PKWARE

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

SMARTCRYPT

SMARTCRYPT APPLICATION AND MANAGER

Next-Generation Encryption and Key Management

The stakes get higher every day. External security threats grow more sophisticated and unpredictable. Internal controls become more complicated and challenging to implement. When data breaches do occur, the financial and PR damage can take years to repair.

Security managers around the globe are facing the unavoidable truth that network and device protection are not enough. True information security requires persistent data-level protection, so that information remains inaccessible even after a security breach.

Until now, organizations have had to choose between two approaches when implementing data-level protection: passphrases or public-key infrastructure (PKI). Each has significant drawbacks.

Passphrases, the more common approach, are difficult to create, store, and exchange in a way that maintains the security of the protected data. PKI, provides stronger protection, but presents serious challenges in usability and key management. The shift toward mobile technology and cloud-based services has slowed PKI's already low rate of adoption.

PKWARE's Smartcrypt is a revolution in enterprise security management. The Smartcrypt solution combines the strength and reliability of PKI-based encryption with the ease and simplicity of passphrase-based security, allowing companies to maintain complete control over their protected data.

Smartcrypt consists of an end-user application and a web-based manager console. The Smartcrypt platform also includes a software development kit, available in every major programming language.

Smartcrypt Application:

Persistent Protection and Remarkable Ease of Use

Featuring a variety of platform-specific user interfaces, the application supports a wide variety of encryption systems, key types, and key

APPLICATION HIGHLIGHTS

- Available for every enterprise operating system, providing true cross-platform functionality
- Facilitates intelligent data discovery on network assets and end-user devices
- Integrates seamlessly with existing PGP and X.509 public key security infrastructure
- Utilizes hardware encryption accelerators for faster encryption processing
- Combines data discovery and strong encryption with PKWARE's industry-leading compression technology, resulting in significant reductions in storage and transit requirements
- Optional integration to the Smartcrypt Cloud to facilitate secure data exchange with customers and partners

interfaces. Smartcrypt also features Smartkeys, an embedded key management solution that simplifies and automates the most challenging aspects of key management.

Once data is encrypted with the Smartcrypt application, the protection stays with the data everywhere it is used, shared, or stored. The application automatically creates, synchronizes, and exchanges encryption keys, ensuring that only authorized parties can access protected data.

Smartcrypt Manager:

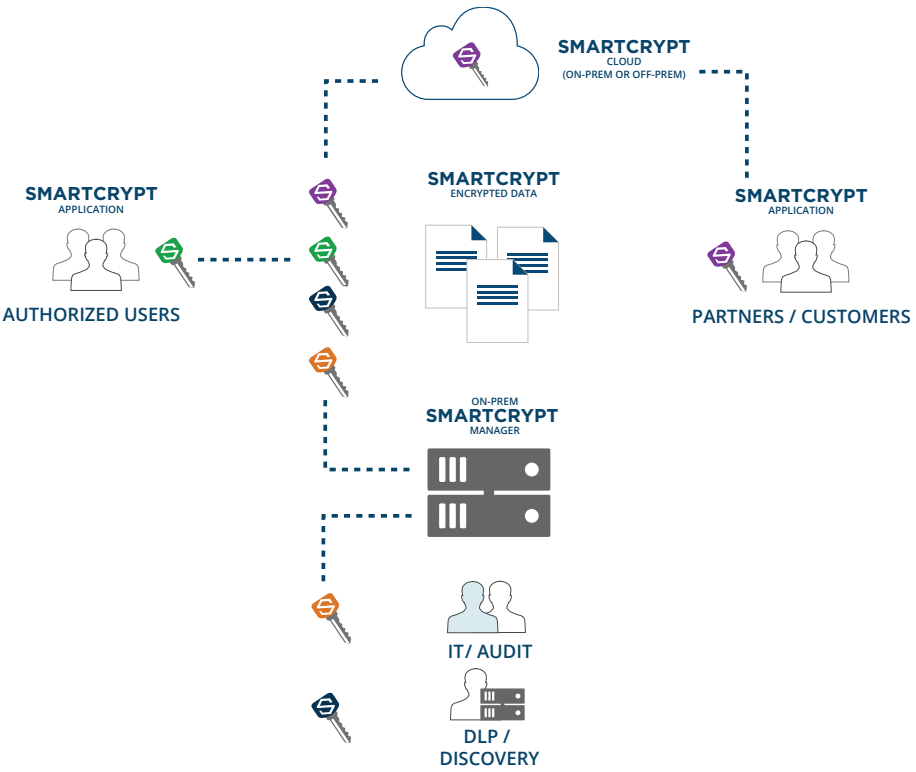
Enterprise Control and Visibility

The Smartcrypt manager console provides centralized key and policy management. The web-based administration console includes granular controls for configuration, policy, and approval management. Smartcrypt's Data Security Intelligence feature provides complete visibility into which files are encrypted, which users have accessed them, and where the events took place.

When auditors, IT personnel, or DLP scanners need to review encrypted data, Smartcrypt's policy keys provide reliable access. The solution can be configured so that every encryption operation contains one or more public keys, ensuring that the organization never loses access to its own data. Customers can elect to use Smartkeys or their own third-party generated keys (in X.509 or PGP format).

Smartkeys

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



MANAGER CONSOLE HIGHLIGHTS

- Integrates with Microsoft Active Directory to provide a seamless user experience
- Administrators can easily grant, revoke, or expire access to encrypted data
- Policy groups allow for retroactive access to content, without the need for re-encryption
- Allows for Data Security Intelligence reporting directly in the console, as well as options for retrieval via SIEM agent or API

A Smartkey is a unique key generated by the Smartcrypt application for a specific file, folder, or other protected asset. With Smartkeys, user access can be added or revoked 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. Smartcrypt also allows users to encrypt data for external parties such as vendors or partners. A cloud-based key server stores and distributes keys based on the organization's security policies, even for external users who are granted access after the encryption takes place.

In addition to the encryption applied to the protected data, each Smartkey itself is encrypted and exchanged according to a policy-driven access list. This innovative approach allows security managers to respond quickly when a user loses a protected device, or when access needs to be revoked from an individual or group. By simply changing the encryption on the Smartkey, administrators can block unwanted access without the need to re-encrypt large amounts of data.

How Smartcrypt Benefits Your Business

Securely Exchange Data

Smartcrypt applies persistent encryption to files before they are exchanged with outside partners and customers. This enables an organization to retain control over information regardless of how many times that information is copied, backed up or forwarded. This approach also allows users to exchange sensitive information through cloud services or protocols like email and FTP that provide little security on their own.

Ensure Regulatory Compliance

Compliance standards in the financial services, healthcare, and government sectors mandate the protection of data at rest and in motion. Smartcrypt facilitates mandated separation of duties, protection from insider threats, and integration with DLP processes. The manager console also provides visibility into where sensitive information is being transmitted and accessed.

Protect Cross Platform

From mainframe to mobile phone, Smartcrypt provides complete cross-platform encryption. 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. Smartcrypt is also easily integrated into back-office and batch processing workflows.

Enhance DLP

Organizations need flexible data security solutions that work with data loss prevention technology and processes. Smartcrypt can be integrated with existing DLP strategies to ensure that DLP scanners can access and remediate encrypted data.

Identify Sensitive Information

Smartcrypt's intelligent data discovery capabilities allow organizations to monitor network servers and end-user devices for regulated or proprietary information. Sensitive data can be encrypted or deleted as soon as it is saved, while administrators can provide detailed reports to demonstrate compliance with internal and external mandates.

Enterprise Cross Platform

- An end-to-end encryption application available for every enterprise operation system

Embedded Key Management (Smartkeys)

- Automatic public/private key generation, synchronization and exchange
- Ability to exchange and manage keys with external collaborators
- Retain control over data after it has left the organization
- Access to data can change without re-encryption
- Delivery of keys to enterprise IT, Audit and DLP people and technology

Advanced platform control

- Smartcrypt Manager provides visibility, policy, control, discovery
- Access easily revoked or automatically expired

High Performance

- Takes advantage of IBM and Intel hardware encryption accelerators
- Data compressed up to 95% before encryption, resulting in significant storage/transit savings

Existing PKI

- Support for OpenPGP encryption and key formats
- Support for X.509 certificate based encryption
- Support for passphrase based encryption

TECHNICAL SPECIFICATIONS

OPERATING PLATFORMS:

» Microsoft Windows
» Linux: RHEL (.rpm) and SLES (.deb)
» UNIX: Oracle Solaris (Sparc and x86), IBM AIX and HP-UX
» IBM z/OS, IBM i, and Linux for Z Systems
» Apple Mac OS X and iOS
» Google Android

ALGORITHM

» Encryption: 3DES, AES128, AES192, AES256, CAST5 IDEA, AE-x
» Signing: SHA-1, SHA-256, HA-384, SHA-512
» Strict checking and check revocation status (optional)

KEY STORAGE AND RETRIEVAL

» Hardware: KMIP HSM, Smartcards including PIV / CAC
» Software: PKCS#11, LDAP, KMIP, CAPI/CNG, Keychain, Keystore, ICSF- CKDS, PKDS, Security Server, RACF, ACF2, Top Secret

FILE ENCRYPTION CERTIFICATE AND KEY TYPES

» Smartkeys
» X.509 Digital Certificates
» OpenPGP

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