PKWARE

NEXT GENERATION **ENCRYPTION** AND **KEY MANAGEMENT**

PERSISTENT DATA SECURITY THAT ENHANCES DLP PROCESSES AND TECHNOLOGY

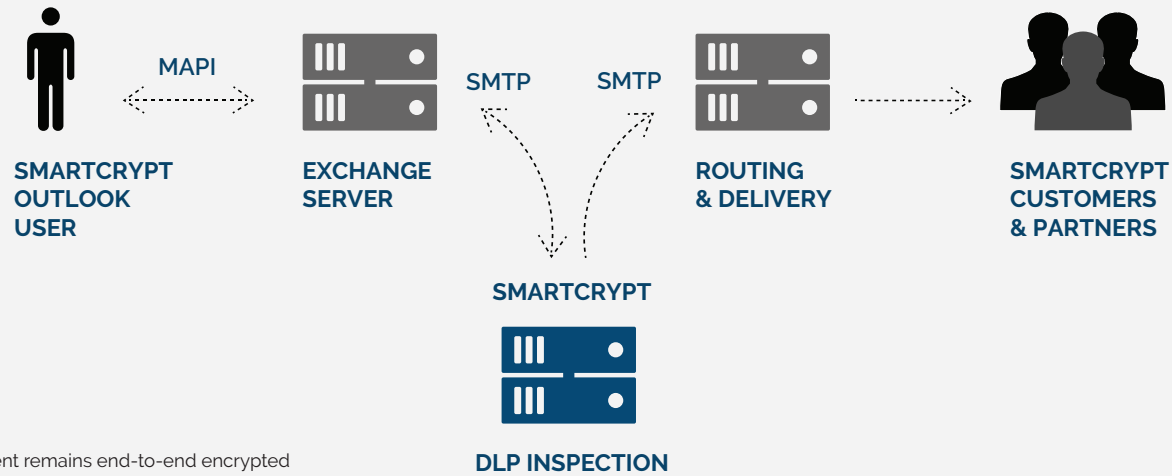
Data loss prevention (DLP) processes and technology prevent unauthorized data exfiltration and are a critical component of data breach detection strategies. Traditional DLP decision points include allowing and blocking transmissions or redirecting transmission to another party for additional decision making. As more organizations adopt end-to-end encryption solutions, their DLP processes and technology have become less effective. This has resulted in more blocks and redirects, which in turn hinder business velocity. Organizations need flexible data security solutions that work with existing DLP to satisfy audit and compliance requirements. This includes the capability to inspect encrypted content and provide encrypted remediation as an additional decision point.

Policy-based encryption to enhance existing DLP

PKWARE's Smartcrypt platform integrates with DLP for both sensitive information discovery and encrypted remediation.

For discovery, Smartcrypt provides policy key access to DLP personnel, along with the ability to decrypt and scan content that has been encrypted elsewhere in the organization. For network DLP, Smartcrypt can help DLP make informed decisions with regards to encrypted content. For example, a sender can use Smartcrypt to encrypt sensitive data before sending a message. If the sender is permitted to share the type of information contained in the transmission, DLP can pass it along, allowing the security to remain intact. If the sender is not allowed to share the information, DLP can block the transmission after it has scanned the encrypted content.

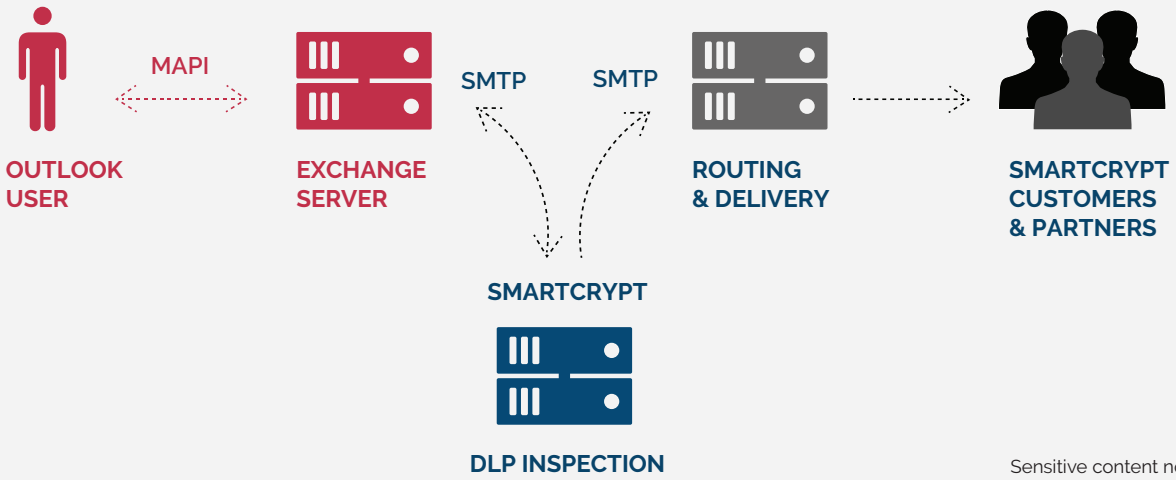
Smartcrypt Outlook Integration auto-encrypts email attachments using recipient key and policy key.
Smartcrypt DLP Integration uses policy key for sensitive information discovery.



Sensitive content remains end-to-end encrypted

For remediation, Smartcrypt allows DLP to secure transmissions it would otherwise have to block. If a sender is authorized to transmit sensitive information but failed to encrypt the data before sending, Smartcrypt can encrypt the message using a public key or a unique Smartkey, rather than re-routing or blocking the transmission.

DLP detects sensitive content is being transmitted. Sender and Recipient are authorized.
Smartcrypt provides DLP remediation.



How it works

PKWARE's Smartcrypt application resides on servers, desktops, and mobile devices and is used to apply persistent file encryption. This protection travels with the files, ensuring they remain encrypted wherever they are transmitted or stored. Strong encryption can be performed with passphrases, PGP keys, X509 digital certificates, or Smartkeys (Smartcrypt's embedded encryption key management system). Regardless of which encryption system is used, administrators can use the manager console to define policy keys to be transparently included in every encryption operation. This ensures that the organization never loses access to encrypted information, and enables administrators to issue and retract policy keys for enterprise IT and audit users as needed. Policy keys can also be issued to third-party DLP and discovery tools, allowing the tools to decrypt any files they need to scan.

Supported key types:

- Smartkeys: Smartcrypt's embedded key management solution. Removes complexity from key generation, synchronization, exchange, and escrow. Smartkeys technology also simplifies formerly challenging tasks such as re-encryption, key rotation, public key creation, and key distribution.
- PGP Public Keys: Any OpenPGP (GPG/PGP) RSA 2048-bit+ public key can be added into endpoint encryption operations.
- X.509 Public Keys: Any X.509 formatted public key including third-party rooted and self-signed keys can be added into endpoint encryption operations.

Summary

PKWARE's Smartcrypt solves problems resulting from uncontrolled encryption, providing the visibility organizations require in order to fully address security, audit, and compliance requirements while providing persistent protection for their data wherever it is used, shared or stored.

Smartcrypt allows organizations to enforce organizational security policies, maintain control of data, and ensure data visibility.

PKWARE®
www.pkware.com

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