

Exchange of secured e-mails with P&TS

Generation and installation of an S-MIME certificate

Introduction

E-mails exchanged with P&TS often contain sensitive and confidential information, including notices of not yet protected inventions, drafts of patent applications or any other information that, if divulged, could harm your interests or those of P&TS. P&TS recommends that these e-mails should be encrypted before sending. For this reason we provide a Trustmail platform for generating S-MIME certificates.

An S-MIME certificate will allow you to:

- > check that the e-mails you receive are really from P&TS and that they have not been modified
- > to decrypt e-mails encrypted by P&TS
- > to send encrypted e-mails to P&TS

The installation of an S-MIME certificate does not require any software or plug-in to be installed; the certificate consists of keys, i.e. by series of personal numbers generated to this effect and to which the e-mail software can access.

How to generate an S-MIME certificate?

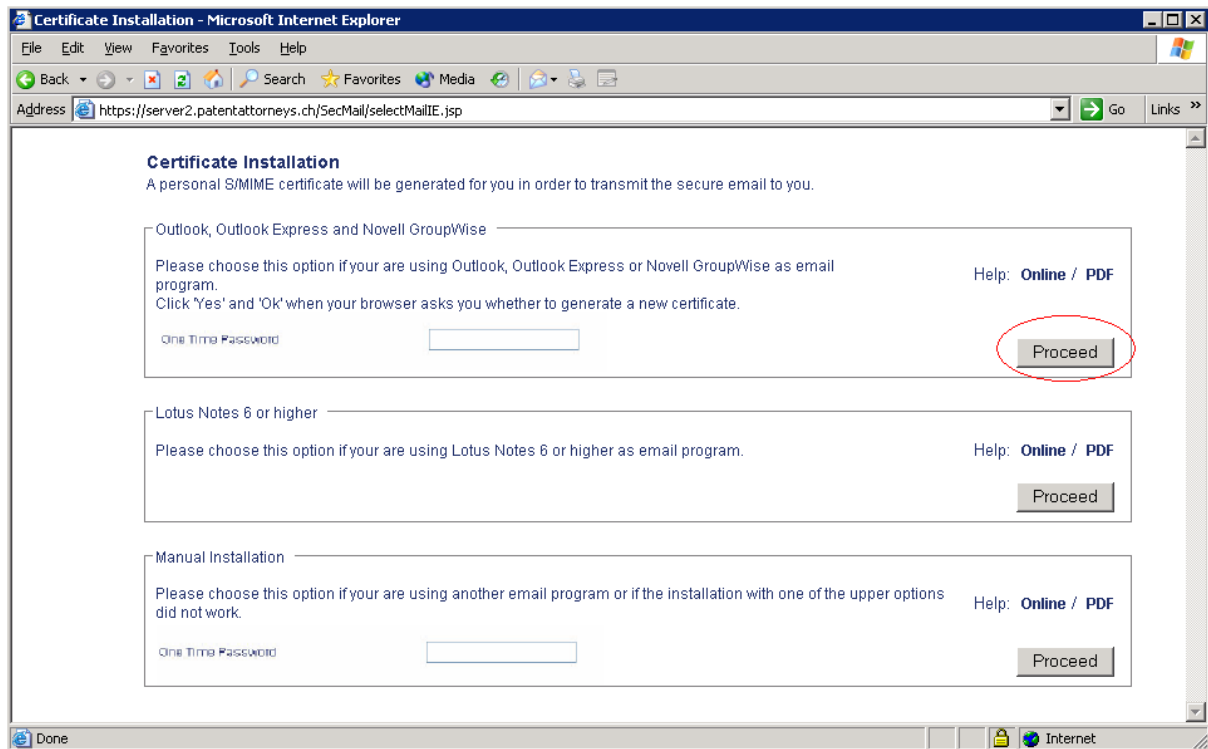
The simplest way to generate a certificate is when you receive an e-mail from P&TS asking you to enroll in the system. A certificate is generated and then installed by selecting option 3 in the e-mail (You would like a personal certificate).

You come to an Internet page with 3 different installation proposals :

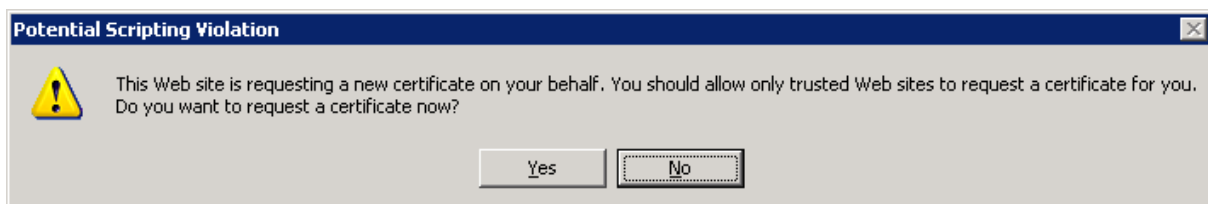
- > Automatic installation for Internet Explorer and Outlook : page 2
- > Installation for Lotus Notes : page 5
- > Manual installation : page 6

Automatic Installation

If you use Internet Explorer and Outlook, in the section « Outlook, Outlook Express and Novell GroupWare », enter the “One Time Password”. This password allows us to make sure that it is you who is signing up. To obtain this password, please call us at +41-32-727 14 27. Click on the button « Proceed » to begin installing the certificate.



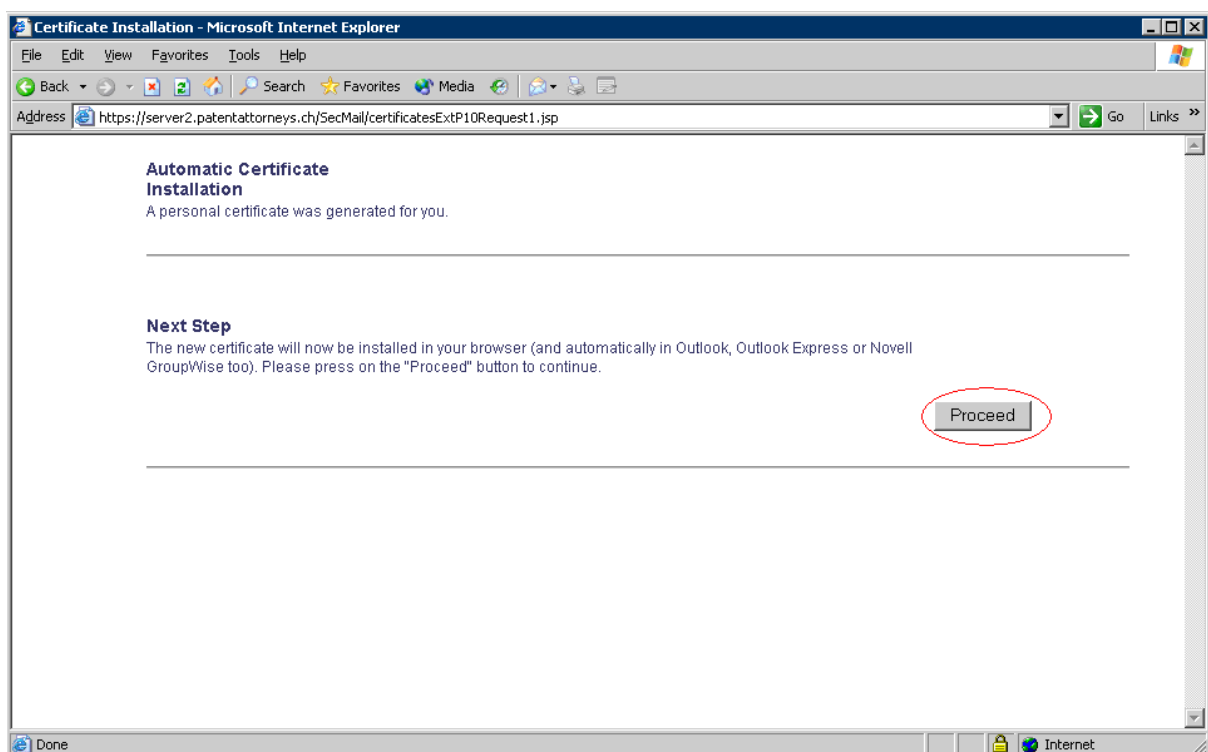
You will see a dialogue box. Reply “Yes” to continue to generate the certificate.



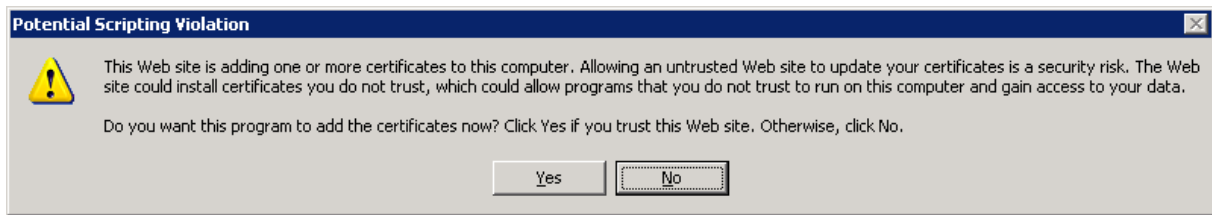
A pair of keys (public and private) will be generated. Click « OK » to continue.



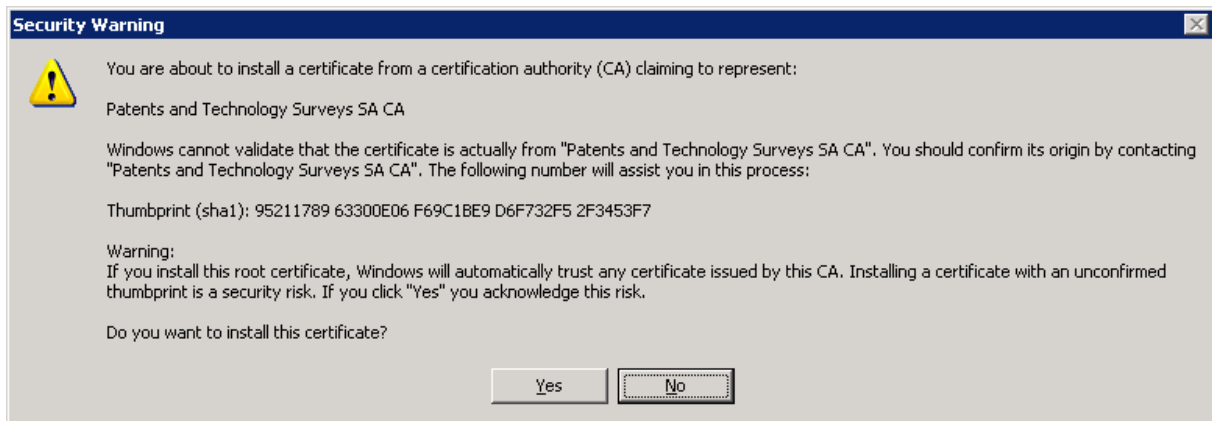
The certificate has been generated. Click on « Proceed » to add the certificate automatically in Outlook.



The system will ask you for a confirmation that you want to add the certificate. Reply « Yes ».



The system will inform you that it was unable to validate the certification authority of « Patents and Technology Surveys SA CA » and will ask you if you want to add the certificate to your computer. Reply « OK ».



Then the certificate will be installed.

From then on, secured e-mails from P&TS will reach you directly in Outlook.

> **Warning** : depending on the configuration of your software, the messages you wish to send to P&TS will not necessarily be encrypted. You will have to indicate manually for each e-mail that you want to encrypt it. The procedure to follow with Outlook 2003 is outlined on page 16.

Received e-mails are stocked encrypted in your message system or on your Exchange server. Access to these e-mails is only possible if you have the relevant certificate. So remember to copy this certificate if you change computer or you reinstall your computer. You should also copy the certificate if you want to use it on multiple computers. **The procedure for saving a certificate is explained on page 18.**

Installation for Lotus Notes

If you use « Lotus Notes » for messages, please contact us to install the certificate correctly.

Manual Installation

If you use a navigator other than Internet Explorer or another messenger software than Outlook, you should choose the « Manual Installation » option.

Please enter the one time password. This password allows us to check that it is you who is signing up on the system. To obtain the password, please call us at +41-32-727 14 27.

Click on « Proceed » to begin installing the certificate.

The screenshot shows a Microsoft Internet Explorer window titled "Certificate Installation - Microsoft Internet Explorer". The address bar contains "https://server2.patentattorneys.ch/SecMail/selectMailE.jsp". The page content is titled "Certificate Installation" and includes the following text: "A personal S/MIME certificate will be generated for you in order to transmit the secure email to you." Below this, there are three sections, each with a "Proceed" button:

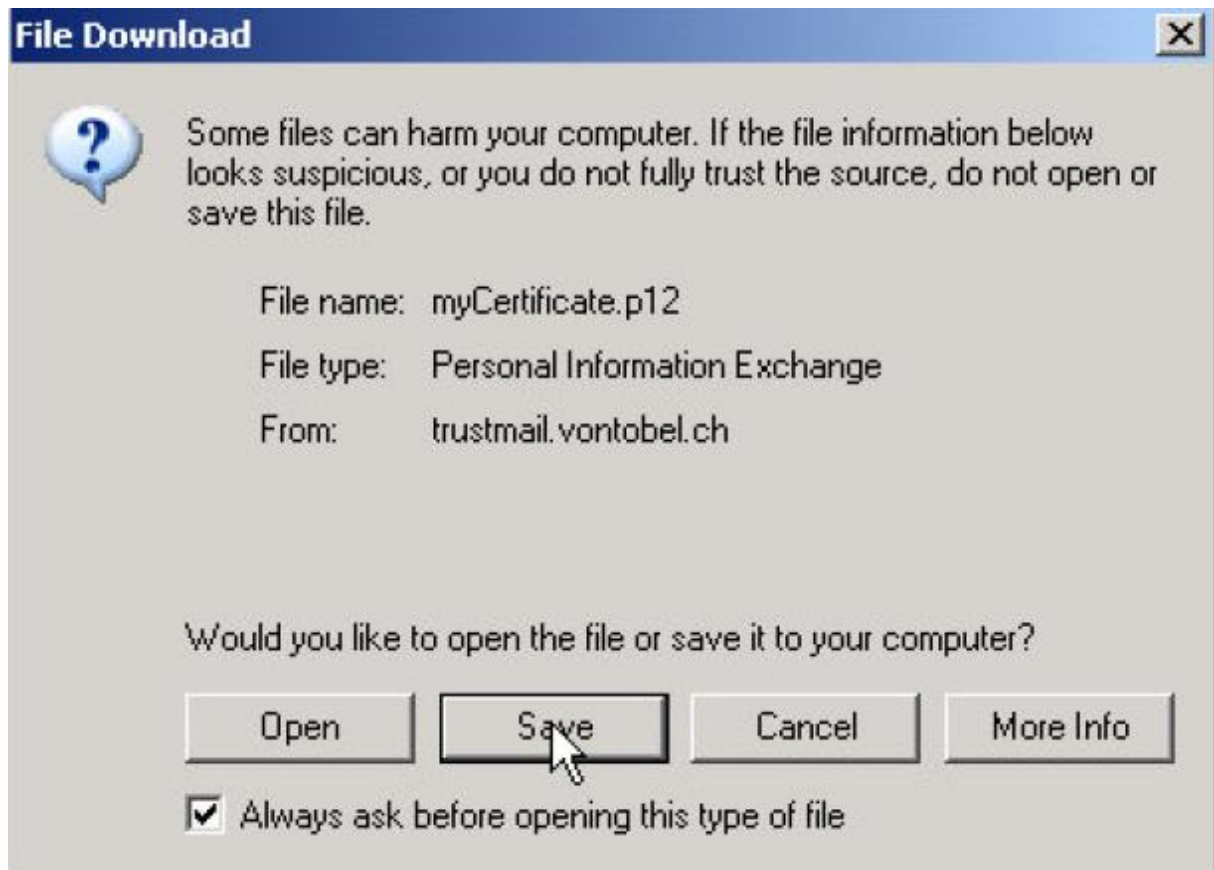
- Outlook, Outlook Express and Novell GroupWise**: "Please choose this option if your are using Outlook, Outlook Express or Novell GroupWise as email program. Click 'Yes' and 'Ok' when your browser asks you whether to generate a new certificate." Includes a "One Time Password" input field and a "Proceed" button.
- Lotus Notes 6 or higher**: "Please choose this option if your are using Lotus Notes 6 or higher as email program." Includes a "Proceed" button.
- Manual Installation**: "Please choose this option if your are using another email program or if the installation with one of the upper options did not work." Includes a "One Time Password" input field and a "Proceed" button, which is circled in red in the image.

Enter a personal password of your choice to protect the installation of the certificate and click on « Download Certificate ».

> Warning : Once you have clicked on the link « Download Certificate », our system will generate a certificate and at the same time encrypt the original message with this certificate and will send it to you. As long as the certificate has not been properly installed, you will not be able to decrypt the original message.

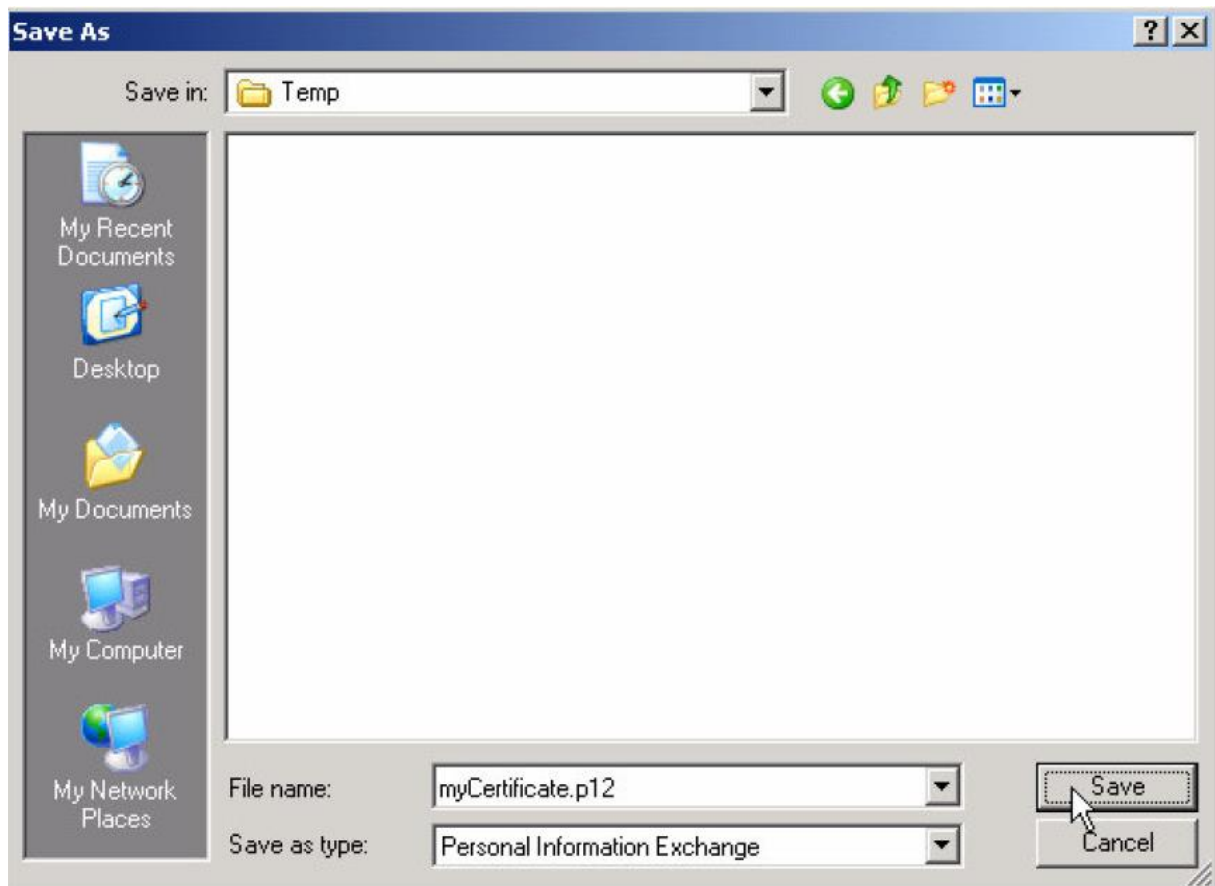
You cannot interrupt the uploading of the certificate while in progress.

If for any reason the upload is unsuccessful, please contact the sender of the notification.

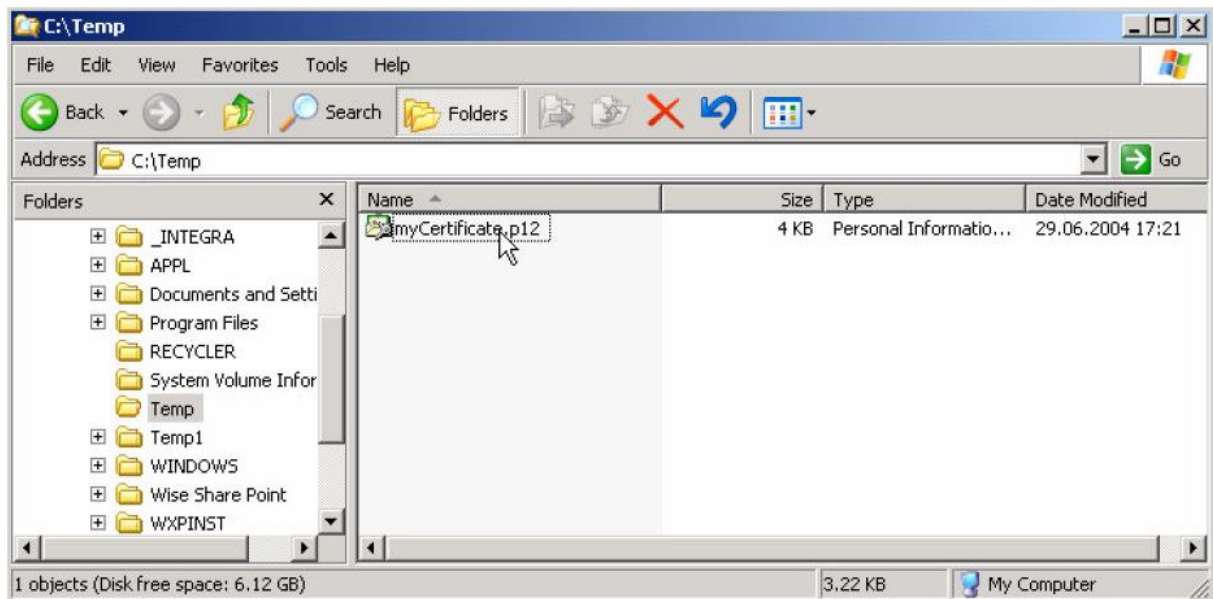


The upload box will propose that you upload the certificate and save it on your hard drive or open it right after uploading it.

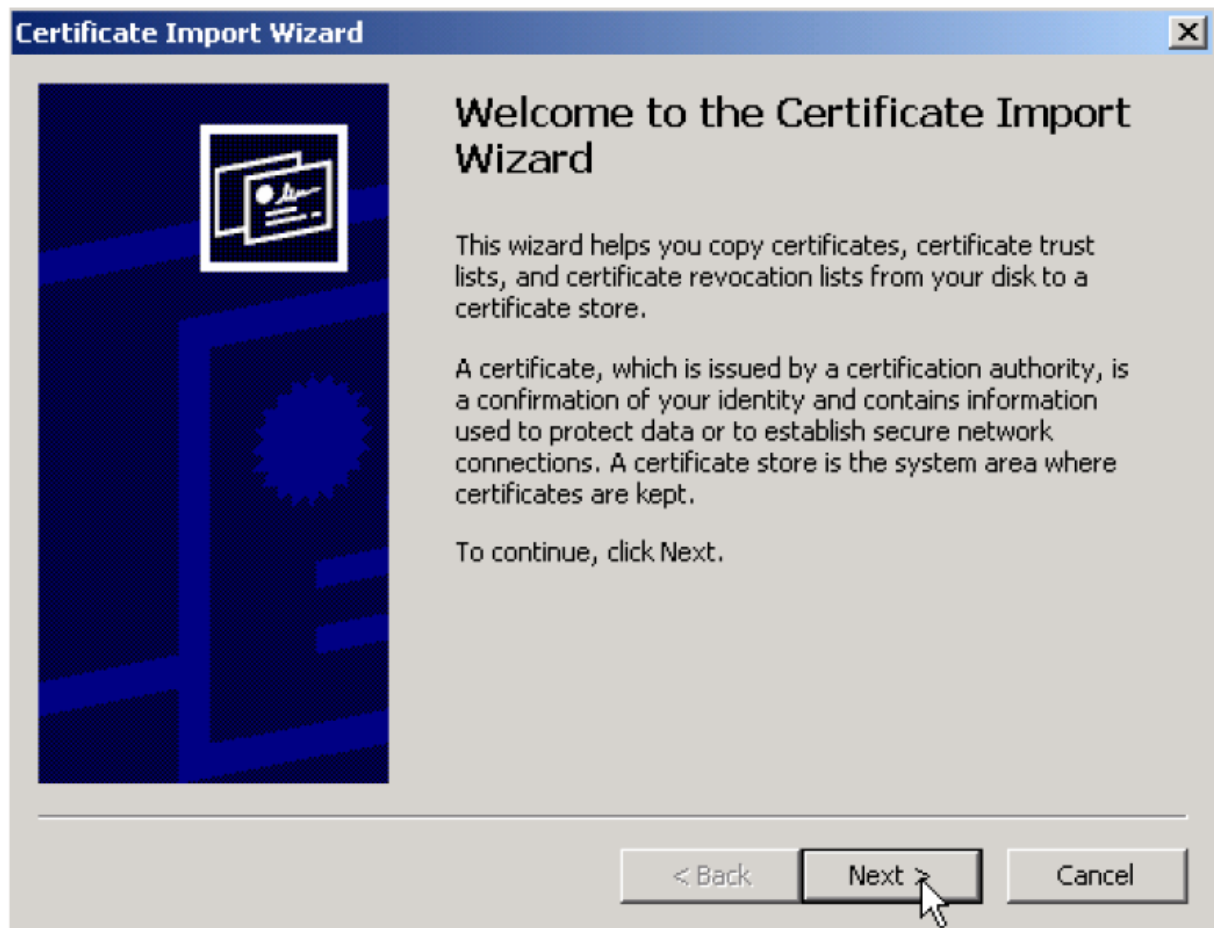
We recommend that you choose to save the certificate on your hard drive.



If you choose the « Save » option, the system will ask you to indicate a place on your hard drive where to save the certificate.

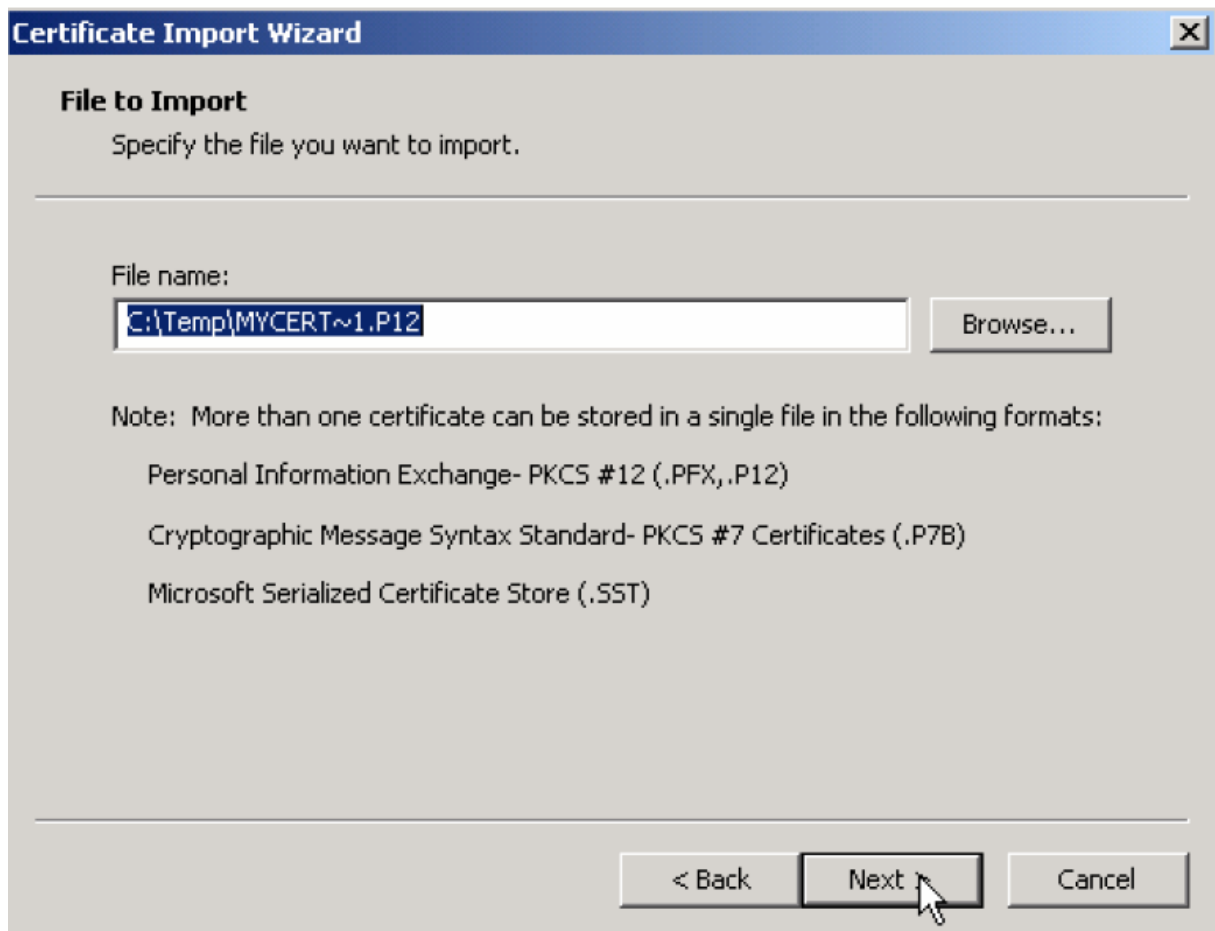


Once the file has been uploaded and saved on to your computer, you can start the installation by double-clicking on the file.



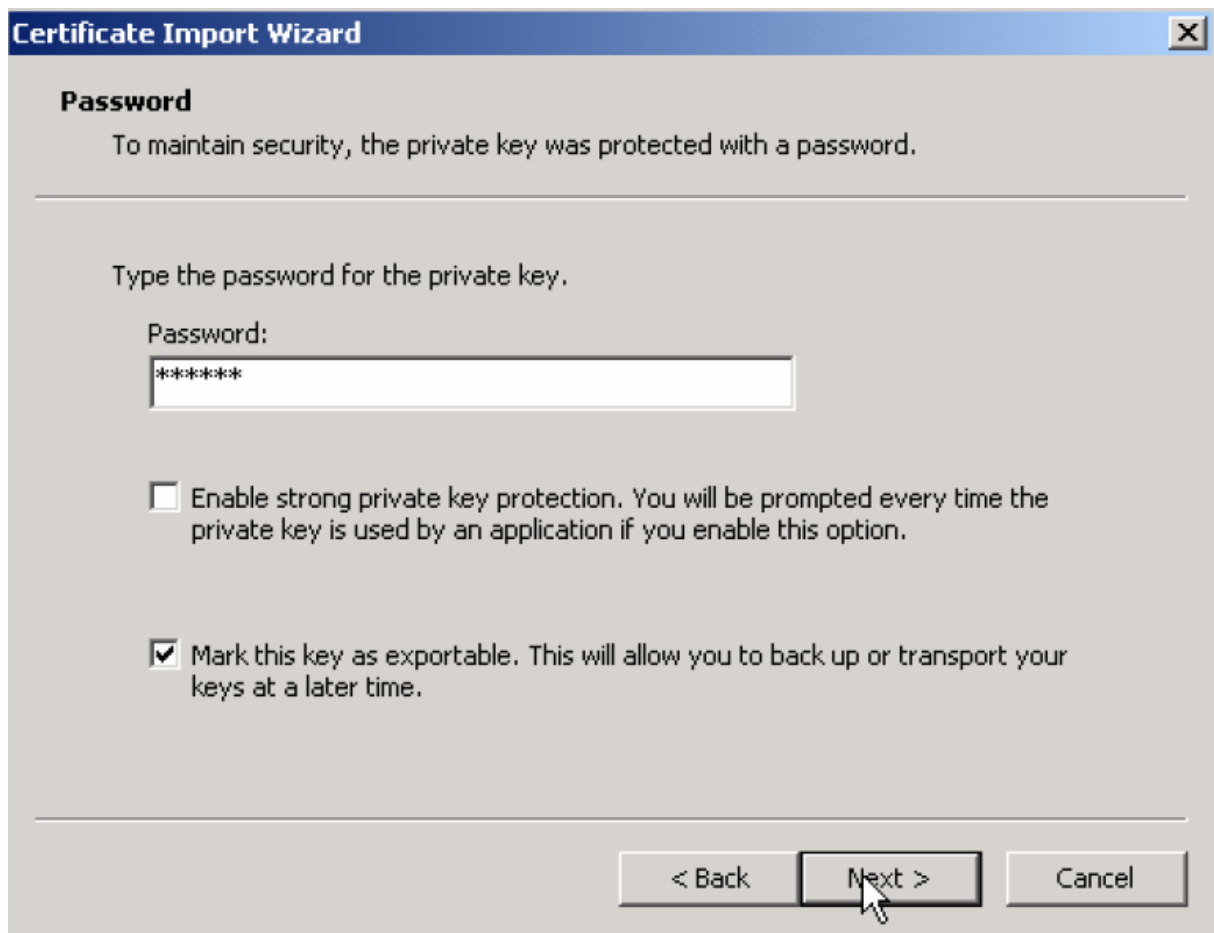
The « Certificate Import Wizard » will open on your computer.

Click on « Next » to start the installation.



Check that the imported file is the one you previously saved.

Click on « Next » to continue the installation.

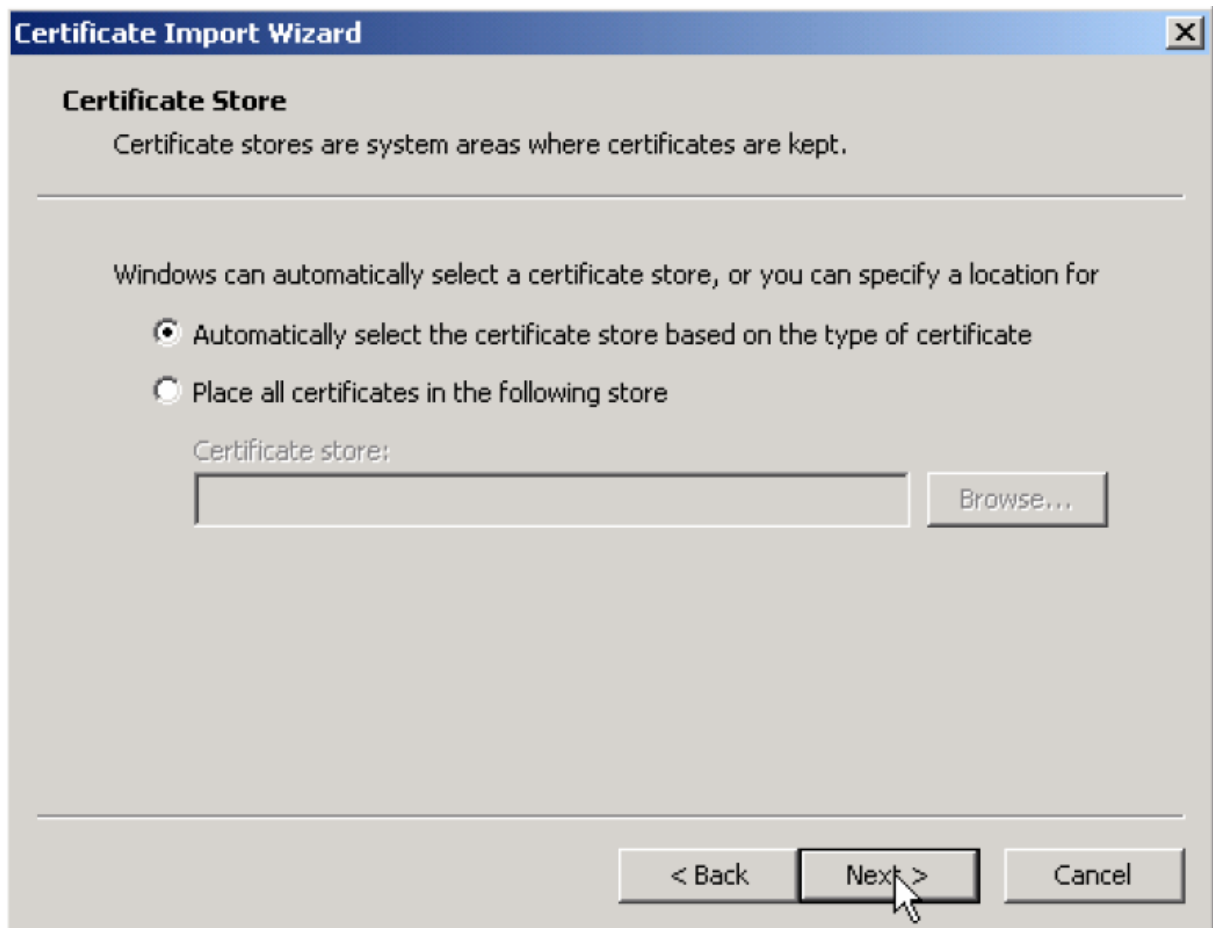


You need to enter a password to protect your certificate (private key).

The assistant will offer you two security options:

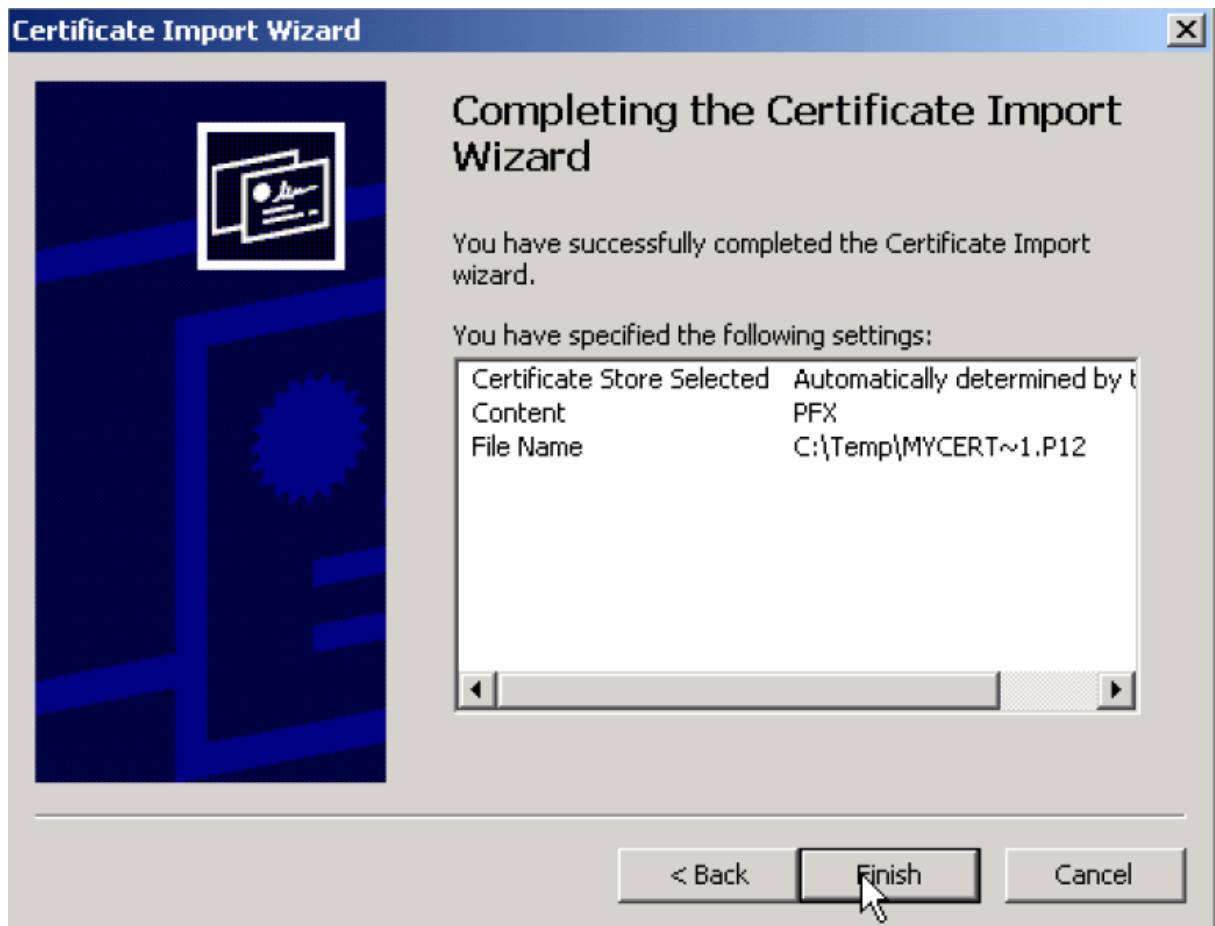
- > If you select « Activate strong private key security », each time your private key is used, for example to decrypt or sign an e-mail, you will need to enter the password (this is important if your computer is shared by several people).
- > We **recommend** that you make your key exportable so that you can save your private key on an external media. In this way, if you have to reinstall your computer, you can reuse the key.

Click on « Next » to continue the installation.



Allow Windows to select the certificate store.

Click on « Next » to continue the installation.



Click on « Finish » to finish the installation of your personal certificate.



Your personal certificate has been successfully installed on your computer.

You will soon receive the original encrypted e-mail in your usual message system.

All subsequent messages that we send you will be automatically encrypted.

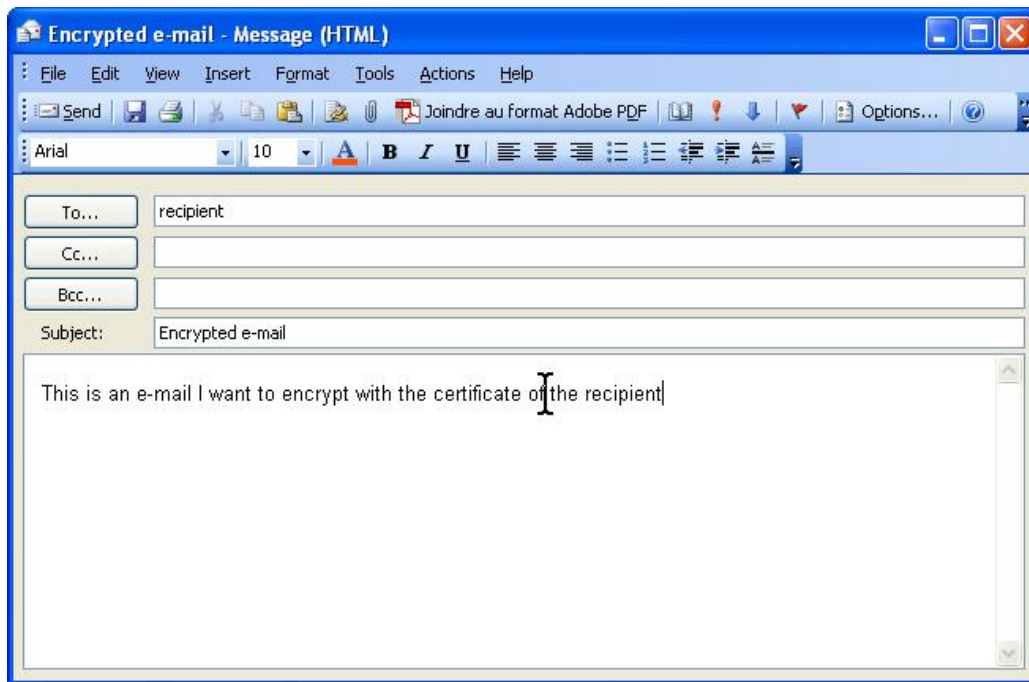
Encryption of e-mails sent to P&TS

Once the certificate has been correctly installed, all e-mails received from P&TS will be in principle signed and encrypted.

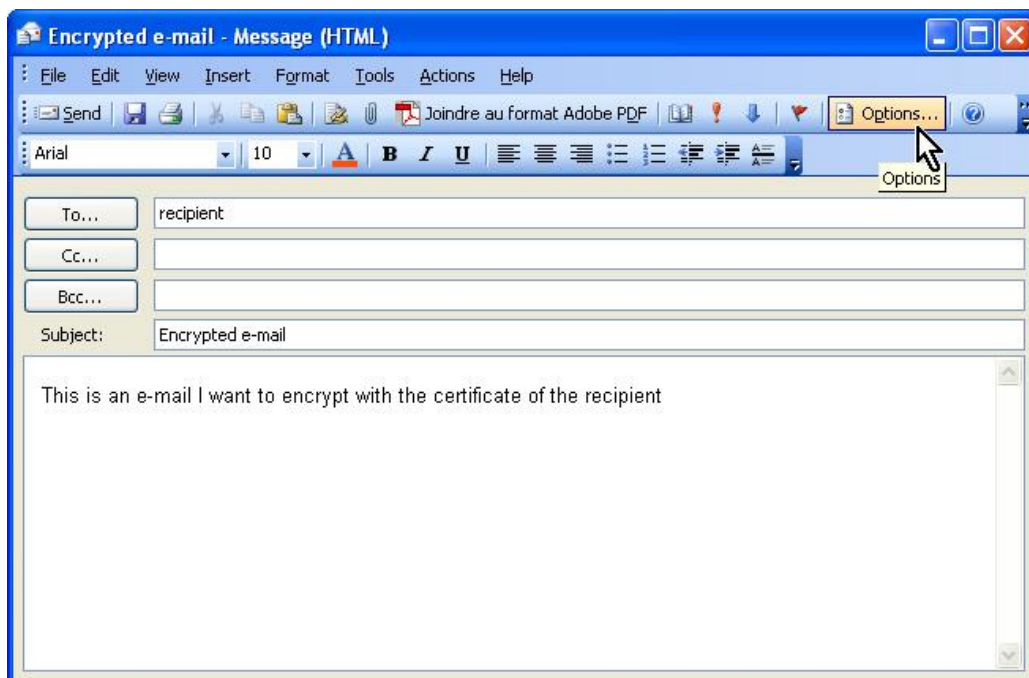
However, the e-mails that you send to P&TS will in principle not be automatically signed or encrypted (depending on the configuration of your software). So you must indicate for each e-mail sent to P&TS that you wish to protect it.

The screen-shots below explain the procedure for encrypting an e-mail with Outlook2003 :

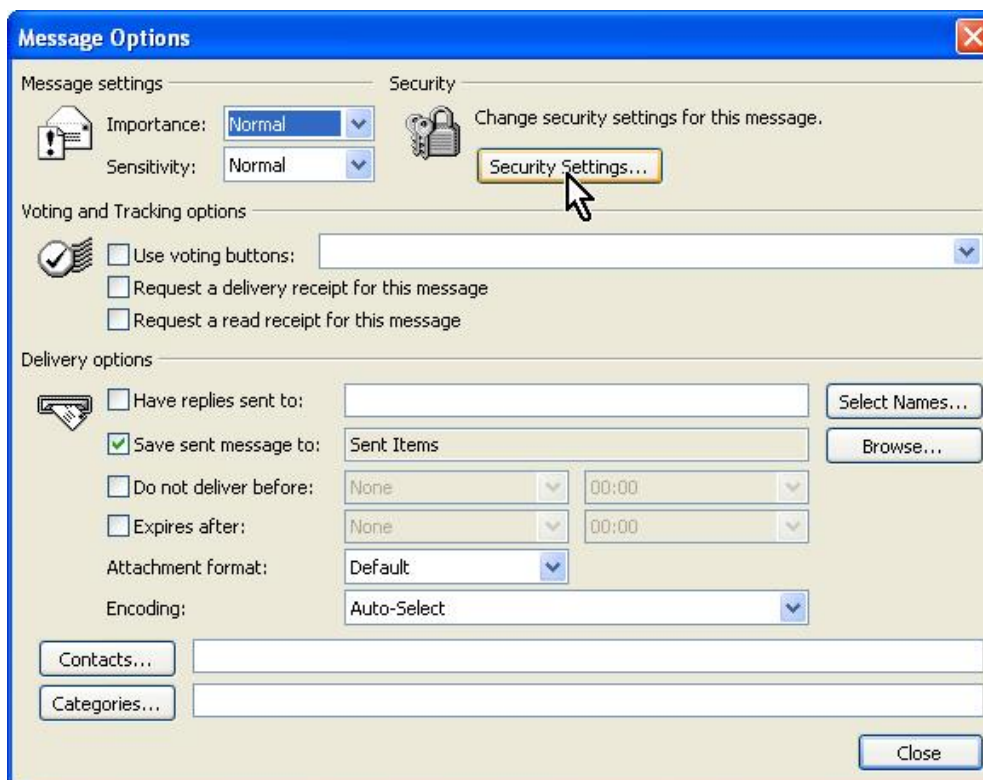
A. Create an e-mail as usual :



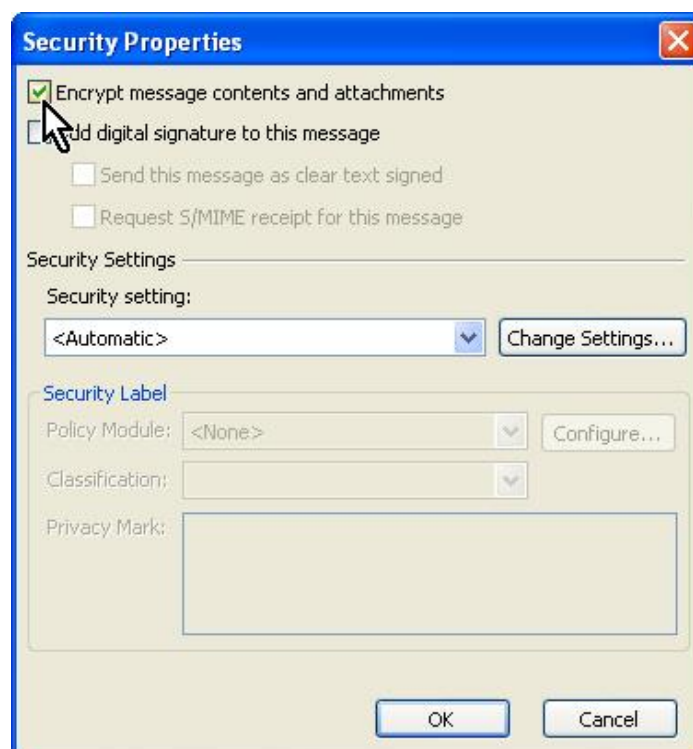
B. Choose « Options » in the menu :



C. Choose « Security Settings » :



D. Click on « Encrypt message contents and attachments »:



E. Click on OK, Close, then Send in order to send the message.

You can also choose to sign your outgoing e-mails electronically with the generated certificate.

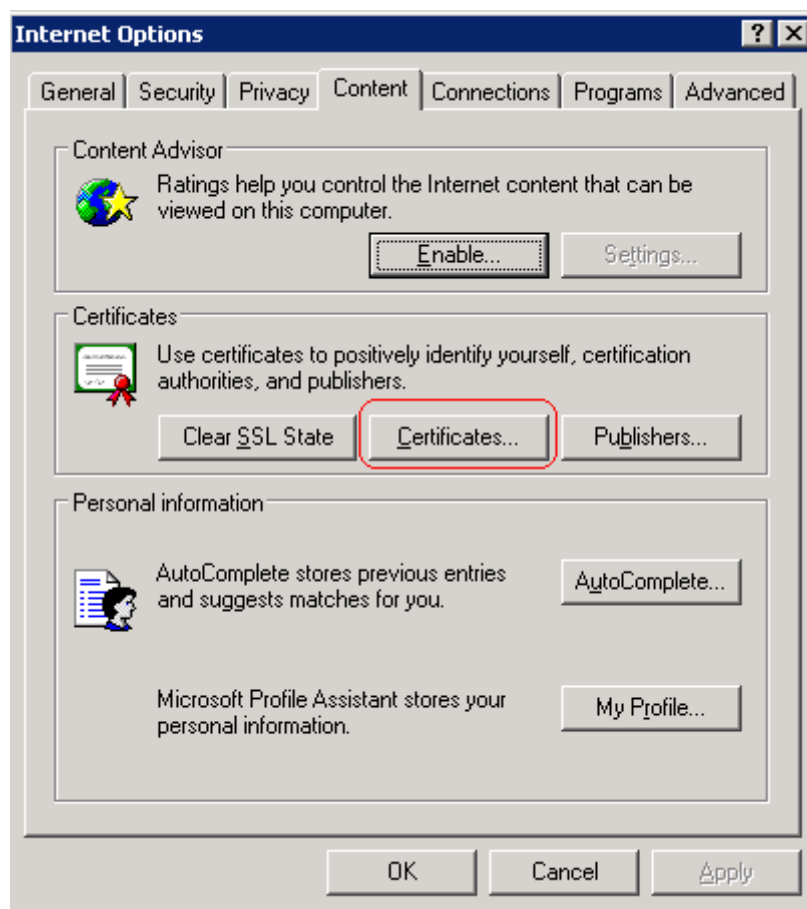
Storing the certificate

You need the S-MIME certificate generated during the sign-up procedure in order to decrypt e-mails received from P&TS. It is advisable to save this certificate in order to be able to transfer it to a new computer or for reinstalling customer software. P&TS does not have a copy of your certificate.

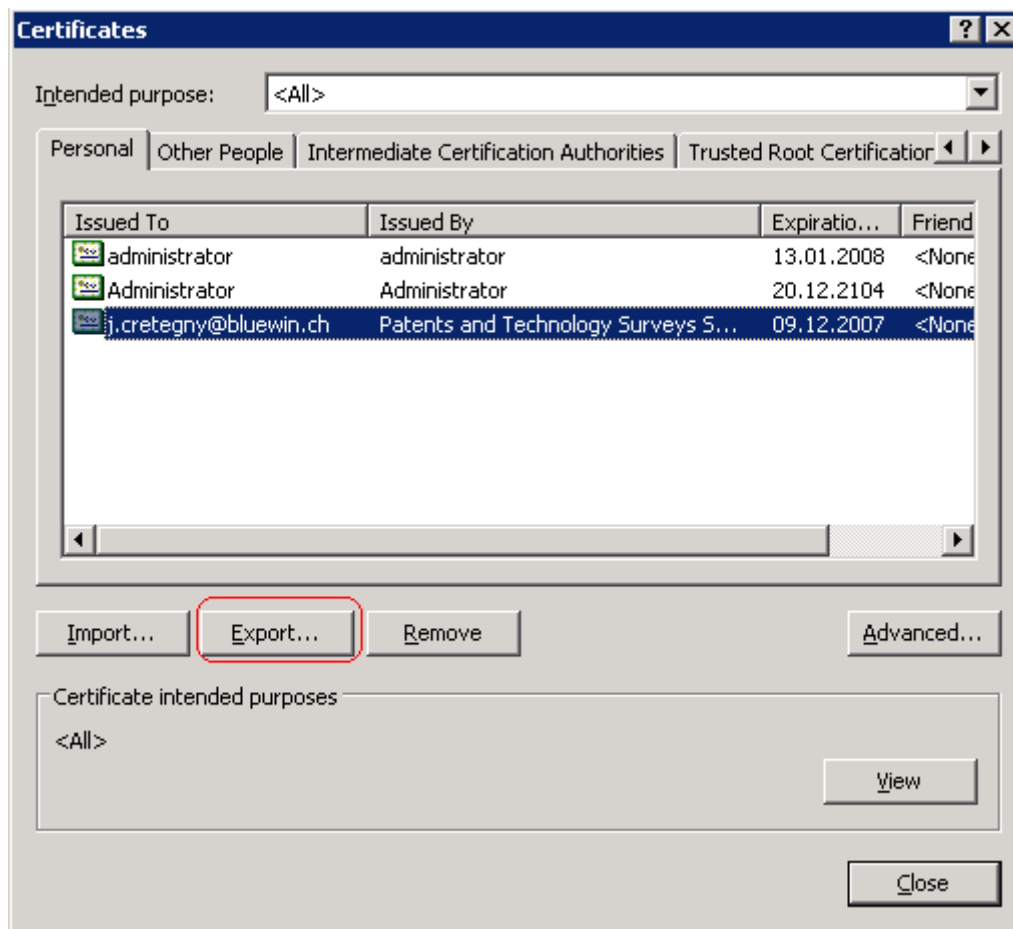
The procedure illustrated below was created using Internet Explorer 6. It may vary depending on the version and browser used.

In the Tool menu in Internet Explorer 6

- A. Go to the Tools->Internet Options->Content menu
- B. Click on « Certificates »



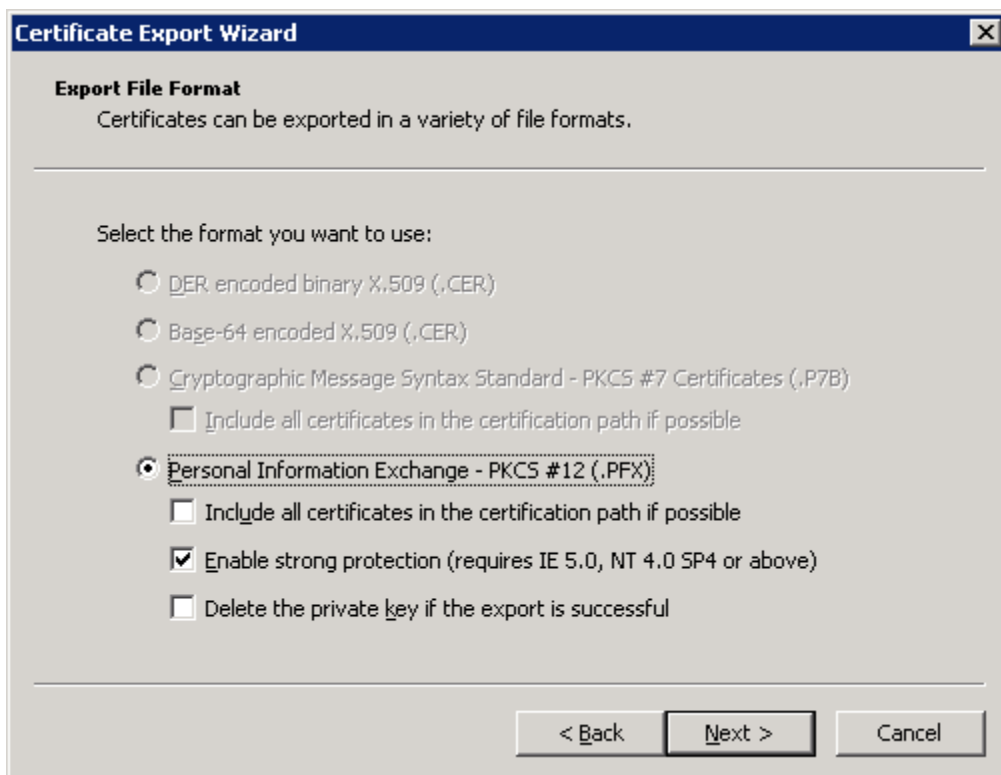
C. In the « Personal» tab select the P&TS certificate and click on « Export »



D. The assistant for exporting certificates will open and ask if you want to export the private key. Reply « yes » as this key will allow you to decrypt e-mails received.



E. Leave the default options and export format.



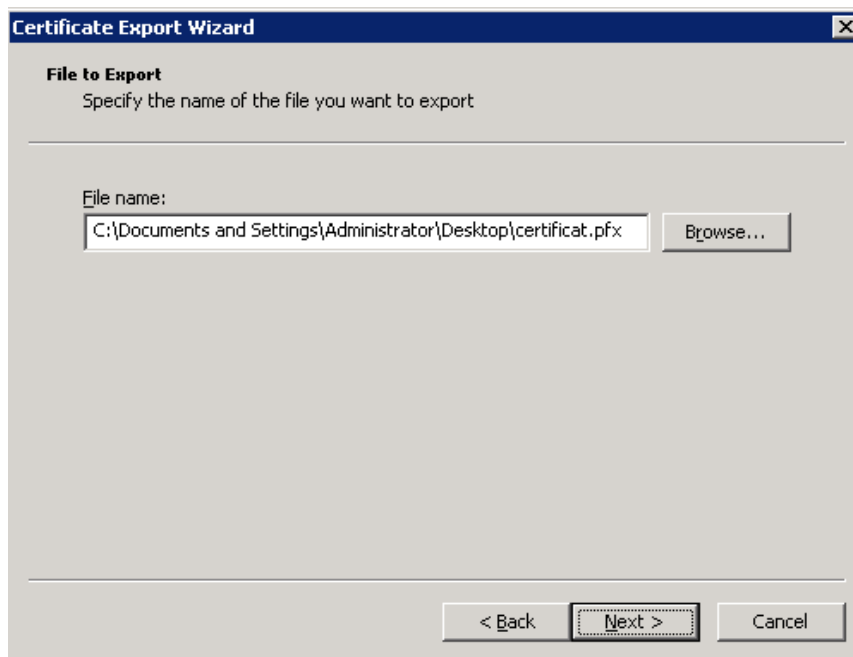
F. Enter a password to protect your private key.

> **Warning** : if you forget your password, you will no longer be able to use your private key and therefore to decrypt e-mails from P&TS.



The screenshot shows the 'Certificate Export Wizard' dialog box. The title bar reads 'Certificate Export Wizard'. The main heading is 'Password'. Below the heading, it says 'To maintain security, you must protect the private key by using a password.' There is a horizontal line. Below the line, it says 'Type and confirm a password.' There are two text input fields: 'Password:' and 'Confirm password:'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

G. Enter a password for the certificate to be exported.



The screenshot shows the 'Certificate Export Wizard' dialog box. The title bar reads 'Certificate Export Wizard'. The main heading is 'File to Export'. Below the heading, it says 'Specify the name of the file you want to export.' There is a horizontal line. Below the line, it says 'File name:'. There is a text input field containing 'C:\Documents and Settings\Administrator\Desktop\certificat.pfx' and a 'Browse...' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- H. A dialogue box will open up and ask if you authorize the system to access the private key. Click on « OK ».



- I. The certificate has been successfully exported.



- J. Copy this file somewhere safe (CD-ROM, diskette, backup drive)