



Z1 SecureMail Gateway

The Market-Proven Server Solution for Email Encryption and Signature

Z1 SecureMail Gateway is a central server solution for economic and efficient email encryption and signature for internal and external use. It acts as an SMTP proxy without any software installation on clients.

PKI Based Encryption

PKI based email encryption and signature are applied according to the international email standards S/MIME and PGP. Internal user's private and public keys are automatically generated, managed and optionally published. Certificate issuance can also be automated locally and for third party CAs or via external trust centres. External communication partner's certificates are automatically retrieved, validated, and stored.

Password Based Encryption

Password based email encryption via WebSafe as secured postbox or via encrypted PDF enable confidential email exchange with everybody without any PKI e.g. in B2C communication. The automated password management enables the use of the application even with a large number of external users.

Automatic Attachment Processing

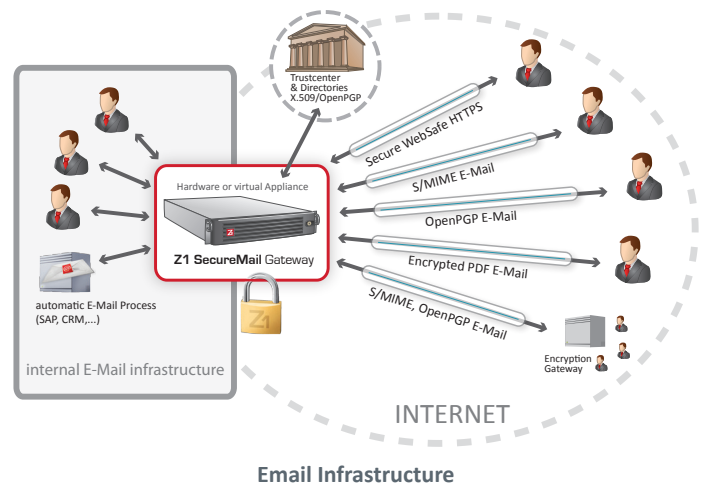
The attachment processing feature including digital signatures can be configured for any specific data format. The feature can be activated not only for single attachments but also for bulk processes (newsletters, reports and invoices). Verification of signatures is flexibly configurable to include special data formats like signed PDFs, industry specific or packed files.

Foto: Z1 Appliance



Zertificon Advice & Support

Zertificon support means fast, competent and flexible help and support for the deployment of your Z1 product. With our wide range of project experience we offer advice and support also during the planning stages of your email security project.



Security Policies

Emails are processed according to configurable security policies based on sender and/or recipient addresses or specific email contents. Processing can be set to mandatory or optional. Clients can also control Z1 SecureMail Gateway's behaviour via command line and x-headers.

For Enterprises Large and Small

Z1 SecureMail Gateway is highly scalable and suits enterprises of all sizes. Economic efficiency is achieved through flexible licensing. Possible configurations range from simple stand-alone systems e.g. in small offices to multi-tenant, highly available computer centre cluster systems for large enterprise and ASP environments which support PKIs, ERP and HSM integration.

Platforms

Z1 SecureMail Gateway is available as easy to administer, low maintenance Z1 Hardware Appliance and also as Z1 Virtual Appliance for virtualization infrastructures based on VMware and Xen. The plain software solution is available for Debian Linux and Solaris.

S/MIME & PGP	Internal Key Management	Multiple Mandators	Password Based Encryption
<p>S/MIME</p> <ul style="list-style-type: none"> opaque + attached signature entire email or attachment only ISIS MTT SigG simple and advanced GOVERNIKUS certified separate keys for sig./encr. attached sending of own Sub-CAs <p>PGP</p> <ul style="list-style-type: none"> mime + classic mode entire email or attachment only separate keys for sig./encr. 	<ul style="list-style-type: none"> automated CA/Trustcenter connection key/cert generation locally or import on demand key/cert generation (e.g. when sig. and/or encr.) local X.509 and OpenPGP OnboardCA connection to 3rd party CAs (MS 2003 Nexus etc.) - connection to external trust centers (TC Hamburg, S-Trust, Comodo, A-Trust, ...) use of HSM & NetHSM entire key/cert life cycle automated cert publishing to LDAP directories and Z1 GTP XKMS interface 	<ul style="list-style-type: none"> operate multiple mandators in parallel separate configurable per mandator domains, groups, user, keys, certificates, policies CA, PKI or trust center (CA-Connector) LDAP for automatic publishing of certificates ERP integration (ActiveDirectory, ID, ...) Logging, Monitoring, Alerting authorization, roles and rights archive integration corporate design (web interface, PDF encryption) virtual host (web interface) 	<ul style="list-style-type: none"> secure web post box (Z1 WebSafe) email incl. attachments encrypted as PDF (Z1 KickMail PDF) multi-lingual user interface configurable password establishment (SplitPW, UserPW, SMS, preinstall, ...) configurable password policies: length, special chars, digits, failures, time-out, ... user friendly password renewal: e.g. security questions configurable quota & inactivity management automated user management team-encryption (extern->extern) to be operated separately on own server
Security Policies	External Certificate Management	Enterprise Integration	Internal Encryption
<p>Centrally on the Gateway</p> <ul style="list-style-type: none"> on the basis of mandator, domain, group and user (internal and external) inbound/outbound mail sender & recipient & content easy to administer detailed, flexible rule system DLP integration <p>User Operated</p> <ul style="list-style-type: none"> user commands in subject line MS Outlook message options RFC822 X-Header (e.g. for Notes) flexibly configurable for mandator 	<ul style="list-style-type: none"> request arbitrary key servers in parallel key server centrally configurable local certificate storage, shared cert-pool validation before every use central CA and SubCA X.509 and PGP certificate management auto retrieval of certificate revocation lists (CRL) automated OCSP-requests access to Z1 Global Trustpoint: www.globaltrustpoint.com 	<ul style="list-style-type: none"> ERP integration (ActiveDirectory, LotusDomino, LDAP etc.) SAP integration/Support for SAP Interface flexibly configurable transfer to archiving and other systems web service interface for custom ERP integration integration for qualified signature SigG for bulk processes database cluster SNMP management 	<ul style="list-style-type: none"> Z1 End2End Gateway & Service (optional) S/MIME, compatible with MS Outlook MS ActiveDirectory and MS CA connection re-encryption for AntiSpam/AntiVirus check for external emails automated internal key/cert management automated key/cert enrolment internal PKI integration mobile client integration: BlackBerry, iPhone, Android
Compliance & Standards	System Security Z1 Appliance	High Availability, Scalability	Operation
<p>Public Government Standards</p> <ul style="list-style-type: none"> Federal Data Protection Act, SigG/SigV KontraG, GDPDU, HIPPA, SOX <p>Technical Standards</p> <ul style="list-style-type: none"> 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 Crypto Algorithm all symmetrical / asymmetrical and hash algorithms 	<ul style="list-style-type: none"> hardened Linux based OS prompt OS security fixes HSM (hardware security module) support regular security products audits on board firewall only encrypted and authenticated admin access via HTTPS & SSH 2 factor authentication 64-bit system AntiSpam/AntiVirus optional 	<ul style="list-style-type: none"> HA clustering with n nodes comfortable, graphic cluster management automated synchronization of the cluster nodes SW-updates without down-time hot standby with auto failover operation with load balancing master-master clustering no single point of failure integration of 3rd party storage systems (NAS) integration of enterprise databases (Oracle etc.) clustering also with HSM operation 	<ul style="list-style-type: none"> stand alone or distributed installation automated back up logic and restore flexible monitoring, logging and alerting of system, mail traffic and admin actions detailed overview and statistics easy installation and update procedure SNMP integration (Tivoly, Patrol, Nagios etc.) use of HSM systems (also clustered) smooth co-operation with all current AntiSpam/AntiVirus systems 5*8 and 24*7 support remote on-site service