# Sichere E-Mail Kommunikation mit SEPPmail

Günter Esch, Country Manager SEPPmail AG

SEPPMAIL
SWISS E-MAIL SECURITY

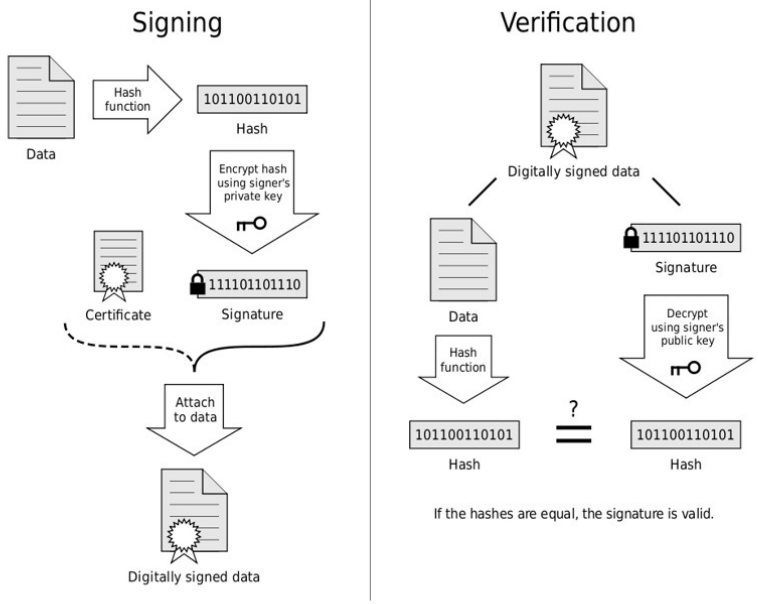
# E-Mail Signatur: Zweck und Nutzen
# E-Mail Verschlüsselung: Die Königsdisziplin
# Large File Management: Überraschung !!

SEPPMAIL
SWISS E-MAIL SECURITY

# E-Mail Signatur: Zweck und Nutzen

## E-Mail Signatur mit Benutzerzertifikat

- Unveränderlichkeit der elektronischen Nachricht
- Verbreitung des eigenen Public Keys
- Echtheitsbestätigung des Absenders bzw des versendenden Unternehmens.
- Unabstreitbarkeit (Beweismittel)




Quelle: http://de.wikipedia.org/wiki/Digitale_Signatur

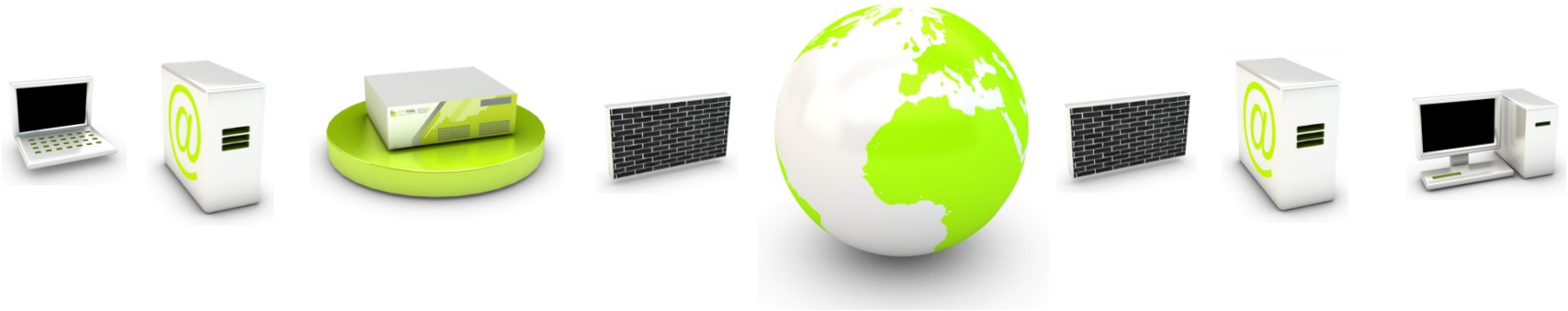


SEPPMAIL
SWISS E-MAIL SECURITY

# 5 Technologien – S/MIME

Interner Empfänger

Externer Sender

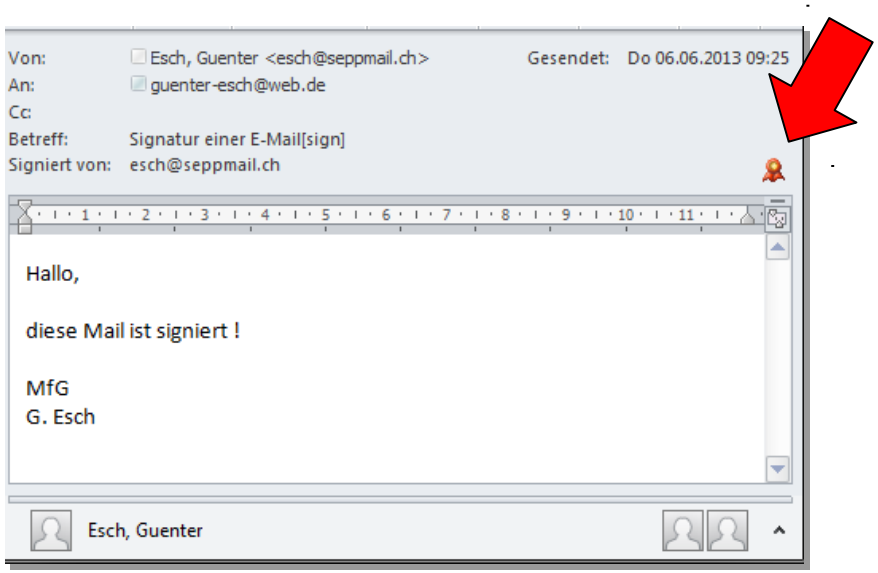


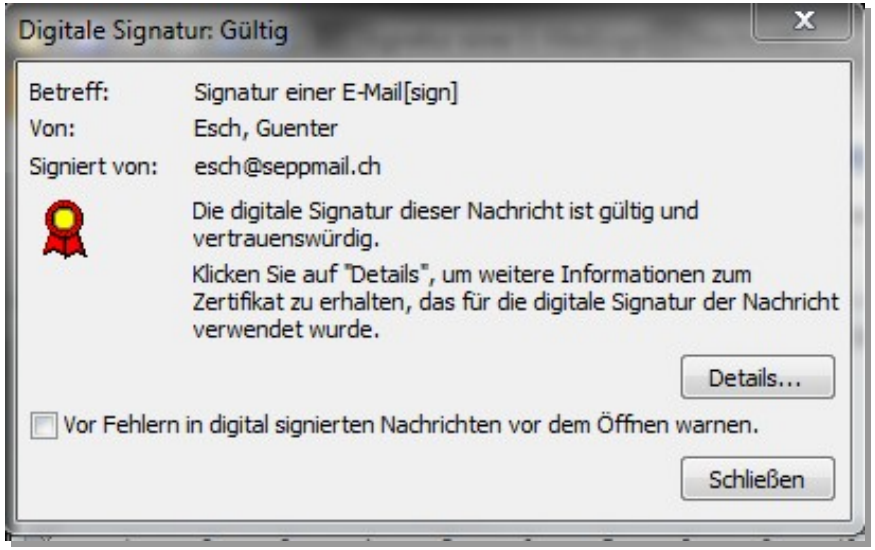
S/MIME

Alle public key‘s werden automatisch aus den Signaturen gesammelt, und bei Bedarf zur Verschlüsselung an den Sender herangezogen. Entlastung des Systemadministrators !

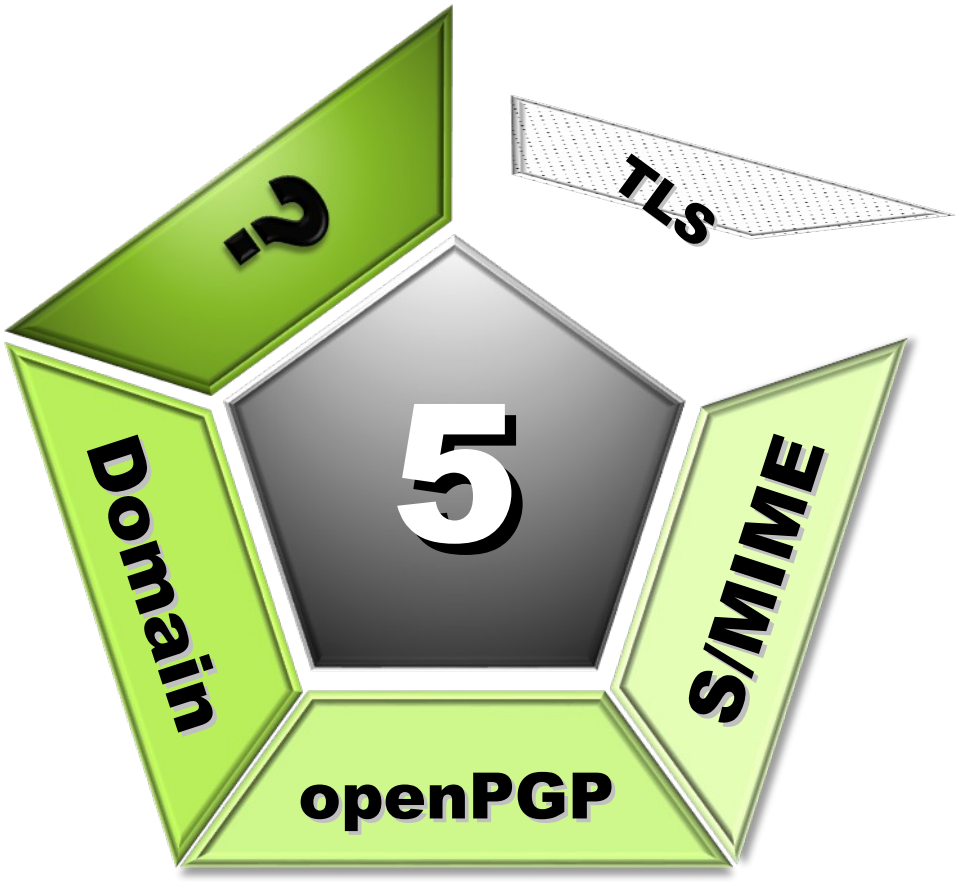
# 5 Technologien – S/MIME

## Automatische Signatur im Namen des Senders am Gateway

# Eine Hand voll Technologien zum Verschlüsseln






SEPPMAIL
SWISS E-MAIL SECURITY

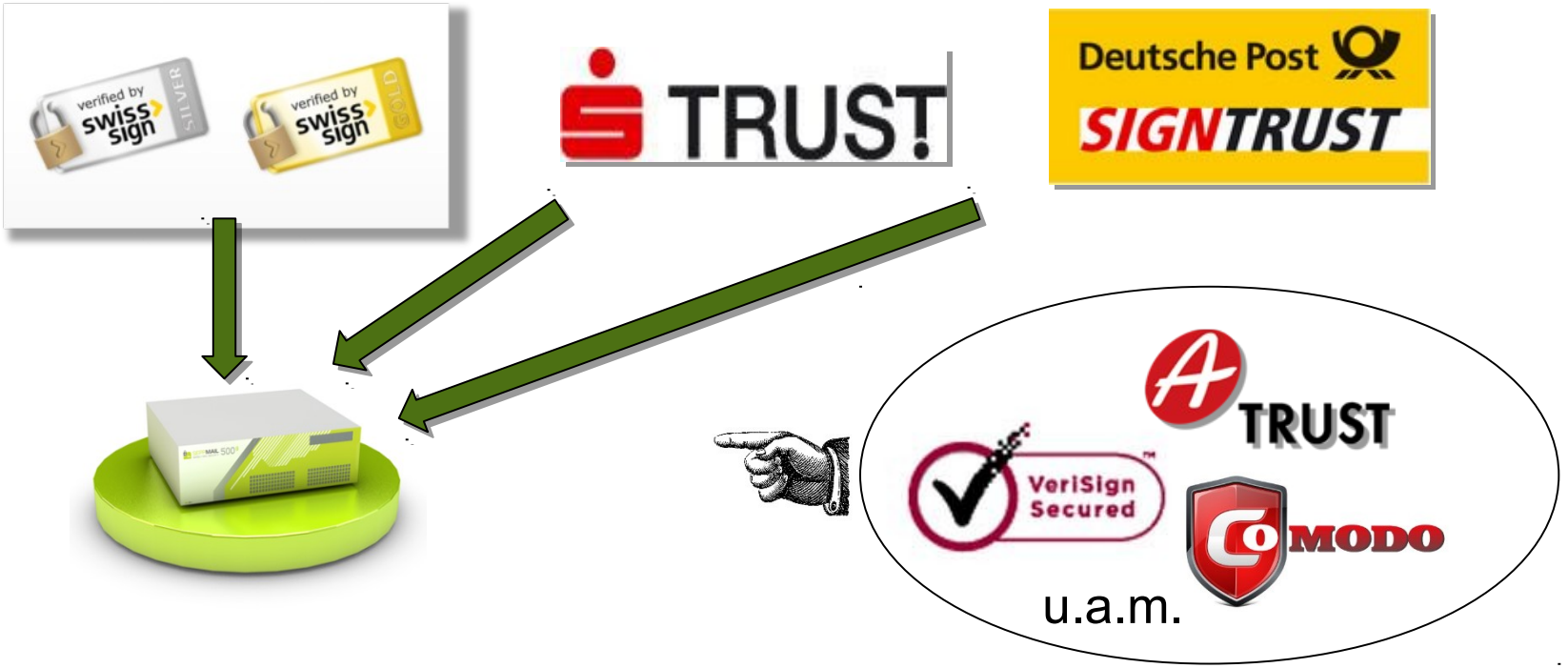
# S/MIME (Secure Multipurpose Internet Mail Extensions)


- **X.509 Zertifikate sollten von einer offiziell anerkannten CA ausgestellt werden, dann funktioniert auch die automatisierte Prüfung einer Signatur.**

- **Funktionalität integriert in den meisten Mail Clients (Outlook, Outlook Express, Netscape,…)**
- **Unterbindet MiM und Phishing Attacken, wenn der Empfänger entsprechend sensibilisiert ist.**

# 5 Technologien – S/MIME

## SEPPmail managed PKI – Konnektor in Basislizenz enthalten




Zusätzliche Kosten durch Einrichtungsgebühr pro Domäne und jährliche Zertifikatskosten sind zu berücksichtigen.
Bezug über Partner oder direkt beim CA



SEPPMAIL
SWISS E-MAIL SECURITY

# openPGP (Pretty Good Privacy)

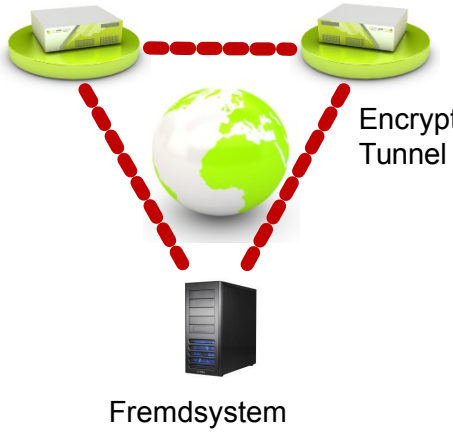

- **OpenPGP ermöglicht die volle Kompatibilität zu bestehenden Systemen !**
- **Zertifikate werden selbst ausgestellt und in einem „Web of Trust“ verteilt**
- **Entwickelt von Phil Zimmermann (erste Version 1991 )**
- **Gekauft von Network Associates Inc. 1997**
- **Windows, Unix, Mac: PGP, GnuPG**
- **Sowohl OpenSource (GnuPG, WinPT) als auch kommerzielle Versionen (PGP) erhältlich**

# Nachteile der openPGP Technologie


- Es muß immer eine zusätzliche Software installiert werden (die meistens recht schwierig zu bedienen ist)
- Der Standard ist schlecht dokumentiert, es muss mit Kompatibilitätsproblemen gerechnet werden (z.B. Sonderzeichen etc.)
- openPGP Keys können nicht automatisiert geprüft werden (kein hierarchisches Modell wie S/MIME).
- Keys werden NICHT mit der Signatur verbreitet wie bei S/MIME. Ein automatisiertes Lernen ist nicht möglich.

# 5 Technologien - Domainverschlüsselung

SEPPmail Managed Domain Service
Domainverschlüsselung zu Fremdsysteme





- **Vollautomatische Verschlüsselung des gesamten Mailverkehrs von Domaine zu Domaine**
- **Alle SEPPmail Appliances kennen sich (SEPPmail Managed Domain Service)**
- **Wird erreicht indem der Public Key beider Maschinen ausgetauscht wird**
- **Ist bei SEPPmail in der Basislizenz enthalten**



SEPPMAIL
SWISS E-MAIL SECURITY

# 5 Technologien - TLS

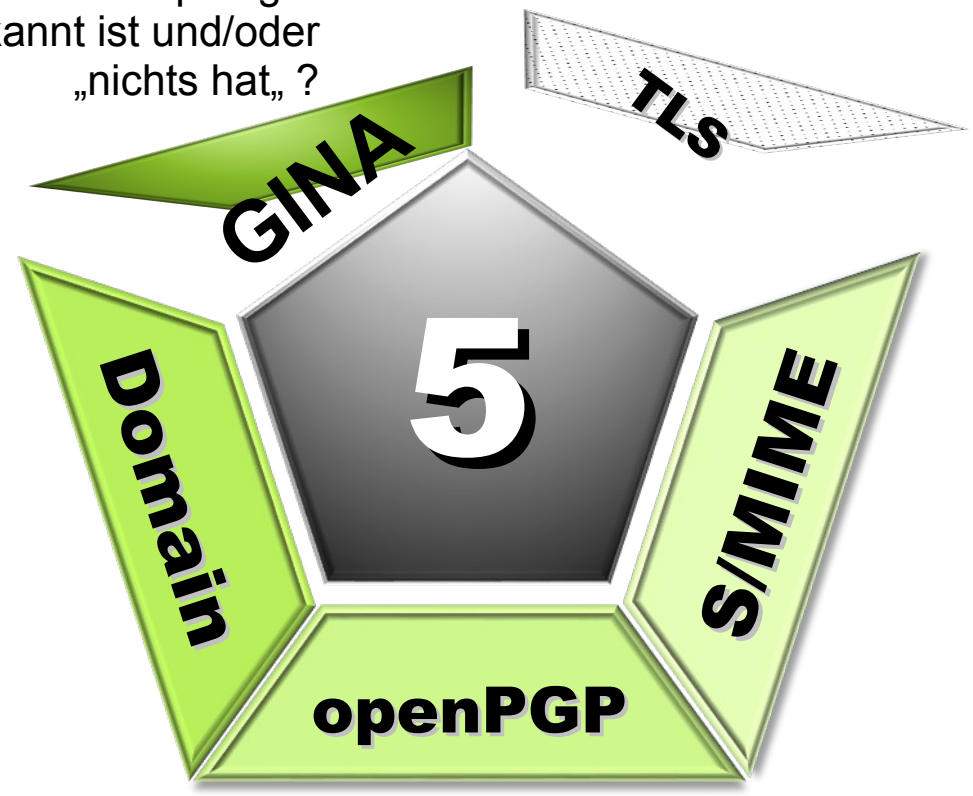
## TLS (Transport Layer Security)


- „Punkt-zu-Punkt“ Verbindung zwischen Mailservern
- Leitungsverschlüsselung only !
- Vergleichbar mit einem „https für Mailserver“
- Geeignet für einzelne Verbindungen
- Hoher Verwaltungsaufwand

# Eine Hand voll Technologien zum Verschlüsseln

Patentierte Primärtechnologie

Was tun, wenn Empfänger unbekannt ist und/oder „nichts hat„ ?





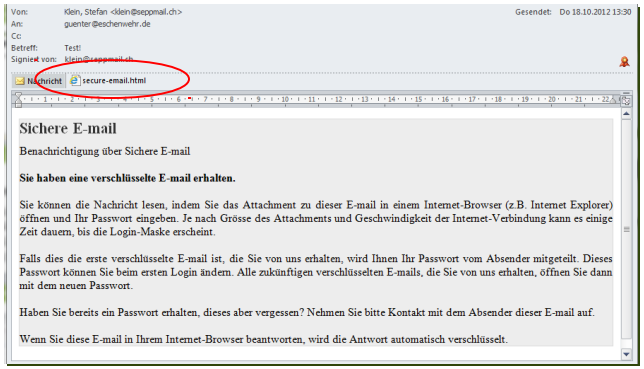

SEPPMAIL
SWISS E-MAIL SECURITY

# Der GINA Vorgang


**Schritt 1: Schreiben und Empfangen**:

•Der Sender verfaßt in seinem Standard E-Mail Client eine vertrauliche Mail und markiert diese entweder mit dem „Vertaulichkeits-Flag“, vermerkt im Betreff zB „[vertraulich]“, oder er verwendet das kostenlose Plugin von SEPPmail.


- Der Empfänger erhält eine Standardnachricht mit Erklärung und einem html-Attachment (rot markiert) welches die vollständig ausgelieferte verschlüsselte Nachricht beinhaltet (b). Parallel dazu empfängt er ein Initialpasswort als SMS. Die Mobiltelefonnummer erhält das System via Rückfrage E-Mail vom Sender, oder dieser liefert die Nummer schon in der Betreffzeile mit.






SEPPMAIL
SWISS E-MAIL SECURITY

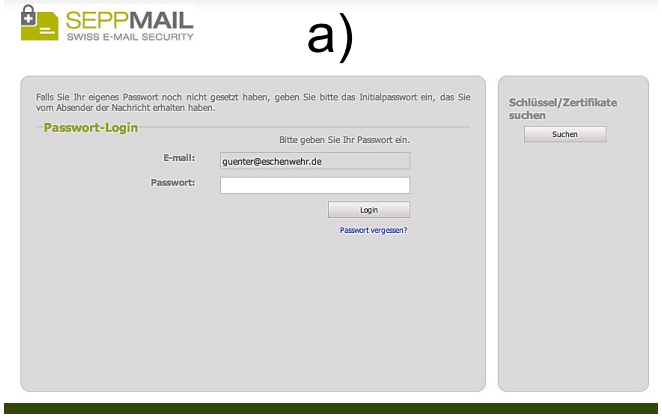
# Der GINA Vorgang


Entschlüsselungsvorgang findet im Hintergrund statt: siehe nächste Folie

**Schritt 2: Anmelden und Lesen**

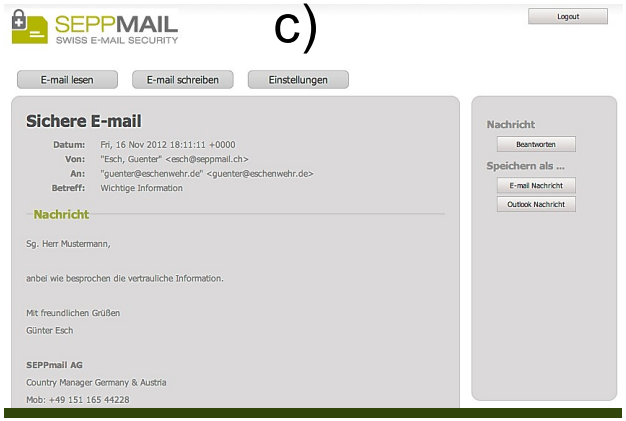
•Der Empfänger öffnet das html-Attachment und wird zur Eingabe seines Initialpasswortes aufgefordert (a) .
•Anschließend muß er sich **einmalig** am System registrieren und sein eigenes Passwort vergeben. Sowie optional für die automatisierte Passwortrücksetzung eine Sicherheitsfrage + Antwort festlegen (b).
•Danach ist die entschlüsselte E-Mail im Webmailer sichtbar (c). Aus diesem kann verschlüsselt geantwortet, die Mails als Klartext ins System gespeichert werden, eigene Key‘s hochgeladen oder seine Einstellungen verändert werden.

a)




b)


c)






SEPPMAIL
SWISS E-MAIL SECURITY

# Der GINA Entschlüsselungsvorgang


via https Strecke wird die verschlüsselte E-Mail beim Anmeldeprozess des Empfängers zum Entschlüsseln temporär an die SEPPmail Appliance gesendet

via https Strecke wird die entschlüsselte E-Mail zum Empfänger ausgeliefert und verschwindet von der SEPPmail Appliance.

**Vorteile des patentierten GINA Verfahrens:**

•Keine zusätzlichen Technologielayer bzw. Konvertierung in pdf, zip oder exe notwendig, da diese nur zusätzliche Komplexität und Fehlermöglichkeiten verursachen.
•Empfänger benötigt nur Mailclient, Browser und Internetzugang. Keinen pdf-Reader, oder sonstige Verschlüsselungsclients am Empfängersystem.
•Wird vom Sender eine **Lesebestätigung** gewünscht, wird diese von der Appliance in dem Augenblick versendet, wenn die Mail zur Entschlüsselung eingeliefert wird.
•Das Zugriffspasswort kann jederzeit vom Empfänger geändert werden.
•Spontane sichere Kommunikation in beide Richtungen möglich

- Die E-Mails werden vollständig an Empfänger ausgeliefert, somit werden auf der SEPPmail nur Anmeldedaten und Keys gespeichert. (Sender fällt nicht in das Telekommunikationsgesetz, was der Fall wäre, wenn E-Mails für Andere länger als 14 Tage gespeichert werden).
- Die GINA Oberfläche und alle Texte können 100% per CSS-Stylesheet verändert werden.
- Empfänger können sich auch am Portal vorgängig anmelden und so Ihre bevorzugte Verschlüsselungsform (Passwort oder Zertifikatskey) wählen



SEPPMAIL
SWISS E-MAIL SECURITY

# SEPPmail Demo

# Lösungsansätze am Markt im Vergleich

SEPPMAIL
SWISS E-MAIL SECURITY

# Lösungsansätze Secure E-Mail „für alle“

**Mitbewerb - Ansatz 1:**

**Generierung selbstextrahierender Dateien mit Passwortschutz ( .exe)**

- Werden von den meisten Firewalls geblockt (ausführbare Dateien)
- Falls nicht geblockt: Ideal zum Verbreiten von Viren
- Brute-force Attacke auf Attachment möglich (nur Passwortschutz)
- Setzt bestimmtes Betriebssystem auf Empfängerseite voraus

# Lösungsansätze Secure E-Mail „für alle“

## Mitbewerb - Ansatz 2:

## Passwortgeschützte PDF – Dateien ( .pdf )

- Ist ein (bei SEPPmail nicht notwendiger) zusätzlicher Technologielayer der so seine Tücken hat :
  - -Die Signatur des Absenders wird zerstört
  - -Abhängigkeit von der PDF–Reader – Version des Empfängers
  - -Brute-force Attacke auf Passwort möglich
  - -Schlechter Ruf von PDF-Sicherheit (entsprechende Tools sind im Internet verfügbar) Formatierungsprobleme bei der Umwandlung der E-Mail in ein PDF
  - -Der normale „Mailverlauf“ wird gestört – sichere Antwort ist nur auf Umwegen möglich und in der Praxis nicht durchsetzbar
- Es ist nur das zur PDF-Erstellung verwendete Passwort gültig und nicht veränderbar !

  Somit muß eine Passworthistorie mitgeführt werden !

# Lösungsansätze Secure E-Mail „für alle“

**Mitbewerb - Ansatz 3:**

**Versenden eines Verschlüsselungsclients (Software)**
zB: (PGP – Satelit Client)

- Nicht alle Empfänger können/dürfen Programme installieren
- Proprietär
- Funktioniert nicht mit allen Clients
- Keine „spontane“ Kommunikation möglich

# Lösungsansätze Secure E-Mail „für alle“

**Mitbewerb - Ansatz 4:**

**Ausstellen von Zertifikaten für externe Benutzer**

- Erlaubt eine relativ transparente Kommunikation mit beliebigen Partnern
- **Erzeugt aber einen hohen Supportaufwand für den Sender da dieser zu einer CA wird**
- Erfahrung zeigt: Empfänger sind nicht bereit für den Einsatz von S/MIME – Zertifikaten
- Verlust von Zertifikaten führt zu Unmut bei den Empfängern

# Lösungsansätze Secure E-Mail „für alle“

**Mitbewerb - Ansatz 5:**

**„sicheres Webmail“ : Mails werden am Server zurückgehalten und nur ein Link dazu versendet:** (PGP Web-Messenger)

- Storage-Bedarf wächst ständig.
- Speicherung der gesamten, als wichtig eingestuften Kommunikation an einem Ort - beim Absender!
- Backup und Sicherung notwendig !
- Ist durch Mailspoofing bzw. Phishing einfach kompromittierbar!

# SEPPmail Produktepräsentation

## Leistungsübersicht


### SEPPmail Key Points

- Gateway Lösung, problemlose Integration in bestehende Infrastruktur
- Out-of-the Box Lösung
- Als Hardware oder VM erhältlich
- Revisionskonforme Secure E-Mail Kommunikation
- Unterstützt alle wichtigen Standards
- Langfristige Investitionssicherheit
- Nutzenorientiertes Lizenzsystem
- Basiert auf 10 Jahren Erfahrung
- Skalierbar und clusterfähig



SEPPMAIL
SWISS E-MAIL SECURITY

# SEPPmail Kunden

## Referenzen (Auszug)

- Helvetia Versicherung (CH)
- Schweizeriche Bankiervereinigung (CH)
- Swiss Life (CH)
- Hubert & Suhner (CH)

- www.hin.ch
- 175.000 User nutzt HIN netzwerk täglich

- SVG Bundeszentralgenossenschaft (Frankfurt)
- FC Bayern München (München)
- Helaba Invest Frankfurt (D)
- Kunst- und Ausstellungshaus (Bonn)
- RZ LOGIS – Banken (A)
- Allg. Rechenzentrum ARZ – Banken (A)
- Noerr Gruppe (München)
- Hellmann Logistik (Osnabrück)
- TÜV-Saarland
- Klinikum Wolfsburg (D)

- **u.v.m.**

Lufthansa Systems



SEPPMAIL
SWISS E-MAIL SECURITY

# Unternehmen SEPPmail AG

Stefan Klein CEO

- Hauptsitz in Neuenhof bei Zürich
- Entwicklung von Secure E-Mail Lösungen
- 14 Jahre Erfahrung mit Secure E-Mail Technologien
- Firma zu 100% eigenfinanziert (keine Investoren)
- Kunden und Vertriebspartner in ganz Europa (2-stufiges Vertriebsmodel)



SEPPMAIL
SWISS E-MAIL SECURITY

# E N D E