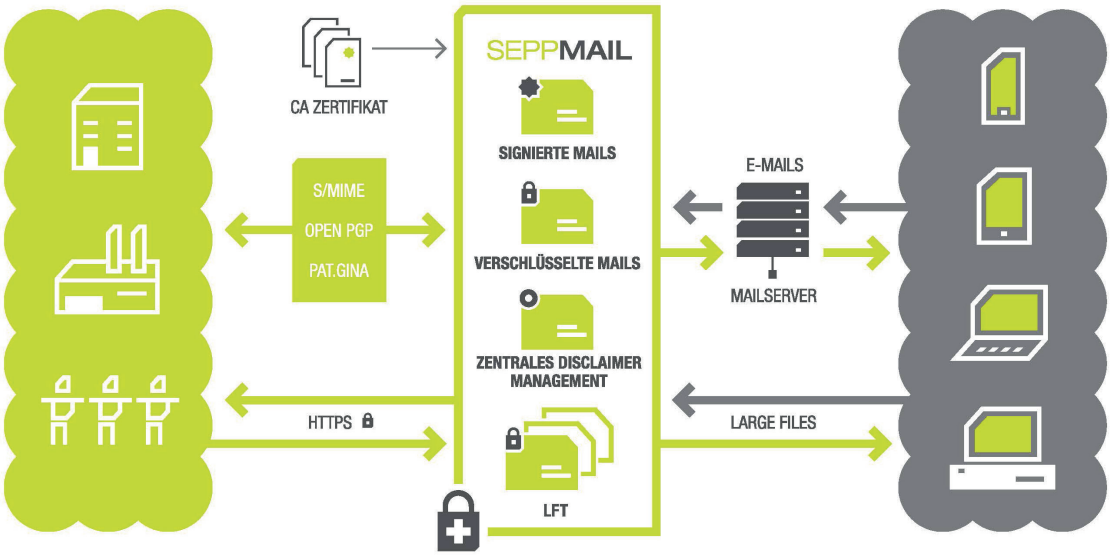
SEPPMAIL

Lösungsbeschreibung:



Das SEPPmail Secure E-Mail Gateway ist eine konsequente All-in-One-Lösung für den wirtschaftlichen und effizienten Einsatz...

- **einer zentralen Verwaltung von Zertifikaten und E-Mail-Signaturen (SIG);**
- **der Ver- und Entschlüsselung von E-Mails (ENC);**
- **des einfachen und sicheren Versands großer Dateien (LFT);**
- **des zentralen E-Mail-Disclaimer-Managements des gesamten Unternehmens (ZDM).**

Die Signatur und Verschlüsselung wird gemäß den internationalen E-Mail-Standards S/MIME und OpenPGP ausgeführt. Eine weitere Technologie – die Domainverschlüsselung – ist in der Basislizenz der Appliance für das gesamte Unternehmen enthalten. Diese Standardtechnologien decken – für den Nutzer vollkommen transparent – die hochfrequente, vertrauliche E-Mail-Kommunikation ab. Für den niederfrequenten, vertraulichen und spontanen E-Mail-Verkehr setzt SEPPmail das patentierte GINA-Verfahren ein.

Das Besondere an dem GINA-Verfahren ist, dass beim externen Empfänger – außer einem beliebigen Mail-Client und Browser – keinerlei weitere Softwarekomponenten oder Schlüssel zum Lesen und Antworten erforderlich sind. Auch der Sender verfasst seine Mails ohne weitere Erweiterungen auf seinem gewohnten Mailclient.

Die SEPPmail-Appliance wird als „out-of-the-box"-Lösung sowohl als Hardware in drei Leistungsklassen als auch als VM-Image für ESX, Hyper Visor und Hyper V geliefert. Optional kann die Appliance noch mit einem Protection Pack für Antivirus und Antispam erweitert werden.

Large File Transfer (LFT)

Jeder kennt das Problem, dass E-Mails mit zu großen Anhängen vom Empfängersystem abgelehnt werden. Die LFT-Funktionalität ermöglicht, dass Mails vollautomatisch – ab einer einstellbaren Größe – verschlüsselt auf der Appliance zum Download zurückgehalten und mit einem Ablaufdatum versehen werden. Der Empfänger erhält eine GINA-Mail mit der Einladung, die für ihn zurückgelegte Mail bis zum vorgegebenen Datum abzuholen. Optional kann der GINA-Anmeldeprozess für LFT-Mails – pro E-Mail – abgeschaltet werden.
Der Download erfolgt über eine gesicherte https-Strecke. Die Datei wird zum Ablaufdatum von der Appliance gelöscht. Dateien können über drei Wege auf die Appliance eingeliefert werden: entweder klassisch via E-Mail, mittels eines Outlook Plug-in, welches die Anhänge automatisch abtrennt und direkt auf die Appliance liefert, oder auch über das standardmäßig eingebaute interne GINA-Webportal. Auch von außen können große Dateien via GINA-Portal angeliefert werden.

Die Vorteile dieser Lösung liegen auf der Hand:

- der Sender kann ohne Umwege große Dateien versenden. Er muss seine gewohnte E-Mail-Umgebung nicht verlassen.
- die Daten sind verschlüsselt und werden nicht in der Cloud (wie z.B. bei Dropbox) zwischengespeichert.
- die Einladung zum Download erfolgt automatisch. Der Empfänger erkennt am eingeblendeten Ablaufdatum, dass es sich um eine Sonderform einer GINA-Mail handelt und wird nicht mit einem neuen, gewöhnungsbedürftigen Interface belastet.
- die Lösung ist von PCI-Experten geprüft und es ist somit möglich, dem PCI-Standard entsprechende Infrastrukturen aufzubauen!

Diese Lösung ist als eigenständiges Produkt oder als Erweiterung zu einem bestehenden SEPPmail-Verschlüsselungssystem erhältlich.

Zentrales Disclaimer-Management (ZDM)

Von Zeit zu Zeit müssen E-Mail-Disclaimer (Footer) angepasst werden; sei es, weil sich ein Text oder ein Logo ändert oder Marketinginformationen wie Hinweise zu Messeauftritten auf bestimmte Zeit im E-Mail-Disclaimer untergebracht werden müssen. Dabei obliegt es meistens dem Nutzer, diese Informationen in seinem E-Mail-Disclaimer zu ändern und anzupassen. SEPPmail bietet mit dem Zentralen Disclaimer-Management die Möglichkeit, Disclaimer Templates zu erstellen, die statische Inhalte wie Texte, Logos und Bilder enthalten. Die personenbezogenen Daten, wie Name, Position, Abteilung und Telefonnummern, werden aus dem angeschlossenen AD bezogen und eingetragen.

Für unsere Kunden ergeben sich damit die folgenden Vorteile:

- eine einheitliche Möglichkeit der Gestaltung der E-Mail-Disclaimer für alle ausgehenden E-Mails (Corporate Identity);
- eine Entlastung der Mitarbeiter;
- die Möglichkeit, zeitlich begrenzte Aktionen für Abteilungen (z.B. Vertrieb) zentral einzustellen und wieder zu entfernen.

Diese Lösung ist als eigenständiges Produkt oder als Erweiterung zu einem bestehenden SEPPmail-Verschlüsselungssystem erhältlich.

SEPPmail E-Mail-Signaturlösung (SIG)

Die Position des Gateway in der DMZ eines Unternehmens ist als zentraler Punkt ideal für die Verwaltung von E-Mail-Zertifikaten und Signaturen aller ausgehenden E-Mails im Namen des Senders. Managed PKI-Konnektoren zu namhaften Certificate Authorities (CA's) garantieren den administrationsfreien Bezug und die Verwaltung von X.509 Zertifikaten. Die Signaturen aller eingehenden Zertifikate werden geprüft und als „Signed OK" oder „Signed NOT OK" angezeigt. Der enthaltene öffentliche Schlüssel des Senders wird eingesammelt und für die Verschlüsselung vorgehalten. Alle ausgehenden E-Mails werden mit dem Nutzerzertifikat signiert. Sollten E-Mails mit dem öffentlichen Schlüssel des Nutzers verschlüsselt angeliefert werden, werden sie am Gateway entschlüsselt.

E-Mail-Ver- und -Entschlüsselung (ENC)

Beim **Design des Produktes** wurde von Anbeginn auf Standardisierung gesetzt und darauf geachtet, die Administration soweit wie möglich zu automatisieren und dem Nutzer nur die absolut notwendigen Handlungen abzuverlangen, damit 100% der als vertraulich gekennzeichneten Mails verschlüsselt werden. Die konsequente Einhaltung dieser Maxime ließ über die Jahre ein massenmarkttaugliches Produkt entstehen.
Der auf der SEPPmail Technologie beruhende Service der DATEV in Nürnberg für sichere E-Mail an alle Rechtsanwalts- und Steuerberatungsmandanten zeigt dies eindrucksvoll. Jahrelange praktische Erfahrung und das Feedback unserer Kunden nehmen Einfluss auf das Layout und die Funktionalität der Lösung. Die erste Version wurde 2001 dem Schweizer Markt vorgestellt. Alle Verbesserungen und Erweiterungen werden seitdem dem Stammprodukt zugefügt und beim Update automatisch allen Installationen auf Knopfdruck zum Download zur Verfügung gestellt. Der Fokus liegt auf Reproduzierbarkeit, Einfachheit und dadurch Stabilität.

Wir teilen die vertrauliche Kommunikation in zwei Arten ein:

a. **Die hochfrequente vertrauliche Kommunikation**
Dabei wird ein für den Nutzer komplett transparenter Technologielayer eingezogen, der E-Mails bidirektional ver- und wieder entschlüsselt.
Die dafür geeigneten und verbauten Techniken sind:

1) S/MIME
2) OpenPGP
3) Domainverschlüsselung
4) TLS

b. **Die spontane, vertrauliche niederfrequente Kommunikation**
Das wichtigste Merkmal unserer Lösung ist die einzigartige Methode, spontan einen Kommunikationspartner anzuschreiben. Dabei benötigt man keinerlei Kenntnis über eine eventuell vorhandene E-Mail Sicherheitsinfrastruktur beim Empfänger – wenn dieser überhaupt eine solche hat.
Hier kommt unsere **patentierte GINA-Webmailtechnologie** zum Einsatz. Um dem „unbekannten" Empfänger eine vertrauliche E-Mail zu senden, benötigt man nur seine E-Mail-Adresse und – wenn vorhanden – die Telefon- oder Mobilnummer.

Die Vorteile für unsere Kunden sind...

- die E-Mail wird zu 100% an den Empfänger ausgeliefert.
- der Empfänger benötigt zum entschlüsselten Lesen nur Standardkomponenten wie einen beliebigen Mailclient, Browser und Internetzugang – sonst nichts! Die GINA-Mail ist auf ALLEN Endgeräten, die Mails empfangen können, zu öffnen!
- der Empfänger kann sofort sicher antworten.

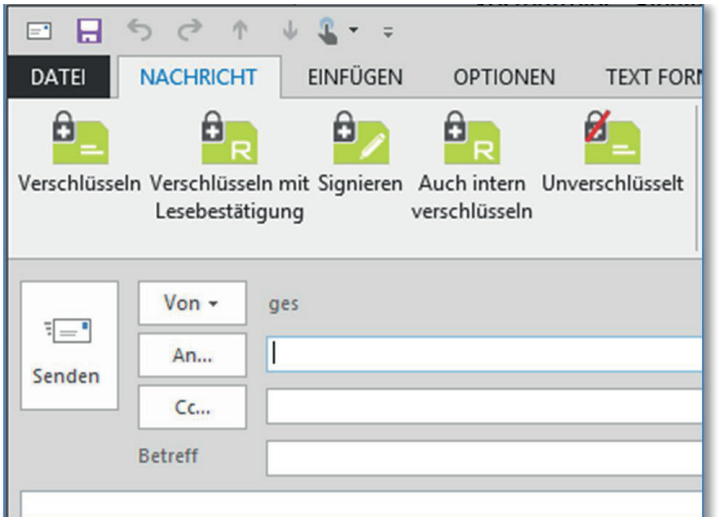
SEPPMAIL

GINA

Schritt für Schritt Vorstellung des Vorganges

Schritt 1: SENDER – Schreiben und Senden
Ein Sender verfasst seine E-Mail in seinem gewohnten E-Mail-Client. Durch setzen der „Vertraulichkeit" wird die Mail verschlüsselt, als HTML-Attachment an eine Standard-Mail angehangen und so vollständig versendet. Die Vertraulichkeit wird entweder durch die Standardfunktionalität des E-Mail- Client gesetzt oder durch sogenannte „Tags" (=Befehlswörter) im Betreff, z.B. [secure]. Auch fest definierte Regeln für dieses Steuern können auf der SEPPmail-Appliance gesetzt werden.

SEPPmail stellt für Outlook Anwender auch ein kostenfreies Add-in zur Vertraulichkeitsklassifizierung der E-Mail zur Verfügung. Die Schaltflächen können nach Bedarf angezeigt werden.

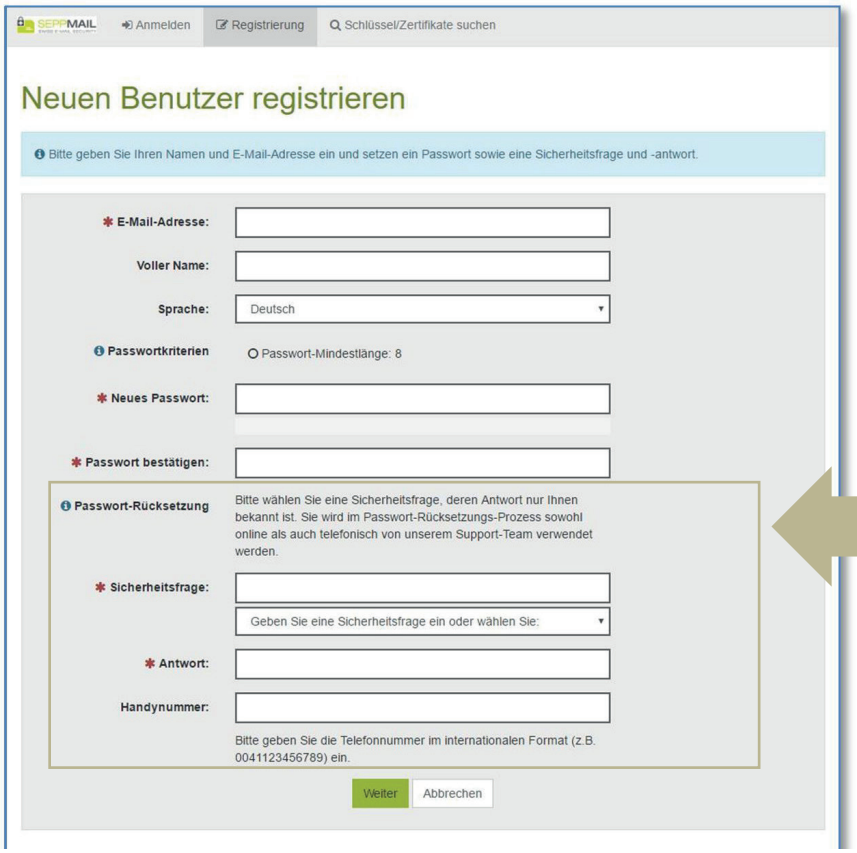


Die E-Mail wird <u>vollständig</u> als verschlüsseltes HTML-Attachment ausgeliefert. Dadurch ergibt sich ein eindeutiger rechtlicher Übergang an den Empfänger. Außerdem werden die eigenen Maschinenressourcen geschont, **da keine Mails auf der Appliance gespeichert und zum Download vorgehalten werden.** Der Sender ist somit auch der Verpflichtung entbunden, Mails zu archivieren und für x-Jahre bereitzustellen. Das HTML-Attachment beinhaltet keinerlei aktive Komponenten, passiert somit jede Firewall und ist in jedem Browser lesbar.

Nur bei der allerersten Kommunikation mit einem „unbekannten" Empfänger wird der Sender darüber informiert, dass seine E-Mail verschlüsselt versendet wurde und die Übermittlung eines Initialpassworts erforderlich ist. Dieses sollte per **SMS oder Telefon** übermittelt werden. Es ist dem Sender aber auch möglich, gleich im Betreff den Vermerk (z.B.: [sms:00491701234561) mitzugeben. Damit werden das verschlüsselte Versenden der E-Mail und der Versand des dazugehörigen Initialpasswortes gleichzeitig ausgelöst.

Der Empfänger erhält dadurch zwei Komponenten: die verschlüsselte E-Mail und eine SMS mit dem Passwort. Somit ist eine **Zwei-Faktor-Authentifizierung** gegeben.

Schritt 2: EMPFÄNGER – Registrieren und Lesen
Der Empfänger öffnet das HTML-Attachment mit dem verschlüsselten Inhalt, gibt sein Initialpasswort ein und wird einmalig auf eine Anmeldeseite geleitet. Hier vergibt er sein persönliches Passwort nach entsprechend eingestellten Regeln. Für den Fall, dass er sein Passwort vergessen hat, kann er optional eine Sicherheitsfrage mit dazugehöriger Antwort definieren (Hilfe zur Selbsthilfe).



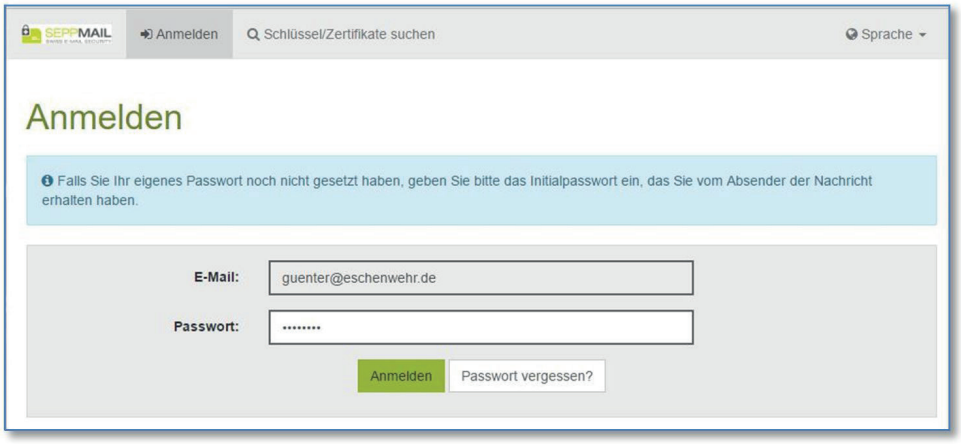
Selfservice-Passwortmanagement:

Optionales Modul zum selbständigen Rücksetzen von vergessenen Passwörtern.

Sollte der Empfänger jedoch **eigenes Schlüsselmaterial** (OpenPGP oder S/MIME) besitzen, so kann er dieses über das folgende GINA-Webmail-Portal zur SEPPmail hochladen. In Zukunft wird dann vorzugsweise sein aktueller Public Key zur Verschlüsselung verwendet. Durch den zuvor durchlaufenen Authentifizierungsprozess (zwei Faktoren: E-Mail + SMS-Passwort) können OpenPGP- und selbst ausgestellte S/MIME-Schlüssel ohne weitere Prüfung akzeptiert werden! Dies ist wieder ein erheblich geringerer Aufwand für den Administrator.

Dieses patentierte Verfahren benötigt keine zusätzlichen Technologien, wie z.B. PDF-Umwandlung und Verschlüsselung oder die Nutzung von zip- bzw. exe-Dateien. Der Empfänger nutzt lediglich seinen Standard-Mailclient, Browser und Internetzugang. Damit sind alle Endgeräte, die Mails empfangen und senden können, in der Lage, spontan verschlüsselte E-Mails zu empfangen und zu beantworten (versenden).

Ein weiterer wesentlicher Vorteil der GINA-Technologie ist das **Passwortmanagement**. PDFs benötigen immer das zum Zeitpunkt der Verschlüsselung vergebene Passwort. Bei SEPPmail kann dieses jederzeit durch den Empfänger zurückgesetzt und verändert werden. Darum legt er bei der Erstanmeldung auch seine Sicherheitsfrage und Antwort fest. Im Falle einer Passwortrücksetzung wird automatisch das neue Passwort per SMS zugestellt.



Natürlich können externe Kommunikationspartner auf den Einsatz einer SEPPmail-Appliance vorbereitet werden. Der zukünftige Empfänger sicherer E-Mails kann sich auch proaktiv via Portal bei SEPPmail anmelden und damit sein Passwort schon vorher festlegen, bzw. seinen eigenen Public-Key hochladen. Damit wird die erste verschlüsselte Kommunikation schon mit den Wunscheinstellungen des Empfängers durchgeführt und die Prozedur des Initialpasswortes entfällt.

Die **Corporate Identity** kann vollständig durch sogenannte CSSs (Corporate Style Sheet) abgebildet werden. Die GINA-Mailoberfläche ist völlig den unternehmerischen Vorgaben in puncto Erscheinungsbild anpassbar. Die Schriften, Farben, Formen, Buttons, Anweisungen und Sprachen sind beliebig veränderbar. Es ist hiermit auch eine vollständige Integration in Unternehmenswebseiten möglich. Auf Wunsch kann auch mit der ersten Mail ein Disclaimer eingeblendet werden, der den Kunden über seine Rechte und Pflichten aufklärt, die bei der Anmeldung zu akzeptieren sind.

!!!All diese Funktionen bleiben selbstredend bei zukünftigen Updates erhalten!!!

Empfang auf allen mobilen Endgeräten möglich: Sichere GINA-E-Mails können nativ auf Windows Phone, Android, i-OS und Blackberry (ab BB10) empfangen und gelesen werden.

Weitere Eigenschaften der SEPPmail-Lösung

1) **Ruleset:** Das zentrale Steuerelement auf der Appliance ist das Ruleset Dieses beinhaltet alle Anweisungen zur Verarbeitung einer E-Mail. Etwa 90% der Kundenanforderungen an eine sichere E-Mail werden mit den Standardeinstellungen (Standard-Ruleset) realisiert. Dabei erfolgt bei jeder ausgehenden E-Mail auf der Appliance eine hierarchische Prüfung:
   a. Existiert ein S/MIME-Schlüssel für den Empfänger? Wenn ja, wird dieser vorrangig zur Verschlüsselung herangezogen.
   b. Gibt es einen OpenPGP-Schlüssel? Wenn ja, wird dieser zur Verschlüsselung verwendet.
   c. Existiert ein S/MIME-Domainschlüssel von der Gegenstelle oder ein OpenPGP-Domainschlüssel? Wenn ja, kommt dieser zum Einsatz.
   d. Erst, wenn keine der oben genannten Standardtechnologien für den oder die Empfänger hinterlegt sind UND die E-Mail als vertraulich markiert wurde, sodass eine Verschlüsselung auf alle Fälle erzwungen wird, kommt die oben beschriebene GINA Technologie zum Einsatz.

Sollten über das Standard-Ruleset hinausgehende **spezielle unternehmensspezifische Anpassungen** notwendig werden, können diese über den flexiblen Rulesetgenerator (Standardwerkzeug) umgesetzt werden. Damit sind auch umfangreiche und komplexe Projekte realisierbar.

2) **Zertifikate aus dem Mailstrom:** Woher kommt aber das Schlüsselmaterial?
   Während der gesamte ankommende Mailstrom durch die SEPPmail-Appliance fließt, sammelt diese alle **S/MIME**-Public Keys der in den Signaturen vorhandenen Zertifikate. S/MIME-Zertifikate werden sofort akzeptiert, sofern sie von einer anerkannt offiziellen CA ausgestellt wurden. Nicht bekannte CAs werden gesammelt und dem Administrator zur Validierung vorgelegt. Nach erfolgter Freigabe werden auch von diesen CAs alle Keys automatisch gesammelt und akzeptiert.

3) Zur nachteiligen Natur von **OpenPGP**-Keys gehört es, dass diese, bevor sie zur Verschlüsselung herangezogen werden können, zuerst validiert werden müssen. Eine automatisierte Prüfung ist somit nicht möglich. Es muss somit bei jedem zu importierenden OpenPGP-Key auf separatem Kanal (Telefon) der Fingerprint geprüft werden. SEPPmail hat ein „umgedrehtes" Verfahren realisiert: Wenn ein Empfänger eine GINA-verschlüsselte E-Mail erhält, dann kann er – in dem sich öffnenden GINA-Webmail-Portal – seinen eigenen Public-Key hochladen. Es ist keine zusätzliche Validierung durch die Administration oder Sender mehr notwendig. Die Praxis zeigt, dass die OpenPGP-Technologie mehr und mehr an Bedeutung verliert.

4) Die **Domainverschlüsselung** ist eine Grundfunktionalität und bereits in der Basislizenz enthalten. Dabei erkennen sich alle SEPPmail-Appliances und verschlüsseln den gesamten Mailverkehr untereinander vollautomatisch – Fremdprodukte können durch einen einfachen Key-Austausch ebenfalls angebunden werden. Es werden somit ohne zusätzliche Lizenzen für das gesamte Unternehmen alle eingehenden und ausgehenden Mails zwischen den Domains verschlüsselt.

   Eine weitere Grundfunktionalität ist das Einfügen verschiedener E-Mail-Standard-Fußnoten (Disclaimer) an ausgehende Mails anhand der Empfänger-E-Mail-Domäne. Das bedeutet, man kann z.B. an E-Mails mit spanischen Adressen die spanische Fußnote oder an französische Adressen die französische Fußnote anhängen lassen.

5) **Managed PKI** ist die automatisierte Anbindung von offiziellen Certificate Authorities (CA). Dabei werden von der SEPPmail für den Benutzer selbständig S/MIME-Keys ausgestellt und der angeschlossen CA zur Freigabe (CSR) vorgelegt. Dieser Vorgang läuft vollautomatisch ohne Eingriff des Administrators ab. Zurzeit sind folgende CA-Konnektoren verfügbar: SwissSign, QuoVadis, DigiCert und GlobalSign. Weitere Konnektoren sind in Vorbereitung. Selbstverständlich werden auch alle anderen CAs (z.B. A-Trust, Comodo) unterstützt. Die Zertifikate können dabei per Bulk-Import in die SEPPmail eingepflegt werden.

6) **Einfacher und automatisierter Betrieb:** Funktionen wie automatisiertes Schlüsselmanagement, Domainverschlüsselung, Portalfunktionen (erlauben einem externen Nutzer, sicher mit dem Unternehmen zu kommunizieren) sowie ein User-Selfservice-Password-Management sorgen für einen reibungslosen, einfachen und kostengünstigen Betrieb ohne viel Support- und Helpdeskaufwand.

7) **Hochverfügbar als Standardfunktionalität:** Master-Master Clustering und auch Geoclustering sind als Basisfunktionen verfügbar und werden mit wenigen Einstellungen ebenso eingerichtet wie Loadbalancing. Das Bankenrechenzentrum GRZ in Österreich betreibt zum Beispiel einen 2x2-SEPPmail-Cluster an den Standorten Innsbruck und Linz und bedient den gesamten Mailverkehr für 14.000 Mailboxen seit Jahren ohne Probleme.

8) **Multidomain und mandantenfähig:** Das System ist mandantenfähig. Es können mehrere Domains eingerichtet werden und/oder an einzelne Mandanten Verwaltungsaufgaben, wie das Account- und Usermanagement, GINA Layouting und Logging, delegiert werden.

9) Ein Beispiel für **Akzeptanz und Verbreitung in Kombination mit Skalierbarkeit und Stabilität** der Lösung SEPPmail ist www.HIN.ch (= Health-Information-Netzwerk) in der Schweiz. Mit dieser zu 100% auf SEPPmail basierenden Lösung verschlüsseln täglich 350 Spitäler und 18'000 Ärzte (insgesamt rund 180'000 Benutzer) ihre gesamte E-Mail-Kommunikation.

Quote eines Administrators eines Schweizer Spitals:

„Guten Tag

Ich habe HIN Mail Gateway auf den neusten Stand gebracht. Ich finde diesen HIN (=SEPPmail) Gateway genial. Button „Update" betätigen und es funktioniert einfach. 211 Tage war die VM „Uptime" ohne die geringsten Probleme. Täglich kommt ein Report und die aktuellen Adresslisten holt er sich selber. Auch die Anleitung ist sehr gut. So anwenderfreundlich, dass SEPPmail fast eine Tochtergesellschaft von Apple sein könnte ;-)"

Eine ansehnliche Anzahl zufriedener Kunden betreiben unsere SEPPmail-Lösung mit hoher Anwenderakzeptanz: www.seppmail.de

Die Erfahrung zeigt, dass die einfache „schnörkellose" Anwendung bei Sendern und Empfängern auf eine hohe Akzeptanz stößt. Zusätzliche Optionen und Technologien wie PDF-Reader oder zip-Verschlüsselung sind nicht notwendig und verursachen daher auch nicht zusätzliche Komplexität und somit auch keine Probleme und Supportaufwand auf Betreiberseite. Eine belastbare Zahl für den Supportaufwand beim GINA-Empfänger lieferte ein Kunde mit über 100.000 GINA-Empfängerkonten. Aus der Praxis wissen wir, dass weniger als 6% der GINA-Erstanwender und weniger als 1% der Dauernutzer Unterstützung bei der Bedienung unserer Lösung benötigen.

SEPPMAIL

Auszug von Funktionen und Komponenten:

Komponente	SEPPmail
Basissystem	Gehärtete openBSD-Appliance mit allen notwendigen Komponenten als Firmware
Updates	Per Knopfdruck wird die gesamte Firmware geladen; kein Update von einzelnen Komponenten erforderlich.
Kundenspezifische Anpassungen	Werden über das Ruleset realisiert. Sind die Kundenwünsche so speziell, dass diese (noch) nicht im Produkt enthalten sind, werden diese standardisiert, in den Entwicklungspfad aufgenommen und allen Kunden zur Verfügung gestellt. Es gibt nur ein Hauptprodukt.
Aufsetzen beim Kunden	„Out of the Box" – Installation, keine externen Komponenten (wie z.B. Datenbank) notwendig
Ressourcenbedarf	Keine Zwischenspeicherung von Mails, daher geringer Bedarf.
Appliance	Standardisierte Hardware in vier Leistungsklassen, aber auch als VM verfügbar (ESX, Hyper Visor, Hyper V).
„Mail an Dritte"	Patentiertes Verfahren GINA, welches sowohl einfach zu bedienen als auch sicher ist. Erstmalige Passwortvergabe durch SMS (eingebaut)
Wartung	Kein eigentliches Housekeeping notwendig, da kein wachsender Speicherbedarf
Backups	Ein einziges Backup, mit welchem ein ganzes System wiederhergestellt werden kann
Clustering / Loadbalancing	Master-Master Clustering ist eine integrierte Grundfunktion, auch für geographisch getrennte Orte.
Technologien	S/MIME, OpenPGP, TLS, GINA (patentierter Webmailer), managed domain key service
Managed PKI	Automatisierte Anbindung zu namhaften Certificate Authorities. Alle weiteren Zertifikate können per Bulk-Import geladen und automatisch den autorisierten Usern zugeordnet werden.

Sie wollen die Lösung testen?

Lassen Sie sich eine Testmail von unserer Homepage www.seppmail.de über die Online Demo zustellen oder kontaktieren Sie: info@seppmail.de. Wir bieten die Möglichkeit, unsere Lösung für 30 Tage – auf Basis einer VM – kostenlos zu testen. Wir begleiten und unterstützen Ihren Test durch unser Fachpersonal.