Solution Overview: totemomail® Encryption Gateway

Around the world, a trend towards more stringent industry regulations and stricter compliance standards is becoming apparent. This sets tougher requirements for email security of businesses and organizations of any size and in any industry. Infringing on regulations such as HIPAA, SOX, DPD and Basel III or losing valuable company information can have serious consequences: financial penalties, economic damage and loss of trust on both the partner and customer side among them.

Email communication is particularly vulnerable to data loss since the SMTP protocol does not include any protective mechanisms. Whoever wants to intercept data traffic can do so with a minimum of effort. As a matter of fact, most breaches of guidelines can be traced back to lacking email security. But despite its obvious shortcomings, it has become unimaginable to stop using email in business communication. Message confidentiality, integrity and authenticity thus need to be ensured with additional measures. Hence using a reliable secure messaging solution that protects sensitive information is becoming increasingly important for most companies. The FIPS 140-2-validated **totemo**mail® Encryption Gateway is optimized for mobile devices and helps to strictly observe security guidelines as well as monitor them comprehensively for internal and external audits.

The **totemo**mail® Encryption Gateway pursues a consistent all-in-one-box approach regarding encryption and protects confidential email communication with any given external and internal partners. Encrypted transmission of all emails including delivery confirmation, sender identification, guaranteed message integrity as well as message non-repudiation are the automatized core functionalities of the solution.

Moreover, it is flexibly scalable and capable of multitenancy. If operated in a clustered environment, all settings can be configured on a single system. Optionally combined with the module **totemo**mail® Internal Encryption - which is also available as a standalone product -, the **totemo**mail® Encryption Gateway becomes the high-performing and innovative hybrid solution **totemo**mail® Hybrid Encryption.

The **totemo**mail® Encryption Gateway is completely transparent, requires neither additional software nor plugins for email clients and is therefore easily and quickly integrated into any existing environment. The sender and the recipient do not need to adapt their work processes since the company security guidelines are centrally defined and applied.

Furthermore, the solution is fully compatible with a number of third-party systems.

How It Works

The **totemo**mail® Encryption Gateway 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.

Before delivering an email to an external recipient, the **totemo**mail® Encryption Gateway checks his credentials. If he is already enrolled, the message is encrypted with the corresponding public key or signed with the matching digital certificate. In case the recipient does not use an encryption technology of his own, the **totemo**mail® Encryption offers secure alternative delivery methods.

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.

Key Facts

Automatized Certificate and Key Management

The **totemo**mail® Encryption Gateway's core function is its automatized certificate and key management. Via the graphic interface of the administration console, the company certificate policies can be easily and comprehensively configured. Amongst other things, 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 the **totemo**mail® Encryption Gateway can be defined. By means of the automatic user enrolment feature, the **totemo**mail® Encryption Gateway independently collects and encrypts the certificates and keys already available, then saves them within the key store.

The **totemo**mail® Encryption Gateway's incorporated PKI component is able to generate, distribute and manage certificates for both internal and external communication partners and thus enables their quick and efficient integration. Alternatively, the **totemo**mail® Encryption Gateway can be connected to an external PKI solution or CA (e.g. S-Trust, Swisscom, SwissSign, QuoVadis, SignTrust etc.) via one of the integrated standard interfaces.

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

Automatized User Enrollment

The **totemo**mail® Encryption Gateway 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, the **totemo**mail® Encryption Gateway retains the original message until they are successfully authenticated. Then they receive their email either digitally signed with the matching key, via **totemo**mail® WebMail or as a **totemo**mail® *Pushed*PDF.

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 automatized 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.

Administration via a Graphic User Interface

The **totemo**mail® Encryption Gateway 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

The **totemo**mail® Encryption Gateway 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 Observation of Compliance Standards

For internal and external audits, complete and easily searchable records of all compliance-related actions are needed. The **totemo**mail® Encryption Gateway caters to that need with 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
- Optional: Internal encryption with S/MIME

Administration

- Easy integration into existing IT infrastructure
- No installation of specific email clients or plugins necessary neither for employees nor business partners nor customers
- Graphic user interface for administration console
- Granular user role definition
- No user training necessary due to transparent handling

User

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

Modules

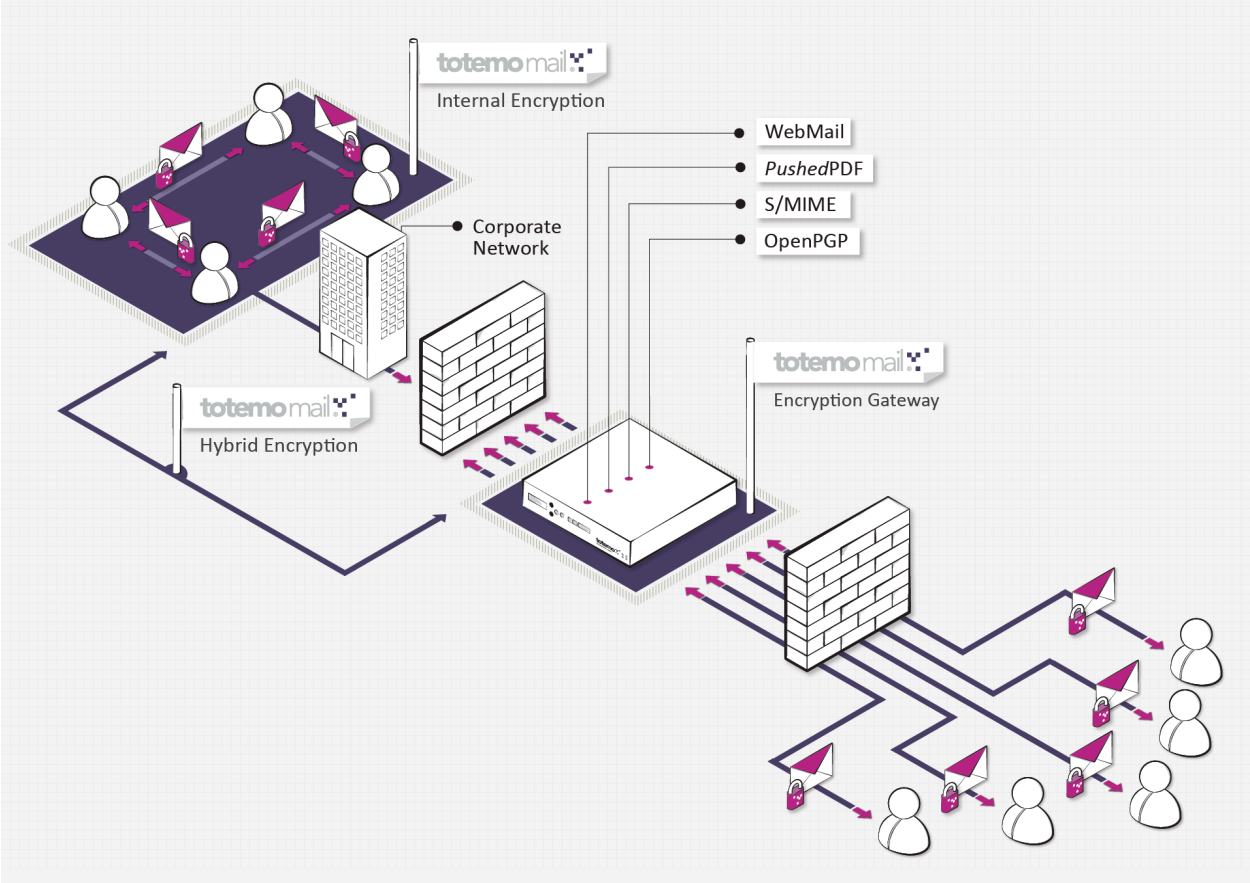
The **totemo**mail® Encryption Gateway consists of the following modules:

- **totemo**mail® Encryption Gateway
  - *Option 1:* **totemo**mail® WebMail
  - *Option 2:* **totemo**mail® *Pushed*PDF
- **totemo**mail® Internal Encryption (available separately)

totemomail® WebMail and **totemo**mail® *Pushed*PDF are two different methods for encrypted email communication with external partners who do not use an encryption technology of their own. The module **totemo**mail® Internal Encryption can be run in combination with the **totemo**mail® Encryption Gateway as the hybrid solution **totemo**mail® Hybrid Encryption or without the gateway as a stand-alone product to secure the organization's internal electronic communication.

Architecture

The **totemo**mail® Encryption Gateway communicates directly with all current email clients. Thus neither internal users nor external communication partners need to install additional components.


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