totemomail®

Solution Overview: totemomail® Hybrid Encryption

Guess who is the biggest threat to your business's data security: It's your staff. They have access to all kinds of sensitive information. However, they do not always have the necessary tools or know-how to securely exchange these with colleagues or external communication partners. But high-quality data is a crucial factor for company success. It therefore needs to be consistently protected against unauthorized access.

Extensive staff training regarding the correct handling of sensitive data is expensive and time-consuming. Implementing complex procedures to secure confidential information is a drag on productivity. Despite these measures, it remains impossible to rule out inadvertent mistakes or errors of reasoning. Moreover, the relevant laws and regulations are constantly revised. That is why an easy-to-handle technical solution that does not require additional software nor affect employee routines is your best bet to protect sensitive data. In this manner, internal security guidelines and legally prescribed compliance standards can be centrally defined, applied and logged.

A hybrid encryption solution secures the transmission of confidential emails all the way from sender to internal or external recipient. For sensitive information can fall into the wrong hands within the company network as well as through communication with customers and business partners. To prevent this, we developed the FIPS 140-2-validated, high-performing and innovative comprehensive solution **totemo**mail® Hybrid Encryption. It seamlessly integrates into any existing IT infrastructure and consists of the **totemo**mail® Encryption Gateway and the module **totemo**mail® Internal Encryption, which is also available as a stand-alone product.

totemomail® Hybrid Encryption is compatible with a variety of third-party systems and offers all automatized core functionalities of the gateway: e.g. encrypted transmission of confidential emails to external recipients including delivery confirmation, sender identification, guaranteed message integrity as well as message non-repudiation.

Confidential messages to internal recipients are encrypted directly within the sender's native email client. Neither additional software nor plugins are needed. Internal encryption also works on laptops, tablets and smartphones based on iOS, Android and BlackBerry®.

How It Works

totemomail® Hybrid Encryption reduces operation costs, administrative load and inadvertent mistakes to an absolute minimum through its high level of automation. All electronic messages are centrally encrypted and decrypted and company security guidelines are automatically applied to the emails. Even the enrollment of both external and internal users takes place automatically.

When communicating with an internal partner, the message is encrypted 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.

Messages to external partners are decrypted at the gateway and undergo the company's usual security checks. Therafter, they are re-encrypted and delivered according to the recipient's preferences.

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 internally encrypted and delivered to the recipient.

Key Facts

Automatized Certificate and Key Management

totemomail® Hybrid Encryption's core function is its automatized certificate and key management. Through automatized user enrollment, the solution independently collects the existing certificates and keys and saves them encrypted in the key store. Amongst other parameters, settings for certificate and key checks, validation and validity period can be defined.

Automatized User Enrollment

totemomail® Hybrid Encryption independently identifies new internal and external users and enrolls them without any manual intervention by the sender or the administrator. For first-time recipients, the solution retains the original message until they are successfully authenticated.

Defining Security Policies

The company security policies as well as the corresponding email workflows are defined in the administration console. The console allows a virtually infinite combination of complex rules as well as their automatized application such as the encryption of any message sent to a specific domain.

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 via Graphic User Interface

totemomail® Hybrid Encryption offers a web-based administration console with a graphic user interface, a dashboard and a message tracking center. No programming skills are required to define the security guidelines for email workflows. The administration of the whole solution can be shared between several employees.

Comprehensive Automatized Reporting

totemomail® Hybrid Encryption offers comprehensive reporting capabilities. The required reports are delivered in scheduled intervals to the defined recipients. The reporting settings can be comfortably configured and managed in the administration console.

Enhanced Observance of Compliance Standards

For internal and external audits, complete and easily searchable records of all compliance-related actions are needed. **totemo**mail® Hybrid Encryption caters to that need by providing auditable log files, a read-only role for audit users and enhanced tracking functionalities.

Benefits

Organization

- Flexible and secure email communication with external partners with or without an encryption technology of their own
- Security and cost-efficiency due to high level of automation
- Central 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
- Internal encryption with S/MIME
- 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
- Automatic generation and management of personal certificates
- Graphic user interface for administration console
- Granular user role definition
- No user training necessary due to transparent handling

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

Modules

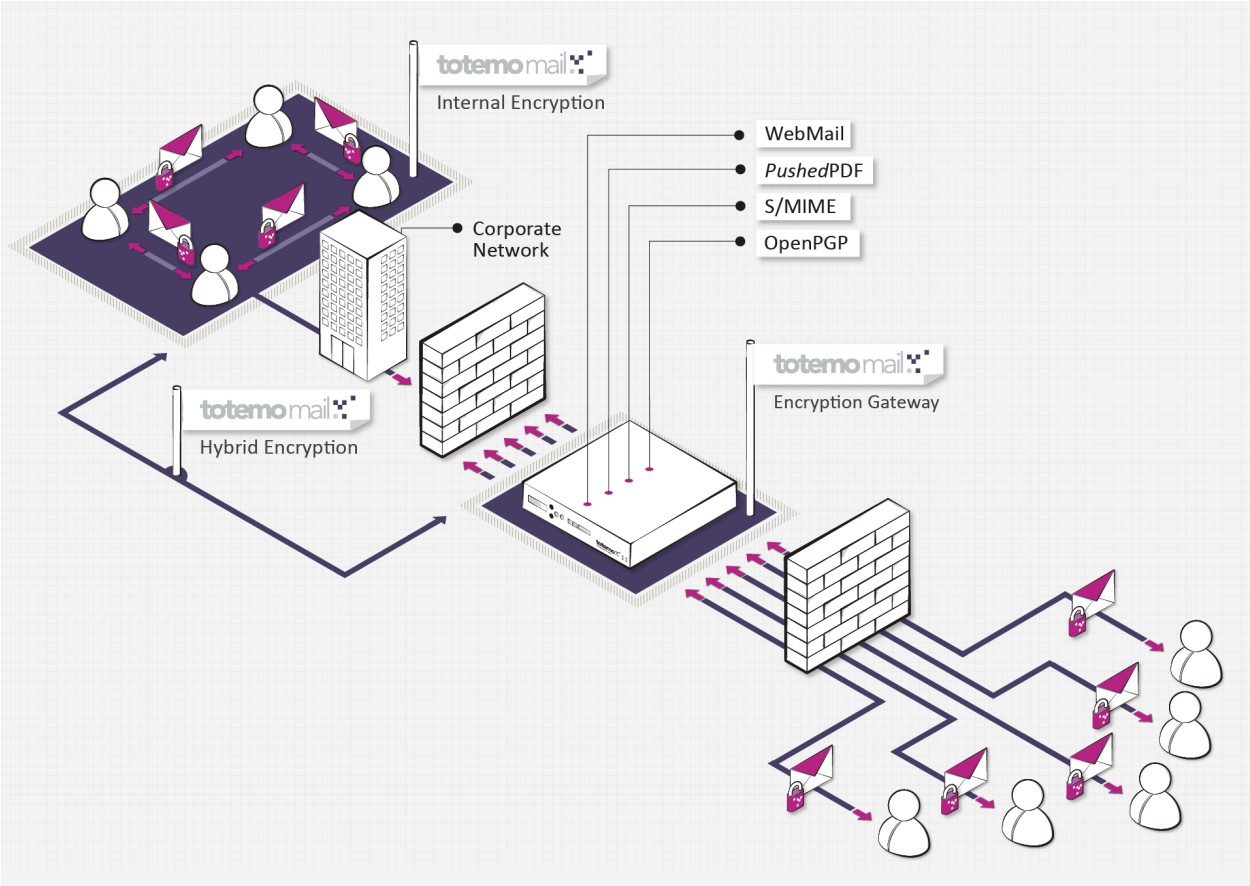
totemomail® Hybrid Encryption consists of the following modules:

- **totemo**mail® Encryption Gateway
  - *Option 1:* **totemo**mail® WebMail
  - *Option 2:* **totemo**mail® *Pushed*PDF
- **totemo**mail® Internal Encryption

totemomail® WebMail und **totemo**mail® *Pushed*PDF are two different technologies for encrypted email communication with external partners. The module **totemo**mail® Internal Encryption can also be run as a stand-alone product to secure your organization's internal electronic communication.

Architecture

The **totemo**mail® Hybrid Encryption solution ensures the de facto end-to-end encryption of all confidential messages. The hybrid solution communicates directly with all current email clients. Thus neither your employees nor your customers and business partners need to install additional components.


totemo mail
Internal Encryption
WebMail
PushedPDF
S/MIME
OpenPGP
Corporate Network
totemo mail
Encryption Gateway
totemo mail
Hybrid Encryption