clearswift
A HelpSystems Company

Clearswift Trust Center

Email is still the preferred method of business collaboration in use. With the growth of sensitive content being shared legitimately between organizations and the pressures to ensure data is being sent in a secure fashion, the use of email encryption is almost essential. Multiple analysts show the email encryption market growing with a 20+% CAGR from 2018-2025.

Products

- Clearswift SECURE Email Gateway

Support

- Clearswift provides 24x7 global support as standard with additional options for premium support.

Encryption Options

There are a wide range of methods to secure data in transfer ranging from basic TLS to password protected documents using a secure staging server or using digital certificates. Different methods exist in order to address different use cases. For example, delivering a monthly utility bill to a domestic user is best served with a secure email portal, whereas frequent communications between parties sharing confidential information is best served using digital certificates.

Whilst there are additional costs to use email encryption, it is money well spent to protect the organization, its information and the costs associated with a data breach.

Benefits of email encryption

- Prevents content tampering
- Sensitive data is preserved
- Content remains unaltered
- Ensures message privacy
- Assures email sent from a certified user

Key Considerations

Previously, use of Digital Certificates has not become ubiquitous due to the manual process of acquiring and issuing them. While possible, it creates overhead for the already busy IT department as certificates also need to be renewed on a regular basis or they expire resulting in insecure or delayed communications. The solution is automation of all the tasks. The only pre-requisite then would be a source of unassigned certificates; these could be generated locally if there is a deployed Public Key Infrastructure (PKI), purchased via a website or alternatively, use a Managed PKI (MPKI) service that can integrate into the existing environment.

Benefits of automated certificate provisioning

- Reduced administration overhead
- Bulk provisioning
- Uses LDAP attributes to populate certificate fields
- Only use what is needed

Supported MPKI

SwissSign

About Clearswift

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to securely collaborate and drive business growth. Its unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption, enabling organizations to gain visibility and control of their critical information 100% of the time.

As a global organization, Clearswift is headquartered in the United Kingdom, with offices in the United States, Germany, Australia and Japan and has an extensive partner network across the globe.

For more information:

www.clearswift.com

Contact Us

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

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 (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
Australia

Tel: +61 (0) 294 241 200
Technical Support: +61 2 9424 1200
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0) 221 8282 9888
Technical Support: +49 (0)800 1800556
Email: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

United States
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

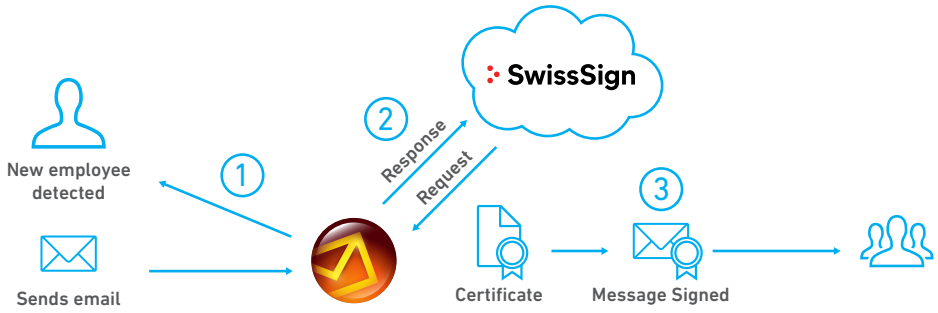
Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

The Clearswift Trust Center Solution

The Clearswift Trust Center component extends the ability of the Clearswift SECURE Email Gateway to connect to MPKI providers to provide the key issuance and renewals in an automated fashion.

In order to use the automation of the MPKI, a corporate user account must be set up and typically, certificates pre-purchased in bulk. When first being deployed, the solution can automatically provision multiple users based on Active Directory or an LDAP service and those with existing certificates will be automatically included into the system:

1) the Gateway will detect new users who require a digital certificate,
2) then automatically provision them through the MPKI service, drawing down from the bulk purchased certificates,
3) to be used automatically for signing and encryption purposes.



Clearswift SECURE Email Gateway detects and provisions new users through the MPKI service.

Once provisioned, the certificate will be replicated across peered Gateway certificate stores to ensure availability.

Certificate expiry dates are constantly monitored and when a certificate is close to expiration, the Gateway will automatically provision a replacement, ensuring that users do not lose the ability to send secure email.

For more information or to contact the Clearswift team for a discussion, visit www.clearswift.com

clearswift
A HelpSystems Company