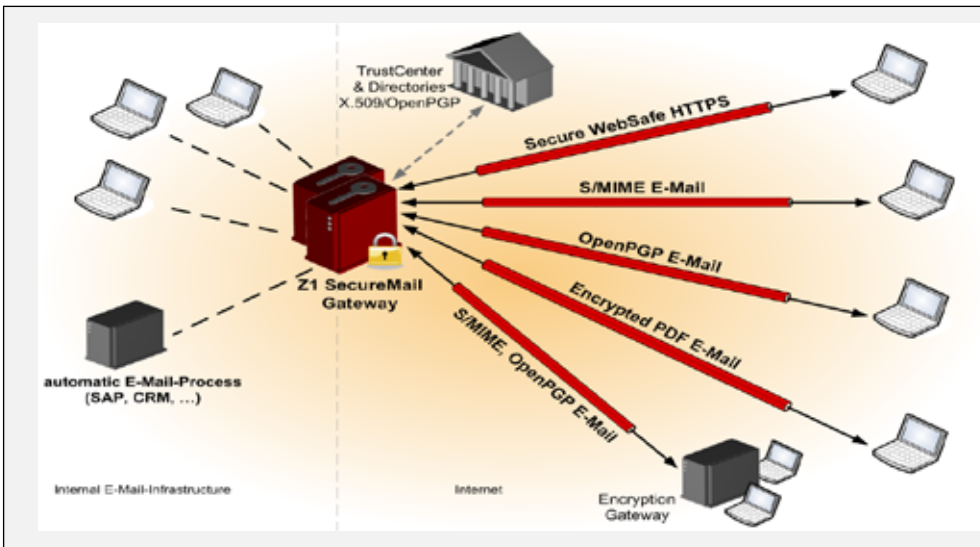


Z1 SecureMail Gateway



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

zertificon
solutions



Z1 SecureMail Gateway

Zertificon Solutions bietet Ihnen mit dem Z1 SecureMail Gateway eine zentrale Serverlösung für die wirtschaftliche und effiziente **Verschlüsselung und Signatur** Ihres gesamten E-Mailverkehrs!

Das Gateway arbeitet als **SMTP-Proxy** ohne jegliche Software-Installation auf Clients.

PKI-basiert

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 Third Party CAs oder durch externe Trustcenter erfolgen. Die Zertifikate externer Kommunikationspartner werden automatisch abgefragt, validiert und auch für eine spätere Nutzung gespeichert.

Passwort-basiert

Die passwort-basierte E-Mail-Verschlüsselung mittels **WebSafe** als gesichertem Postfach oder via **PDF-Verschlüsselung** ermöglichen den vertraulichen Austausch mit jedermann ganz **ohne PKI** – z.B. in der B2C-Kommunikation. Das automatisierte Passwortmanagement ermöglicht den Einsatz auch bei einer hohen Zahl externer Nutzer.

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. Zusätzlich können Clients das Verhalten des Gateways 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, hoch verfügbaren Rechenzentrums-Cluster** im Enterprise- bzw. **ASP-Umfeld** mit **PKI-** und **ERP-Integration** sowie **HSM-Nutzung**.

Date	Status	Time	Size	Internal	External	Subject	Security
01.08.08 08:00:23	OK	1.4s	1.8KB	internal@demo.zertificon.com	end@end@demo.com	Re: End To End	
01.08.08 07:29:11	OK	0.6s	0.4KB	internal@demo.zertificon.com	end@end@demo.com	End To End	
01.08.08 07:57:45	OK	1.1s	0.4KB	internal@demo.zertificon.com	end@end@demo.com	Signed	
01.08.08 07:49:09	OK	1.0s	0.4KB	jan@demo.zertificon.com	i-have-two-keys@zertificon.com	Signed Encrypted Multiple Keys	
01.08.08 07:48:01	OK	0.3s	1.1KB	user@demo.zertificon.com	user@company.com	Domain encrypted	
01.08.08 07:47:23	OK	0.1s	0.5KB	internal.user@demo.zertificon.com	user@company.com	Re:	
01.08.08 07:47:15	OK	0.1s	0.5KB	internal.user@demo.zertificon.com	user@company.com	Re:	
01.08.08 07:46:55	OK	0.2s	0.4KB	internal.user@demo.zertificon.com	ppg.one.key@external.com	S/mime signed	

Screenshot: Z1 Admin-Weboberfläche

Z1 SecureMail Gateway



S/MIME & OpenPGP	Internes Keymanagement	Multiple Mandanten	Passwort-basierte Verschlüsselung
<p>S/MIME</p> <ul style="list-style-type: none"> - opaque + attached Signatur - ganze E-Mail oder Attachment only - ISIS MTT - SigG einfach & fortgeschritten - GOVERNIKUS zertifiziert - separate Keys für Sig./Encr. - Mitsenden eigener SubCAs <p>OpenPGP</p> <ul style="list-style-type: none"> - mime + classic mode - ganze E-Mail oder Attachment only - separate Keys für Sig./Encr. 	<ul style="list-style-type: none"> - automat. CA-/Trustcenter-Anbindung - Key/Cert Generation lokal oder Import - on demand Key/Cert generation (z.B. bei Sig. und/oder Encr.) - lokale OnboardCA für X.509 und OpenPGP - Anbindung von 3rd Party-CAs (z.B. MS 2003, Nexus, ...) - Anbindung von externen TrustCentern (TC Hamburg, S-Trust, Comodo, A-Trust, ...) - Nutzung von HSM & NetHSM (Hardware Security Module) - kompletter Key/Cert-Lifecycle - automat. Publishing von Certs in LDAP-Directories und Z1 GTP - XKMS - Schnittstelle 	<ul style="list-style-type: none"> - beliebig viele Mandanten betreibbar - pro Mandant separat konfigurierbar • Domains, Gruppen, User, Schlüssel, Zertifikate, Sicherheitsrichtlinien (Policies) • CA, PKI oder Trustcenter (CA-Connector) • LDAP für autom. Veröffentlichung von Zertifikaten • ERP-Anbindung (ActiveDirectory, ID, ...) • Logging, Monitoring, Alerting • Administratoren, Rollen und Rechte • Archivierungsanbindung • Corporate Design (Web-Interface, PDF-Verschlüsselung) • Virtueller Host (Web-Interface) 	<ul style="list-style-type: none"> - sicheres Webpostfach (Z1 WebSafe) - E-Mail inkl. Anhänge verschlüsselt als PDF (Z1 KickMail PDF) - mehrsprachige Benutzeroberfläche - konfigurierbare Passwortetablierung (Split PW, UserPW, SMS-Versand, Preinstall, ...) - konfigurierbare Passwort-Policies: Länge, Sonderzeichen, Ziffern, Falschversuche, Blockzeit etc. - benutzerfreundliche Passwörterneuerung, optional mit zusätzlichen Sicherheitsfragen - konfigurierbares Quota- & Inactivity-Management - automatisiertes User-Management - Team-Encryption (extern<->extern) - separat auf eigenem Server betreibbar
Security Policies	Externes Zertifikatsmanagement	Enterprise Integration	Interne Verschlüsselung
<p>Zentral auf Gateway</p> <ul style="list-style-type: none"> - auf Basis Mandanten, Domänen, Gruppen und User (intern u. extern) - inbound/outbound mail - sender & recipient & content - einfach zu administrierendes detailliertes, flexibles Regelwerk - DLP-Anbindung <p>Benutzergesteuert</p> <ul style="list-style-type: none"> - User-Befehle im E-Mail-Betreff - MS Outlook message Options - RFC822 X-Header (für z.B. Notes) - flexibel konfigurierbar f. Mandanten, Domänen, Gruppen und User 	<ul style="list-style-type: none"> - parallele Abfrage beliebiger Key-Server - Key-Server zentral konfigurierbar - lokale Speicherung von Zertifikaten, shared Cert-Pool - Validierung vor jeder Nutzung - zentrales CA und SubCA Zertifikatsmanagement - Validierung für X.509 und PGP - auto retrieve von Sperrlisten (CRL) - automat. OCSP-Abfragen - Zugriff auf Z1 Global Trustpoint - www.globaltrustpoint.com 	<ul style="list-style-type: none"> - ERP-Anbindung (ActiveDirectory, Lotus Domino, LDAP etc.) - SAP-Anbindung/Unterstützung SAP-Interface - flexibel konfigurierbare Ausleitung an Archivierungs- und Drittsysteme - Webservice Interface für projektspezifische ERP-Anbindung - Anbindung Qualifizierte Signatur SigG für Massenprozesse - Datenbank-Cluster - SNMP-Management 	<ul style="list-style-type: none"> - Z1 End2End Gateway & Service (optional) - S/MIME, kompatibel zu MS Outlook - Anbindung MS ActiveDirectory und MS CA - Umverschlüsselung für AntiSpam/ AntiVirus-Check für externe E-Mails - automat. internes Key/Cert-Management - interne Platzhalter-Zertifikate für externe User - automat. Key/Cert-Enrollment - Anbindung interne PKI - Anbindung Mobiler Clients Blackberry, iPhone, Android
Compliance & Standards	Betrieb	Hochverfügbarkeit Skalierbarkeit	System Sicherheit Z1 Appliance
<p>Public Government Standards</p> <ul style="list-style-type: none"> - Bundesdatenschutzgesetz, SigG/SigV - KontraG, GDPDU, HIPAA, SOX tech. 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 	<ul style="list-style-type: none"> - standalone oder verteilt installierbar - automatisierte Backuplogiken und Restore - flexibles Monitoring, Logging und Alerting von System, Mailverkehr und Admin-Aktionen - umfangreiche Auswertungen und Statistiken - einfache Installations- und Updateprozesse - Einsatz von HSM-Systemen (auch clustered) - problemloses Zusammenspiel mit allen gängigen AntiSpam/AntiVirus Systemen - 5*8 und 7*24 Support - Remote onsite Service 	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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

Plattformen

Das Z1 SecureMail Gateway ist als Appliance-Lösung wirtschaftlich und einfach einsetzbar, als Virtual Appliance auch für Virtualisierungsinfrastrukturen auf 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.

Rufen Sie uns an +49 (0)30 5900300-0 oder nutzen Sie unser umfangreiches **Informations-Angebot auf www.zertificon.com** für Ihre Produktentscheidung:

- Online-Demo
- Download Evaluierungsversion
- Unverbindliche Preisanfrage
- Try & Buy - Z1 Appliances
- Tutorial „E-Mail-Verschlüsselung Basics & Trends“
- Umfangreiche Referenzen