zertificon®
Easy. Secure. Encrypted.

WHITE PAPER

End-to-End Email Encryption for Enterprises

How end-to-end encryption for email is defined and easily implemented in enterprise infrastructures

End-to-End Email Encryption for Enterprises

How end-to-end encryption for email is defined and easily implemented in enterprise infrastructures

Edward Snowden's revelations about the NSA brought email encryption to the public's attention in 2014. Since 2018, the topic has received constant attention due to the EU General Data Protection Regulation (GDPR) and an increasing rate of digitalization. From 2014 until today, countless articles have promoted end-to-end encryption for email exchange as a one-size-fits-all solution for companies and private users – but almost always without considering the security and compliance requirements in the business environment.

Businesses that already use email encryption are aware of the discrepancies between their needs and the existing recommendations for private user solutions. It can be challenging for IT departments without any experience in that area to realize what they actually need. We want to help people in charge of confronting the secure communication challenge get acquainted with the technical standards, implications, and possibilities of end-to-end encryption in a business environment.

Definition: End-to-End Encryption

End-to-end email encryption (E2EE) implies encryption at the sender's device and decryption at the recipient's device. The concept is based on the fundamental premise that only the recipient can access the keys necessary to decrypt a message intended for them.

Some vendors who call their encryption solutions end-to-end, define the business – rather than the individual employee sending or receiving the email – as one "end" in the communication. From a business point of view, that is easily understandable. We call that "gateway encryption," which secures emails in transit on routes over the Internet.

Then there are also business use cases, where protection against attacks over the Internet is not enough. That is when emails need to be protected on servers and cloud environments. There are also many use cases in between, depending on email infrastructure, individual business risks, and compliance regulations.

A rule of thumb at the start:

- End-to-end encryption for emails must consider the parties involved and the specific use cases.
- The higher the security level you want, the more skills are required at every user's end, and the less automation is offered from encryption software.

How private and business needs differ for email security and compliance

Much like many other areas, a solution that makes sense for individuals may only be of limited use for corporations. This case definitely applies to email encryption.

Companies need insight into email traffic for compliance and IT security purposes. Business-critical security and compliance driving forces for documentation and privacy protection do not apply to personal use whatsoever. Data loss prevention and central spam and virus checking are of great importance for corporations. On personal home applications, spam and virus checks are performed locally on the machine before any encryption and respectively after any decryption takes place.

E2EE needs the sender and recipient to use the same encryption technology

OpenPGP, an open and free version of the Pretty Good Privacy (PGP) standard, is very popular for private email communication. However, in the corporate environment, S/MIME, which uses paid X.509 certificates from certificate authorities as public keys, is the established and preferred standard over OpenPGP in most industries.

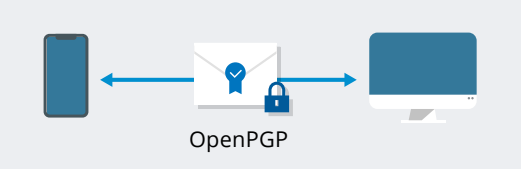

Fig. 1: In the private sector, email encryption is always end-to-end.

S/MIME and PGP standards are incompatible. So it seems the private and the business world are also incompatible. Companies need a proxy solution to exchange secure emails on an end2end basis with individuals or other companies who use PGP keys.

Usually, with some effort, private users can manage communication partners' keys on their devices. In the corporate environment, encryption key management on a larger scale cannot be left to the individual employee. Automation is the only way to scale efficiently and prevent human error in the process; for example, when checking the validity of a key. Also, compliance demands auditable solutions. This is hard to establish when the end user is responsible for key management and encryption on their device.

Secure email gateways may represent one end in business communication

Unlike private individuals, companies do not generally use end-to-end encryption from the sender's device to the recipient's device. In most cases, companies use secure email gateways as the company's secure communication "end."

A secure email gateway acts as a central interface to the Internet. It assumes the responsibility to encrypt and decrypt incoming and outgoing messages for the entire staff and automated company systems.

Secure email gateways are equipped to handle encryption with both X.509 certificates and OpenPGP keys. They may even incorporate encryption technologies that work when the communication partner holds neither X.509 certificates nor OpenPGP keys. Keyless encryption uses passwords and is very convenient for confidential ad hoc communication with private individuals, like whenever GDPR compliance calls for it. Zertificon solutions come with an automated logic that makes this more secure than average password protection.

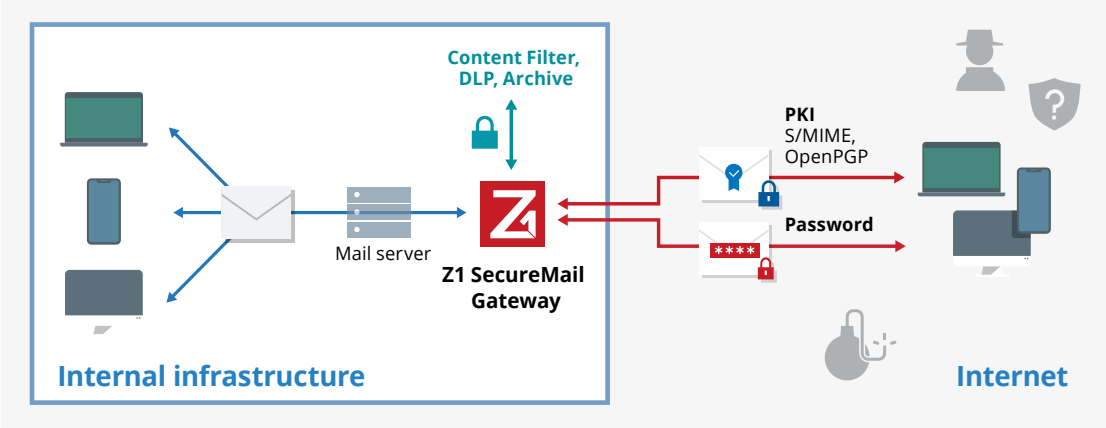

Fig. 2: Email encryption with Secure Email Gateway. All emails are protected against attacks when sent over the Internet.

However, a standard secure email gateway solution will not encrypt email inside the company's network. Companies use firewalls to prevent unauthorized access. So if your goal is protection against cyberattacks, and economic and industrial espionage over the Internet, consider it achieved. A secure email gateway is a safe and established method. You can stop here and check out our Z1 SecureMail Gateway and even argue that this is indeed end-to-end encryption.

When you choose Zertificon, not only do you get email compliance enforcement through centrally configurable security policies. You also get an unparalleled degree of automation in the very complex, error-prone, and challenging world of enterprise-level certificate management. Your end in communication would be safe!

Read on if you feel the need for end device email encryption for your business.

End-to-End encryption: Motivation and challenges for companies

So we learned that individuals can only use end-to-end encryption from the sender's device to the recipient's device. What requirements can possibly determine the need for end-to-end encryption for emails on the device level in the corporate environment? There are a few use cases when businesses require encryption for threat protection over the Internet and inside the company's network also.

The frequent use of mobile devices such as smartphones and notebooks for business communication without a VPN connection can be a reason for E2EE. Mobile devices send emails over mobile and public WLAN networks in plain text. And as we know, cyber-criminals can easily access email content when sent over unprotected networks.

Another security motive behind E2EE is the storage of messages on company email servers. Companies that have their email infrastructures run as a service might especially want to block administrator access to email content.

When it comes to end-to-end encryption use in a corporate environment, a solution should address the following challenges:

- Will the solution ask you to enforce one specific encryption standard for all your communication contacts, or will you stay flexible and able to communicate securely with any contact?
- Is E2EE even possible when the recipients do not have a certificate?
- How can you decrypt incoming encrypted emails locally on all the company's end-user devices?

- How do data loss prevention systems access the messages?
- How can you conduct a virus scan when the message is encrypted?
- How can you implement central key management for the internal keys and those of external communication partners?
- When messages are only accessible by the employee, what happens in case of leave or absence?

At Zertificon, we are familiar with these challenges. And we have overcome them all with a new approach called Organizational End2End encryption.

Organizational end-to-end encryption with a gateway twist

Zertificon solves corporate E2EE encryption obstacles with an extension to the renowned Z1 SecureMail Gateway: **Z1 SecureMail End2End**. Together, these solutions combine encryption on internal and external routes and even in the cloud to make organizational end-to-end encryption possible.

The Gateway is the proxy between internal and external routes. And while the gateway deals with all possible encryption methods for email exchange over the Internet, the internal route is reserved for S/MIME encryption only. Z1 SecureMail End2End takes charge of the S/MIME certificate management for the internal devices. Internally, relying just on S/MIME keeps things uncluttered and easy since all the mail programs support S/MIME out-of-the-box. For mobile use, Apps are provided.

How Organizational E2EE works

Outgoing emails are encrypted on the client with an S/MIME gateway certificate. The secure email gateway can decrypt the outgoing email and search for the actual recipient's certificate. It can be S/MIME or OpenPGP. If nothing is found, the mail will be encrypted with a password.

The gateway decrypts, re-encrypts, and delivers **incoming messages** to your staff or automated systems as S/MIME encrypted emails no matter what the original encryption method.

The gateway can allow access to third-party tools such as Anti-virus/Anti-spam solutions, Data-Loss Prevention, or archiving solutions, whether inbound or outbound, between encryption and re-encryption.

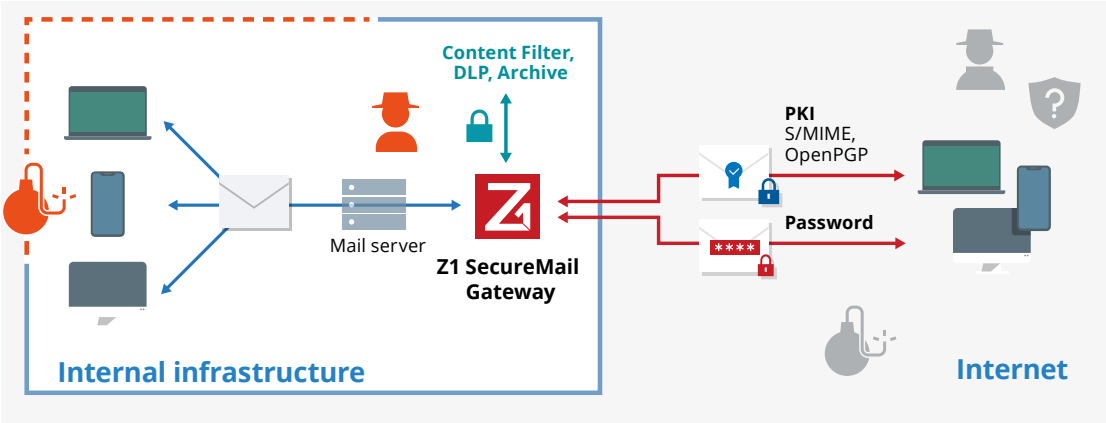

Fig. 3: When using mobile devices or when admins must not have access to emails at the server, email encryption should also protect the internal route.

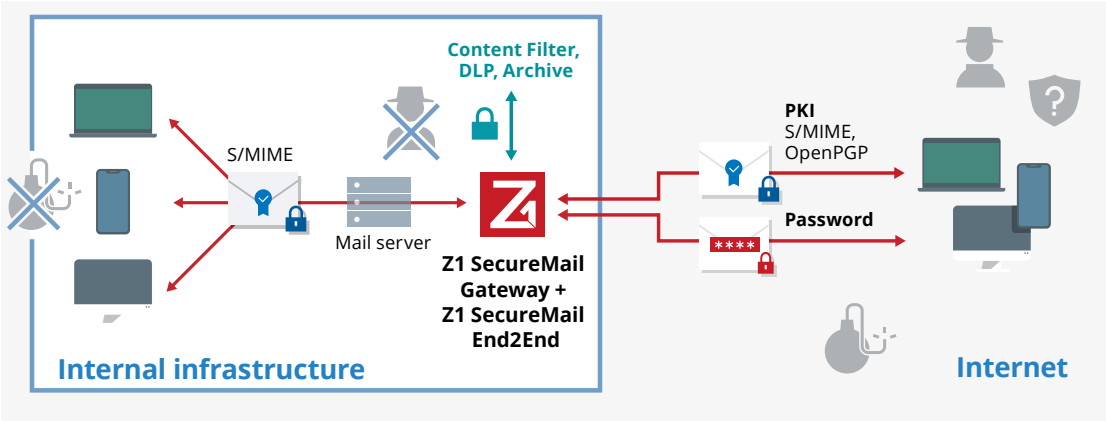

Fig. 4: Organizational End2End State-of-the-Art email encryption – Internal S/MIME, external encryption, and decryption depending on communication partner technology.

What remains is the prerequisite to issuing your own internal S/MIME keys and certificates for exclusive use on your internal routes. Z1 SecureMail Solutions then do the translation between internal and external key management.

Personal End2End Encryption

Z1 SecureMail End2End also supports Personal E2EE encryption. You might not even want the re-encryption on the gateway for some use cases. Hypersensitive communication between board members might be a use case where you wish to encrypt from the sending device to the recipient's device.

If you want to save the hassle of certificate management and prevent human error, Z1 SecureMail End2End is the appropriate solution. It provides E2EE analogous to end-to-end encryption as used by private individuals outside the corporate world.

How to proceed

Whatever your End2End encryption requirements are, Zertificon can fulfill them. With Z1 Solutions, emails can be encrypted on all routes, mail servers, and end devices, efficiently guaranteeing corporate-wide compliance, data protection, and data sovereignty – no matter whether you have chosen on-premises or cloud deployments. You will make digitalization secure and your workflows compliant.

All possible encryption methods are supported. Now, it is up to you to think about your needs and use cases. Choosing Z1 SecureMail Gateway is always the right decision you can't go wrong with for a start. And, you can always take it from there at a later point in your secure email journey.

Learn more:

Z1 SecureMail Gateway

Z1 SecureMail End2End

Or get in touch directly:
sales@zertificon.com

Be the first to know about new white papers, webinars, etc.
Subscribe to Zertificon's newsletter

Zertificon Solutions GmbH

Zertificon is a leading software manufacturer in the IT security field based in Berlin. The company is independent and founder-managed with its own in-house development, sales, and support departments. Zertificon is about 120 employees strong and still growing.

The Zertificon team pioneered the server-based email encryption market over 15 years ago with the award-winning **Z1 SecureMail Gateway**. Today, the company is one of the driving forces in IT security and data protection for electronic business communications with innovative, forward-looking solutions.

Zertificon focuses on developing user-friendly and cost-effective comprehensive security concepts for confidential email and data exchange. In addition to **Z1 SecureMail Gateway**, the proven solution for email encryption and email signature, and **Z1 CertServer** for central certificate management and validation, Zertificon's portfolio includes **Z1 SecureHub**: a web-based portal solution for secure file transfer of all formats and sizes. With **Z1 MyCrypt BigAttach**, **Z1 SecureHub** is operated directly from the mail program.

Last but not least, Zertificon's latest innovation, **Z1 SecureMail End2End**, offers enterprise-grade end-to-end encryption as an extension of the **Z1 SecureMail Gateway** and defines state-of-the-art Organizational or Personal End2End. **Z1 MyCrypt Mail** is available as an add-in for MS Outlook and Lotus Notes or as iOS and Android apps for use on end devices. Zertificon developed virtual **Z1 Appliances** for easy integration and efficient and smooth operation of Z1 solutions. As an operating system, Zertificon has been deploying Linux based on Debian distribution, which is highly regarded in the IT security community.

Zertificon's support services are highly renowned and offer fast and expert help in case of operational questions. Zertificon also enables your company to easily meet the highest security and compliance requirements in secure business communications.

Contact us today. We are sure to have the right offer for you.