Clearswift Email Encryption

HIGHLIGHTS

- Automatic encryption and decryption, centrally and without user interaction
- Full support of the S/MIME and OpenPGP standards
- Adhoc password protected zip file to recipient not using encryption
- Comprehensive signature verification and signing of emails with the user or the company key
- Easy management and administration with centralised key management
- Intelligent and flexible encoding scenarios using Content and Policy based encryption

Email Encryption/Decryption and Signing integrated into a comprehensive content security solution

Clearswift's SECURE Email Gateway provides an easy to use approach to providing secure email conversations. The technology enables customers to provide the privacy, authenticity and integrity of the communication that secure messaging offers, but without the complexity and high administration cost of other systems.

The Clearswift SECURE Email Gateway with integrated encryption technology enables business to communicate with confidence and protects them from the risk of sensitive data loss.

Security using standards encryption protocols

The SECURE gateway supports both international standards of OpenPGP and S/MIME message formats to enable communications to recipients who use standard mail clients such as Outlook, Notes and Outlook Express.

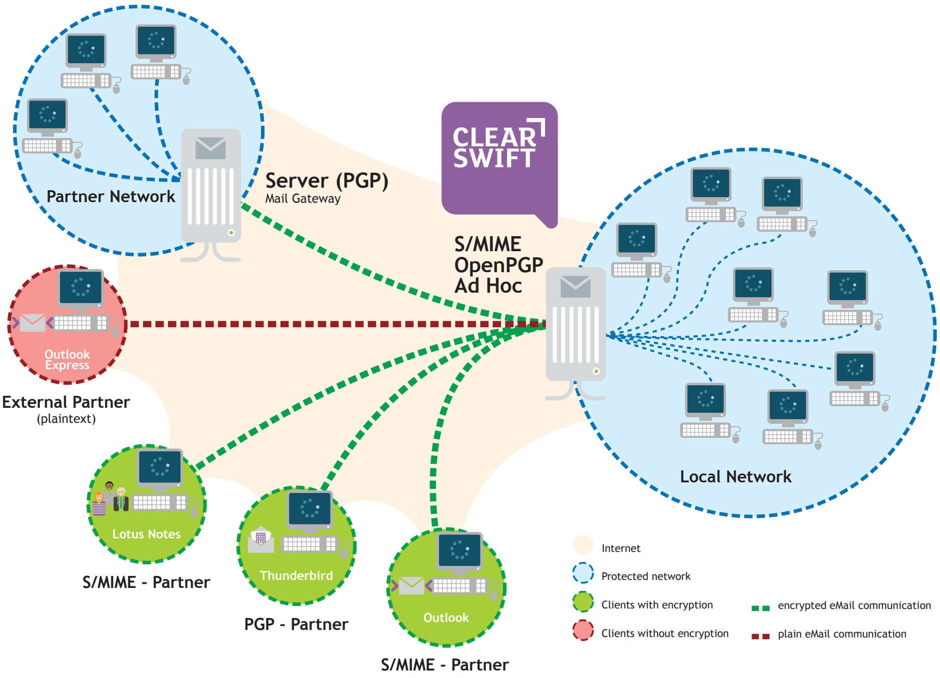
Ad Hoc Encryption - Encryption for everyone !

For recipients who do not use either PGP or S/MIME then the SECURE mail gateway can still send the message in a secure format using a password protected zip. This file can then be opened without needing any additional software and can also be opened when the recipient is not connected to the internet.

Content scan encrypted messages

With integrated encryption the Clearswift SECURE Email Gateway can decrypt encrypted messages by the comprehensive Anti-spam, Anti-virus and content filtering engines to ensure email adheres to the corporate email policy.

Decryption can apply to both inbound and outbound messages providing correct key material.



FEATURES

- Support for S/MIME and Open PGP
- Flexible Encryption options
- Content based encryption
- Site-to-site encryption
- Signature verification
- Support for domain, group and gateway certificates
- Built-in generation of keys and certificates
- Transparent to end-users

ENCRYPTION FORMATS

- S/MIME (RFC 2633)
- Support for Opaque and detached signing
- OpenPGP (RFC 2015/3156)
- Support for PGP MIME and PGP Inline
- Asymmetric encryption: RSA, RSA-E,RSA-S, ELG, ELG-E, DSA
- Symmentric encryption: DES, 3-DES, CAST5, AES (128/192/256), RC2, RC5, Blowfish, Twofish

Automatic Encryption / Signing

Messages can also be signed with a corporate signing key. This will ensure that recipients can be sure that messages arrive from your organisation are valid, and they are not being subjected to a Phishing attack.

Central Management

Certificate stores and policies can be replicated across Gateway nodes permitting high scalable solutions for encryption.

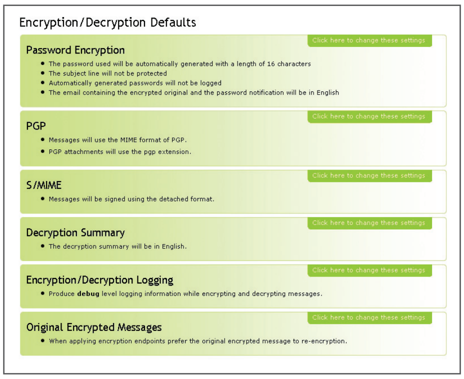
The administration is centralised to make manageing the Encryption features very easy. Granular access control Permits only the correct Systems Administrators to modify the encryption rules

The intuitive, web based management interface combines ease of configuration and efficient management

No user training

The encryption and signing of emails can be configured centrally without any interaction of the users.

No certificates and no keys for users to worry about removes end user confusion.



Encryption/Decryption Defaults

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

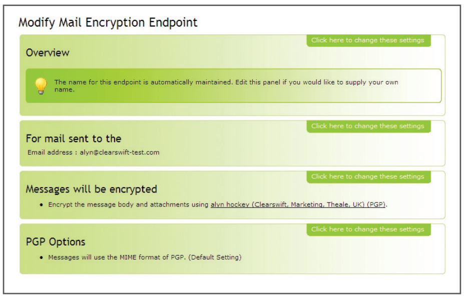
PGP
- Messages will use the MIME format of PGP.
- PGP attachments will use the pgp extension.

S/MIME
- Messages will be signed using the detached format.

Decryption Summary
- The decryption summary will be in English.

Encryption/Decryption Logging
- Produce **debug** level logging information while encrypting and decrypting messages.

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



Modify Mail Encryption Endpoint

Overview

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

For mail sent to the

Email address : alyn@clearswift-test.com

Messages will be encrypted
- Encrypt the message body and attachments using alyn hockey (Clearswift, Marketing, Theale, UK) (PGP).

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

Get in Touch

Clearswift Ltd.
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire RG7 4SA
England
www.clearswift.com/

Contact Clearswift

Standard support is available to any Clearswift customer (or during an evaluation).

Standard support

- 24/7 Phone and Email Support
- Knowledge Base Access
- Service feeds to update your deployment
- Service packs and patches

Japan only

9-5 Monday to Friday Phone & Email Support