RMAIL FACTSHEET

EMAIL ENCRYPTION

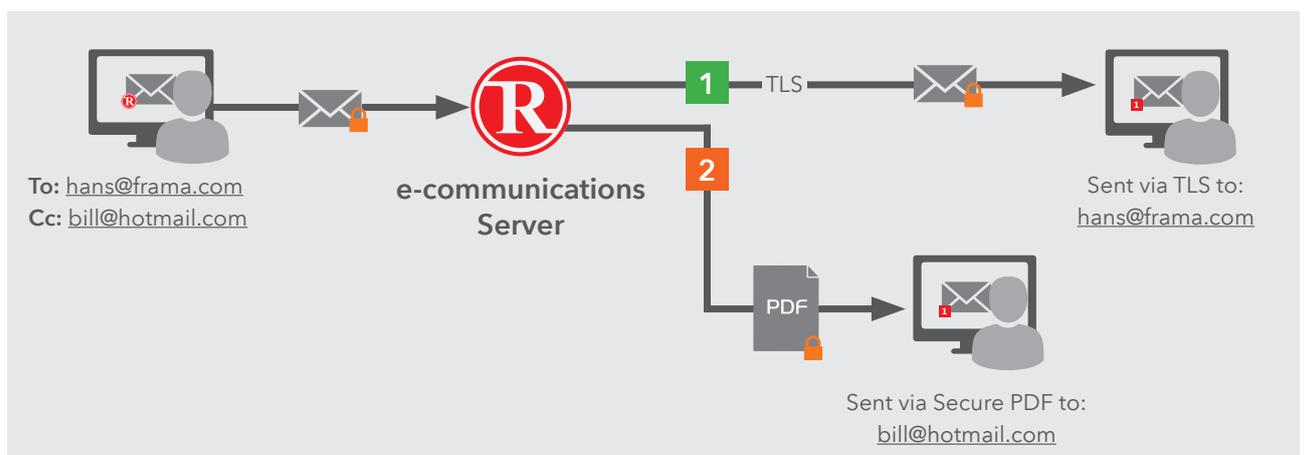## Encryption with RMail: Auto-TLS with password fallback option

Simplest integration with proof of compliance: The Auto-TLS encryption of RMail ensures that confidential information stays confidential. Thanks to Secure Reply, recipients can reply encrypted from any platform. This allows secure communication in both directions without any obstacles. RMail enables you to encrypt email messages with just a single mouse click and allows you to implement the encryption process in your current workflow. The Registered Receipt shows the encryption method used for sending. It also protocols the encrypted transmission to the recipient's server. No exchange of certificates or any kind of registration by the recipient is required. RMail works with any email program.

The workflow is easy and simple. For each encrypted email sent, the availability of TLS gets checked by the e-communications system for the entire transaction path. If TLS once is not available, the RMail server converts the encrypted message into a Secure PDF and delivers this password-protected PDF file to the recipient's inbox via standard email. Auto-TLS can be set as default in the user account.

General Data Protection Regulation (GDPR)

It's not very difficult to encrypt emails. The market offers a variety of solutions for this. But why are so many emails containing personal data still sent without encryption? The answer: It is difficult to find a solution that is easy to use with all email clients and at the same time is accepted by the recipients.
RMail works with any common email client on the recipient's side (high user experience) and is easy to implement into your current email program. RMail provides one-click-encryption (GDPR article 5, paragraph 1f and article 32, paragraph 1) in combination with the Registered Receipt, which documents compliance to GDPR article 5, paragraph 2.

To: hans@frama.com
Cc: bill@hotmail.com

e-communications Server

1 TLS

Sent via TLS to:
hans@frama.com

2

PDF

Sent via Secure PDF to:
bill@hotmail.com

1 **TLS available:** The message is delivered encrypted to the recipient server using a secure tunnel. The email is shown in standard email format with markings so the recipient knows it was transmitted securely and contains sensitive or protected information.

2 **TLS not available:** If TLS is unavailable, the message is securely transmitted via Password Mode as an AES 256bit encrypted PDF.

Functions

For reasons of security and compliance, companies are increasingly relying on email encryption by RMail. The service not only contributes to the protection of sensitive data, but is proven to reduce costs and increases customer satisfaction. RMail offers a unique combination of features, including:

- Automatic TLS encryption with a record of GDPR compliant delivery.

- Straight-through encrypted delivery. No temporary storage, click-throughs or downloads.

- Compliance of transmission is recorded by the unique Registered Receipt.

- No end-user encryption keys; option to auto-deliver decryption passwords.

- Keep using your current email address, no web mailer.

- Optional encrypted replies back to the sender via pre-configured web mailer (no user account needed!).

Secure Reply

Recipients are able to reply encrypted by clicking the "Secure Reply" button.
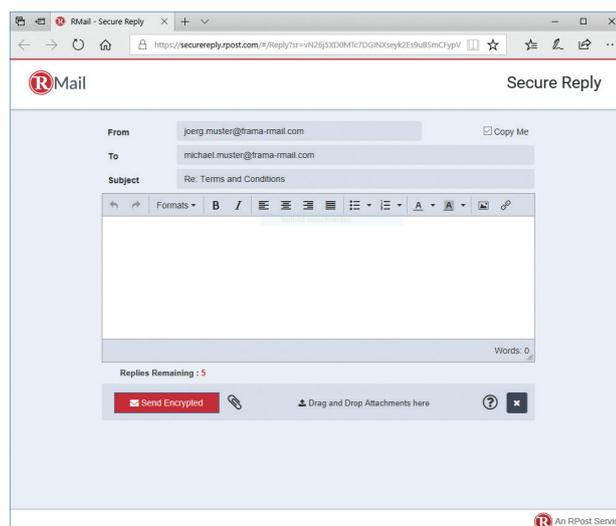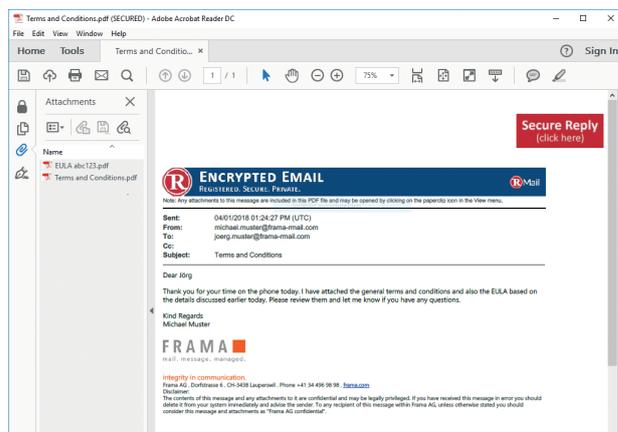
Your Benefits

Compliance	Compliance Record: The Registered Receipt is your proof of compliance with the General Data Protection Regulation (in terms of article 5, paragraph 1f, 2 and article 32, paragraph 1).
Easy to use	RMail can easily be integrated into your workflow - automated or manual: A maximum of two additional clicks are required and the confidentiality of the message is ensured. Best of all, no knowledge or actions on the recipient end are required to read an encrypted message.
Increased efficiency	Your employees do not need any additional web accounts or software to manage the sending and retrieving of encrypted email messages. All emails are archived centrally. There is no longer any need to print and store physical copies of confidential documents.

integrity in communication.