P&TS
INTELLECTUAL PROPERTY

Exchange of secured e-mails with P&TS

Introduction

E-mails are not considered a secured means for the transmission of confidential information. We recommend that confidential information sent by e-mail to P&TS should be encrypted, notably invention notices, drafts of patent applications or any other information that, if divulged, could harm your interests or those of P&TS.

We use according to your own preference the protocols S-MIME or PGP for e-mail encryption and we encourage you to do the same and let us have your public key. If you do not already have an S-MIME or PGP certificate, we will be happy to supply one for free for all your exchanges with P&TS. The installation of an S-MIME certificate can ensure:

- your e-mail exchanges with P&TS will be encrypted reliably
- the messages will be signed electronically
- the message's originator cannot dispute having sent the e-mail (non-repudiation)
- the contents of the e-mail have not been modified or tampered with (integrity)

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

In the case of difficulties with the installation of S-MIME certificates, or if for any reason this type of certificate is not desired, you can also access the e-mails we send you through our webmail, on a secured page to which you can connect with a login and a password which we would be happy to supply.

Please do not hesitate to contact us so that we may send you an e-mail allowing you to register and use these secured communication possibilities.

P&TS SA
Av. J.-J. Rousseau 4
2001 Neuchâtel
Suisse
Tél : +41 32 727 14 27
Fax : +41 32 727 14 24
E-mail : info@patentattorneys.ch

E-mail encryption

Encryption allows the contents of an e-mail to be made illegible for anyone who does not have the right key. Thus, even if the message is intercepted when transiting over the Internet, it cannot be decrypted.

S-MIME or PGP encryption used by P&TS uses different keys for encrypting and decrypting:

- a public key: the key freely transmittable over the Internet; allows messages to be encrypted.

- a private key: secret key, installed only on the user's computer; allows messages encrypted with the corresponding public key to be decrypted.

For example, if the user A wishes to send an encrypted e-mail to the user B, A must have B's public key. The e-mail is encrypted with B's public key and the recipient B can decrypt the message with his private key.

Electronic signature

An e-mail's signature allows it to be signed electronically. Like the handwritten signature on a letter, the electronic signature of an e-mail has the following advantages:

- the message's originator cannot dispute having sent the e-mail (non-repudiation)
- the recipient can verify the originator's identity
- the recipient is certain of the message's integrity and can verify that neither the e-mail's body nor the attachments have been modified or tampered with in any way

The e-mail is signed with the originator's private key. No one else has this key so that no one can usurp the originator's identity.

What is a certificate?

A certificate is a file containing a person's public key and data relating to his identity, e.g. name and e-mail address. The certificates are issued by Certification Authorities – P&TS is such an authority. The certificates are usually limited in time and must be renewed, in the case of certificates issued by P&TS every two years.

If you send us an e-mail signed with a key issued by P&TS, we use your certificate to verify that the e-mail originates from you and has not been modified. We also need your certificate so that we may send you encrypted e-mails which only you will be able to decrypt with your private key.

What does PKI mean?

PKI means "Public Key Infrastructure". A PKI infrastructure allows digital certificates to be issued to the users. The entity having this type of infrastructure is called "Certification Authority”.

P&TS is thus a Certification Authority, which allows us to issue digital certificates.