Secure Email mit SEPPmail

Stefan Burkhardt | IT Consultant
klopfer datennetzwerk gmbh
22.11.2018

Agenda

- Sichere Email im Trend
- Wer ist SEPPmail?
- Bereitstellung
- Email-Signatur, Zertifikate und mPKI
- Verschlüsselung
- Demo

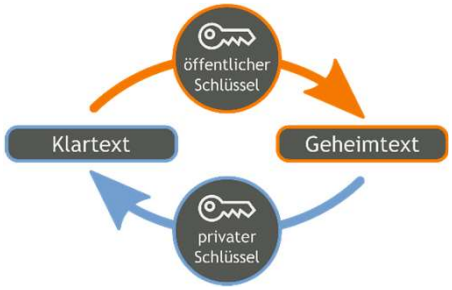
- Alle Unternehmen, die sicher Daten via E-Mail versenden möchten
  - größenunabhängig
  - branchenunabhängig

Warum Secure Email?

Compliance	Einhaltung gesetzlicher Bestimmungen, regulatorischer Standards und freiwilliger Richtlinien Haftbarkeit des Managements bei Nichtbeachtung
Kosteneinsparung	Digitalisierung bestehender Geschäftsprozesse (Integration von ERP- / Lohnsysteme) Modernisierung bestehender, „alter“ Technologie
Umfeld	Lieferanten bzw. Kunden führen Secure E-Mail Lösungen ein Kunden erwarten in Projekten verschlüsselte Kommunikation
Image	Signatur in E-Mail ist Zeichen für Qualität im E-Mail-Verkehr Schutz vor Datenspionage/-manipulation hat hohe Priorität im Geschäftsverkehr

- Wettbewerbsvorteile durch Signatur / Verschlüsselung
  - Wertvolle Informationen, die für den Geschäftserfolg entscheidend sind, werden geschützt
  - Schutz vor Phishing-, Man in the Middle- und sonstigen E-Mail-Attacken
  - Geschäftspartner verlangen verschlüsselte Kommunikation
  - Kriterium bei Ausschreibungen
  - keine Pflicht, betroffene Person im Falle einer Datenschutzverletzung zu informieren; Art. 34 Abs. 3a

Exkurs Verschlüsselung



Austausch über Email mit Signatur

Absender verschlüsselt Mail mit öffentlichem Schlüssel des Empfängers

- Hohe Benutzerfreundlichkeit
- Einfache Administration
- Einfachste Integration / kurze Einführungszeit
- Kompatibel mit anderen Technologien und Anbietern
- Unterstützung aller Standardtechnologien
  - S/MIME
  - openPGP
  - Domainverschlüsselung
  - TLS
- Einfache Möglichkeit der Spontankommunikation

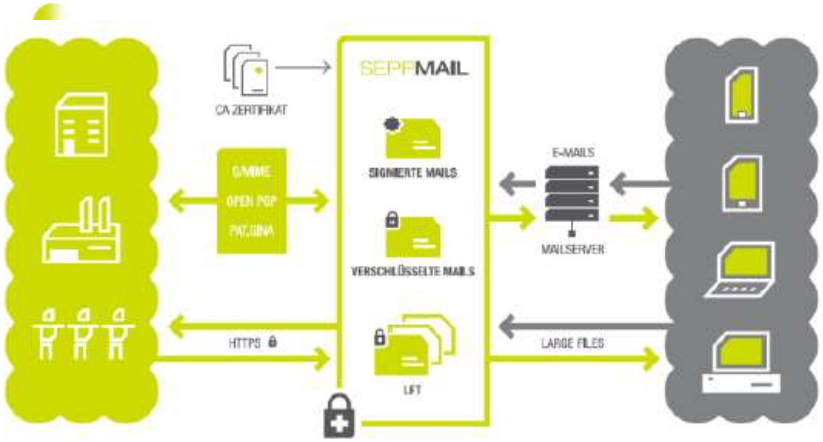
Wer ist SEPPmail?

- Entwicklung von Secure Email-Lösungen
- SEPPmail AG in Neuenhof bei Zürich
- SEPPmail - Deutschland GmbH in Brunnthal
- SEPPmail - Deutschland Entwicklungscenter in Leipzig
- über 17 Jahre Erfahrung mit Secure E-Mail Technologien
- Firma zu 100% eigenfinanziert (keine Investoren)
- Kunden und Partner in ganz Europa

SEPPmail Portfolio

Digitale Signatur und mPKI

Secure E-Mail Gateway



Large File Transfer

Zentrales Disclaimer Management

- Produktvarianten:

Secure E-Mail Gateway 500B

- Bis 50 User
- Desktop Format
- Solid State Disk
- clusterfähig / kaskadierbar

Secure E-Mail Gateway 1000B

- Bis 500 User
- 19" Rack Format / 1 HE
- Integrierte Festplatte
- clusterfähig / kaskadierbar

Secure E-Mail Gateway 3500B

- Bis 5000 User
- 19" Rack Format / 1 HE
- Redundante HD und Netzteile
- clusterfähig / kaskadierbar

Secure E-Mail Gateway 5000B

- Ab 5000 User
- 19" Rack Format / 2 HE
- Redundante HD und Netzteile
- clusterfähig / kaskadierbar

- auch als virtuelle Appliance für VMware und HyperV

Zielsetzung

E-Mail-Signatur:

- ✓ Integrität
- ✓ Authentizität
- ✓ Verbreitung des öffentlichen Schlüssels
- ✓ Anscheinsbeweis vor Gericht

E-Mail-Verschlüsselung:

- ✓ Vertraulichkeit des E-Mail-Inhaltes

Zertifikate

SSL/TLS-Zertifikate

Sichere Kommunikation zwischen Internetbenutzern und Webportalen

Zwingend erforderlich für die Spontankommunikation über SEPPmail GINA

Bezeugen die Echtheit des Webauftritts durch Überprüfung der Domäne und weiterer Unternehmensinformationen

Schützen vor Phishing und Man-in-the-Middle Angriffen

Persönliche E-Mail-Zertifikate

Signieren und verschlüsseln von E-Mails

Fortgeschrittene Signatur für Dokumente

E-Mail / Dokument wurde nicht verändert während des Transportes und stammt von der benannten E-Mail-Adresse

- bietet eine vollständige Certification Authority (CA), welche als Self-Signed-, aber auch Sub-CA genutzt werden kann
- verwaltet Schlüssel bzw. Zertifikate der Benutzer zentral im System
- E-Mail Zertifikate können von beliebigen CAs eingespielt werden
- über Konnektoren können weltweite CA angeschlossen werden
- automatischer Schlüsselbezug und sichere Ablage auf Appliance

- alle Konnektoren sind ohne Mehrkosten in der Basislizenz verfügbar.
- Unternehmensprüfung erfolgt einmalig beim Setup der mPKI-Schnittstelle
- Bezug, Verwaltung und Erneuerung der E-Mail Zertifikate erfolgt vollautomatisch über den Konnektor der Appliance
- Zertifikate ohne Konnektoren können importiert und zur zentralen Signatur von E-Mails herangezogen werden

mPKI Konnektoren

swiss sign TRUSTED IDENTITY

WISeKey | QuoVadis

GlobalSign GMO Internet Group

digicert

DFN Deutsches Forschungsnetz

in Vorbereitung:

A-TRUST

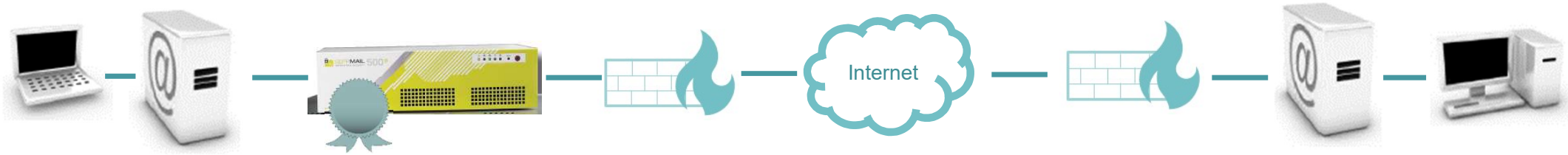
Entrust Securing Digital Identities & Information

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

Mail-Fluss Eingang

Interner Empfänger

Externer Sender



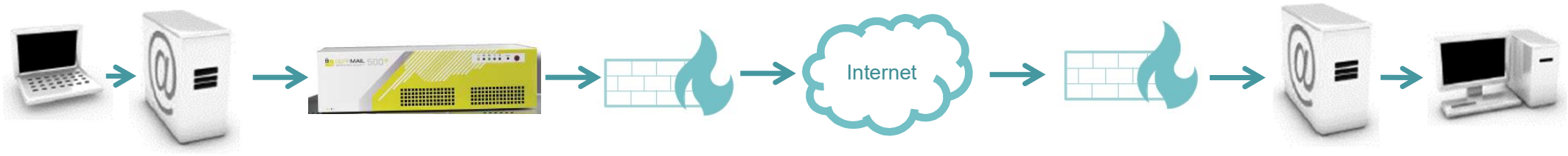
Herauslösen und Ablage
PublicKey aus Signatur

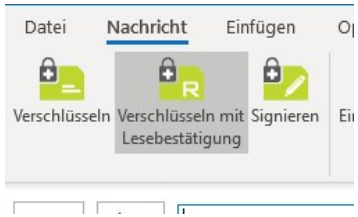
signierte Email

Verschlüsselung

Interner Sender

Externer Sender





Senden
(Addin oder Kenn-zeichen im Betreff)

Prüfen, ob …
- S/MIME
- OpenPGP

für Empfänger vorhanden, sonst

GINA-Technologie

Empfänger erhält eine Trägermail mit einem html-Container. (vollständig ausgeliefert)

Login auf Webmailer für Lesen und Beantworten der Mail

Live Demo

SEPPMAIL