SEPPMAIL

DIGITAL SIGNATURE MANAGEMENT

In addition to email encryption, SEPPmail also supports the RFC-compliant signing of transmitted messages. Thanks to DSM (Digital Signature Management), the integrity and authenticity of the message, as well as the authenticity of the sender, can be confirmed. This results in elevated trust and in a stronger company image. In addition, the sender's public key is transmitted through DSM. This is required to encrypt e-mails addressed to the original sender (encrypted reply).

Integrated connectors allow for fully automatic acquisition and management of certificates from external Certification Authorities (CAs). The signature solution allows all incoming encrypted e-mails to be decrypted with the recipient's private key.

HIGHLIGHTS AT A GLANCE

- Signing of outgoing e-mails with fully automated certificates
- Automatic checking and marking of incoming signed emails
- Guaranteed message integrity
- Confirmation of sender authenticity
- Local CA with automatic key generation (S/MIME and Open-PGP)
- Automatic generation of signature certificates
- Automatic acquisition and administration of certificates through Managed PKI (connectors to well-known CAs)

CERTIFICATES

SwissSign

digicert + QuoVadis

GlobalSign GMO INTERNET GROUP

BUNDESDRUCKEREI

... and others

CONTACT

Switzerland

SEPPmail AG Schweiz
Industriestrasse 7
CH-5432 Neuenhof

Tel. +41 56 648 28 38
info@seppmail.ch
www.seppmail.ch

Germany

SEPPmail-Deutschland GmbH
Ringstrasse 1c
85649 Brunnthal b. München

SEPPmail-Deutschland GmbH
Kohlgartenstrasse 15
04315 Leipzig

Tel. +49 8104 8999 030
info@seppmail.de
www.seppmail.de