Z1 SecureMail Gateway

Nachhaltiger Wirtschaftsschutz durch zentrale E-Mail-Verschlüsselung und -Signatur

Sichere Kommunikation ist Chefsache

Wirtschaftsschutz und Compliance lassen sich für die E-Mail als die wichtigste Kommunikationsform in der Geschäftswelt schnell und flächendeckend einführen. Die größte Herausforderung bei der E-Mail-Verschlüsselung liegt darin, dass der Kommunikationspartner „mitspielen" muss. Mit Z1 SecureMail Gateway brauchen Sie nicht zu wissen, welche Technologien Ihr Kontakt verwendet. Sie können spontan vertrauliche E-Mails austauschen – mit jedem Kontakt, auf jedem Endgerät.

Ihre Vorteile:

- Enorme Effizienz durch hohen Automatisierungsgrad
- Kein Schulungsbedarf, keine Akzeptanzprobleme bei den Nutzern
- Garantierte flächendeckende Compliance-Umsetzung
- Sehr schnell integriert, installiert und betriebsbereit
- Über Weboberfläche leicht zu administrieren
- Kompetenter Hersteller-Support, auditfähige Logs

Qualitätssiegel für echte Sicherheit

Wer Daten wirklich sicher und ohne Hintertüren verschlüsseln möchte, ist gut beraten auf IT-Sicherheit aus Deutschland zu setzen.

SecurITy made in Germany

Zertificon ist offizieller Träger des TeleTrusT Qualitätssiegels *„IT Security made in Germany"*.

Verlässliche Zertifikatsvalidierung

Der sicherste Verschlüsselungsalgorithmus ist nutzlos, wenn niemand prüft, ob die verwendeten Zertifikate echt und gültig sind. Z1 SecureMail Gateway greift zur Suche und Validierung auf LDAP-Verzeichnisse und OCSP-Schnittstellen zu und nutzt zusätzlich Zertificons Z1 Global TrustPoint.

Für alle Firmengrößen

Z1 SecureMail Gateway ist einfach skalierbar. Mögliche Konfigurationen reichen vom einfachen Stand-Alone-System bis zum voll mandantenfähigen, hochverfügbaren Rechenzentrums-Cluster im Enterprise- oder ASP-Umfeld mit PKI- und ERP-Integration sowie HSM-Nutzung. Optionale Erweiterungen werden in der umseitigen Tabelle beschrieben.

Effiziente Plattform

Z1 SecureMail Gateway wird auf einem Komplettsystem als DELL-Hardware Appliance oder virtuelle Appliance (VMware, Xen und Hyper-V) betrieben. Office 365 wird ebenfalls unterstützt.

Sichere Kommunikation flächendeckend automatisiert:

Z1 SecureMail Gateway ...

... ver- und entschlüsselt E-Mails & signiert und prüft Signaturen
der E-Mails und Anhänge
gemäß den zentral hinterlegten Sicherheitsrichtlinien.

... übernimmt die automatische Verwaltung

... eigener Zertifikate
- Schlüsselpaare ausstellen
- Zertifikatsbeschaffung über beliebige Trustcenter
- Veröffentlichen
- Erneuern
- Zurückrufen

... fremder Zertifikate
- Suche in Verzeichnissen
- Sammeln aus E-Mail-Anhängen (Harvesting)
- Zwischenspeichern
- Validieren in Echtzeit (LDAP/OCSP)
- Vertrauenslevel etablieren

... erstellt für Empfänger ohne Zertifikate
E-Mails als **verschlüsselte PDF** oder **HTML-Anhang**
oder sichere **Webmailaccounts** zum vertraulichen Austausch.

Z1 SecureMail Gateway

– Funktionen und technische Daten

zertificon

S/MIME & OpenPGP

S/MIME

- opaque und attached Signatur
- Signatur für ganze E-Mail oder nur Anhang
- SigG einfach und fortgeschritten
- separate Signatur- und Verschlüsselungsschlüssel
- Mitsenden eigener SubCAs
- Common PKI-Spezifikationen

OpenPGP

- mime und classic mode
- Signatur für ganze E-Mail oder nur Anhang
- separate Signatur- und Verschlüsselungsschlüssel

Internes Zertifikatsmanagement

- Key/Cert Generation lokal oder Import
- Bedarfsabhängige Schlüssel-/Zertifikatserstellung (z.B. bei Signatur und/oder Verschlüsselung)
- automat. CA-/TrustCenter-Anbindung (S-Trust, Comodo, A-Trust, etc.)
- lokale X.509 & OpenPGP Onboard CA
- Anbindung von 3rd Party CAs (z.B. MS 2003, Nexus, ...)
- Nutzung von HSM & NetHSM (Hardware Security Module)
- Key/Cert-Lifecycle-Management
- automatisierte Zertifikatsveröffentlichung in LDAP-Verzeichnisse und Z1 Global TrustPoint
- XKMS-Schnittstelle

Externes Zertifikatsmanagement*

- parallele Abfrage beliebiger Key-Server
- Key-Server zentral konfigurierbar
- lokale Speicherung von Zertifikaten, allgemeiner Zertifikatspool
- Echtzeit-Validierung
- zentrales CA und SubCA Zertifkatsmanagement für X.509 und PGP
- Automatisierte Abfrage von Sperrlisten (CRLs)
- automatisierte OCSP-Abfragen
- Zugriff auf Z1 Global TrustPoint: www.globaltrustpoint.com
- inklusive EBCA-Zertifikatspool

Passwortverschlüsselung*

- sicheres Webpostfach (Z1 WebSafe)
- E-Mail als PDF (Z1 KickMail PDF) oder HTML-Datei (Z1 KickMail HTML) verschlüsselt
- mehrsprachige Benutzeroberfläche
- konfigurierbare Passwortzustellung (z.B. SMS-Versand)
- konfigurierbare Passwort-Policies: Sonderzeichen, Fehlversuche etc.
- benutzerfreundliche Passwortverwaltung mit Sicherheitsfragen
- konfigurierbares Quota- & Inactivity-Management
- automatisiertes User-Management
- Team-Encryption (extern zu extern)
- separat auf eigenem Server betreibbar

Security Policies

Zentral auf Z1 SecureMail Gateway

- auf Basis Mandanten, Domänen, Gruppen, User (intern & extern)
- inbound/outbound mail
- flexibel konfigurierbar für Sender, Empfänger, Inhalt
- einfach zu administrierendes detailliertes, flexibles Regelwerk

Benutzergesteuert

- User-Befehle im E-Mail-Betreff
- MS Outlook Message Optionen
- RFC822 X-Header (z.B. für Notes)
- User-Befehle flexibel konfigurierbar für Mandanten, Domänen, Gruppen und User

Multiple Mandanten

- beliebig viele Mandanten parallel betreibbar
- separat konfigurierbar
- Domains, Gruppen, User, Schlüssel, Zertifikate, Sicherheitsrichtlinien (Policies)
- CA, PKI oder TrustCenter (CA-Connector)
- LDAP für automatische Zertifikatsveröffentlichung
- Logging, Monitoring, Alerting
- rollenbasierte Administrationsrechteverwaltung
- Archivierungsanbindung
- Corporate Design (Web-Interface, Z1 KickMail PDF Template)
- Virtueller Host (Web-Interface)

Hochverfügbar, Skalierbar

- HA Clustering mit n Nodes
- komfortables, graphisches Clustermanagement
- automatische Synchronisierung der Clusternodes
- SW-Updates ohne Down-Zeiten des Mailflows
- Hot-Standby mit autofailover
- Loadbalancing-Betrieb
- Master-Master-Clustering
- kein Single Point of Failure
- Anbindung von 3rd Party Storage-Systemen (NAS)
- Anbindung von Enterprise DBs (Oracle etc.)

Ende-zu-Ende-Verschlüsselung*

- Z1 SecureMail End2End: Ende-zu-Ende-Verschlüsselung ad hoc mit jedermann
- *Organizational* End2End mit Umverschlüsselung; intern S/MINE, extern flexibel verschlüsseln
- *Personal* End2End: Durchgehende Verschlüsselung von Client zu Client, basierend auf S/MIME
- *Organizational* und *Personal* End2End parallel konfigurierbar
- Zugriff für Antispam- / Antivirus-Check und Data Loss Prevention möglich
- Verschlüsselte Ablage der E-Mails auf Servern und Mobilgeräten
- intern S/MIME / Notes ID, kompatibel zu MS Outlook, Domino etc.
- Nutzung nativer Clients oder optional Client-Erweiterung Z1 MyCrypt als Plug-in oder App

Compliance & Standards

Public Government Standards

- Bundesdatenschutzgesetz, SigG/SigV
- KonTraG, GDPDU, HIPAA, SOX

Technische Standards

- S/MIME v2+v3; X.509; OpenPGP; XKMS; PKCS#7; PKCS#11; FIPS (140-2) (OpenSSL/HSM), PEM, DER, PKCS#10, PKCS#12,
- OpenSSl, SMTP, TLS, SNMP, HTTPS, SSH, SCP, NTP, LDAP(S), OCSP, HKP, SOAP WebService; XML
- Kryptoalgorithmen: alle symmetrischen/asymmetrischen und Hashalgorithmen

Sonstiges

- GOVERNIKUS Edition verfügbar
- Anbindung an **De-Mail***

Z1 Appliance Systemsicherheit*

- gehärtetes OS auf Linux-Basis
- zeitnahe OS Security Fixes
- Unterstützung von HSMs (Hardware Security Modules)
- OnBoard-Firewall
- nur verschlüsselter und authentifizierter Admin-Zugriff via HTTPS & SSH
- 2-Faktor-Authentifizierung
- 64 Bit System
- AntiSpam/AntiVirus optional

Enterprise Integration

- ERP-Anbindung (ActiveDirectory, Lotus Domino, LDAP etc.)
- SAP-Anbindung/-Schnittstelle
- flexibel konfigurierbare Ausleitung an Archivierungs- und Drittsysteme
- WebService Interface für projektspezifische ERP-Anbindung
- Anbindung Qualifizierte Signatur nach SigG für Massenprozesse
- Datenbank-Cluster
- SNMP-Management
- HSM-Anbindung möglich

Betrieb

- standalone / verteilt installierbar
- automatisierte Backup-Logiken und Restore
- flexibles Monitoring, Logging und Alerting von System, Mailverkehr und Adminaktionen
- umfangreiche Auswertungen und Statistiken
- einfache Installation und Updates
- SNMP-Anbindung (Tivoly, Patrol, Nagios etc.)
- Einsatz von HSM-Systemen (auch clustered)
- problemloses Zusammenspiel mit allen gängigen Antispam-/Antivirus-Systemen
- 5*8 und 7*24 Support
- Onsite und Remote onsite Service

** separates Produktdatenblatt verfügbar*

Abb. 1: Z1 Appliances

Zertificon Solutions GmbH
Berlin, Germany
www.zertificon.com

Tel.: +49 (0)30 5900300-0
E-Mail: sales@zertificon.com
www.globaltrustpoint.com