| Product name | Confidentiality level |
|---|---|
| mToken CryptoID | |
| Product version | |
| V1.1 | |

# mToken CryptoID

# Smart Card Application Guide

| Prepared by | | Date | |
|---|---|---|---|
| Reviewed by | | Date | |
| Approved by | | Date | |

Century Longmai Technology Co., Ltd.

# Revision Record

| Date | Revision Version | Sec No. | Change Description | Author |
|---|---|---|---|---|
| 2015/1/23 | V1.0 | | Initial Version | Longmai ITD |
| | | | | |
| | | | | |
| | | | | |

# Contents



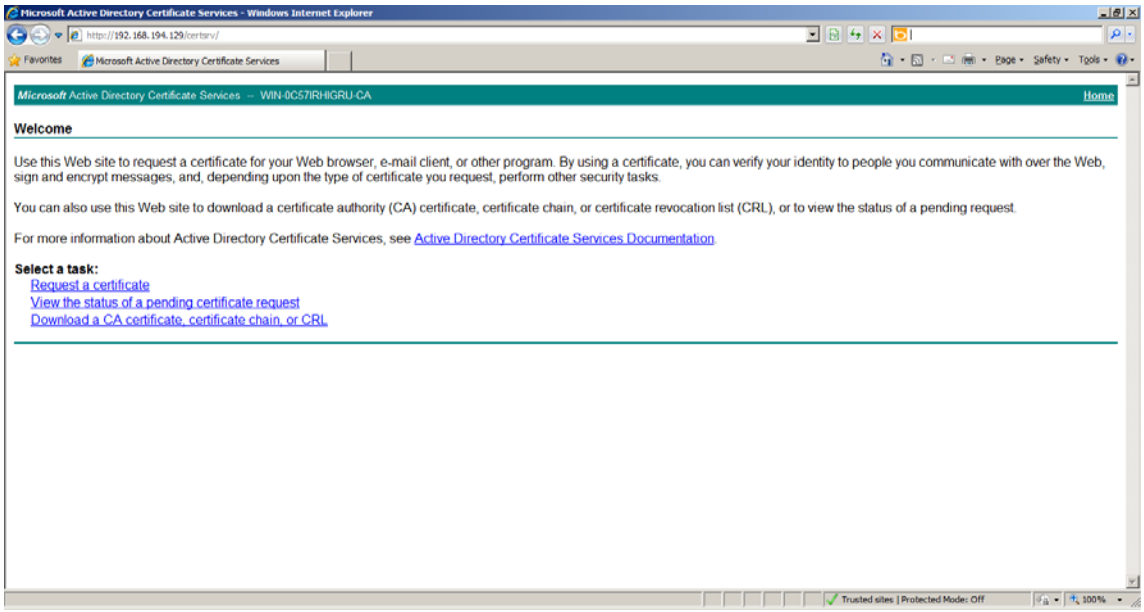
 

# Chapter 1. Smart Card Logon

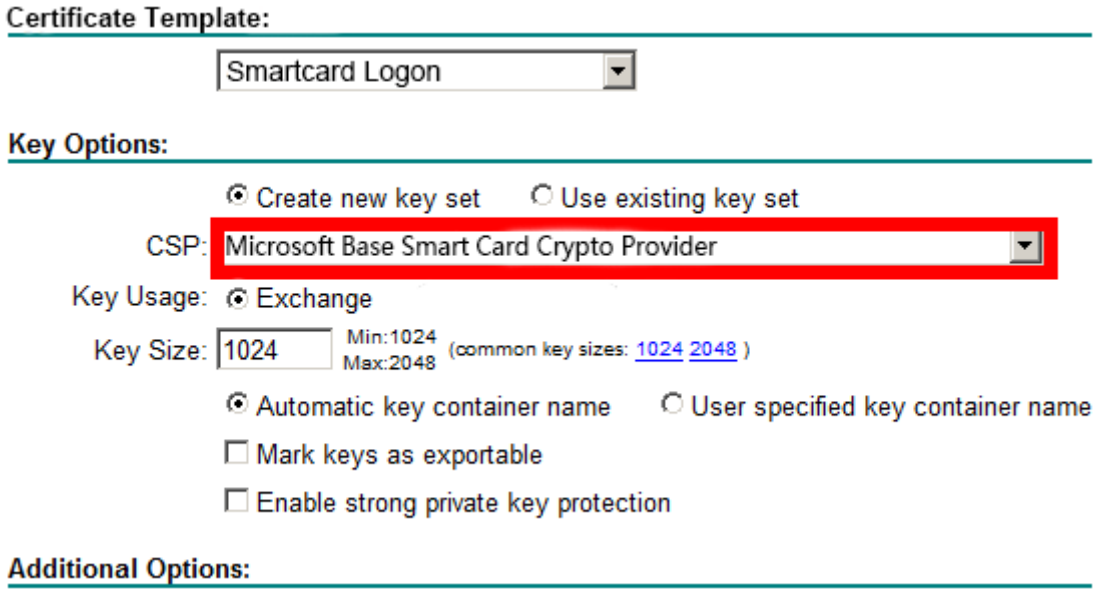
Form Microsoft Windows 2000 and above, MS included in-built smart card logon verification; the system user can either use traditional "username + password" to verify domain user or use smart card to automatically verify user identity. Comparing the two methods, smart card logon can be much safer and easy-to-use since the user is only needs to remember PIN of his/her smart card being used to logon.

## 1.1 Prerequisites – Request for Smart Card Logon Certificate

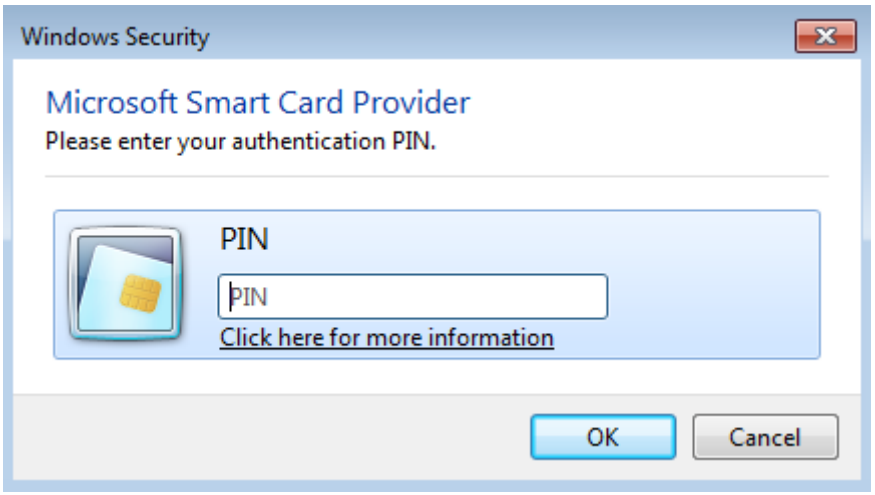
1. Make sure the mToken device has been connected to your computer.
2. Open the certificate server page through Internet Explorer. (Here I will access my CA Server at http://192.169.194.129/certsrv)



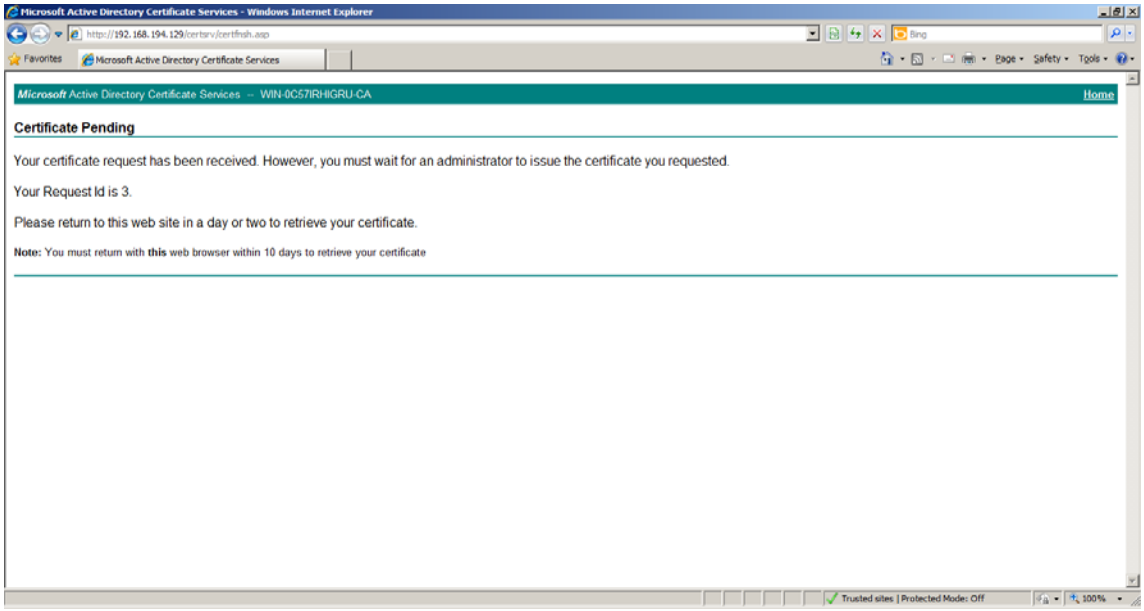

3. Select **Request a certificate → Advanced Certificate Request → Create and submit an application to the CA**.
4. In Certificate Template Area, select smart card related template (Smartcard User or Smartcard Logon).
5. Select **Microsoft Base Smart Card Crypto Provider** as the CSP.



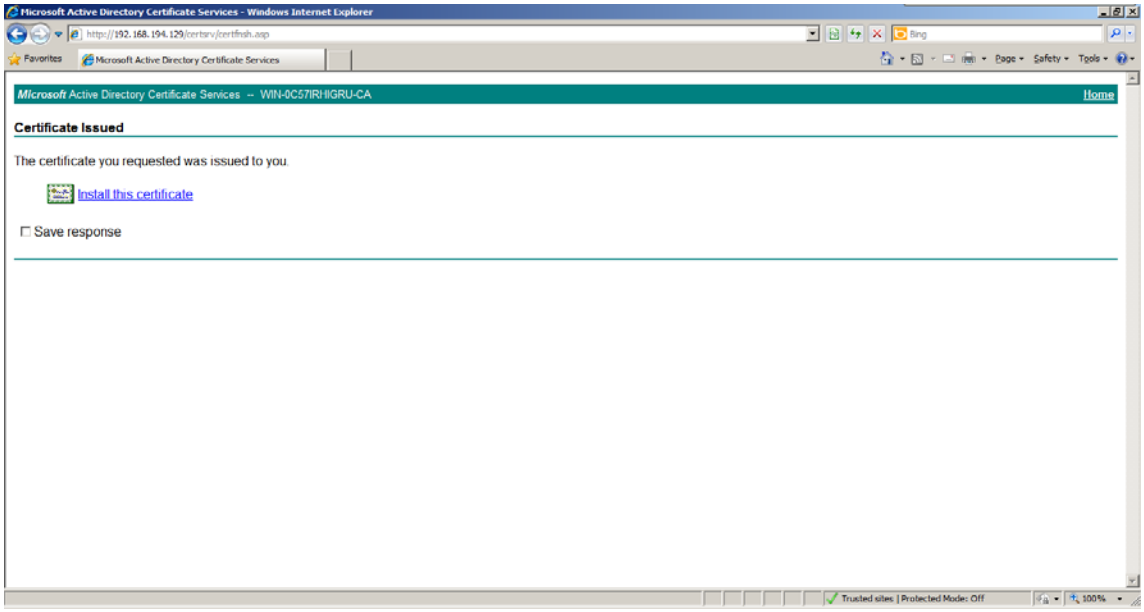

6. Finish the above Settings; click **Submit**, the PIN dialog box pops up.

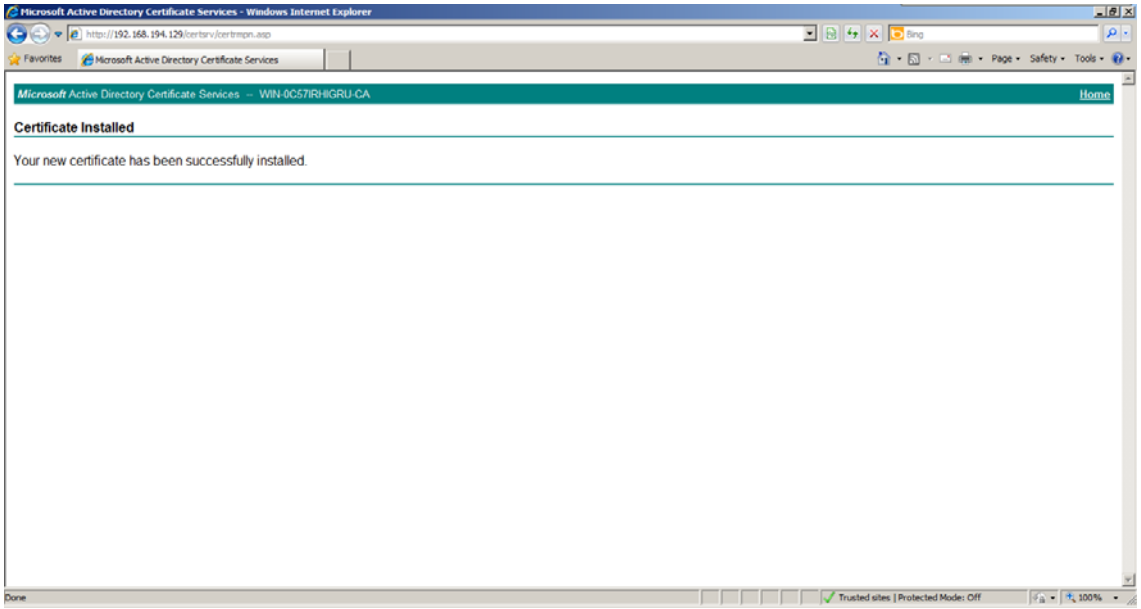



7. Type the correct PIN and click **OK**,a pending certificate page will be displayed, you need to wait for issuer to authenticate and issue you the certificate:



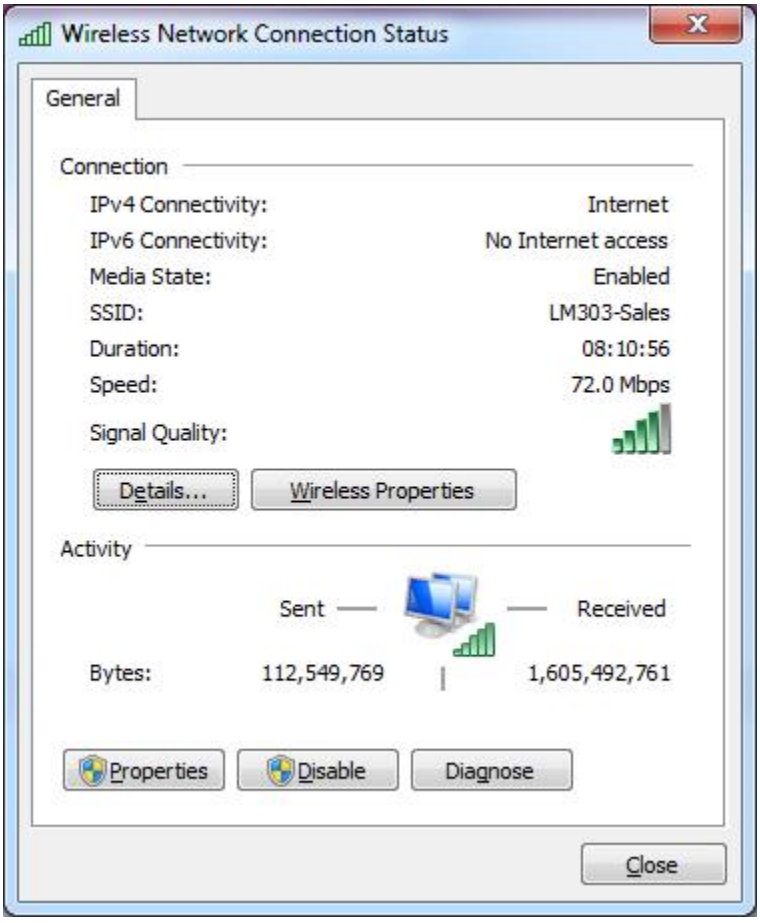

8. Back to **Step 1**, select **view pending certificate request status**. After receiving the notification from your Certificate Authority (CA), you can get the certificate.
9. When installing the certificate, system will also verify your PIN, click **Install this certificate**, you can determine whether the certificate is correctly installed according to the prompts.





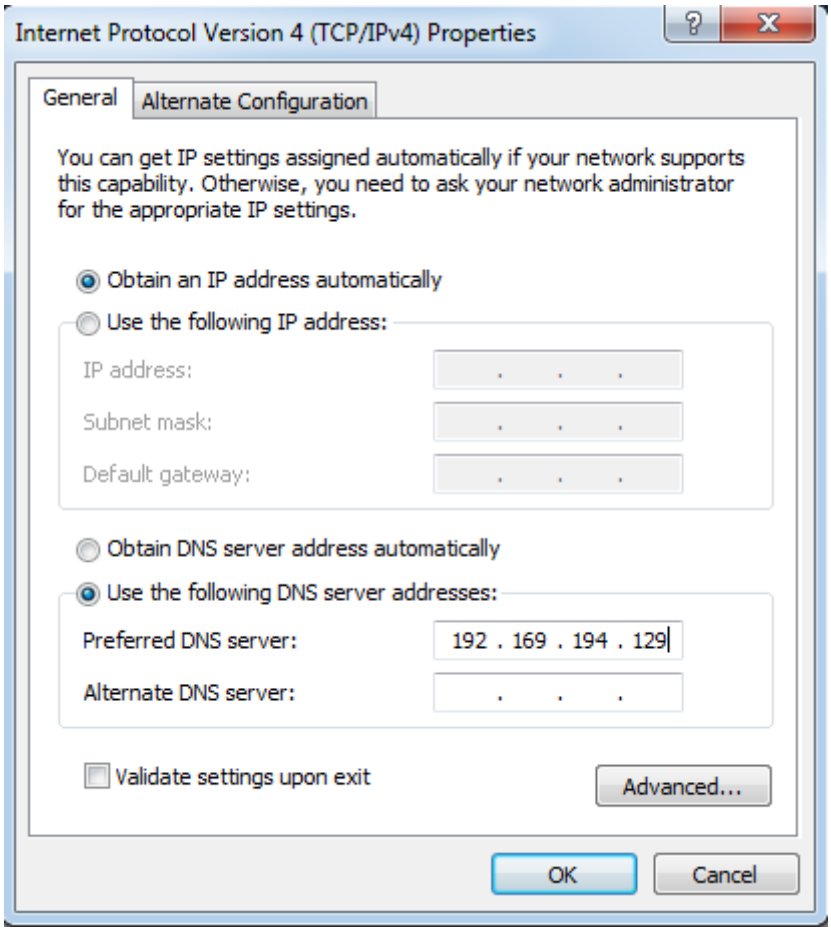

## 1.2 Smart Card Logon

1. Open **Wireless Network Connection Status**

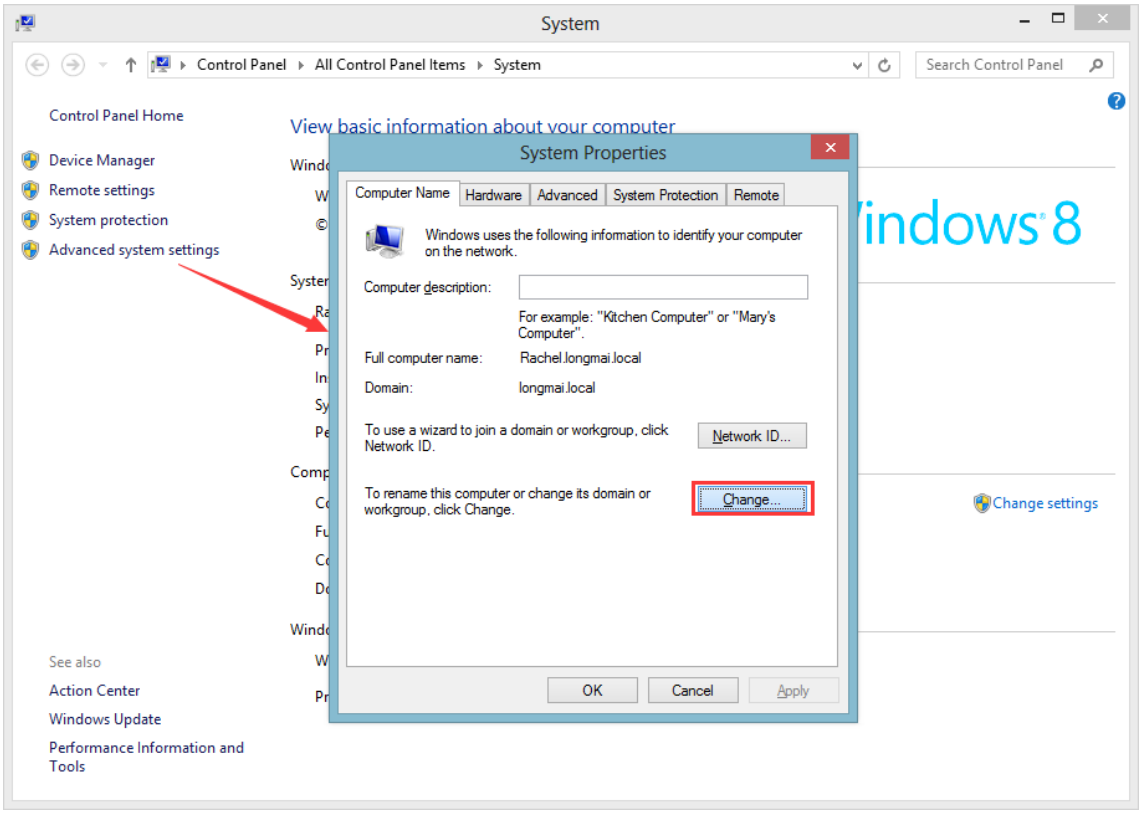



2. Click **Properties** and double-click "*Internet Protocol Version 4(TCP/IPv4)*". Set the Server address, here I will set my server address: as *192.169.194.129*

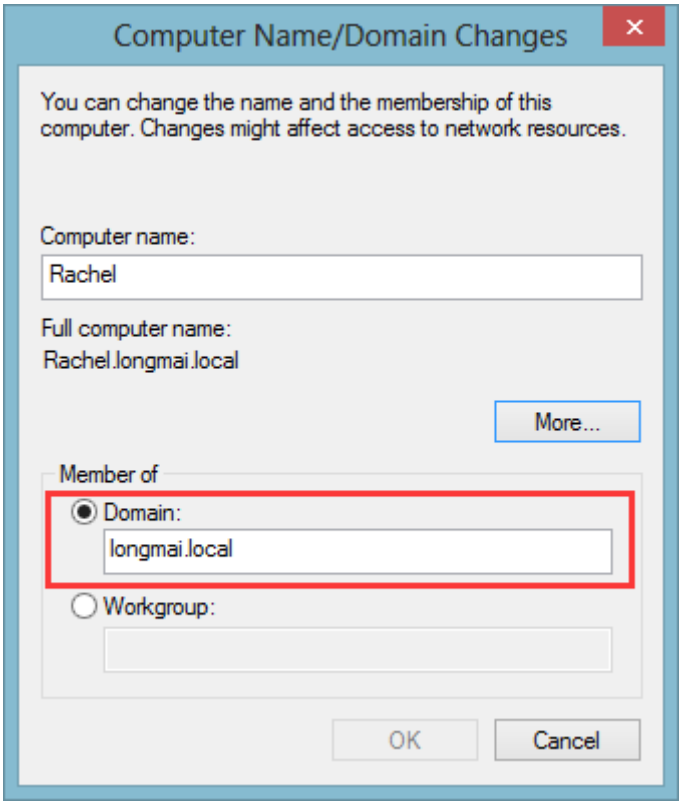
 




3. Back to the desktop, right-click **Computer**, select **Properties → Advanced system settings → Change**



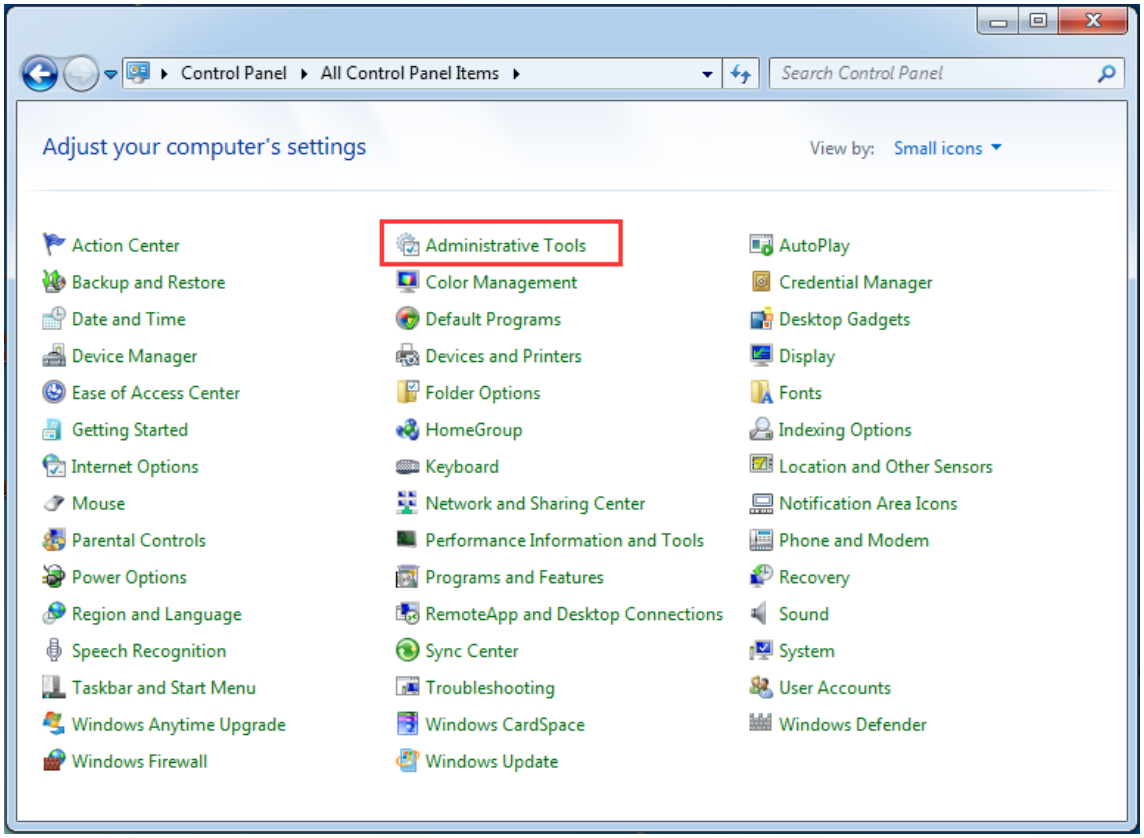

4. Input domain name, here I input longmai.local as my domain name.



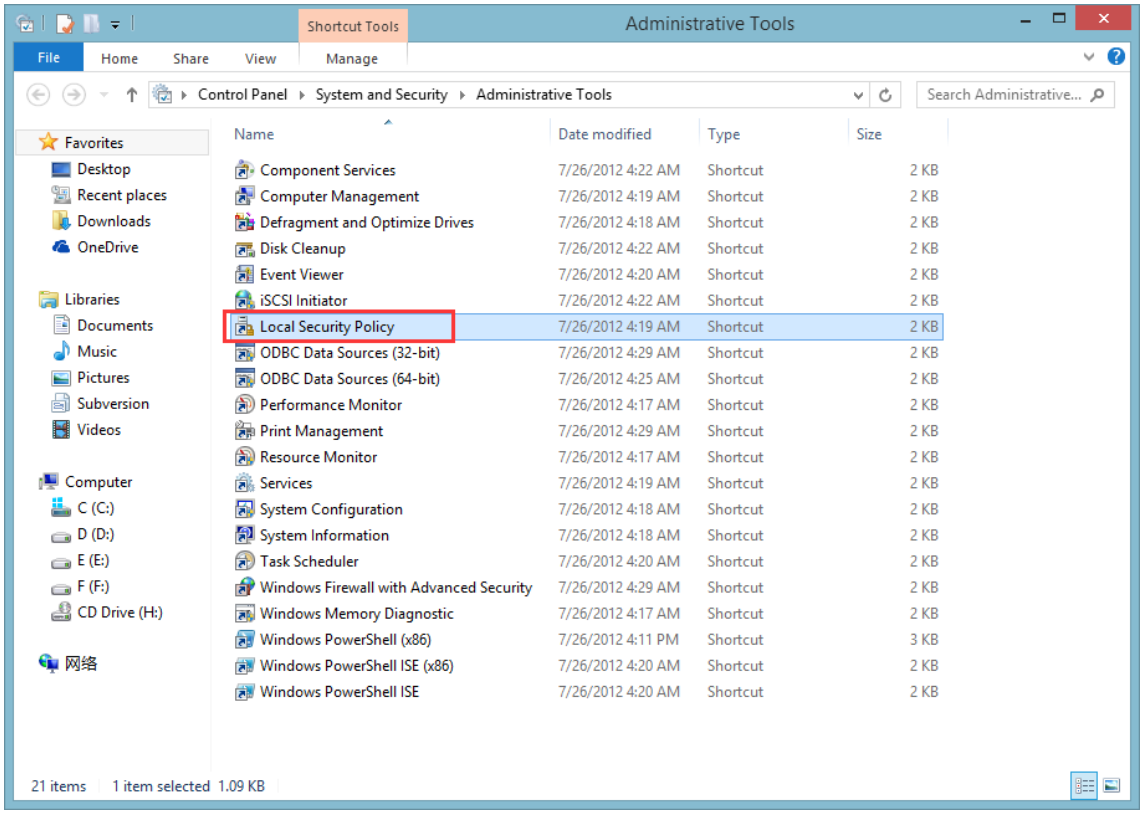

5. Finish all steps, and click **OK** (must input correct domain name and domain password to join in domain successfully).

6. Connect your smart card certificate device to the computer.
7. Switch account, login with smart card device.
8. After entering system with smart card device, if you want the system can automatically lock screen after device is unplug from the computer.

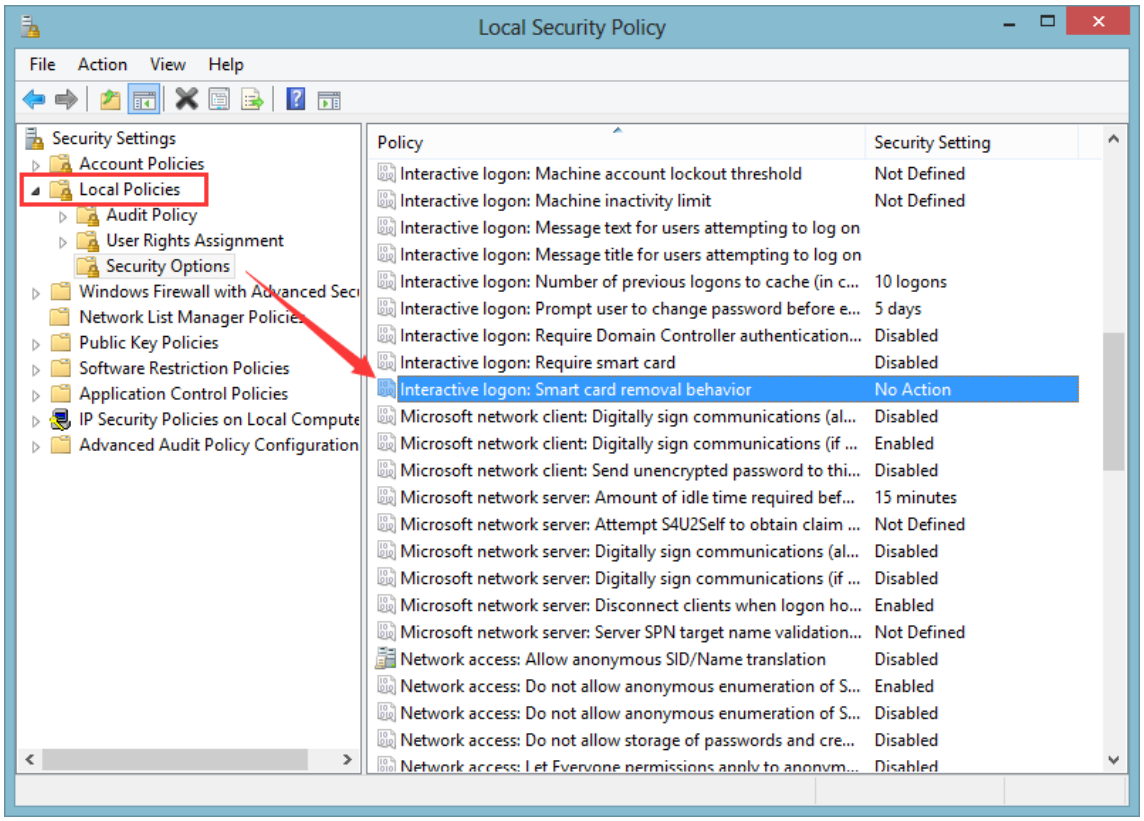
   Optional: change some local properties - Select **Control Panel → Administrative Tools**



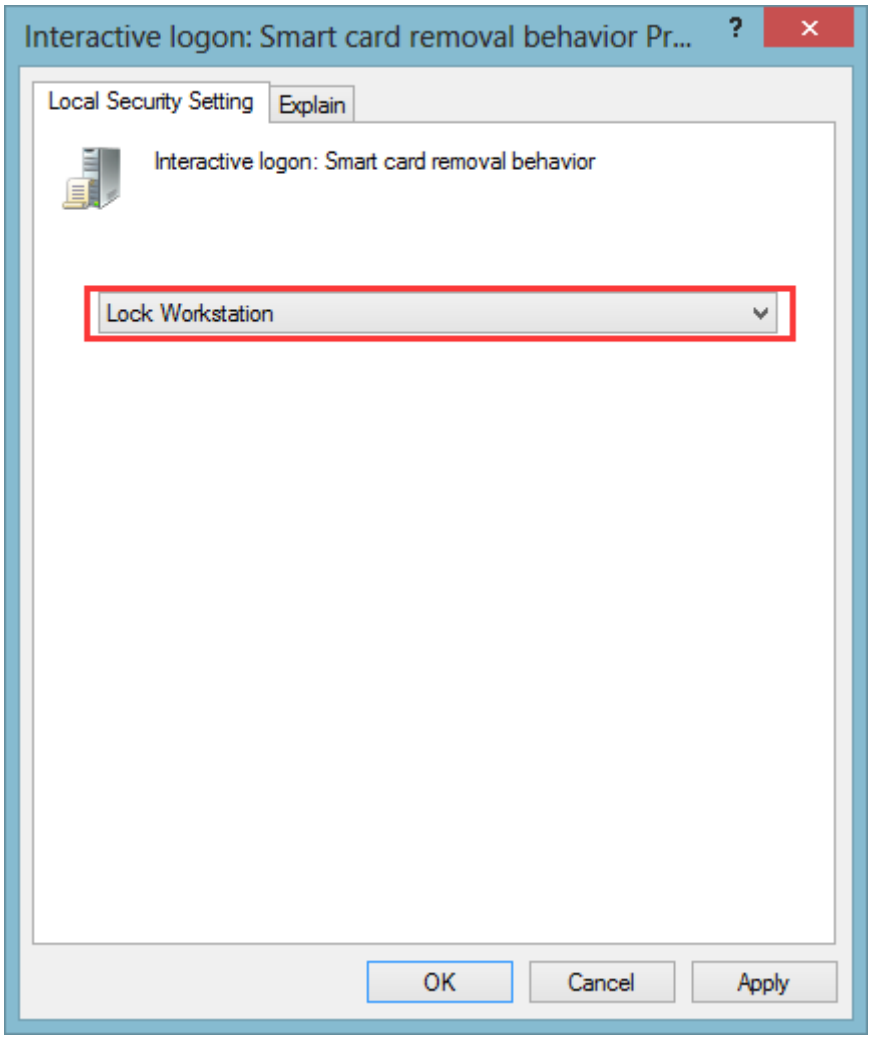

9. Double-Click **Local Security Policy**



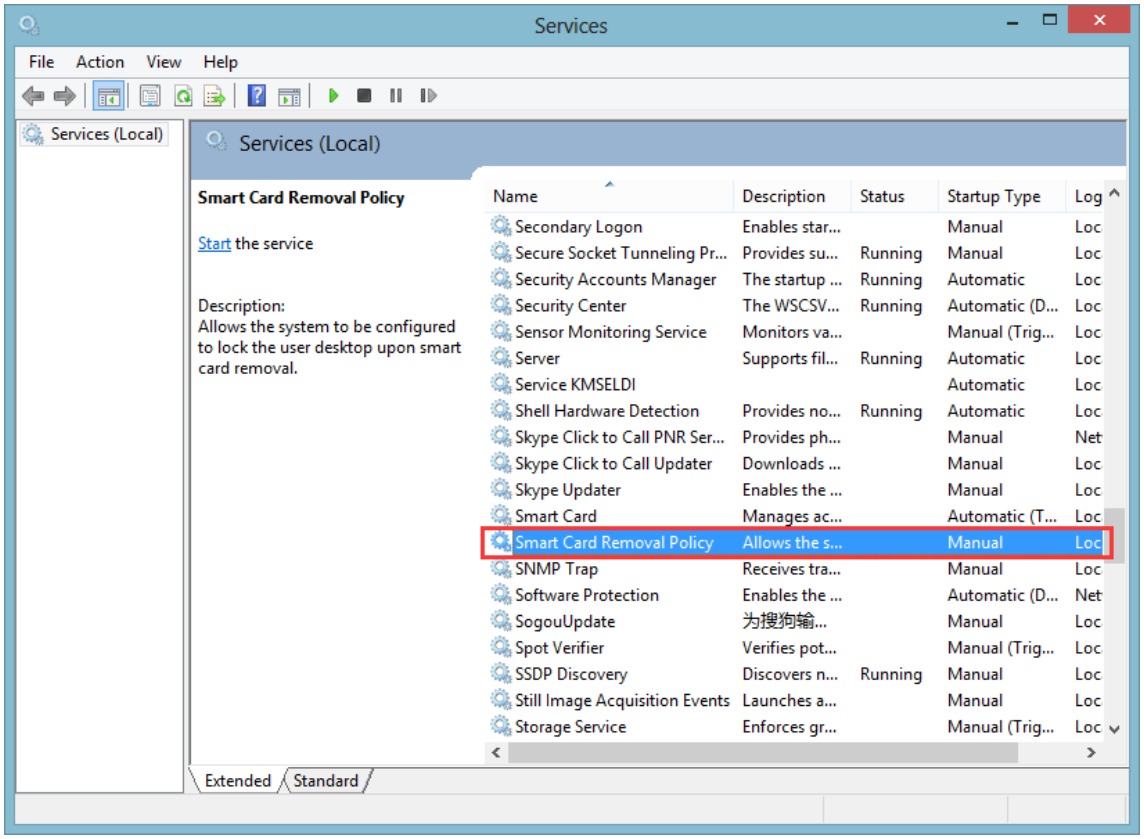

10. Select **Local Policies →Security Options →Interactive logon: Smart card removal behavior**



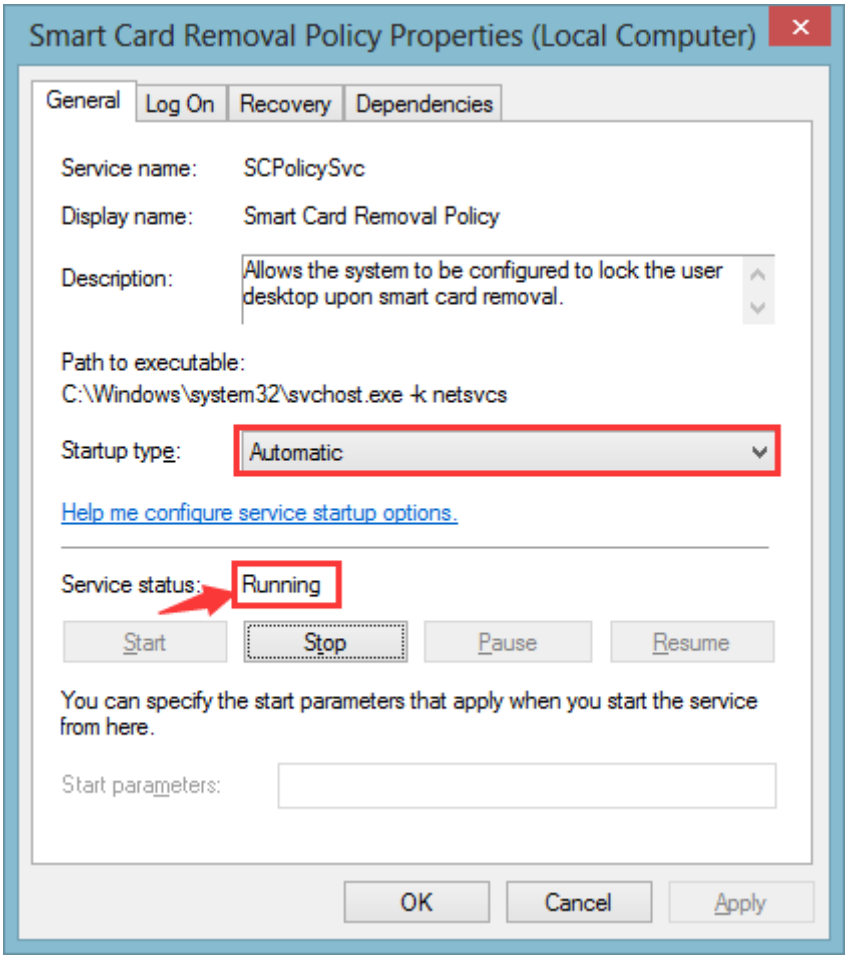

11. Select **Lock Workstation** from drop-down list, click **OK**




12. Then select **Control Panel →Administrative Tools →Services**, double-click **Smart Card Removal Policy**




13. Select **Automatic** from drop-down list and start service



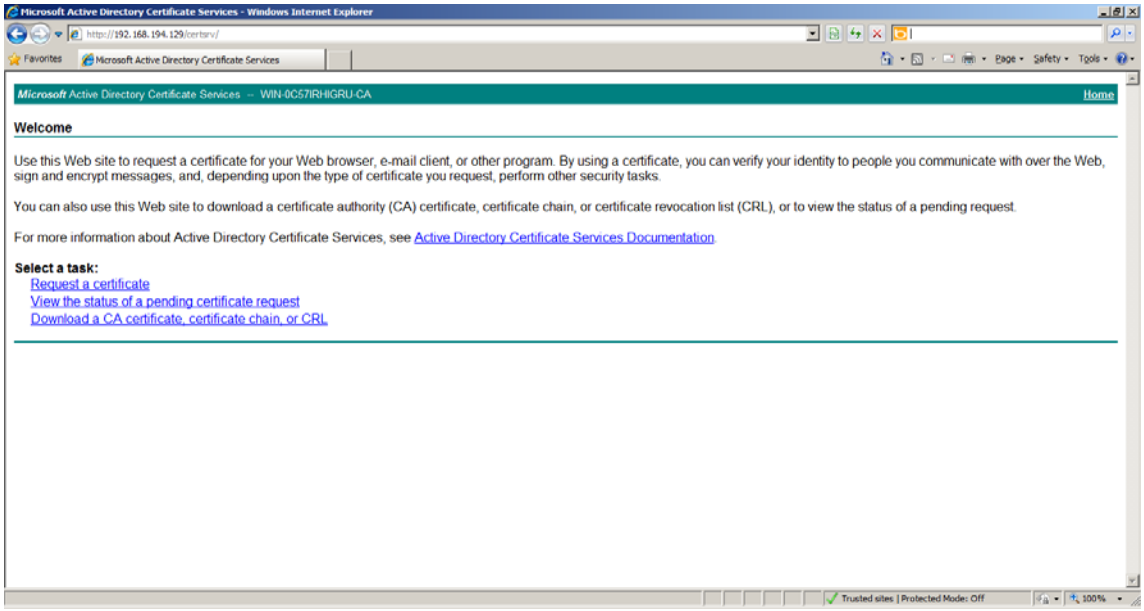

14. Now the system will lock screen when user unplugs the mToken device.

# Chapter 2. BitLocker Drive Encryption

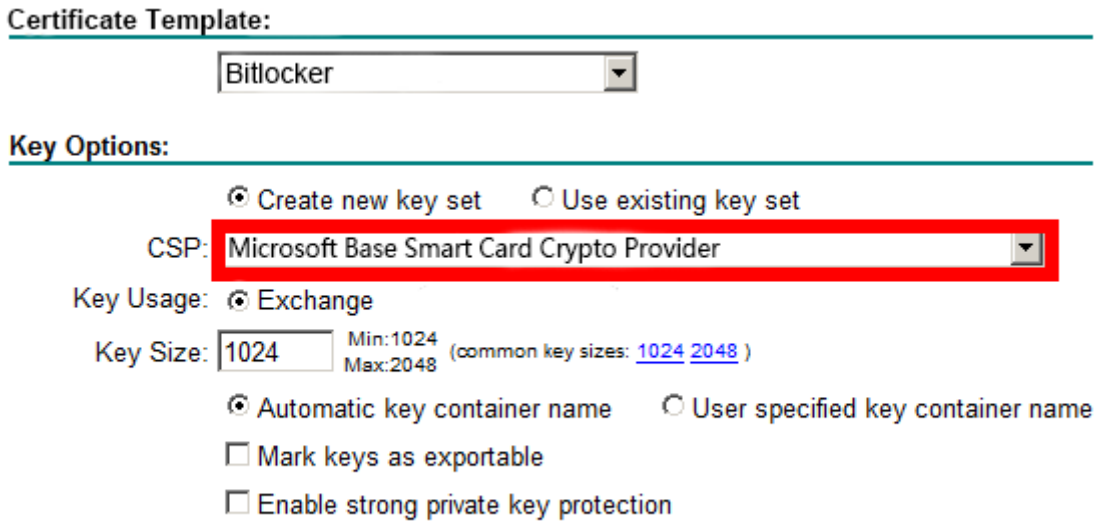
This Chapter mainly describes how to request a BitLocker certificate and how to use mToken CryptoID to encrypt the hard drive.

## 2.1 Request a BitLocker Certificate

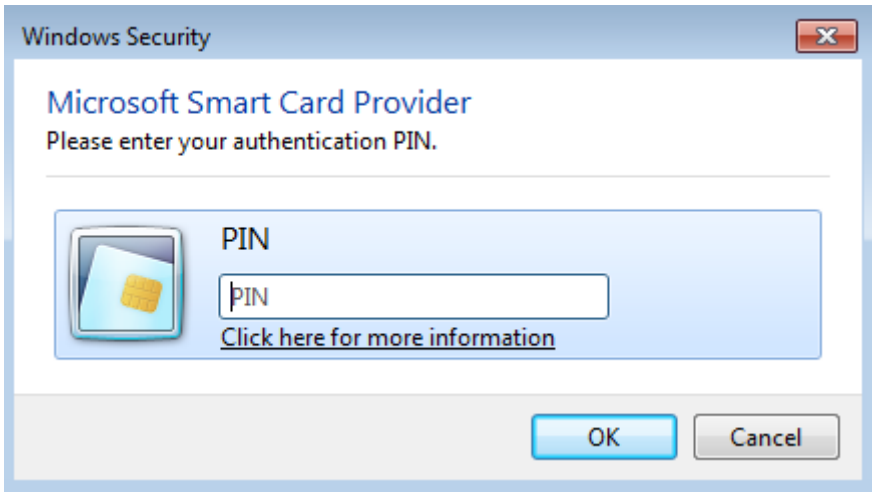
1. Make sure mToken device has been connected to your computer. Then, open the certificate server page through Internet Explorer. (Here I will access my CA Server at http://192.169.194.129/certsrv)



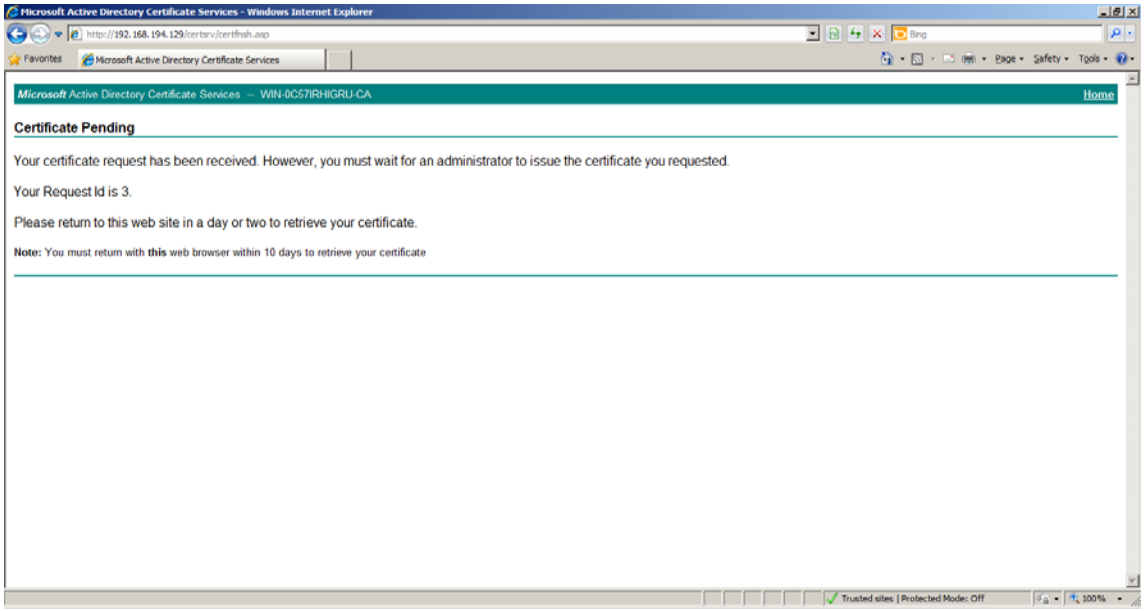

2. Select **Request a certificate** →**Advanced Certificate Request** →**Create and submit an application to the CA**. In Certificate Template Area, select **Bitlocker** template. Select **Microsoft Base Smart Card Crypto Provider** as the CSP.



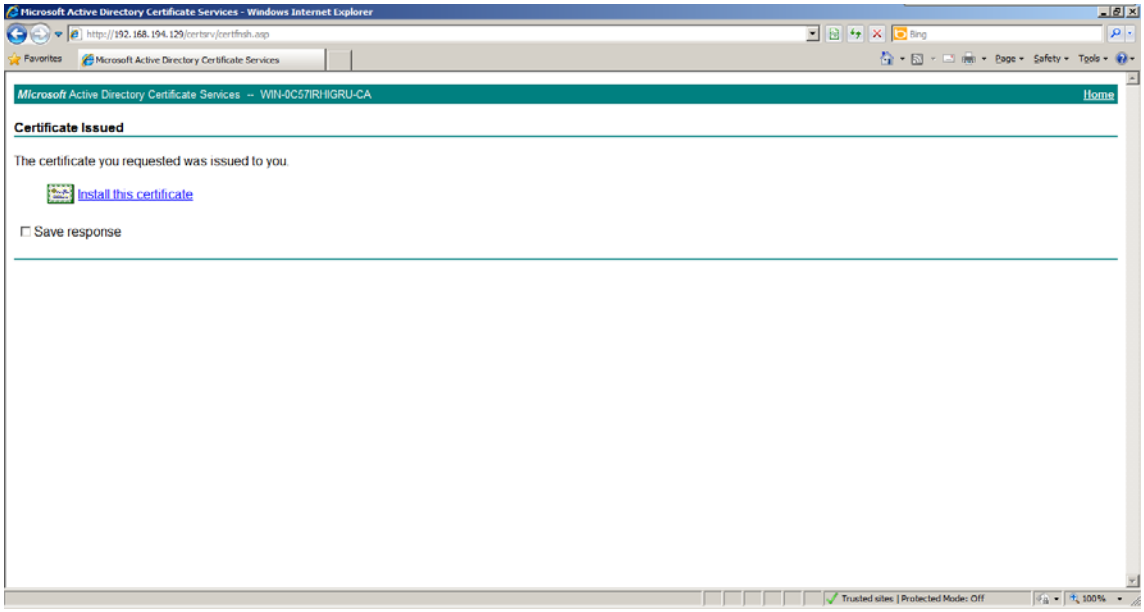

3. Finish the above Settings,click**Submit**, the PIN dialog box pops up.




4. Type the correct PIN and click **OK**, a pending certificate page will be displayed,you need to wait for issuer to authenticate and issue the certificate:



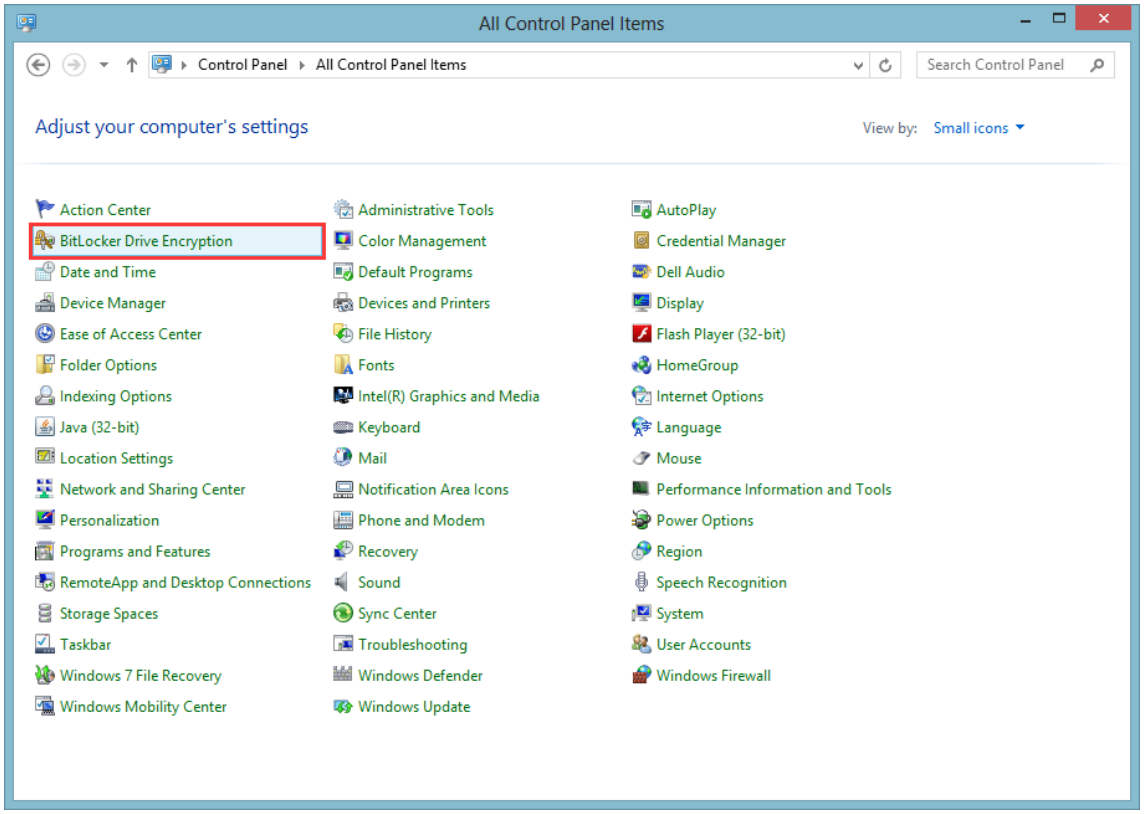

5. Back to **Step 1**, select **view pending certificate request status**. After receiving the notification from the Certificate Authority, you can obtain the certificate. When installing the certificate, system will also verify the PIN, click **Install this certificate**, you can determine whether the certificate is correctly installed according to the prompts.

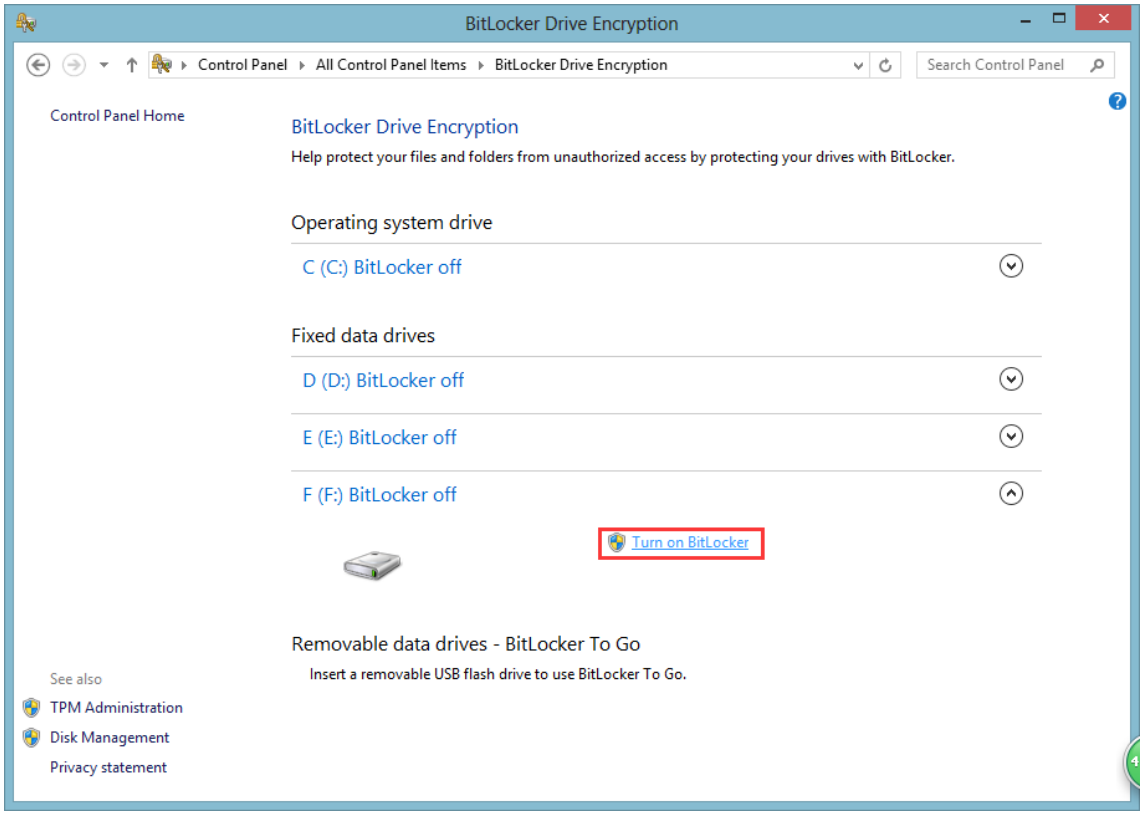



## 2.2 Drive Encryption

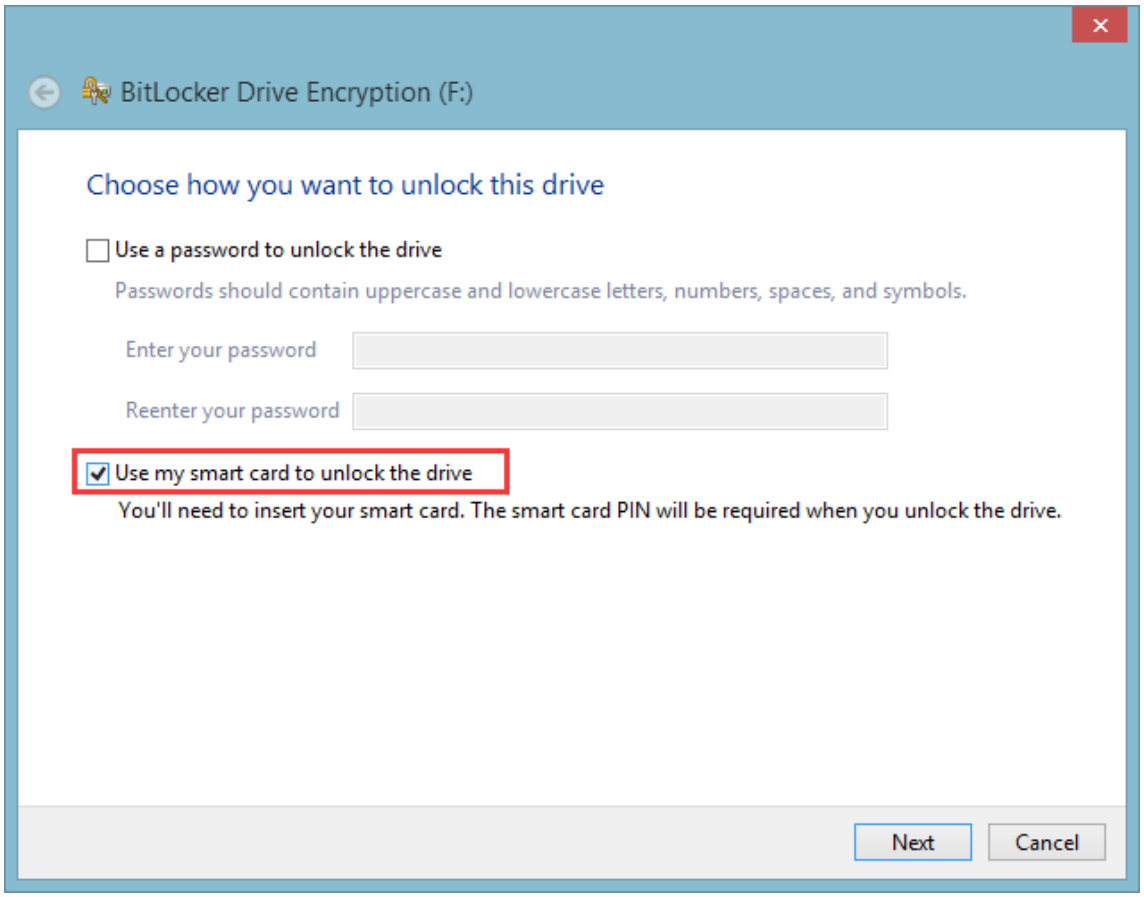
1. Select **Control Panel** →**BitLocker Drive Encryption**, here I will test with encrypting F: disk.
2. **Turn on BitLocker**

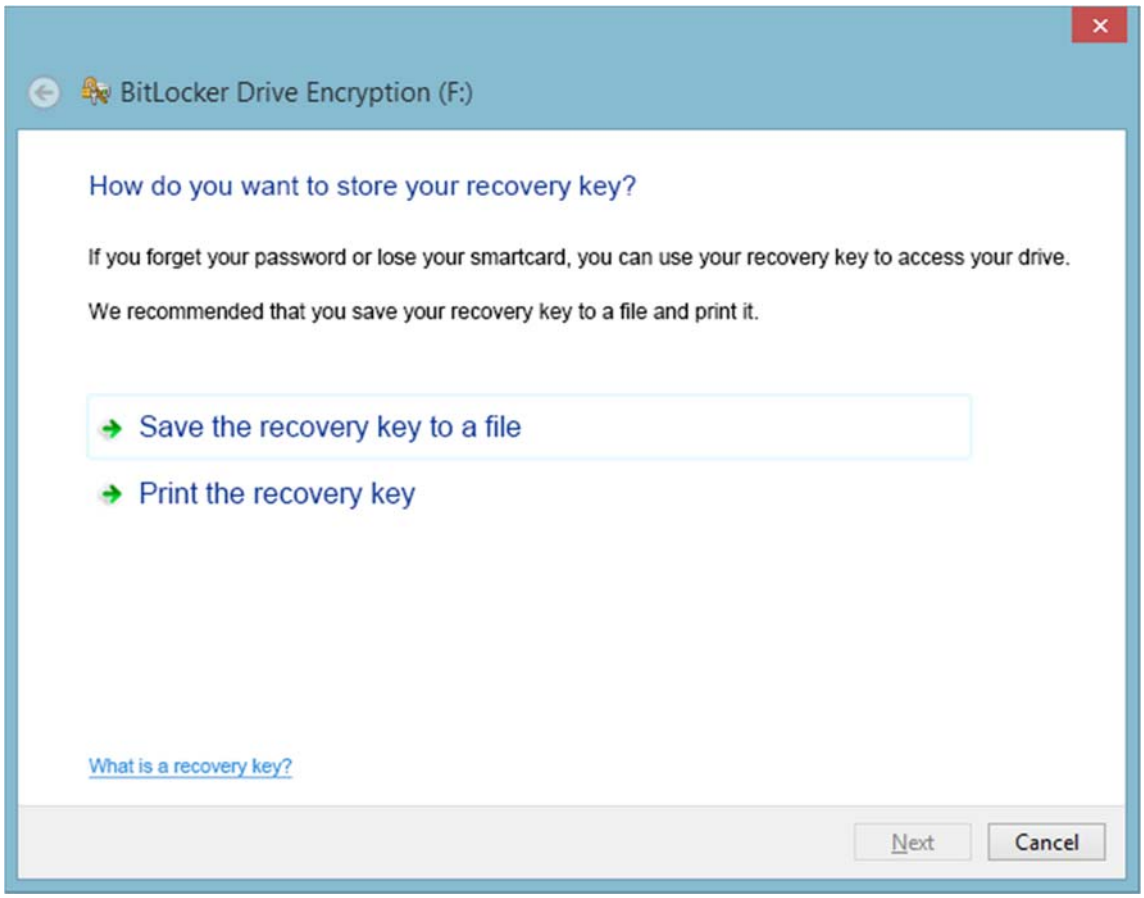


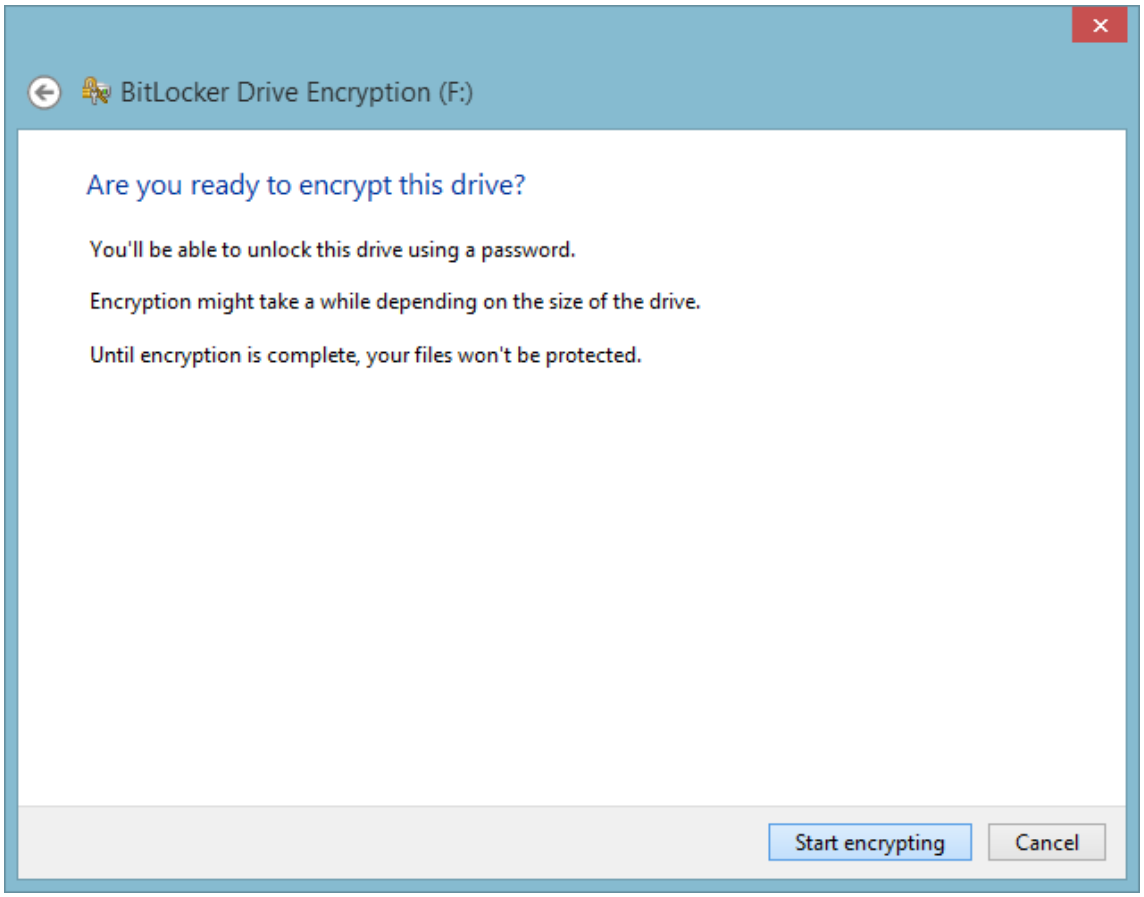

3. Select **Use my smart card to unlock the drive**, click **Next**




4. Select how to back-up your recovery key

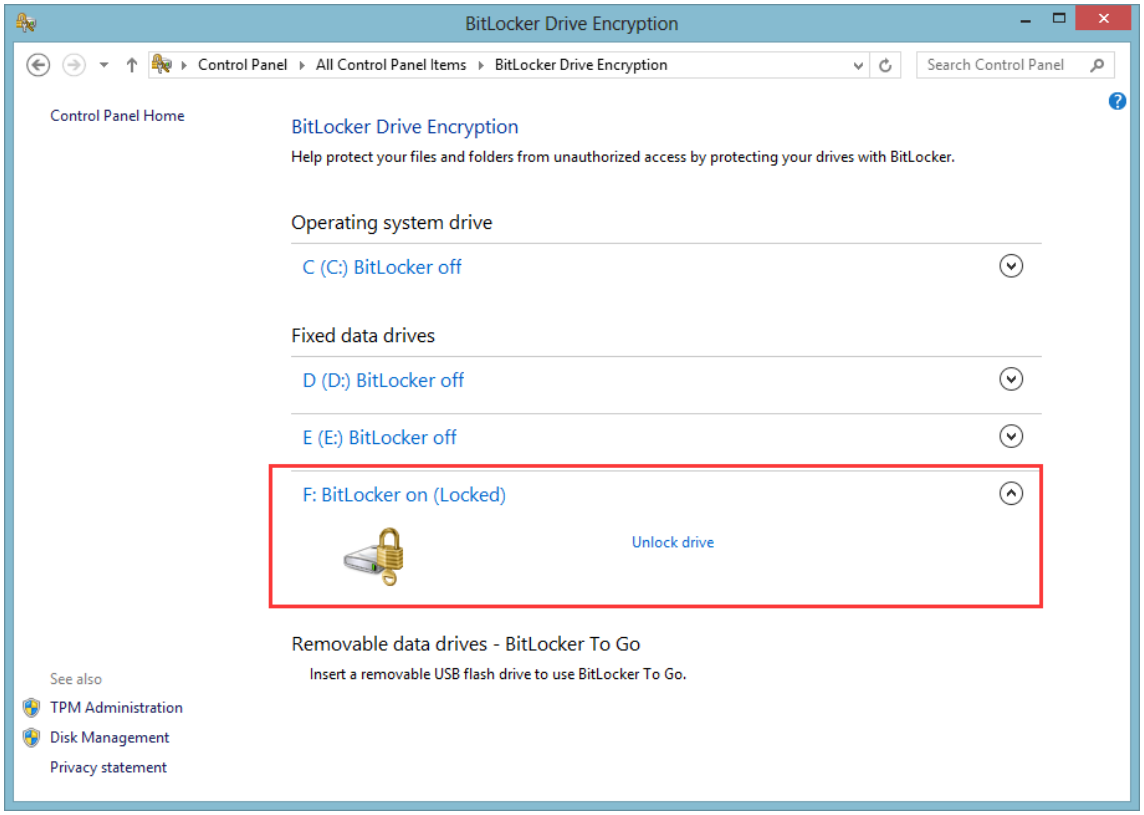



5. Click **Next**, you will see below pop up message.



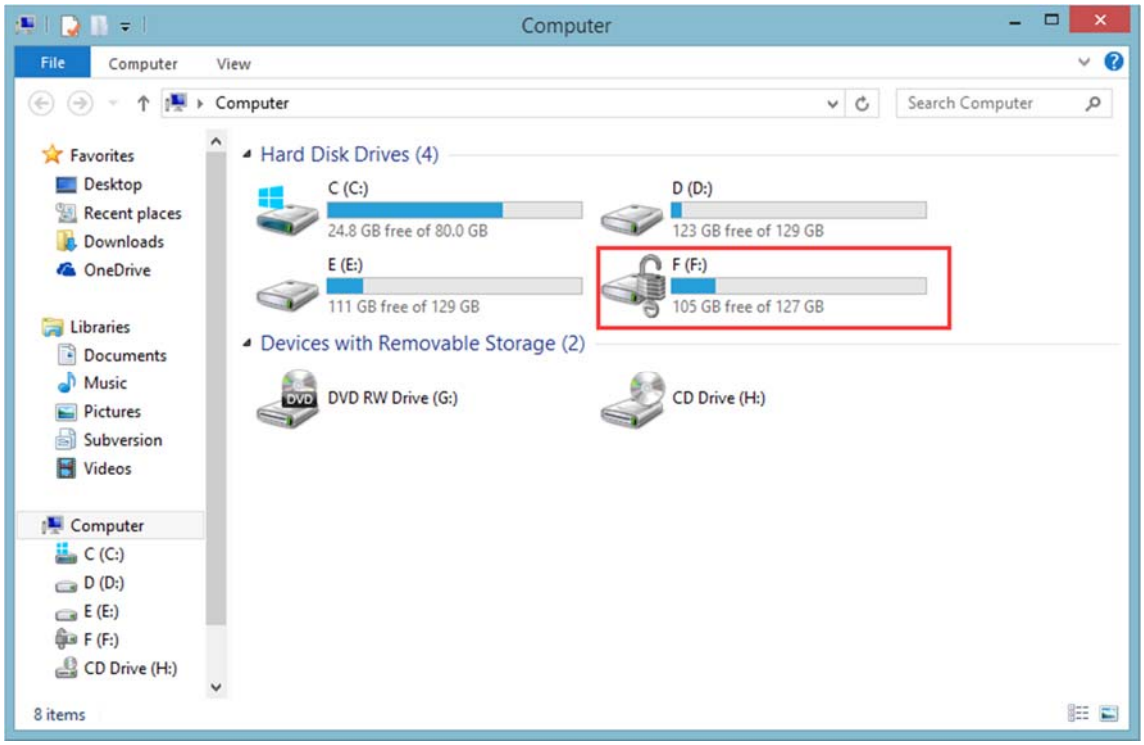

6. Click **Start encrypting**, the encryption progress window will be displayed.


7. You can find the drive has been encrypted




8. To open this drive, you need to first unlock it with smart card


9. Click **Unlock**, input correct device PIN in pop-up window and click OK. The drive is now unlocked and can be accessed normally.



# Chapter 3. VPN

mToken CryptoID can be integrated with existing PKI applications seamlessly ( the developer needn't to execute any programming tasks except for some corresponding services' configuration).

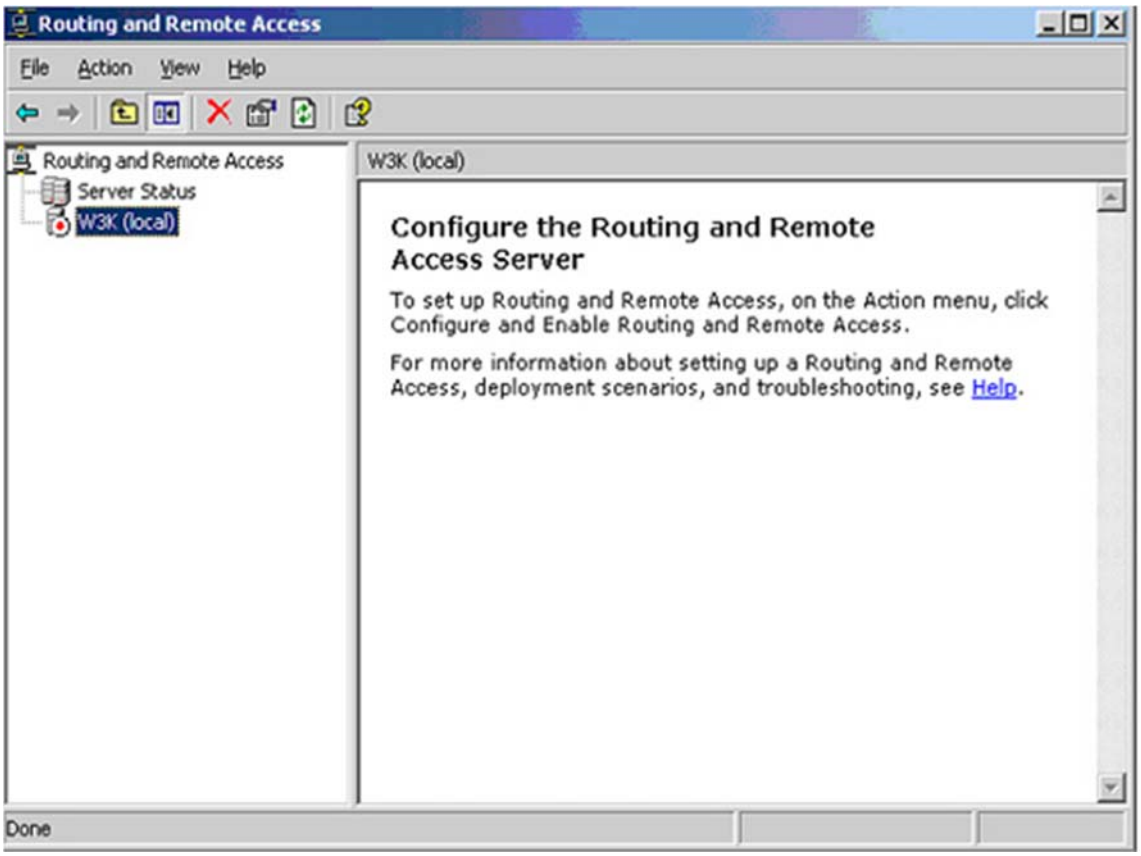
Currently, we can see most PKI applications use PKCS#11 and Crypto API (CAPI) standard interface; CAPI is mainly used on Windows platform while PKCS#11 can be used on cross-platform systems like Windows, Linux as well as Mac OS X.

This chapter mainly describes how to connect VPN with mToken CryptoID.

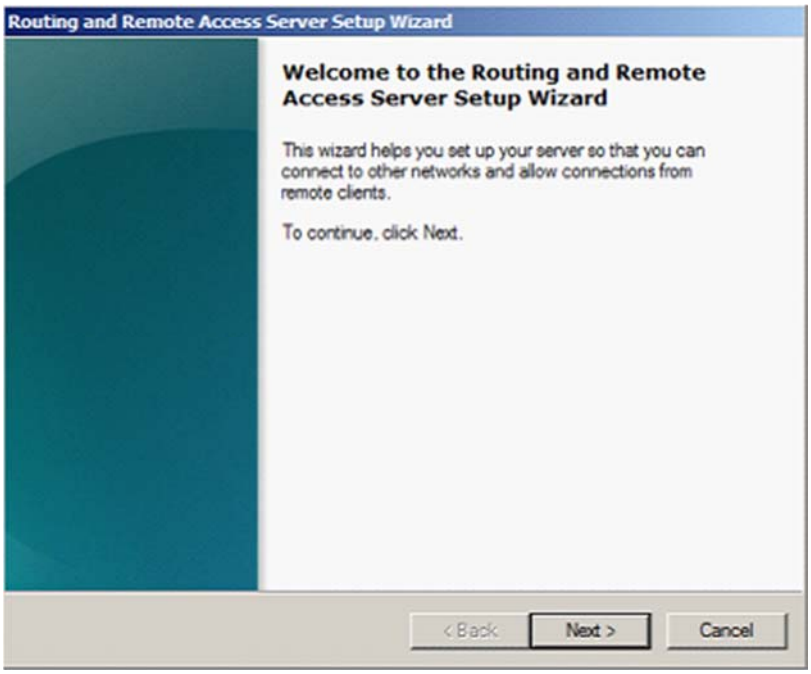
## 3.1 Server Configuration

### 3.1.1 VPN Installation

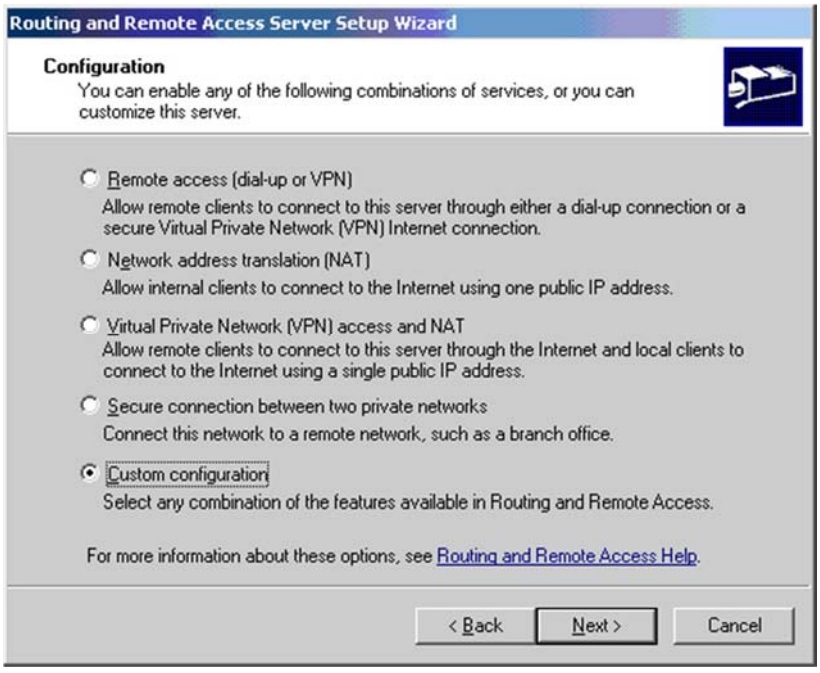
1. Select **Control Panel →Administrative Tools →Routing and Remote Access**



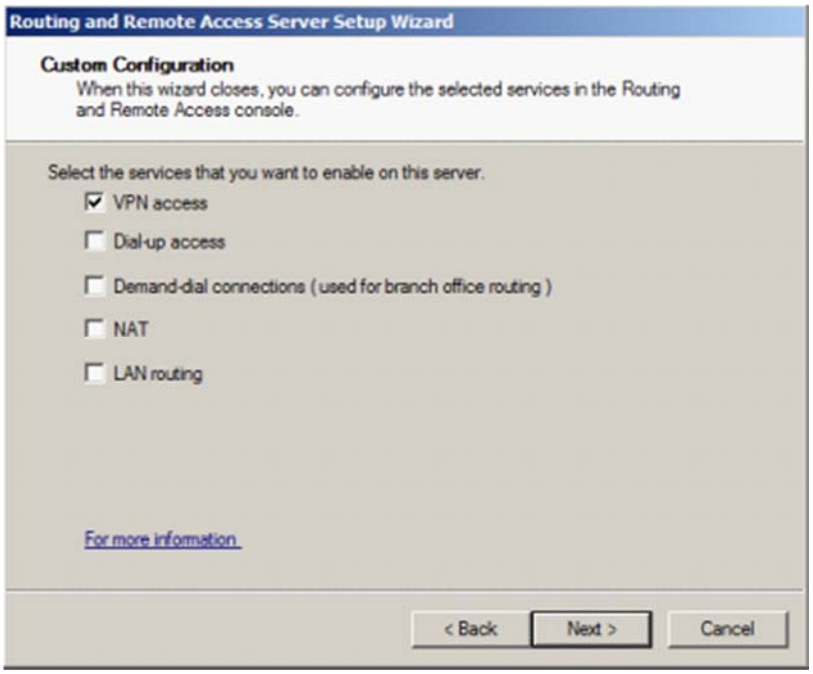

2. Right-Click W3K(local) and select **Configure and Enable Routing and Remote Access**



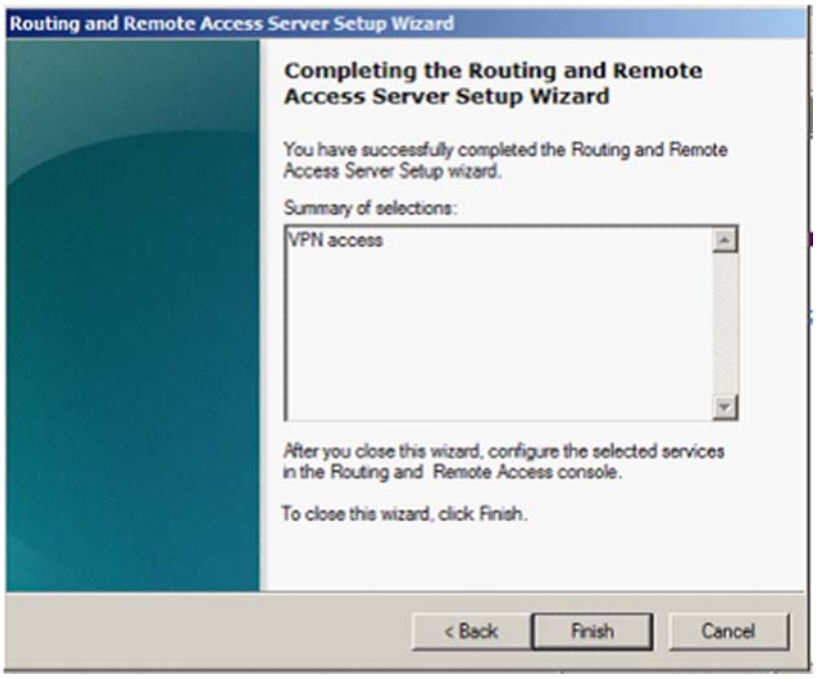

3. Follow the setup wizard and click **Next**, select **Custom configuration**




4. Click **Next** and select **VPN access**

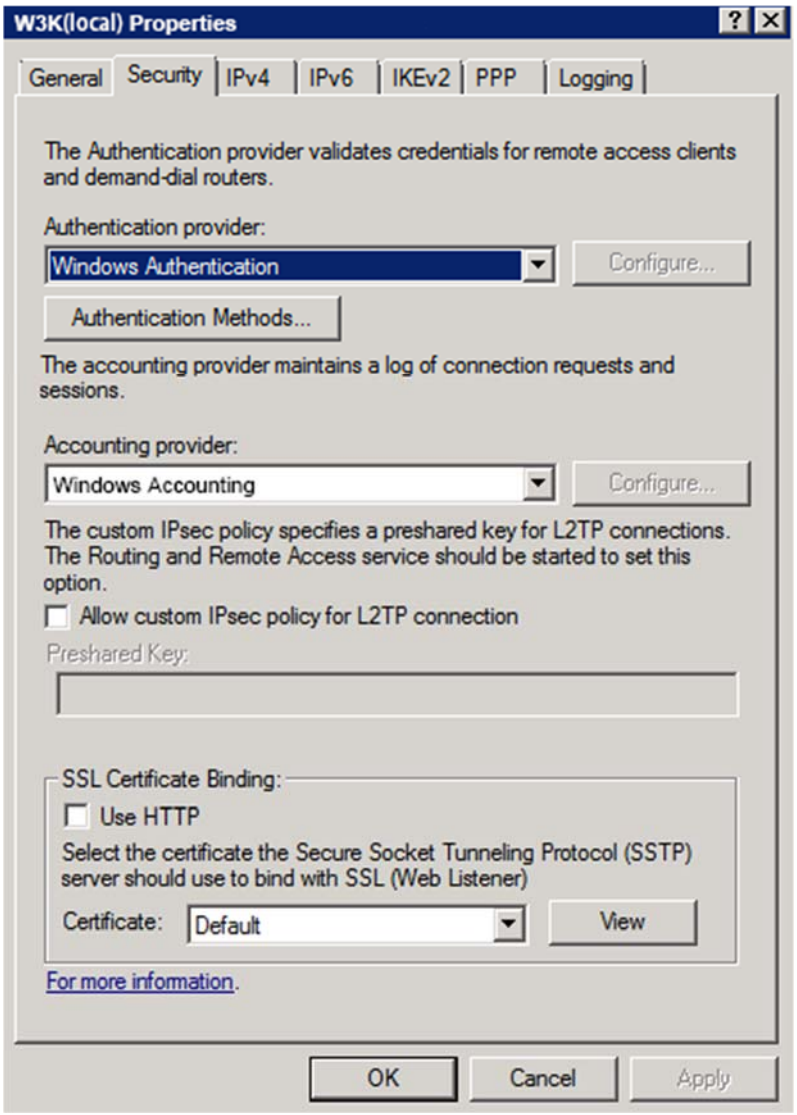



5. Click **Next** and **Finish**

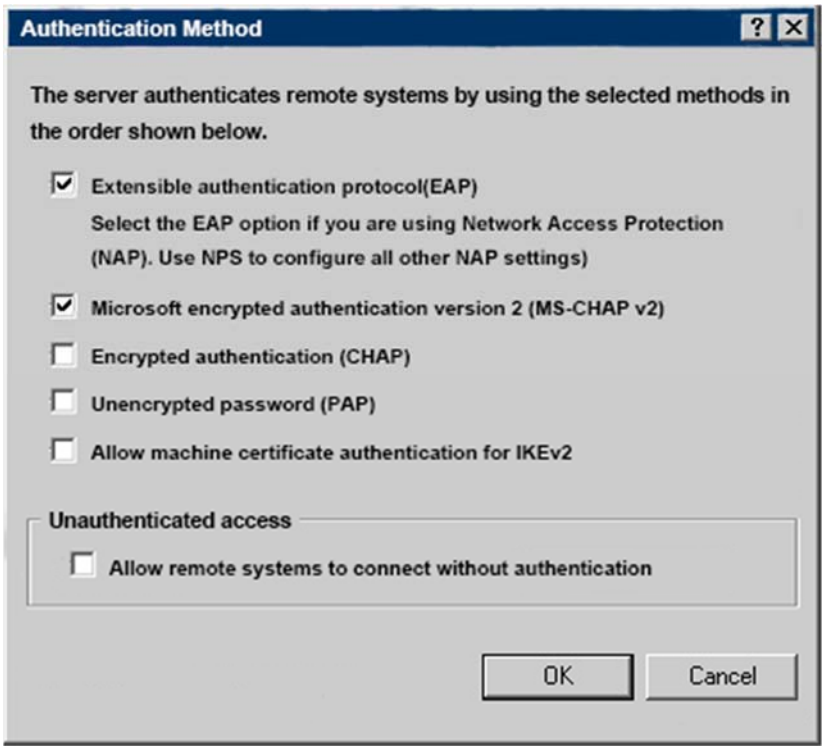



### 3.1.2 VPN Configuration

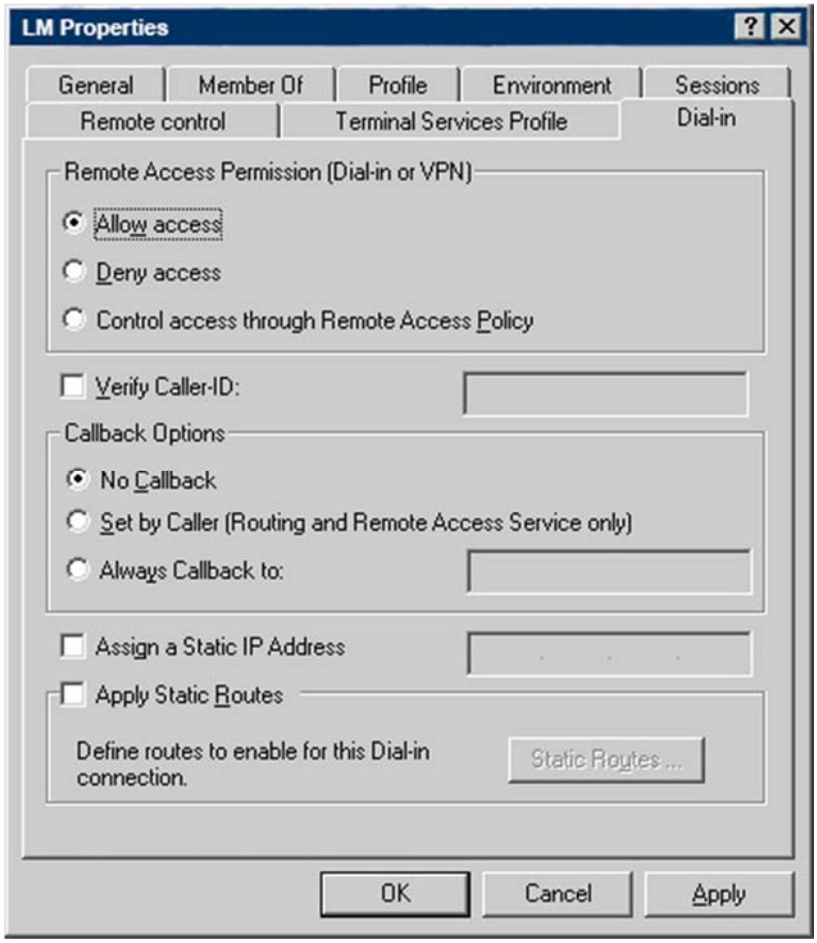
1. Back to **Routing and Remote Access**, right-click W3K(local) and select **Properties** → **Security**




2. Click **Authentication Methods** button, select **Extensible Authentication Protocol** to support smart card identity authentication




3. Set user permission, allow dial-in VPN

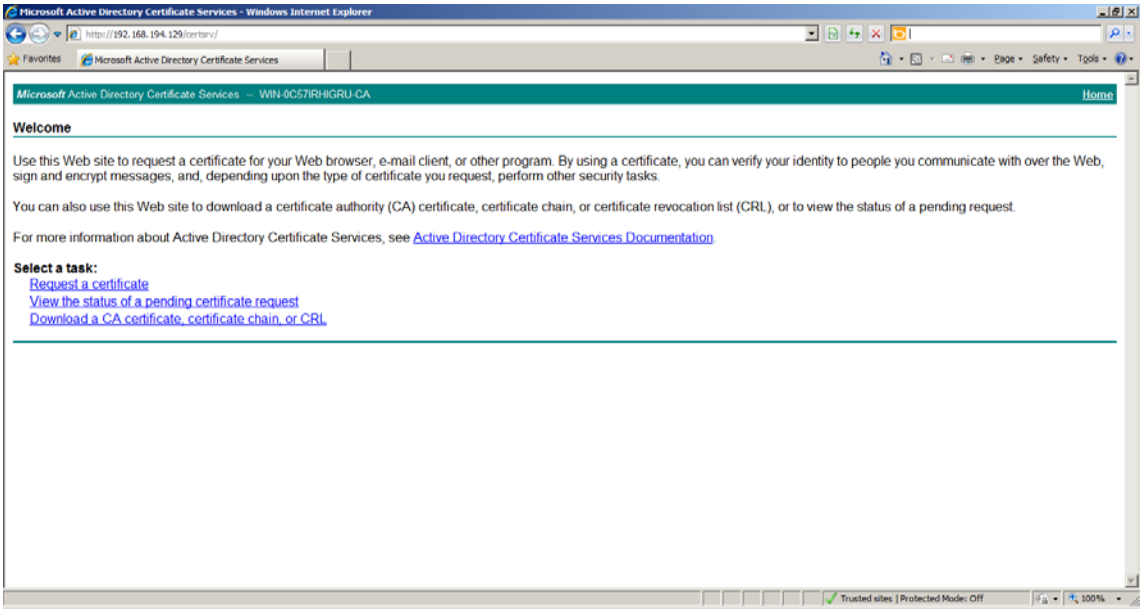


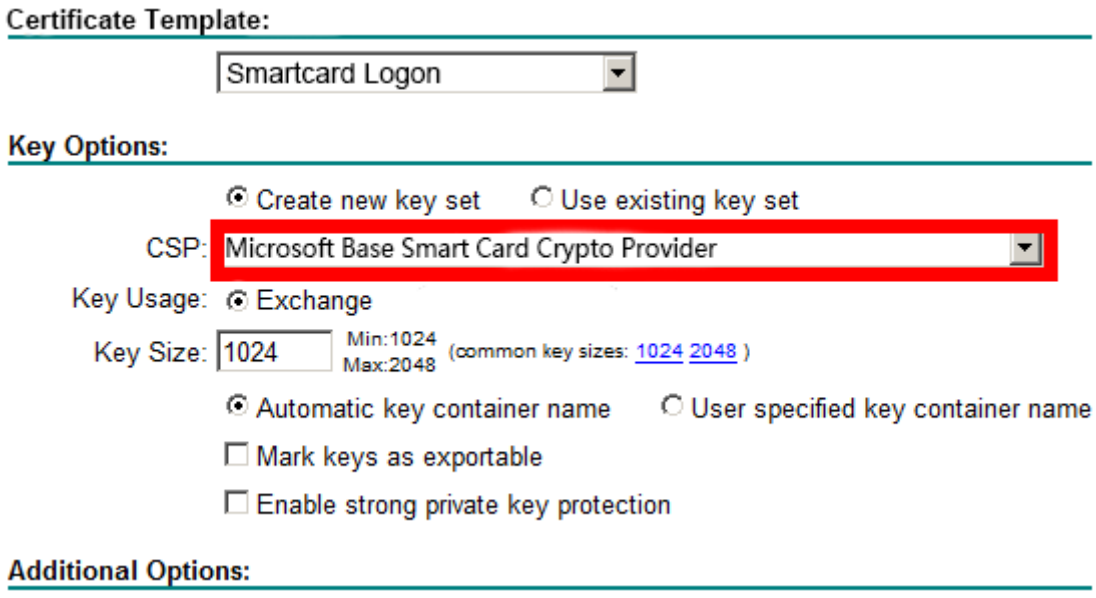
## 3.2 Client Configuration

### 3.2.1 Request a Smart Card Logon Certificate

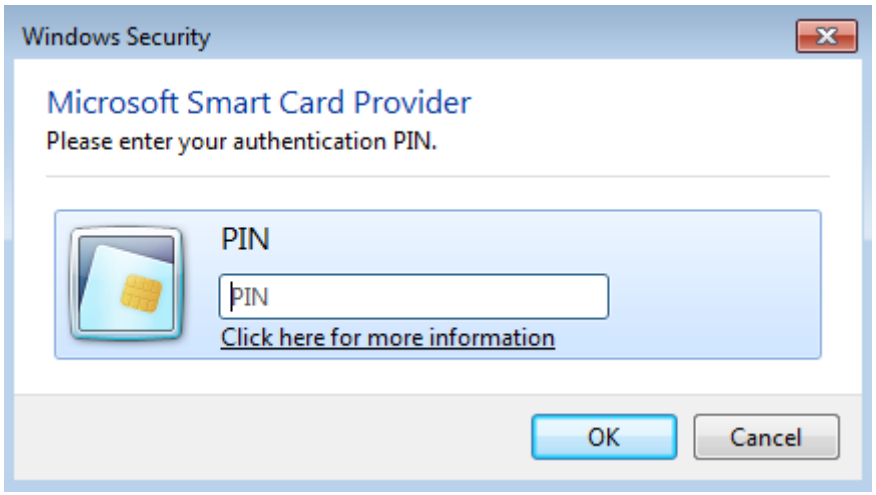
1. Make sure mToken CryptoID device has been connected to your computer. Open the certificate server page through Internet Explorer. (Here I will access my CA Server http://192.169.194.129/certsrv)



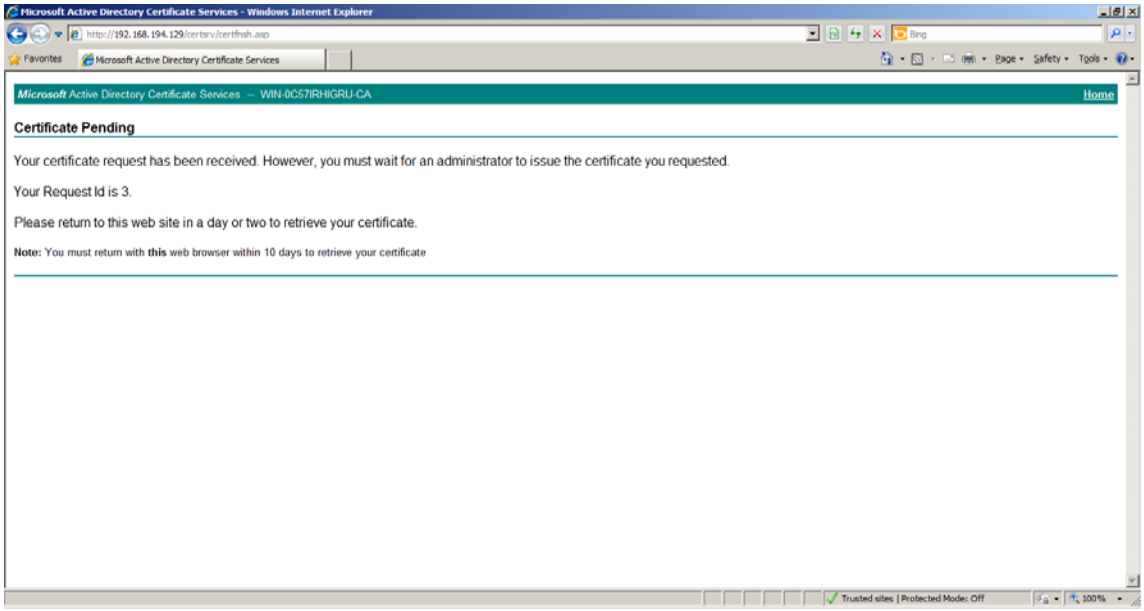

2. Select **Request a certificate →Advanced Certificate Request →Create and submit an application to the CA**. In Certificate Template Area, select smart card related template (Smartcard User or Smartcard Logon). Select **Microsoft Base Smart Card Crypto Provider** as the CSP.



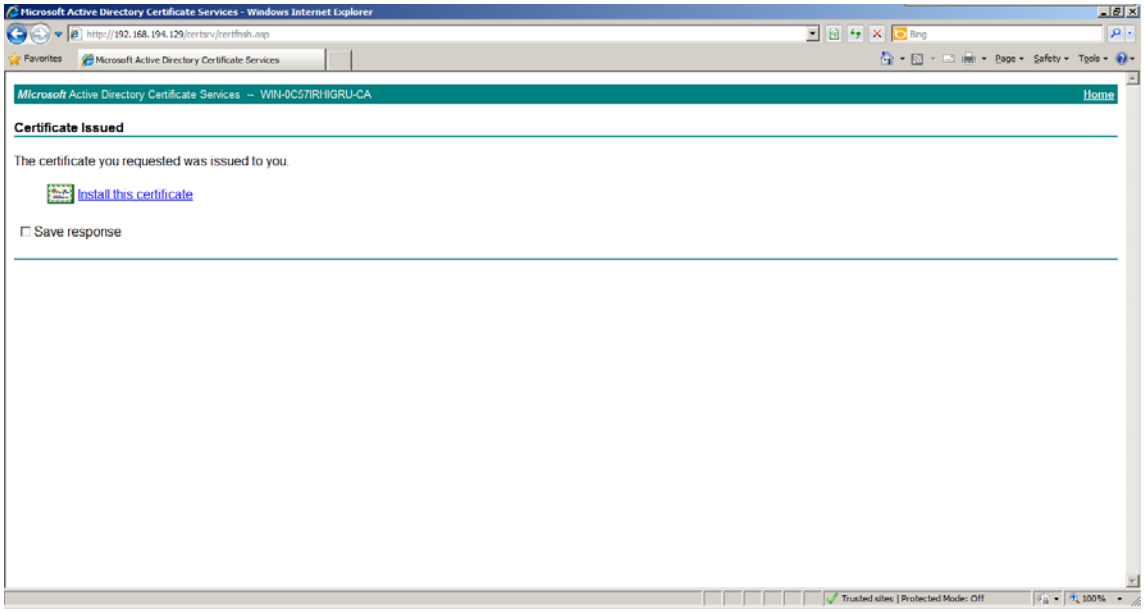

3. Finish the above Settings,click**Submit**, the PIN dialog box pops up.




4. Type the correct PIN and click **OK**, a pending certificate page will be displayed; you need to wait for issuer to authenticate and issue the certificate:

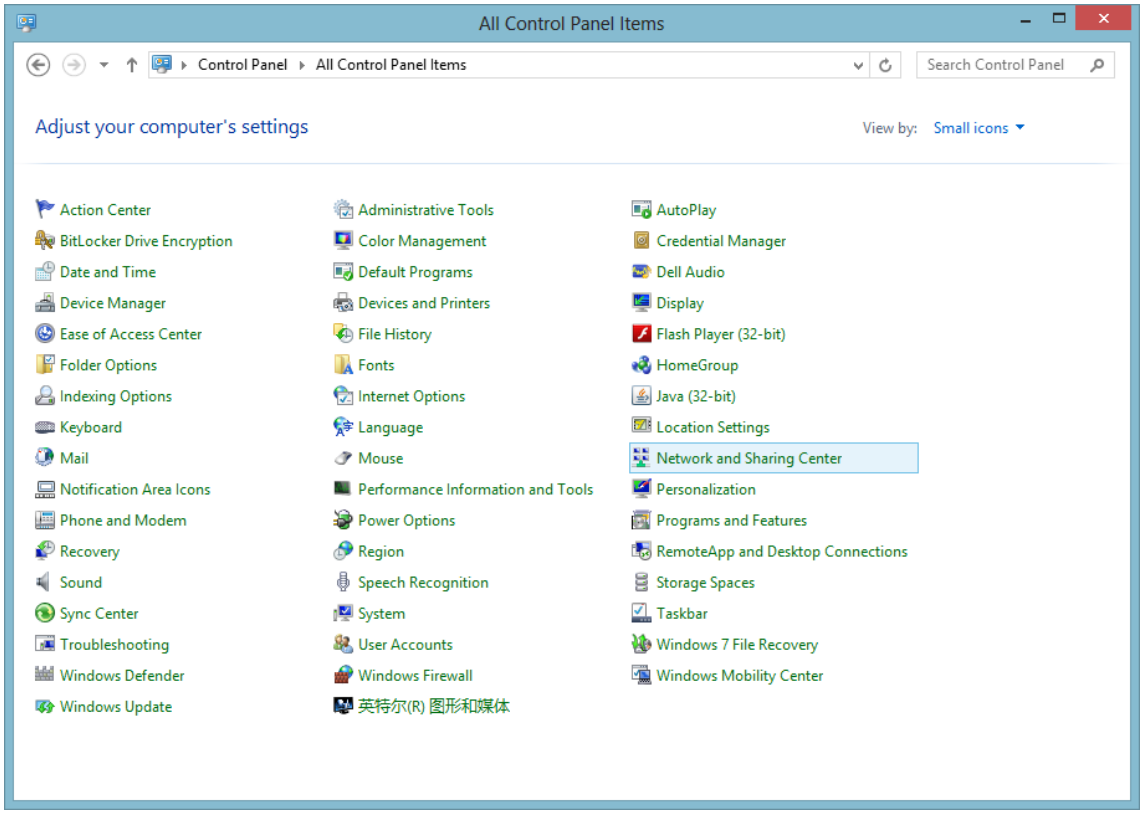



5. Back to **Step 1**, select **view pending certificate request status**. After receive the notification from the Certificate Authority, you can get the certificate. When installing the certificate, system will also verify the PIN, click **Install this certificate**, you can determine whether the certificate is correct installed according to the prompts.

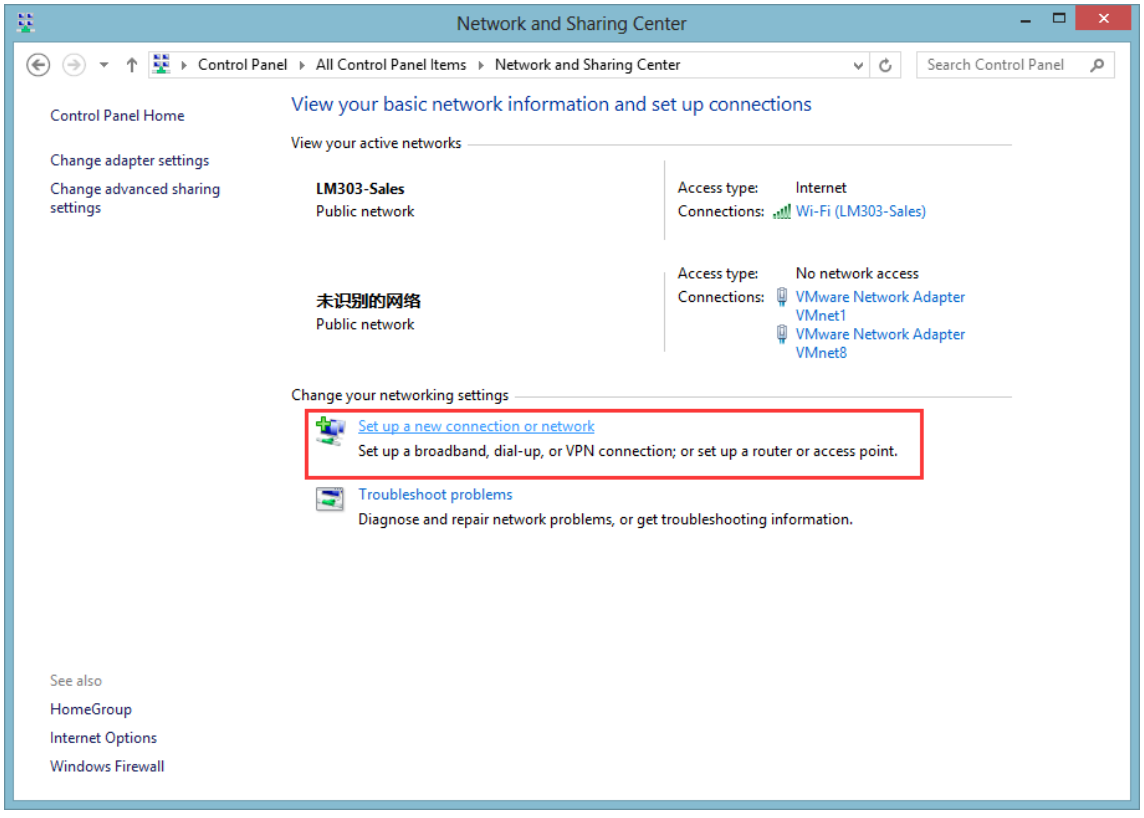



### 3.2.2 Establish Connection

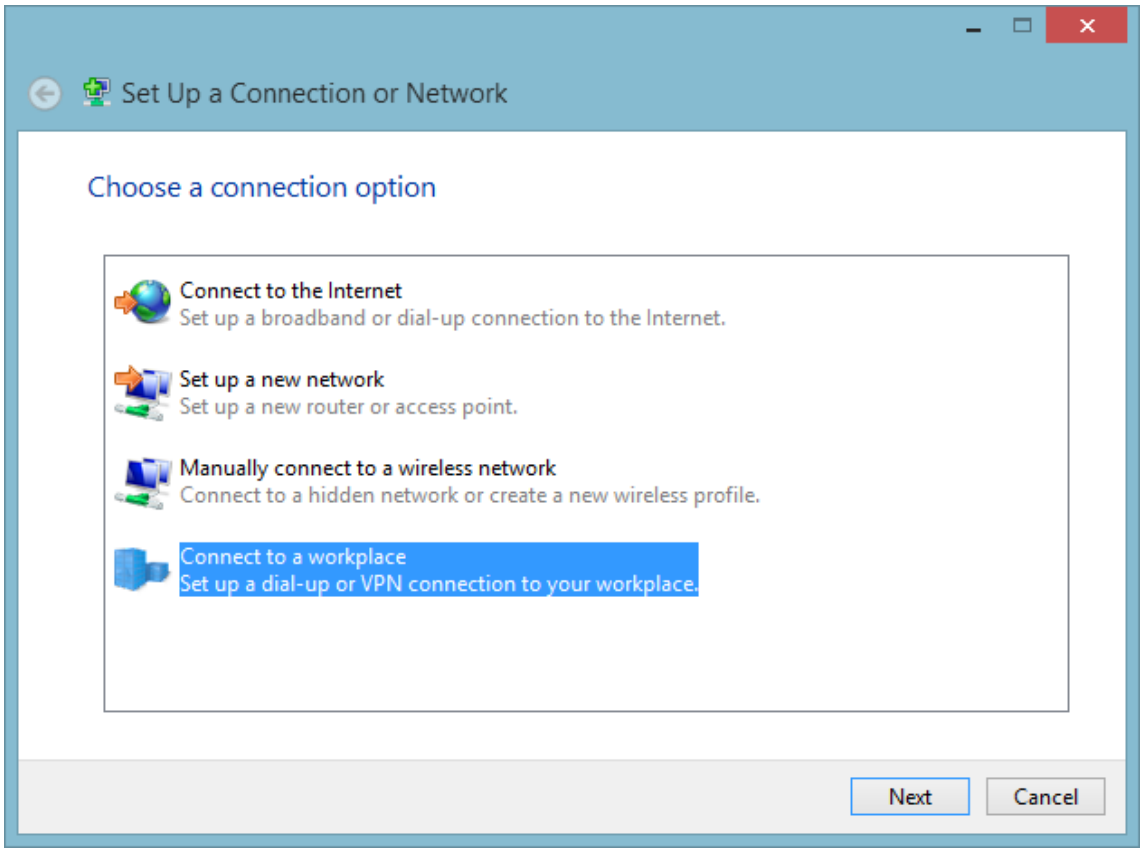
1. Select **Control Panel →Network and Sharing Center**



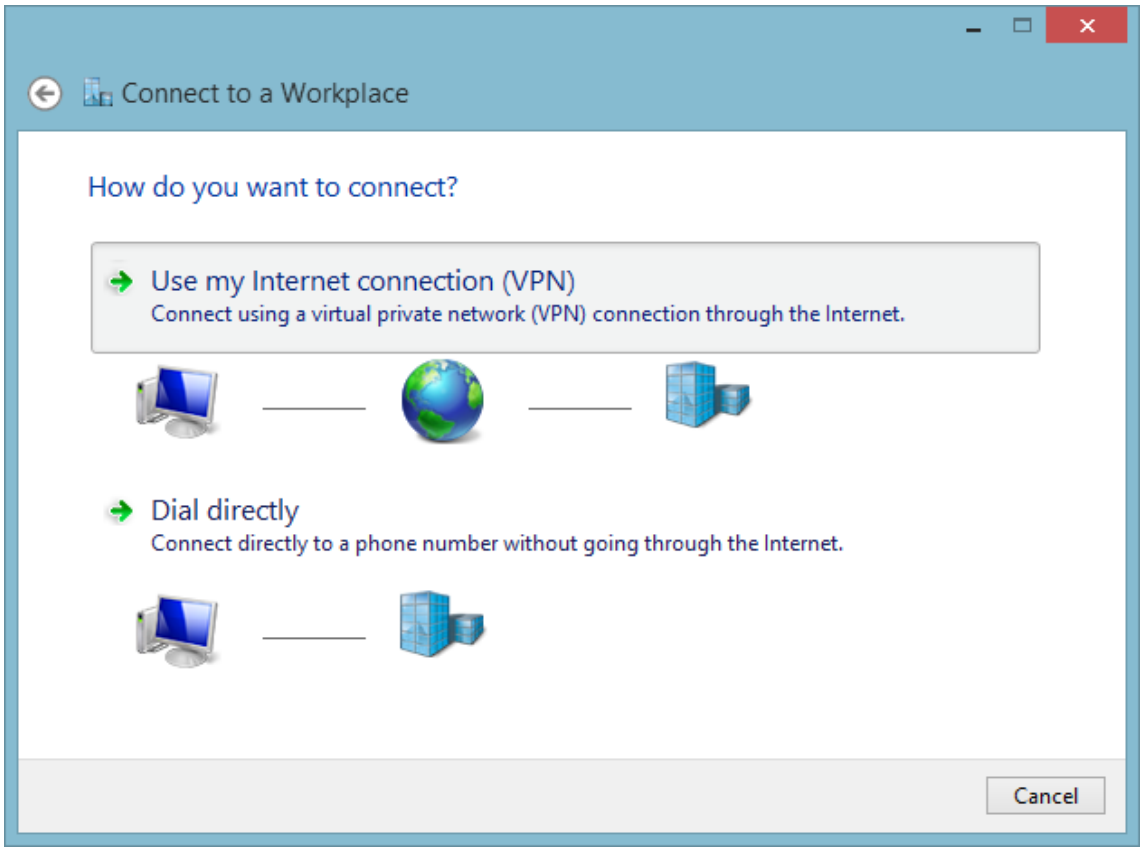

2. Select **Set a new connection or network**



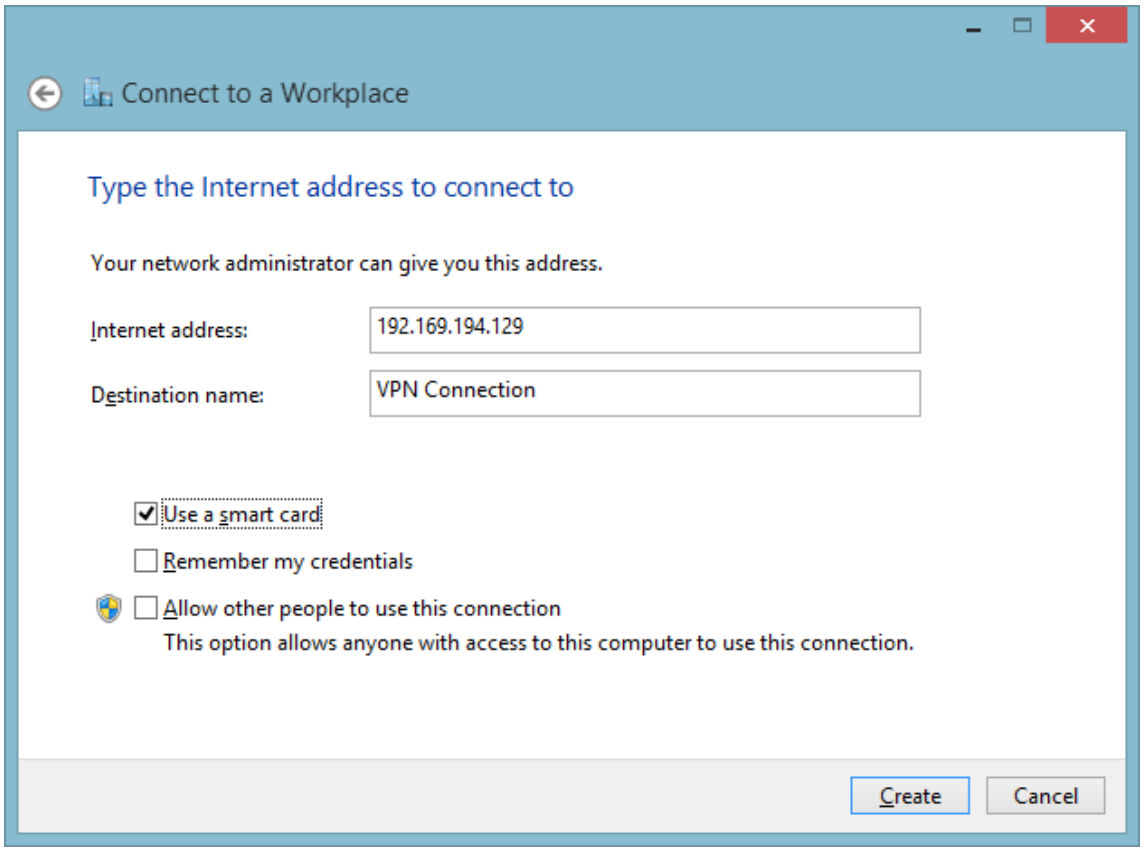

3. Select **Connect to a workplace**, click **Next**



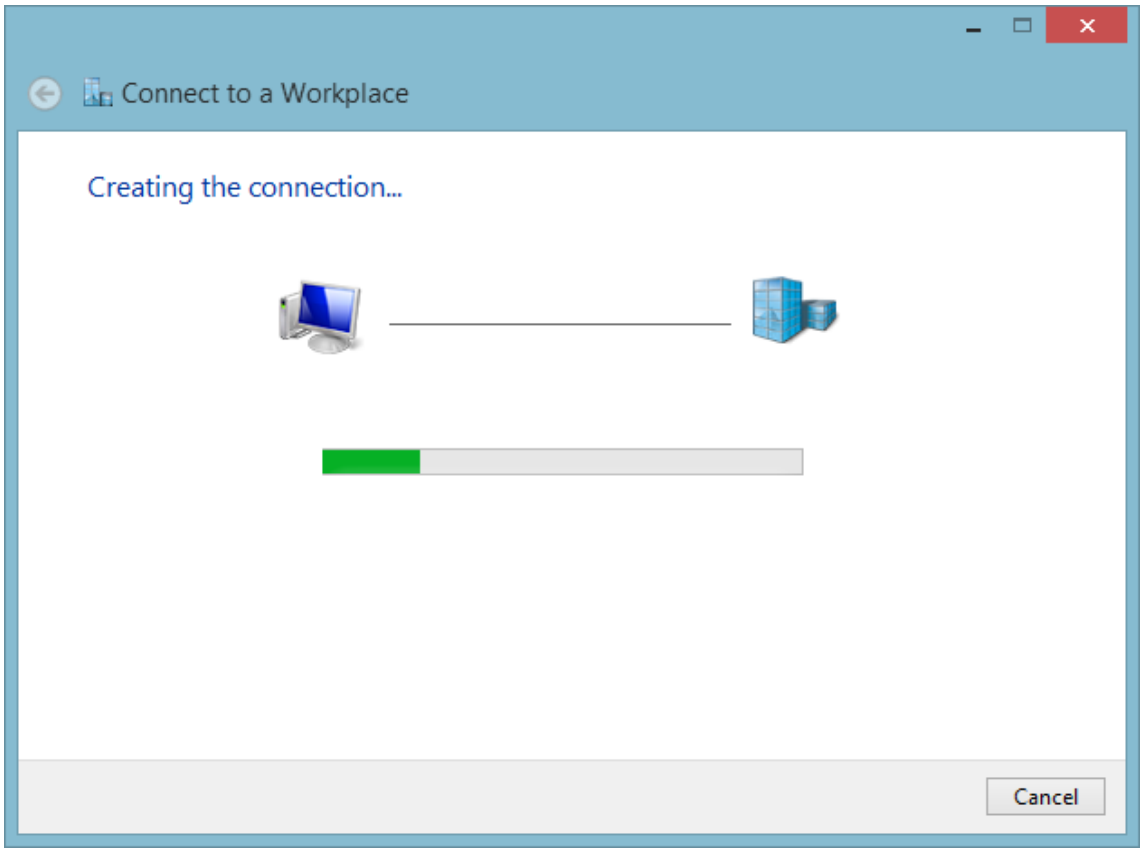

4. Select **Use my Internet connection(VPN)**



5. Type the server address and select Use a smart card, click **Create**



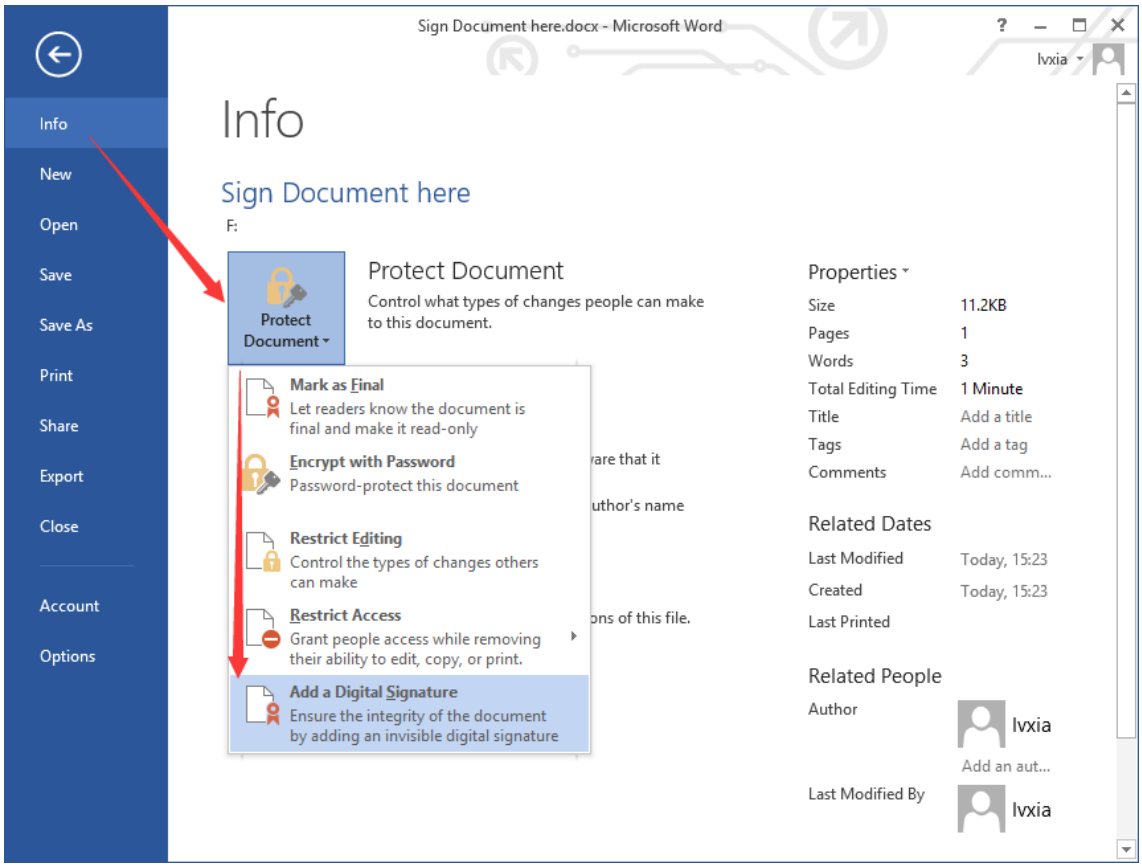

6. Now your VPN connection has established



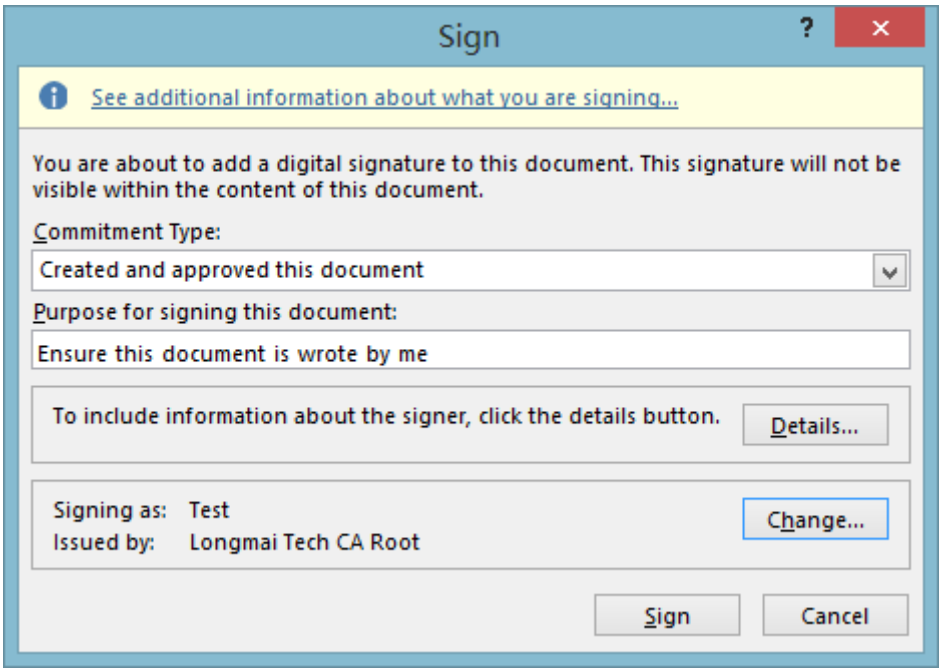
# Chapter 4. Office Document Signature

## 1. Sign office document

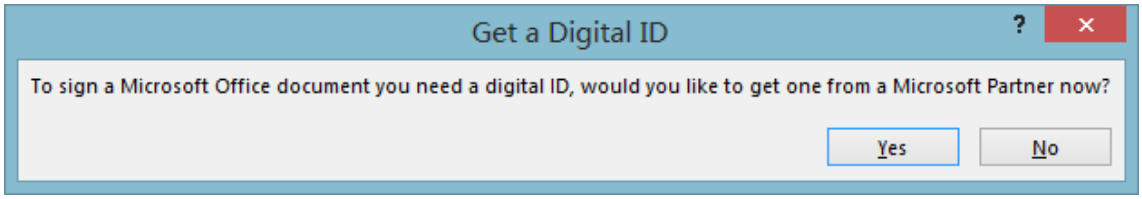
1. Ensure mToken CryptoID contains required certificate. Connect mToken CryptoID to the PC.
2. In office word document, select **File →Info →Add a Digital Signature**




3. Select **Commitment Type** and write your **Purpose**. By default, the latest certificate will be selected, but you can also click **Change** to select your preferred signature certificate.

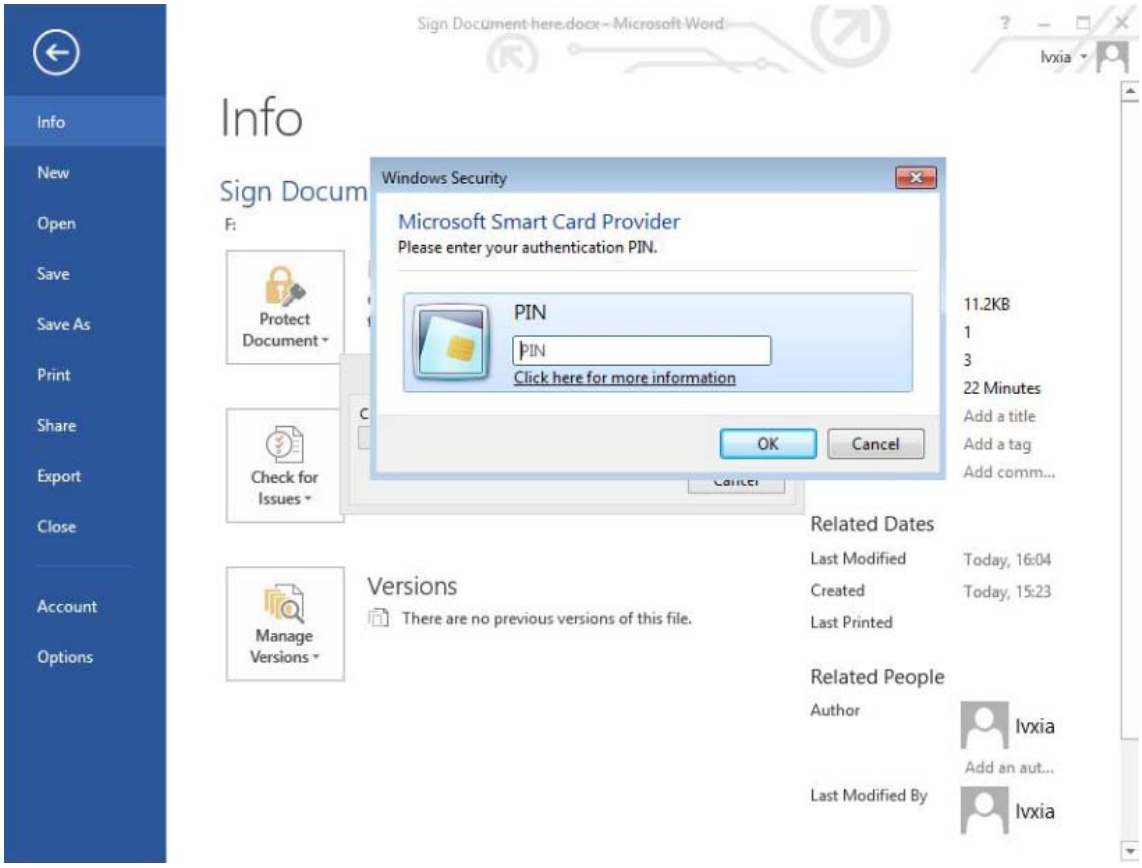



4. If you don't see the window above, but instead receive below pop-up window. It means there is no certificate found on your computer; please make sure the connected mToken CryptoID contains corrected certificate. If you can see the window above, please **Sign** and skip this step.




5. Then click **Sign**, you will be asked to input device User PIN.

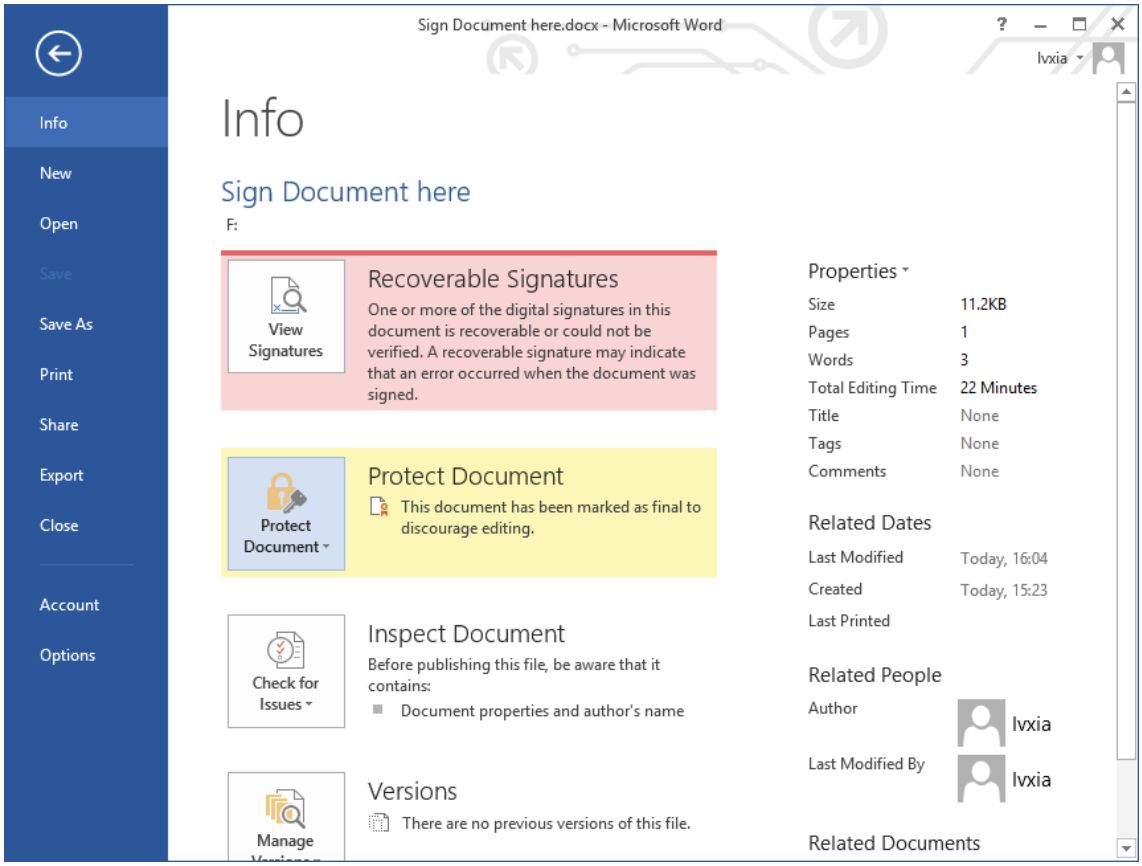
   Default User PIN is: 12345678 (If you changed it, please use your new user pin)



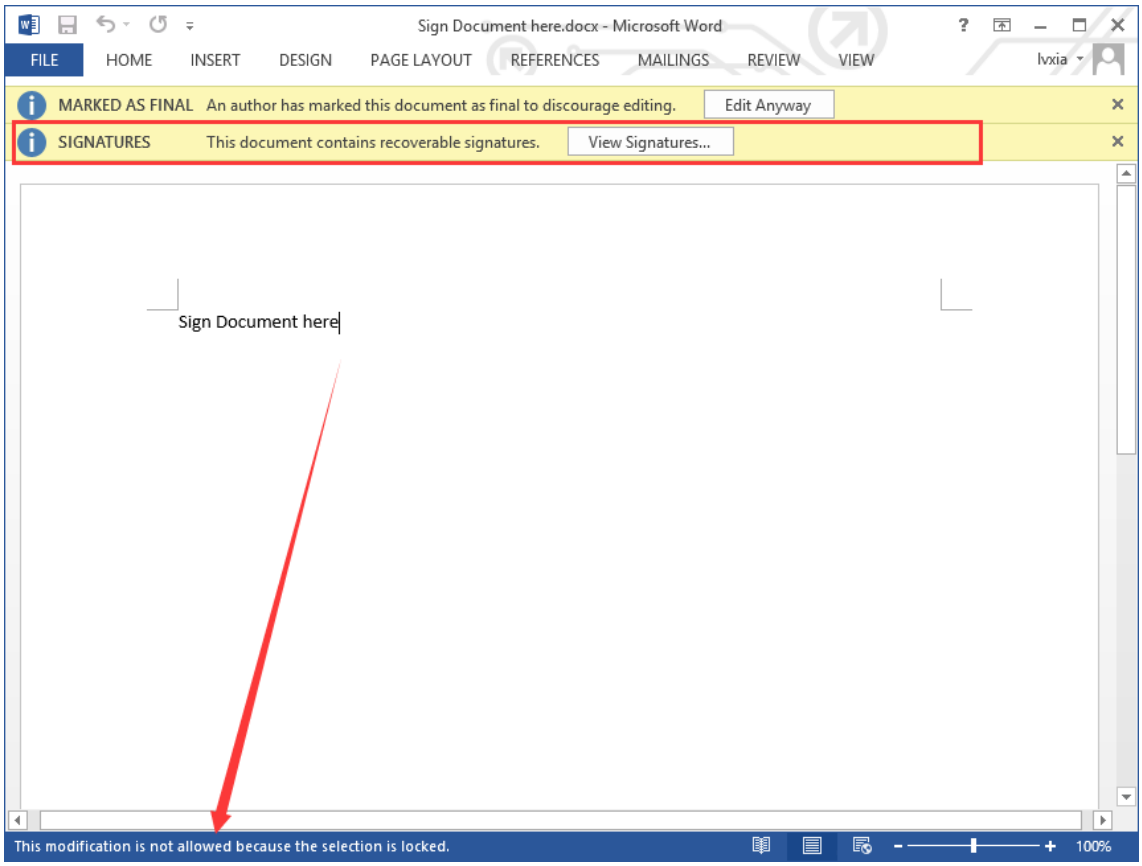

6. Click **OK** to sign this document; you will get a success confirmation dialog.


7. Click **OK. (**you will find that the document has been signed)

c




8. For example, when I try opening this document and attempt to modifying it, the message about document is locked is displayed, and modifying it needs token verification. Meanwhile, the information we have shown us that this document is signed.




9. Click **View Signatures**, select certificate to view details.