ECHOWORX™

IT PAYS TO BE SECURE

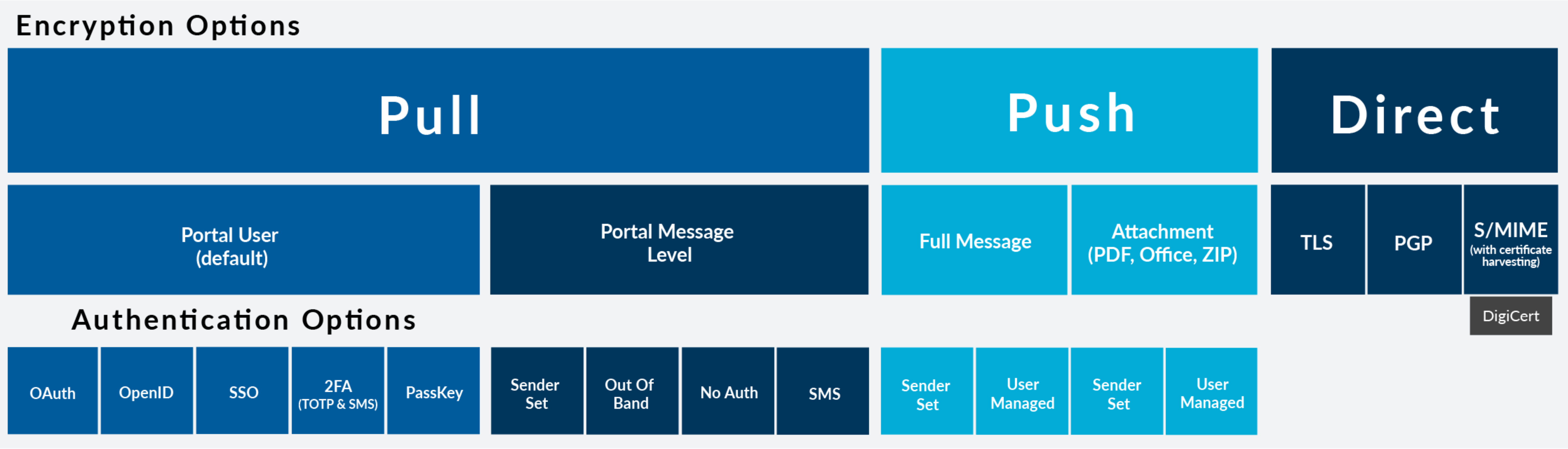
Echoworx Delivery Options

Table of contents

Introduction

In today's digital era, organizations face challenges in their business communication environments. Business leaders prioritize security, data compliance, and preventing unauthorized access to ensure a reliable communication infrastructure. Inconsistencies in multilingual communications, regional language regulations, and device consistency hinder productivity and innovation. Achieving uniform capabilities and a seamless user experience is a top priority.

Echoworx Email Encryption offers secure delivery options to meet diverse business needs. These include TLS Encryption, Encrypted PDF and Attachment, Certificate Encryption, and Web Portal. This versatility allows organizations to choose the most suitable delivery methods on a case-by-case basis, ensuring effective and tailored communication.



Encryption Options

Pull

Portal User (default)

Portal Message Level

Push

Full Message

Attachment (PDF, Office, ZIP)

Direct

TLS

PGP

S/MIME (with certificate harvesting)

DigiCert

Authentication Options

OAuth

OpenID

SSO

2FA (TOTP & SMS)

PassKey

Sender Set

Out Of Band

No Auth

SMS

Sender Set

User Managed

Sender Set

User Managed

Web Portal Encryption

Encrypted messages can be delivered securely via a protected website, like a customer portal. Recipients are notified of a waiting message on the Web Portal. Key features include:

1. Recipients receive a single registration message to sign up and set their password.
2. It supports 28 languages.
3. Optional out-of-band confirmation is available during registration.
4. Full OAuth access support is provided for Office 365, Gmail, Hotmail, Facebook, LinkedIn, Salesforce, and more.
5. OpenID Connect support allows customers to log into the portal with their existing credentials if your business uses OpenID for authentication. Web services integration support also enables auto-login through your existing business portal.
6. Recipients receive a URL that directly opens the message without registration under the No-Authentication option.
7. Recipients enter a password set by the sender at the time of sending, either through the plugin or subject line trigger, in the Sender Sets Password option.
8. The system generates a unique password for each message and emails it to the sender for Out-of-Band Password. Recipients must obtain this password from the sender through a separate channel to access the message.
9. Passwordless Access with Passkeys utilizes fingerprint scanners and biometrics for secure message validation. Users can enjoy the convenience of passkeys for login, authenticating with PINs or biometric autofill. Customers with a vanity domain can streamline the login process by enabling passkey auto-fill.

Additional Features

- Provides flexible delivery options, accessible on any device.
- Offers extensive branding features for customer-facing webpages, encrypted messages, and message notifications.
- Ensures message encryption at-rest for enhanced security.
- Allows users to save messages locally in various formats, including Outlook and Encrypted PDF.
- Enables senders or recipients to set secure passwords.
- Includes secure reply functionality and read receipts.
- Provides full message audit and recall capabilities for both senders and administrators.
- Offers a standard retention period of 30, 60, or 90 days, with flexibility for longer periods upon request.

Limitations

- Requires recipients to access messages online instead of their local mailbox.

Encrypted PDF

Outgoing emails can be secured by encrypting both the body and attachments using standard Secure PDF, Office 365, and ZIP technologies. The key features include:

1. Self-Registration: Recipients have the ability to set their own password with a one-time prompt.
2. Password Management: Each message includes a self-service password management link, enabling recipients to recover existing PDF passwords, set new ones, or update their security information.
3. Sender-Set Password: Senders can set a shared passphrase (with a hint) at the time of sending, either using an optional plug-in or a subject line keyword. This passphrase can be provided to recipients out-of-band, allowing them to open the message without the need to register.

Additional Features

- Delivery flexibility to any device, anywhere.
- Extensive branding options for customer-facing webpages, encrypted messages, and notifications.
- Support for 28 languages.
- Direct delivery of encrypted PDFs to inboxes.
- At-rest encryption for secure messages.
- Offline message access.
- Options for sender or recipient-set passwords.
- Secure reply functionality, with the option for recipients to have a secure copy.
- Access via any standard PDF viewer on any device.

Limitations

- Please note that once the messages are delivered, message auditing or recall is not available, unlike Web Portal Encryption.

Encrypted Attachment

Sensitive documents can be securely transmitted by sending them as encrypted attachments via regular email. This option proves valuable when dealing with tasks such as generating and processing bulk electronic statements.
The key features include:

1. Encrypted PDF attachments preserve native file integrity.
2. It supports Office Document encryption.
3. ZIP file encryption is supported.
4. Option to bundle files into Encrypted PDF or ZIP formats.
5. Self-Registration feature available (similar to Encrypted PDF).
6. Senders can set passwords (similar to Encrypted PDF).
7. Branded headers and/or footers can be added to the message body, including a password management link or a hint for a shared secret passphrase.

Additional Features

- Read secure messages anywhere, on any device.
- Message body remains clear-text, only attachments are encrypted.
- Supports multiple encrypted attachments in their original formats.
- Offers extensive branding options for customer-facing webpages, encrypted messages, and notifications.
- Multilingual support available in 28 languages.
- Directly delivers encrypted PDFs and Office documents to recipient's inbox.
- Encrypted attachments remain secure at rest.
- Provides flexible password options for senders or recipients and supports offline message access.

Limitations

- Recipients must have ZIP software capable of opening AES 256-bit files (e.g., WinZip, Secure ZIP, WinRAR, 7-ZIP) for Secure ZIP.
- Limited options for message audit and tracking.
- Delivered messages cannot be audited or recalled like Web Portal Encryption.

TLS Encryption with Fallback

The platform seamlessly encrypts messages and attachments during transport, ensuring secure delivery to recipients without any additional setup or password requirements. The key features include:

1. The validity of TLS connections is verified on-the-fly.
2. An 'Allow List' can be easily configured to only send messages to TLS domains.
3. A 'Block List' can be created to exclude certain TLS domains using the web-based administration console.

Additional Features

- Senders can simply send messages while the encryption platform handles the rest.
- Recipients don't need to change their behavior as transparent delivery is ensured.
- In cases where TLS is unavailable, Echoworx automatically provides secure fallback options like the Web Portal or Secure PDF to prevent undeliverable or unprotected messages.
- Extensive message branding options for headers and footers are available.
- Support for 28 languages.
- Perfect for B2B environments where both parties utilize TLS.

Limitations

- Please note that secure messages are not encrypted at-rest after they are received.
- TLS must be available to enable secure replies.

Certificate Encryption

It is highly advantageous when recipients already possess a third-party S/MIME or PGP. The key features of this encryption method include:

1. Establishing Certificate Encryption on a user-uploaded public certificate.
2. Utilizing external lookup in LDAP to obtain the public recipient certificate.
3. Enabling complete creation and management of PGP keys for senders to communicate with external PGP users. External users receive a PGP encrypted email that is digitally signed, with a public key attached for the sender's convenience.
4. Providing seamless support for PGP migration to the cloud, allowing the consolidation of all PGP activities within a secure communication platform.

Additional Features

- The system automatically extracts public keys from incoming signed and encrypted S/MIME messages, eliminating the need for manual certificate uploads by administrators or recipients. This enables customers to encrypt outbound S/MIME messages effortlessly.
- Existing keys can be seamlessly uploaded to the Echoworx Email Encryption platform.
- New keys can be generated on-demand to ensure the maintenance of current and future identities.
- Recipients experience a user-friendly process without the need to change their behavior or take any additional steps.
- Secure delivery is available to any email address worldwide, assuming the key exists.

Limitations

- In order to detect encrypted reply messages, one needs to configure the inbound email flow.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx Email Encryption provides a variety of secure delivery options to customize communication on a case-by-case basis. With a strong emphasis on security, accessibility, and delivering a seamless user experience, organizations can enhance their overall secure communication capabilities while ensuring effective and tailored communication.

Learn more:

Echoworx Email Encryption - Technical Validation

Get Instant Insights: Watch Our On-Demand Demonstrations

Discover Customer Success Stories

For more information, www.echoworx.com