Solution Overview: totemomail® Internal Encryption

totemomail® **Internal Encryption is an innovative FIPS 140-2-validated module that protects sensitive emails within an organization's network all the way from sender to recipient. It is able to encrypt messages not only on workstations, but also on laptops and mobile devices based on iOS and Android. Accordingly, companies protecting their emails with totemo**mail® **Internal Encryption are thoroughly prepared for BYOD strategies. Moreover, the module neither requires additional software nor plugins for email clients and thus seamlessly integrates into any existing email environment.**

totemomail® Internal Encryption can be run in combination with the **totemo**mail® Encryption Gateway or as a stand-alone product.

How It Works

Traditional gateways encrypt and decrypt emails between the gateway and the external recipient. But within the company network, confidential messages remain unprotected and fully readable for unauthorized third parties. With a conventional solution, this issue can only be addressed through end-to-end encryption. However, this calls for extra software components, proprietary email protocols or encrypted connections. Thus the company loses control over its email security: central spam and virus filtering or content scanning can no longer be ensured. **totemo**mail® Internal Encryption solves these gateway concept issues while preserving the advantages of a server-based approach. For the module is able to automatically collect and manage keys and certificates. Moreover, the company security policies are centrally defined and applied to the messages.

When communicating with an internal partner, the message is encrypted via S/MIME directly in the sender's email client and delivered to the recipient by the company email server. The recipient's email client decrypts the email and thus makes it readable again. In this case, there is no need for central data flow control since the email never leaves the company network.

Communication with external partners remains secure due to de facto end-to-end encryption between the device and the gateway. At the gateway, the message encrypted directly in the sender's email client is decrypted and undergoes the company's usual security checks. This protects the encrypted emails not only against external attacks, but also against curious co-workers and administrators. Before transmission, the gateway converts the confidential email into the recipient's preferred encryption technology (e.g. WebMail, *Pushed*PDF, S/MIME or OpenPGP).

Emails sent by external partners - whether encrypted or not - are also processed according to the company's predefined security guidelines. After inspection at the gateway, they are encrypted with S/MIME and delivered to the recipient.

Key Facts

Internal Encryption on Desktops

totemomail® Internal Encryption is able to independently generate certificates for business partners and customers. Thus messages can be directly encrypted in every email client, which keeps email communication secure with any given internal or external partner. Moreover, the need to integrate third-party products is eliminated. This substantially simplifies solution installation, operation and support.

Internal Encryption on Mobile Devices with ActiveSync

totemomail® Internal Encryption adds certificate management functionalities to the Exchange ActiveSync protocol. This enhancement sustainably facilitates the implementation of BYOD strategies. Combined with **totemo**mail®'s automatic certificate distribution, this provides a comprehensive solution for email encryption on smartphones and tablets. iPhones and iPads as well as Android-based devices are thus able to send and process both internally and externally encrypted messages. Users will go on working with their device's standard email client. No extra software component nor apps need to be installed.

Internal Encryption with BlackBerry® Devices

In combination with the S/MIME Support Package (SSP) by BlackBerry®, **totemo**mail® Internal Encryption is able to encrypt all communication between the email client and the BlackBerry®. Device integration works rapidly and in analogy to that of an internal email client. Thus SSP and the user's private key need to be stored on the device. Once these requirements are fulfilled, the BlackBerry® can send and receive encrypted messages by any given internal and external communication partner.

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

Benefits

Organization

- Exchange of encrypted emails with internal communication partners, business partners and customers even without an encryption technology of their own
- Security and efficiency due to high level of automation
- Centralized encryption and decryption as well as application of security policies and compliance standards
- Investment protection and strategic freedom through numerous interfaces with third-party systems
- Security checks such as virus control, content scanning, anti-spam protection etc. remain ensured

Administration

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

User

- Secure and flexible communication with internal and external partners
- Work processes and software remain unaffected by implementation
- Consistent observance of security guidelines and compliance standards

Architecture

totemomail® Internal Encryption can be used in combination with the **totemo**mail® Encryption Gateway as the high-performing and innovative hybrid solution **totemo**mail® Hybrid Encryption.

The module also runs independently from the **totemo**mail® Encryption Gateway as a stand-alone product to secure all internal emails. Secure communication with external partners is also possible directly out of the email client – without additional software or plugins – using pro-forma certificates.