CLEARSWIFT
MIMEsweeper™
Simplifying content security

FACTSHEET

Email encryption

Comfortable Encryption for Clearswift MIMEsweeper for SMTP

Secure email correspondence with CompanyCRYPT Encryption

The challenge

Unprotected email traffic on the way to the recipient is permanently at risk to be read, intercepted, manipulated and secretly forwarded by third parties. Lack of security awareness repeatedly leads to business secrets being distributed via email or confidential data being lost. Hence, companies are being increasingly compelled by new laws and regulations to protect their email traffic.

COMPANYCRYPT®
The encryption module for MIMEsweeper

The risks of unknown content within encrypted emails

The encryption of emails and the use of digital signatures are helpful for the protection of confidential data, however, these technologies also raise new safety issues. If an encrypted email is received or sent it must be ensured that it does not contain any risks such as malicious code, viruses or unauthorised transfers of confidential information (this also includes the keys for the encryption).

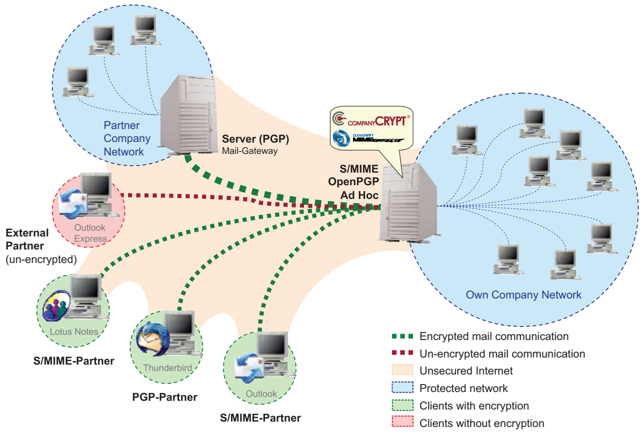
MIMEsweeper has been developed in such a way that it supports the leading encryption technologies for the generation of gateway signatures, encryption and decryption. It also supports the guideline-based management of risks, which goes hand in hand with the encrypted emails.

It is the nature of encrypted emails that the content may not be checked, even not for possible risks. Thus the protected incoming emails must be decrypted first before MIMEsweeper can carry out a content analysis. During the sending process MIMEsweeper checks emails for security risks before they are forwarded to be encrypted. The transfers that are confidential in accordance with the guidelines are encrypted automatically once they passed the content inspection.

The solution

With the help of CompanyCRYPT confidential emails are encrypted centrally in compliance with legal without the need for any user interaction. Besides the personal signing and encryption of eMails the gateway also allows the signing with a company key, much like an internal post office.

The seamless integration of CompanyCRYPT into MIMEsweeper is the key to have encrypted content checked by virus scanners, anti-Spam filters and content-scan engines. Only this way security guidelines may be also applied to encrypted emails.



Your checklist when selecting an encryption solution

1. **Choose a solution that is transparent and that requires no separate action on the part of the users. Often the activation of vital security measures is forgotten and users have to be trained additionally**

2. **Decrypt at the gateway. Thus content analysis, virus protection and company guidelines may be applied to encrypted contents across the company.**

3. **Use several international standards. This makes you flexible and open to the method used by your communication partner and because you can use both standards (OpenPGP and S/MIME).**

4. **In addition to the standard processes choose further technology for ad hoc encryption, if the external partner cannot use PGP or S/MIME or if agreed levels of security must be complied with in the event of spontaneous encryption requirements.**

5. **Choose a solution with comfortable user control to carry out guideline-based encryption This will help you achieve the requirements for revision security and flexible activation of confidentiality.**

6. **For the simple administration the encryption must integrate optimally into the content security system, a) so that the encryption solution does not make your mail-infrastructure more complex or that no single points of failure may result, b) so that the guideline management and encryption may be controlled from one station only and c) so that no further hardware is required for encryption.**

7. **Use granular encryption guidelines for various user groups, e.g. policy-based methods for users or systems with obvious encryption obligations. Activate site2site encryption in order to encrypt the traffic to and from entire mail domains. Still let specific senders personally activate the gateway encryption for sensitive documents.**

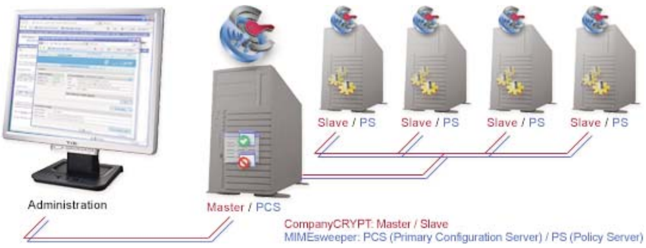
CLEARSWIFT
MIMEsweeper™
Simplifying content security

FACTSHEET

Email encryption

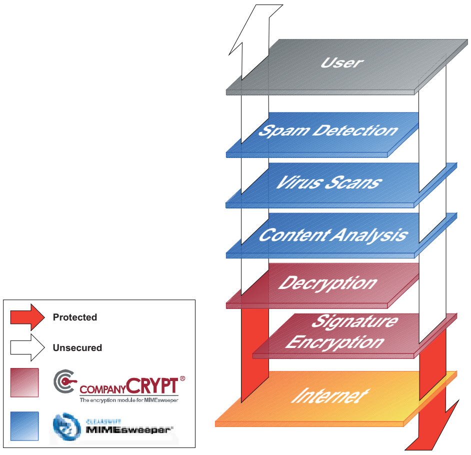
Flawless integration into MIMEsweeper

- Complete integration directly into the content security gateway MIMEsweeper for SMTP without the need for additional hardware
- Allows for the full use of all security policies including content check, virus protection and anti-Spam also for encrypted emails
- Central, web-based management on the MIMEsweeper
- Scalable due to the MIMEsweeper clustering


Administration
Master / PCS
Slave / PS
Slave / PS
Slave / PS
Slave / PS
CompanyCRYPT: Master / Slave
MIMEsweeper: PCS (Primary Configuration Server) / PS (Policy Server)

Highlights

- Automatic encryption and decryption, central and without interaction on the part of the user
- Full support of the standards S/MIME and OpenPGP
- Ad hoc encryption for the immediate encryption to communication partners without access to encryption technology
- Extensive signature check and signing of emails with user or company key
- Low administrative expenses due to automated key generation (onboard CA), independent key exchange and fully automated key import
- Intelligent encryption scenarios, such as best effort, guarantee the optimal use of email encryption without any configuration expenses
- Encryption of emails in compliance with legal regulations
- Support of domain, team and gateway certificates



FAQs

On which MIMEsweeper systems may CompanyCRYPT be installed?

CompanyCRYPT is compatible with all versions of the software MIMEsweeper for SMTP.

Does the recipient also require CompanyCRYPT in order to be able to receive encrypted emails?

No, he does not specifically require CompanyCRYPT. Each email solution, which supports one of the two standards S/MIME or OpenPGP, is suitable for secure communication – no matter whether it is a gateway or desktop solution

What are the additional requirements for the system hardware?

As CompanyCRYPT is installed directly onto the MIMEsweeper servers no additional hardware is required.

How can I encrypt if my communication partner does not yet use any encryption technology?

If your partner uses neither S/MIME nor OpenPGP CompanyCRYPT uses an ad hoc process. In this case the information is protected using a highly secure AES encryption algorithm and sent as a self-decrypting archive.

Can I continue to use existing PGP keys and certificates with CompanyCRYPT?

Yes, your existing certificates and keys, which you have already acquired from a trust centre, may be easily imported. As CompanyCRYPT has its own onboard CA the generation of new keys and certificates is also possible without any additional costs.

Secure Internet Traffic

Secure Internet Traffic
S.I.T. GmbH & Co. KG
Goseriede 4, D-30159 Hannover
Tel. +49 511 89 997-10
Fax +49 511 89 997-12
Email: info@companycrypt.com
www.companycrypt.com

Contact Clearswift

07-08

United States
100 Marine Parkway, Suite 550
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

United Kingdom
1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Spain
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón, Madrid
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

Germany
Amsinckstrasse 67, 20097 Hamburg
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Australia
Level 5, Suite 504, 165 Walker Street,
North Sydney, New South Wales, 2060
Tel : +61 2 9424 1200 | Fax : +61 2 9424 1201

Japan
Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
Tokyo 105-0011
Tel : +81 (3) 5777 2248 | Fax : +81 (3) 5777 2249