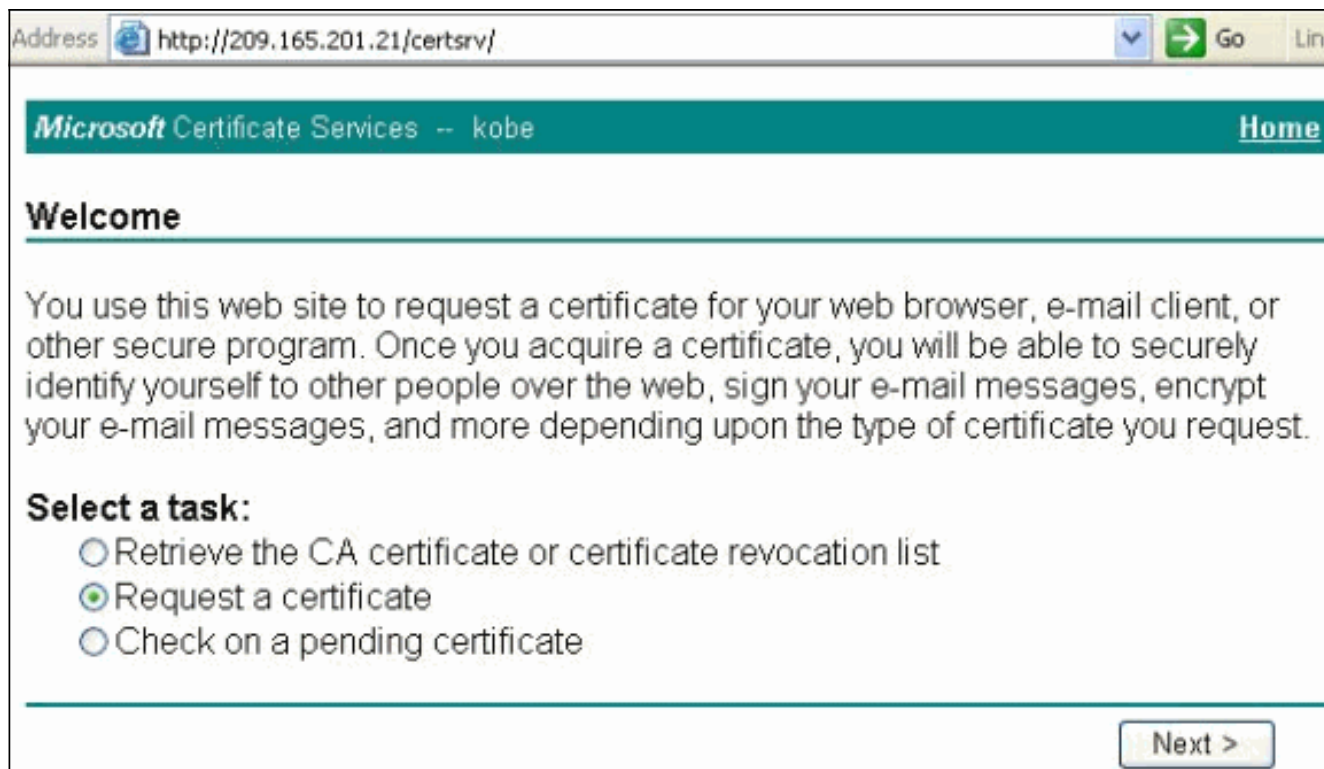
```
255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
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 クライアント 認証を登録して下さい

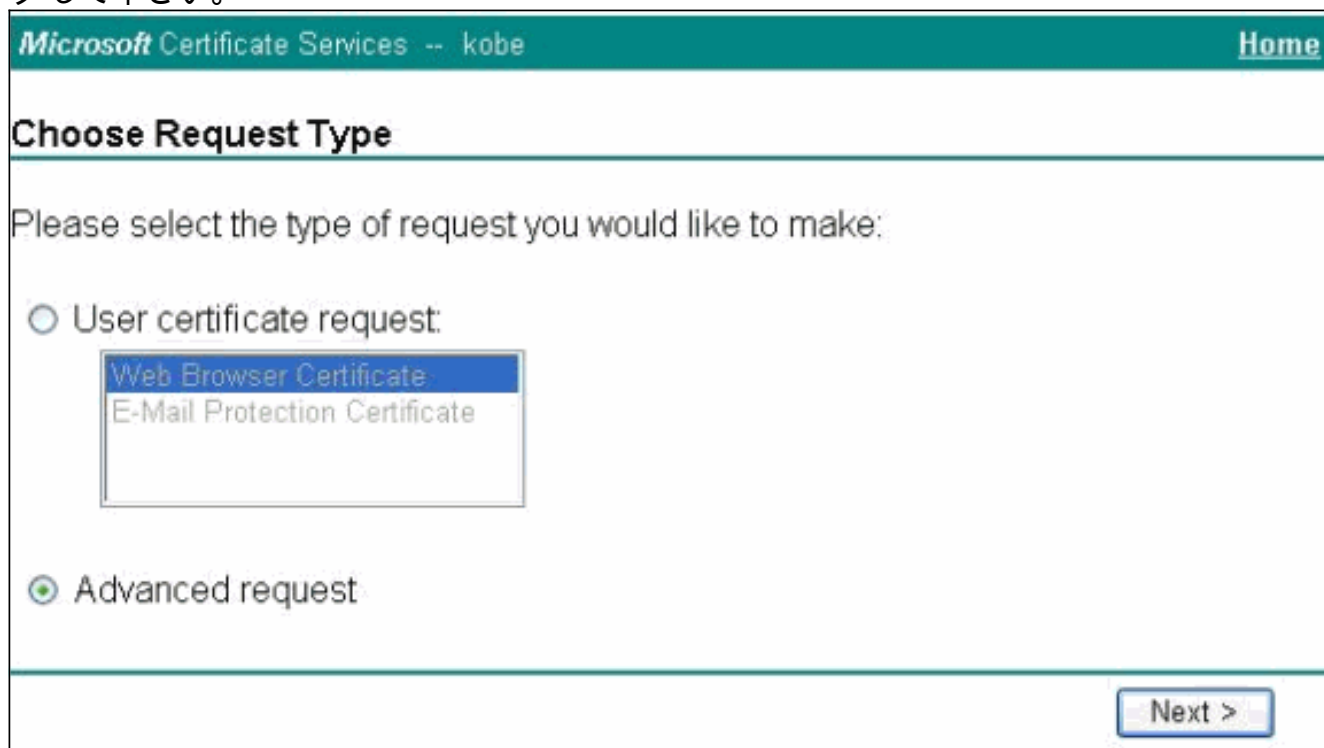
Cisco VPN Client と使用するべき PC のスマートカード デバイスが付いているユーティリティおよびすべての必要なドライバをインストールすることを忘れないようにして下さい。

これらのステップは MS 認証のための Cisco VPN Client を登録するのに使用される手順を示します。認証は [Aladdin](#) eTokenスマートカードストアで保存されます。

1. ブラウザを起動させ、認証サーバ ページ (この例の <http://CAServeraddress/certsrv/>、) に行ってください。
2. 『Request a certificate』 を選択し、 『Next』 をクリックして下さい。



3. Choose Request Type ウィンドウで、『Advanced request』を選択し、『Next』をクリックして下さい。



4. 『Submit a certificate request to this CA using a form』を選択し、『Next』をクリックして下さい。

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. Advanced Certificate Request フォームのすべての項目を記入して下さい。部門が Organizational Unit (OU) が Cisco VPN Client グループ名に対応することを PIX vpngroup 名前の設定によって、確かめて下さい。適切なセットアップ用に正しい Certificate Service Provider (CSP) を選択して下さい。

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. 潜在的なスクリプトを書く検証の警告を得るときインストールを続けるために『Yes』を選択して下さい。

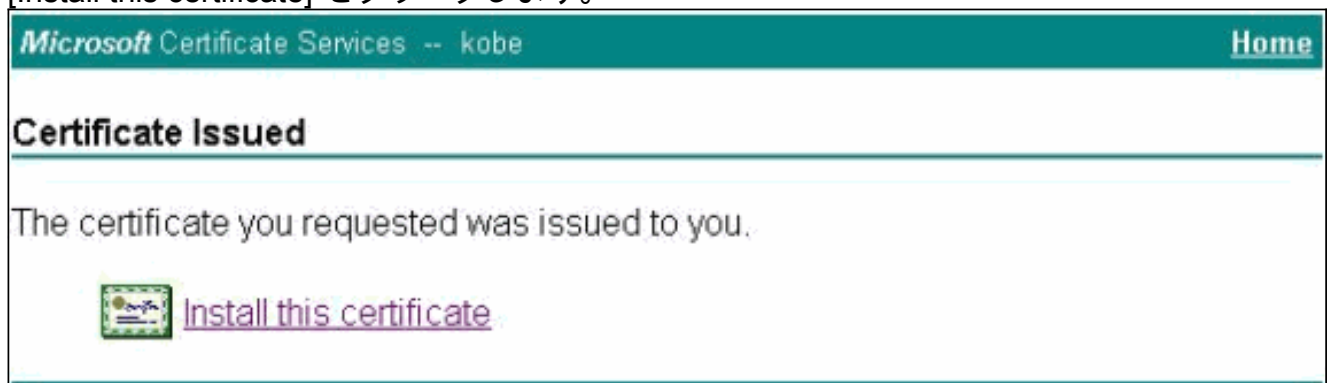


7. 証明書登録は eToken ストアを呼び出します。パスワードを入力し、『OK』をクリックし



て下さい。

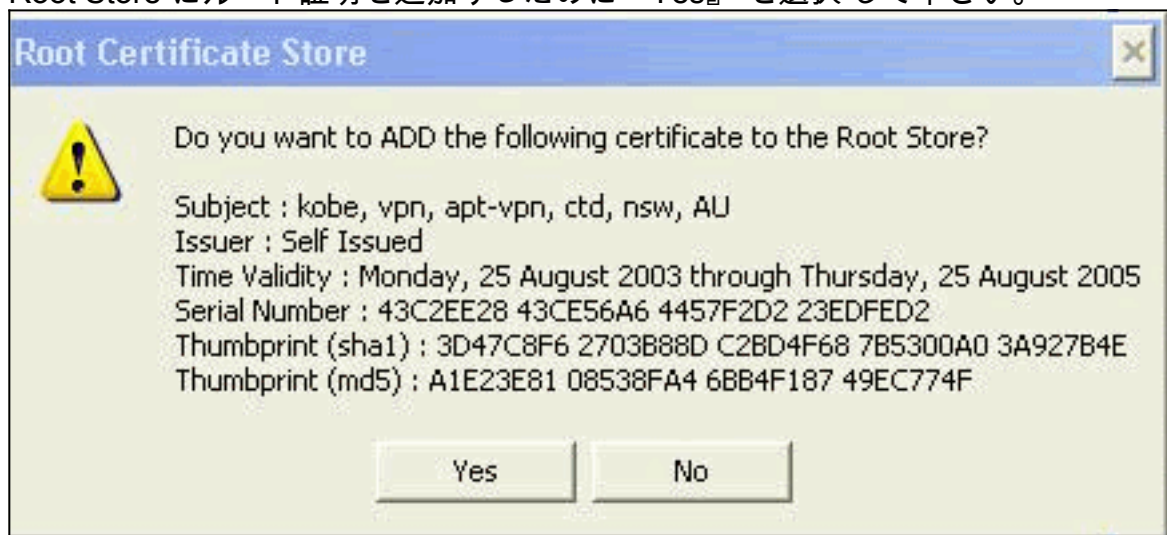
8. [Install this certificate] をクリックします。



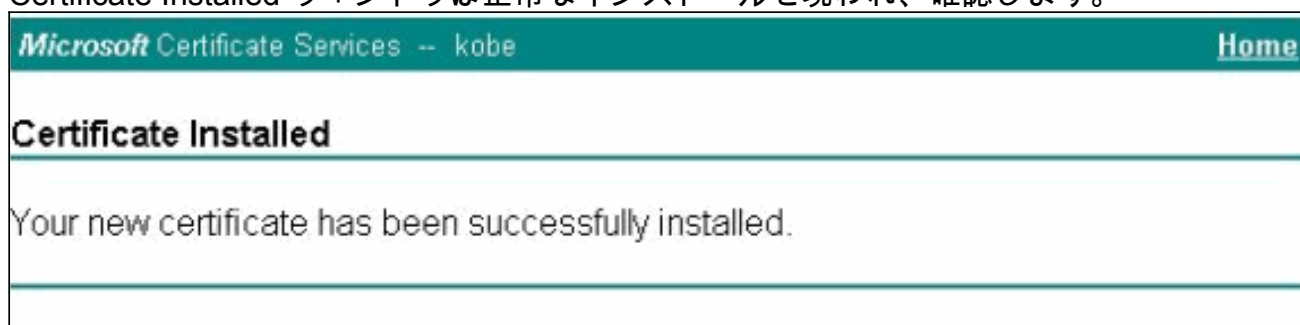
9. 潜在的なスクリプトを書く検証の警告を得るときインストールを続けるために『Yes』を選択して下さい。



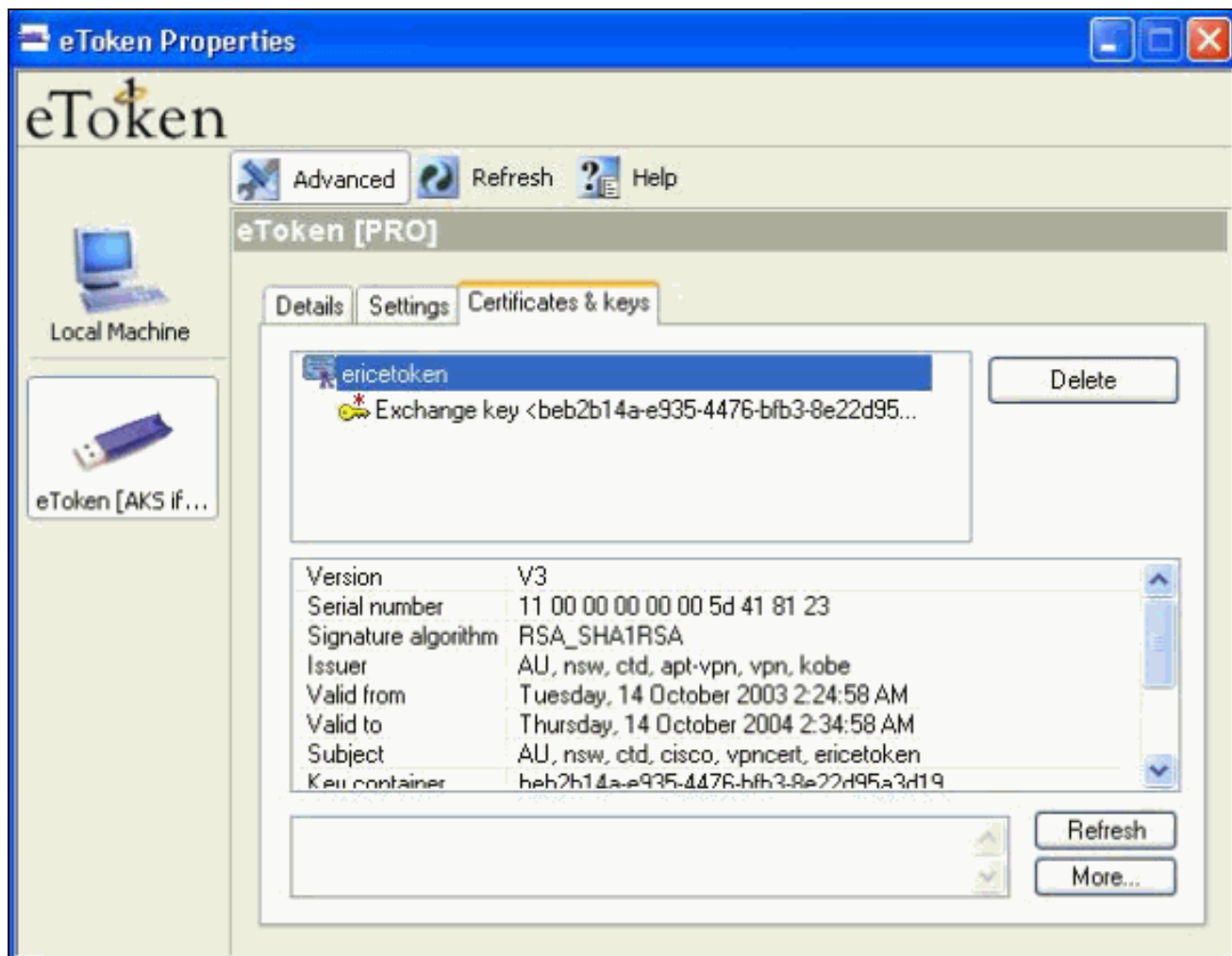
10. Root Store にルート証明を追加するために『Yes』を選択して下さい。



11. Certificate Installed ウィンドウは正常なインストールを現われ、確認します。



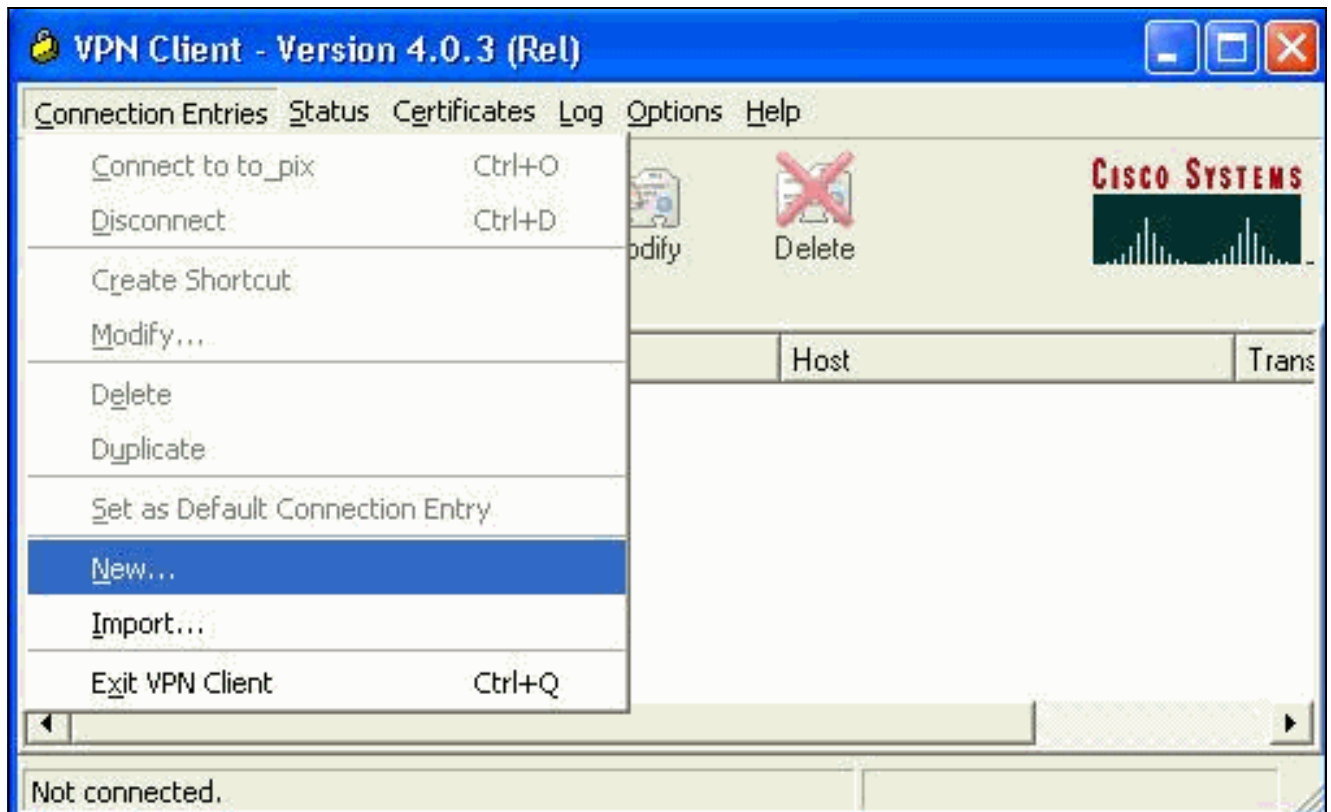
12. スマートカードで保存される認証を表示するために eToken アプリケーション ビューアを使用して下さい。



PIX への接続のために認証を使用するために Cisco VPN Client を設定して下さい

これらのステップは PIX 接続のために認証を使用するために Cisco VPN Client を設定するのに使用される手順を示します。

1. Cisco VPN Client を起動します。接続 エントリの下で新しい接続を作成するために『New』をクリックして下さい。

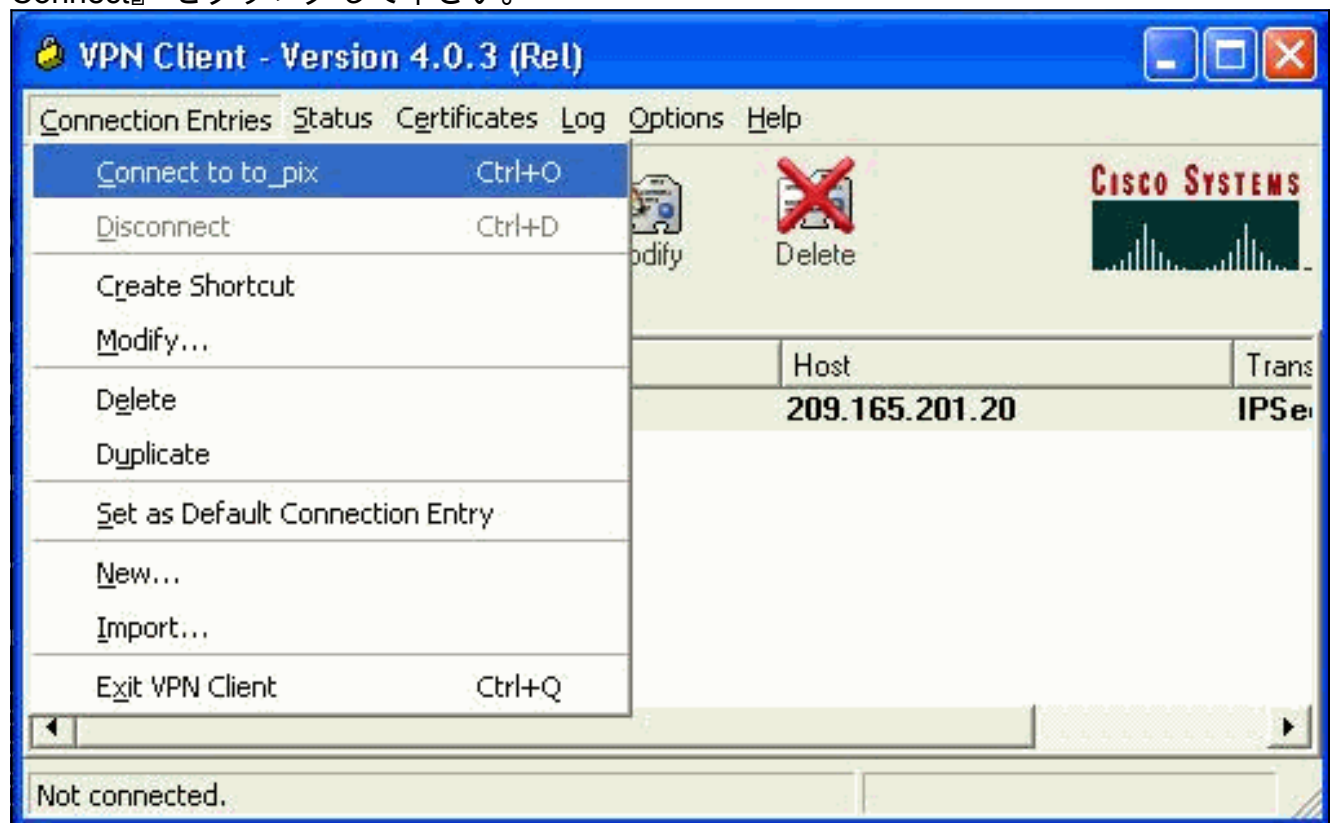


2. 接続詳細を完了して下さい、証明書認証を規定して下さい、登録から得られる認証を選択して下さい。[Save] をクリックします。



3. PIX への Cisco VPN Client 接続を開始するために、望ましい接続 エントリを選択し、『

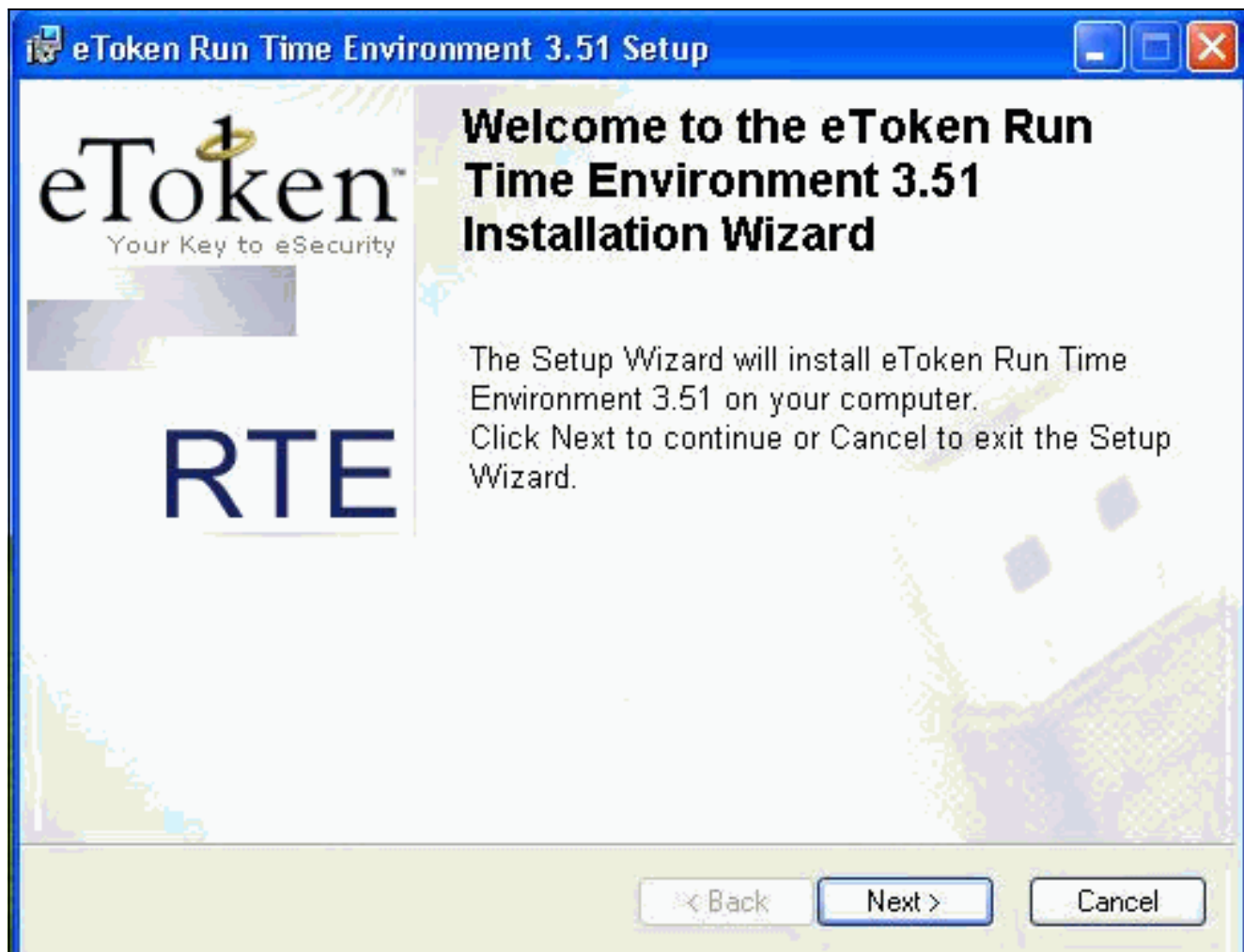
Connect』をクリックして下さい。



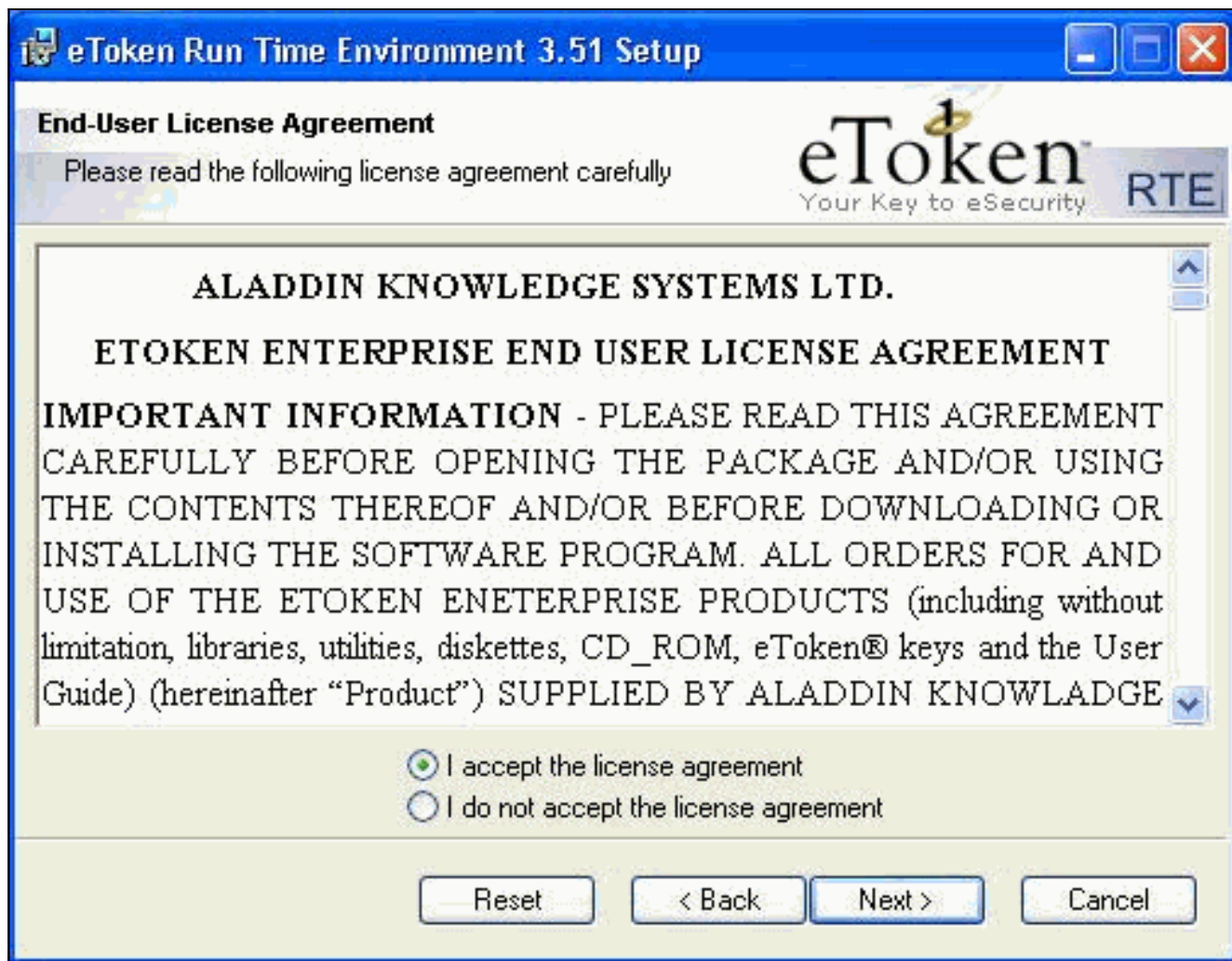
[eToken Smartcard ドライバーをインストールして下さい](#)

これらのステップは [Aladdin eToken Smartcard ドライバー](#) のインストールを示します。

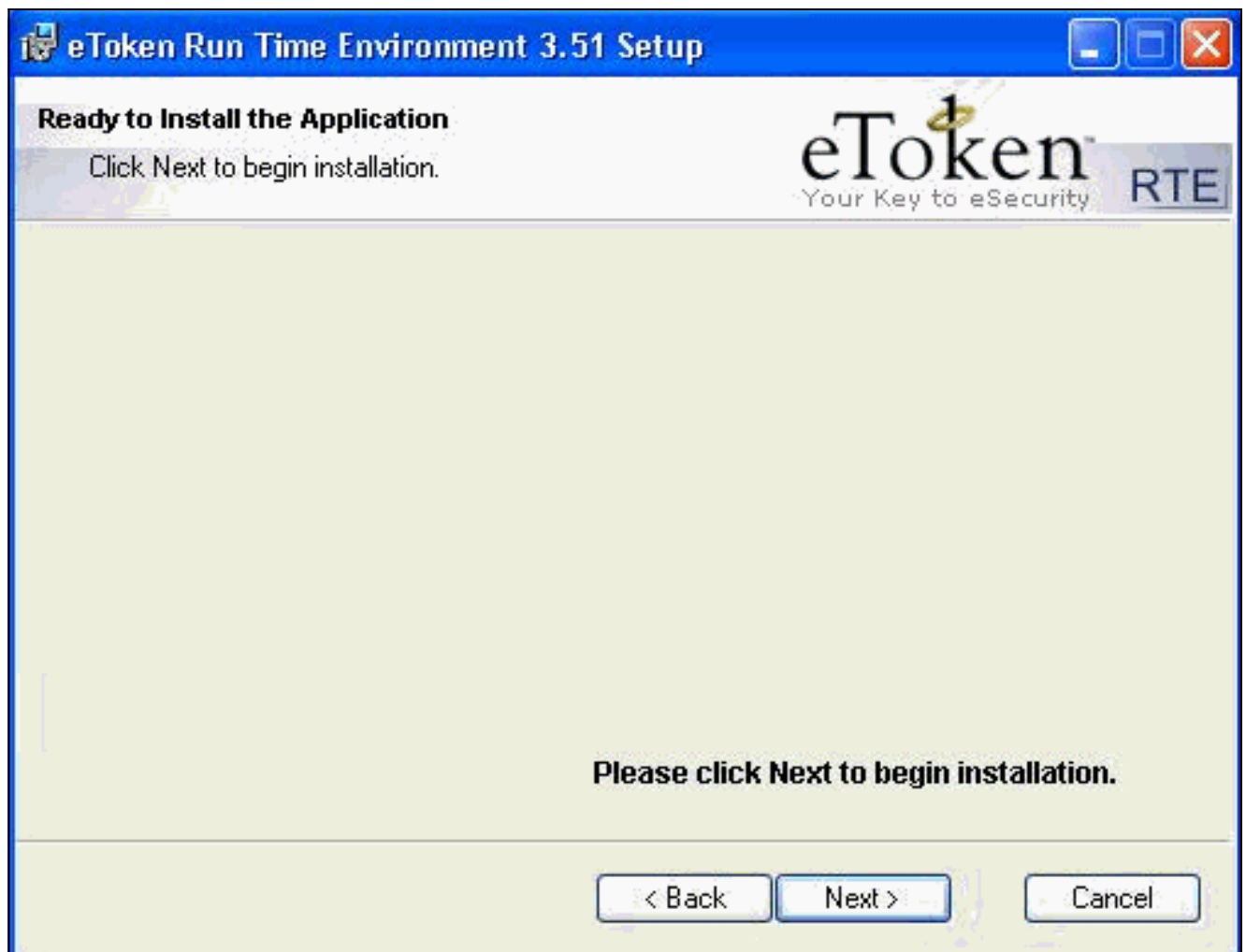
1. eToken ランタイム環境 3.51 セットアップ ウィザードを開いて下さい。



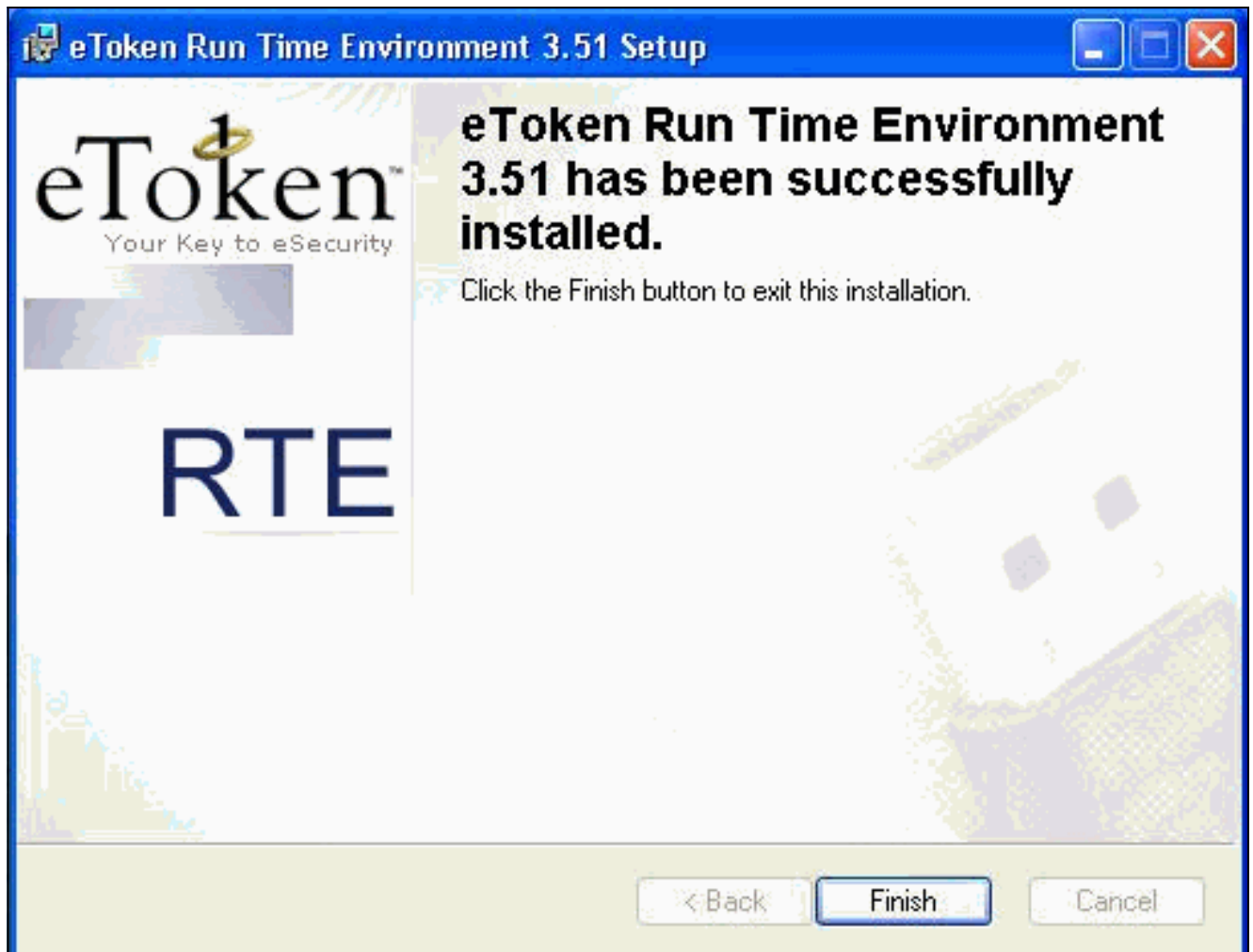
2. 使用許諾契約条件を受け入れ、『Next』をクリックして下さい。



3. [Install] をクリックします。



4. eToken Smartcardドライバーは今インストールされています。セットアップウィザードを終了するために『Finish』をクリックして下さい。



確認

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供しています。

特定の **show** コマンドは、[Output Interpreter Tool](#) (登録ユーザ専用) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto isakmp sa** : ピアにおける現在のインターネット鍵交換 (IKE) セキュリティアソシエーション (SA) をすべて表示します。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** — 現在のセキュリティアソシエーションが使用する設定を表示する。

```
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:
```

トラブルシューティング

この設定のトラブルシューティングのさらに詳しい詳細については[確立済みの IPSec トンネルでデータトラフィックを伝送する PIX のトラブルシューティング](#)を参照して下さい。

関連情報

- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [Requests for Comments \(RFC \)](#)
- [IPSec \(IP セキュリティ プロトコル \) に関するサポート ページ](#)
- [Cisco VPN Client に関するサポート ページ](#)
- [PIX 500シリーズ ファイアウォール サポートページ](#)
- [テクニカルサポート - Cisco Systems](#)