

## Secure Digital Mailroom

Organisations are increasingly embracing e-communications across a range of channels, including the digitisation of incoming traditional mail. By digitising the incoming mail process and indexing the documents on the fly, companies can not only gain control of their mail processes internally, but gain the opportunity to combine electronic mail formats (email, fax) in the same document processing flow.

However, the key challenge for many organisations is the ability to access digitised mail in a secure environment, across various applications and devices. This challenge is magnified as organisations move to activity based working environments.



### The benefits

- Reduced decision cycle through faster access to incoming mail
- Increased mail control and visibility
- Reducing paper costs
- Detailed audits and reports
- Flexible secure access across desktop and mobile devices
- Brand in line with your corporate requirements
- Role-based security policies

### Secure mail capture and delivery made easy

Secure Digital Mailroom – powered by Egress®, provides end-to-end data protection without compromising access to critical business mail. All inbound traditional mail can be collected and sent to state based scanning bureaus where it is opened, sorted, scanned and then delivered electronically to the receiver. Digital mail can then be securely viewed and retrieved from any internet-enabled device, enabling receivers to access from any location.

### Sophisticated control over digital mail

Secure Digital Mailroom offers highly flexible granular permissions for individual users, as well as read-only and rights management control, ensuring only the intended recipients can access and edit shared information. This not only simplifies process management, but also means documents and data never leave your control, regardless of collaboration requirements.

Users can be added or removed from a secure workspace at any point throughout the collaborative process. Files can also be shared from within a digital mailbox using a secure link that offers real-time control, including the ability to revoke a user's access. In addition, control over the file types that can be uploaded to a digital mailbox extends the internal management and assurance over the information being shared from within an organisation's network. The customisable user interface and branding options also ensure that every digital mailbox reflects both an individual or departmental data sharing requirement and corporate guidelines.

### Contact:

Justin Cybul  
National Business Development Manager

T: +61 3 9676 1250

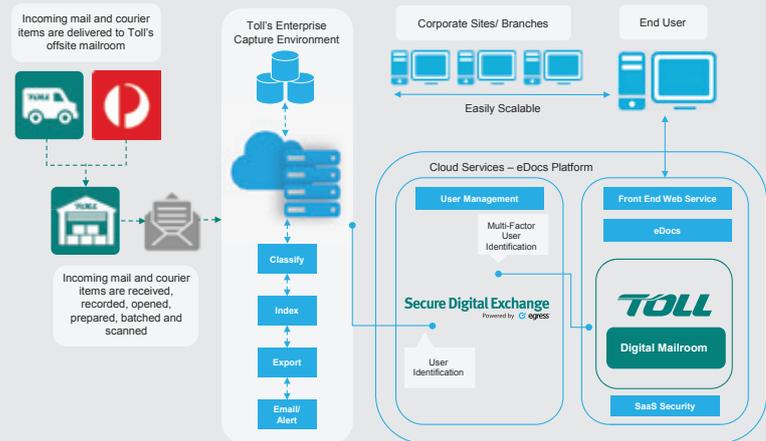
M: +61 413 018 409

E: [SDX@tollgroup.com](mailto:SDX@tollgroup.com)

W: [www.tollgroup.com/secure-digital-exchange](http://www.tollgroup.com/secure-digital-exchange)

## Internal management and control

Each individual secure digital mailbox offers detailed auditing and reporting functionality, including the date and times that users access, download, upload and edit files. This information can be exported to meet compliance and regulatory rules. Role-based security, meanwhile, means system administrators can remain in control of their users and their content at all times. These individual user permissions can be altered throughout the lifecycle of shared digital mailboxes, and extend to online editing functionality to maintain ongoing security.



## Flexible system integration

Secure Digital Mailroom integrates seamlessly with DMS and CMS systems, and email clients such as MS Outlook and Lotus Notes. In addition, the unique email address provided to each secure workspace enables content to be sent to the Secure File Inbox from where it can be manually or automatically processed. In addition, Secure Digital Mailroom supports single-sign-on via Microsoft Active Directory using ADFS (Active Directory Federation Services) for internal users and for external third parties to provide unified identity management and streamlined access to secure collaboration functionality. This flexibility means users and groups can centralise all project files, resulting in more efficient, more organised workflow.

## Security overview

- Secures data at rest and in transit using AES-256 bit encryption
- Utilises FIPS 140-2 certified libraries
- Secure authentication and user enrolment
- ISO 27001:2013 certified
- Skyhigh Cloud Trust™ rating of Enterprise-Ready
- Uses data centres accredited to ISO 27001/27018/9001
- Listed under Cyber Security Supplier to Government Scheme (UK)
- Patent protected (GB 0806429.7 | US12/353,390 | GB 0907665.4)

## About Secure Digital Exchange

Toll is already renowned as a world-class integrated logistics provider and is pleased to be enhancing its offerings in the digital space with its Secure Digital Exchange for email, documents, web forms, digital workspaces and mailrooms – for both internal and external communications in a completely secure environment.

Our new product suite is powered by Egress®, the world leader in encryption platforms, which today enables over 1,000 global organisations and is certified by the UK Government and NATO.

Taking a holistic approach to information security, the solution enables users to securely share and collaborate on sensitive data. Using patented key management, the platform utilises a unique community-based licensing model that consists of paying subscribers and designated recipients, who are able to share information securely with one another using a single global identity.

Toll is delighted to present Secure Digital Exchange – powered by Egress® – to our clients in Australia and New Zealand.

## Egress® Certifications

UK Government

NATO IACD