zertificon

Z1 SecureMail End2End

Maximum security for companies through end-to-end encryption and signatures

When is end-to-end encryption necessary?

End-to-end encryption becomes important for companies when smartphones and notebooks are being used for business emails. Even internal company emails are sent in clear text from mobile devices via phone networks and public Wi-Fi connections, where they are easy to intercept and may be read or manipulated.

Another security issue involves storing unencrypted emails on email servers. This applies particularly to the use of cloud-based services such as Office 365. Anyone who does not want intelligence services or administrators to read the emails left there will also have to use encryption on internal routes. And last but not least, when used correctly, end-to-end encryption also prevents data leaks in the event of devices being lost.

IT Security made in Germany

Zertificon's Z1 products carry the *„IT Security made in Germany"* seal of quality from the German Federation for IT Security TeleTrusT.

SecurITy made in Germany

Why end-to-end encryption presents companies with a special challenge

End-to-end encryption refers to the uninterrupted encryption of content between the sending device and the receiving device. Only the sender and the recipient are in possession of the relevant key. However, this technology – which works well enough for private communications – is not suitable for extensive use in companies.

For companies, end-to-end encryption means:

The company does **not have sovereignty over end-to-end encrypted emails**: only the employee has access to them.

- Limited application, as both sender and recipient need the same encryption technology
- Complicated key/certificate management at end devices with high error potential
- Intensive administration and maintenance required therefore not scalable
- Responsibility for encryption lies with individual user
- Cannot be centrally audited therefore not guaranteed tamper-proof
- No access for central content filters therefore high risks with no monitoring option

The solution: end-to-end encryption for companies with *Organizational End2End*

Emails are encrypted and decrypted at the employee's end devices. The company is given access at a secure point and re-encrypts the communication. This type of end-to-end secured communication allows:

- **Recognition of the company's obligation to monitor e.g. via content filters (anti-virus, anti-spam, DLP, etc.)**
- **Guarantee of tamper-proofing and auditability plus enforcement of compliance regulations**
- **Economic, spontaneous, highly secure email exchange in any encryption format**

Organizational End2End combines Z1 SecureMail End2End and Z1 SecureMail Gateway – business grade end-to-end encryption with re-encryption

Organizational End2End is a clever combination of policy-based encryption at both the client and the server end. The complex processes run automatically in the background and the user is completely relieved of the time-consuming, error-prone certificate management process.

Internal encryption is homogeneous and exclusively via S/MIME. As S/MIME is supported by standard email programmes, administration and maintenance are extremely efficient.

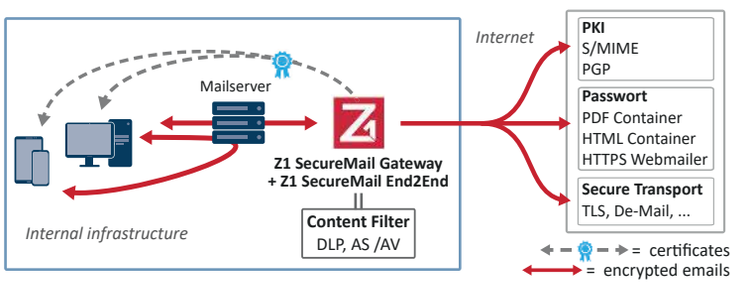

Fig. 1: With Organizational End2End emails are re-encrypted at the gateway.

Encryption from and to external sources is effected by the trusted Z1 SecureMail Gateway, using various technologies as required. From S/MIME and OpenPGP to password-protected PDFs or secure transport methods (TLS, De-Mail, etc.) – there are no limits to the secure email (see fig.1). The gateway will adapt flexibly to whatever system is used by the counterparty. During re-encryption at the Z1 SecureMail Gateway, all emails can be accessed by **content filters** such as archive, data loss prevention and anti-virus and anti-spam programmes. *Organizational End2End* enables highly secure email exchange at any time: it is compliant, efficient and economical – and with any recipient.

Personal End2End – convenient uninterrupted encryption for the high-security environment

With *Personal End2End*, emails are not re-encrypted; encryption is limited to the S/MIME standard. This form of end-to-end encryption is only recommended for individual, particularly security-sensitive emails, for example at executive management level. Z1 SecureMail End2End takes responsibility for certificate management, including the provision and validation of all certificates. This makes *Personal End2End* encryption very efficient to use. The encryption status of all emails is verifiable via log files and so auditability is guaranteed. Central content filters cannot be used with *Personal End2End*, however.

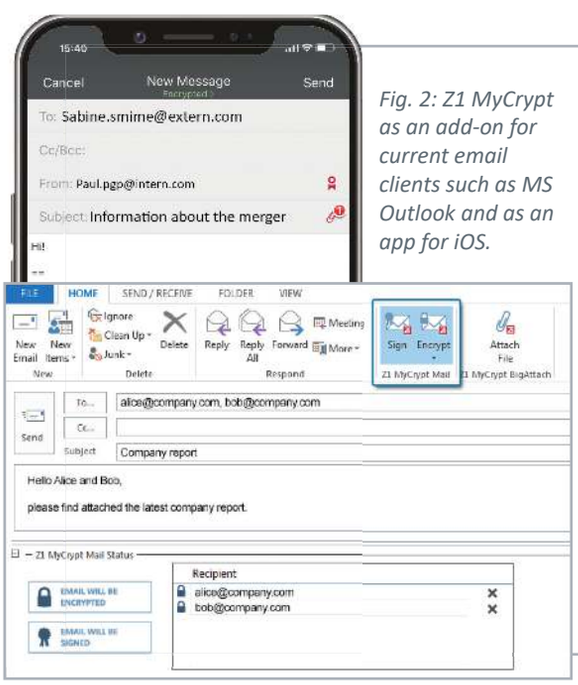

Fig. 2: Z1 MyCrypt as an add-on for current email clients such as MS Outlook and as an app for iOS.

Encryption with on-board tools at the end device...

Connection via ActiveSync and LDAP proxies enables Z1 SecureMail End2End to be used with all standard email programmes. No need for your employees to adjust to new systems, though they will have to actively trigger the encryption and the signature. However, depending on the platform, there is only limited access, if any, to central policies without the app or plug-in.

...or use Z1 MyCrypt as an app or plug-in

The apps (see fig. 2) are extremely convenient for the user to control, and take responsibility for the time-consuming, complex management of certificates. Z1 MyCrypt also features some highly-integrated functions. For example, when entering a recipient's address, the user can choose to display full details of configured policies and the security level. Compliance guidelines can generally be met easily on a company-wide basis with Z1 MyCrypt.

Z1 SecureMail End2End can be used in tandem with current mobile device management solutions.

Zertificon Solutions GmbH
Berlin, Germany
www.zertificon.com

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