



K I E L , 2 5 . 0 6 . 2 0 2 4



&





# SEPPMAIL

Secur|Ty  
made  
in  
Germany

Trust Seal  
[www.teletrust.de/itsmig](http://www.teletrust.de/itsmig)

Secur|Ty  
made  
in  
EU

Trust Seal  
[www.teletrust.de/itsmie](http://www.teletrust.de/itsmie)

# M365 E-Mail-Kommunikation ist EU-DS-GVO-konform! Sind Sie sicher?

SEPPmail: DIE Erweiterung für den Microsoft365-Schutz

STEPHAN HEIMEL, LL.M.

Prokurist – Sales Director

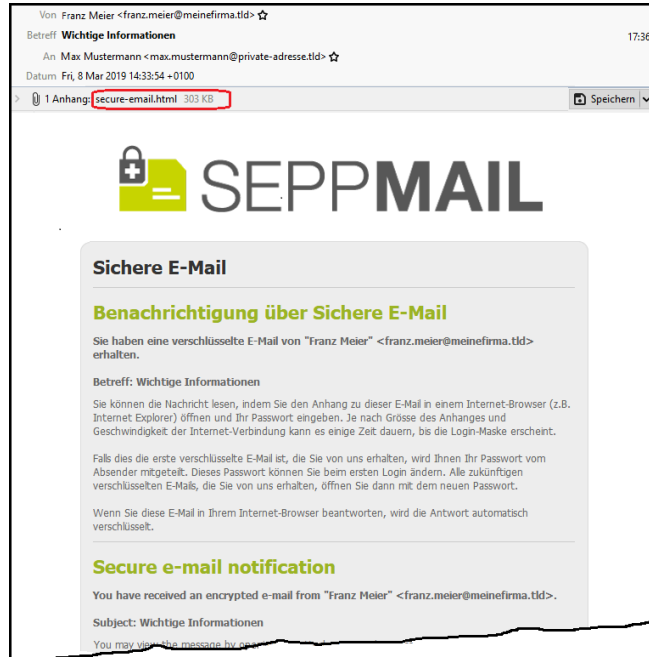
SEPPmail - Deutschland GmbH | Stephan Heibel  
Disclaimer:

Soweit dieser Vortrag juristische Erläuterungen und Ratgeber enthält, so stellen diese unverbindliche Informationen ohne jede Gewähr für Vollständigkeit und Richtigkeit dar. Es handelt sich insoweit nicht um Rechtsberatung und der Referent erhebt auch keinesfalls den Anspruch, eine solche darzustellen oder gar zu ersetzen.

# VORAB ...

- weder Freibrief noch Verbot
  - DSK-Anwendungshinweise
    - Keine Firma kann bei Abschluss eines Vertrages mit Microsoft über M365 davon ausgehen, dass personenbezogene Daten in den Produkten von M 365 grundsätzlich datenschutzkonform verarbeitet werden.
    - Auch der Datenschutznachtrag von Microsoft vom September 2022 reicht nicht.
    - Der Verantwortliche in den Firmen muss sich selbst kümmern, dass Microsoft 365 datenschutzkonform eingesetzt wird.
    - Restrisiko bleibt und realisiert sich beim Anwender
  - US-EU-Data Privacy Framework
    - <https://www.it-finanzmagazin.de/fisa-702-vs-trans-atlantic-data-privacy-framework-ist-das-alles-nur-alter-wein-in-neuen-schlaeuchen-164667/>
  - M365 Bordmittel für die Verschlüsselung
    - TLS (default opportunistisch oder forced)
    - <https://netzpalaver.de/2023/09/26/e-mails-ueber-tls-verschluesseln-die-unangenehme-wahrheit/>
    - S/MIME (Zertifikat am Client)

# 23 JAHRE SEPPMAIL



- ✓ Hohe Benutzerfreundlichkeit
- ✓ Einfache Administration - unser Anspruch ist, (fast) unsichtbar zu werden.
- ✓ Einfachste Integration / kurze Einführungszeit
- ✓ Kompatibel mit anderen Technologien und Anbietern
- ✓ Unterstützung aller Standardtechnologien
  - S/MIME
  - openPGP
  - Domainverschlüsselung
  - TLS
- ✓ Einfache Möglichkeit der Spontankommunikation (kein pdf, kein Webportal) mit der ursprünglich von SEPPmail patentierten **GINA-Technologie**



# DAS 100% - VERSPRECHEN

- ✓ ALLE als vertraulich gekennzeichnete E-Mails werden verschlüsselt versendet
- ✓ JEDER Empfänger kann darauf verschlüsselt antworten

Egal,

- ob der Empfänger über eine Verschlüsselungslösung verfügt oder nicht,
- ob der Empfänger MS-Nutzer ist oder nicht

Voraussetzungen beim Empfänger:

- Datenendgerät
- E-Mail-Client
- Internetzugang und -browser

Kein Agent, kein pdf-Reader, kein «Entzipper,» ...



# AGENDA

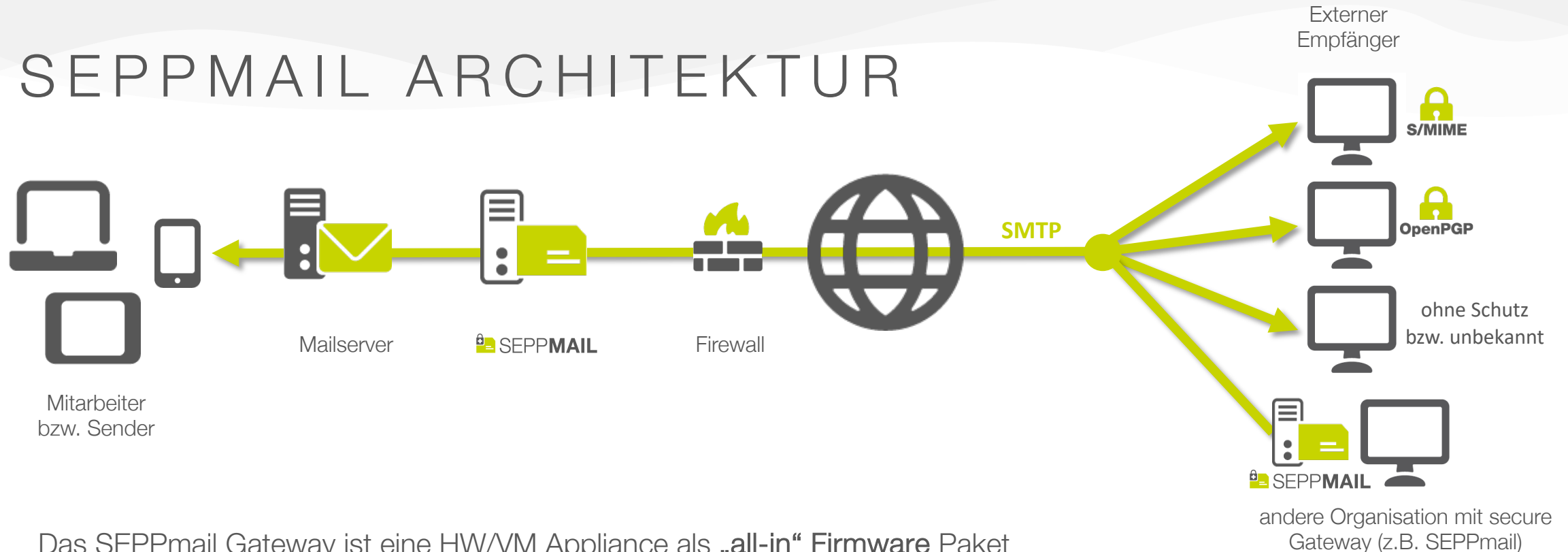
- ✓ Architektur und Funktionen
  - ✓ E-Mail Signatur, Zertifikate und mPKI
  - ✓ Verschlüsselung
  - ✓ Large File Transfer – sicherer Austausch übergroßer Daten
  - ✓ Zentrales Disclaimer – Management
- ✓ Betriebsmodelle
  - ✓ On Premises
  - ✓ Cloud
- ✓ Unternehmen, Kunden



SecurITy  
made  
in  
Germany

Trust Seal  
[www.teletrust.de/itsmig](http://www.teletrust.de/itsmig)

# SEPPMAIL ARCHITEKTUR



Das SEPPmail Gateway ist eine HW/VM Appliance als „all-in“ Firmware Paket

- ✓ beinhaltet OS: openBSD
- ✓ verfügbare VMs sind ESX, Hyper-V, Hyper-Visor, KVM oder Azure
- ✓ zentralisierter Download-, Update- und Lizenz-Server
- ✓ als Cloud-Lösung erhältlich
- ✓ M365 und Exchange-online fähig

# 5 LÖSUNGEN – 1 MANAGEMENT



Secure E-Mail Gateway

Filter



Digitale Signatur und mPKI



Large File Transfer



Zentrales Disclaimer Management

# BEGRIFFSBESTIMMUNG



## Digitale E-Mail-Signatur:

- ✓ Integrität
- ✓ Authentizität
- ✓ Verbreitung des öffentlichen Schlüssels



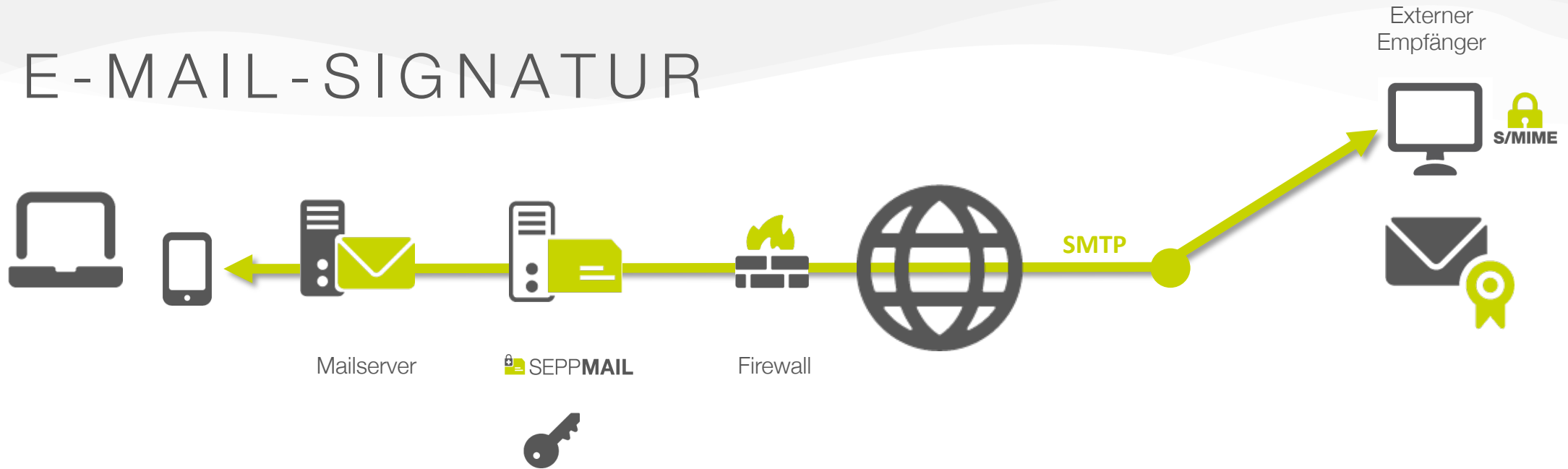
## E-Mail-Verschlüsselung:

- ✓ Verschlüsselung des Transportweges (TLS)
- ✓ Vertraulichkeit des E-Mail-Inhaltes

# E-MAIL SIGNATUR – SCHAFFT VERTRAUEN

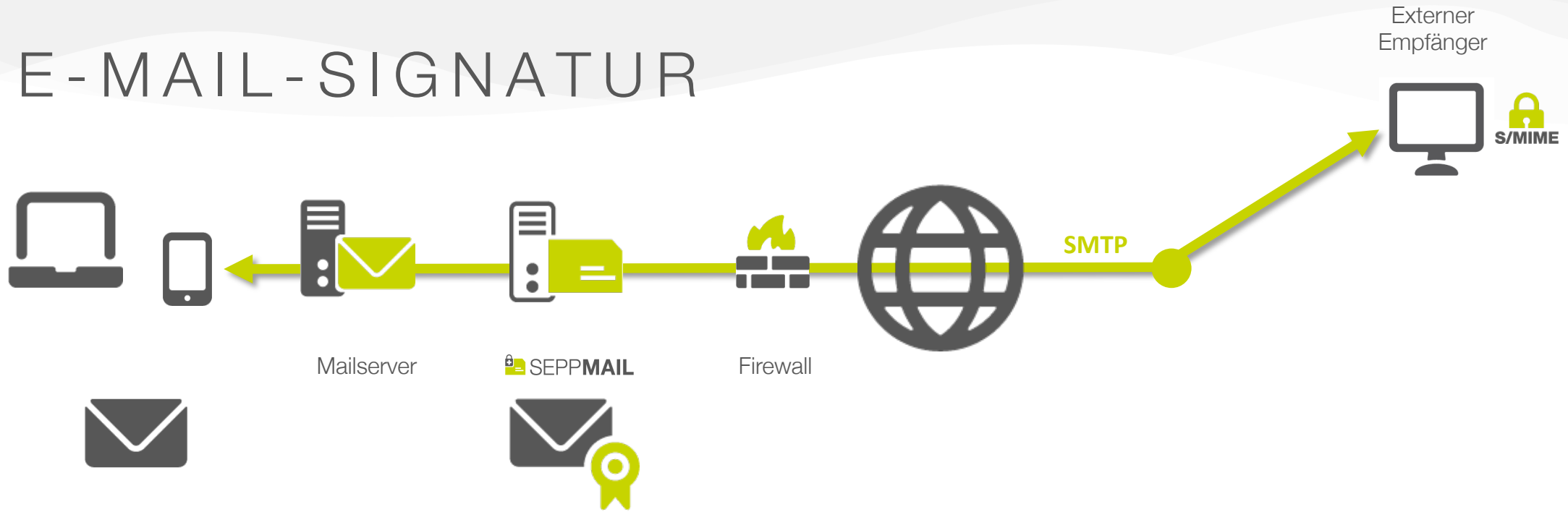


# E-MAIL-SIGNATUR



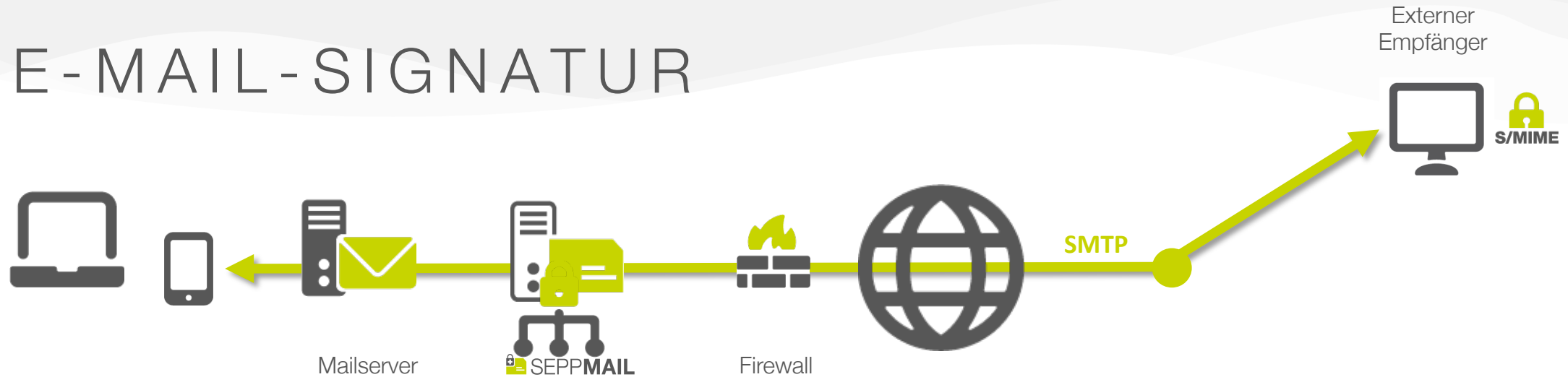
1. Alle öffentlichen Schlüssel werden automatisch aus den Signaturen gesammelt und bei Bedarf zur Verschlüsselung an den Sender herangezogen

# E-MAIL-SIGNATUR



1. Alle öffentlichen Schlüssel werden automatisch aus den Signaturen gesammelt und bei Bedarf zur Verschlüsselung an den Sender herangezogen
2. Alle ausgehenden E-Mails werden am Gateway automatisch im Namen des Senders signiert

# E-MAIL-SIGNATUR



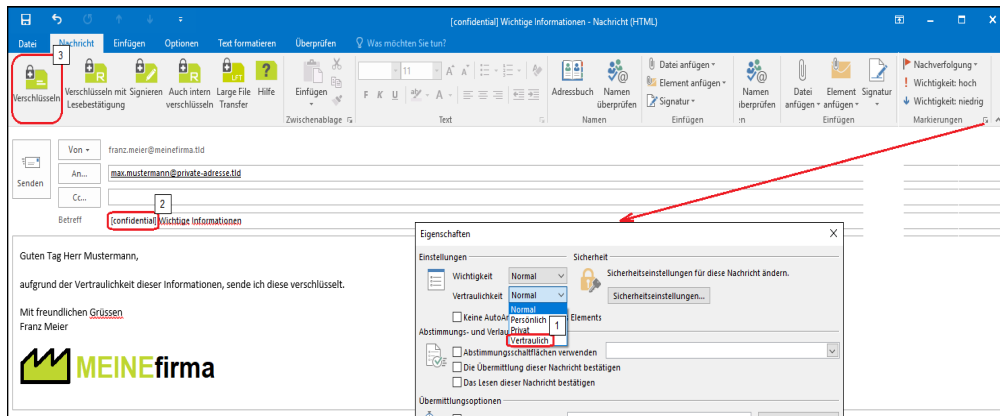
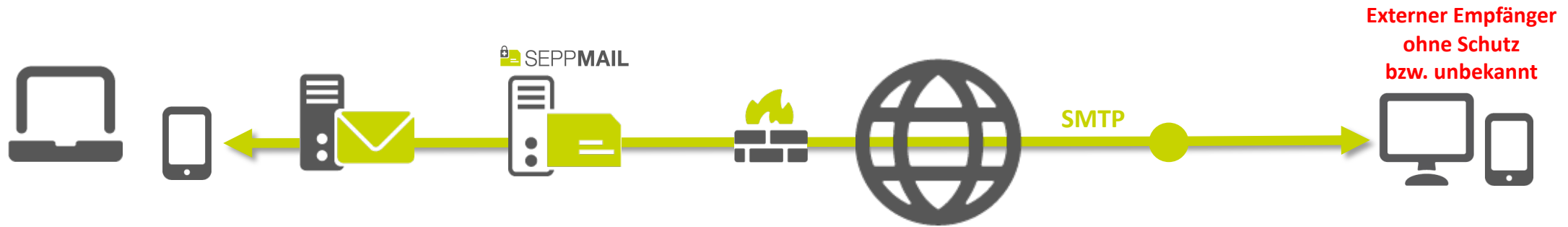
1. Alle öffentlichen Schlüssel werden automatisch aus den Signaturen gesammelt und bei Bedarf zur Verschlüsselung an den Sender herangezogen
2. Alle ausgehenden E-Mails werden am Gateway automatisch im Namen des Senders signiert
3. Integrierte Konnektoren erlauben vollautomatischen Bezug und Verwaltung von Zertifikaten

# E-MAIL-VERSCHLÜSSELUNG



DAS 100%-VERSPRECHEN

# VORGANG



## Schritt 1: Schreiben

Der Sender verfasst seine E-Mail in seinem Standard Client und klassifiziert diese als VERTRAULICH



# WEITERE BASISFUNKTIONEN

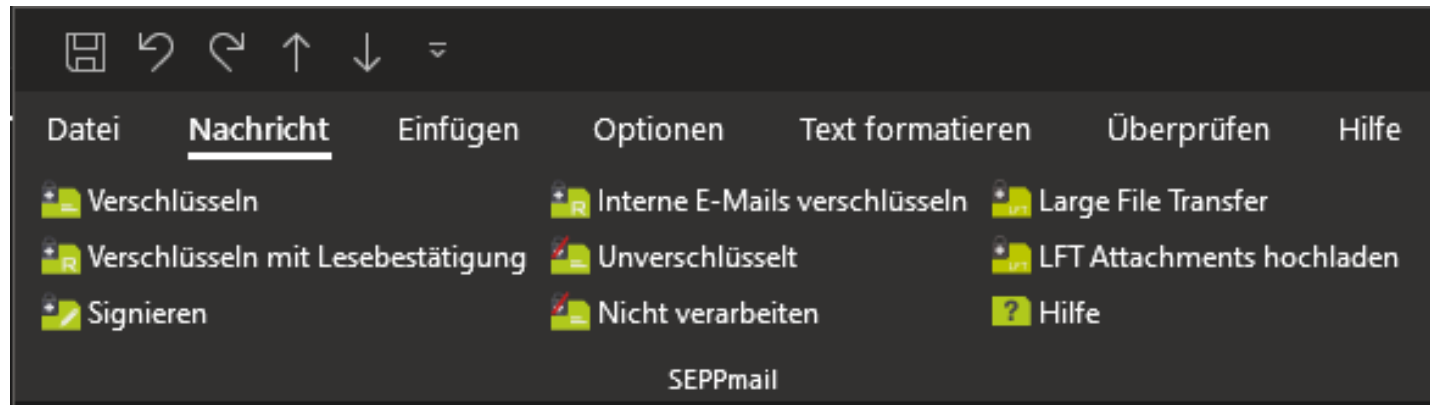
## E-MAIL CLIENT INTEGRATION: MS OUTLOOK

Kostenfreies COM-Add-In für die on-premises Version von Microsoft

(Verfügbar im SEPPmail Download Bereich <https://downloads.seppmail.com/index.php/outlook-plugin/>)

Aufgrund der Möglichkeiten der verfügbaren COM-Schnittstelle erweiterter Funktionsumfang

- + Internal Mail Encryption (IME)
- + Large File Transfer (LFT)

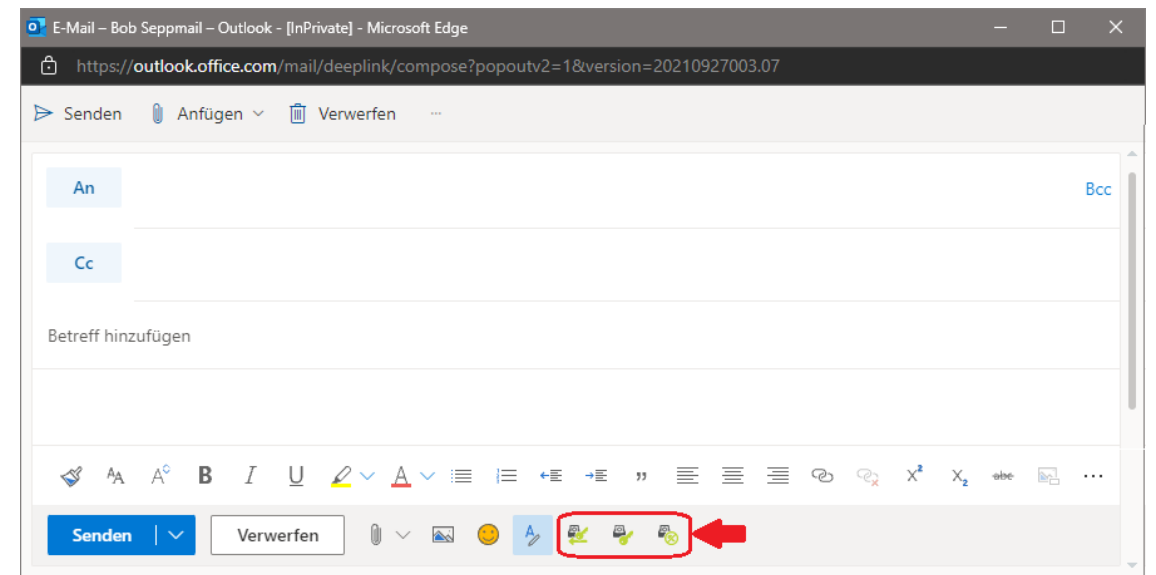
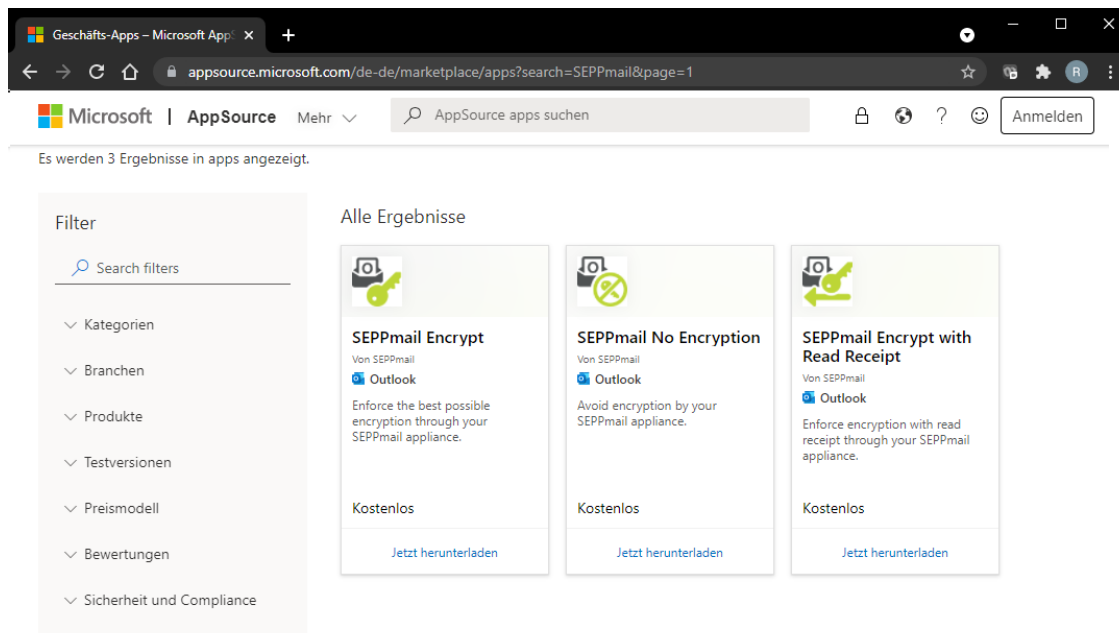


Die Anzeige der einzelnen Schaltflächen und deren Standard Status (aktiv/inaktiv) ist frei konfigurierbar, auch zentral per Group Policies für einzelne Benutzergruppen.

# WEITERE BASISFUNKTIONEN

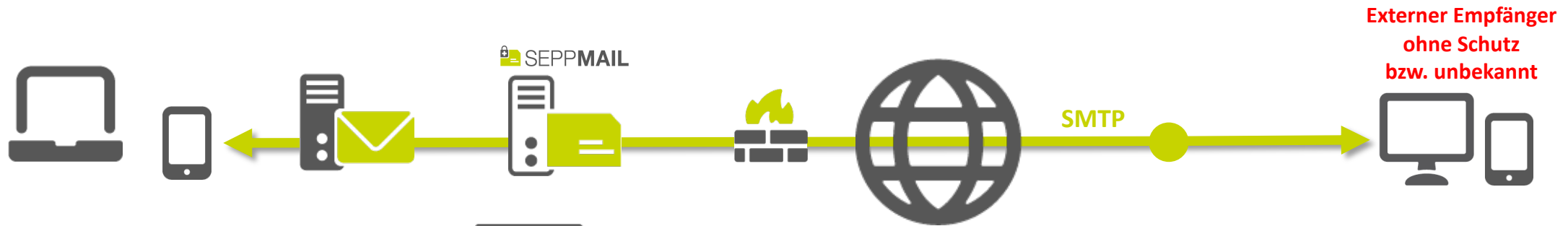
## E-MAIL CLIENT INTEGRATION: MS OUTLOOK

Kostenfreies X-Platform Add-In für die online Version von Microsoft Outlook  
(Verfügbar im Microsoft AppStore <https://apps.microsoft.com/>)



Zentrales Verteilen bei Business/Edu Accounts möglich

# RULESET



## Schritt 2: Prüfung der besten Option

Bei jeder E-Mail wird geprüft ob

öffentlicher S/MIME Schlüssel des Empfängers vorhanden ?

JA: verschlüsseln - > versenden

NEIN kein S/MIME ..... openPGP Schlüssel vorhanden ?

JA: verschlüsseln - > versenden

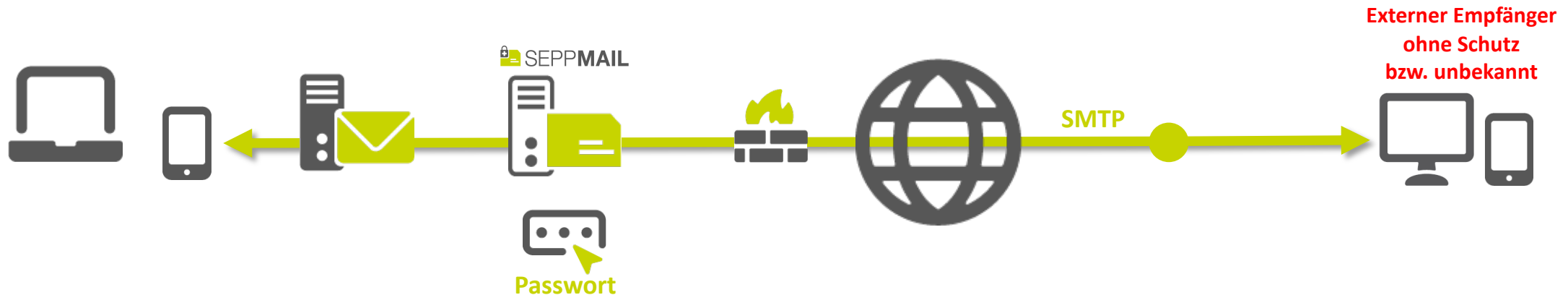
NEIN kein openPGP ..... Domainschlüssel bekannt ?

JA: verschlüsseln - > versenden

NEIN kein Domainschlüssel und VERTRAULICH, dann **GINA**



# GINA-TECHNOLOGIE RULESET



- ✓ Für den “ungeschützten – unbekanntem“ Empfänger wird ein sehr langer symmetrischer Schlüssel gerechnet
- ✓ Damit wird die gesamte E-Mail verschlüsselt und in einem html-Container an einer Träger-Mail versendet
- ✓ Gleichzeitig wird dem Sender ein Initialpasswort per E-Mail zur Übermittlung an den Empfänger per SMS, Fax, Telefon mitgeteilt
- ✓ Dieser Vorgang ist **einmalig** und der externe Empfänger ist in der Lage, die E-Mail zu öffnen



# GINA-TECHNOLOGIE

## ALTERNATIVE AUTHENTISIERUNG (IDP)

Anmelden [Registrierung](#)  Sprache ▾






### Nutzeranmeldung

E-Mail:

Passwort:

[Anmelden](#) [Passwort vergessen?](#)

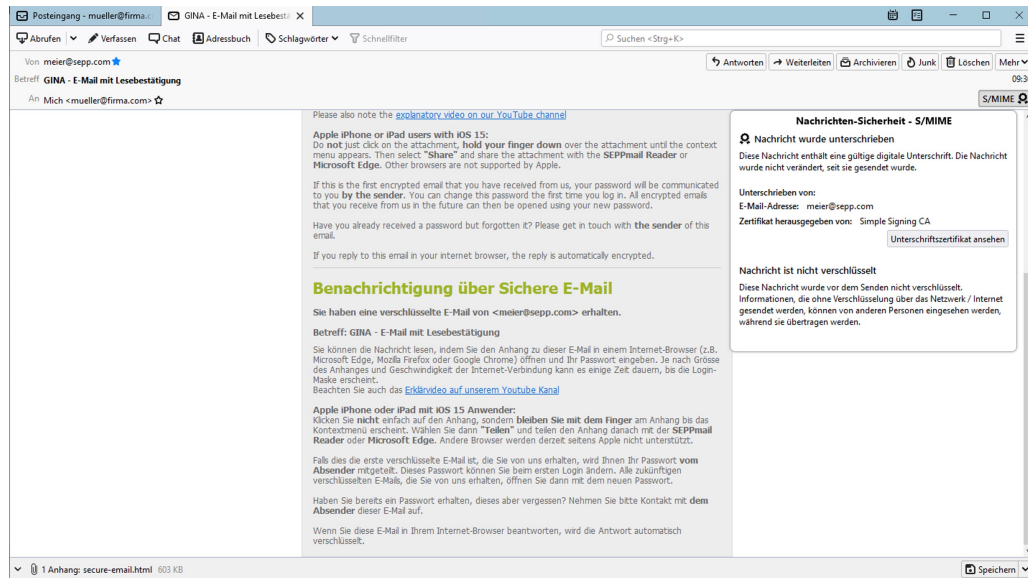
ODER

 Login with Facebook  Login with FideAS IAM  Login with Google  Login with LinkedIn  Login with M365

Powered by SEPPmail



# GINA-TECHNOLOGIE VORGANG



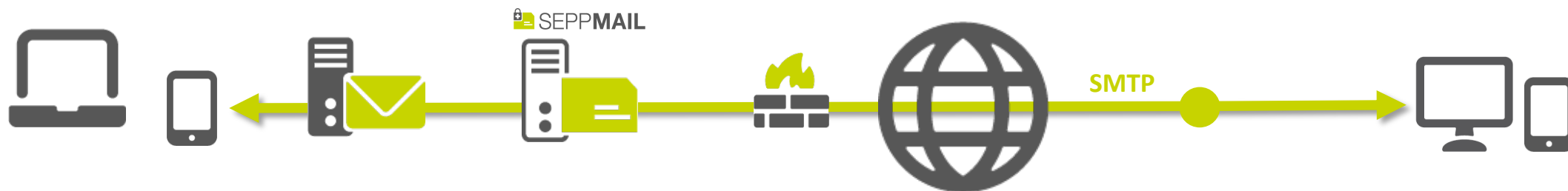
## Schritt 3: Empfangen

- ✓ Der Empfänger erhält eine Trägermail mit einem Container. Darin befindet sich vollinhaltlich die verschlüsselte Mail, aber keinerlei aktive Komponenten
- ✓ Corporate Identity (CI) kann voll und ganz abgebildet werden





# GINA-TECHNOLOGIE VORGANG



## Schritt 4: Registrieren

Empfänger hinterlegt sein eigenes Passwort.

Optional: Passphrase zur automatischen  
Passworrücksetzung

The screenshot shows the SEPPMAIL registration page. The title is 'Neuen Benutzer registrieren'. Below the title, there is a blue box with the instruction: 'Bitte geben Sie Ihren Namen und E-Mail-Adresse ein und setzen ein Passwort sowie eine Sicherheitsfrage und -antwort.' The form contains three input fields: 'E-Mail-Adresse' (with the example 'erika.muustermann@example.com'), 'Voller Name' (with the example 'Erika Muustermann'), and 'Neues Passwort'. Below the password field, there is a list of password requirements:

- Passwort-Mindestlänge: 8
- Das Passwort muss mindestens einen Großbuchstaben enthalten
- Das Passwort muss mindestens eine Zahl enthalten
- Das Passwort darf nicht ihren Namen oder Ihre E-Mail-Adresse enthalten
- Das Passwort darf nicht gleich einem ihrer letzten 4 Passwörter sein





# GINA-TECHNOLOGIE

## VORGANG

SEPPMAIL



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 von SEPPmail ursprünglich patentierten GINA-Verfahrens:

- ✓ E-Mails werden immer **AUSGELIEFERT**
- ✓ 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 GINA-Oberfläche und alle Texte können 100% per CSS-Stylesheet verändert werden
- ✓ Empfänger können sich vorgängig anmelden und so ihre bevorzugte Verschlüsselungsform (Passwort oder Zertifikatskey) wählen
- ✓ Empfänger kann über das Portal seine bevorzugte Verschlüsselungsform einstellen



# Kundenbeispiel



- ✓ Über 2,5 Mio secure GINA Mailaccounts
- ✓ Wachstum von + 1.000 Accounts pro Tag
  
- ✓ 55.000 bis 88.000 Entschlüsselungen pro Tag
- ✓ Peak: 7.000 pro Stunde (entspricht ca. 2 Entschlüsselungen pro Sekunde)
  
- ✓ Technologie-Split:
  - 95% GINA Technologie
  - 4,5% S/MIME
  - 0,5% openPGP

# ERWEITERUNGSMÖGLICHKEITEN & MODULE 1/2



## Large File Transfer:

- ✓ Wie GINA .... nur Mails werden auf Appliance zeitlich begrenzt zum Abruf zurückgehalten und nach Ablauf der Haltefrist gelöscht.
- ✓ Einlieferung der Files von Intern über 3 Wege:
  - Per E-Mail
  - Per GINA-Webmailer
  - Per Outlook Add-In



## Central Disclaimer Management:

- ✓ Zentrales einheitliches unternehmensweites E-Mail-Disclaimer-Management
- ✓ Anlegen unterschiedlicher Disclaimer-Templates
- ✓ Zugriff auf die individuellen Daten des Senders über AD-Anschluss
- ✓ Möglichkeit Bildern und Logos einzubauen
- ✓ Der Disclaimer wird immer an der RICHTIGEN Stelle eingefügt

# ERWEITERUNGSMÖGLICHKEITEN & MODULE 2/2



## Filtertechnologie (AS/AV)

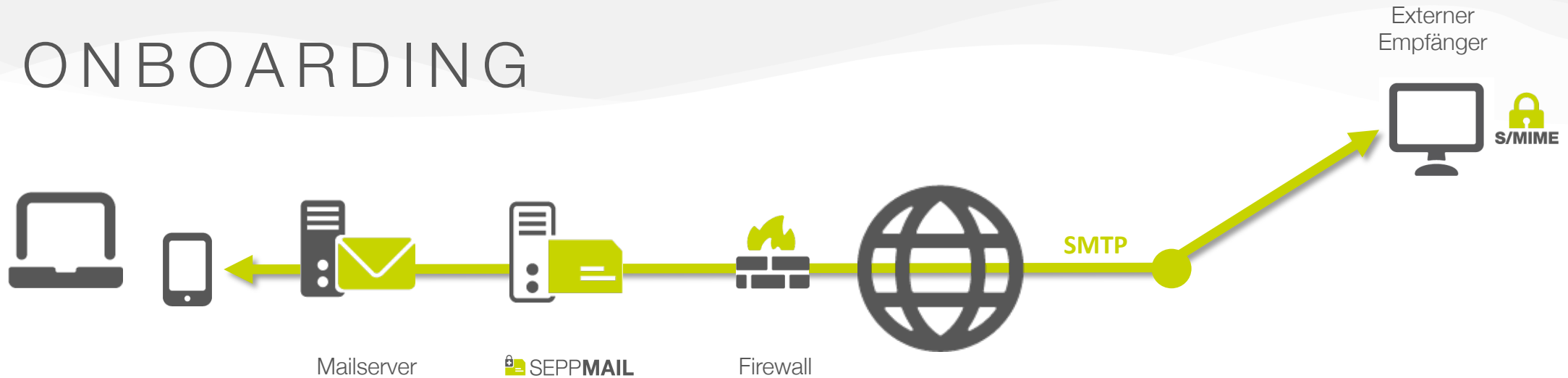
- ✓ onPrem: Protection Pack: ClamAV und Spam Assassin
- ✓ Seppmail.cloud: erweiterte Filtermöglichkeiten
  - (pro-) aktiv gemanagter Dienst
  - Support durch SEPPmail

## Internal Mail Encryption (IME 2.0)

- ✓ erweitert den Funktionsumfang von IME 1.0 um eine inhaltlich verschlüsselte Kommunikation vom E-Mail-Client bis zum SEPPmail Secure E-Mail Gateway
  - eine Träger-E-Mail mit konfigurierbarer IME-Empfängeradresse erstellt
  - die eigentliche E-Mail verschlüsselt als Anlage zur Träger-E-Mail bis zum SEPPmail Secure E-Mail Gateway übertragen  
Durch die Träger-E-Mail wird gewährleistet, dass die Header- und somit Routing-Informationen auf dem Übertragungsweg nicht manipuliert werden können.
  - die E-Mail über das SEPPmail Secure E-Mail Gateway mit dem für den Empfänger - egal ob intern oder extern - geeignetsten Verfahren (siehe [Verschlüsselungshierarchie](#)) verschlüsselt und ausgeliefert.



# ONBOARDING



1. Mitarbeiter sendet seine erste Mail über das neu implementierte Gateway
2. Das Gateway prüft nun, ob der Nutzer im angeschlossenen AD-Mitglied einer angelegten Gruppe ist  
Wenn ja:
  - Wird ihm eine Lizenz zugewiesen
  - und über den Konnektor ein Zertifikat ausgestelltWenn nein:
  - entsprechend der Konfiguration

# PLATTFORMEN



Secure E-Mail Gateway  
HW

Incl. 5 Jahre Wartung  
7 x 24

Austausch next Business Day  
Hot fix replacement innerhalb 4 Stunden



Secure E-Mail Gateway  
VM

- ESX
- Hyper Visor
- Hyper V
- KVM
- Azure



Secure E-Mail Gateway  
Service

# BETRIEBSMODELLE – VOLLKOMMENE FLEXIBILITÄT



on premises:

- ✓ Perpetual
- ✓ Subscription



CLOUD:

- ✓ MSP
- ✓ seppmail.cloud

# SEPPMAIL - DAS UNTERNEHMEN



Stefan Klein  
Gründer & CEO

- ✓ SEPPmail AG in Neuenhof bei Zürich
- ✓ SEPPmail – Deutschland GmbH in Brunnthal bei München
- ✓ SEPPmail – Deutschland Entwicklungszentrum Leipzig
- ✓ Vertriebsbüros in Aschaffenburg, Wien und Marbella
- ✓ Entwicklung von Secure E-Mail-Lösungen
- ✓ 23+ Jahre Erfahrung mit Secure E-Mail-Technologien
- ✓ Firma zu 100% eigenfinanziert (keine Investoren)
- ✓ Kunden und Vertriebspartner in ganz Europa (2-stufiges Vertriebsmodell)



[heimel@seppmail.de](mailto:heimel@seppmail.de)



Konfuzius

551 v.Chr. – 479 v.Chr.

**ERZÄHLE** es mir – und ich werde es **VERGESSEN**

**ZEIGE** es mir – und ich werde mich **ERINNERN**

Lass es mich **TUN** – und ich werde es **BEHALTEN**

**TESTEN** Sie uns ...