Echange de e-mails sécurisés avec P&TS

Introduction

Les e-mails ne sont pas considérés comme un moyen sûr pour la transmission d'informations confidentielles. Nous recommandons de crypter les informations confidentielles envoyées par e-mail à P&TS, notamment les annonces d'inventions, les projets de demandes de brevet, ou toute autre information dont la divulgation pourrait nuire à vos intérêts ou à ceux de P&TS.

Nous utilisons à choix les protocoles S-MIME ou PGP pour l'encryptage de e-mails, et vous encourageons à faire de même et à nous communiquer votre clé publique. Si vous ne disposez pas de certificat S-MIME ou PGP, nous pouvons en mettre gratuitement à votre disposition dans le cadre de vos échanges avec P&TS. L'installation d'un certificat S-MIME permet d'assurer que :

- Vos échanges d'e-mails avec P&TS seront encryptés de manière fiable
- Les messages seront signés électroniquement
- L'expéditeur ne puisse pas contester avoir envoyé le e-mail (non répudiation)
- Le contenu du e-mail n'a pas été modifié (intégrité)

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.

En cas de difficultés avec l'installation de certificats S-MIME, ou si pour d'autres raisons ce type de certificats n'est pas désiré, vous pouvez également accéder aux e-mails que nous vous faisons parvenir au travers de notre webmail, sur une page web sécurisée à laquelle vous pouvez vous connecter avec un login et un mot de passe que nous vous faisons volontiers parvenir.

N'hésitez pas à nous contacter afin que l'on vous envoie un e-mail permettant de vous inscrire et d'utiliser ces possibilités de communications sécurisées.

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

Cryptage de e-mails

Le cryptage permet de rendre le contenu d'un e-mail illisible à celui qui ne dispose pas de la bonne clé. Ainsi, même si le message est intercepté lorsqu'il transite par Internet, il ne sera pas décryptable.

Le cryptage S-MIME ou PGP utilisé par P&TS utilise des clés différentes pour le cryptage et pour le décryptage:

- Une clé publique: clé transmissible librement sur Internet. Permet de crypter les messages.
- Une clé privée: Clé secrète, installée uniquement sur l'ordinateur de l'utilisateur. Permet de décrypter les messages encryptés avec la clé publique correspondante.

Par exemple, si l'utilisateur A désire envoyer un e-mail crypté à l'utilisateur B, A doit posséder la clé publique de B. L'e-mail est crypté avec la clé publique de B et le destinataire B peut le décrypter le message avec sa clé privée.

Signature électronique

La signature d'un e-mail permet de le signer électroniquement. Comme la signature manuscrite d'une lettre, la signature électronique d'un e-mail apporte les avantages suivants :

- L'expéditeur ne pourra pas contester avoir envoyé le e-mail (non répudiation)
- Le destinataire peut vérifier l'identité de l'expéditeur
- Le destinataire est certain de l'intégrité du message, et peut vérifier que ni le corps de l'e-mail, ni les pièces annexées n'ont été modifiées

L'e-mail étant signé avec la clé privée de l'expéditeur. Nul autre ne possède cette clé en sorte que personne ne peut usurper l'identité de l'expéditeur.

Qu'est-ce qu'un certificat ?

Un certificat est un fichier contenant la clé publique d'une personne et des données relatives à son identité, par exemple son nom et son adresse e-mail. Les certificats sont émis par des autorités de certification; P&TS constitue une telle autorité. Ils ont généralement une durée limitée et doivent être renouvelés, tous les deux ans dans le cas des certificats émis par P&TS.

Si vous nous envoyez un e-mail signé avec une clé émise par P&TS, nous employons votre certificat pour vérifier que le e-mail provient de vous et qu'il n'a pas été modifié. Nous avons aussi besoin de votre certificat pour vous envoyer des e-mails cryptés que vous serez seuls à pouvoir décrypter avec votre clé privée.

Que veut dire PKI ?

PKI signifie "Public Key Infrastructure". Une infrastructure PKI permet de délivrer des certificats numériques aux utilisateurs. La société qui possède ce type d'infrastructure est appelée "Autorité de certification".

P&TS est donc une autorité de certification, ce qui nous permet de vous délivrer des certificats numériques.