PKWARE

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

SMARTCRYPT

SMARTCRYPT TRANSPARENT DATA ENCRYPTION

Reliable Encryption for Structured and Unstructured Data

Smartcrypt Transparent Data Encryption (TDE) protects sensitive information at rest on enterprise servers, ensuring compliance with a wide range of regulatory requirements and customer privacy mandates. Smartcrypt TDE secures file and application data without application changes, additional infrastructure, or professional services. No endpoint software is required, and the user experience is unaffected.

Smartcrypt TDE is installed on application, file, and database servers containing sensitive information. Data is encrypted at the block level by a file system driver, between the operating system and the file system. Agents perform automatic encrypt/decrypt operations as data is written/read across the network.

Smartcrypt Manager

- Provides a web-based administration console for the deployment and management of Smartcrypt TDE agents.
- Organizes agents into security groups for the purposes of segregating administrator access to policies, encryption keys, etc.
- Generates encryption keys and assigns them to Smartpoints. Encryption keys can be stored in an encrypted state in the local database or via HSM.
- Allows encryption keys to be managed in the customer's private cloud, even if servers and data reside in other public or private clouds.
- Manages key rotation schedules for online and offline re-encryption of data. Offline key rotation is faster, but requires maintenance windows to take applications offline. Online key rotation is slower, but applications can continue to run.
- Defines system and security administrators. Actions can be configured for single- or multiple-administrator mode requiring approval from other administrators for all actions.
- Submits Manager and Agent events to designated SIEM or Syslog servers.

SMARTCRYPT TDE PROTECTION FOR DATA AT REST

APPLICATION DATA

FULL ACCESS

Performs encrypt / decrypt for authorized applications (oracle.exe, explorer.exe)

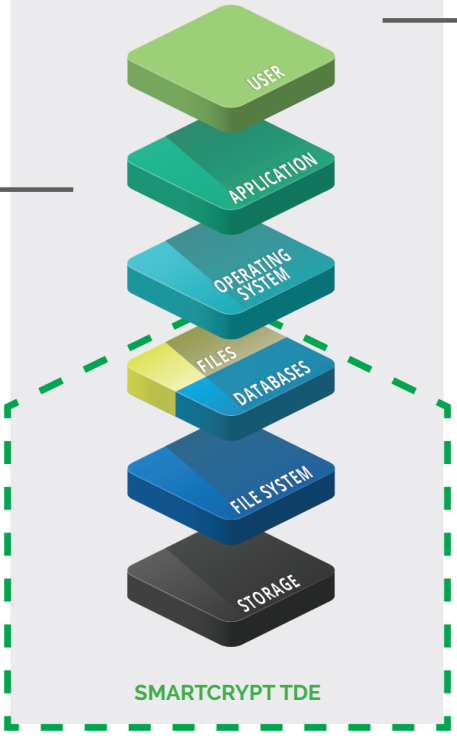
LIMITED ACCESS

Allows copy access of encrypted files by named applications (backup.exe, dropbox.exe)

DENIED ACCESS

Denies access to all unnamed applications (fsociety.exe)

No application changes required



File system driver encrypts data at the block level

FILE SERVER DATA

FULL ACCESS

Performs encryption / decryption for authorized parties (e.g. Auditors, Users)

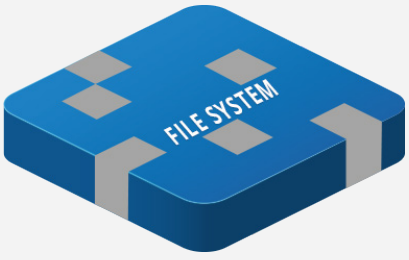
LIMITED ACCESS

Allows copying of encrypted files by named parties (e.g. Backup Operators)

DENIED ACCESS

Denies access to unnamed parties (e.g. Thieves, Snoops)

No software required



Smartpoints

Smartpoints are designated locations on a file system that contain sensitive application data and files. Policy driven TDE agents manage encryption keys and rotation schedules for each Smartpoint. Policies support whitelists and blacklists, which allow only authorized users and applications to access and decrypt/encrypt data. TDE file system drivers manage access to specified directories and perform encryption and decryption during read and write operations.

The Smartcrypt Platform

Smartcrypt Application

Facilitates end-to-end client-side encryption for existing processes and workflows. Available for every enterprise operating platform (Windows, Linux, Solaris, HP-UX, AIX, IBM i, System z, Mac OS, iOS, and Android).

Smartcrypt Manager

Provides policy, control and data security intelligence.

Smartcrypt SDK

Easily adds security to existing applications. Secures sensitive information in files and databases. Available in every major programming language.

Smartcrypt TDE

Ensures compliance with industry- and government-mandated security requirements by adding strong protection for data at rest in files, applications, and databases.

TECHNICAL SPECIFICATIONS

OPERATING PLATFORMS

- Microsoft Windows
- Linux: RHEL (.rpm) and SLES (.deb)*
- UNIX: Oracle Solaris (Sparc and x86)*
- IBM AIX and HP-UX*

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

HIGH PERFORMANCE

- All-software solution that scales at the speed of your application
- Takes advantage of existing hardware accelerators (Intel AES-NI and IBM Crypto Express)

HIGH AVAILABILITY / FAULT TOLERANCE

- Each manager can support up to 2000 agents
- Managers can be configured for failover providing fault tolerance
- Managers can be clustered together across multiple regions for high availability

* December 2016

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

PKWARE is a trusted leader in global business data protection. For three decades PKWARE has focused on data. Building on our compression expertise with the latest encryption technology, PKWARE protects data for over 35,000 customers, including government agencies and global corporations. Our software-defined solutions provide cost-effective and easy-to-implement protection that is transparent to end users and simple for IT to administer and control.