ECHOWORX™

IT PAYS TO BE SECURE

Echoworx Delivery Options

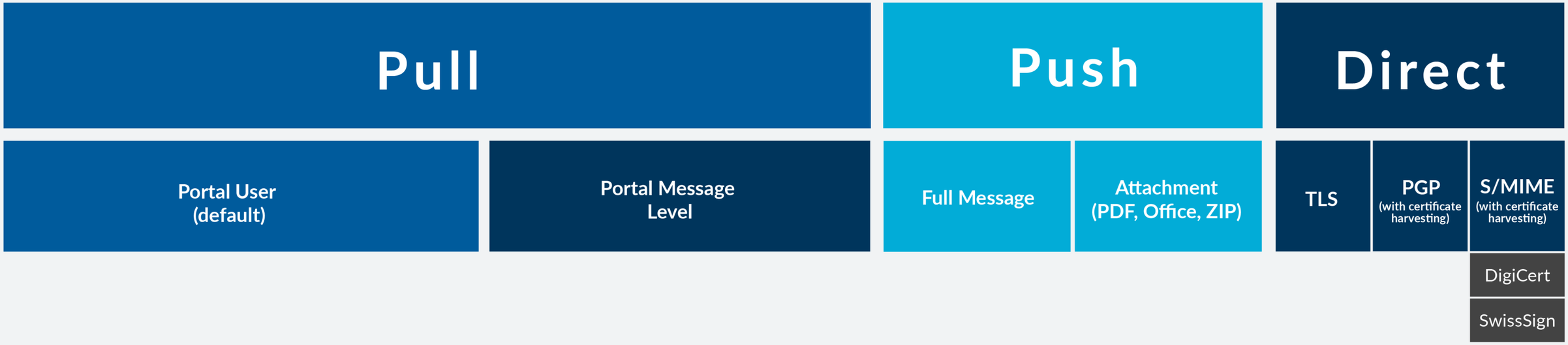
Introduction

In a world where digital communication defines business success, security professionals face a critical question: is your email encryption strategy truly up to par? For leaders tasked with safeguarding sensitive data, basic solutions are no longer enough. The demand for seamless, secure, and adaptive communication has never been higher.

Echoworx Email Encryption rises to this challenge, offering tailored delivery options like TLS Encryption, Encrypted PDFs, Certificate Encryption, and Web Portals. It's not about checking a box—it's about redefining how secure communication drives productivity, compliance, and trust.

Are you ready to go beyond the basics?

Encryption Options



Authentication Options

Table of Contents

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

1. Recipients receive a single registration message to sign up and set their password.
2. Optional out-of-band verification code is available during registration.
3. Full OAuth access support is provided for Microsoft 365, Gmail, Hotmail, Facebook, LinkedIn, Salesforce, and more.
4. OpenID Connect allows recipients to log into the portal with their existing credentials if your business supports OpenID for authentication.
5. SSO Web services integration allows auto-login through your existing business portal.
6. No-Authentication mode allows recipients to access messages via a direct link, bypassing the need to log in. This feature is particularly useful when the focus is on tracking message activity or facilitating secure inbound replies.
7. Sender-Set Password allows senders to create a shared passphrase (with an optional hint) using the M365 Outlook Add-On. Recipients can receive the passphrase through an alternate channel, enabling them to access the message without needing to register.
8. SMS Verification Codes enable senders to input the recipient's phone number via the M365 Outlook Add-On. A verification code is then sent directly to the recipient's mobile device, ensuring quick and secure authentication for portal access.
9. Passwordless Access with Passkeys leverages fingerprint scanners and biometric authentication for a seamless login experience. Users can conveniently use passkeys a their PIN or biometric autofill for secure access.

Additional Features

- Provides flexible delivery options, accessible on any device.
- Offers extensive branding features for customer-facing webpages, encrypted messages, and message notifications.
- Support for 28 languages.
- Messages are stored encrypted at-rest in the Echoworx cloud.
- 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 to 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.

Tech Notes

- Recipients are accessing messages online and should save them to their local device for permanent retention.

Encrypted PDF

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

Key Features

1. Self-Registration mode allows recipients to set their own password via a one-time prompt.
2. Password Management mode provides recipients with a self-service link within each message, enabling them to recover existing PDF passwords, set new ones, or update their security details.
3. Sender-Set Password mode lets senders create a shared passphrase (with an optional hint) at the time of sending via the Gmail or M365 Outlook Add-On. This passphrase can be shared out-of-band, enabling recipients to access the message without needing to register.
4. Encrypted PDF and Office document viewing is supported directly within the Outlook for Web and Gmail client.

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 to functionality, with the option for recipients to have a secure copy.
- Access via any standard PDF viewer on any device.

Tech Notes

- Push Encryption methods deliver the email immediately to the recipient and therefore cannot be recalled by Echoworx.

Encrypted Attachment

Send sensitive documents securely with encrypted email attachments—ideal for tasks like processing bulk electronic statements.

Key Features

1. PDF, Microsoft Office, and ZIP attachments are encrypted natively.
2. Native encryption preserves original file name and file properties.
3. Encrypted PDFs and Office documents can be viewed directly within Outlook for Web and Gmail client.
4. Other attachment types can be bundled into Encrypted PDF or ZIP format.
5. Self-Registration for recipient managed password.
6. Sender can set shared secret passphrase.
7. Customized, branded message body headers and footers, including options to add a password management link or a subtle hint for a shared secret passphrase.

Additional Features

- Read secure documents anywhere, on any device.
- Message body remains clear-text, only attachments are encrypted.
- Supports multiple encrypted attachments in their original formats.
- Multilingual support available in 28 languages.
- Directly delivery to recipient's inbox.
- Encrypted attachments remain secure at rest.
- Provides flexible password options for senders or recipients.
- Offline secure document access.

Tech Notes

- Echoworx recommends the following ZIP software for recipients that is capable of opening AES 256-bit files: WinZip, Secure ZIP, WinRAR, and (our favourite) 7-zip.
- Push Encryption methods deliver the email immediately to the recipient and therefore cannot be recalled by Echoworx.

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.

Key Features

1. The validity of TLS connections is verified on-the-fly.
2. An ‘Allow List’ can be configured to only send messages to TLS domains.
3. A ‘Block List’ can be created to exclude certain TLS domains.
4. If a domain is not eligible for TLS delivery, Echoworx seamlessly switches to alternative secure delivery methods, such as the Web Portal or Secure PDF, ensuring uninterrupted protection.

Additional Features

- Senders can simply send messages while the encryption platform determines when to use TLS or another method.
- Recipients don’t need to change their behavior as transparent delivery is ensured.
- Extensive message branding options for headers and footers are available.
- Perfect for B2B environments where both parties utilize TLS.

Tech Notes

- Once a message is delivered via TLS, it is not encrypted at-rest in the recipient mailbox.
- Secure replies are sent outside the Echoworx platform and rely on the recipient using TLS for transmission.

Certificate Encryption

It is highly advantageous when recipients already possess a third-party S/MIME or PGP.

Key Features

1. Recipient certificates can be accessed through external lookup in various LDAP directories.
2. Recipients have the option to upload their x509 certificate or PGP public key directly via the web portal.
3. Recipients can generate a self-signed S/MIME certificate through the web portal.
4. Outbound messages are digitally signed using a key linked to the sender's email address, either uploaded or generated. If unavailable, an enterprise- level (e.g., domain-wide) key serves as a fallback.
5. Echoworx offers seamless integration with DigiCert & SwissSign, enabling on-the-fly retrieval and generation of trusted S/MIME credentials for employees whenever a key is needed.
6. Echoworx can automatically create PGP public/private key pairs for senders in real time when required. The recipient of the PGP-encrypted email will also receive the sender's public key as an attachment.
7. Inbound S/MIME and PGP-encrypted messages can be decrypted using private keys securely stored within the Echoworx platform.

Additional Features

- Customers can import all their employees' certificates and keypairs for a smooth migration.
- Auto-generate new keys as needed, in a fully automated manner.
- No need for recipients to change behavior.
- Branded footers and headers on inbound decrypted messages.
- Secure delivery can be made to any email address in the world (assuming recipient key is retrievable).
- Full support for PGP and S/MIME migration to the cloud, consolidating all certificate-based email activity under one secure communication platform.

Tech Notes

- To decrypt messages and extract certificates from incoming communications, you need to configure additional rules in your gateway to route these messages to Echoworx.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx Email Encryption delivers more than just secure messages—it redefines how organizations approach email security. With flexible, tailor-made delivery options, it empowers you to protect sensitive communications without compromising efficiency or user experience. This isn't a one-size-fits-all solution—it's a powerful tool designed to meet the unique demands of your business. In an era where basic encryption is no longer enough, it's time to rethink your approach.