Secure Internet Traffic

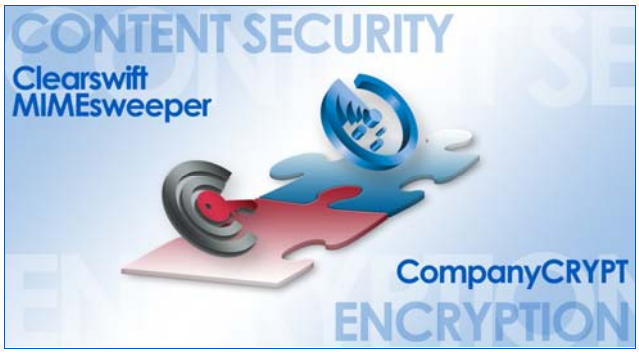
COMPANYCRYPT®
The encryption module for MIMEsweeper

CompanyCRYPT the encryption module for MIMEsweeper

Technical Specifications

Product

CompanyCRYPT is an add-on for Clearswift MIMEsweeper for SMTP. It extends the company eMail policies by centralized encryption and signatures. Through full support of the two encryption standards S/MIME and OpenPGP a market coverage of 100% is achieved.



Key benefits

Security

- Protects valuable corporate information and personal data within eMails
- Level of encryption, applied on eMails, even meets strict legal obligations
- Safeguards eMail communication against manipulation or falsification during transmission
- Enables you to really apply all security policies including content-scan, virus-scan and anti-spam even on encrypted eMails
- Best choice security solution for MIMEsweeper infrastructures
- Top level security and performance architecture based on the unique MIMEsweeper-Integration

Features

- Universal encryption scenarios, like "Best Effort" or "Always Encrypt"
- Ability to enforce encryption and signing methods by individual MIMEsweeper policies
- Flexible eMail encryption (Message body and attachments or attachment only encryption)
- User controlled activation of various protective measures (End user can influence functions with easy to use keywords)
- Support for S/MIME and OpenPGP
- Spontaneous ‚Ad Hoc Encryption' for recipients that have no encryption technology available
- Utilizes accredited and validated security algorithm based on GnuPG and OpenSSL
- Support for domain-, team- and gateway certificates
- Onboard certification authority (CA) with support for a local CRL (Certificate Revocation List)
- On-demand generation of keys and certificates
- Fully automatic import of keys and certificates
- Site-to-Site encryption (Secures the complete traffic between two eMail/SMTP domains)
- Comprehensive signature validation across the whole chain of issuer
- Integrated Update-Check

MIMEsweeper Integration & deployment

- Simple installation and a quick start into operation is provided by the direct integration into the MIMEsweeper content security solution using top level technology
- No investment in hardware and maintenance for a stand alone gateway required
- Concerted integration into the existing eMail infrastructure (No modification on the eMail routing or the fail-over concept)
- An extensive selection of encryption scenarios, added to the MIMEsweeper, enable a flexible adoption of encryption policies
- Completely independent from the internal groupware like Lotus Notes, Microsoft Exchange or GroupWise
- Scalable from a single site system to geographically distributed implementations in a MIMEsweeper cluster
- Server-based and thereby transparent to the end user
- Best acceptance from the end user – no additional training required

Administration

- Centralized management and key handling even in distributed environments
- Secure and yet intuitive administration via a web based interface (HTTPS)
- Keyserver functionality (automatic key exchange) for S/MIME and OpenPGP with MIKE (Mail Initiated Key Exchange)
- Administration of trusted issuer in a dedicated Trusted-CA-Store
- Automatic scheduled backup and restore function for the configuration, keys and certificates
- Detailed statistics and graphical traffic reports are available through the MIMEsweeper reporting
- Minimised administrative effort by automation of key import, key generation, key exchange, update of local CRL and system backup

Highlights:

- Automatic central de- and encryption, without end-user interaction
- Full support for the standards S/MIME and OpenPGP
- Spontaneous ‘Ad Hoc Encryption' for communication partners that have no encryption technology available
- Simple integration into the content security gateway MIMEsweeper without need for extra hardware
- Allows to fully apply all security policies including content-scan, virus-scan and anti-spam even on encrypted eMails
- Single point of management and key handling
- Scaleable based on the MIMEsweeper clustering

Free trial version at: www.companycrypt.com

Secure Internet Traffic

COMPANYCRYPT®
The encryption module for MIMEsweeper

CompanyCRYPT the encryption module for MIMEsweeper

Technical Specifications

System requirements

Hardware

The requirements for MIMEsweeper for SMTP and CompanyCRYPT are outlined in the following.

- Pentium IV or better (Dual Core 2 GHz recommended)
- 2GB RAM or more
- 20 GB HDD space

Software

- Windows Server 2003 Standard or Enterprise, Windows Server 2008 R2 Standard or Enterprise
- MIMEsweeper for SMTP 5.x

Standards & Formats

- SMTP, HTTP(S)
- S/MIME (RFC 2633), OpenPGP (RFC 3156, RFC 2440, RFC 4880)
- X.509, PEM, DER, KEY, PKCS#7, PKCS#12
- OpenPGP-Keys, PGP/MIME, PGP/Inline
- Asymmetric encryption: RSA, RSA-E, RSA-S, ELG-E, DSA, ELG
- Symmetric encryption: DES, 3DES, CAST5, AES (128/192/256), RC2, RC5, BLOWFISH, TWOFISH
- Hash: MD5, SHA1, RIPEMD160, SHA (224/256/384/512)

Generation keys

- 1024 Bit – 4096 Bit (OpenPGP and S/MIME)

Importing keys

- 168 Bit – 4096 Bit (OpenPGP and S/MIME)
- OpenPGP: Any file extension (ASCII- or binary encoded)
- S/MIME: X.509 v3 Any file extension (DER- or PEM encoded)
- Private or public keys/certificates, as well as CA certificates or self signed keys

S/MIME - Additional features

- Option to select between „opaque“- and „detached“ signing on all signing jobs
- S/MIME-Attachments without declaration in the SMTP-data section (MIME header: unspecific ‘Content-Type’)
- Support for different certificates for signing and encryption
- Support for S/MIME v3 extension (i.e. usage restrictions)
- Preinstalled root certificates from well known CA’s in a local certificate store

PGP - Additional features

- Personal or company signature only on body text
- Only encryption of attachments
- Automatic decryption of single (manually) encrypted PGP-file attachments (Binary or ASCII encoded, *.PGP *.GPG *.ASC)

Ad Hoc Encryption - Additional features

- Passphrase based protection method without certificate or key exchange
- Symmetric encryption using AES-128 CBC cipher
- Automatically generated or manual password
- Encryption of all email parts including the subject

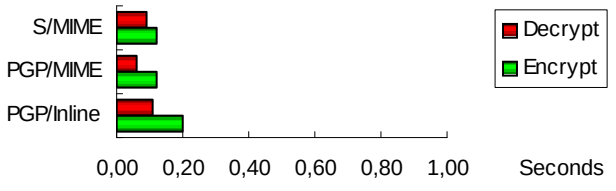
Performance

The extreme processing speed of this solution, decryption and encryption alike, will even meet the requirements of heavy duty environments.

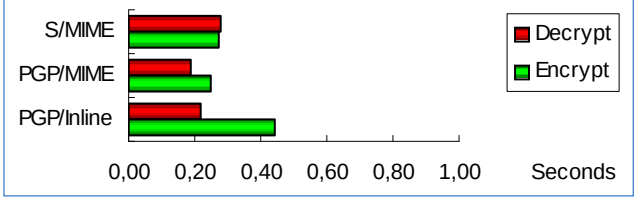
Each gateway will be able to process eMail data up to 5 Gigabyte per hour.

Processing times

eMail size 10 Kbytes



eMail size 1024 Kbytes (1 MB)



Test parameter/environment:
- Hardware: AMD Athlon 2,7GHz, 1 GB RAM
- Key length (de- and encryption): 2048 bit
- Sym. algorithm: AES-128 (PGP) / 3DES (S/MIME)

Issued by:

Contact Secure Internet Traffic

Address:
S.I.T. GmbH & Co. KG
Kaiser-Wilhelm-Str. 9
30559 Hannover
Germany

Phone:
+49 511 89997 10

Fax:
+49 511 89997 12

eMail:
info@companycrypt.com

Internet:
www.companycrypt.com

Secure Internet Traffic