

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 pour Internet Explorer et Outlook : page 2
- > Installation pour Lotus Notes : page 5
- > Installation manuelle : page 6

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.

Clia	uez sur	le bouton	« Proceed »	pour	commencer	l'installation	du certificat.
	acr 201	ie boaton	. I I O CCCC .	pour	commencer	1 milliona cioni	aa certincati

Edit <u>Vi</u> ew F <u>a</u> vorites Iools <u>H</u> elp		4
ack 🔹 🕥 🛩 😰 🐔 🔎 Search 🛭 👷 Favorites 🚳 Media 🔗 🔗 🖘 😓 🚍		
ass 🥘 https://server2.patentattorneys.ch/SecMail/selectMailIE.jsp	💌 🄁 Go	Links
Certificate Installation A personal S/MIME certificate will be generated for you in order to transmit the secure email to you.		
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.	Help: Online / PDF	
One Time Password	Proceed)
Lotus Notes 6 or higher		
Please choose this option if your are using Lotus Notes 6 or higher as email program.	Help: Online / PDF	
	Proceed	
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.	^s Help: Online / PDF	
One Time Password	Proceed	
ne	🔒 🥶 Internet	

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

Potential	Scripting Violation
1	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	<u>Y</u> es

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

Creating a new RSA exchange key				
	An application is creating a Protected item.			
	CryptoAPI Private Key			
	Security level set to Medium Set <u>S</u> ecurity Level			

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

🚰 Certificate Installation - Microsoft Internet Explorer		_ 🗆 🗵
File Edit View Favorites Tools Help		
🔇 Back 🔹 🕘 👻 😰 🥎 🔎 Search 💠 Favorites 🜒 Media 🔣 😥 😓		
Address 🕘 https://server2.patentattorneys.ch/SecMail/certificatesExtP10Request1.jsp	💌 🄁 Go	Links »
Automatic Certificate Installation A personal certificate was generated for you.		*
Next Step The new certificate will now be installed in your browser (and automatically in Outlook, Outlook Express or Novell GroupWise too). Please press on the "Proceed" button to continue. (Proceed	
		¥
(2) Done	🗀 📿 Internet	4

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 ».

Security	Warning
	You are about to install a certificate from a certification authority (CA) claiming to represent:
	Patents and Technology Surveys SA CA
	Windows cannot validate that the certificate is actually from "Patents and Technology Surveys SA CA". You should confirm its origin by contacting "Patents and Technology Surveys SA CA". The following number will assist you in this process:
	Thumbprint (sha1): 95211789 63300E06 F69C1BE9 D6F732F5 2F3453F7
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
	Do you want to install this certificate?
	<u>Y</u> es

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.

🚰 Certificate Installation - Microsoft Internet Explorer		_ 🗆 X
<u>File Edit Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
🔾 Back 🔹 🕥 🛩 🗷 🙎 🏠 🔎 Search 🤹 Favorites 😵 Media 🛷 😥 😓 🚍		
Address 🕘 https://server2.patentattorneys.ch/SecMail/selectMailIE.jsp	💌 🄁 Go	Links »
Certificate Installation A personal S/MIME certificate will be generated for you in order to transmit the secure email to you.		A
Coutlook, 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.	Help: Online / PDF	
One Time Password	Proceed	
Lotus Notes 6 or higher		
Please choose this option if your are using Lotus Notes 6 or higher as email program.	Help: Online / PDF	
	Proceed	
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.	Help: Online / PDF	
One Time Password	Proceed	
		~
Done State S	🔒 😂 Internet	

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.

File Down	nload			×
2	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not op save this file.			ation below , do not open or
	File name:	myCertificate.p12		
	File type:	Personal Information B	xchange	
	From:	trustmail.vontobel.ch		
	Would you like !	o open the file or save	it to your con	nputer?
	Open	Save	Cancel	More Info
	🔽 Always ask	pefore opening this type	e of file	

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.

Save As					<u>? ×</u>
Save in:	Temp		•	G 🕫 🖻 🖽	•
My Recent Documents					
Desktop					
My Documents					
My Computer					
My Network Places	File name: Save as type:	myCertificate.p12 Personal Information E	xchange	-	Save

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

🚉 C:\Temp				
File Edit View Favorites Tools He	elp			
🌀 Back 🔹 🕥 🖌 🏂 🔎 Search	Folders	< 🍤 💷 ·		
Address 🗁 C:\Temp				💌 🔁 Go
Folders × Na	me 🔺	Size	Туре	Date Modified
INTEGRA APPL Documents and Setti Program Files RECYCLER System Volume Infor Temp Temp1 WINDOWS Wise Share Point Wise Share Point	myCertificate,p12	4 KB	Personal Informatio	29.06.2004 17:21
1 objects (Disk free space: 6.12 GB)			3.22 KB 🚺 My (Computer

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

Certificate Import Wizard



×

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

Cliquez sur « Next » pour commencer l'installation.

Certificate Import Wizard	×
File to Import Specify the file you want to import.	
File name: C:\Temp\MYCERT~1.P12 Browse	
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
< Back Next Cancel	

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

Cliquez sur « Next » pour poursuivre l'installation.

Certificate Import Wizard	×
Password	
To maintain security, the private key was protected with a password.	
Type the password for the private key.	

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
< Back Next > Cancel	

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.

Certificate Import Wizard			×
Certificate Store			
Certificate stores are system areas where	certificates are kept.		
Windows can automatically select a certific	ate store, or you can speci	fy a location for	
Automatically select the certificate :	store based on the type of	certificate	
O Place all certificates in the following	store		
Certificate store:			
		Browse	
	< Back Next :	> Cancel	
Windows can automatically select a certific Automatically select the certificate select Place all certificates in the following Certificate store:	ate store, or you can speci store based on the type of store	fy a location for certificate Browse,	

Laissez Windows sélectionner automatiquement le magasin de certificat.

Cliquez sur « Next » pour poursuivre l'installation.

Certificate Import Wizard		×
	Completing the C Wizard You have successfully comple wizard.	Certificate Import
	You have specified the follow	ving settings:
	Certificate Store Selected Content File Name	Automatically determined by t PFX C:\Temp\MYCERT~1.P12
	< Back	Finish Cancel

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 :

🖻 Encrypted e-mail - Message (HTML)
Eile Edit View Insert Format Iools Actions Help
🗄 📼 Send 🚂 🎒 🐰 📭 🏨 🌛 🕕 🏗 Joindre au format Adobe PDF 🛄 🍷 🥾 👻 🖹 Options 🕢 🍟
Arial - 10 - ▲ B I U 를 를 들 는 는 課 課 ∰
To recipient Cc
Subject: Encrypted e-mail
This is an e-mail I want to encrypt with the certificate of the recipient
8

B. Choisissez « Options » dans le menu :

📫 Encrypted	d e-mail - Message (HTML)
Eile Edit	<u>View Insert Format Tools Actions H</u> elp
] 🖃 <u>S</u> end 🔓	🛿 🎒 🐰 📭 🏨 🏂 🕕 🏗 Joindre au format Adobe PDF 🛄 🕴 🦊 👻 📴 Options 🥝 📲
Arial	• 10 • <u>A</u> B Z U 言言言注言律律言 ,
To Cc Bcc	Options recipient
Subject:	Encrypted e-mail
This is an e	e-mail I want to encrypt with the certificate of the recipient
	8

C. Choisissez « Security Settings :

Message Options				
Message settings Importance: Normal Sensitivity: Normal Voting and Tracking options Use voting buttons: Request a delivery recei Request a read receipt f	Security Change Security	security settings for th	nis message.	<u> </u>
Delivery options				Select Names
Save sent message to:	Sent Items			Browse
Do not deliver before:	None	00:00	~	
Expires after:	None	✓ 00:00	~	
Attachment format:	Default	~		
Encoding:	Auto-Select		~	
Contacts Categories				Close

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

Security Prop	erties ge contents and attachments		X
Send this	nature to this message message as clear text signed		
Request	5/MIME receipt for this message		
Security Settings Security setting			
<automatic></automatic>	*	Ch	ange Settings
Security Label			
Policy Module:	<none></none>	\sim	Configure
Classification:		Ý	
Privacy Mark:	-		
		_	
	ОК		Cancel

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 »

Internet Options ? 🗙
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear <u>S</u> SL State <u>C</u> ertificates Pu <u>b</u> lishers
Personal information
AutoComplete stores previous entries AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

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

Certificates			? ×
Intended purpose: <a>All>			•
Personal Other People Interm	ediate Certification Authorities	Trusted Root Certifica	atior 🔸 🕨
Issued To	Issued By	Expiratio	Friend
administrator	administrator	13.01.2008	<none< th=""></none<>
Administrator	Administrator	20.12.2104	<none< td=""></none<>
j.cretegny@bluewin.ch	Patents and Technology Survey	ys S 09.12.2007	<none< th=""></none<>
			Þ
Import	<u>R</u> emove	Adv	anced
Certificate intended purposes			
<aii></aii>		<u></u>	ew
			⊆lose

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

rtificat	te Export Wizard	
Export Yo	t Private Key ou can choose to export the private key with the certificate.	
Pr	rivate keys are password protected. If you want to export the private key with the ertificate, you must type a password on a later page.	
De	o you want to export the private key with the certificate?	
	O No, do not export the private key	
	< <u>B</u> ack <u>N</u> ext > Cancel	

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

oort File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (IER)
C Bage-64 encoded X,509 (,CEF	2)
C Gryptographic Message Synta	ax Standard - PKCS #7 Certificates (.P7B)
🔲 Include all certificates in t	he certification path if possible
Personal Information Exchange	je - PKCS #12 (.PFX)
Include all certificates in t	he certification path if possible
Enable strong protection ((requires IE 5.0, NT 4.0 SP4 or above)
🔲 Delete the private <u>k</u> ey if t	he export is successful
	< <u>B</u> ack <u>N</u> ext > Cano

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.

Certificate Export Wizard	x
Password To maintain security, you must protect the privat	e key by using a password.
Type and confirm a password.	
Password:	
Confirm password:	
<	Cancel

G. Entrez un nom pour le certificat à exporter

Eile name:	
C:\Documents and Settings\Ac	dministrator\Desktop\certificat.pf× Browse

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

Exporting your	private exchange key 🛛 🗙	1
	An application is requesting access to a Protected item. CryptoAPI Private Key	
	OK Cancel <u>D</u> etails	

I. Le certificat a été exporté avec succès.

Certificate Export Wizard	×
The export was successful.	
ОК	

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