zertificon®
Easy. Secure. Encrypted.

White paper

End-to-End Email Encryption for Everybody?

Why private individuals and corporations need different solutions

White paper

End-to-End Email Encryption for Everybody?

Why private individuals and corporations need different solutions

Ever since Edward Snowden's unveiling of NSA activities including PRISM and Tempora, email encryption has risen in importance. In various media reports, end-to-end encryption has been propagated as an ideal "one size fits all" solution for email security.

Despite this, end-to-end email encryption requirements should be considered depending on the intended use case. End-to-end encryption implies comprehensive encryption from the sending to the receiving devices. At no point will messages be stored or sent in plain format, not even for fractions of a second on the provider site. Only the sender and the recipient have access to the keys necessary for en- and decryption of a message.

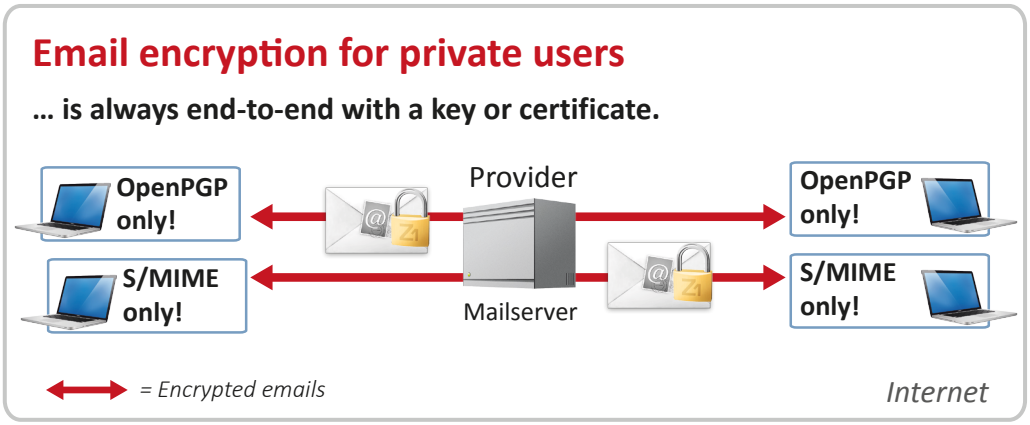
Regulations for email usage

Just as in many other areas, a solution which makes sense for individuals may only be of limited use for corporations. This similarly applies to email encryption. The key driving forces, coupled with legal requirements for documentation and privacy protection, are very different in the private and corporate sectors. Data loss prevention, along with central spam and virus checking, do not generally play a central role for the private user. On home applications, spam and virus checking is performed locally on the machine before any encryption respectively after any decryption takes place. Furthermore, the scalability of encryption key management is irrelevant for the private user, whilst being of prime importance in the corporate environment where manual key management cannot be implemented efficiently with large numbers of employees and communication partners.

Encryption standards

In private email communication, free encryption with OpenPGP has become increasingly popular. In corporate environments, S/MIME using X.509 certificates from certificate authorities as public keys has established itself and is preferred over PGP encryption.

The two standards S/MIME and PGP are not compatible. Private individuals therefore use one approach and require their communication counterparts to use the same standard as they do. When emails are encrypted on the client and no proprietary suppliers are used there is nothing but end-to-end encryption. Emails can be sent and received without having to worry about the confidentiality of the messages.



SecureMail Gateway is compatible with all standards

In many cases, companies use secure email gateways that can handle both X.509 certificates as well as OpenPGP keys for encryption. Sometimes, these devices even incorporate alternative approaches such as password based encryption. This can be quite useful in confidential ad hoc communication when the communication partner holds neither X.509 certificates nor OpenPGP keys. During password based encryption, messages are encapsulated into a PDF or HTML container and sent as an attachment, or accessed via a web-based inbox secured with HTTPS. De-Mail connectors, VPN or TLS further enlarge the functional scope of some gateways. Accordingly, companies can communicate immediately and confidentially with any recipient.

In most cases, companies do not use end-to-end encryption. A secure email gateway is the central interface to the Internet, and is responsible for the encryption and decryption of in- and outgoing messages. Inside the company network though, emails are transported in plain state. This is a safe and established method for protection against government and economic espionage. The need for end-to-end encryption in corporate environments is based upon a different set of requirements than for individuals who are only able to use end-to-end encryption.

End-to-End: Motivation and challenges for companies

End-to-end encryption for companies is becoming increasingly interesting as more and more smartphones and notebooks are used for business communication. Even company internal emails are sent in plain text over mobile and public WLAN networks. Another security aspect is the unencrypted storage of messages on company email servers. Internal communication channels and email storage have to be encrypted to ensure full confidentiality and prevent administrators from reading the messages. The implementation of end-to-end encryption in a corporate environment has to consider a variety of problems:

- Which encryption standard should be used, considering that the standards are not compatible with each other while the goal is nonetheless confidential and immediate communication with everybody?
- How is encryption conducted for those recipients without certificates?
- How to decrypt incoming encrypted emails locally on all the company's end user devices?
- How do data loss prevention systems access the messages? How to conduct a virus scan when the message is encrypted?
- How to implement central key management for the internal keys and those of external communication partners?
- What happens when employees leave or in cases of absence, when only the employee is able to access his messages?

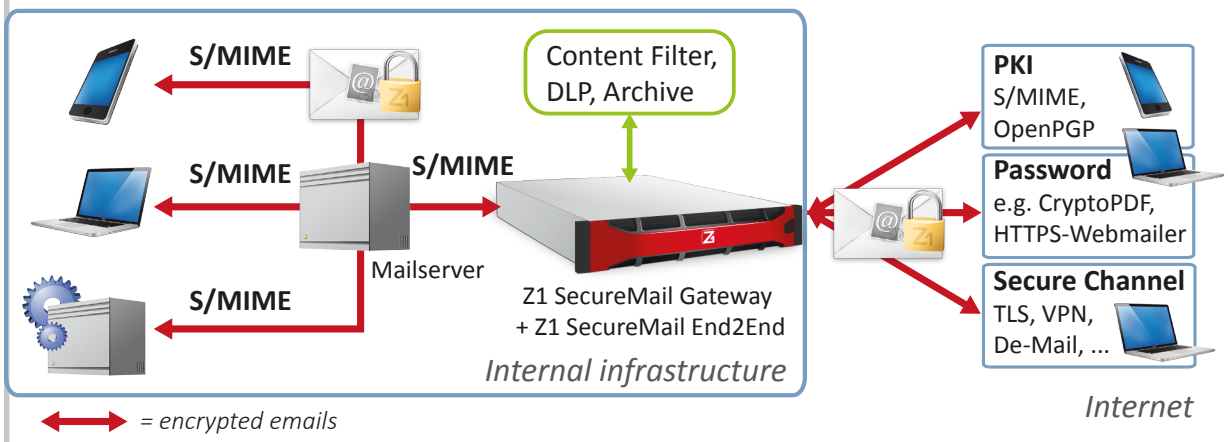
These implications need a clever solution:

State of the art end-to-end encryption with flexible re-encryption on the gateway

Modern secure email gateways with the appropriate extensions combine internal and external email encryption. Emails are transmitted in an encrypted state not only over the Internet but also within the internal company network. To achieve this, an encapsulated internal PKI is created which implements an S/MIME encryption immediately on the client. The X.509 certificates issued specifically for this purpose never leave the company.

Outgoing emails are encrypted on the client with the S/MIME gateway certificate – email clients support S/MIME directly, whereas several easily installable Apps are available for mobile devices. The secure email gateway decrypts the outgoing email and searches for the recipient's certificate. Depending on the external communication partner's certificate, a re-encryption into S/MIME, OpenPGP, CryptoPDF, De-Mail, TLS, etc. is performed.

Business solution for email encryption with everyone



State of the Art email encryption incl. end-to-end components
– S/MIME internally, flexible de-/encryption externally –

In the same way, every encrypted incoming message will be delivered to the internal end user as an S/MIME encrypted email. During re-encryption, anti-virus, anti-spam, DLP or archiving systems can access the message.

For smaller numbers of recipients, secure mail gateways can be combined with a real end-to-end encryption solution, where the advantages of such a solution outweigh the disadvantages.

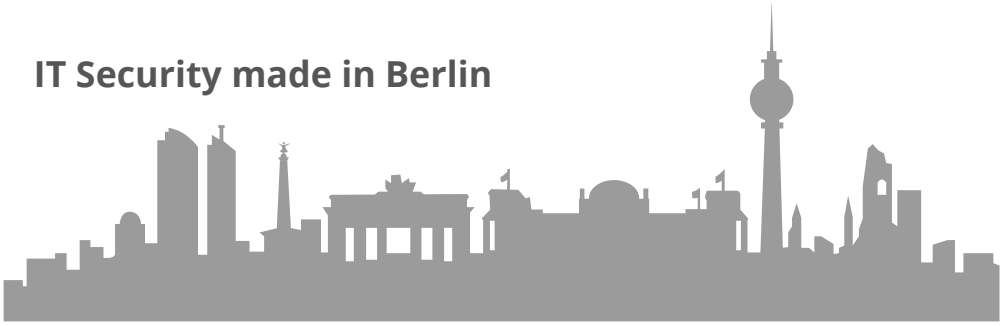
By combining Z1 SecureMail End2End with Z1 SecureMail Gateway, Zertificon distinguishes between **Organizational End2End** with the advantages of flexible re-encryption by the Gateway and **Personal End2End** which is analogous to private end-to-end encryption.

In the post-Snowden era, the much spoken about end-to-end encryption has to be regarded differently in private and company environments. Solutions exist for both environments and of course companies can encrypt their communications with private individuals.

The central port of call for anyone wishing to encrypt their emails with X.509 certificates or OpenPGP keys is Z1 Global TrustPoint (www.globaltrustpoint.com) where everyone can publish their own keys. Foreign keys can not only be searched for and retrieved, but also validated. Even the most secure encryption algorithm is useless if no one checks to see if the keys are genuine and valid.

Zertificon Solutions GmbH

Zertificon is a leading software manufacturer for IT security located in Berlin, Germany. An independent, founder-led company, Zertificon currently has more than 50 employees in its in-house development, sales and support departments. The award winning Z1 SecureMail Gateway has established Zertificon as a pioneer in the market for server-based email encryption for more than ten years. Through ground-breaking developments, Zertificon remains one of today's driving forces in email encryption solutions.



The focus is on delivering user friendly and economical turn-key solutions for secure email and data exchange. The popular **Z1 SecureMail Gateway** and **Z1 CertServer** for email encryption, digital signing and certificate management are complemented by Zertificon's **Z1 SecureHub** for secure web-based exchange of data files in any size and format.

The latest innovation from Zertificon – **Z1 SecureMail End2End** – provides state of the art end-to-end email encryption for organizations when combined with Z1 SecureMail Gateway. The organizational end-to-end mode allows immediate end-to-end encryption – all that is required is a recipient email address. Clients are able to connect seamlessly using the Z1 MyCrypt add-in for MS-Outlook and Lotus Notes or mobile app for iOS & Android. Z1 MyCrypt Mail supports end-to-end encryption alongside security features for server-based encryption whilst Z1 MyCrypt BigAttach integrates the web-based Z1 SecureHub into mail clients. Z1 MyCrypt integrate closely with all Z1 Server products. These new developments reliably meet the unique security demands of increased mobile communication via smart phones, tablets etc. in corporate environments.

For a simple, efficient and smooth operation of Z1 products, Zertificon offers its **Z1 Appliances** – as hardware or virtualized – optimized platforms for a full integration into existing IT infrastructures. Additionally, Zertificon's renowned support service offers rapid and personalized help for all product-related questions.

Accordingly, Zertificon enables companies and institutions of all branches and sizes to easily fulfill the highest security and compliance demands.

Zertificon Solutions GmbH
Berlin, Germany
www.zertificon.com

Phone: +49 (0)30 5900300-0
Email: sales@zertificon.com
www.globaltrustpoint.com