Echange d'e-mails sécurisés avec P&TS

Génération et installation d'un certificat S-MIME

Introduction

Les e-mails échangés avec P&TS contiennent souvent des informations sensibles et confidentielles, y compris des annonces d'invention non protégées, des projets de demandes de brevet, des études de liberté d'exploitation, etc. P&TS recommande d'encrypter ces e-mails avant leur transmission, et met à cet effet une plateforme Trustmail permettant de générer des certificats S-MIME.

Un certificat S-MIME permet :

- De vérifier que les mails reçus proviennent bien de P&TS, et qu'ils n'ont pas été modifiés
- De décrypter des e-mails encryptés par P&TS
- D'envoyer des e-mails encryptés à P&TS

L'installation d'un certificat S-MIME ne nécessite aucune installation de software ou de plug-in ; le certificat est constitué par des clés, c'est-à-dire des suites de nombres personnels, générés à cet effet et auxquelles le logiciel d'e-mail peut accéder.

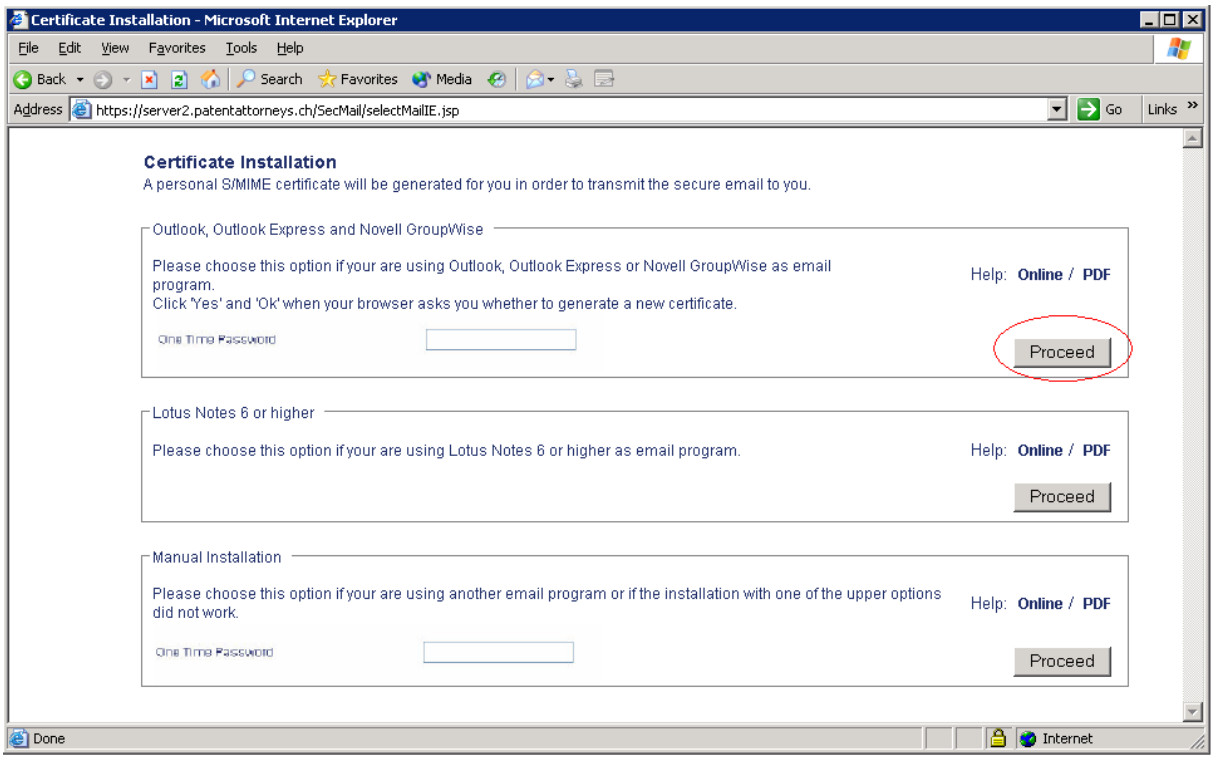
Comment générer un certificat S-MIME ?

La génération d'un certificat s'effectue de la manière la plus simple si vous avez reçu un e-mail de P&TS vous demandant de vous enrôler dans le système. Un certificat est généré puis installé en sélectionnant l'option 3 (Vous désirez un certificat personnel) proposée dans l'e-mail.

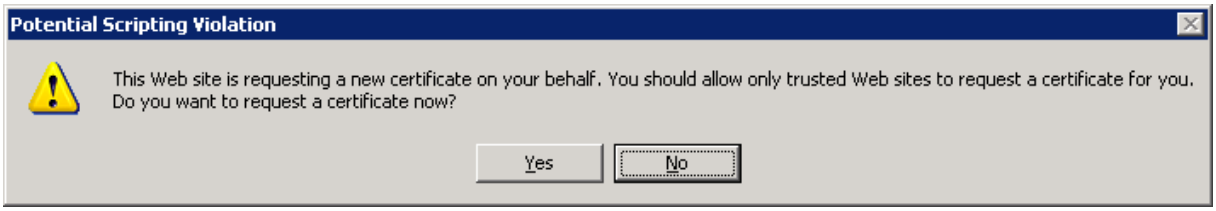
Vous arrivez sur une page Internet vous proposant 3 types d'installations :

Installation automatique

Si vous utilisez Internet Explorer et Outlook, dans la partie « Outlook, Outlook Express and Novell GroupWare », entrez le mot de passe à usage unique (One Time Password). Ce mot de passe nous permet de nous assurer que c'est bien vous qui vous enrôlez dans le système Pour l'obtenir, veuillez nous contacter au +41-32-724 96 60.
Cliquez sur le bouton « Proceed » pour commencer l'installation du certificat.

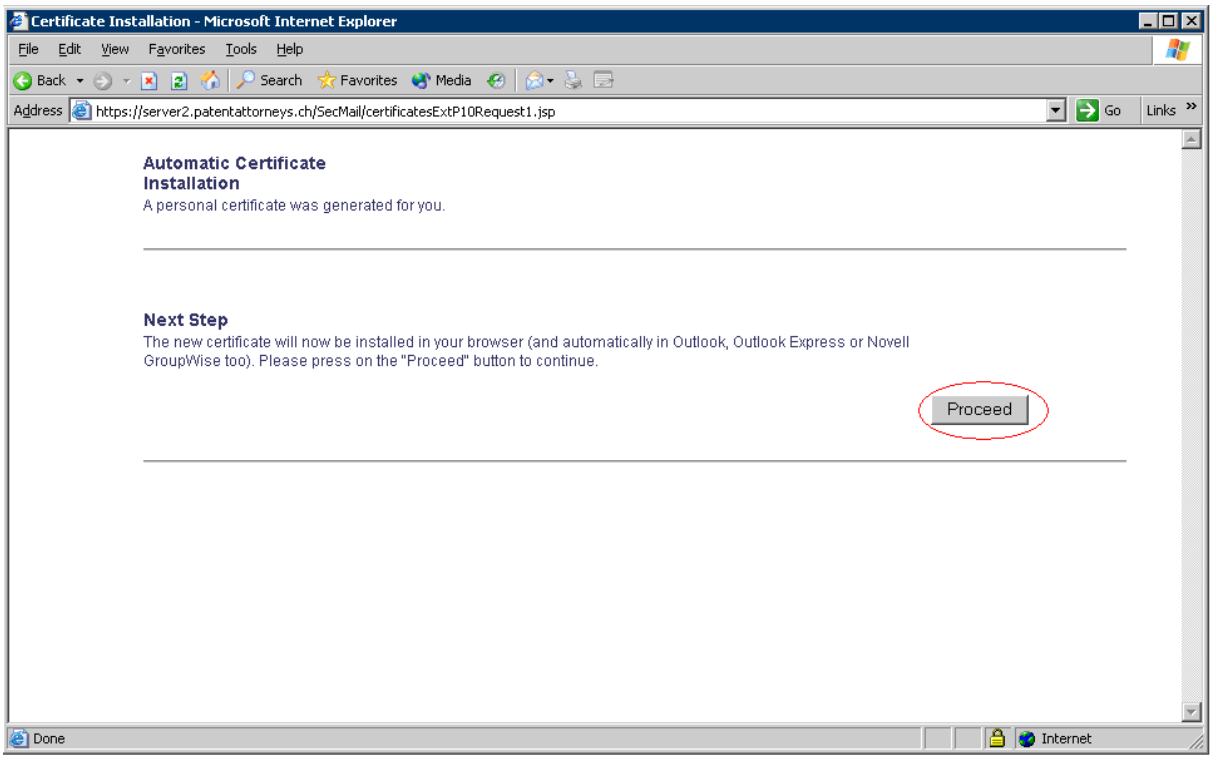


Une boîte de dialogue s'affiche. Répondez « Oui » (« Yes ») pour poursuivre la génération du certificat.

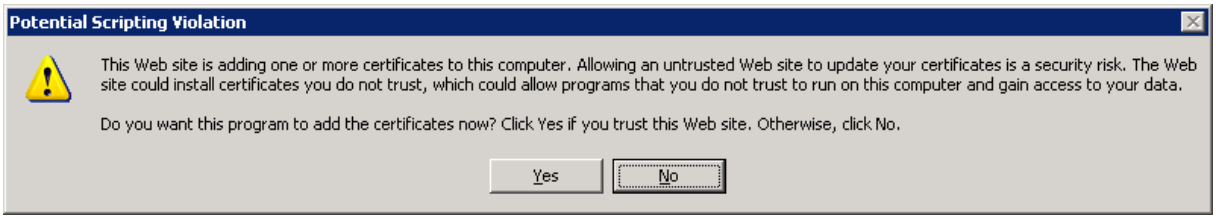


Une paire de clés (publique et privée) va ensuite être générée. Cliquez « OK » pour poursuivre.

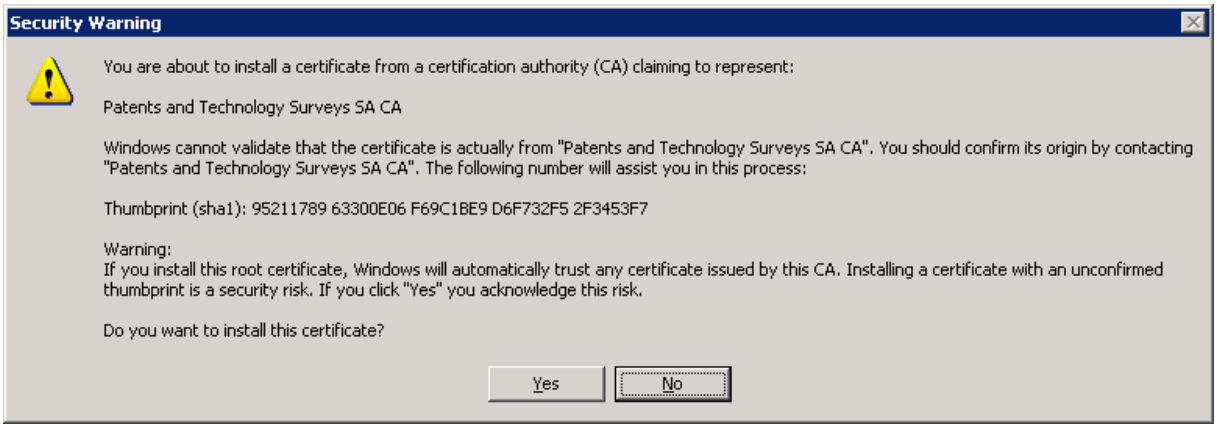
Le certificat a été généré. Cliquez sur le bouton « Proceed » afin d'ajouter le certificat automatiquement dans Outlook.



Le système vous demande une confirmation d'ajout du certificat. Répondez « Yes »



Le système vous informe qu'il n'a pas pu valider l'autorité de certification « Patents and Technology Surveys SA CA » et vous demande si vous voulez ajouter le certificat dans votre ordinateur. Répondez « OK ».



Le certificat est ensuite installé.

Dorénavant, les e-mails sécurisés de P&TS vont vous parvenir directement dans Outlook.

> **Attention :** selon la configuration de votre logiciel de messagerie, les messages que vous souhaitez envoyer à P&TS ne seront probablement pas automatiquement encryptés. Il sera nécessaire d'indiquer manuellement, pour chaque e-mail, que vous souhaitez l'encrypter. La procédure à suivre avec Outllok2003 est indiquée en page 16.

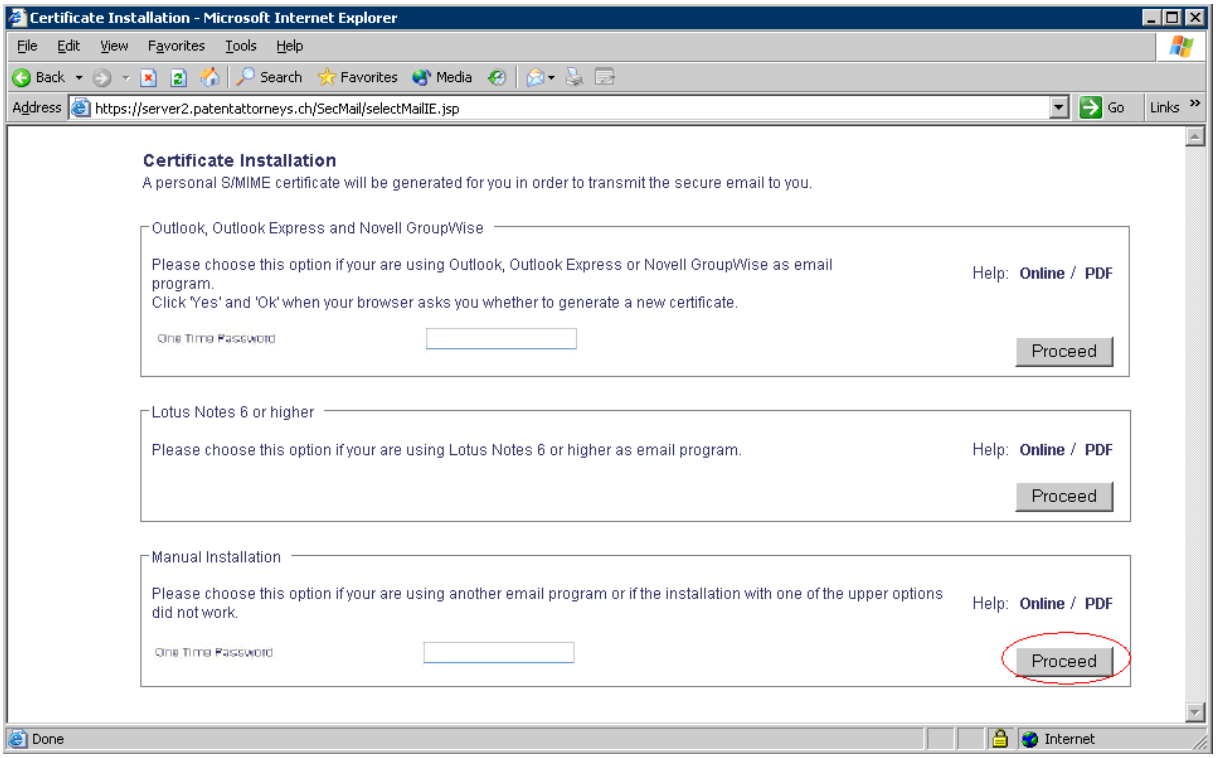
Les e-mails reçus sont stockés de façon encryptée dans votre logiciel de messagerie ou votre serveur Exchange. L'accès à ces e-mails est uniquement possible si vous disposez du certificat correspondant. Pensez donc à copier ce certificat si vous changez d'ordinateur ou réinstallez votre ordinateur. Vous devez également copier le certificat si vous désirez pouvoir l'utiliser sur plusieurs ordinateurs. **La procédure pour sauvegarder un certificat est expliquée en page 18.**

Installation pour Lotus Notes

Si vous utilisez « Lotus Notes » pour la messagerie, veuillez nous contacter afin d'installer correctement le certificat.

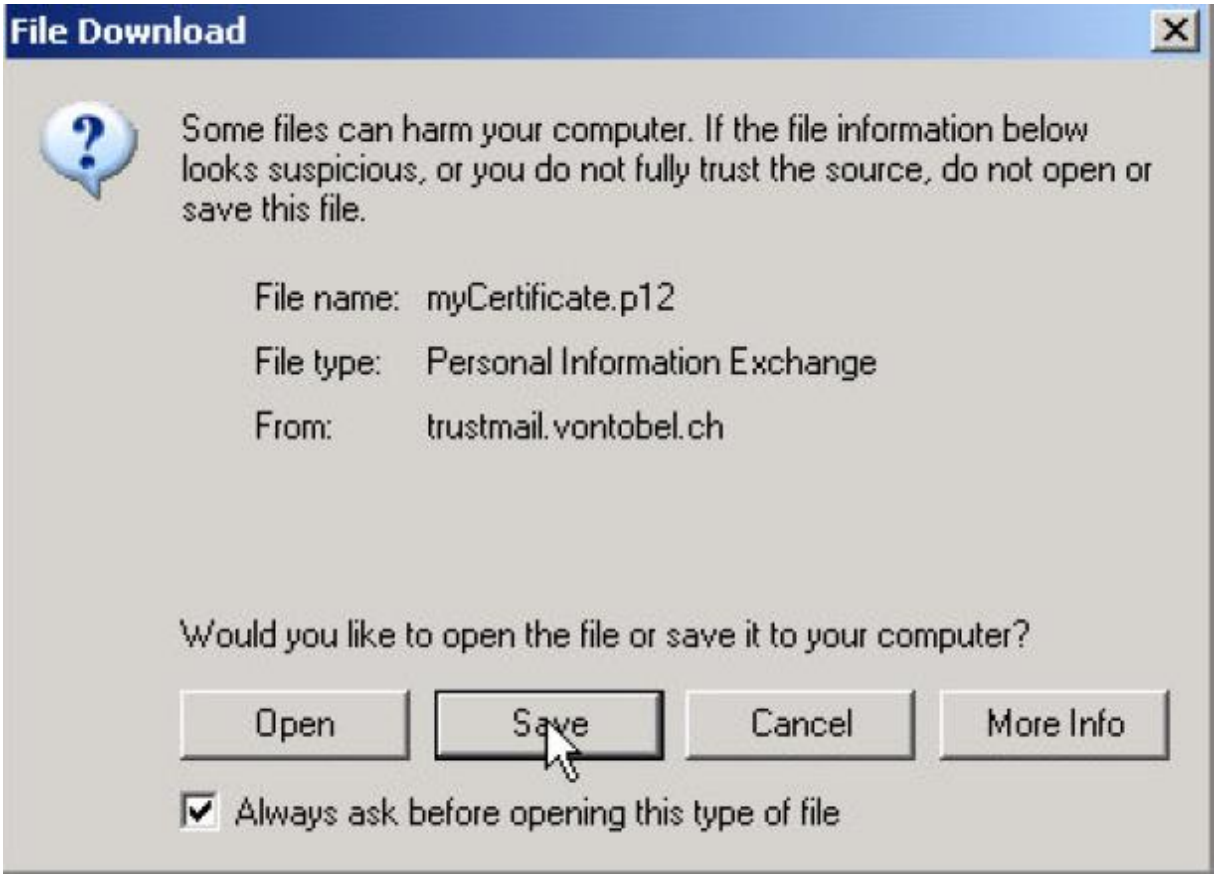
Installation manuelle

Si vous utilisez un autre navigateur qu'Internet Explorer ou un autre logiciel de messagerie qu'Outlook, vous devez choisir l'option « Manual Installation ».
Veuillez entrez le mot de passe à usage unique. Ce mot de passe nous permet de nous assurer que c'est bien vous qui vous enrôlez dans le système. Pour l'obtenir, veuillez nous contacter au +41-32-724 96 60.
Cliquez sur le bouton « Proceed » pour commencer l'installation du certificat.



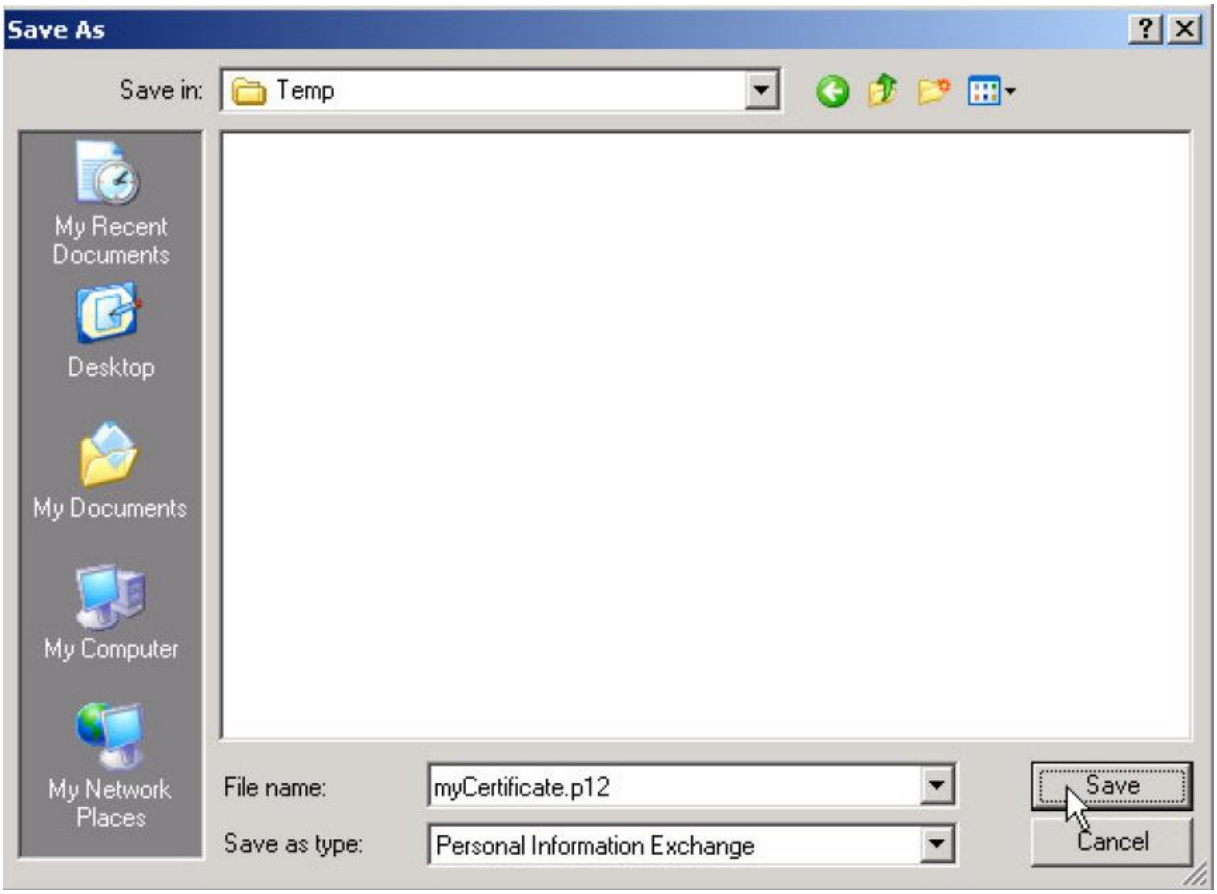
Entrez un mot de passe personnel de votre choix pour protéger l'installation du certificat et cliquez sur « Download Certificate ».

> **Attention :** Une fois que vous avez cliqué sur le lien « Download Certificate », notre système va générer un certificat et dans le même temps va crypter le message d'origine avec ce certificat et vous l'envoyer. Tant que le certificat n'est pas correctement installé, vous ne pourrez pas décrypter le message d'origine.
Vous ne pouvez pas interrompre le téléchargement du certificat en cours.
Si pour une quelconque raison, le téléchargement ne se déroulait pas correctement, veuillez contacter l'expéditeur de la notification.

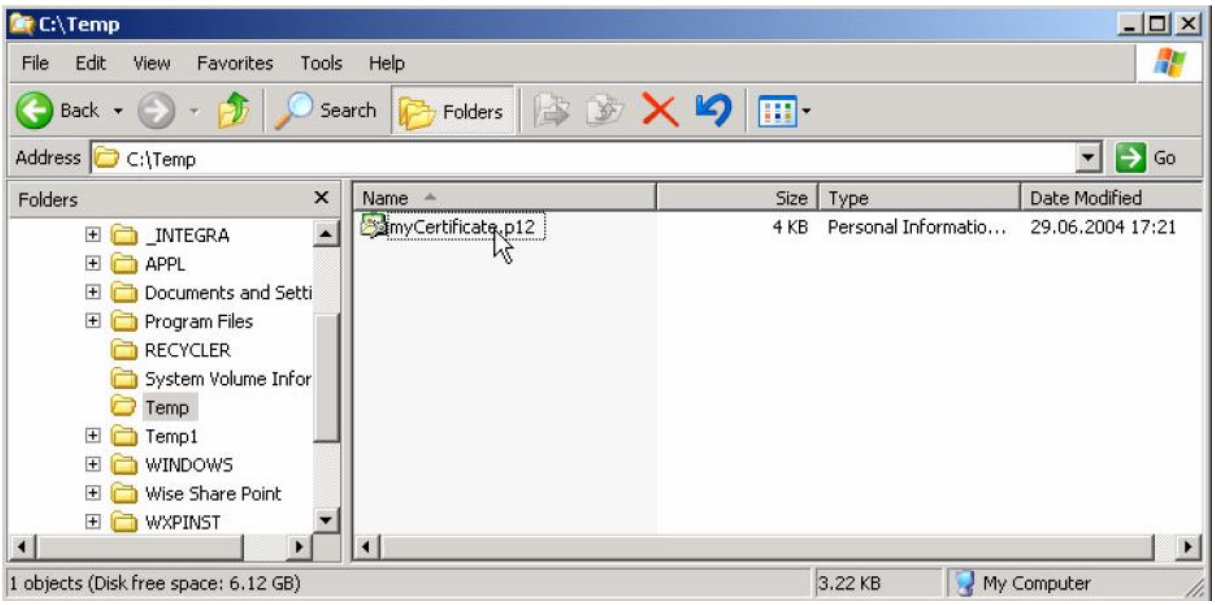


La boîte de téléchargement vous propose de télécharger le certificat et de le sauver sur votre disque dur ou de l'ouvrir directement après le téléchargement.

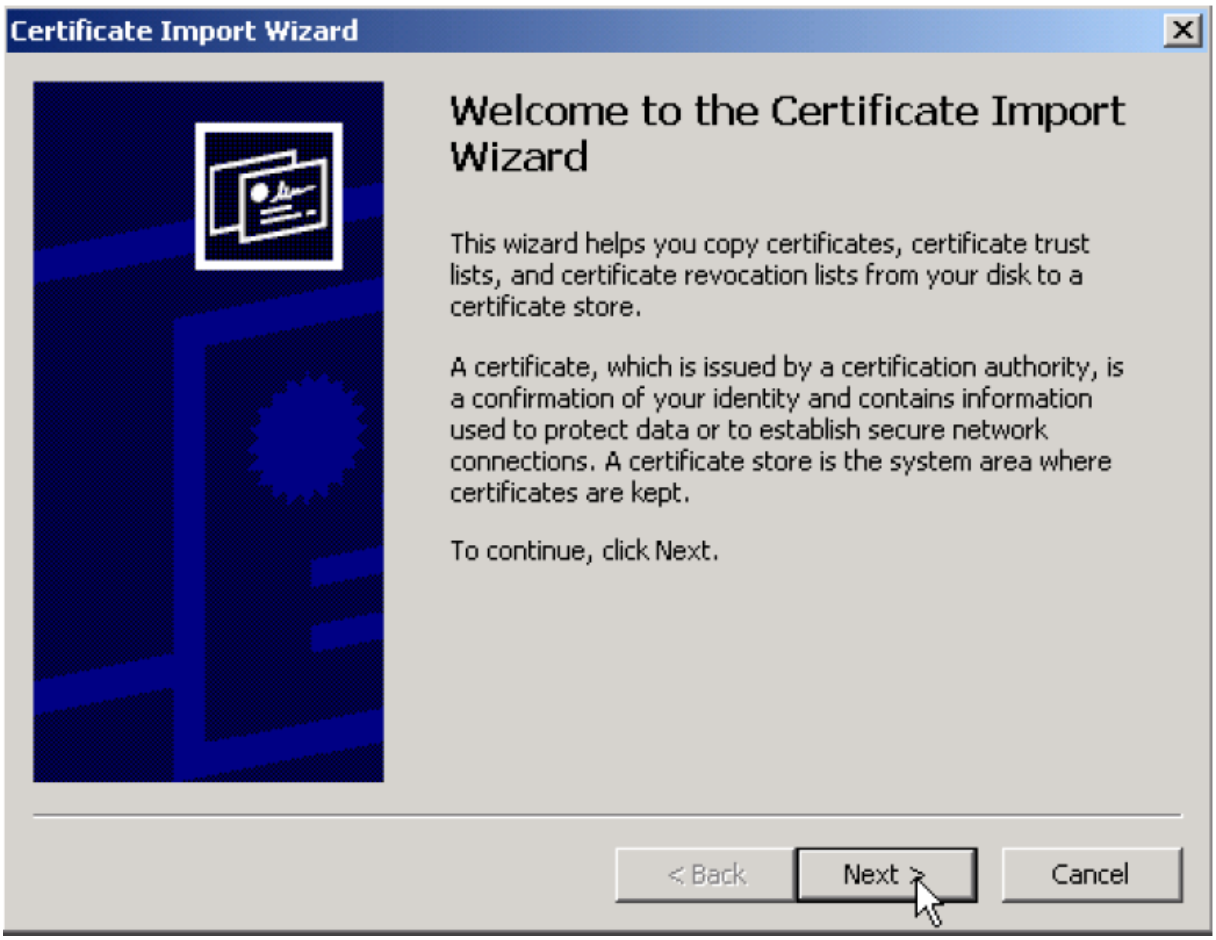
Nous vous recommandons de choisir de sauver le certificat sur votre disque dur.



Si vous choisissez l'option « Sauver », le système vous demande d'indiquer un emplacement sur votre disque dur pour sauvegarder le certificat.

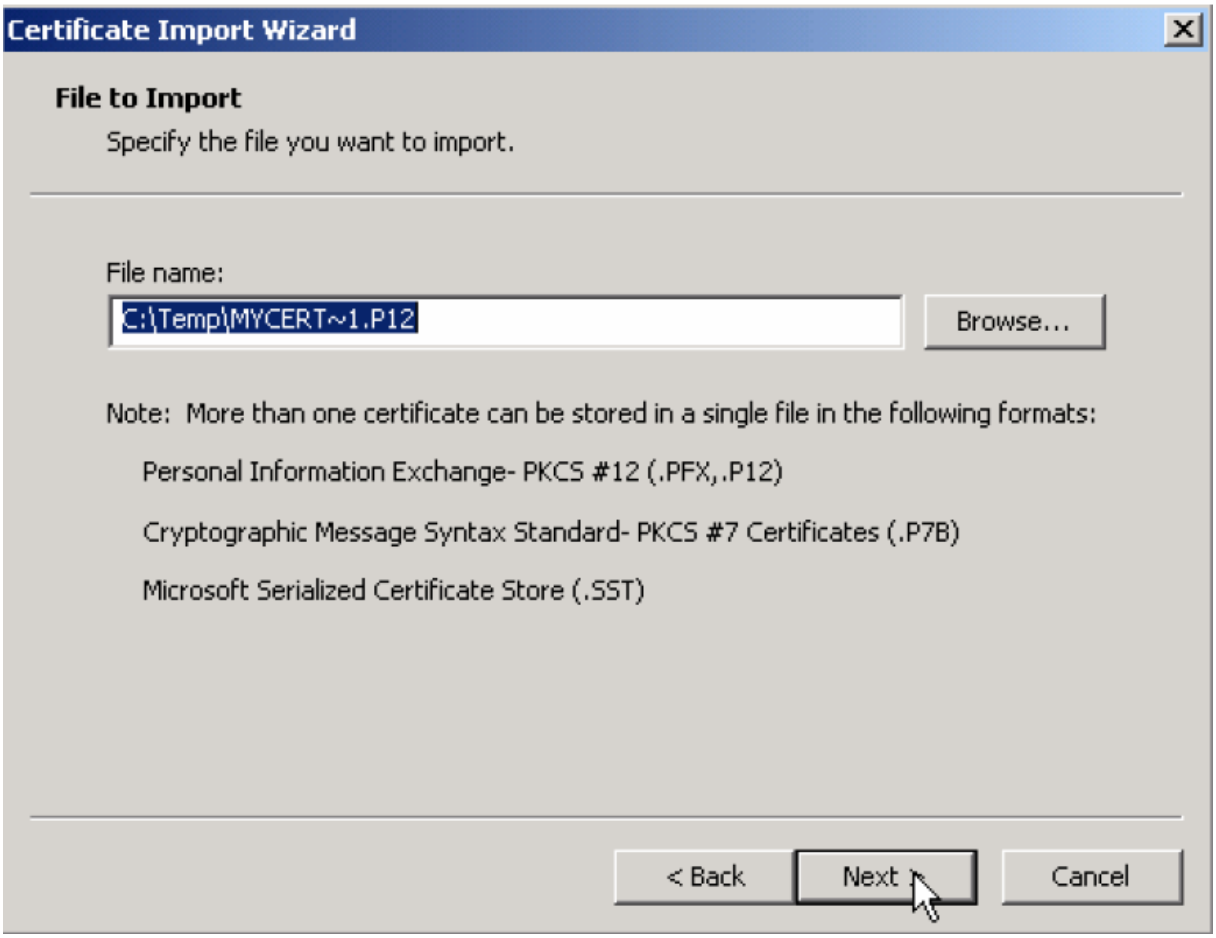


Une fois que le fichier a été téléchargé et sauvé sur votre ordinateur, vous pouvez commencer l'installation en double-cliquant sur le fichier.



L'assistant « Importation de certificat » s'ouvre sur votre ordinateur.

Cliquez sur « Next » pour commencer l'installation.



Contrôlez bien que le fichier importé soit bien le fichier que vous avez sauvé précédemment.

Cliquez sur « Next » pour poursuivre l'installation.

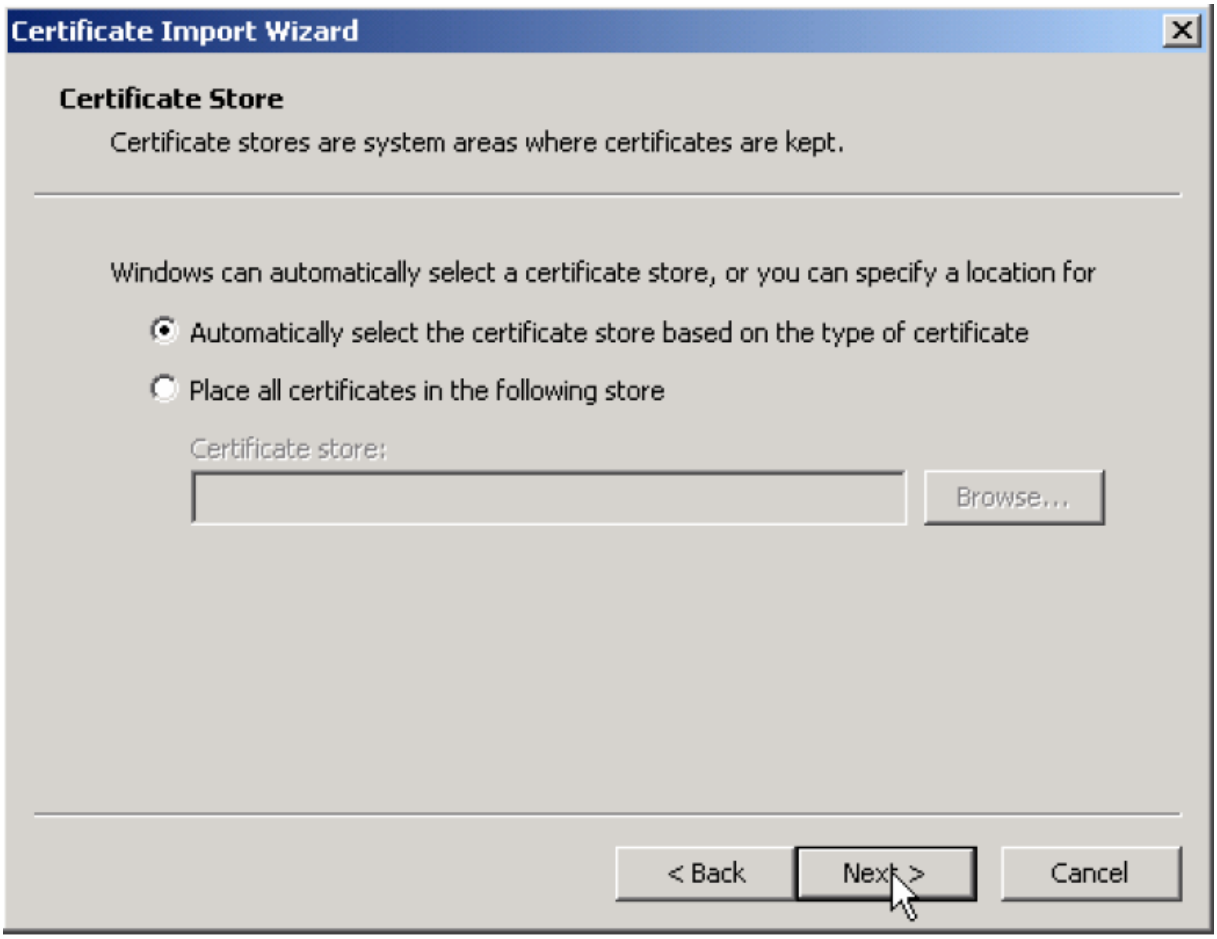
Vous devez entrer un mot de passe afin de protéger votre certificat (clé privée).

L'assistant vous propose deux options de sécurité :

> Si vous sélectionnez « Activer la sécurité renforcée des clés privées », à chaque fois que votre clé privée sera utilisée, par exemple pour décrypter ou signer un e-mail, vous devrez entrer le mot de passe (important si votre ordinateur est utilisé par plusieurs personnes).

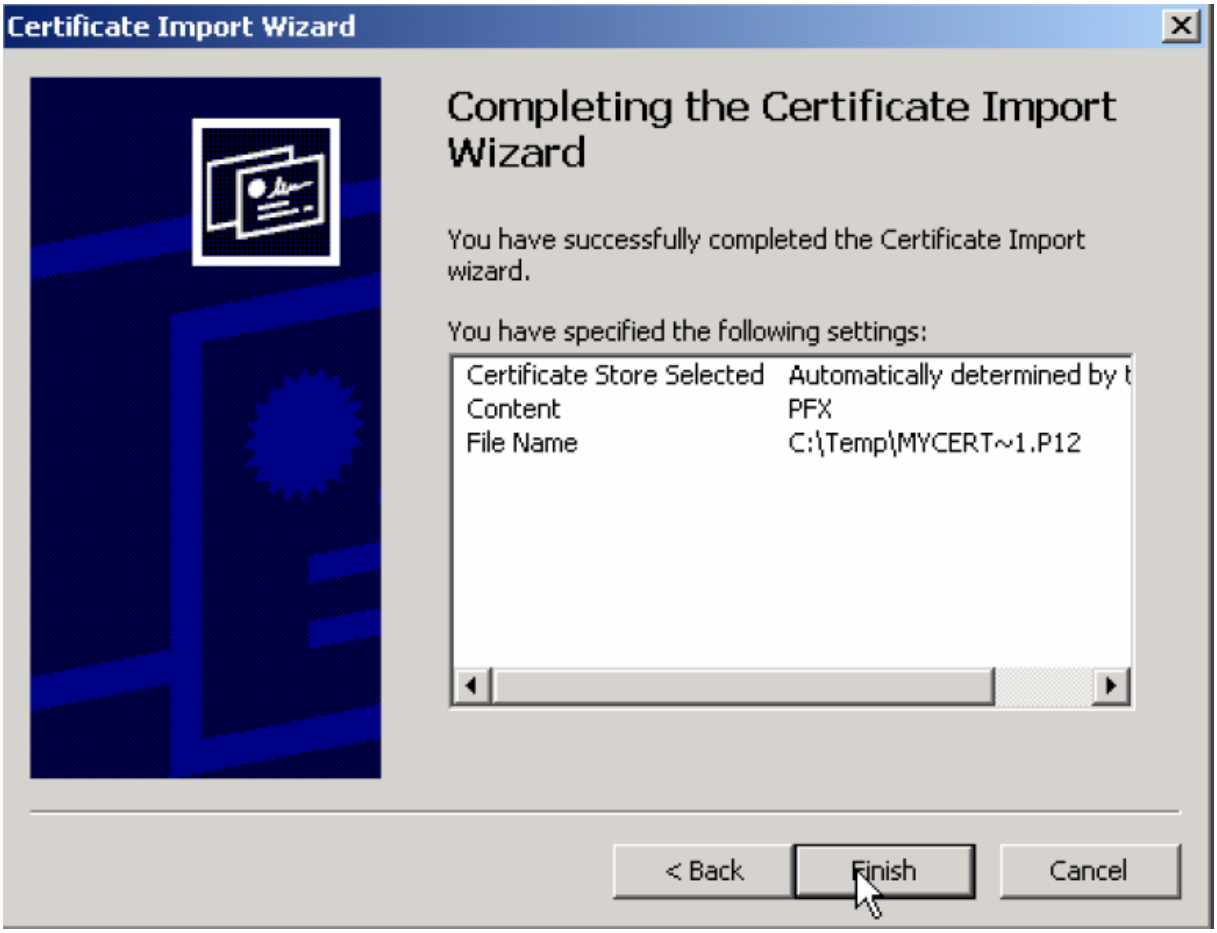
> Nous vous **recommandons** de rendre votre clé exportable afin de sauvegarder votre clé privée sur un média externe. Ainsi, si vous devez réinstaller votre ordinateur, vous pourrez réutiliser cette clé.

Cliquez sur « Next » pour poursuivre l'installation.



Laissez Windows sélectionner automatiquement le magasin de certificat.

Cliquez sur « Next » pour poursuivre l'installation.



Cliquez sur « Finish » pour finir l'installation de votre certificat personnel.

Votre certificat personnel a été installé avec succès sur votre ordinateur.

Vous allez recevoir très rapidement l'e-mail crypté d'origine dans votre logiciel de messagerie habituel.

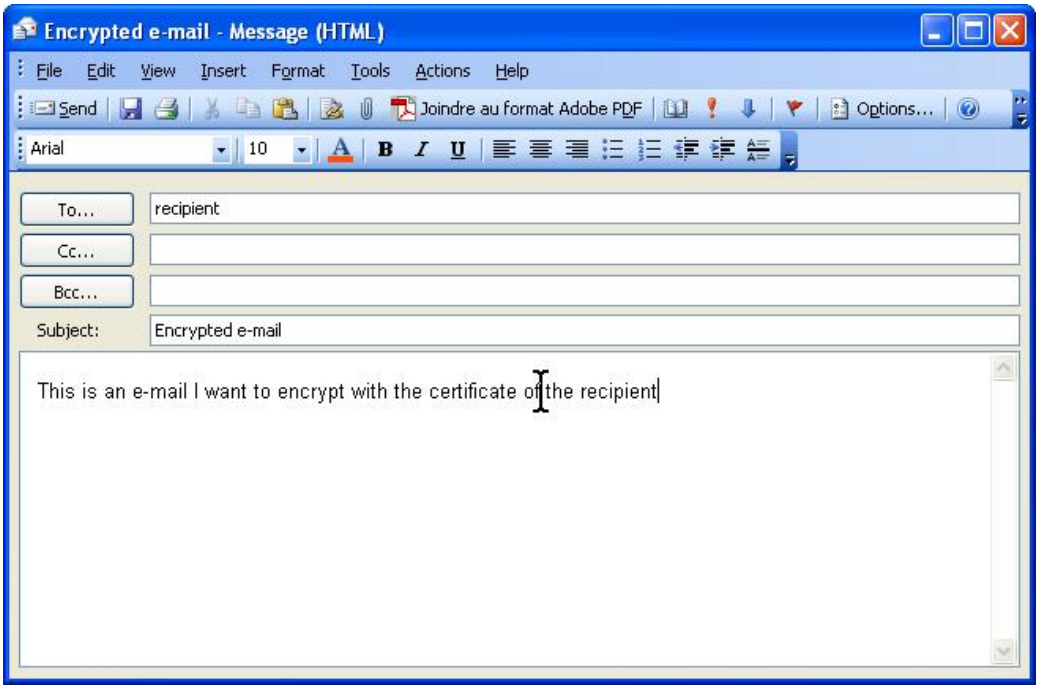
Tous les messages ultérieurs que nous vous enverrons seront automatiquement cryptés.

Encryption d'emails envoyés à P&TS

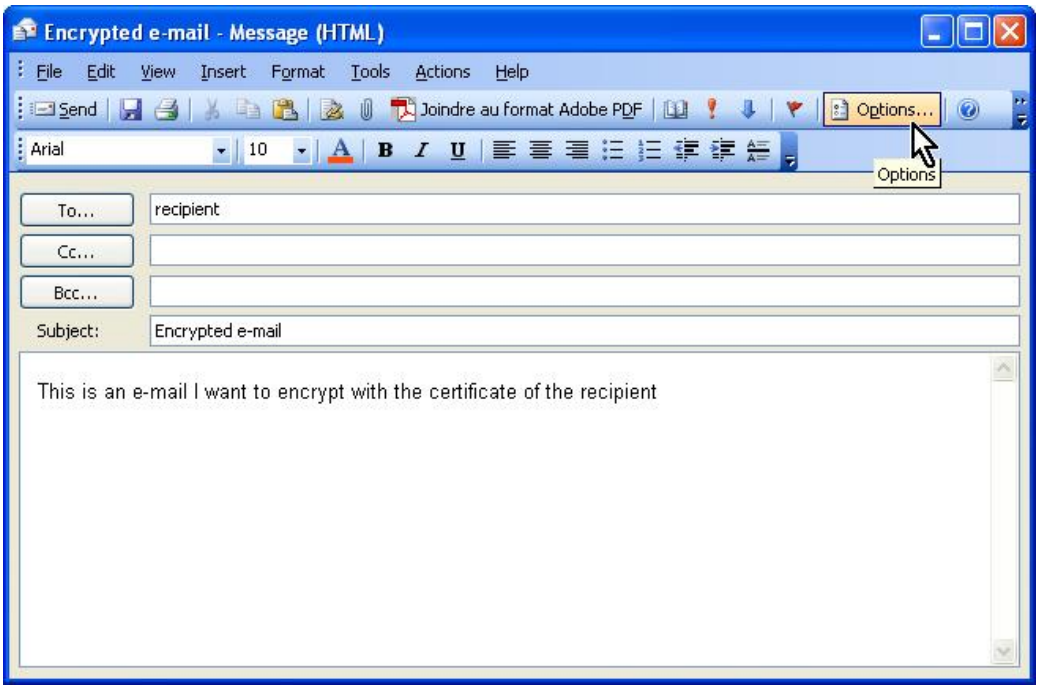
Lorsque le certificat a été correctement installé, tous les e-mails reçus de P&TS seront en principe signés et encryptés.
Par contre, les e-mails que vous enverrez vous-même à P&TS ne seront en principe ni signés, ni encryptés par défaut (dépend des configurations de votre logiciel). Il est donc nécessaire d'indiquer, pour chaque e-mail envoyé à P&TS, que vous souhaitez le protéger.

Les copies d'écran ci-dessous illustrent la procédure pour encrypter un e-mail avec Outlook2003 :

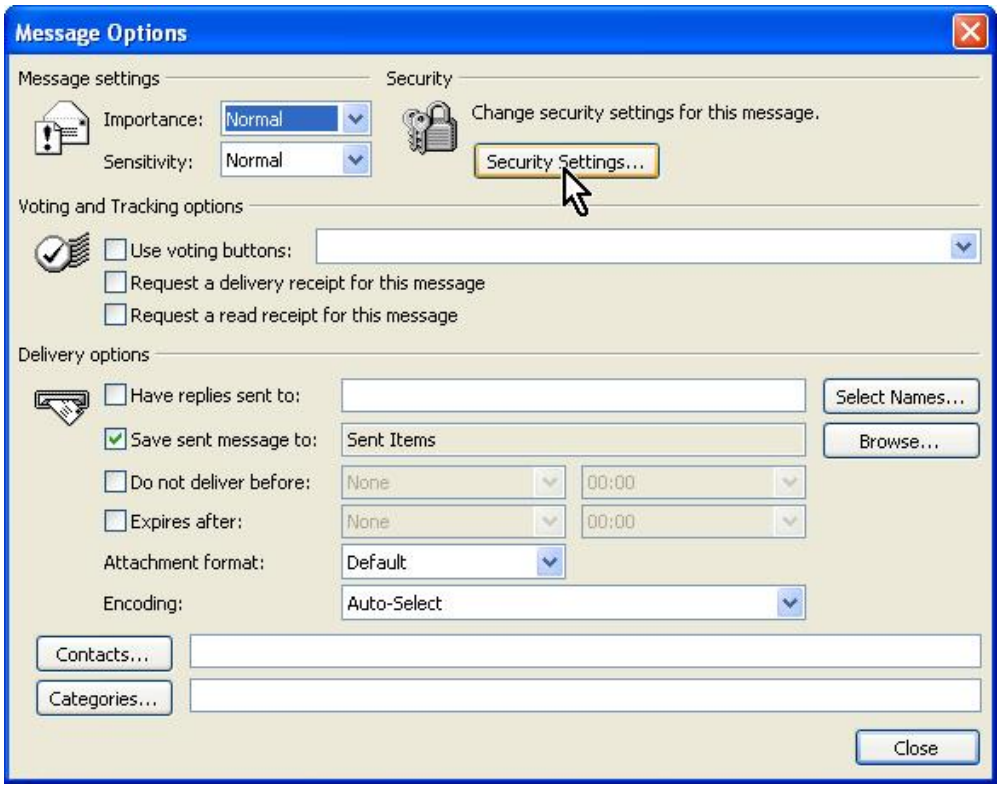
A. Créez un e-mail de la manière ordinaire :



B. Choisissez « Options » dans le menu :



C. Choisissez « Security Settings :



D. Cliquez sur « Encrypt message contents and attachments »:

E. Cliquez sur OK, Close, puis Send pour envoyer le message

Vous pouvez aussi choisir de signer électroniquement les e-mails sortant avec le certificat généré.

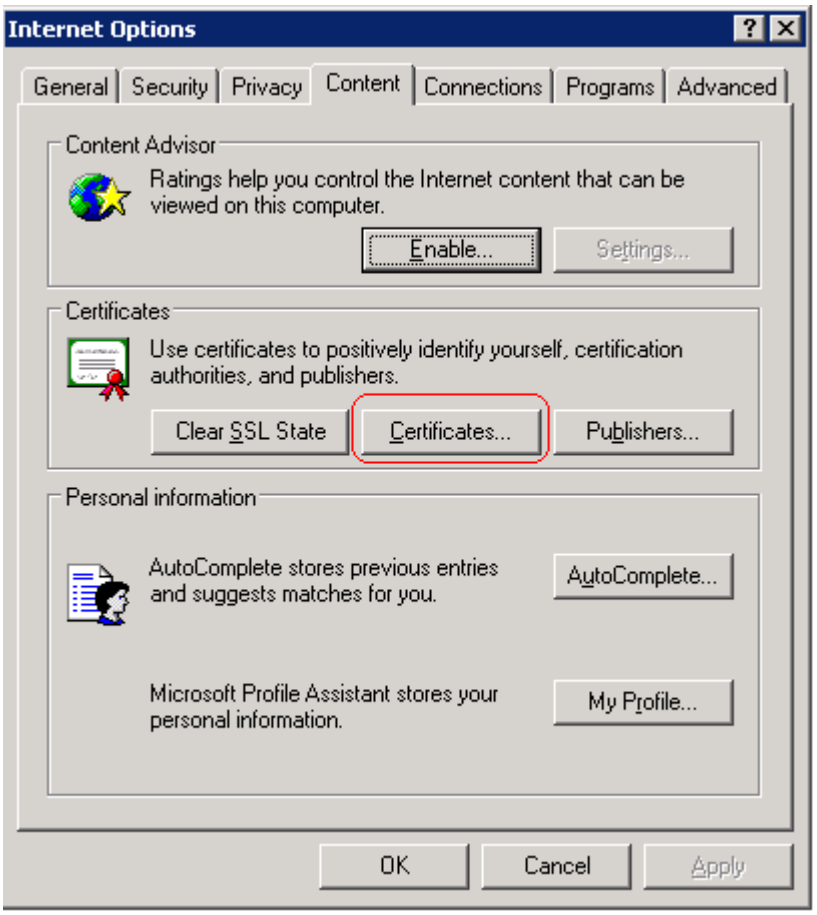
Sauvegarde du certificat

Le certificat S-MIME généré au cours de la procédure d'enrôlement vous est nécessaire pour décrypter les e-mails reçus de P&TS. Il est recommandé de sauvegarder ce certificat pour pouvoir le transférer sur un nouvel ordinateur ou pour en disposer en cas de réinstallation du logiciel client. P&TS ne dispose pas de copie de votre certificat.

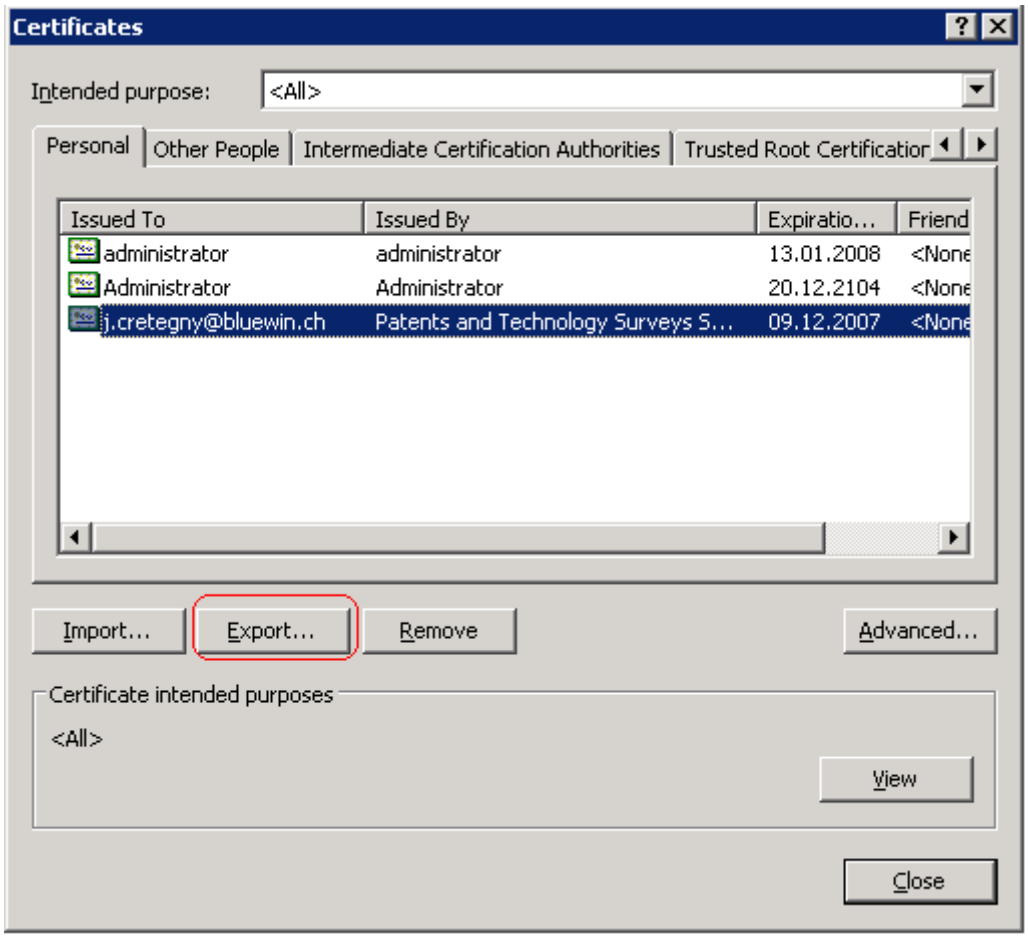
La procédure illustrée ci-dessous a été réalisée à partir d'Internet Explorer 6. Elle peut donc différer selon la version et le navigateur utilisé.

Dans le menu Outil d'Internet Explorer 6

A. Allez dans le menu Tools->Internet Options->Content
B. Cliquez sur « Certificates »



C. Dans l'onglet « Personal»- > Sélectionnez le certificat P&TS et cliquez sur « Export »



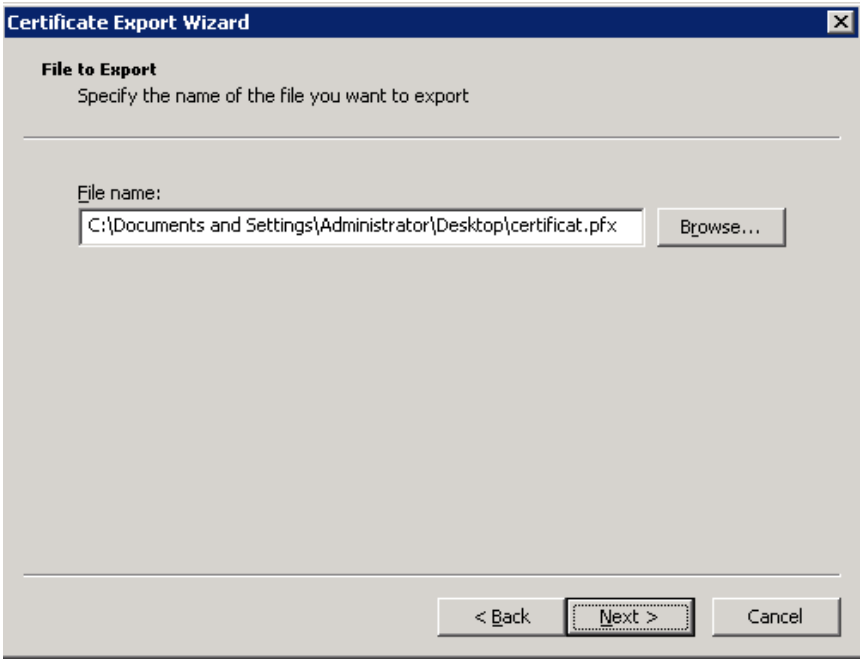
D. L'assistant d'exportation des certificats s'ouvre et demande si l'on veut exporter la clé privée. Il faut répondre oui car c'est cette clé qui vous permet de décrypter les e-mails reçus

E. Laissez les options et le format d'exportation par défaut

F. Entrez un mot de passe pour protéger votre clé privée.

> **Attention :** En cas d'oubli du mot de passe, vous ne serez plus en mesure d'utiliser votre clé privée et donc de décrypter les e-mails de P&TS.

G. Entrez un nom pour le certificat à exporter



H. Une boîte de dialogue s'ouvre et demande si l'on autorise le système à accéder à la clé privée. Cliquez sur « OK »

I. Le certificat a été exporté avec succès.

J. Copiez ce fichier en lieu sûr (CD-ROM, disquette, lecteur de sauvegarde)