

Secure E-Mail – plus nécessaire que jamais

La communication par e-mail, totalement sécurisée

Grâce à SEPPmail, le transfert d'e-mails cryptés et signés numériquement, satisfaisant aux normes juridiques élevées en matière de protection des données et de conformité, n'a jamais été aussi simple.

Lors du transfert électronique de messages, les aspects de sécurité sont souvent occultés. Même des informations confidentielles sont souvent envoyées par e-mail sans aucune protection. Il ne doit pas toujours en aller ainsi. Grâce à SEPPmail, la solution Secure E-Mail développée en Suisse par le fabricant du même nom, SEPPmail, plus rien ne s'oppose à la communication sécurisée par e-mail. La solution complète Secure E-Mail comprend toutes les fonctionnalités et technologies permettant de protéger efficacement l'envoi de données sensibles et confidentielles par e-mail, de garantir l'authenticité de l'expéditeur ainsi que d'assurer la confidentialité et l'intégrité du message.

Echange de messages sécurisés

SEPPmail permet à tous les acteurs du marché – des PME aux entreprises et instituts financiers en passant par les études notariales, autorités et institutions de la santé – d'échanger des messages sécurisés avec tous les destinataires de leur choix. La plate-forme est ainsi compatible avec toutes les normes de cryptage usuelles, telles que S/MIME, TLS et openPGP.

Grâce à S/MIME, SEPPmail permet la signature numérique de tous les e-mails sortants, afin de confirmer l'intégrité (non-falsification) du message ainsi que l'authenticité de l'expéditeur. A cet effet, le dispositif Secure E-Mail autorise l'intégration immédiate de CA (Certifica-

tion Authorities) sélectionnés et donc la création automatique de signatures numériques.

Afin qu'une communication par e-mail sécurisée en continu soit disponible, même avec des réseaux de cryptage supérieurs comme HIN et IncaMail, SEPPmail a développé des «connecteurs» spécifiques. Ces derniers permettent d'échanger des informations sur tous les réseaux par le biais de Secure E-Mail. Cela profite notamment aux cantons, villes et communes, ainsi qu'aux institutions et aux acteurs de la santé (tels que les hôpitaux, offices AI, etc.).

SwissSign – acquisition automatique de certificat

Pour faciliter la création de signatures numériques, SEPPmail mise sur l'intégration de la «Certificate Authority» (CA) SwissSign. Ce qui permet d'accélérer considérablement l'ensemble du processus PKI («Public Key Infrastructure»). Il ne reste plus qu'à définir les personnes qui doivent signer les e-mails – toutes les autres étapes sont exécutées automatiquement.

IncaMail – une communication par e-mail conforme au règlement

IncaMail, le Managed Service dans le Cloud de la Poste Suisse, permet l'envoi sécurisé et traçable (conforme eGov) d'e-mails confidentiels à des destinataires ne disposant pas d'une infrastructure de cryptage. Les utilisateurs du service SEPPmail disposent d'un accès direct au réseau IncaMail grâce à l'option «SEPPmail IncaMail Edition», ce qui leur permet par exemple de communiquer des données aux autorités par voie électronique.

Aperçu des caractéristiques du service SEPPmail

Grâce à SEPPmail, l'envoi et la réception d'e-mails signés numériquement n'ont jamais été aussi confortables.



SEPPmail sécurise l'ensemble de la communication par e-mail au plus haut niveau:

- Cryptage et décryptage automatiques des e-mails et compatibilité avec toutes les normes usuelles
- Signature numérique des e-mails avec certificat utilisateur pour confirmer l'intégrité du message et l'authenticité de l'expéditeur
- Emission automatique de certificats par un organisme de certification accrédité (Managed Public Key Infrastructure, PKI)
- Cryptage automatique des e-mails entre les dispositifs SEPPmail (Managed Domain Encryption, MDE)
- Large File Management pour l'envoi sécurisé de fichiers volumineux

BOLL
IT Security Distribution

BOLL ENGINEERING SA

En Budron H15, 1052 Le Mont s. Lausanne
Tél 021 533 01 60, contact@boll.ch
www.boll.ch