Solution Overview: **totemo**mail® 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 maintaining the confidentiality of business data is crucial to gain a competitive advantage and thus, for your company's success. Therefore, information 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 unintended errors. 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. With the use of such a solution, internal security policies and mandatory 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 **totemo**mail® Encryption Gateway and **totemo**mail® Internal Encryption.

How It Works

Internal Sender – Internal Recipient

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.

Internal Sender – External Recipient

Messages are encrypted directly in the sender's email client to ensure its confidentiality along the email's route within the company network. At the company gateway, the message is decrypted and undergoes the company's usual security checks.

Thereafter, the gateway converts the email into the recipient's preferred encryption technology and sends it, completing the followings steps:

totemomail® Hybrid Encryption checks if there is a user profile for this external recipient stored in an encrypted database.

If the **software finds an entry for the recipient**, the email is encrypted/signed and sent according to the existing user profile, which also contains information on the user's preferred encryption method.

As an option, the software can automatically perform a search on key servers for existing public OpenPGP or S/MIME keys.

If **there is no entry for this external recipient**, an email is automatically sent to the recipient to initiate the registration process. The recipient is registered and authenticated through this process. He can also establish a preferred method for receiving encrypted messages.

The original message is retained and remains encrypted until the user is authenticated. Thus the solution ensures that sensitive information does not leave the company network unprotected.

The methods are different depending on whether or not the recipient uses a specific encryption technology.

If the **recipient uses one of the standard email encryption technologies** such as S/MIME or OpenPGP, he replies to the email with a signed message using one of his own certificates or attaches his public OpenPGP key to the email. **totemo**mail® Hybrid Encryption validates the key and stores it in the user profile. The original email is accordingly encrypted and sent to the recipient.

In case the **recipient does not use an encryption technology of his own**, **totemo**mail® Hybrid Encryption offers **totemo**mail® WebMail, **totemo**mail® Registered Envelope, and **totemo**mail® *Pushed*PDF as secure alternative delivery methods.

External Sender – Internal Recipient

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

Automated Certificate and Key Management

totemomail® Hybrid Encryption's core function is its automated certificate and key management. The company certificate policies can be easily and comprehensively configured using the graphical user interface of the administration console.

Among other things, you can define the settings for trustworthy certificate authorities (CA), the online validation of certificates, the required attributes for certificate and key checks as well as the validity period of certificates generated by **totemo**mail®.

By means of the automatic user enrollment feature or request to a key server, the software independently collects and encrypts the certificates and keys already available, and then saves them within the key store. **totemo**mail® Hybrid Encryption's incorporated PKI component is able to generate, distribute and manage certificates for both internal and external communication partners, enabling their quick and efficient integration.

Alternatively, **totemo**mail® Hybrid Encryption can be connected to an external PKI solution or CA via one of the integrated standard interfaces.

Automated User Enrollment

totemomail® Hybrid Encryption independently identifies internal and external users and enrolls them without any manual intervention by the sender or an administrator. Thus the administrative load is kept as low as possible.

For first-time recipients, **totemo**mail® Hybrid Encryption retains the original message until they are successfully authenticated. Then they receive the message as one of the following options: as regular email digitally signed and encrypted with the matching key, via **totemo**mail® WebMail, as **totemo**mail® Registered Envelope message, or as **totemo**mail® *Pushed*PDF message.

Administration via Graphical User Interface

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

Defining Security Policies

The company security policies as well as the corresponding email workflows are defined in the administration console. It allows a virtually infinite combination of complex rules as well as their automated application such as the encryption of any message sent to a specific domain. Along with the integrated group management, even functional mailboxes, escalation procedures, etc. can be easily configured and applied.

Comprehensive Automated Reporting

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

Enhanced Observance to Compliance Standards due to Auditability

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

Benefits

Organizational benefits

- Flexible and secure email communication with internal partners as well as external partners with or without an encryption technology of their own
- Internal encryption with S/MIME
- Security and cost-efficiency due to high level of automation and ease-of-use
- Central encryption and decryption of emails
- Central definition and application of security policies and compliance standards
- Investment protection and strategic freedom through numerous interfaces with third-party systems

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 personal 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

Available Modules

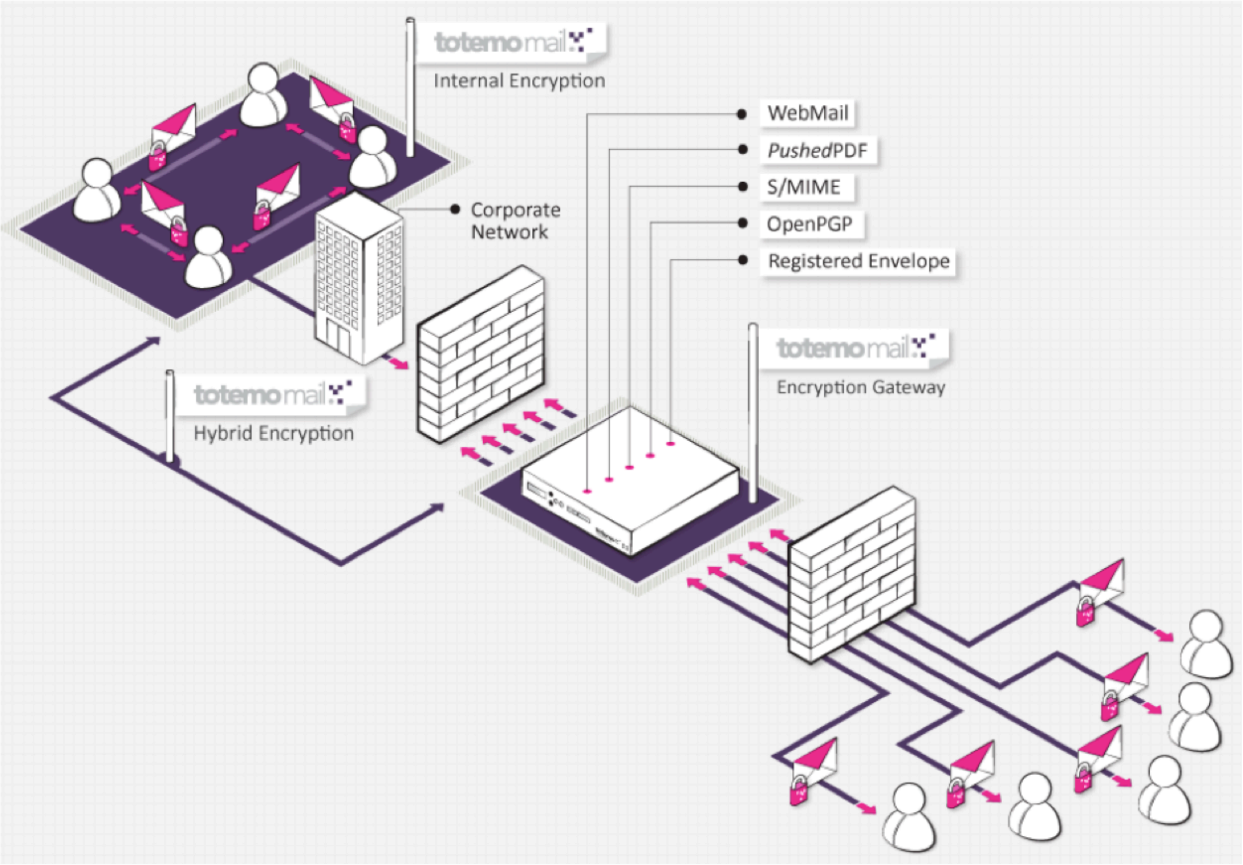
In order to be able to communicate securely with business partners and customers who do not use an encryption technology of their own, the modules **totemo**mail® WebMail, **totemo**mail® *Pushed*PDF, and **totemo**mail® Registered Envelope are integrated into the solution.

On receiving his first **totemo**mail® message, the recipient chooses pull or push technology to process it.

A solution that implements pull technology means that the recipient needs to actively initiate the request for the encrypted email. For recipients preferring this option, **totemo**mail® WebMail is the best solution. If the recipient prefers to use push technology, **totemo**mail® Registered Envelope and **totemo**mail® *Pushed*PDF are the modules available. With these methods, the encrypted email is sent directly to the recipient's mailbox.

Architecture

The following shows the standard architecture of **totemo**mail® Hybrid Encryption with all its components.


totemomail
Internal Encryption
WebMail
PushedPDF
S/MIME
OpenPGP
Registered Envelope
Corporate Network
totemomail
Encryption Gateway
totemomail
Hybrid Encryption