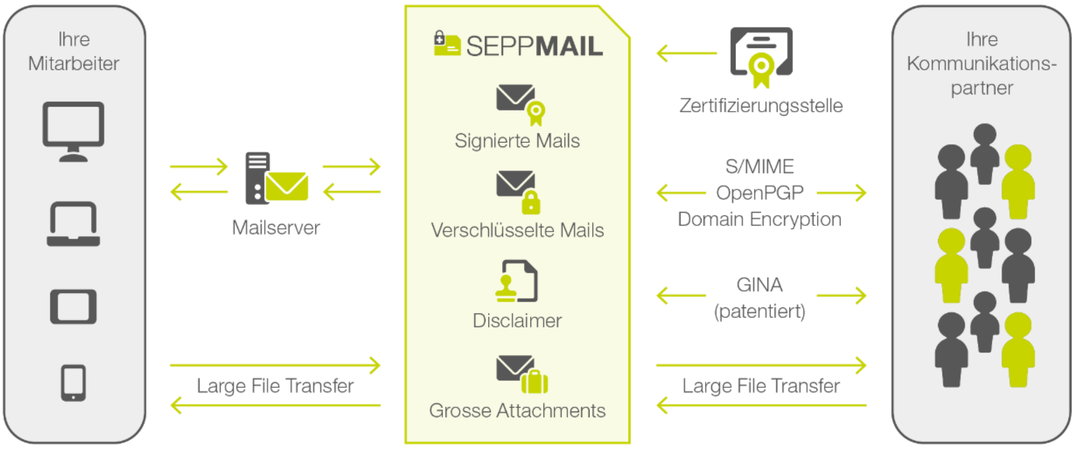


HOW DO I SEND E-MAILS SECURELY?

SEPPMAIL

Gültig ab 01.01.2020
Version 1.2

EMAIL PROTECTION WITH SEPPMAIL SERVER

Your company has a SEPPmail server which is used to automatically encrypt emails. This greatly simplifies the process for ensuring secure email communications.

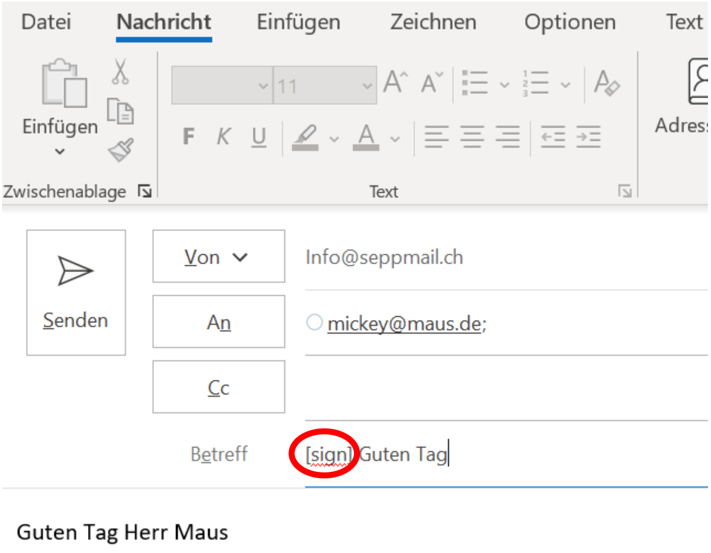
Depending on the recipient's situation, the following procedures are required before using encryption for the first time:

- If your recipient is using S/MIME, follow the instructions under A
- If your recipient is using OpenPGP, follow the instructions under B
- If your recipient is not using any encryption software, follow the instructions under C
- If your recipient also has a SEPPmail server, follow the instructions under D
- TLS encryption is also used whenever possible. See E

A. THE RECIPIENT IS USING S/MIME CERTIFICATES

S/MIME standard encryption can be used if the recipient has an S/MIME certificate. Follow these steps to do so:

- The recipient sends you a digitally signed email with their certificate. The SEPPmail server automatically extracts the key from this email. From then on, the key will be used to encrypt every email your company sends to this recipient.
- If your company issues certificates for colleagues, the process also works in the other direction. If you want the recipient to send you encrypted emails as well, send them an email



Von: Info@seppmail.ch

An: mickey@maus.de;

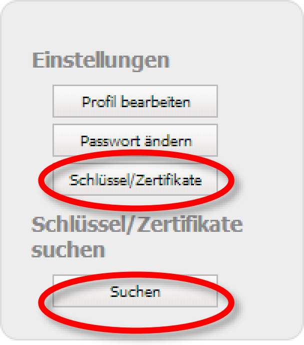
Betreff: [sign] Guten Tag

Guten Tag Herr Maus

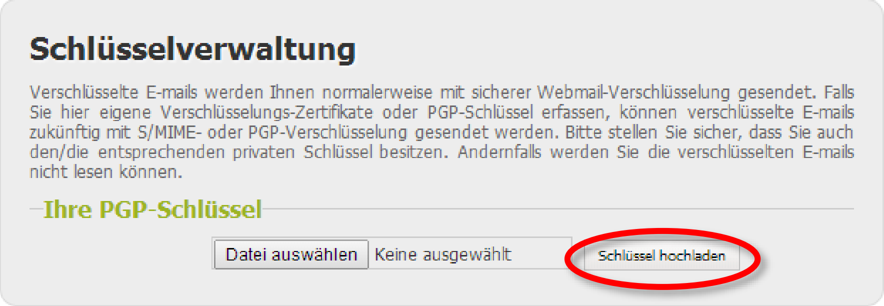
B. THE RECIPIENT IS USING OPENPGP ENCRYPTION

You can use OpenPGP standard encryption if the recipient is using OpenPGP-compatible software. Follow these steps:

- Send the recipient an encrypted email (a GINA mail) as described under C
- The recipient will receive an email with login details. You provide them with the password.
- The encrypted email appears after the recipient has logged in. On the right-hand side under Settings, the recipient can also upload their own OpenPGP key and search for the OpenPGP keys of other recipients.



- Clicking on Keys/certificates opens a form that enables the recipient to upload a file containing their own OpenPGP key.
- From then on, every email sent to the recipient will be encrypted using this key.



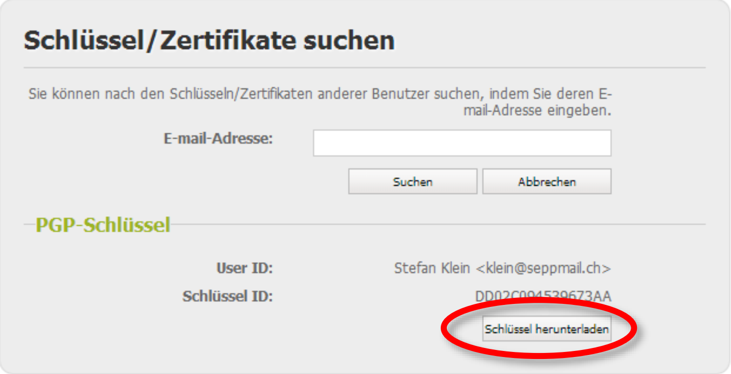
Schlüsselverwaltung

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.

Ihre PGP-Schlüssel

Datei auswählen: Keine ausgewählt

- Clicking on Search and then entering your email address in the search box provides the recipient with your individual OpenPGP key as was generated by the SEPPmail server.



Schlüssel/Zertifikate suchen

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

E-mail-Adresse:

PGP-Schlüssel

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

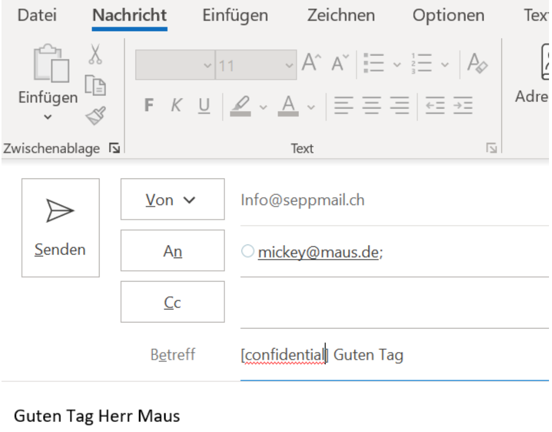
Schlüssel ID: DD02C094539673AA

- The recipient can then download your individual public key and use it to send you encrypted emails. The emails are automatically decrypted by the SEPPmail server.

C. THE RECIPIENT IS NOT USING ANY ENCRYPTION SOFTWARE

If the recipient is not using any encryption solution, SEPPmail still allows you to send them encrypted emails. These are what are known as GINA mails, which are sent using a patented technology that does not require the recipient to have a special key. Follow these steps:

- Send your e-mail tot he recipient with a subject line beginning with [confidential] or mark the email in Outlook as confidential

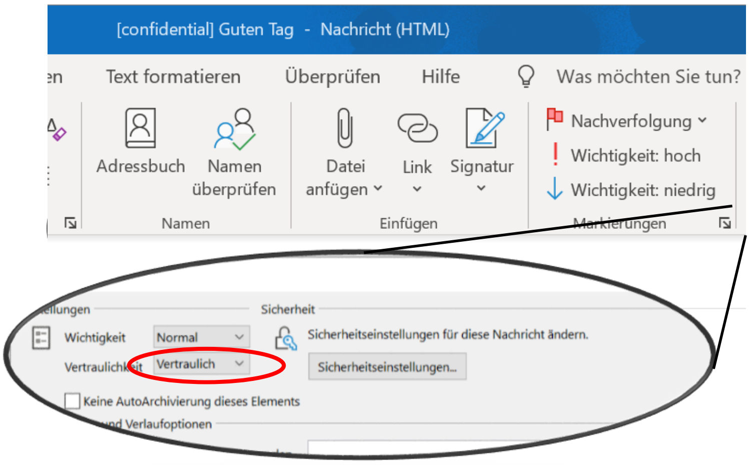


Von: Info@seppmail.ch

An: mickey@maus.de;

Betreff: [confidential] Guten Tag

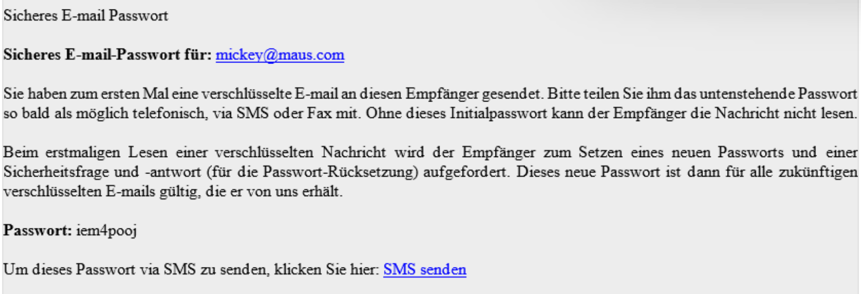
Guten Tag Herr Maus


[confidential] Guten Tag - Nachricht (HTML)

Wichtigkeit: Normal

Vertraulichkeit: Vertraulich

- The first time an encrypted email is sent to the recipient, you will receive an email containing their password. You then communicate this password to them by phone or 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

Alternatively, you can include the mobile phone number of the recipient in the email described under 1 by adding '(SMS: +49123456789)' to the subject line. This text will then be removed and the password sent automatically via text message/SMS.

- The recipient receives the encrypted email and can then decrypt it by entering the password. The recipient can also send an encrypted response in the same window as the decrypted email.

- Each additional confidential email your company sends to the recipient will be encrypted automatically and can be read by entering this password. The recipient has the option to change this password at any time.

D. THE RECIPIENT IS USING AN SEPPMAIL SERVER

If the recipient is part of a company that is also using the SEPPmail server to automatically encrypt emails, neither party needs to do anything. The SEPPmail server automatically recognizes the SEPPmail server at the other end and encrypts all emails sent between the two companies.

E. TLS ENCRYPTION WHENEVER POSSIBLE

In addition, communication between the SEPPmail server and other email servers is always handled via a TLS/SSL-secured channel in the standard configuration if this is supported at the other end. TLS/SSL offers extra security to complement the encryption methods described above.

SEPPmail therefore enables you use encrypted communication with all recipients, regardless of the encryption technology the other party wishes to use. We wish you all the best with your secure communications.