totemomail®

Datasheet: totemomail® Encryption Gateway

Key Features

Security

- Hybrid Secure Messaging Gateway with end-to-end encryption capabilities (end-to-end, end-to-gateway, gateway-to-end)
- Comprehensive and fully scalable central secure messaging solution
- No need for plugins or additional desktop software (nor for sender nor recipient)
- Automatic certificate and key generation for S/MIME and OpenPGP
- Comprehensive policy and key management
- Flexible definition of corporate security policies
- Dynamic certificate generation for internal email encryption (patented in CH, EU, USA and Canada)

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 directories
- 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

Transparent Handling

- Fully automated registration of internal and external communication partners (Auto User Enrollment)
- No need for additional user training
- Definable status messages for end-users
- Alternative email encryption methods without the need of a certificate infrastructure (e.g. *Pushed*PDF, WebMail)

Supported Standards

- S/MIME, OpenPGP and SSL / TLS
- Integration into any email infrastructure and groupware systems such as Microsoft Exchange, Lotus Domino
- Connectivity to external Certificate Authorities through RFC2797 and PKCS#10
- Connectivity to external PKI systems through RFC2797 and PKCS#10
- Connectivity to various Directory Services such as Microsoft Active Directory, Key Server and X500 Directories
- Connectivity to Hardware Security Modules (HSM) from Thales and SafeNet
- Online validation of certificates through CRL / ARL and OCSP
- Compatible with Java 7

System Features

Supported Operating Systems

- Microsoft Windows (2003, 2008, 2012)
- Linux (CentOS, Red Hat, SuSE)
- Sun Solaris

Virtual Environments

- VMware®

Language Versions

English, German, French, Italian

Interfaces & Formats

- SMTP(S), HTTP(S), SNMP
- LDAP(S), OCSP
- 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, XKMS, CRL / ARL, OCSP
- PKCS#11

Cryptographic Standards

Asymmetric Encryption: RSA, DSA, El Gamal

Symmetric Encryption: RC2, RC4, DES, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA, Safer-SK128

Hash: MD2, MD5, MDC2, SHA, SHA-1, SHA-256, SHA-384, SHA-512, RipeMD160, Tiger, Haval

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