

SMARTCRYPT FOR FILES AND FOLDERS

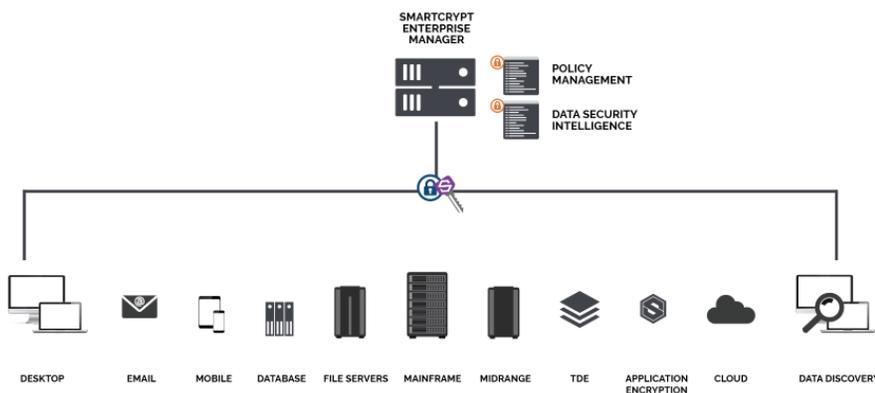
Intelligent Data Discovery and Encryption for User Devices

PKWARE's Smartcrypt is the only enterprise data protection solution that combines intelligent data discovery, persistent encryption, and streamlined key management. With Smartcrypt, organizations can secure sensitive data against internal and external cyber threats, and apply encryption policies across every enterprise operating system.

Smart Encryption for User Devices

The Smartcrypt for Files and Folders agent enables data discovery, encryption, and decryption on desktops, laptops, and mobile devices. The agent is installed on each device that will be used to access or store sensitive information, and applies the organization's discovery and encryption policies as defined by administrators using the web-based Smartcrypt Enterprise Manager console.

Once installed, Smartcrypt is linked to a user profile via integration with the organization's Active Directory. The agent can be configured to encrypt sensitive data automatically, or to allow users to choose which files should be protected. Administrators can grant or revoke user access to encryption keys at any time, and can define policy keys to be included in every encryption operation.



PRODUCT SUMMARY

- » Installed on user devices that are used to access or store sensitive data.
- » Smartcrypt agent can perform automated discovery scans to identify and encrypt sensitive information.
- » Persistent encryption remains with data even when moved, copied, or shared outside the organization's network.
- » PKWARE's industry-best compression technology reduces file sizes before encryption.
- » Administrators apply encryption policies and monitor encryption activity across the organization using the web-based Smartcrypt Enterprise Manager.

Smartkey Technology

At the core of the Smartcrypt platform is PKWARE's revolutionary Smartkey technology. With Smartkeys, businesses gain across-the-board control over who can decrypt files and read data.

A Smartkey is a unique key generated by the Smartcrypt agent for a specific file, folder, or other protected asset. Smartkeys allow administrators to add or revoke user access at any time—even if the files have been shared, copied, renamed, transferred, or emailed—ensuring full lifecycle protection.

Smartkeys are automatically generated, shared, and synchronized between authenticated devices without changing or interrupting user workflows. Smartkeys also allow users to encrypt data for external parties such as vendors or partners.

Intelligent Data Discovery

Smartcrypt provides sophisticated data discovery capabilities, allowing organizations to identify and protect sensitive data as soon as it appears on a user device.

Each time a file is created or modified, Smartcrypt initiates a scan based on the organization's definition of sensitive data. If the data fits one of the defined patterns, Smartcrypt applies strong encryption, keeping sensitive data secure wherever it is used, shared or stored.

Enterprise-Wide Protection

Smartcrypt for Files and Folders is available for Windows, Linux, and Unix operating systems, enabling organizations to protect sensitive data regardless of their IT architecture.

Files encrypted by the Files and Folders agent are fully interoperable with Smartcrypt's solutions for file servers, mainframe, midrange, and databases, ensuring that authorized users can always access encrypted files.

TECHNICAL SPECIFICATIONS

OPERATING PLATFORMS

- » Microsoft Windows
- » Linux: RHEL (.rpm) and SLES (.deb)*
- » Apple Mac OS X and iOS
- » Google Android

ALGORITHMS

- » Encryption:
AES256 (block level encryption in AES-CBC mode)
- » Signing:
RSA 2048 SHA 512 PSS (metadata)

KEY STORAGE AND RETRIEVAL

- » OASIS KMIP
- » PKCS#11

FILE ENCRYPTION CERTIFICATE AND KEY TYPES

- » Smartkeys
- » X.509 Digital Certificates
- » OpenPGP