

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.

🚰 Certificate Installation - Microsoft Internet Explorer		_ 🗆 🗵
Eile Edit <u>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 »
		<u> </u>
Certificate Installation		
A personal Similiae centricate will be generated for you in order to transmit the secure email to you.		
Cutlook, Outlook Express and Novell GroupWise		
Please choose this option if your are using Outlook, Outlook Express or Novell GroupWise as email		
program.	Help: Unline / PDF	
Click tes and ok when your browser asks you whether to generate a new centilicate.		
One Time Password	Proceed	
Lotus Notes 6 or higher		
Place chose this ontion if your are using Latus Notes 6 or higher as email program	Heln: Online / DDF	
	Theip. Children P.D.	
	Proceed	
Manual Installation]	
Please choose this option if your are using another email program or if the installation with one of the upper options	Halm Online (DDF	
did not work.	Help. Online / PDF	
One Time Password	Procood	
	Floceed	
		-
Done	🔒 🅐 Internet	1.

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

Potential	Scripting Yiolation
⚠	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?
	Yes No

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

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

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

🚈 Certificate Installation - Microsoft Internet Explorer		_ 🗆 🗵
Eile Edit View Favorites Tools Help		-
🔇 Back 🔻 🕥 🛩 🖻 👔 🏠 🔎 Search 🔹 Favorites 🜒 Media 🥴 😥 😓 🗔		
Address 🕘 https://server2.patentattorneys.ch/SecMail/certificatesExtP10Request1.jsp	💌 ラ 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	
Done	🔒 🔹 Internet	_

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.

🚰 Certificate Installation - Microsoft Internet Explorer	
Eile Edit View Favorites Tools Help	🥂
🔇 Back 🔻 🕥 🖌 😰 🏠 🔎 Search 🨾 Favorites 🜒 Media 🤣 😥 🗧	
Address 🙆 https://server2.patentattorneys.ch/SecMail/selectMailIE.jsp	💌 🌛 Go 🛛 Links 🎽
	<u> </u>
Certificate Installation A nersonal SMIME 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	Help: Online / PDF
program. Click Yes' and 'Ok' when your browser asks you whether to generate a new certificate.	
	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
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 Tree Parciaper	
	Proceed
Done	🔒 👩 Internet

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.

File Dowr	nload			×
?	Some files can h looks suspicious save this file.	narm your compu ;, or you do not f	ter. If the file inform ully trust the source	ation below , do not open or
	File name:	myCertificate.p1	12	
	File type:	Personal Inform	ation Exchange	
	From:	trustmail.vontob	el.ch	
	Would you like (o open the file o	r save it to your con	nputer?
	Open	Save	Cancel	More Info
	🔽 Always ask	before opening t	his type of file	

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.

Save As						? ×
Save in:	Temp		•	000	•	
My Recent Documents						
Desktop						
My Documents						
My Computer						
My Network Places	l File name: Save as type:	myCertificate.p12 Personal Informa	tion Exchange	•		Save

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

🚉 C:\Temp				
File Edit View Favorites Tools	Help			
🕝 Back 🔹 🕥 🖌 🏂 🔎 Searc	h 🔀 Folders	K 🍤 💷-		
Address 🗁 C:\Temp				💌 🔁 Go
Folders ×	Name 🔺	Size	Туре	Date Modified
 INTEGRA APPL Documents and Setti Program Files RECYCLER System Volume Infor Temp Temp1 WINDOWS Wise Share Point WXPINST 		4 KB	Personal Informatio	29.06.2004 17:21
1 objects (Disk free space: 6.12 GB)	ч		3.22 KB	Computer

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

Certificate Import Wizard



X

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

Click on « Next » to start the installation.

Certificate Import Wizard	X
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 Cance	

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

Click on « Next » to continue the installation.

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

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	

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.

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

Allow Windows to select the certificate store.

Click on « Next » to continue the installation.

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

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 :

🗈 Encrypted e-mail - Message (HTML)
Eile Edit View Insert Format Iools Actions Help
🗄 🖃 Send 🔛 🎒 🐰 🤖 隆 💩 🕕 🌄 Joindre au format Adobe PDF 💷 📍 🦊 🌪 🖹 Options 🙆 🏅
Arial - 10 - ▲ B I U 国 喜 喜 汪 汪 課 課 無 -
To recipient Cc
Bcc Subject: Encrypted e-mail
This is an e-mail I want to encrypt with the certificate of the recipient

B. Choose « Options » in the menu :

😰 Encrypted	d e-mail - Message (HTML)
Eile Edit	<u>View Insert Format Tools Actions Help</u>
] 🖃 <u>S</u> end 🔓	🛿 🍓 🔏 📭 🅦 🌛 🕕 📆 Joindre au format Adobe PDF 💷 📍 🦊 🍸 📴 Options @ 🛛 🚆
Arial	• 10 • <u>A</u> B Z U 書 書 語 語 譯 譯 編 💂 😽
To Cc Bcc	recipient
Subject:	Encrypted e-mail
This is an e	e-mail I want to encrypt with the certificate of the recipient

C. Choose « Security Settings » :

Message Options Message settings Importance: Normal	Security	Change sec	urity settings for	this message	
Sensitivity: Normal		Security S	ettings		
Voting and Tracking options			12		
Use voting buttons:					~
Request a delivery rece	ipt for this messa	ige			
Request a read receipt	for this message				
Delivery options					
Have replies sent to:					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	6				
					Close

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

Send this	nature to this messag message as clear te S/MIME receipt for th	ge xt signed nis message	
ecurity Settings Security setting]:	–	ange Settings
Security Label			lange bettingsn
Policy Module:	<none></none>	~	Configure
Privacy Mark:		Y	<u> </u>
	-		

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 »

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 <u>Au</u> toComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

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

Certificates			? ×
Intended purpose: <a>			•
Personal Other People Intern	nediate Certification Authorities	Trusted Root Certifi	catior 💶 🕨
Issued To	Issued By	Expiratio	Friend
🔛 administrator	administrator	13.01.2008	3 <none< th=""></none<>
Administrator	Administrator	20.12.2104	ł <non∈< th=""></non∈<>
🕮 j.cretegny@bluewin.ch	Patents and Technology Surve	ys S 09,12,2007	7 <none< th=""></none<>
•			Þ
Import	<u>R</u> emove	A	dvanced
Certificate intended purposes			
			View
			⊆lose

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.

Certificate Export Wizard	×
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with certificate, you must type a password on a later page.	the
Do you want to export the private key with the certificate?	
 Yes, export the private key 	
C No, do not export the private key	
< <u>B</u> ack <u>N</u> ext >	Cancel

E. Leave the default options and export format.

rtificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (,CER)	
C Bage-64 encoded X.509 (,CER)	
C ⊆ryptographic Message Syntax Standard - PKCS #7 Certificates (,P7B)	
\square Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
\square Delete the private <u>key</u> if the export is successful	
< <u>B</u> ack <u>N</u> ext > Cancel	

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.

ertificate Export Wizard	
Password To maintain security, you must protect the p	private key by using a password.
Type and confirm a password.	
<u>P</u> assword:	
Confirm password:	
	< <u>B</u> ack <u>N</u> ext > Cancel

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

<u>File name:</u>				
C:\Documents and	d Settings\Administra	ator\Desktop\certif	icat.pfx	B <u>r</u> owse

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

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

I. The certificate has been successfully exported.

Certificate Export Wizard	×
The export was successful.	
OK]	

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