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

SMARTCRYPT

SMARTCRYPT USE CASES

PKWARE's Smartcrypt is a revolutionary data security solution that persistently protects critical information, even when it moves outside the organization.

THE SMARTCRYPT APPLICATION
provides data-level encryption with embedded key management, simplified in a way that no one thought possible. All key creation, synchronization, and exchange operations take place in the background, making it easy to securely store and exchange data with partners and customers. Smartcrypt is available for every operating system and storage platform, eliminating gaps in existing security infrastructure.

THE SMARTCRYPT MANAGER
provides identity integration with Microsoft Active Directory and policy management that controls encryption across the enterprise, including existing data leakage prevention processes and technology. Smartcrypt's Data Security Intelligence provides enterprise IT, security, and audit personnel with visibility into which files were encrypted, the users who accessed them, what devices they were on, and where the events took place

Companies use Smartcrypt for:

SECURE DATA EXCHANGE
Secure data exchange takes place between individuals, applications, and servers. Smartcrypt applies encryption at the file level so that the protection travels with the information, preventing unauthorized access no matter where the files are copied or shared. Smartkeys, PKWARE's innovative key management technology, can be used to manage access control at the folder or individual file level, even after a file has left the organization.

Smartcrypt is a data security solution, not a data exchange mechanism itself, so it can be used to add encryption to existing transfer workflows and processes. Smartcrypt delivers complete cross-platform encryption from mainframe to mobile, securing data through transfer mechanisms including email, FTP, private line, file sync and share solutions, and even removable media.

With integrations for common applications like Office and Outlook, Smartcrypt can be used to protect information stored on end-user devices, network shares, and even file sharing services like Box, Dropbox and OneDrive. Smartcrypt is also easily integrated into back-office and batch processing workflows.

ENCRYPTION AT REST
Many regulations mandate the encryption of data at rest. Smartcrypt applies persistent file level encryption, which provides a greater level of security than other approaches, such as full disk encryption or transparent data encryption. Organizations can choose from Smartcrypt's built in key management technology, or third-party X.509 or OpenPGP certificates.

The Smartcrypt application can be used to protect files at rest in a variety of ways:

- **Automatic folder encryption:** Every file placed in a folder is automatically encrypted for users who have access to that folder. Encryption keys are automatically distributed to an authorized user's devices.

- **Microsoft Office:** Office documents can be directly saved to and opened from encrypted files.

- **Microsoft Outlook:** Email attachments are automatically encrypted, using unique encryption keys that are automatically generated and distributed to recipients.

- **Individual file/folder encryption:** Files can be encrypted directly by users or through back office/batch processes.

- **Stream support:** Applications can stream data directly to encrypted files without pre-staging to disk.

DISCOVERY AND DATA LOSS PREVENTION
Organizations need flexible data security solutions that work with existing DLP process and technology to satisfy audit and

compliance requirements, including the capability to inspect encrypted content and provide encrypted remediation as an additional fourth decision point.

Encryption has historically reduced the effectiveness of DLP because it typically requires more blocks and redirects within the DLP system. Smartcrypt actually enhances DLP with discovery and remediation tools that fill the gaps left by previous encryption/DLP integrations.

PKWARE has integrated Smartcrypt with DLP for both sensitive information discovery and encrypted remediation.

To address discovery needs, Smartcrypt provides policy key access to DLP personnel and technology, enabling decryption and scanning of end-to-end encrypted content when it has been encrypted elsewhere in the organization.

Smartcrypt can also help network DLP make informed decisions regarding encrypted content. For example, depending on sender permissions, DLP can pass the encrypted content along, allowing the security to remain intact, or block the transmission after it has scanned the encrypted content.

For remediation, Smartcrypt allows DLP to apply protection to transmissions it would otherwise need to block. If a sender is authorized to transmit sensitive information but failed to encrypt it beforehand, rather than re-routing or blocking, Smartcrypt can encrypt the message for the recipient using a public key or a unique Smartkey.

AUDIT AND CHAIN OF CUSTODY

Increasing regulations and customer demands require enterprise computing systems and processes to eliminate exposure. While every organization's obligations are different, any forensic investigation needs to have a complete chain of custody. Multiple agents working in multiple locations constantly have sensitive information at their fingertips, and every time data moves, there is the potential for a security gap.

The Smartcrypt Manager provides an immutable audit log of every encryption, decryption (including failed decryption), and key exchange operation throughout the enterprise.

Digital signing and authentication can further enhance your organization's chain of custody and provide non-repudiation.

SEPARATION OF DUTIES

Separation of duties requirements within each company are unique. Even if following the principles of least privilege, there are still security gaps between the different IT administrative groups where administrators have the potential to access sensitive information.

Smartcrypt's data-centric approach and key management capabilities can be applied to protect data in such a way that IT personnel can still perform their duties without actually having access to the sensitive information itself. For example, encryption keys can be stored separately on hardware security modules accessible via PKCS#11 or KMIP.

Further, integration with third party PKI systems allows organizations to adopt split-key access to sensitive information, ensuring that no single individual is able to access sensitive information.

MOBILE AND BYOD

Data volumes are growing exponentially, and as more organizations move to "bring your own device" (BYOD) policies for employee phones and other mobile devices, a new threat to data security has emerged. Employees often fail to install or update the appropriate security software on their devices, creating ample opportunity for data theft or compromise. Even when security policies are enforced across the general employee population, many companies feel compelled to make exceptions for top executives—the very employees who are most likely to be targeted by data thieves.

The Smartcrypt mobile app can be used for encryption or decryption of files, and supports integrations with popular enterprise file sync and share providers like Box and OneDrive. Smartcrypt also supports native email workflows and is essential for protecting sensitive files on mobile devices. In the event a device is lost or stolen, organizations can immediately revoke access to encryption keys for that device. This renders any sensitive files stored in the app useless to thieves and helps to minimize the otherwise disastrous effects of a data breach.

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