PKWARE | SMARTCRYPT

SMARTCRYPT

TECHNICAL BRIEF: OUTLOOK INTEGRATION

PKWARE's Smartcrypt provides persistent data-level encryption for email messages and attachments, using an Outlook plugin that incorporates encryption and decryption without disrupting typical user workflows.

With Smartcrypt, documents, spreadsheets, and other sensitive files remain safe from unauthorized access, even when saved to a message recipient's computer or shared in the cloud.

OUTLOOK PLUGIN

The Smartcrypt plugin for Outlook enables users to encrypt and decrypt messages and attachments without the need to open a second application. The plugin applies users' default encryption settings, and can be configured to allow users to modify those settings for individual messages.

When encrypting an email, the plugin converts the message, along with any attachments, into a single MIME-format .eml file and then encrypts and zips the file. The name of the .eml file, like the name of the containing ZIP file, is based on the subject of the message plus a timestamp.

When a Smartcrypt user receives an encrypted message, Smartcrypt will either decrypt the message automatically upon opening or prompt for decryption, depending on the organization's security policies. When automatic decryption is enabled, the user experience of opening an encrypted email is identical to opening an unencrypted email.

Message recipients who do not use Smartcrypt can decrypt email messages using the free Smartcrypt Reader.

If an encrypted email is sent or forwarded to users who are not authorized to access the data, the message and attachments remain inaccessible, no matter how many times the message is forwarded or saved.

TECHNICAL SPECIFICATIONS

SYSTEM REQUIREMENTS

- Windows 7 or above
- 128 MB RAM (512 MB recommended)
- For 32-bit versions: 45 MB of free HD space
- For 64-bit versions: 50 MB of free HD space
- Office/Outlook 2002 or later

ENCRYPTION KEY TYPES

- Smartkeys
- OpenPGP certificates
- X.509 certificates
- Passphrases

ENCRYPTION ALGORITHMS

- AES-256, AES-192, AES-128
- AE-2
- 3DES

User creates email containing sensitive data

Smartcrypt agent scans text & attachments and encrypts email

Authorized recipients can open and read the email (using Smartcrypt or the free Smartcrypt reader)

If the message is forwarded to unauthorized recipients, it remains encrypted and inaccessible

OUTGOING EMAIL WORKFLOWS

Smartcrypt supports multiple encryption key types and encryption workflows, enabling organizations to create tailored solutions for secure data exchange via email.

User-directed workflow: Smartcrypt can be configured to open an encryption dialog box before an email is sent. The dialog box allows users to choose from a variety of email encryption options:

- Encryption method: Smartcrypt can encrypt the message body, attachments, or both
- Encryption key: users can select from available Smartkeys or digital certificates, or create a passphrase for each outgoing message
- Encryption algorithm: available options include AES-256, AES-192, AE-2, and 3DES
- Re-encryption: decrypts attachments that were already encrypted, and re-encrypts them to ensure that authorized recipients will be able to access them
- Auto-search for recipients: automatically searches for Smartkeys or certificates for each of a message's recipients

Automated workflow: Rather than allowing users to manage the process, organizations can define policies that determine when and how emails should be encrypted.

Administrators can configure Smartcrypt to encrypt all messages, or only messages that contain sensitive information as defined by the organization. Administrators can also pre-select the encryption keys to be used in each encryption operation. Policies can be applied to specific users or groups, or to the entire organization.

INCOMING EMAIL WORKFLOWS

An encrypted message is stored encrypted in Outlook and must be decrypted each time it is read. However, when encrypted messages are sent to users who have the Smartcrypt plugin for Outlook installed on their computers, the decryption process is transparent to message recipients.

Smartcrypt provides two user-friendly options for external users who need to open emails that have been encrypted by a Smartcrypt user: guest accounts and the free Smartcrypt Reader.

Guest accounts: A guest account allows a user to encrypt and decrypt email (and access authorized Smartkeys) using the Smartcrypt Outlook plugin just like an organization's internal users. To create a guest account, an organization simply adds the external user in Active Directory, grants access to the appropriate Smartkeys using the Smartcrypt Enterprise Manager, and provides a Smartcrypt license for use on the external user's laptop, desktop, or mobile device.

Smartcrypt Reader: The Smartcrypt Reader is a free, no-install app that allows anyone to decrypt files, provided that they have been granted access to the appropriate Smartkey or other encryption key. To access an encrypted email, the external recipient simply downloads the Smartcrypt Reader and registers using the app interface.

After verifying their credentials, the user can decrypt and extract the .eml file that contains the message and encrypted attachments. The .eml file can then be opened manually (for example, by double-clicking it in Windows Explorer) in an email program such as Outlook. Opening the .eml file decrypts and displays the original message, and makes any attachments accessible.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249