

# Z1 SecureMail Gateway

## Snail mail or email?

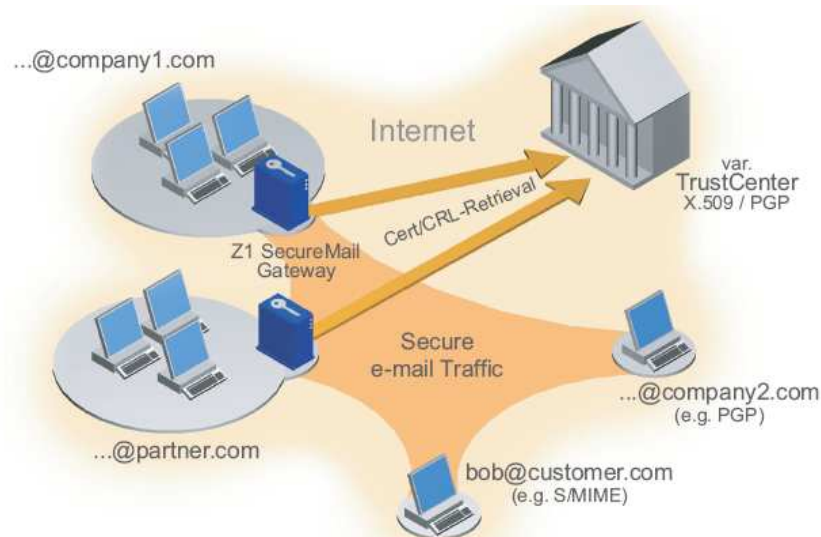
Nowadays, there are basically two possibilities of sending sensitive information: either the secure but expensive and slow way of postal communication is chosen or the documents are sent unencrypted via email in the hope that they will not be scanned, filtered or read.

## Email Security: not optional but mandatory for the IT

The official confirmation that there exists a world-wide listening device for telephone, fax and email communication called Echelon was not even the first evidence that it would be naïve to believe in the confidentiality of electronically transmitted data. There are large numbers of institutions and persons who are interested in accessing other people's emails and who have the technical devices to do so.

That is why organizations are obliged to take appropriate measures for an adequate data protection (in Germany this is regulated for example in the Bundesdatenschutzgesetz (federal data protection law, BDSG)).

## The Solution: Z1 SecureMail Gateway



## Centrally administered security for your email traffic

The Z1 SecureMail Gateway works like a central post office that opens incoming mail and puts outgoing letters into envelopes. Because it secures and releases the complete email traffic of an organization, it is also called a "virtual post office". Depending on the policy, it automatically encrypts, decrypts, signs and verifies signatures. In the process of this, the Z1 SecureMail Gateway remains absolutely invisible (transparent) for the sender of the email.

Because of its compatibility with the most widely spread international mail standards (S/MIME, PGP, ISIS-MTT), it offers a maximum of communication possibilities with all current email security products. The Z1 SMGW makes a perfectly smooth integration into existing email infrastructures possible. Zertifikat und Passwort und nur durch den Inhaber des USB Sticks erfolgen.

## Highlights

### Highest Security and Processing Speed

The integration of Hardware Security Modules that are certified according to international standards (e.g. FIPS) renders utmost security for key storage.

### Performance, Load Balancing and High Availability

The parallel installation of several Z1 SecureMail Gateways as well as the automated synchronization make the performance scalable and guarantee high availability. By these means, the Gateway satisfies even the highest requirements in enterprise environments.

### Simplest Integration into Email Infrastructures

The Z1 SecureMail Gateway uses only one single interface: the internationally standardized SMTP protocol (optionally POP and IMAP). Therefore the Gateway can quickly be integrated into any existing email infrastructure and works smoothly with Lotus Domino, MS Exchange, Sendmail, to name only a few examples.

### Scalable Security

Z1 SecureMail Gateway can be equipped with Hardware Security Modules (HSM) from renowned providers (Eracom, Chrysalis etc.). This makes the storage of the private and confidential keys highly secure. The timestamp functionality provides the opportunity to prove the date and time at which an email was sent and can thus ensure that legal requirements regarding eBusiness and eGovernment are met.

## The Product

Z1 SecureMail Gateway acts as an SMTP-Proxy that automatically encrypts, decrypts and signs emails and verifies signatures. It processes the entire email traffic according to the central security policy that is configured as a whole by the security officer via a management console integrated in the web browser (Admin Webclient). The Z1 SecureMail Gateway normally uses a so-called organization or domain certificate for its security mechanisms. This certificate can be ordered from any official Certification Authority (CA), in Germany for example from TC TrustCenter. However, it is also possible to import and use existing user certificates. This way, Z1 SecureMail Gateway supports individual email policies for persons, groups, departments and branch offices and thus adds value to investments made in a Public Key Infrastructure (PKI). The Z1 SecureMail Gateway retrieves certificates of communication partners as well as certificate revocation lists (CRLs) from Certification Authorities, Directory Services and Key Servers regularly and without user interaction.

## Range of Application

Modern eBusiness systems like for example online shops, CRM or supply chain applications generate large numbers of emails. Z1 SecureMail Gateway is perfectly suited for securing those systems as well. Bills, order confirmations, transaction data or newsletters are affixed with digital signatures and encrypted if desired. Furthermore, the integration of qualified timestamp services is possible. Your secure eBusiness will obtain greater acceptance and trust from your customers and business partners.

## System Requirements

PC system with Intel x86 processor, at least 1 GHz CPU, at least 1 GB RAM, at least 20 GB IDE HDD, CDROM drive for the installation.

Operating Systems:

SuSE, Red Hat, Sun Solaris (others on request)

**Talk to us. apsec offers a complete service around all areas of data security.**

Applied Security GmbH  
Industriestraße 16  
D-63811 Stockstadt

Fon: +49 (0) 60 27 / 40 67-0  
Fax: +49 (0) 60 27 / 40 67-99

Internet: <http://www.apsec.de>  
Email: [info@apsec.de](mailto:info@apsec.de)