

# Clearswift E-Mail Verschlüsselung

## HIGHLIGHTS

- Automatische Ver- und Entschlüsselung, zentral und ohne Interaktion der Benutzer
- Vollständige Unterstützung der Standards S/MIME und Open PGP
- Ad Hoc Encryption zur sofortigen Verschlüsselung auch an Kommunikationspartner ohne Verschlüsselungstechnologie
- Umfassende Signaturprüfung und Signierung von Emails mit User- oder Firmenschlüssel
- Einfache Verwaltung und Administration mit zentralem Keymanagement
- Intelligente und flexible Verschlüsselungsszenarien, wie Content based Encryption
- Gesetzeskonforme Verschlüsselung

## VERSCHLÜSSELUNG UND SIGNATURPRÜFUNG ALS TEIL EINER UMFASSENDEN E-MAIL CONTENT SECURITY LÖSUNG.

Vertraulichkeit, Integrität und Authentizität versendeter Informationen gewinnen immer mehr an Bedeutung. Ähnlich wie Sie im geschäftlichen Alltag vertrauliche Unterlagen als verschlossenen Brief oder Einschreiben versenden, verhält es sich auch mit der E-Mail-Kommunikation.

Die im Clearswift SECURE Email Gateway integrierte Verschlüsselungstechnologie schafft durch Verschlüsselung und Signaturprüfung ein hohes Maß an Vertraulichkeit und bewahrt vor dem Verlust sensibler Unternehmensdaten.

### Content-Scan trotz Verschlüsselung

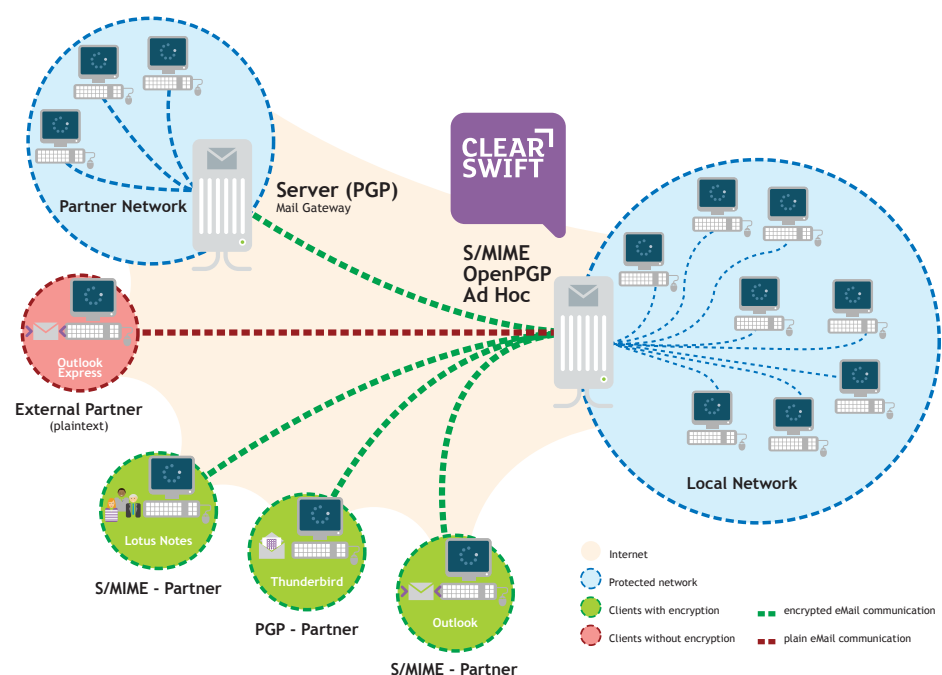
Durch die nahtlose Integration von CompanyCRYPT in Clearswift SECURE Email Gateway wird die Überprüfung verschlüsselter Inhalte durch zentrale Virens Scanner, Anti-Spamfilter und Content-Scan-Engine möglich und Richtlinien können einheitlich angewendet werden.

### Sichere Standardverfahren PGP und S/MIME

Beide international etablierten Verschlüsselungsstandards Open PGP und S/MIME werden vollständig unterstützt. Damit können Sie mit allen erhältlichen Client-Implementationen bei Ihren Kommunikationspartnern verschlüsseln.

### Ad Hoc Encryption - Verschlüsselung für Jedermann

Das Clearswift SECURE Email Gateway bietet mit der Ad Hoc Verschlüsselung eine komfortable Möglichkeit, sofort und an jeden Empfänger verschlüsselte Nachrichten zu schicken. Somit ist eine gesicherte Übertragung von E-Mails jetzt an alle Kommunikationspartner möglich, auch wenn diese selbst keine eigene Verschlüsselungstechnologie einsetzen.



## FUNKTIONEN

- Unterstützung von S/MIME und Open PGP
- Flexible Verschlüsselungsszenarien
- Content-bezogene Verschlüsselung
- Site-to-site Verschlüsselung
- Vollständige Signaturprüfung
- Support für Domänen-, Team- und Gateway-Zertifikate
- Kostenfreie Generierung eigener Schlüssel und Zertifikate
- Einsatz transparenter Verschlüsselungsroutinen

## VERSCHLÜSSELUNGSFORMATE

- S/MIME (RFC 2633)
- Support für Opaque und abgehängte Signatur
- OpenPGP (RFC 2015/3156)
- Support für PGP MIME und PGP Inline
- Asymmetrische Verschlüsselung: RSA, RSA-E, RSA-S, ELG, ELG-E, DSA
- Symmetrische Verschlüsselung: DES, 3-DES, CAST5, AES (128/192/256), RC2, RC5, Blowfish, Twofish

## Automatische Verschlüsselung/Signierung

Neben einer personalisierten E-Mail-Signierung und -Verschlüsselung ermöglicht das Modul auch die Signierung per Firmenschlüssel im Sinne einer hausinternen Poststelle. Damit beugen Sie dem Missbrauch Ihrer E-Mail-Adressen (Phishing) und Ihres Markennamens vor und schaffen Vertrauen bei Ihren Kommunikationspartnern.

## Zentrales Management

Clearswift Verschlüsselung unterstützt die Clusterfähigkeit des SECURE Email Gateway und ist somit beliebig skalierbar.

Durch eine automatische Synchronisation wird die Verwaltung in komplexen und verteilten Umgebungen enorm vereinfacht. Die Administration erfolgt zentral und in einem Schritt.

## Keine Anwenderschulung

Die Verschlüsselung und Signierung der E-Mails erfolgt zentral und ohne jede Interaktion der Benutzer. Der Installations- und Schulungsaufwand reduziert sich dadurch erheblich, da keine Anpassung am Client nötig ist.

### Encryption/Decryption Defaults

[Click here to change these settings](#)

**Password Encryption**

- The password used will be automatically generated with a length of 16 characters
- The subject line will not be protected
- Automatically generated passwords will not be logged
- The email containing the encrypted original and the password notification will be in English

[Click here to change these settings](#)

**PGP**

- Messages will use the MIME format of PGP.
- PGP attachments will use the .pgp extension.

[Click here to change these settings](#)

**S/MIME**

- Messages will be signed using the detached format.

[Click here to change these settings](#)

**Decryption Summary**

- The decryption summary will be in English.

[Click here to change these settings](#)

**Encryption/Decryption Logging**

- Produce **debug** level logging information while encrypting and decrypting messages.

[Click here to change these settings](#)

**Original Encrypted Messages**

- When applying encryption endpoints prefer the original encrypted message to re-encryption.

### Modify Mail Encryption Endpoint

[Click here to change these settings](#)

**Overview**

The name for this endpoint is automatically maintained. Edit this panel if you would like to supply your own name.

[Click here to change these settings](#)

**For mail sent to the**

Email address - alyn@clearswift-test.com

[Click here to change these settings](#)

**Messages will be encrypted**

- Encrypt the message body and attachments using **also holder / Clearswift, Hacking, Threats, UAT (PGP)**.

[Click here to change these settings](#)

**PGP Options**

- Messages will use the MIME format of PGP. (Default Setting)

## Kontakt



Clearswift GmbH  
Amsinckstr. 67  
D-20097 Hamburg  
info@clearswift.de  
www.clearswift.de

### Clearswift

Standard Support ist für alle Clearswift-Kunden (bzw. während der Evaluation) erhältlich.

### Standard Support

- 24x7 Telefon und E-Mail Support
- Zugang zur Knowledge Base
- Service Feeds zur Aktualisierung
- Service Packs und Patches

## Ihr Reseller vor Ort

