Product Overview: totemomail® End-to-End Encryption

Sometimes keeping a message confidential is given higher priority than protecting the communication partners from threats such as malware and spam. This is where end-to-end encryption comes into play. Messages do not get decrypted at the gateway, which is usually undertaken in order to detect threats.

With **totemo**mail® End-to-End Encryption, messages are encrypted in the sender's mailbox and only decrypted once they reach the recipient's mailbox. The solution uses an innovative approach and for the first time enables end-to-end encryption without the use of plug-ins.

totemomail® End-to-End Encryption works with the email encryption standard S/MIME and can be operated either with **totemo**mail® Encryption Gateway and/or **totemo**mail® Internal Encryption or as a stand-alone.

How It Works

Until now, using end-to-end encryption with communication partners outside the enterprise without deploying plug-ins at the same time was often doomed to fail. This was due to the inability of the sender's email client to validate the certificate chain of the recipient's public key during message encryption. **totemo**mail® End-to-End Encryption solves this problem with an innovative approach that makes the recipient's certificate verifiable.

Internal Sender – Internal Recipient

End-to-end encryption without plug-ins for communication with internal partners was already possible with S/MIME. This is because there is no need for central data flow management since the email never leaves the company network.

Internal Sender – External Recipient

Messages for external communication partners are encrypted directly in the sender's mailbox. **totemo**mail® checks if there is an existing user profile for the external recipient that contains the required S/MIME certificates.

If the **software finds an entry for the recipient**, the email is encrypted/signed with the existing keys and sent to the recipient.

If **there is no entry for this external recipient**, an email is automatically sent to the recipient to initiate the registration process. The recipient replies to the email with a signed message using their S/MIME certificate. **totemo**mail® validates the certificate and stores it in the recipient's user profile. The original message is meanwhile retained until the user is registered. It is then signed/encrypted and sent.

External Sender – Internal Recipient

S/MIME encrypted emails from external communication partners are delivered to the internal recipient's mailbox where they are decrypted.

Key Facts

Highest security for particularly sensitive data

With **totemo**mail® End-to-End Encryption, your sensitive messages are encrypted without any decryption whatsoever taking place during the entire transfer.

Standard-based process without plug-ins

totemomail® End-to-End Encryption's special feature is encrypting end-to-end without requiring the installation of specific email clients or plug-ins – neither for co-workers nor external communication partners. In order to achieve this, the solution is based on the proven email encryption standard S/MIME, which is integrated natively into all commonly used email clients. Moreover, **totemo**mail® utilizes an innovative approach that makes the certificate of the recipient verifiable.

Benefits

Organizational benefits

- End-to-end protection for extremely sensitive communication
- Encryption with S/MIME
- The requirement for end-to-end encryption can be defined on a per-user basis

totemo ag

Freihofstrasse 22, CH-8700 Küsnacht, info@totemo.com, www.totemo.com, T +41 44 914 99 00, F +41 44 914 99 99

Administration benefits

- Easy integration into existing IT infrastructure
- No installation of specific email clients or plug-ins necessary – neither for co-workers nor external communication partners
- Automatic generation and management of certificates
- Graphical user interface for administration console
- Granular definition of user roles
- No user training necessary due to transparent handling

User benefits

- Easy and secure communication with internal and external partners
- Work processes and software remain unaffected by implementation, no need to learn new software program
- Consistent observance of security policies and compliance standards