Lösungsbeschreibung:

Das SEPPmail secure E-Mail Gateway ist eine konsequente All-in-One Lösung für den wirtschaftlichen und effizienten Einsatz einer zentralen Signatur und Verschlüsselung von E-Mails sowie den einfachen und sicheren Versand großer Dateien. 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.

Die SEPPmail Aplliance wird als out-of-the-box Lösung sowohl als Hardware in 4 Leistungsklassen, als auch als VM-Image für ESX, Hyper Visor und Hyper V ausgeliefert.

12 Gründe:

1) Beim **Design des Produktes** wurde von Anbeginn auf Standardisierung gesetzt und darauf geachtet, dem Administrator so wenig wie möglich aufzubürden und dem Nutzer nur so viel wie notwendig an die Hand zu geben, damit 100% der als Vertraulich gekennzeichneten Mails verschlüsselt werden. Die konsequente Einhaltung dieser Maxime ließ über die Jahre ein massenmarkttaugliches Produkt entstehen, wie der auf der SEPPmail Technologie beruhende „INCAmail“-Service der Schweizerischen Post beweist. 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.

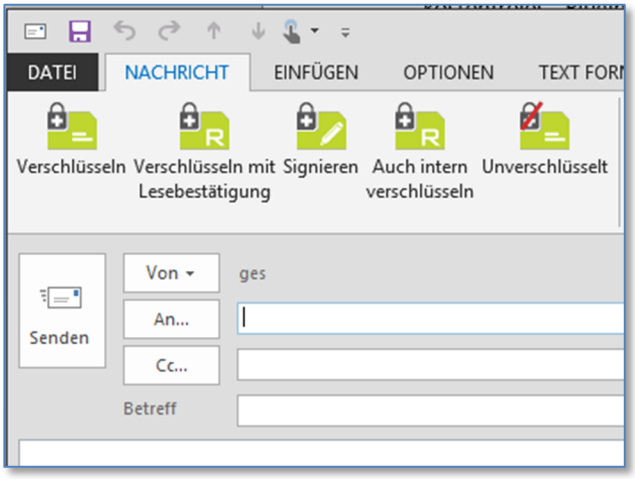
2) Das wichtigste Merkmal unserer Lösung ist die einzigartige Methode spontan einen Kommunikationspartner anzuschreiben. Dabei benötigt man keinerlei Kenntnis über eine eventuell vorhandene E-Mail Sicherheitsinfrastruktur beim Empfänger, wenn dieser überhaupt eine solche hat.

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 die Telefonnummer (idealer Weise die Mobilnummer). Dieser wiederum benötigt zum entschlüsselten Lesen nur Standardkomponenten wie einen beliebigen Mailclient, Browser und Internetzugang – sonst nichts !

Auf den folgenden Seiten nun die 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 und als HTML Attachment an eine Standard Mail gefügt und so versendet. Die Vertraulichkeit wird entweder durch die Standardfunktionalität des E-Mail Clients gesetzt, oder durch sogenannte „Tag’s“ (=Befehlswörter) im Betreff zB [secure]. Auch fest definierte Regeln für dieses Steuern können auf der SEPPmail Appliance gesetzt werden.

SEPPmail stellt für Outlook Anwender auch ein kostenfreies AddIn zur Vertraulichkeits-Klassifizierung der E-Mail zur Verfügung. Die Schaltflächen können nach Bedarf beliebig angezeigt werden.



Die E-Mail wird vollständig als verschlüsseltes HTML-Attachment ausgeliefert. Dadurch ergibt sich ein eindeutiger rechtlicher Übergang an den Empfänger. Außerdem werden die eigenen Maschinen-Ressourcen geschont, **da keine Mails auf der Appliance gespeichert und zum Download vorgehalten werden.** Der Sender ist damit auch der Verpflichtung entbunden Mails zu Archivieren und 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 eMail 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 (zB: [sms:0049170123456]) mitzugeben. Damit wird das verschlüsselte Versenden der E-Mail + SMS 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.

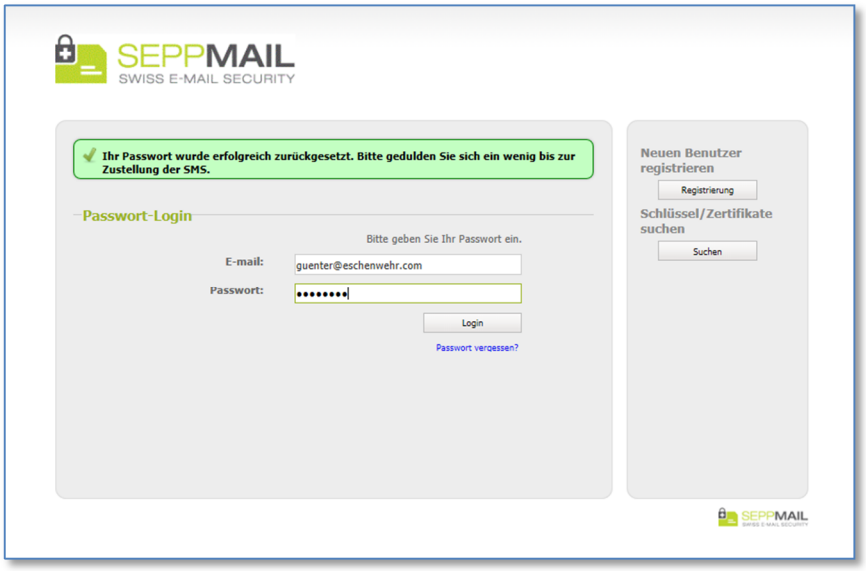
Schritt 2: EMPFÄNGER - Registrieren und Lesen: Der Empfänger öffnet das HTML Attachment mit dem verschlüsselten Inhalt, gibt sein Initialpasswort ein und wird einmalig auf eine Anmeldeseite geleitet.

Hier vergibt er sein persönliches Passwort nach entsprechend eingestellten Regeln und definiert seine Sicherheitsfrage mit Antwort, für den Fall er hat sein Passwort vergessen (Hilfe zur Selbsthilfe) (optionales Modul).

Sollte der Empfänger jedoch **eigenes Schlüsselmaterial** (OpenPGP oder S/MIME) besitzen, so kann er über das folgende GINA-Webmail-Portal dieses zur SEPPmail hochladen. In Zukunft wird dann vorzugsweise sein aktueller Public Key zur Verschlüsselung verwendet. Durch den zuvor durchlaufenen Authentifizierungsprozess (2 Faktoren: E-Mail + SMS Passwort), ist es nun auch möglich OpenPGP und selbst ausgestellte S/MIME Schlüssel ohne weitere Prüfung zu akzeptieren! Somit wieder ein erheblich geringerer Aufwand für den Administrator.

Dieses patentierte Verfahren benötigt keine zusätzlichen Technologielayer, wie zB pdf-Umwandlung und Verschlüsselung, zip oder exe. Der Empfänger findet mit seinem Standard Mailclient, Browser und Internetzugang sein Auslangen! Damit sind alle Endgeräte die Mails empfangen und senden können in der Lage, spontan verschlüsselte E-Mails zu empfangen und zu beantworten (versenden).

Ein wesentlicher Punkt ist das **Passwortmanagement.** Pdf's 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 an der 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 dem unternehmerischen Vorgaben in Punkto Erscheinungsbild anpassbar. Die Schriften, Farben, Formen, Buttons, Anweisungen und Sprachen sind beliebig veränderbar. Es ist hiermit auch eine vollständige Integration in Unternehmens-Webseiten 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 Anpassungen bleiben selbstredend bei zukünftigen Updates erhalten!!!

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

3) **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 (Standardruleset) realisiert. Dabei wird bei jeder ausgehenden E-Mail geprüft ob

   a. ein S/MIME Schlüssel für den Empfänger existiert? Wenn ja, wird dieser vorrangig zur Verschlüsselung herangezogen.

   b. Gibt es einen OpenPGP Schlüssel, wird dieser zur Verschlüsselung verwendet.

   c. Existiert eine S/MIME Domainschlüssel von der Gegenstelle oder ein OpenPGP Domainschlüssel kommt dieser zum Einsatz.

   d. Erst wenn keine der oben genannten Standardtechnologien für den oder die Empfänger hinterlegt sind UND die E-Mail wurde als vertraulich markiert – so dass eine Verschlüsselung auf alle Fälle erzwungen wird – kommt die oben beschriebene GINA Technologie zum Einsatz.

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

4) **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, sofern diese von einer anerkannt offiziellen CA ausgestellt wurden, sofort akzeptiert. 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.

5) 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. Daher muss bei jedem zu importierenden

OpenPGP-Key auf separatem Kanal (Telefon) der Fingerprint geprüft werden. SEPPmail hat ein "umgedrehtes" Verfahren realisiert: Wenn ein Empfänger ein GINA - verschlüsseltes Mail erhält, dann hat er - in dem sich öffnenden GINA-Webmail-Portal - die Möglichkeit seinen eigenen Public-Key hochzuladen. Ihre Arbeit wird dadurch erleichtert! 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.

6) 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 Domainen 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 zB an E-Mails mit spanischen Adressen die spanische Fussnote, nach Frankreich die französische Fussnote, usw anhängen.

7) **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 und D-Trust. Weitere Konnektoren sind in Vorbereitung. Selbstverständlich werden auch alle anderen CA's (zB A-Trust, Comodo) unterstützt. Die Zertifikate können dabei per Bulkimport in die SEPPmail eingepflegt werden.

8) **Einfacher und automatisierter Betrieb:** Funktionen wie automatisiertes Schlüssel-Management (siehe Punkt 4 und 5), Domainverschlüsselung (Punkt 6), 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.

9) **Hochverfügbar als Standardfunktionalität**: Master-Master Clustering und auch Geoclustering ist als Basisfunktion verfügbar und wird mit wenigen Klicks ebenso eingerichtet wie Loadbalancing. Das Bankenrechenzentrum GRZ in Österreich betreibt

zum Beispiel einen 2x2 SEPPmail Cluster an den Standorten Innsbruck und Linz und bedienen den gesamten Mailverkehr für 14.000 Mailboxen seit Jahren ohne Probleme.

10) **Multidomain und Mandantenfähig**: Das System ist mandantenfähig, als dass sowohl mehrere Domains eingerichtet werden können, aber auch an einzelne Mandanten Verwaltungsaufgaben, wie das Account- und Usermanagement, GINA Layouting und Logging, delegiert werden können.

11) Ein Beispiel für **Akzeptanz und Verbreitung vs. 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 HIN fast eine Tochtergesellschaft von Apple sein könnte ;-)“

Eine ansehnliche Anzahl zufriedener Kunden betreiben unsere SEPPmail Lösung mit hoher Anwenderakzeptanz: www.seppmail.ch/kunden/

Die Erfahrung zeigt, dass die einfache „schnörkellose“ Anwendung für Sender und Empfänger letztendlich die hohe Akzeptanz der Lösung bei ebendiesen erreicht. 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 sehr großer Kunde mit über 100.000 GINA-Empfängerkonten. Der Supportaufwand für GINA-Erstempfänger liegt bei 6 bis 7% und Supportfälle bei GINA-Bestandsanwender liegen bei < 1% !

12) SEPPmail: Large File Management (LFM)

Jeder kennt das Problem, dass E-Mails mit zu großen Anhängen vom Empfängersystem abgelehnt werden. Die LFM 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 LFM 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 zwei Wege auf die Appliance eingeliefert werden. Entweder klassisch via E-Mail, oder auch über das standardmäßig eingebaute Webportal. Auch von außen, können große Dateien via GINA-Portal angeliefert werden.

Der Vorteil dieser Lösung liegt auf der Hand.

- Der Sender kann ohne Umwege große Dateien versenden.
- Die Daten sind verschlüsselt und werden nicht in der Cloud (wie zB bei Dropbox) zwischen gespeichert.
- Die Einladung zum Download erfolgt automatisch. Der Empfänger erkennt nur 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 man kann damit pci-compliant Infrastrukturen aufbauen!

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

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 4 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 von SwissSign (weitere Konnektoren in Vorbereitung). 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.ch über die Online Demo zustellen, oder Sie kontaktieren: info@seppmail.ch