PKWARE

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

SMARTCRYPT

SMARTCRYPT SOFTWARE DEVELOPMENT KIT

Application Layer Encryption for Structured and Unstructured Data

The stakes get higher every day. External security threats grow increasingly 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 traditional approaches to data security are no longer sufficient. Common solutions such as full disk, volume, and transparent data encryption provide single use case, non-persistent protection applied below the data level, leaving sensitive information exposed to database and IT administrators. To meet today's cybersecurity challenges, organizations need persistent data-level protection, so that information remains inaccessible even after a security breach.

Introducing the Smartcrypt SDK

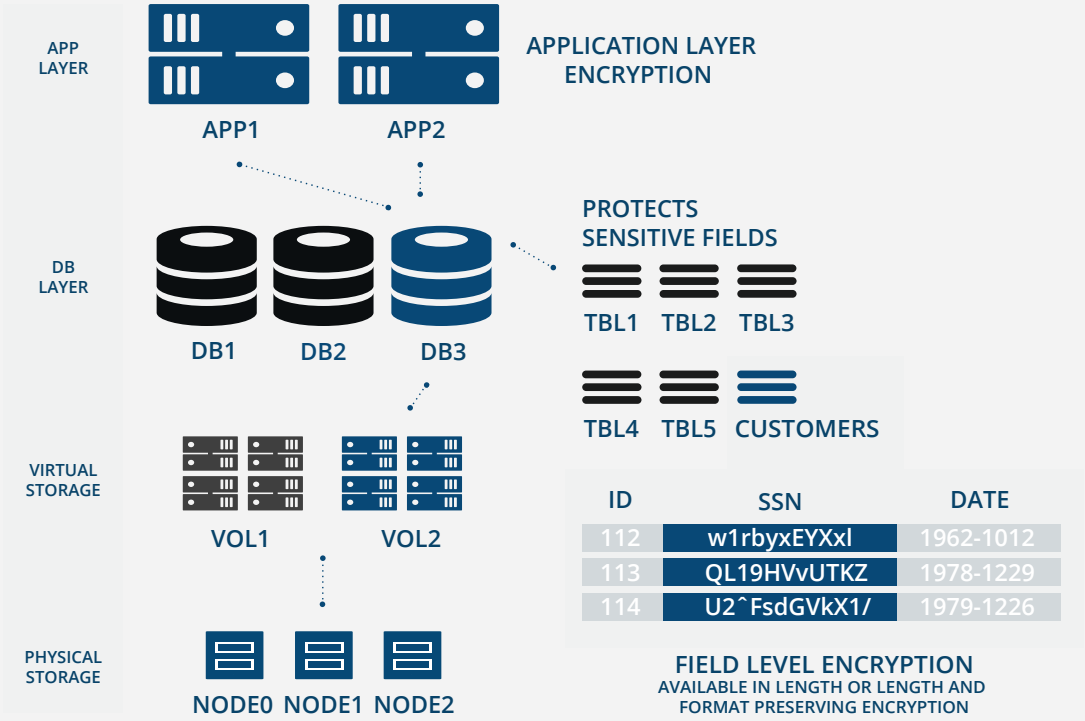
PKWARE's Smartcrypt Software Development Kit delivers high performance, cross-platform security that is easily embedded and managed without changing the way people work. Embedding encryption operations directly into an application increases protection from security gaps existing in people, processes, and technology. Application layer encryption also provides end-to-end protection, eliminating vulnerabilities in adjacent applications and downstream systems used to process store and exchange sensitive information.

Available for both structured and unstructured data, the Smartcrypt SDK integrates at the data access layer of the application (not the database or storage layer), ensuring that information is encrypted on capture and only decrypted when being displayed by an authorized application or device.

Encrypting Structured Data

For applications that process structured data, only columns/fields that contain sensitive information, like credit cards or social security numbers need to be encrypted. This approach allows easy integration into an existing application, and enables both application developers and database administrators to continue performing their duties while restricting only the visibility of sensitive information. For maximum compatibility there are available options for length preserving and length + format preserving encryption to aid in maintaining referential integrity.

Application Layer Encryption



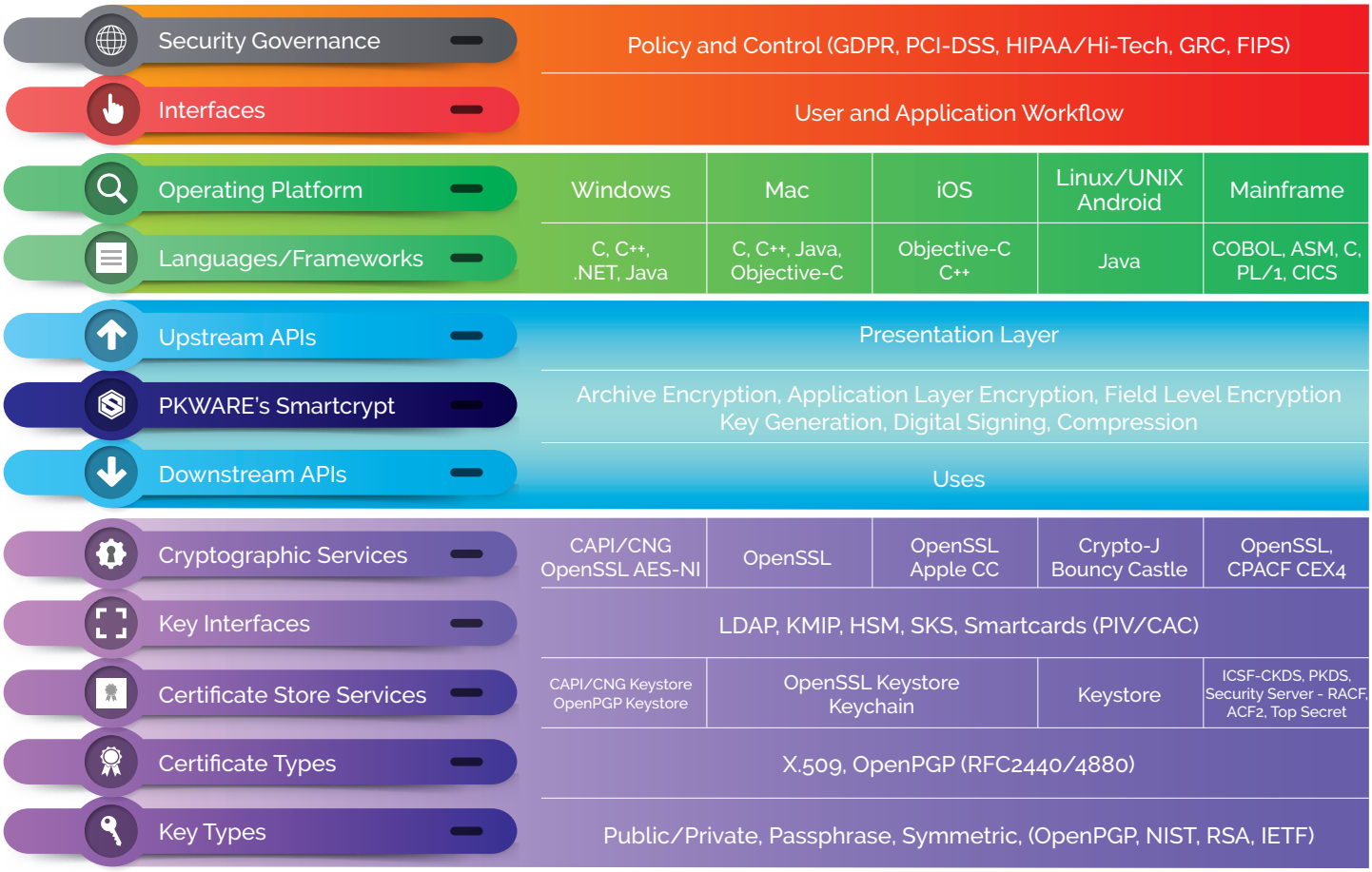
Encrypting Unstructured Data

For applications that process sensitive information stored in files, encryption travels with the data and prevents unauthorized access.

Highlights

- Application Integration: Stream data directly to/from applications without staging data to disk
- File Name Encryption: Encrypt the file names and other file metadata to ensure no sensitive information is exposed
- Secure Wipe: Shred files using the DOD 5220 standard. This provides organizations with an additional level of configurability and assurance that deleted files are not recoverable.
- Compression: All the compression, decompression and archive management capabilities available for .ZIP
- Self Extracting: Create self-extracting ZIP files for automatic unzip and extraction

The Smartcrypt SDK is available in multiple languages and is easy to use. It handles the complexity and heavy lifting of the most well vetted cryptographic services, key interfaces, key stores and key types accessible on each operating platform.



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.

Exceed Compliance Requirements

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, 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 enable sensitive information discovery and encrypted remediation.

The Smartcrypt Platform

Smartcrypt Application

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.

SOLUTION DIFFERENTIATORS

INTEGRATES INTO EXISTING APPLICATIONS

- Encryption at the application level preserves user workflows and functionality
- Stream data directly to/from applications without staging data to disk
- All encryption key management can occur in a single, callable external application
- Not required to rip and replace systems

STRUCTURED DATA

- Enables applications to protect data at the field/column level
- No changes to field length or format are required. Eliminates increase to the size/structure of the database
- Encrypts/decrypts one or more columns/fields in one step
- Changes consist of two to three lines of code

UNSTRUCTURED DATA

- Allows applications to produce and consume encrypted files
- Allows applications to produce and consume digitally signed files

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)

STANDARDS BASED

- 100% standards based; no proprietary crypto
- Supports multiple encryption systems, algorithms, key formats, and key stores
- Uses NIST FIPS 140-2 validated cryptographic libraries for .ZIP encryption

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