



澳門郵政 CORREIOS DE MACAU
電子認證服務 SERVIÇOS DE CERTIFICAÇÃO

Personal Secure Email Certificate Enrollment Guide

Version. 2020-03

Personal Secure Email Certificate Enrollment Guide

Content

Registration	3
Download Certificate	7
Import Certificate into Computer	14

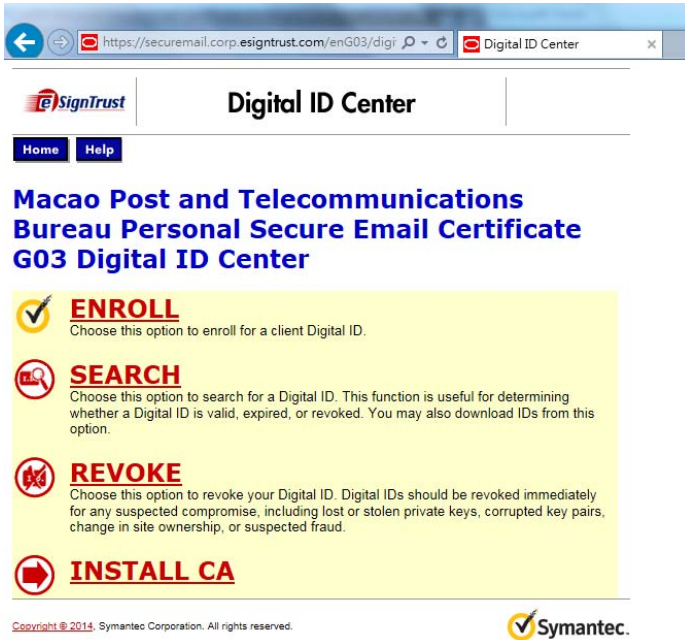
Registration

1. Upon receiving the Secure Email Certificate voucher from eSignTrust Registration Authority, user can proceed to the following link to enroll the certificate:

<https://securemail.corp.esigntrust.com/enG03/digitalidCenter.htm>

Please enroll the certificate with Windows user account who has the administrator rights.

Enter the Personal Secure Email Certificate G03 Enrollment Page, and select “Enroll”.



2. Input the user's information, the Passcode and Passcode ID on the voucher, and setup the Challenge Phrase password, which can be used to revoke the Email Certificate. (The Challenge Phrase must not be disclosed to others)

The screenshot shows the "End-user enrollment for ..." page in a web browser. The URL is <https://securemail.corp.esigntrust.com/enG03/client/userEnrollNS.htm>. The form has a yellow background and contains the following fields:

Nickname or middle initial allowed (Example: Jack B.)	estEmailCertG03Firefox
Last Name: * (required) (Example: Doe)	JBEREVOKED20APR2017
E-mail Address: * (required) (example - jbdoe@esigntrust.com)	nykuan@esigntrust.com
Passcode: (required)	TESTG03FIREFOX
PassCodeID: (required)	000001039
Country: (required) (example - MO)	MO

Annotations with arrows point from text boxes to the following fields:

- First Name: points to the Nickname field.
- Last Name: points to the Last Name field.
- Email address: points to the E-mail Address field.
- Passcode on the voucher: points to the Passcode field.
- Passcode ID on the voucher: points to the PassCodeID field.
- Challenge Phrase password for certificate revocation: points to the Enter Challenge Phrase field.

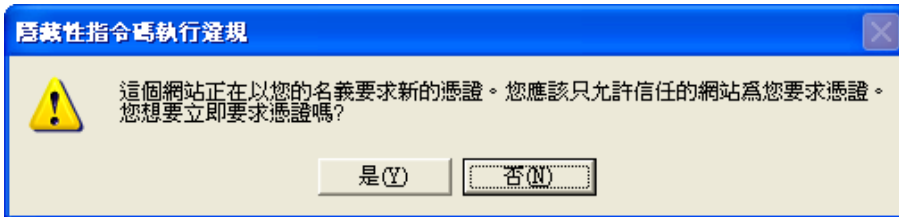
Below the main form, there is a "Challenge Phrase" section with a warning: "The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID." The "Enter Challenge Phrase" field is currently empty and masked with dots.

At the bottom, there is an "Optional: Choose Your Encryption Strength" section with a dropdown menu set to "高等级".

To confirm the email address registered on the certificate, click "OK".



3. After confirming the email address, another message will be prompted to remind that the website is requesting a new certificate on the user's behalf, and asks the user to reconfirm.

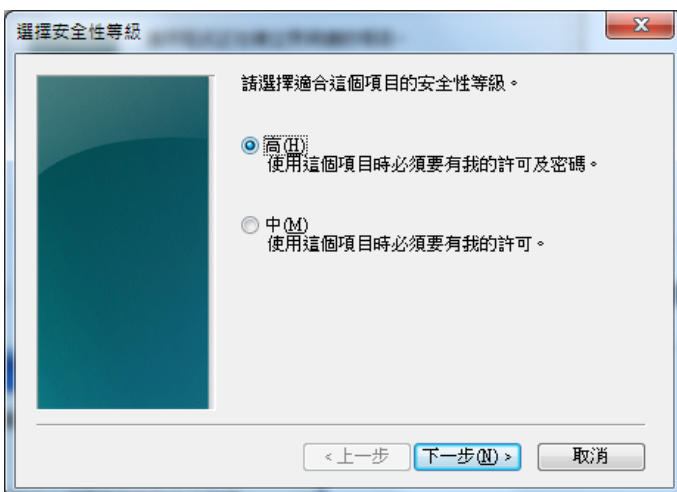


4. During certificate generation, it will be required to set the Security Level.

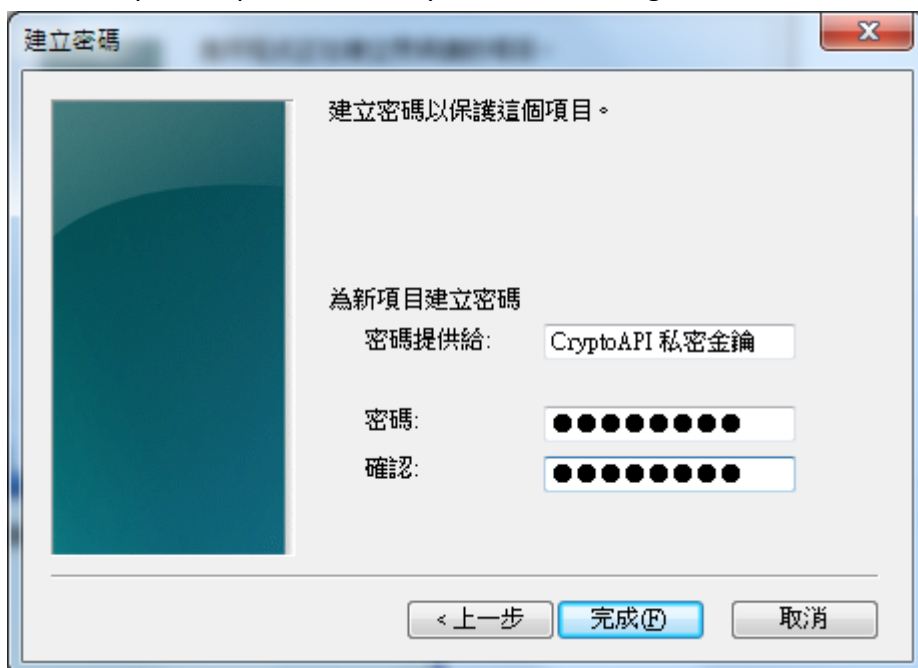


5. Setting Security Level

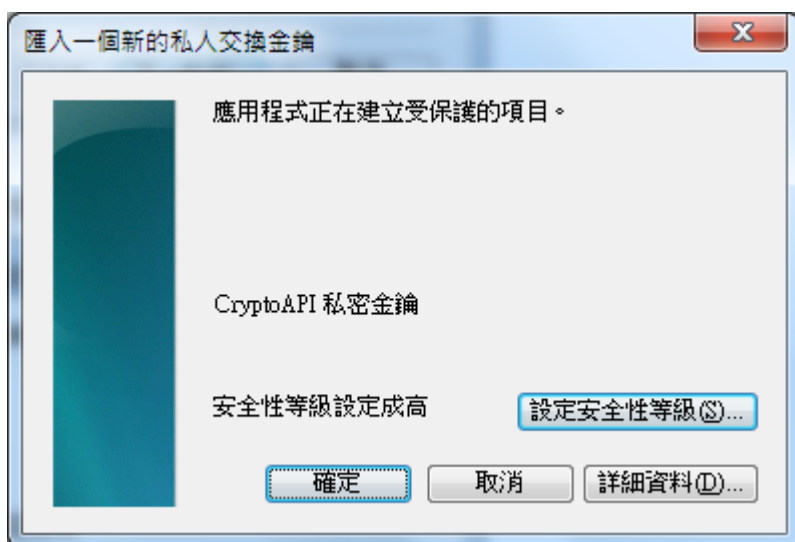
A password will not be needed for Medium Level Security. However, with this level, any other person who can access your computer can also have access to your certificate. Therefore Medium Level is not recommended.



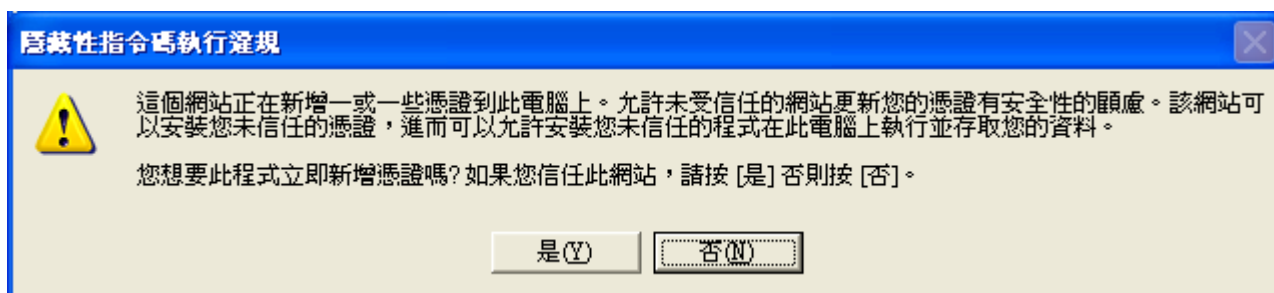
A password will be required to setup to protect your certificate if High Level Security is chosen. User will need to input the password every time when using the certificate.



6. Select "OK" after the Security Level and Password have been set.



7. Select "Yes" to confirm adding the certificate into the computer.



8. Message will show up after successful generation of the certificate. The certificate will be stored in the Windows Certificate Repository and ready to be used on Email software such as Microsoft Outlook.

Digital ID Installation and... x

https://securemail.corp.esigntrust.com/enG03/cgi-bin/haydn.exe

SignTrust Digital ID Services

Congratulations!

Your Digital ID has been successfully generated and installed.

Your Digital ID Information.

Organization = Macao Post and Telecommunications Bureau
Organizational Unit = Personal Secure Email Certificate G03
Organizational Unit = Terms of use at www.esigntrust.com
Common Name = TestEmailCertG03Firefox TOBEREVOK
Email Address = tammykuan@esigntrust.com
Serial Number = 3cc8b66c58fe3f0a930040d92b1f0c77

Consult our Help Desk and Tutorials:

1. Go to the [Help Desk](#) to view our tutorials and other useful information.
2. Go to the [Digital ID Center](#) to find out more about Digital IDs and Digital ID services.

Copyright © 2014, Symantec Corporation. All rights reserved.

Symantec

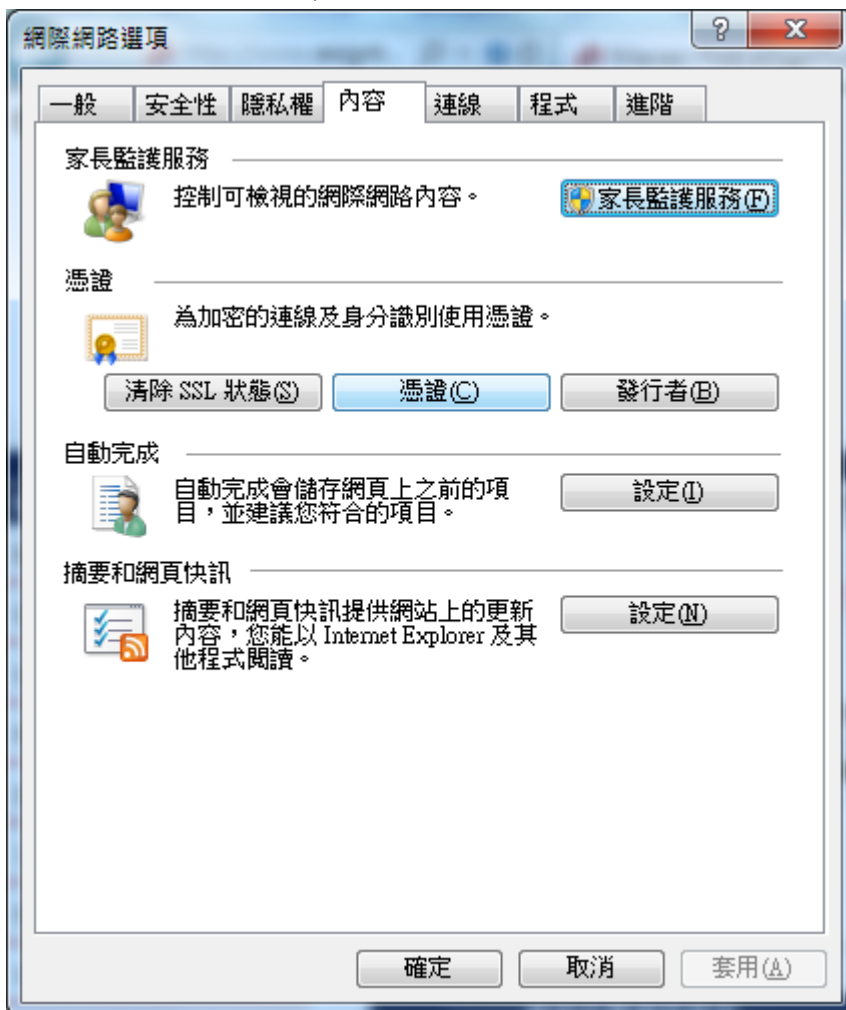
Download Certificate

In order to download the certificate and use on other computers, please follow the instructions below:

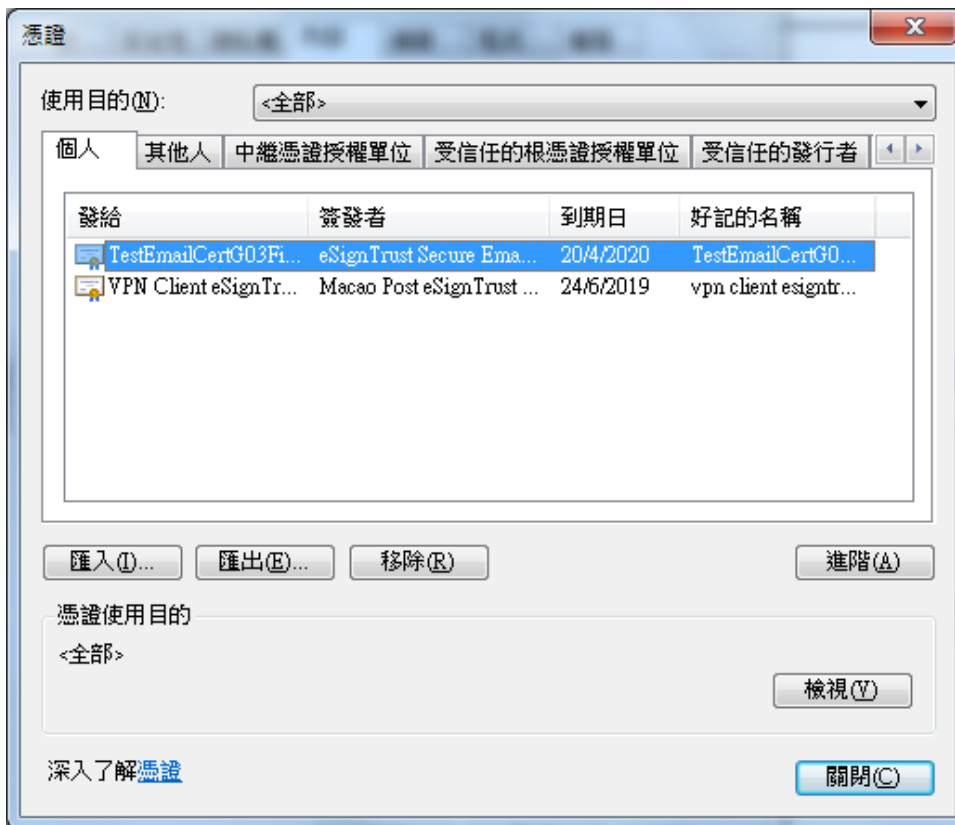
1. On the Internet Explorer web browser, select “Tools” -> “Internet Options”.



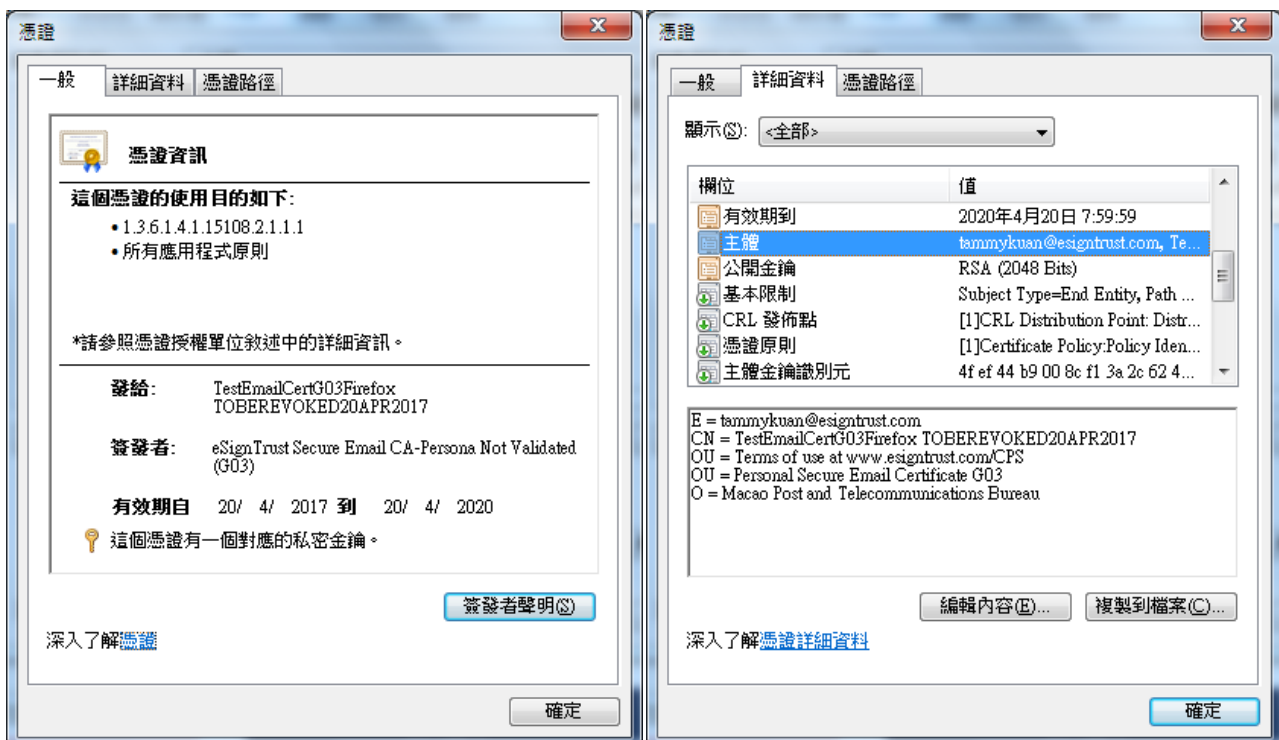
2. Go to the tab “Content”, then select “Certificates”.



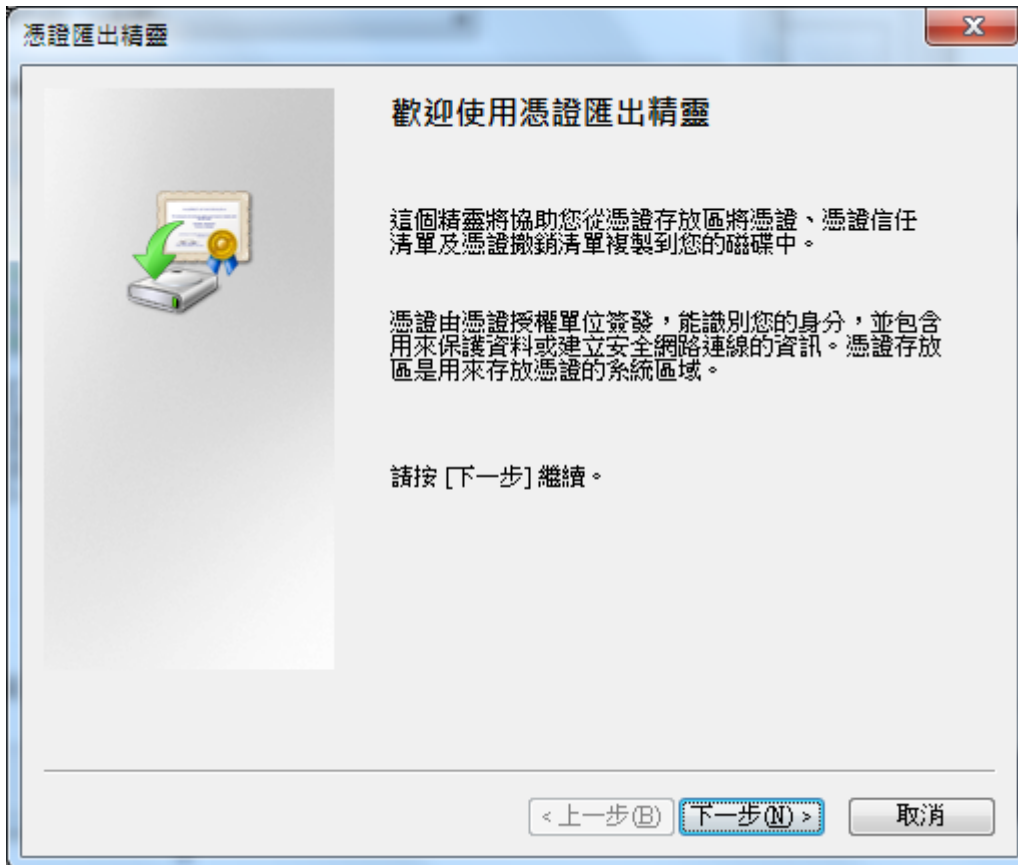
3. Select the required certificate.



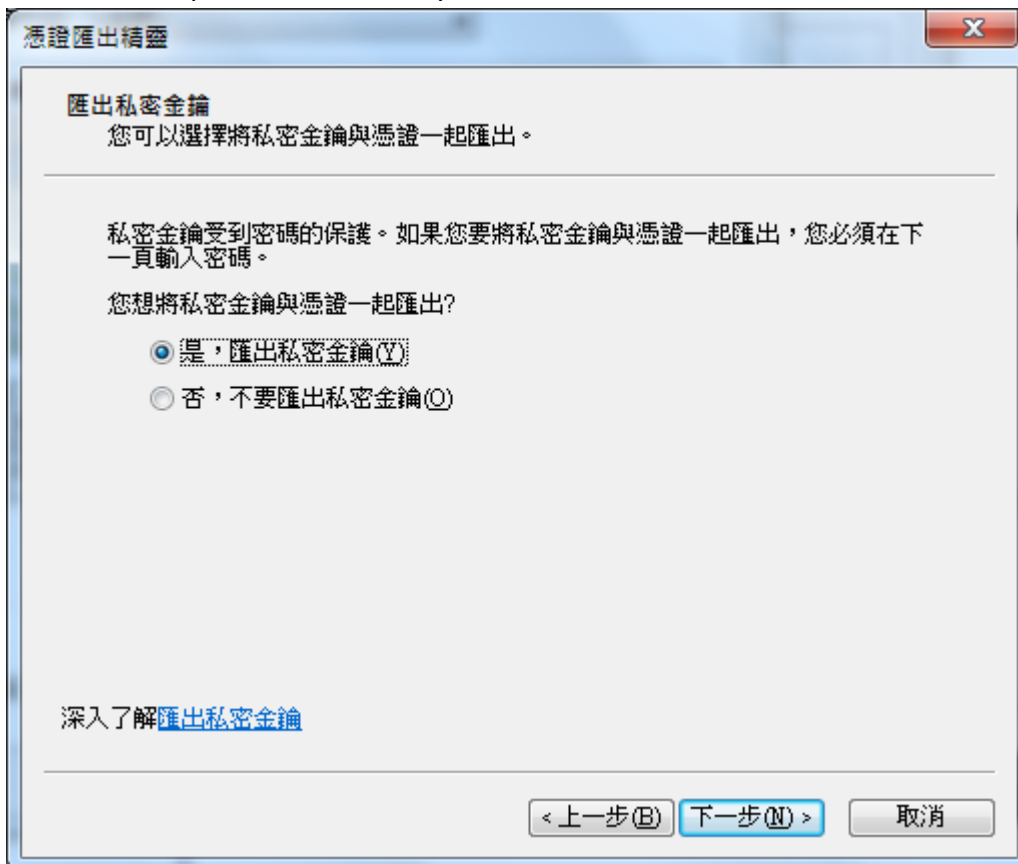
4. Select "View" to open the certificate, then choose "Details" to check the certificate information.



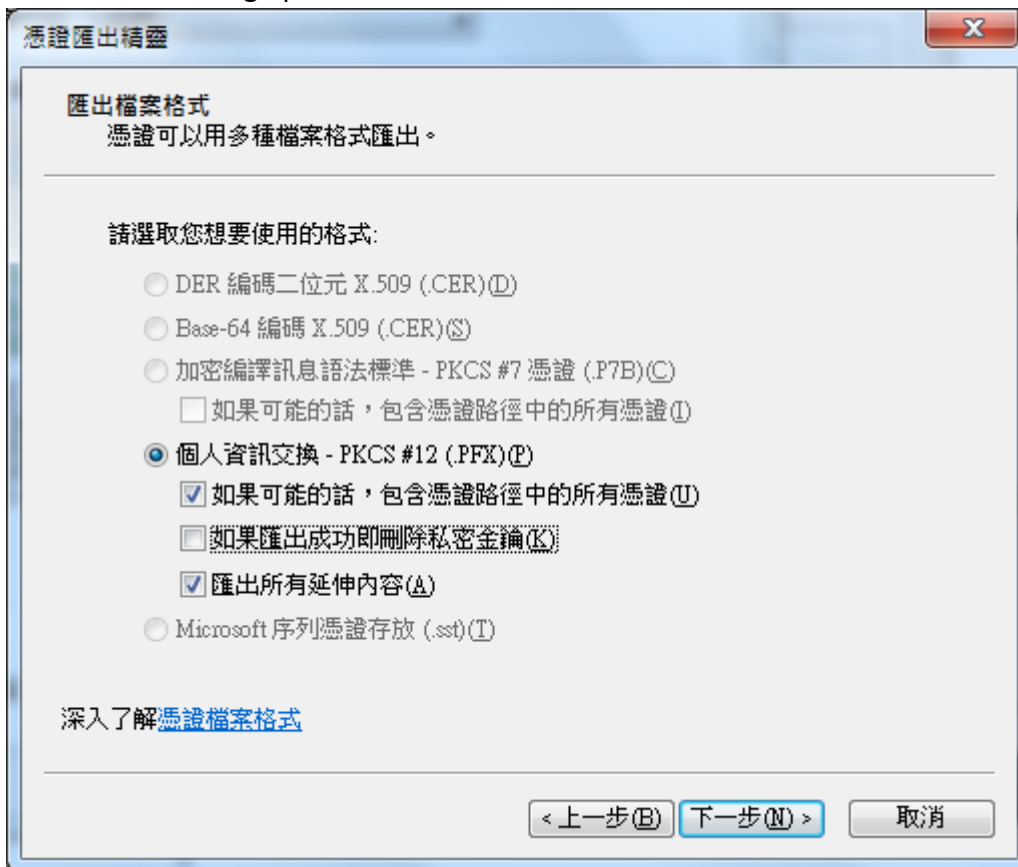
5. To download/export the certificate, select “Copy to file”, then “Next”.



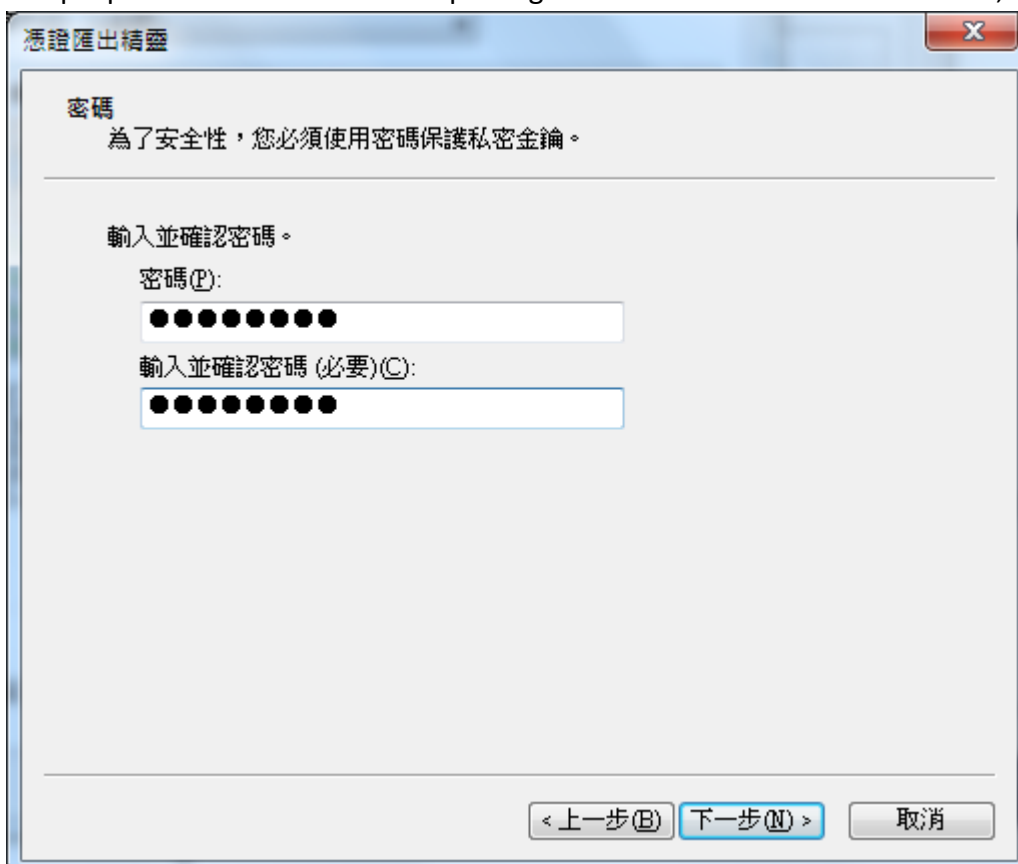
6. Select “Yes, export the Private Key”, then “Next”.



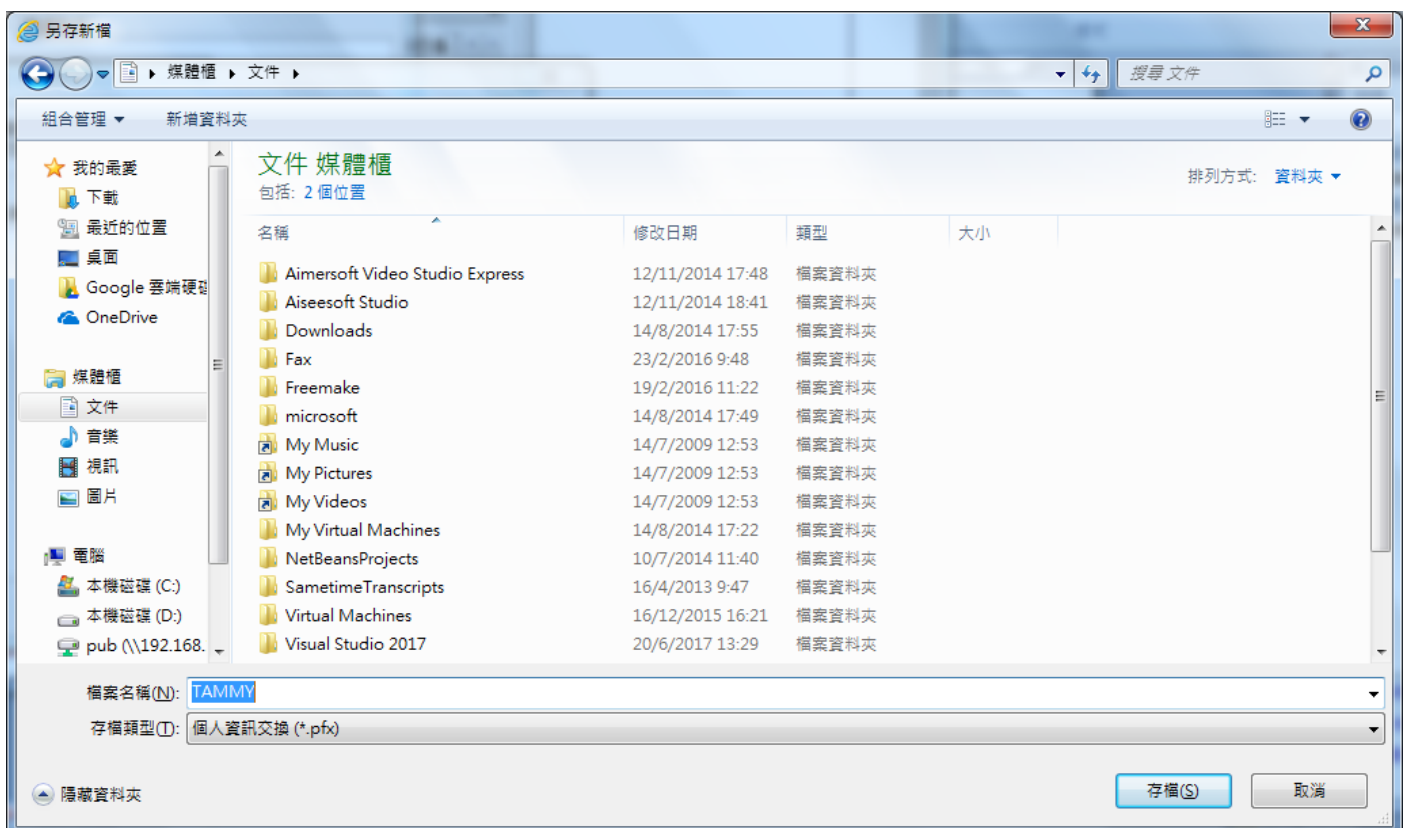
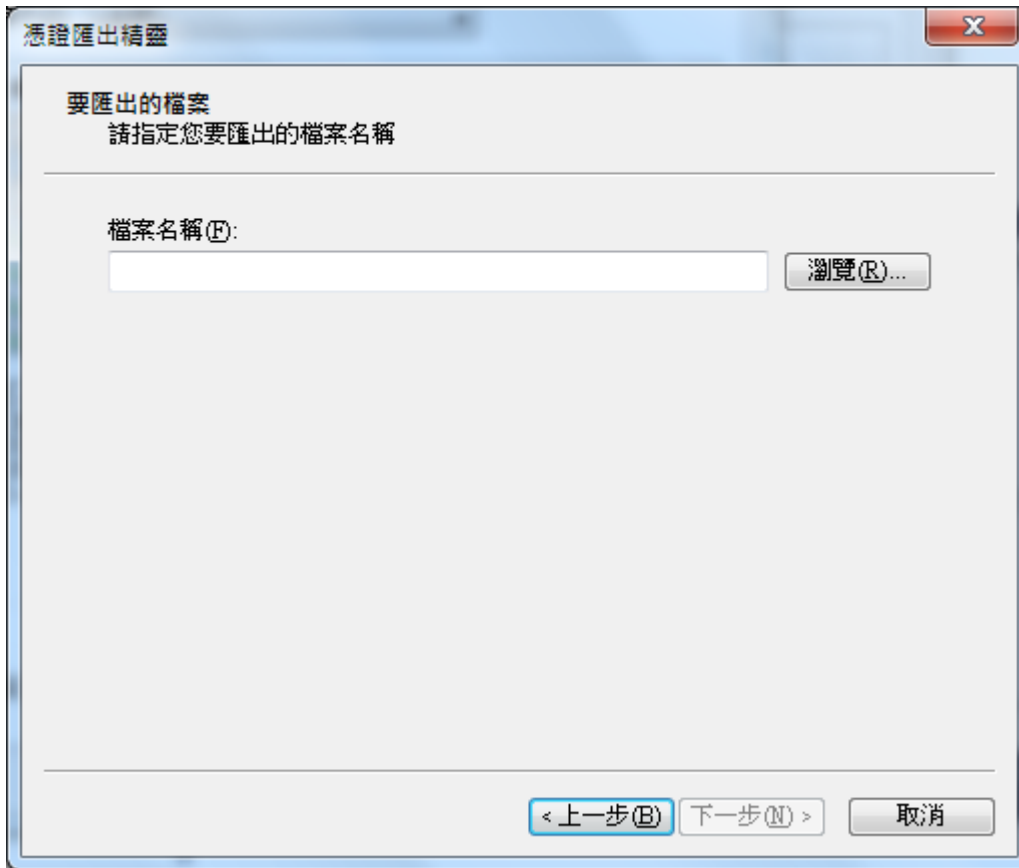
7. Select the following options then click “Next”.



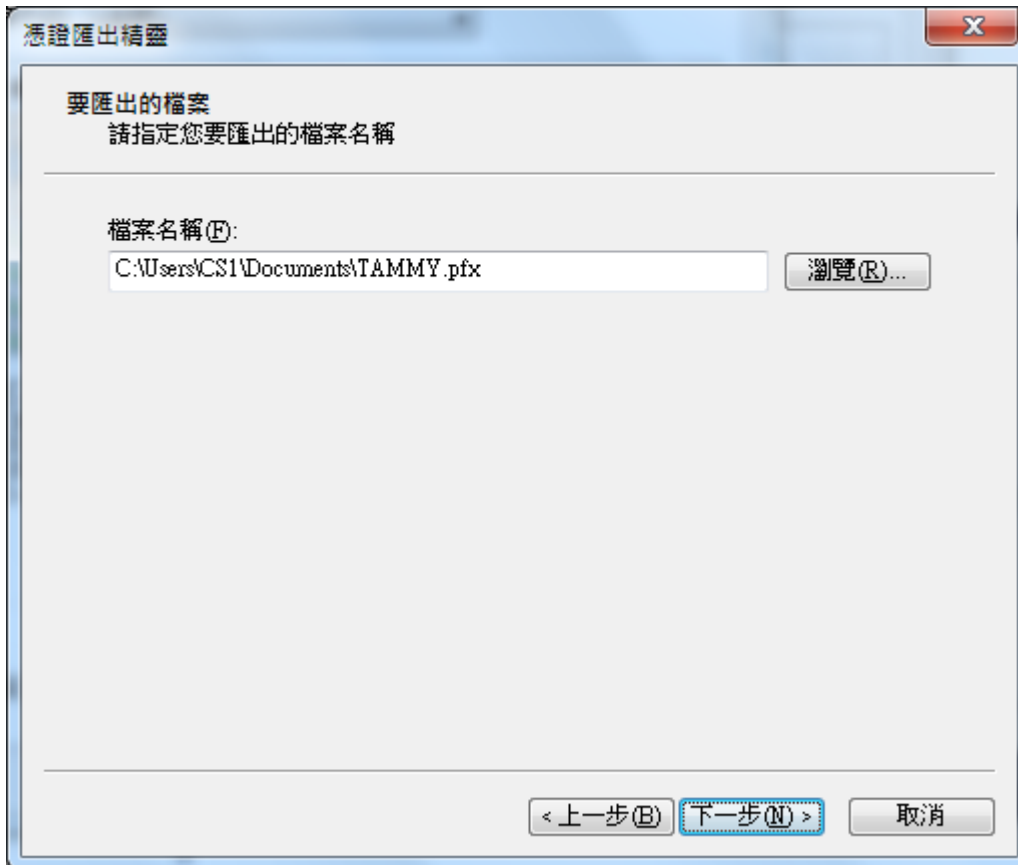
8. Setup a password for use when importing the certificate to the web browser, then click “Next”.



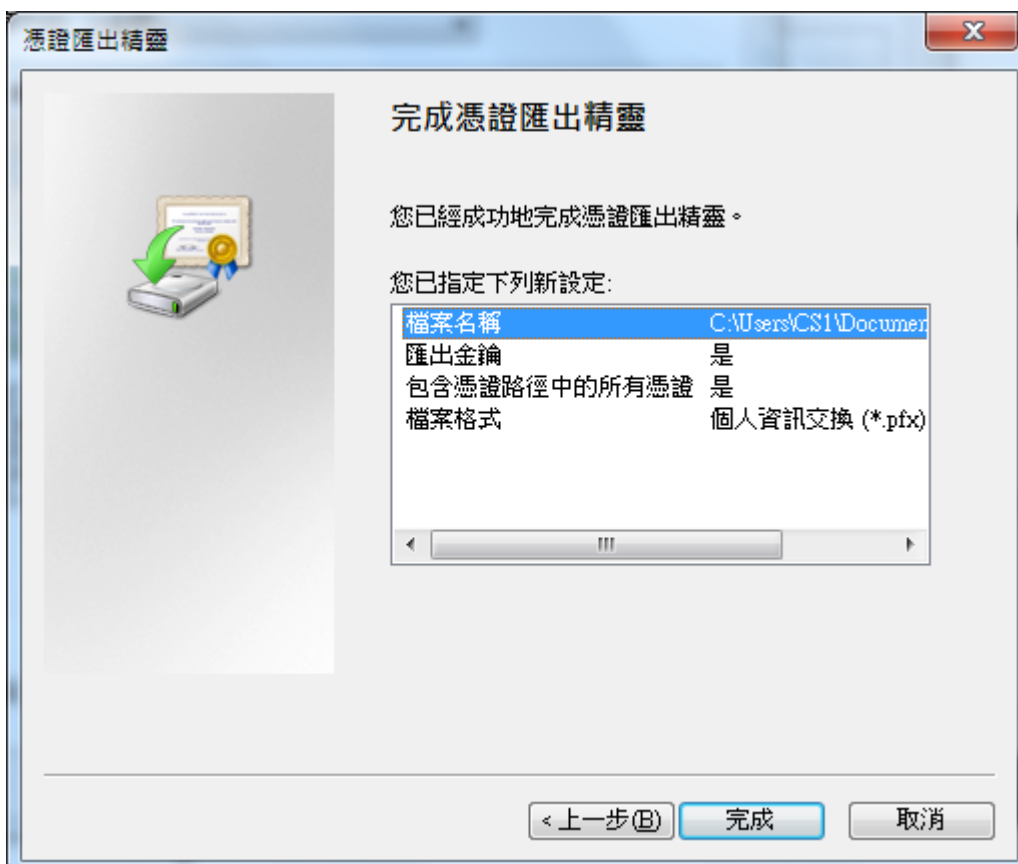
9. Choose a location to store the downloaded certificate and create a filename for the certificate.



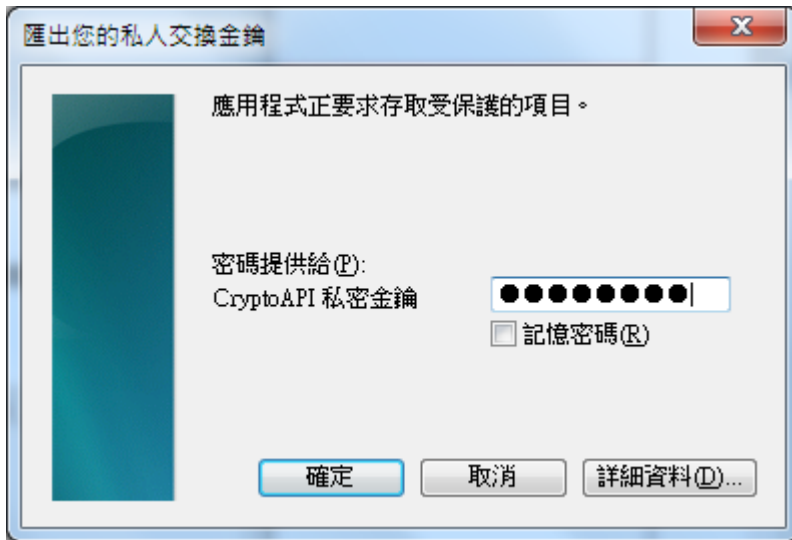
10. Click "Next".



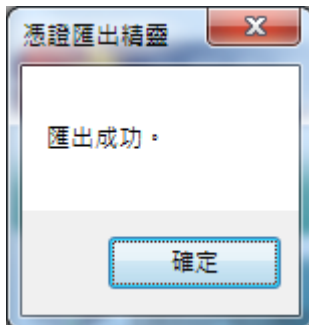
11. Click "Finish".



12. If the Security Level is previously set to High, please enter the security password and click “OK”.



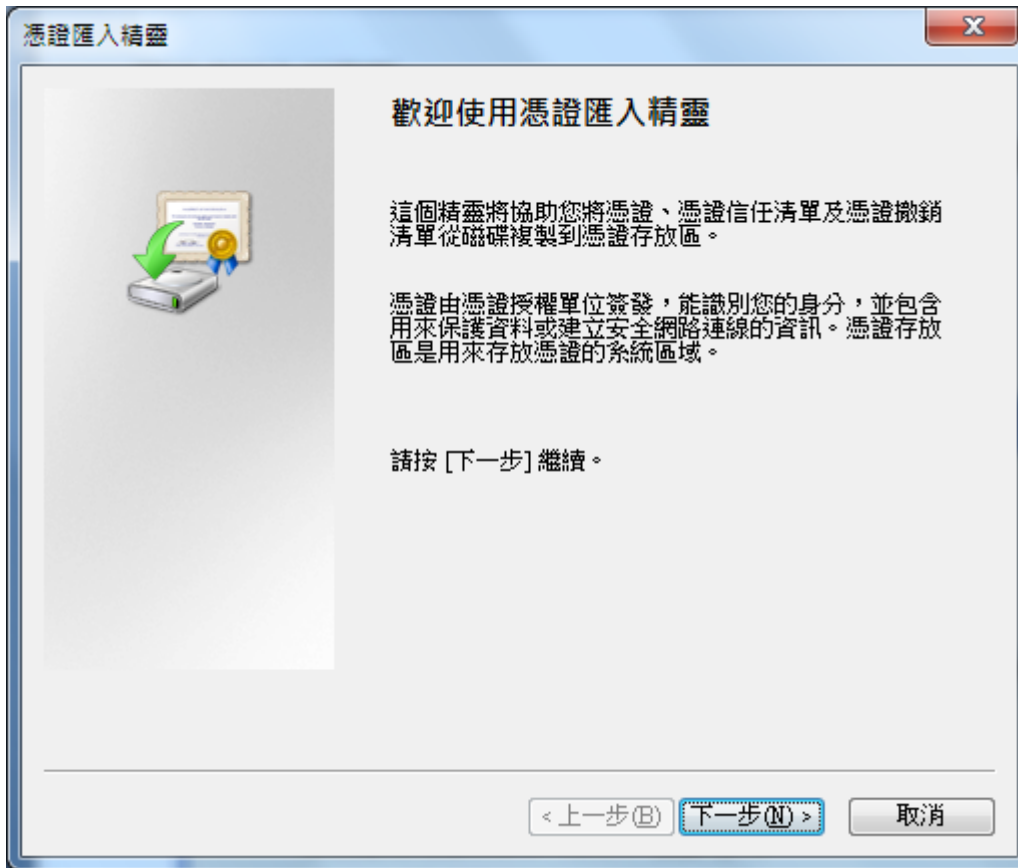
13. Successful message will be shown and the certificate (.pfx) file will be found at your defined location.



Import Certificate into Computer

In order to use the certificate on other computers, please follow the instructions below:

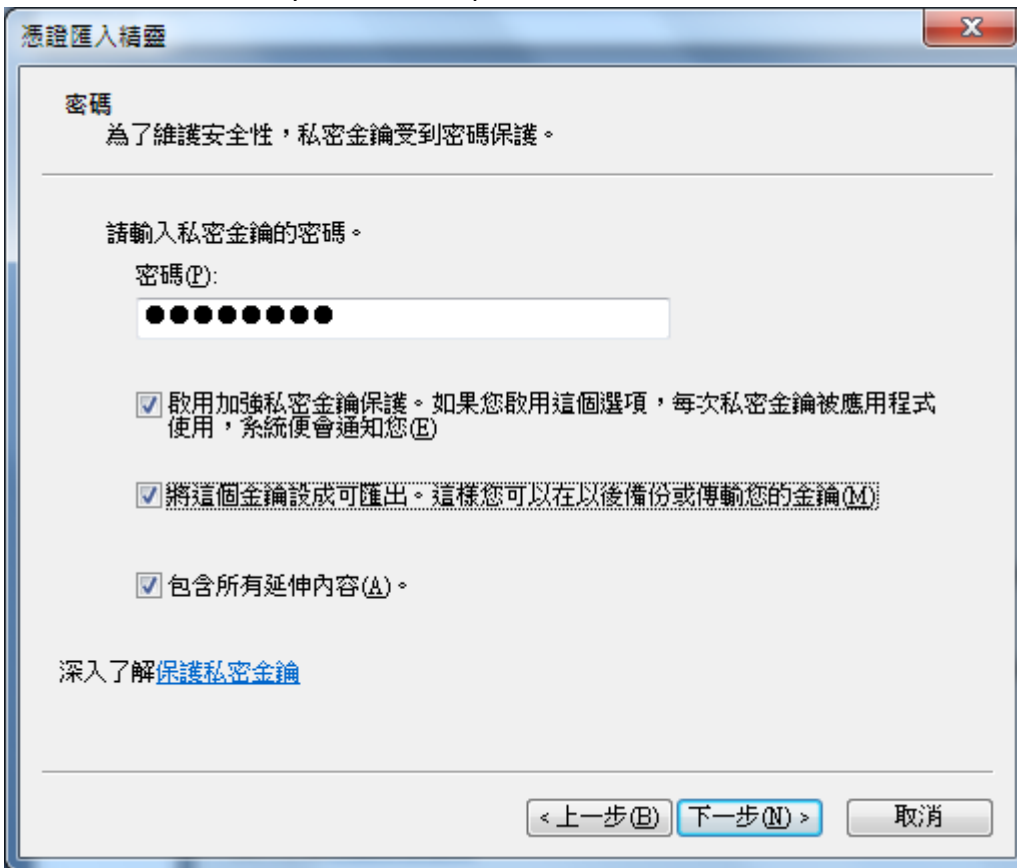
1. Copy the downloaded certificate (.pfx) file to the destination computer, open it and click “Next”.



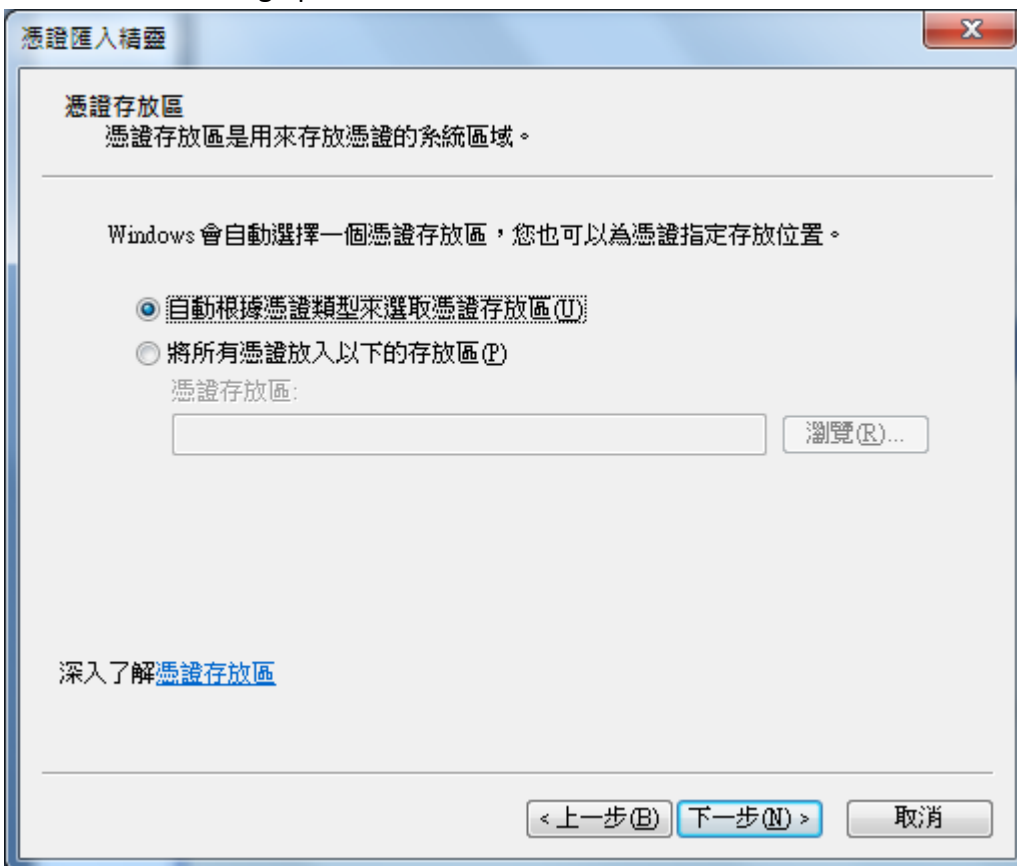
2. Click “Next”.



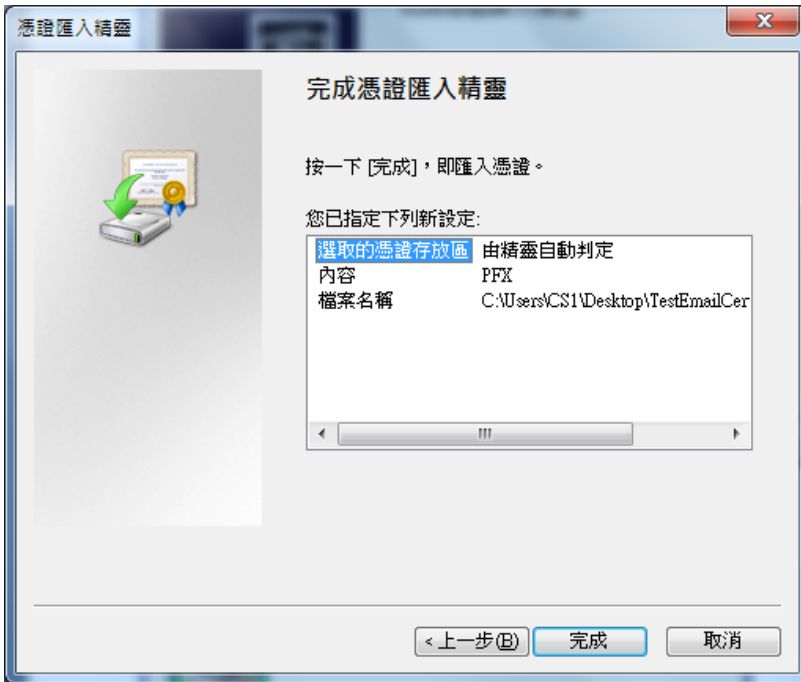
Please enter the password previously set when exporting the certificate from the original computer, and tick the Private Key Protection option, then click “Next”.



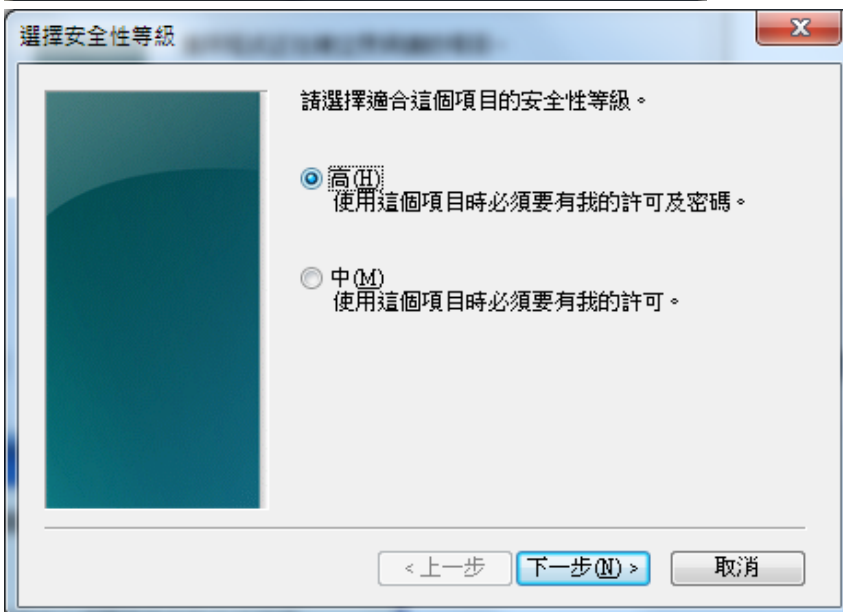
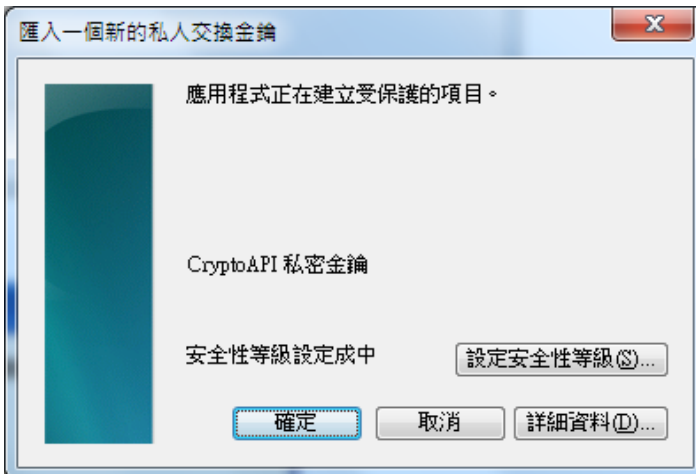
3. Choose the following option and click “Next”.



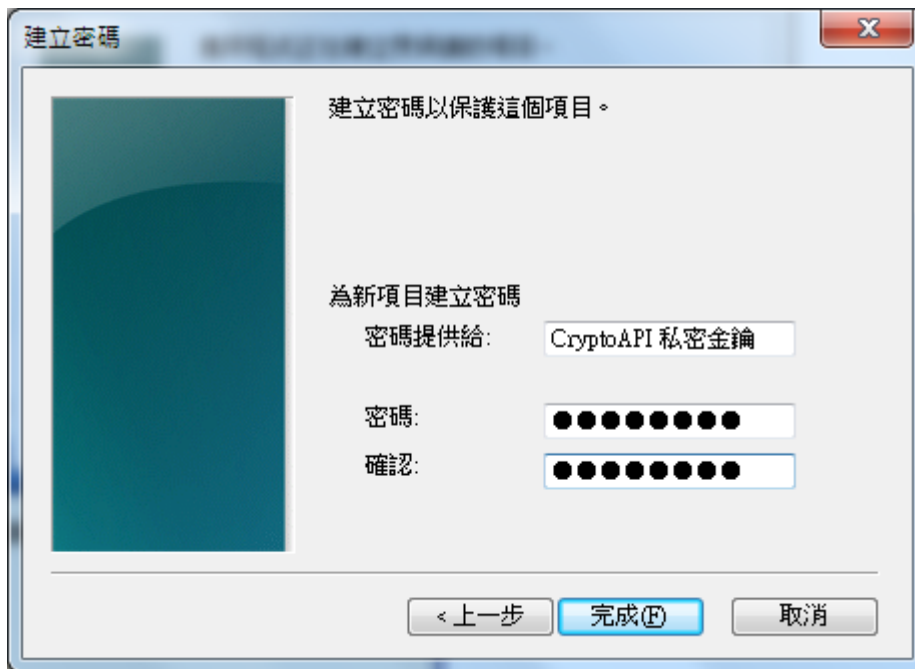
4. Click "Finish".



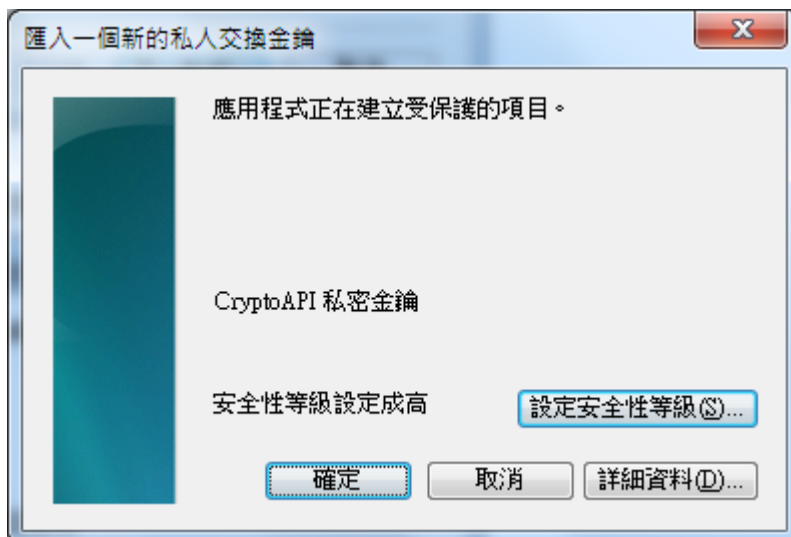
5. Set the Security Level



6. If High Security Level is selected, a password will be required to setup.



7. Click "OK".



8. Message dialog will be shown after successful import of certificate.

