Z1 SecureMail Gateway

Die marktbewährte Serverlösung für E-Mail-Verschlüsselung und -Signatur!

Z1 SecureMail Gateway als zentrale Serverlösung ermöglicht die wirtschaftliche und effiziente Verschlüsselung und Signatur Ihres gesamten E-Mail-Verkehrs! Das Gateway arbeitet als SMTP-Proxy ohne jegliche Software-Installation auf Clients und wird per Web-GUI administriert.

PKI-verschlüsselte E-Mails

PKI-basierte E-Mail-Verschlüsselung und -Signatur wird gemäß den internationalen E-Mail-Standards S/MIME und OpenPGP ausgeführt. Private und öffentliche Schlüssel interner Nutzer werden automatisch generiert, verwaltet und ggf. publiziert. Ebenso kann die Zertifikatsausstellung voll automatisiert lokal, wie über 3rd Party CAs oder durch externe Trustcenter erfolgen. Zertifikate externer Kommunikationspartner werden automatisch abgefragt, validiert für die spätere Nutzung gespeichert.

Passwortverschlüsselte E-Mails

E-Mail-Verschlüsselung mit Passwörtern erlaubt einen vertraulichen E-Mail-Austausch mit jedermann z.B. in der B-to-C Kommunikation. Z1 SecureMail Gateway erstellt automatisch gesicherte Postfächer oder sendet E-Mails als verschlüsselte PDFs. Empfänger benötigen lediglich einen Browser und/oder PDF Reader - ohne zusätzliche Softwareinstallation. Das automatisierte Passwortmanagement ermöglicht den Einsatz auch bei einer hohen Zahl externer Nutzer.

Automatische Bearbeitung von Anhängen

Die automatisierte Bearbeitung von E-Mail-Anhängen z.B. zur Signaturerstellung, -prüfung sowie zur Archivierungsanbindung oder Verschlüsselung kann für beliebige Dateiformate und auch für die Massenbearbeitung (Newsletter, Reports, Rechnungen, ...) konfiguriert werden.

Foto: Z1 Appliance

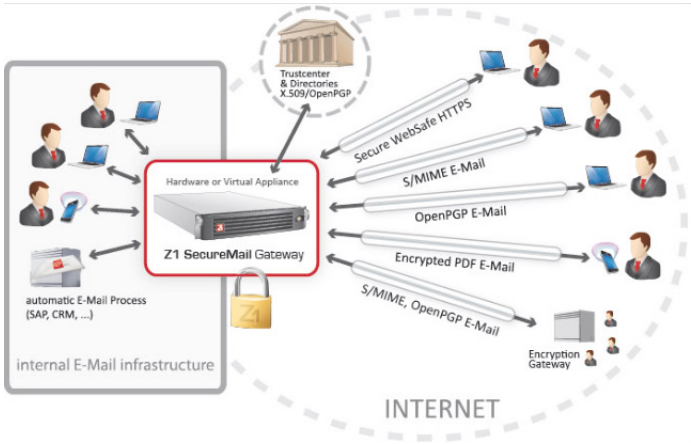

Abb.: E-Mail-Kommunikation über Z1 SecureMail Gateway

Security Policies

Zur Umsetzung unternehmenseigener Sicherheitsrichtlinien können zentrale Security Policies konfiguriert werden. Basierend auf Sender- und Empfängeradressen oder Inhalten werden E-Mail-Verschlüsselung und/oder -Signatur zwingend oder optional eingestellt. Clients können das Verhalten des Gateways zusätzlich per Nutzerbefehl in der Betreffzeile und über X-Header steuern.

Für jede Unternehmensgröße

Z1 SecureMail Gateway ist skalierbar für alle Unternehmensgrößen und in der Lizenzierung flexibel. Mögliche Konfigurationen reichen vom einfachen Stand-Alone-System z.B. in einer Kanzlei bis zum voll mandantenfähigen, hochverfügbaren Rechenzentrums-Cluster im Enterprise- bzw. ASP-Umfeld mit PKI- und ERP-Integration sowie HSM-Nutzung.

Plattformen

Das Z1 SecureMail Gateway ist als Appliance-Lösung wirtschaftlich und einfach einsetzbar, als virtuelle Appliance auch für Virtualisierungsinfrastrukturen auf der Basis von VMware und Xen. Die reine Softwarelösung ist für Debian Linux und Solaris verfügbar.

Zertificon Beratung & Support

Zertificon Support bedeutet für Sie schnelle, kompetente und flexible Unterstützung und Hilfe beim Einsatz Ihres Z1 Produktes. Mit unserer umfangreichen Projekterfahrung bieten wir Ihnen unsere Beratung auch bei der Lösungskonzeption während der Planungsphase.

Z1 SecureMail Gateway

zertificon

S/MIME & OpenPGP

S/MIME

- opaque + attached Signatur
- ganze E-Mail oder nur Anhang
- ISIS MTT
- SigG einfach & fortgeschritten
- GOVERNIKUS zertifiziert
- separate Signatur- und Verschlüsselungsschlüssel
- Mitsenden eigener SubCAs

OpenPGP

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

Internes Keymanagement

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

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
- ERP-Anbindung (ActiveDirectory, ID, ...)
- Logging, Monitoring, Alerting
- rollenbasierte Administrationsrechteverwaltung
- Archivierungsanbindung
- Corporate Design (Web-Interface, crypto PDF Template)
- Virtueller Host (Web-Interface)

Passwortverschlüsselung

- sicheres Webpostfach (Z1 WebSafe)
- E-Mail inkl. Anhänge verschlüsselt als PDF (Z1 KickMail PDF)
- mehrsprachige Benutzeroberfläche
- konfigurierbare Passwortetablierung (Split PW, UserPW, SMS-Versand, Pre-Install, ...)
- konfigurierbare Passwort-Policies: Länge, Sonderzeichen, Ziffern, Falschversuche, Blockzeit, etc.
- benutzerfreundliche Passworterneuerung, optional mit zusätzlichen Sicherheitsfragen
- konfigurierbares Quota- & Inactivity-Management
- automatisiertes User-Management
- Team-Encryption (extern<->extern)
- separat auf eigenem Server betreibbar

Security Policies

Zentral auf Gateway

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

Benutzergesteuert

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

Externes Zertifikatsmanagement

- parallele Abfrage beliebiger Key-Server
- Key-Server zentral konfigurierbar
- lokale Speicherung von Zertifikaten, allgemeiner Zertifikatspool
- Validierung vor jeder Nutzung
- 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

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 SigG für Massenprozesse
- Datenbank-Cluster
- SNMP-Management

Interne Verschlüsselung

- Z1 End2End Gateway & Service (optional)
- S/MIME, kompatibel zu MS Outlook
- Anbindung MS ActiveDirectory und MS CA
- Umverschlüsselung für AntiSpam/AntiVirus Check eingehender E-Mails
- automatisiertes internes Key/Cert-Management
- automat. Key/Cert-Enrollment
- Anbindung an interne PKI
- Anbindung Mobiler Clients: Blackberry, iPhone, Android

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

- Anbindung an De-Mail verfügbar

Z1 Appliance Systemsicherheit

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

Hochverfügbarkeit, Skalierbarkeit

- HA Clustering mit n Nodes
- komfortables, graphisches Clustermanagement
- automatische Synchronisierung der Clusternodes
- SW-Updates ohne Down-Zeiten
- 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.)
- Clustering auch mit HSM-Betrieb

Betrieb

- standalone / verteilt installierbar
- automatisierte Backuplogiken 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
- Remote onsite Service

Advantix. Groupware AG
Bahnhofstrasse 33b
CH - 8703 Erlenbach
Tel +41 44 914 88 44
Fax +41 44 914 88 45
welcome@advantix.ch

Besuchen Sie uns auf www.zertificon.com für weitere Produktinformationen und umfangreiche Referenzen. Starten Sie dort Ihre Anfragen zu Online-Demos, Downloads, Evaluierungsversionen, unverbindliche Preisauskünfte, Try & Buy - Z1 Appliances, etc ...