#becrypt

se-mail provides a secure email and messaging platform that has a familiar webmail user expererience. Not only does it give peace of mind for across organisation adoption but it's intuitive webmail user interface minimises user training and support. requirements.

HM Government

Built with UK Government

Designed for government and critical national infrastructure organisations, **se-mail** development was government funded, and developed in close collaboration with UK Government Security Architects following High Assurance principles.

For more information contact:

info@becrypt.com

se-mail

se-mail is a secure email and messaging platform that allows the controlled exchange of information for communities of collaborating Partners that need to work across different levels of trust and information sensitivity, including government classified systems.

By using se-mail with compatible High Assurance Cross Domain technology, such as Becrypt's APP-XD Gateway, organisations can securely interface their 'High-Side' email server (e.g. Exchange) to Partner-accessible devices. Trusted Partners interact using a dedicated se-mail client application that may be secured using the Paradox End User Device platform.

se-mail offers a familiar webmail user experience, but ensures:

- Encrypted messages are only accessible by authorised recipients, with user identity and authentication enforcement using Yubikey two factor authentication
- All messages are end to end encrypted between the "High Side" email servers (e.g. Exchange) and "Low Side" users, providing cryptographically assured confidentiality even in the event of a Service or supporting Partner infrastructure breach
- Cross Domain Gateway compatibility to support secure document import and export for email attachments
- All messages sent to Partner or "Low-Side" users are preserved within the system for a duration defined by policy
- Partner messages cannot be forwarded to an external system from the "Low Side"
- Policy controls ensure that Partners or "Low Side" users can only send messages to an allowed recipient list
- No data stored on Partner client devices
- Monitoring and audit of security related events including file import and export

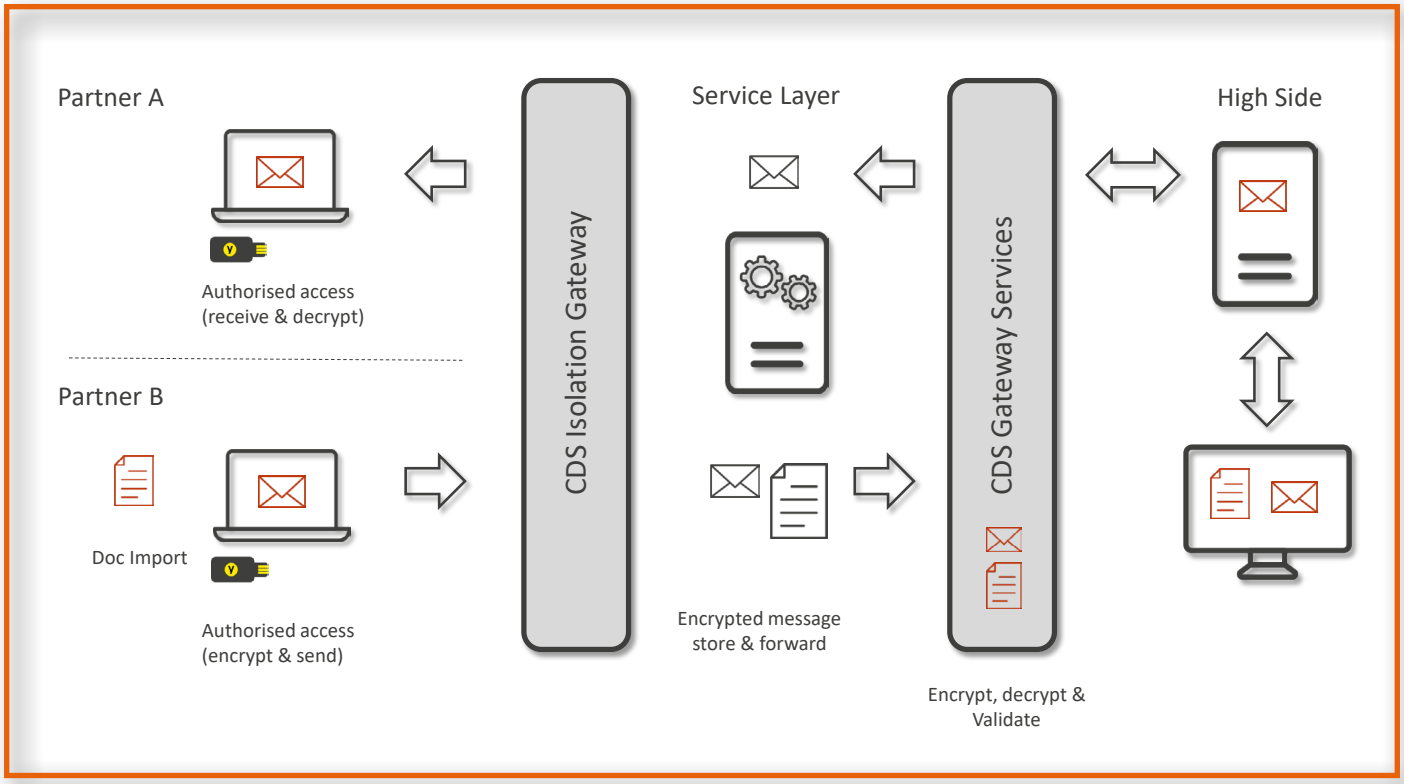
As **se-mail** implements end to end message encryption, it may easily be consumed as a service, without exposing message content to service providers.

- Share emails and attachments with collaborating organisations from your most sensitive environments without having to trust theirs.
- Deploy an easy to use import and export system for a High Side environment, with access control and audit.
- Consume secure email as a Service without exposing sensitive data to Service Providers.
- Developed with UK Government se-mail provides a level of assurance appropriate for classified government systems. Contact Becrypt for further information on encryption and message validation standards applied.

se-mail provides an intuitive webmail user interface to simplify set-up, and minimise user training and support requirements.

- Paradox client device health measurements and authentication prevents client access in event of tamper
- No clear-text data within Service layer
- Configurable user account mapping protects High Side user identity and address
- Hardware-based CDS validation of structured data types removes low-side data attack vectors
- Containerised Service infrastructure supports ease of deployment and scale for on premise installations
- Configurable High Side Integration components support a range of High Side Service Integration options

As se-mail implements end to end message encryption, it may easily be consumed as a service, without exposing message content to service providers.



An APP-XD application