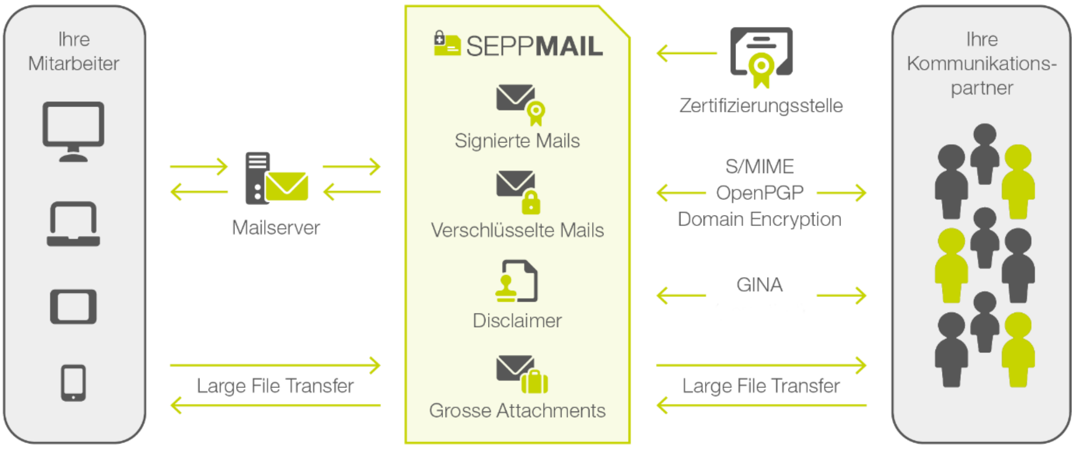


WIE KOMMUNIZIERE ICH SICHER PER E-MAIL?

SEPPMAIL

Gültig ab 01.01.2020
Version 1.2

E-MAIL-SCHUTZ DANK SEPPMAIL SERVER

Ihr Unternehmen besitzt einen SEPPmail Server welcher der automatischen Verschlüsselung des E-Mail-Verkehrs dient. Dies vereinfacht für Sie den Aufwand zur sicheren Kommunikation per E-Mail erheblich.

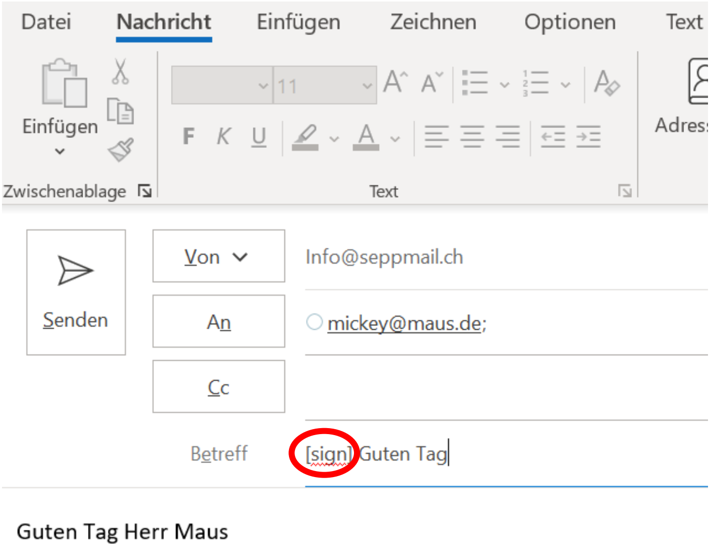
Abhängig davon was Ihr Kommunikationspartner (Empfänger) einsetzen möchte, sind vor der ersten Verschlüsselung folgende Schritte notwendig:

- Falls Ihr Empfänger S/MIME einsetzt, folgen Sie Punkt A
- Falls Ihr Empfänger OpenPGP einsetzt, folgen Sie Punkt B
- Falls Ihr Empfänger keine Verschlüsselungssoftware einsetzt, folgen Sie Punkt C
- Falls Ihr Empfänger auch einen SEPPmail Server besitzt, folgen Sie Punkt D
- Zusätzlich wird wenn möglich immer per TLS verschlüsselt, siehe Punkt E

A. DER EMPFÄNGER SETZT S/MIME ZERTIFIKATE EIN

Falls der Empfänger ein S/MIME Zertifikat besitzt, kann die Verschlüsselung nach dem S/MIME Standard erfolgen. Für dies sind folgende Schritte notwendig:

- Der Empfänger sendet Ihnen eine mit seinem Zertifikat signierte E-Mail. Der SEPPmail Server extrahiert aus diesem E-Mail automatisch den Schlüssel und verschlüsselt fortan jede E-Mail aus Ihrem Unternehmen an diesen Empfänger.
- Sofern Ihr Unternehmen für die Mitarbeiter Zertifikate ausstellt, funktioniert auch die Gegenrichtung. Wenn der Empfänger also Ihnen auch verschlüsselte E-Mails senden soll, senden Sie ihm ein E-Mail, die mit dem Betreff „[sign]“ beginnt und er erhält automatisch Ihren S/MIME Schlüssel.



Von: Info@seppmail.ch

An: mickey@maus.de;

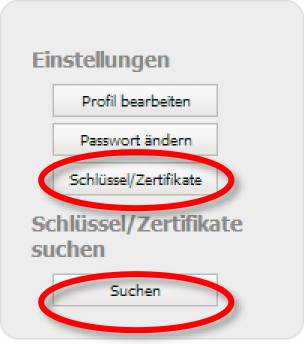
Betreff: [sign] Guten Tag

Guten Tag Herr Maus

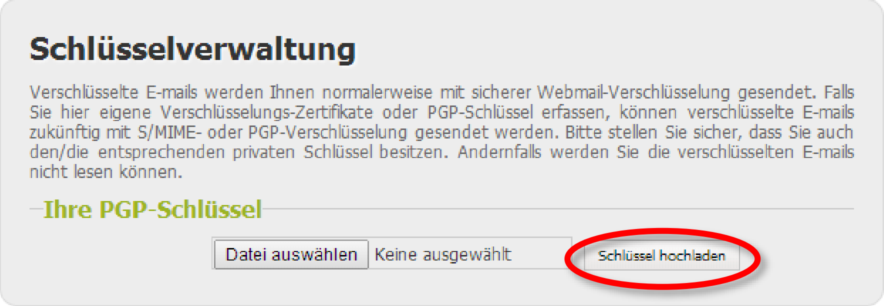
B. DER EMPFÄNGER SETZT OPENPGP VERSCHLÜSSELUNG EIN

Falls der Empfänger ein OpenPGP kompatible Software einsetzt, kann die Verschlüsselung nach dem OpenPGP Standard erfolgen. Für dies sind folgende Schritte notwendig:

- Senden Sie dem Empfänger ein verschlüsseltes E-Mail (sog. GINA Mail) gemäss Punkt C
- Der Empfänger erhält ein Mail mit Login. Das Passwort teilen Sie ihm mit.
- Nachdem der Empfänger eingeloggt hat, erscheint das entschlüsselte Mail. Auf der rechten Seite unter „Einstellungen“ kann er zudem einerseits seinen eigenen OpenPGP Schlüssel hochladen und andererseits fremde OpenPGP Schlüssel suchen.



- Per Klick auf „Schlüssel/Zertifikate“ erscheint ein Formular mit dem der Empfänger seinen eigenen OpenPGP Schlüssel als Datei hochladen kann.
- Jede E-Mail, die ab diesem Zeitpunkt an ihn verschickt wird, wird mit diesem Schlüssel verschlüsselt.



Verschlüsselte E-mails werden Ihnen normalerweise mit sicherer Webmail-Verschlüsselung gesendet. Falls Sie hier eigene Verschlüsselungs-Zertifikate oder PGP-Schlüssel erfassen, können verschlüsselte E-mails zukünftig mit S/MIME- oder PGP-Verschlüsselung gesendet werden. Bitte stellen Sie sicher, dass Sie auch den/die entsprechenden privaten Schlüssel besitzen. Andernfalls werden Sie die verschlüsselten E-mails nicht lesen können.

- Durch Klicken auf „Suchen“ erhält er zudem den vom SEPPmail Server für Sie persönlich generierten OpenPGP Schlüssel, indem er Ihre E-Mail-Adresse ins Suchfeld eingibt.

Sie können nach den Schlüsseln/Zertifikaten anderer Benutzer suchen, indem Sie deren E-mail-Adresse eingeben.

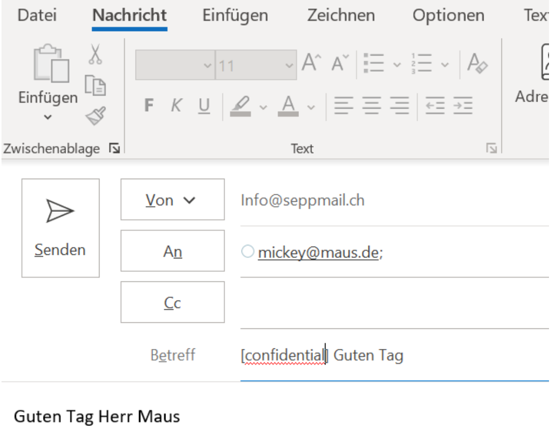
User ID: Stefan Klein <klein@seppmail.ch>
Schlüssel ID: DD02C094539673AA

- Diesen persönlichen öffentlichen Schlüssel von Ihnen kann er dann herunterladen und Ihnen somit auch verschlüsselte Nachrichten senden. Diese werden vom SEPPmail Server automatisch entschlüsselt.

C. DER EMPFÄNGER SETZT KEINE VERSCHLÜSSELUNGSSOFTWARE EIN

Falls der Empfänger keine Verschlüsselungslösung besitzt, können Sie ihm dank SEPPmail trotzdem verschlüsselte E-Mails senden. Es sind die sogenannten GINA-Mails, eine Technologie, bei der der Empfänger keinen speziellen Schlüssel benötigt. Für dies sind folgende Schritte notwendig:

- Senden Sie Ihr E-Mail an den Empfänger und starten Sie im Betreff mit „[confidential]" oder markieren Sie die E-Mail in Outlook als „Vertraulich"

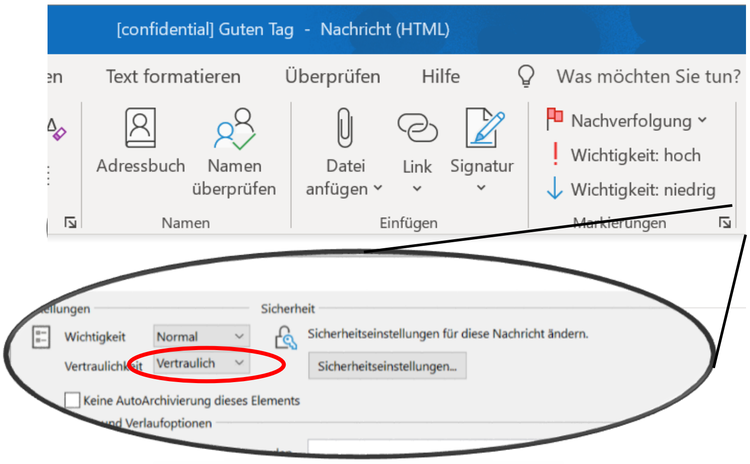


Von: Info@seppmail.ch

An: mickey@maus.de;

Betreff: [confidential] Guten Tag

Guten Tag Herr Maus

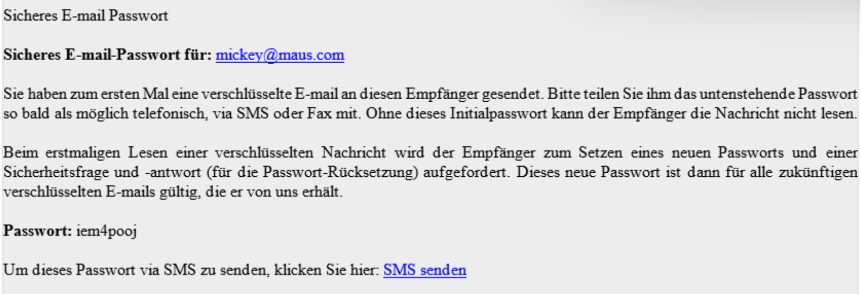


[confidential] Guten Tag - Nachricht (HTML)

Wichtigkeit: Normal

Vertraulichkeit: Vertraulich

- Falls dies die erste verschlüsselte E-Mail an den Empfänger war, bekommen Sie eine E-Mail mit seinem Passwort. Dieses übermitteln Sie Ihrem Empfänger entweder per Telefon oder SMS.



Sicheres E-mail Passwort

Sicheres E-mail-Passwort für: mickey@maus.com

Sie haben zum ersten Mal eine verschlüsselte E-mail an diesen Empfänger gesendet. Bitte teilen Sie ihm das untenstehende Passwort so bald als möglich telefonisch, via SMS oder Fax mit. Ohne dieses Initialpasswort kann der Empfänger die Nachricht nicht lesen.

Beim erstmaligen Lesen einer verschlüsselten Nachricht wird der Empfänger zum Setzen eines neuen Passworts und einer Sicherheitsfrage und -antwort (für die Passwort-Rücksetzung) aufgefordert. Dieses neue Passwort ist dann für alle zukünftigen verschlüsselten E-mails gültig, die er von uns erhält.

Passwort: iem4pooj

Um dieses Passwort via SMS zu senden, klicken Sie hier: SMS senden

Alternativ können Sie der im Punkt 1 verschickten E-Mail gleich die Mobilenummer des Empfängers mitgeben, in dem Sie in der Betreffzeile „(sms: +49123456789)" hinzufügen. Dieser Text wird dann entfernt und das Passwort automatisch per SMS geschickt.

- Der Empfänger erhält die verschlüsselte E-Mail und kann diese nach Eingabe des Passwortes entschlüsseln. Im gleichen Fenster, wo er die entschlüsselte E-Mail liest, hat er die Möglichkeit Ihnen verschlüsselt zu antworten.

- Jede weitere vertrauliche E-Mail aus Ihrer Firma an den Empfänger, wird automatisch verschlüsselt und er kann sie mit diesem Passwort wieder lesen. Natürlich kann er dieses Passwort jederzeit ändern.

D. DER EMPFÄNGER BESITZT EINEN SEPPMAIL SERVER

Falls der Empfänger in einem Unternehmen tätig ist, das auch den SEPPmail Server zur automatischen Verschlüsselung einsetzt, braucht niemand etwas zu tun. Der SEPPmail Server erkennt automatisch den SEPPmail Server auf der Gegenseite und verschlüsselt den gesamten E-Mail-Verkehr zwischen den beiden Unternehmen.

E. WENN MÖGLICH TLS VERSCHLÜSSELUNG

Die Kommunikation zwischen dem SEPPmail Server und anderen E-Mail-Servern wird zusätzlich in der Standardkonfiguration immer über einen TLS/SSL gesicherten Kanal aufgebaut, sofern die Gegenstelle dies unterstützt. TLS/SSL bietet eine zusätzliche Sicherheit und ergänzt die bisher beschriebenen Verschlüsselungsmethoden.

Dank SEPPmail können Sie somit mit allen Empfängern verschlüsselt kommunizieren, unabhängig davon welche Verschlüsselungstechnologien Ihr Gegenüber einsetzen möchte. Wir wünschen Ihnen viel Vergnügen in der sicheren Kommunikation.