DATASHEET

totemomail®

KEY FACTS

Security

- Hybrid Email Encryption Gateway (with end-to-end, end-to-gateway, gateway-to-end and gateway-to-gateway encryption capabilities)
- No installation of specific email clients or plug-ins
- Automatic certificate and key generation for S/MIME and OpenPGP
- Support for Microsoft Rights Management Services (AD RMS and AIP)
- Comprehensive policy and key management
- Flexible definition of corporate security policies
- Dynamic certificate generation for internal email encryption (patented in Switzerland, the European Union, the US and Canada)
- Integrated malware protection (optional module for **totemo**mail® appliances)
- Optional module to send large files by email
- **totemo**mail® Domain Encryption Service
- High availability ensures reliability

System Administration

- Central installation and configuration as well as highly automated system administration
- Simple, rapid and efficient integration with any existing email infrastructure as well as with existing PKI systems, certificate authorities and directory services
- Web-based administration console with GUI including dashboard and message tracking center
- Capable of multi-tenancy and highly scalable
- Single point of configuration for clustered and multiple instances environments
- Role-based administration (rights management)
- Comprehensive reporting capabilities with charts and diagrams
- Audit logs, audit user role and enhanced tracking capabilities for internal and external reviews
- DLP functionalities, additional connectivity to external DLP systems (RSA, Symantec) possible
- Comprehensive and fully scalable solution

Transparent Handling and Ease of Use

- Fully automated registration of internal and external communication partners (auto user enrollment)
- No need for additional user training
- System notifications to end-users can be freely defined
- Alternative email encryption methods without the need of a certificate infrastructure (optional modules, available as push and pull technology)

SUPPORTED STANDARDS

- S/MIME, OpenPGP and TLS
- Connectivity to external certificate authorities and PKI systems through automated interfaces
- Connectivity to various directory services such as Microsoft Active Directory, Key Server and X.500 Directories
- Connectivity to Hardware Security Modules (HSMs) from Thales, SafeNet/Gemalto and Utimaco
- Online validation of certificates through CRL/ARL and OCSP
- SAML 2.0 connection for single sign-on

SYSTEM FEATURES

Deployment as...

Software

- Microsoft Windows
- Linux (CentOS, Red Hat, SuSE)
- Sun Solaris

Virtual Appliance

- VMware ESXi, Microsoft Hyper-V, Microsoft Azure*

Software Appliance

- On any industry-standard hardware**

Supported External Databases

- MySQL, Postgres, IBM Db2, Microsoft SQL Server and Oracle Database

Language Versions

- English, German, French, Italian

* Requires an additional external database.

** The Software Appliance is based on CentOS 6, so the hardware used is subject to the same compatibility restrictions that apply to CentOS 6 itself.

INTERFACES & FORMATS

- SMTP(S), HTTP(S), SNMP
- LDAP(S), OCSP
- AD RMS, AIP
- S/MIME (v2, v3), X.500, X.509, PEM, DER, PKCS#7, PKCS#12
- OpenPGP, PGP Keys, PGP/MIME, PGP/Inline, HKP
- PKCS#10, PKCS#7, RFC2797, CMP, CRL/ARL, OCSP
- PKCS#11

CRYPTOGRAPHIC STANDARDS

Asymmetric Encryption: RSA, DSA, El Gamal

Symmetic Encryption: 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA, Safer-SK128

Hash: SHA-256, SHA-384, SHA-512, RipeMD160, Tiger, Haval