SECURE EMAIL OVERVIEW

A BETTER APPROACH FOR SHARING SENSITIVE DATA

Secure email gateways create nearly as many problems as they solve. The multi-step process required to open a protected email, together with forgotten passwords, password resets, and account lockouts, create frustration for senders and recipients. These issues can obstruct the flow of information and damage important business relationships.

SECURE EMAIL WITHOUT FRUSTRATION

PKWARE Secure Email is a simpler, better approach for organizations that need to share sensitive information with external recipients. Banks, healthcare organizations, and other companies use PKWARE to protect critical information while facilitating access by customers, partners, and other external parties.

Rather than relying on the gateway model—which requires the recipient to click away from their email application and log in to a third-party website in order to retrieve a message—PKWARE's technology provides simple functionality that eliminates confusion and frustration.

EASY FOR SENDERS & RECIPIENTS

PKWARE allows senders and recipients to use their existing email applications, and allows organizations to grant and revoke access to protected information at any time.

Message senders use PKWARE's Outlook add-in to encrypt emails containing sensitive data. Senders can encrypt the message body and any attachments, using keys that only the intended recipient can use. Administrators can also create rules to automatically encrypt outgoing messages based on message contents, user permissions, and other criteria.

To open a secure email, the authorized recipient simply downloads the message file and uses the free Smartcrypt Reader to decrypt and open it. Secure emails cannot be accessed by anyone but the intended recipient, even if they are accidentally sent or forwarded to other parties.

SOLUTION HIGHLIGHTS

- Organizations can securely email clients, partners, and other external recipients without the frustrations of an email gateway.

- Outgoing messages are encrypted via an easy-to-use Outlook add-in.

- Sensitive information is protected with strong AES-256 encryption, facilitating compliance with government and industry mandates.

- Message recipients use the free Smartcrypt Reader to decrypt and open attachments.

- Simple drag-and-drop functionality eliminates customer frustration over complicated workflows, forgotten passwords, and other common gateway challenges.

- Encrypted information can only be accessed by the intended recipient.

- Smartcrypt Reader can be white-labeled and branded with the sending organization's logo.

- PKWARE's security management console streamlines policy definition and administration.

INNOVATIVE TECHNOLOGY FROM PKWARE

No other email solution delivers the security, simplicity, and flexibility that PKWARE provides.

SMARTKEYS

PKWARE's Smartkey technology allows organizations to share encrypted information without the challenges associated with public-key infrastructure, password sharing, secure email gateways, or other common approaches.

Smartkeys are tied to recipient identities—typically email addresses—and allow sending organizations to grant and revoke access to encrypted data at any time, even after an email has been sent.

OUTLOOK ADD-IN

PKWARE's add-in for Microsoft Outlook allows senders to create and select the appropriate Smartkey for each outgoing message. Sender options and permissions are defined using PKWARE's web-based administrator console.

SMARTCRYPT READER

The Smartcrypt Reader is a zero-install application that recipients use to open secure emails and attachments.

The Reader involves a one-time setup process, in which the user enters an address and creates a password. The application then automatically downloads any Smartkeys to which the user has been granted access.

To open a secure email, the recipient downloads the message and drags the encrypted file onto the Smartcrypt Reader icon. As long as the recipient has been granted access to the proper encryption key, the message will open with no further action by the user.

The Smartcrypt Reader is available for free from PKWARE, and can be white-labeled and rebranded with the sending organization's logo, creating an integrated experience that strengthens customer and business relationships.

TECHNICAL SPECIFICATIONS

MANAGEMENT CONSOLE:
- Hardware appliance
- Virtual appliance
- Software-based (Windows Server)

OUTLOOK ADD-IN:

Operating Platforms
- Windows (supported versions)
- Microsoft Office 2007 or later
- AES-256 encryption
- Options to encrypt message body, message attachments or body attachments

SMARTCRYPT READER:
- Zero-install application
- Windows (supported versions)
- 256 MG RAM or higher