SEPPMAIL

Eine Appliance – ein Management – drei Lösungen

- Verschlüsselung und digitale Signatur
- Managed Public Key-Infrastruktur (mPKI)
- Large File Transfer (LFT)

Herausforderungen für Kunden

Unternehmen schützen ihre Geschäftsdaten mit Firewalls, Antispam-, Antivirus- und Einmal-Passwort-Lösungen vor den Angriffen bzw. dem Zugriff Dritter. Trotzdem werden nach wie vor geschäftskritische Informationen ungesichert und offen via E-Mail versendet.

Vier Gründe, warum sich Unternehmen mit sicherer E-Mail-Kommunikation auseinandersetzen:

- **COMPLIANCE:** Firmen unterliegen gesetzlichen Verpflichtungen wie SOX, HIPAA, BASEL-II, PCI etc. Werden diese Bestimmungen nicht beachtet, besteht ein hohes Haftungsrisiko.
- **KOSTENEINSPARUNGEN:** Das Digitalisieren postalischer Prozesse kann die Kosten deutlich senken, z.B. beim Senden der monatlichen Gehaltsabrechnung oder anderer Schreiben mit persönlichen Inhalten.
- **UMFELD:** Kunden, Dienstleister und Geschäftspartner erwarten beim Austausch sensibler Daten sichere und verschlüsselte Kommunikationswege.
- **IMAGE + VERTRAUENSWÜRDIGKEIT:** Die digitale Signatur ist im Rahmen des E-Mail-Versands ein Zeichen von Qualität und zeigt dem Empfänger, dass der Absender und der Mailinhalt echt und unverändert sind. Besonders wichtig bei Unternehmen, die mit Daten Ihrer Kunden agieren, wie z.B. Steuerberater, Anwälte, Wirtschaftsprüfer usw.

Zielgruppen

Alle Unternehmen möchten sensible Daten sicher via E-Mail versenden. Die Unternehmensgrößen variieren von fünf bis zu Tausenden Mitarbeitern/Nutzern.

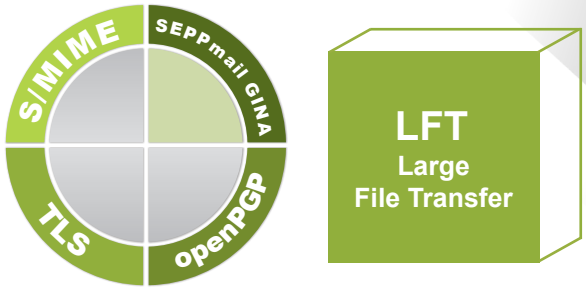
Typische Branchen, die auf eine sichere E-Mail-Kommunikation angewiesen sind

- Banken
- Versicherungen
- Industrieunternehmen mit hoher Innovationskraft
- Recht- und Steuerunternehmen
- Regierungseinrichtungen
- Gesundheitswesen

Vorteile für Unternehmen

1. Sensible Informationen, Angebote und Daten 100 % sicher aus dem Standard-E-Mail-System heraus an den Geschäftspartner versenden.
2. Übergroße Dateien können intern wie extern automatisch (Ende-zu-Ende-Verschlüsselung) ausgetauscht werden – ohne ein weiteres System mit weiteren Anmeldeprozessen.
3. Sicher mit jedem Empfänger weltweit kommunizieren – ohne nähere Kenntnis der E-Mail-Infrastruktur sowie der Sicherheitseinrichtungen des Gegenübers zu haben: mit GINA.
4. Die Möglichkeit, „vertraulich“ markierte E-Mails spontan an jedermann zu versenden, weltweit; das System verwendet automatisch die am besten für den Empfänger geeignete Verschlüsselungstechnologie (S/MIME, openPGP, Domain-Verschlüsselung, GINA).
5. Digitale Signaturen aller eingehenden Mails werden automatisch überprüft; der Public Key des Senders wird herausgezogen und gespeichert. Damit ist das System für eine gesicherte Rückantwort gerüstet und wendet diese auch automatisch an.
6. Digitale Signaturen aller ausgehenden Nachrichten erhöhen die Qualität der E-Mail-Kommunikation.
7. Die Lösung lässt sich schnell und einfach in die IT-Infrastruktur integrieren und arbeitet quasi unsichtbar für den Endnutzer. Der Empfänger erkennt an einer ungebrochenen Signatur, dass Absender und Mailinhalt echt und unverändert sind.
8. Die einfache, automatisierte und intuitive Administration entlastet die IT-Abteilung.

Top-Features im Überblick



- **Patentierte GINA-Technologie**
- **Das GINA-Portal kann via CSS (Cascade Style Sheets) an die Corporate Identity des jeweiligen Unternehmens angepasst werden.**
- **100 %ige Verschlüsselung durch Anwendung der Technologien S/MIME, openPGP und GINA**
- **Absender erhält auf Wunsch eine Lesebestätigung sobald eine GINA-Mail geöffnet wird.**
- **S/MIME-Zertifikate werden automatisch gesammelt und geprüft.**
- **Managed PKI zu Swisssign und QuoVadis Trustlink**
- **Domain-zu-Domain-Verschlüsselung ist in der Basislizenz enthalten. Damit erkennen sich alle SEPPmail-Instanzen automatisch. Somit ist eine transparente Instant-Verschlüsselung zu mehr als 3000 Domainen im Raum DACH ohne Mehrkosten möglich.**
- **Multidomain- und Mandantenfähigkeit**
- **Ein-Klick-Update**
- **Erstellen einer eigenen Signatur (Impressum)**
- **Einfache Anpassung der Ruleset Engine für firmenspezifische Regeln in Bezug auf verschlüsselte E-Mails**
- **Clustering ist in der Basislizenz enthalten (Hochverfügbarkeit und Load Balance).**
- **Automatische Schlüsselerstellung (S/MIME & openPGP)**

SEPPMAIL

Eine Appliance – ein Management – drei Lösungen

- Verschlüsselung und digitale Signatur
- Managed Public Key-Infrastruktur (mPKI)
- Large File Transfer (LFT)

10 Gründe für SEPPmail

- Patentierte Methode (GINA) zur sicheren und einfachen Kommunikation mit jedem Empfänger. Fehleranfällige Technologien wie PDF und ZIP sind nicht notwendig. Der Empfänger benötigt lediglich einen E-Mail-Client, eine Verbindung zum Internet und einen Browser, um die Mail zu erhalten, zu entschlüsseln und zu antworten.
- Verschlüsselte E-Mails und deren Anhänge werden immer zu 100 % ausgeliefert. Die eigenen Appliance-Ressourcen bleiben stabil und wachsen nicht an (Backup, Festplattenbedarf). Backups bewegen sich im Umfang weniger Megabytes.
- Hinzufügen verschiedener Standardsignaturen (Impressum) in ausgehende E-Mails für verschiedene Domain-Adressen sowie die jeweiligen Länder.
- Es ist möglich, für jede versendete vertrauliche E-Mail eine Lesebestätigung anzufordern, die vom Empfänger nicht weggeklickt werden kann. Die Lesebestätigung erhält der Absender der verschlüsselten GINA-Mail.
- Das GINA-Portal ermöglicht externen Empfängern die Auswahl, welche Technologie sie zur weiteren sicheren Kommunikation einsetzen möchten. Der Empfänger verwaltet seine Security-Daten selbst: Er lädt seinen Public Key (S/MIME, openPGP) hoch. Diese Keys werden bei der nächsten Kommunikation mit ihm sofort angewendet. Durch die vorgängige GINA-Authentifizierung ist keine weitere Prüfung des eingelieferten Schlüsselmaterials notwendig. Zusätzlich ist es möglich, das Passwort zu ersetzen oder zu erneuern. Der Empfänger kann auch Keys des Absenders für die sichere Kommunikation verwenden.
- GINA-Mails können von allen Mobilgeräten empfangen werden – Blackberry 10 und Windows Phone ohne Limitierung, iOS mit einer kostenlosen App und Android via Firefox Browser.
- Schlankes, hoch standardisiertes “out of the box”-Produkt, das sich schnell integrieren und intuitiv anwenden lässt.
- Einfache Administration mit übersichtlichen Menüs und Funktionen, z.B. einem Ein-Klick-Upgrade auf die neue Version, einem Managed PKI (Public-Key-Infrastructure)-Connector zu renommierten CAs (Certificate Authorities) oder einer automatischen Lizenzvergabe.
- Managed Domain-Verschlüsselung und TLS (Transport Layer Security) sind in der Basisversion enthalten. “Managed Domain” bedeutet, dass sich die weltweit eingesetzten SEPPmail-Appliances untereinander erkennen und der komplette Traffic dazwischen verschlüsselt abläuft.

- Die SEPPmail-Lösung kann mit dem Feature „Large File Transfer“ ergänzt werden und ist als Standalone-Produkt oder als Erweiterung eines existierenden SEPPmail-Systems erhältlich.

Überblick der SEPPmail-Lösungen

Basis

Basissystem inkl. Basislizenz für TLS und Domain-Verschlüsselung

Hardware-Appliance
4 Modelle: 500B (bis 50 User); 1000B (bis 500 User); 3500B (bis 7500 User) und 5000B (unlimitiert)

Virtuelle Appliance
(VMware, Hyper-V und Red Hat Hypervisor)

Lösungen

Verschlüsselungslösung

Signatur und Verschlüsselung
für S/MIME, openPGP und GINA, TLS, Domain-Verschlüsselung

LFT-Lösung

Large File Transfer
zum Austausch von übergroßen Dateien auf Basis der GINA-Technologie

Module

Modul

Self Service-Passwortmanagement
als Ergänzung zur GINA-Verschlüsselung

Modul

Interne Mailverschlüsselung (IME)
interne Ende-zu-Ende-Verschlüsselung für Outlook/Exchange

Modul

Protection Pack
Antivirus(AV)-/Antispam(AS)-Module auf Basis von Clam Antivirus und Spam Assassin (jährlicher Betrag)

Preis- und Lizenzinformationen

Appliances Lösungen Module

Hardware/VM Maintenance	renewal
SEPPmail Hardware/VM Appliance	initial
Software Maintenance	renewal
SEPPmail Secure E-Mail User (inkl. App/Plugin) SEPPmail LFT User	initial
Protection Service (AV/AS)	renewal
SEPPmail-Modul (SSPM/IME)	initial

Kontakt

SEPPmail Deutschland GmbH
Ringstraße 1c
D-85649 Brunnthal b. München
Tel: 08104 88 89 25
E-Mail: info@seppmail.de
www.seppmail.de

Reseller K3 Innovationen GmbH
Hohenzollernstr. 66-68
D-52351 Düren
Tel: 02421 50 59 90
contact@k3-innovationen.de
www.k3-innovationen.de
www.emailverschluesselung.com