CLEAR SWIFT

Frequently Asked Questions

CLEARSWIFT SECURE ENCRYPTION PORTAL

Alyn Hockey
06/09/2011

Introduction

This document answers some of the frequently asked questions about Clearswift's SECURE Encryption Portal.

How is this feature licensed?

Licensing for the SECURE Encryption Portal is based on the number of senders using it. Customers should not exceed the number of licensed users in any given month.

SECURE Encryption Portal is **not** licensed according to the number of message recipients.

Are there restrictions on message volumes?

The feature is licensed on the basis that the average number of email messages sent per month by each sender is no more than 240 messages, with an average size of no more than 500kb.

If I want to send thousands of messages from a single address, do I need a 1 user license?

The feature is priced for "normal" usage as described above. If a customer wants to use the feature for this type of volume messaging, a separate pricing model is used. For more details contact Clearswift.

In order to buy this feature, do customers also have to buy the S/MIME, PGP and Password encryption features?

No.

Do customers have to license all SMTP users for this feature?

No. Customers need only license users that require this feature. If required, this can be a subset of total user numbers. User numbers and volumes will be audited and verified against customer licensed values.

Is there a minimum number of licenses I have to buy?

Customers must buy at least 25 user licenses.

How long can messages be stored at the pickup centre for?

The default period of time any message can stay on the portal for is 30 days. Customers may extend that period, but may incur additional charges.

Does the portal support both push and pull encryption techniques?

Yes.

What's the difference between push and pull encryption?

Pull encryption sends a notification to the recipient to come to the pickup centre to read their message over an http/s connection. They have a user-specific password that authenticates them with the system, ensuring that messages can only be opened by them. Most deployments use this method of encryption.

Push encryption sends the encrypted message directly to the recipient; messages are opened using a pre-defined password. Recipients must use the Secure Reader plugin to open the message.

What factors influence the decision to encrypt?

The decision to encrypt the message can be based on:

Direction: Such as sender or recipient

Content: Such as subject line, message body text, attachment name or type, attachment content, message headers (such as X-header).

Is there a restriction on the size of message that can be encrypted?

Yes. In order to provide an acceptable level of performance for the recipient, the maximum message size is currently 25Mb.

Where are the data centres hosted?

UK, North America and Canada.

Are the data centres secure?

Yes, they have been certified with numerous agencies and standards bodies:

- SAS 70
- PCI security standards council
- CCTM – CESG Tested
- Deloitte Webtrust Certification Authorities

What encryption methods are used to get messages to and from the pickup centre?

The initial message is sent using the Transport Layer Security (TLS) protocol. On arrival at the pickup centre, the message is immediately encrypted using a PKI based encryption technology, whereby only the recipient of the message can open it.

A notification message containing an hyperlink to a secure HTTP/S web site is generated and sent to the recipient, who simply clicks the link and is taken to the pickup centre, where they can read and respond through their browser.

Are the pickup centres fault-tolerant?

Yes, multiple servers are deployed for each configuration. If any one of those servers were to fail, the other servers in the cluster would continue to handle the workload while the failed server is replaced.The system is designed not to have a single point of failure at any level, from the network up to the application.

Do I need a particular version of the Secure Email Gateway?

Clearswift always recommends that you use the latest version of our software, but any version from 3.2 or later is supported.

For further information

Contact Information:
Product Manager Alyn.Hockey@Clearswift.com

Contact Clearswift

UK - International HQ
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA
UK
Tel: +44 (0) 118 903 8903
Fax: +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201
Email: info@clearswift.com.au

Germany
Clearswift
Landsberger Straße 302
D-80 674 Munich
GERMANY
Tel: +49 (0)89 904 05 206
Fax: +49 (0)89 904 05 810
Email: info@clearswift.de

Japan
Clearswift K.K
7F Hanai Bldg.
1-2-9 Shibakouen,
Minato-ku, Tokyo
105-0011
JAPAN
Tel: +81 (3)5777 2248
Fax: +81 (3)5777 2249
Email: info.jp@clearswift.co.jp

Spain
Clearswift España S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón
Madrid
SPAIN
Tel: +34 91 7901219 / +34 91 7901220
Fax: +34 91 7901112
Email: info.es@clearswift.com

United States
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
UNITED STATES
Tel: +1 856-359-2360
Fax: +1 856-359-2361
Email: info@us.clearswift.com