FORTRA™

SOLUTION BRIEF (CYBERSECURITY)

Encryption for the Public Sector

With an ever-growing need for secure business communication and collaboration methods, email remains the primary channel for information sharing. However, the challenge for many in the public sector, including government departments, local government, government agencies and public bodies, is how to share and receive information securely with each other, third-party organisations, and citizens. Encryption is the answer, providing it is easy-to-use and as transparent as possible.

Business Problem

Today's businesses run on information and collaboration. Collaboration which used to be internal is now just as likely to include external parties and while communication methods are established, the type of communication and the risks associated have also changed. With the advent of data breaches and the consequential legal fines, there is an imperative to reduce the risk. Encrypting emails ensures that messages intercepted cannot be viewed by anyone apart from the intended recipient.

However, with encryption can come complexity. There are different solutions for different business uses. The optimal solution required for inter-governmental / inter- department communications is different from that which can be used with citizens. Understanding the differences and benefits will help determine the most cost efficient and effective solution for the business problem which needs to be solved.

There are two common business problems which email encryption can resolve:

1. Secure communication between government departments and third-party organisations.
2. Secure communication between a government department and citizens.

For those organisations with large files to be transferred between organisations, a Managed File Transfer solution with advanced content scanning is becoming more commonplace.

PRODUCT SUMMARY

Products

Clearswift Secure Email Gateway (SEG)

Encryption options available:

- On-premise portal-based encryption
- Cloud portal-based encryption
- PGP, S/MIME & Ad Hoc enterprise encryption

Managed File Transfer solution (MFT, which incorporates Clearswift Secure ICAP Gateway)

Support

Clearswift's Professional Services can help with architecture, design and implementation of all encryption solutions.

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

Pricing

Priced per user based on the solution or solutions used.

Encryption Solutions

For any encryption solution to be adopted by users, it needs to be as frictionless and transparent to both the sender and the recipient as possible. Clearswift's Deep Content Inspection (DCI) Engine, can use both content (for example PCI or PII) and context (the sender and the recipient) in conjunction with the business policy to automatically make the choice on which encryption method needs to be used. This removes the decision from the sender. Further automation makes it simple for the authorised recipient to open and decrypt the received email.

Transport Layer Security (TLS)

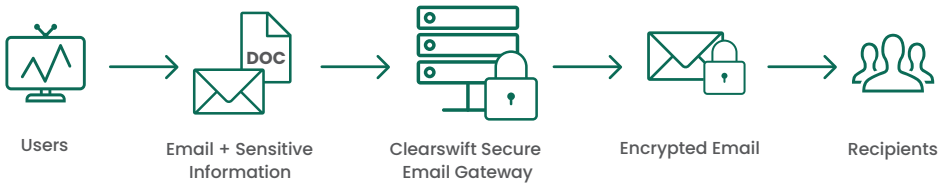
General email is secured in the transfer between compatible solutions using TLS. Polices can be set to ensure that TLS is used either opportunistically or enforced depending on the recipient organisation. However, TLS only encrypts server-to-server and does not encrypt to the end user, potentially leaving it open to being read by an unauthorised person, hence the need for more robust options.

The Clearswift Secure Email Gateway (SEG) meets the Government's and NCSC's Cyber Security Standard by supporting multiple other mechanisms to ensure that the email is genuine and from an authorised, non-spoofed source, including the use of DKIM, DMARC, and SPF functionality.

Government-to-Government / Third-Party Solutions

When dealing with regular communication between individuals in government departments or third-party organisations, the solution is to use the widely recognised PGP or S/MIME approach. The Clearswift solution automatically handles the required encryption certificates, using the public and private keys of the individual. Once a key has been automatically registered with the system, it is applied transparently, encrypting outgoing email and attachments with the recipient and key-guardian's public key after it has been scanned with the DCI engine.

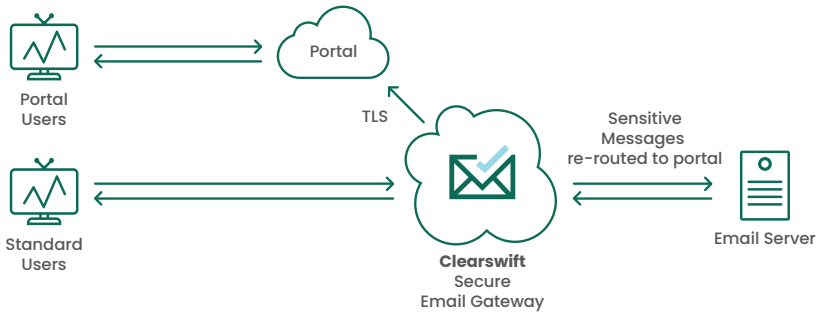
Upon receipt of an encrypted message, the content will be decoded with the key guardian's private key to enable full scanning for malware and any potential unwanted data acquisition issues. For those recipients who do not have a registered encryption certificate, there is the option to use Ad Hoc zip-based encryption, using a variety of encryption algorithms, including AES. This is where the email and its contents are encrypted in a zip archive with a password and the sender is then informed of the password which can be readily communicated with the recipient.



Government-to-Citizen Encryption Solution

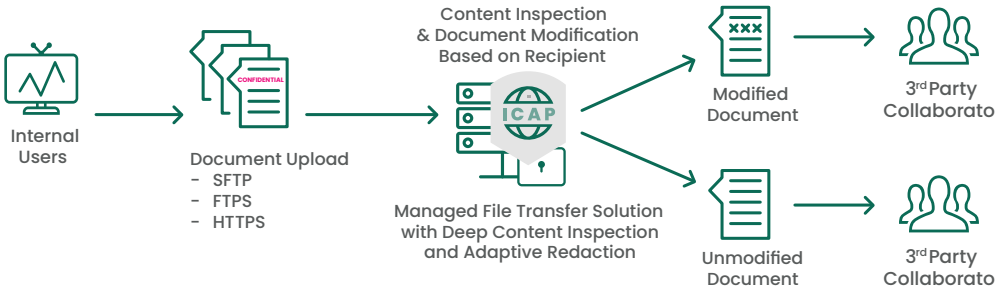
One of the best methods of secure email delivery for the non-technical user is to use an encryption portal which provides complete control for the organisation sending the email. It means the recipient can access the email using any web browser, over HTTP/S, and so can be assured that only they have access. The solution consists of deploying an additional host where email with sensitive content is routed by the Clearswift Secure Email Gateway to the portal, the portal then sends a notification message to the recipient about the new content and who then follows the instructions provided to retrieve the message from the portal via a browser.

The portal application and the data can be located wherever the organisation needs it, whether that is on-premise or in the cloud. Additional options are available for both secure webmail and PDF encryption, to provide flexibility for both the sending organisation and the recipient.



Managed File Transfer Solution

Increasingly large files are needing to be shared between collaboration partners, and unfortunately email has a limit to the size of the file which can be sent or received. The answer to this problem is to use a Managed File Transfer (MFT) solution which is combined with a DCI engine and policies to ensure that the information being shared has been fully authorised. Clearswift's Secure ICAP Gateway when used in conjunction with HelpSystems GoAnywhere MFT product provides this ability.

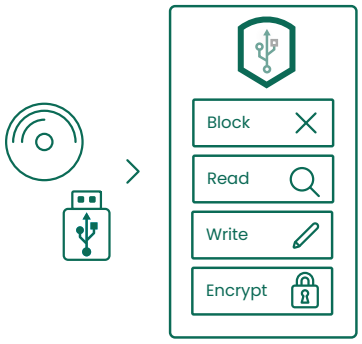


The MFT solution can also be used as a secure way for citizens to send electronic files into public bodies. In this configuration, the system will ensure encrypted transit of the files while the DCI engine will provide assurance that malware isn't being uploaded to infect government systems.

Small File Transfer (via USB)

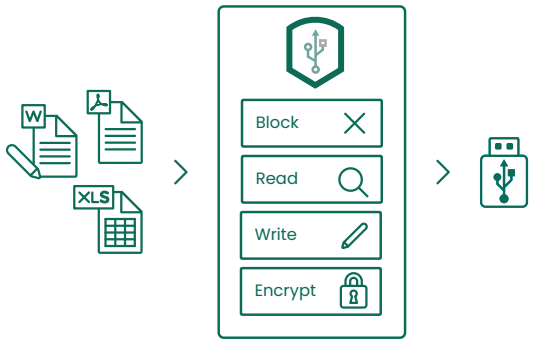
In many circumstances, using a USB stick to share a file is a lifesaver. Whether it is internally, or with third parties while 'on the road', the need to have to share something quickly is a weekly or even daily occurrence. Far from just handling small files, USB sticks can now be more than 1TB in size, making it the fastest way to share data – but it comes with a risk. The file could be malware, but this is the risk around data loss. Losing the stick and an unauthorised individual finding it and then the information on it. The solution to this issue is to use device control and/or encryption.

Device control enables organisation to determine which devices can or cannot be used. Granularity of policy enables organisations to determine the type, make or even the serial number of the devices which can be used. This works well but does create limitations (and therefore frustrations) around whether the person has access to the authorised device.



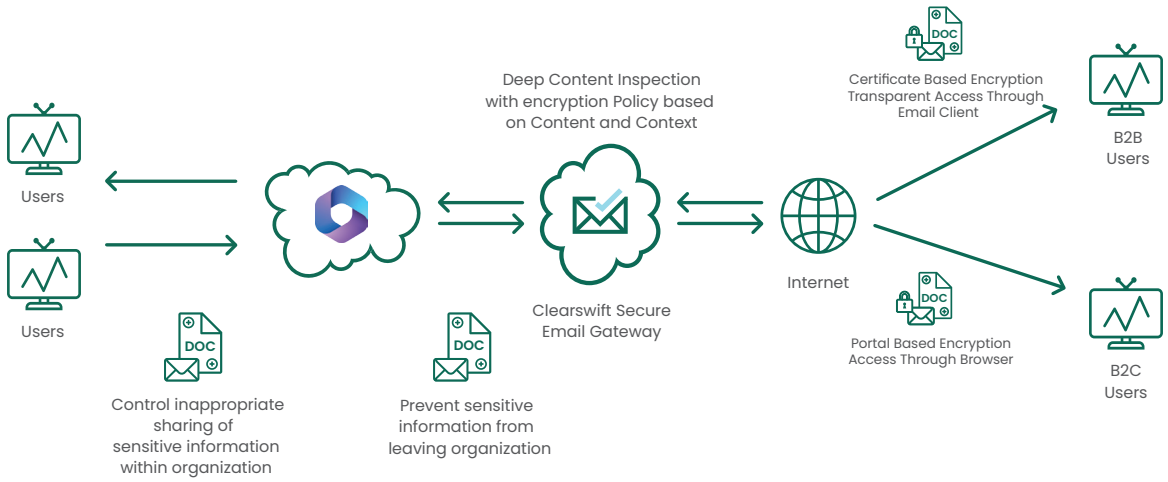
Device Control

Encryption, while it can be applied to authorised devices, can also be used on any USB stick and the information encrypted according to organisation policy and standards. Furthermore, DCI can be used, a process known as "data-in-use", to inspect the file before it is copied and policy based actions applied, for example requiring an auditable comment to explain the need for the transfer can be recorded. There is still an option to block the copying of the content onto the device – it is all based on policy.



Data in Use

Removable device encryption applies to more than just USB sticks, it can be used with any form of removable media. The process is virtually transparent to users, protecting the information while leaving it inaccessible to people should the device be lost. Strong encryption, AES 256, can be used to assure the protection of the information.



User Experience

Clearswift's encryption solutions are designed to ensure the best user experience. While PGP and S/MIME encryption can be transparent to both sender and recipient, in the case of Ad Hoc and portal-based encryption there is a simple additional step which needs to be followed. For the portal, the recipient automatically receives a message with instructions on how to login and retrieve their message. Using any Internet browser, they connect to the portal and can set their own password for current and future use.

Encryption and GDPR

When the EU General Data Protection Regulation (GDPR) came into force in 2018, there was a great deal made of encryption as being the route to compliance. This is partially true, it is a key part of becoming compliant, but it is not the only technology. Encrypting the information and sending it to an unauthorised person, along with the password is still a data breach, so ensuring that the appropriate processes are in place is critical. Furthermore, deploying encryption solutions means that the organisation remains in control of the information, leaving an individual in control of encryption opens up a series of risks should access to the information be required – but no one knows the password.

Summary

Encryption solves many business problems around secure email communication. There is no silver bullet, so understanding the benefits of each is important when choosing the right solution. Successful deployment depends on a seamless integration into the environment and frictionless use for the sender as well as the recipient. For those organisations with large files to be shared an MFT solution can be deployed, which through Deep Content Inspection and policy-driven Adaptive Data Loss Prevention, ensures that only authorised information is shared with the appropriate people.

For more details, please contact info@clearswift.com.

Solution	Features	Benefits	Target Audience*
TLS	Server-to-Server email encryption	• Secure email transfer from organisation to organisation • Transparent use for all users	Gov2Gov
PGP / S/MIME	User to User email encryption	• Transparent use	Gov2Gov / Gov2Org
On-Premise Portal	Secure email between government and citizens	• Transparent use after initial registration • Full control over portal and infrastructure	Gov2Cit
Cloud-Based Portal	Secure email between government and citizens	• Transparent use after initial registration • Managed service	Gov2Cit
MFT (Outbound)	Secure large file transfer for collaboration projects	• Secure transfer of large files • Ability to apply content inspection to ensure no unauthorised information is shared • Content modification to tailor information to recipient based on policy	Gov2Gov / Gov2Org
MFT (Inbound)	Simple mechanism for citizens to upload files to government departments	• Full security around file upload. • Content inspection ensure no malware is uploaded.	Cit2Gov
Removable media encryption	Automatically encrypt files on USB and other removable media	• Even if the USB stick is lost, the information is secured.	Gov2Gov

Target audience: Cit: Citizen | Gov: Government / Public Sector | Org: Organisation

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

