



SEPPmail®

SEPPmail macht Ihre E-Mails sicher - ohne Mehraufwand für den Empfänger

Der Versand von verschlüsselten E-Mails, die den hohen gesetzlichen Standards bezüglich Datenschutz genügen, war bisher ein teures und kompliziertes Unterfangen.

Für eine sichere Verschlüsselung brauchte es bisher auf beiden Seiten – also sowohl beim Versender als auch beim Empfänger – aufwendige Softwareinstallationen.

Die SEPPmail-Technologie schafft dem Abhilfe:

Der Empfänger Ihrer E-Mails benötigt zur Entschlüsselung nichts weiter als sein gewohntes E-Mail-Programm.

Durch die patentierte SEPPmail-Technologie ist auch ein Zwischenspeichern der versandten Mails – wie dies bei einem „sicheren Webmail“ der Fall ist – nicht nötig. Die Mails werden vollständig verschlüsselt an den Empfänger ausgeliefert.

Wollen Sie sich von den Vorzügen von SEPPmail selbst überzeugen?

Dann fordern Sie unter www.seppmail.ch ein Testmail an!



Facts:

- Automatische Verschlüsselung und Entschlüsselung
- Verschlüsselungsstandards: OpenPGP, S/MIME, SEPPmail und TLS
- Vollautomatische Verschlüsselung zwischen allen SEPPmails (E-Mail VPN)
- Versenden und Empfangen von E-Mails im gewohnten E-Mail Client, kein Plugin nötig
- Der Empfänger benötigt keine Software zur Entschlüsselung
- Hochverfügbarkeit (integrierter Multimaster Cluster)
- Anpassung an Security Policy durch programmierbare Rule Engine
- Optionale Verschlüsselung interner E-Mails
- Anbindung an LDAP/ADS möglich
- Optionale Viren, Spam und Phishing Protection VSPP
- Automatische Firmensignatur und Disclaimer
- Zentrale User- und Schlüsselverwaltung
- Übersichtliche Mail-Logs und Statistikfunktionen
- Geringer Administrationsaufwand
- Keine Softwareinstallation notwendig

SEPPmail 500

- Kleine Unternehmungen, bis zu 50 SEPPmail Benutzer
- Desktop Format

SEPPmail 1000

- Kleine und mittlere Unternehmungen, bis zu 1000 SEPPmail Benutzer
- 19" Rack Format

SEPPmail 3000

- Unternehmungen mit über 1000 SEPPmail Benutzer
- Hochverfügbarkeit
- 19" Rack Format

SEPPmail VM

- Virtueller Server für VMware

Virus, Spam and Phishing Protection **VSPP**



Leistungsumfang	SEPPmail 500	SEPPmail 1000	SEPPmail 3000
Abmessung (B x H x T)	275 x 44 x 180 mm	1HE 19" Rack T= 356 mm	1 HE 19" Rack T= 681 mm
Leistungsaufnahme	25 Watt	200 Watt	700 Watt/ Redundant
Netzwerkschnittstellen	3 x 10/100 MBits	2 x 10/100/1000 MBits	2 x 10/100/1000 MBits
Speicher	CF Card	Harddisk	2x SCSI Harddisk (RAID1)
Verschlüsselung	OpenPGP, S/MIME, TLS SEPPmail		
Asymmetrische Algorithmen	RSA, DSA, ElGamal, Diffie-Hellman u.a.		
Symmetrische Algorithmen	AES, 3DES, CAST5, Blowfish, Twofish u.a.		
Sprachen SEPPmail-Viewer	D, E, F, I		
Zentrale Signaturprüfung	✓	✓	✓
Domainbasierte Verschlüsselung	✓	✓	✓
Backup/Restore	✓	✓	✓
Virus, Spam, Phishing Protection	Option	Option	Option
Empfohlen max. User	50	500	unbegrenzt



Die Vorteile der patentierten SEPPmail Push-Technologie auf einen Blick

Die SEPPmail-Technologie beruht auf einem patentierten Push-Verfahren. Die E-Mails werden dabei in einem verschlüsselten HTML-Attachment an den Empfänger ausgeliefert. Um das Mail lesen zu können, braucht der Empfänger neben dem empfangenen E-Mail ein Passwort, welches ihm einmalig per SMS, Telefon oder Fax übermittelt wird. Im Vergleich zu anderen Lösungen, bei denen ein „sicheres Webmail“, „PDF-Verschlüsselung“ oder ähnliches eingesetzt wird, entstehen durch die SEPPmail-Technologie folgende Vorteile:

Two-Factor Authentication: Ein „sicheres Webmail“ ohne zusätzliche technische Sicherheitseinrichtungen wie OTP-Tokens ist in der Praxis weniger sicher als herkömmlicher, unverschlüsselter E-Mailverkehr, da es relativ einfach durch Phishing bzw. durch eine Mailspoofing – Attacke ausgehebelt werden kann. SEPPmail bietet den Komfort eines „sicheren Webmail“ mit einer Two-Factor Authentication (empfangenes E-Mail und Passwort) auch ohne zusätzliche, teure Tokens.

Clustering: Bei SEPPmail werden die gesendeten E-Mails nicht auf der Appliance gespeichert. Neben geringerem Verwaltungsaufwand und höherer Sicherheit bietet dies den Vorteil, dass eine SEPPmail-Appliance mit einem einfachen Backupfile jederzeit wiederhergestellt werden kann und dass Clustering standortunabhängig auch über langsame Verbindungen realisierbar ist.

Schutz vor Brute Force Attacken: Im Gegensatz zu anderen Systemen, welche mit verschlüsselten Anhängen arbeiten (wie z.B. PDF-Verschlüsselung) wird bei SEPPmail eine Brute Force Attacke (maschinelles Ausprobieren von Passwörtern) verhindert.

Produktion:

ZOE-One GmbH
D4 Platz 4
CH-6039 Root-Längenbold
Tel. +41 +41 455 40 50
info@seppmail.ch
www.zoe-one.com

Distribution:

Intellicomp GmbH
Theodor-Bergmann-Str. 6
63877 Sailauf
Tel. +49 +6093 / 208995
info@intellicomp.de
http://www.intellicomp.de

Autorisierter Partner: