

Key Features

Security

- Hybrides Secure Messaging Gateway (End-to-End, End-to-Gateway, Gateway-to-End)
- Umfassende und voll skalierbare zentrale Secure Messaging Lösung
- Keine Plug-Ins oder andere Client-Komponenten (weder beim Sender noch beim Empfänger)
- Automatische Zertifikats- und Schlüsselgenerierung für S/MIME und PGP
- Beinhaltet ein umfassendes Policy und Key Management
- Flexible Definition der unternehmensweiten Security Policies
- Dynamische Zertifikatsgenerierung für die interne E-Mail-Verschlüsselung (Verfahren zum Patent angemeldet)

System Administration

- Zentrale Installation, Konfiguration und Administration
- Web-basierte Administration Console mit integriertem Dashboard sowie Message Tracking und Reporting Center
- Rollenbasierte Administration (Rights Management)
- *Single Point of Configuration* bei verteilten oder Cluster Konfigurationen
- GUI unterstützte Definition der Security Policies
- Einfache, schnelle und effiziente Einbindung in jede beliebige E-Mail-Infrastruktur
- Automatisierte System Administration
- Einfache Integration in bestehende PKI-Systeme, Certificate Authorities und Directory Services
- Mandantenfähig

Benutzerkomfort

- Vollständig transparent für Endbenutzer
- Automatische Benutzer Registrierung (Auto User Enrolment)
- Definierbare Statusmeldungen für Endbenutzer
- Keine zusätzliche Schulung der Anwender notwendig
- Alternative Verschlüsselungsverfahren für die zertifikatslose E-Mail-Verschlüsselung (z.B. *PushedPDF*, *WebMail*)

Unterstützte Standards

- S/MIME, PGP und SSL / TLS
- Integration in jede beliebige E-Mail-Infrastruktur wie
 - Microsoft Exchange, Lotus Domino, Novell GroupWise, Oracle Collaboration Suite, etc.
- Anbindung an externe Certificate Authorities mittels
 - RFC2797, PKCS#10, CMP und XMKS
- Anbindung an externe PKI-Systeme mittels
 - PKCS, PKIX, CMP und RFC2797
- Anbindung an verschiedene Directory Services wie
 - Microsoft Active Directory, Key Server und X500 Directories
- Anbindung an Hardware Security Modules (HSMs) von
 - nCipher und SafeNet
- Online Validierung von Zertifikaten mittels
 - CRL / ARL und OCSP

Zwei Produktversionen – Eine Technologie

Totemo TrustMail® ist in zwei verschiedenen Versionen erhältlich:

- **Totemo TrustMail® Professional Edition**
richtet sich an Unternehmen, welche eine zentrale, voll skalierbare und regelbasierte Secure Messaging Lösung wünschen
- **Totemo TrustMail® Enterprise Edition**
richtet sich an Unternehmen, welche eine zentrale, voll skalierbare und regelbasierte Secure Messaging Lösung mit PKI-Funktionalität wünschen

Beide Produktversionen basieren auf der gleichen innovativen Software-Architektur, arbeiten nach internationalen, etablierten Standards und zeichnen sich durch transparente Bedienung und hohe Kosteneffizienz aus.

Systemeigenschaften

Unterstützte Betriebssysteme

- Microsoft Windows (2000, XP, 2003, Vista)
- Linux (Red Hat, SuSE, Trustix, Fedora, Mandrake, Ubuntu, Debian)
- Sun Solaris
- IBM AIX
- VMware®

Sprachversionen

- Englisch, Deutsch, Französisch und Italienisch

Schnittstellen und Formate

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

Kryptographische Standards

Asymmetrische Verschlüsselung: RSA, DSA, El Gamal

Symmetrische Verschlüsselung: RC2, RC4, DES, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA (muss separat lizenziert werden), Safer-SK128

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

Kontakt

totemo ag

Seestrasse 134/a,
P.O. Box 1574,
CH-8700 Küsnacht
Phone: +41 (0) 44 914 9900
Fax: +41 (0) 44 914 9999
www.totemo.ch

© Totemo AG