PKWARE
ENCRYPTION WITHOUT COMPROMISE

SMARTCRYPT

SMARTCRYPT USE CASES

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

THE SMARTCRYPT ENTERPRISE MANAGER
is the central hub of a Smartcrypt implementation. The 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 tools provide 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.

SMARTCRYPT AGENTS
are installed on user devices, servers, or other IT assets that store or process sensitive information. Smartcrypt agents can scan file locations for sensitive data and apply persistent encryption with embedded key management, minimizing user disruption. 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.

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 Transparent Data Encryption provides a strong foundation for regulatory compliance and data protection.

For enhanced security, Smartcrypt can apply persistent file level encryption, which protects data at rest, in transit, and in use. Persistent encryption can be applied to data 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.

Organizations can use Smartcrypt's built in key management technology, or third-party X.509 or OpenPGP certificates.

DATA DISCOVERY
PKWARE's Smartcrypt integrates intelligent data discovery with strong data-level encryption, allowing organizations to identify sensitive information and protect it against loss, theft or misuse.

Smartcrypt agents scan desktops, laptops, and servers for sensitive information. Each time a file is added or modified in a protected location, the agent inspects the file contents and applies pattern identification logic to determine whether the file contains sensitive data as defined by administrators using the Smartcrypt Enterprise Manager.

If a file or email message does contain sensitive information, Smartcrypt can encrypt the data using the encryption keys specified in the organization's policies. Encryption and decryption can be configured to take place without the need for intervention by the end user, eliminating disruptions to existing workflows.

Smartcrypt Data Discovery can scan for sensitive data based on mandates such as PCI-DSS or HIPAA, or based on search terms and regular expressions.

DATA LOSS PREVENTION
In addition to providing intelligent data discovery capabilities with integrated encryption, Smartcrypt can be used to enhance the effectiveness of an organization's existing DLP process and technology.

When integrated with existing DLP, 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. After scanning, DLP can pass the encrypted content along, allowing the security to remain intact, or block the transmission after it has scanned the encrypted content.

Smartcrypt also 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
Evolving regulations and customer demands require that organizations maintain complete control over their data in order to demonstrate regulatory compliance and respond to security events.

The Smartcrypt Enterprise 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 the basis for non-repudiation.

SEPARATION OF DUTIES
Separation of duties requirements often leave security gaps between different IT groups, raising the possibility that administrators may be able 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 perform their duties without having access to 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, ensuring that no single individual is able to access sensitive information.

MOBILE AND BYOD
As more organizations move to "bring your own device" policies for employee mobile devices, a new threat to data security has emerged. Organizations often have no control over employee devices, yet must allow employees to use their phones to access sensitive information in order to do their jobs.

The Smartcrypt mobile app supports native email workflows, integrates with popular file share providers, 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 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