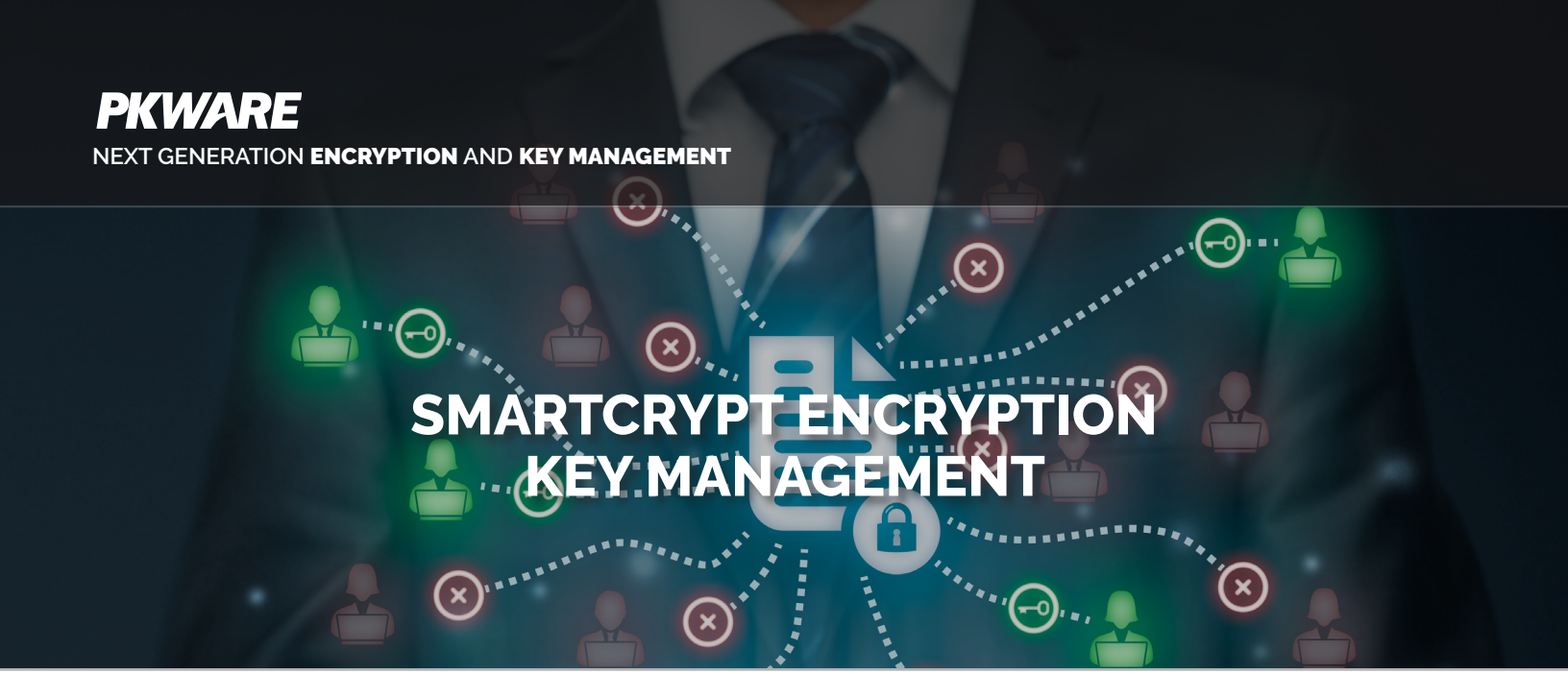
PKWARE

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



SMARTCRYPT ENCRYPTION KEY MANAGEMENT

Executive Summary

Encryption key management is the cornerstone of any enterprise encryption solution. The National Institute of Standards and Technology (NIST) has provided guidelines on best practices for key management. These guidelines (below) are recognized by federal and industry standards as critical steps to building strong key management solutions.

- **Dual control means no one person should be able to manage an individual's encryption keys.** Creating, distributing, and defining access controls should require at least two people.
- **Separation of duties means different people should control different aspects of key management strategies.** The person who creates and manages the keys should not have access to the data. In addition, the person with access to protected data should not be able to manage encryption keys.
- **Split knowledge applies to the manual generation of encryption keys, or the point where they are available in the clear.** In this situation, more than one person should be required to constitute or reconstitute a key.

However, these best practices do not allow storing encryption keys along with encrypted data, which makes it impossible to meet compliance requirements such as PCI-DSS Section 3. Dual control, separation of duties, and split knowledge can only be achieved when an external key manager is used.

Challenges with key management:

- Multiple, separate, and possibly incompatible encryption tools may be used unknowingly in large enterprises. This results in thousands of encryption keys, and each must be securely stored, protected, and retrievable in a reliable fashion.
- Sensitive data resides in multiple locations throughout an organization. This means keys must be managed in a practical, automated, and risk-mitigated way throughout their lifecycle, and only credentialed entities can access them.
- Keys grow exponentially as companies manage the data encryption lifecycle. Companies must understand how to control and protect access to keys to ensure they do not get into the wrong hands.
- Encryption implementation requires the establishment of a shared key in advance.
- Lack of unified tools that reduce management overhead. Keys and key management software from different vendors are not interoperable. If a key management system is purchased from a supplier such as IBM, it cannot manage keys from another supplier like Seagate, since vendors implement encryption in different ways.

Introducing Smartcrypt

PKWARE's Smartcrypt provides seamless key management in order to avoid direct user access to keys, key-rings, and public/private key files, etc. It allows encryption to be managed on an owner/recipient level, which avoids common key sharing and access issues that occur with traditional PKI systems today. All keys are stored securely on each device on that platforms native encryption key storage mechanism and encrypted copies of those keys are maintained and managed utilizing PKWARE's Smartcrypt Manager.

The Smartcrypt Manager

- Windows application that runs in the customer private cloud, backed by an application layer encrypted SQL database.
- Integrated with Active Directory users and groups for authentication, policy management and encryption key issuance / withdrawal. (note: also supports non-AD managed accounts)
- Facilitates automatic synchronization of private keys among authenticated systems
- Performs identity federation for public key retrieval through the Smartcrypt (note: can be run in island mode if external key exchange is not required)
- Improves upon traditional key escrow through policy groups and policy keys
- Includes Data Security Intelligence reporting for regulatory compliance
- Supports SIEM integration through Splunk
- Provides licensing and activation for client devices / users within an organization

The Smartcrypt Application

- Agent based application that performs encryption, decryption, digital signing and authentication of files
- Installs on mobile, desktop and server endpoints
- Integrates with Microsoft Outlook for encrypted e-mail (attachments and body) and Microsoft Office for "Save Secure"
- Rich command-line interface for batch processing
- Integrates with Windows Explorer / Mac Finder
- Full encryption / decryption support on iOS and Android
- Supports multiple encryption systems including OpenPGP, X.509, passphrases

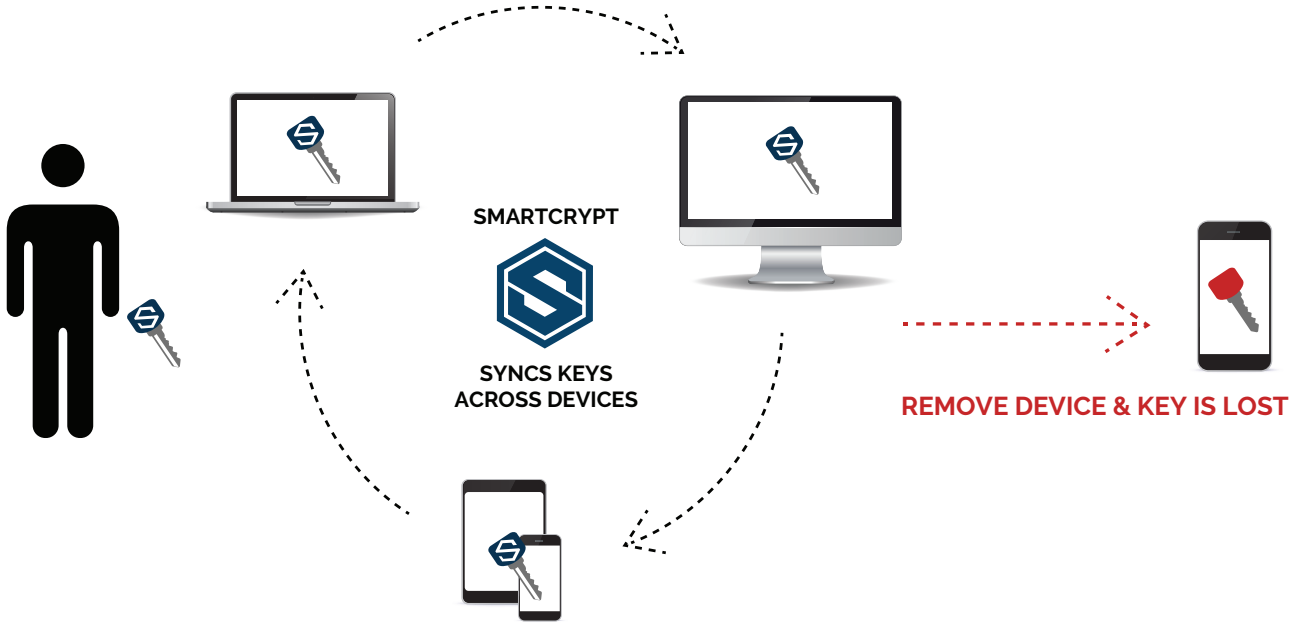
Smartkeys

What are they?

Smartkeys are long, random, unique symmetric keys generated by the Smartcrypt Application. They can be user defined or admin defined and are essential in providing a seamless experience. They are a replacement for passwords and traditional PKI.

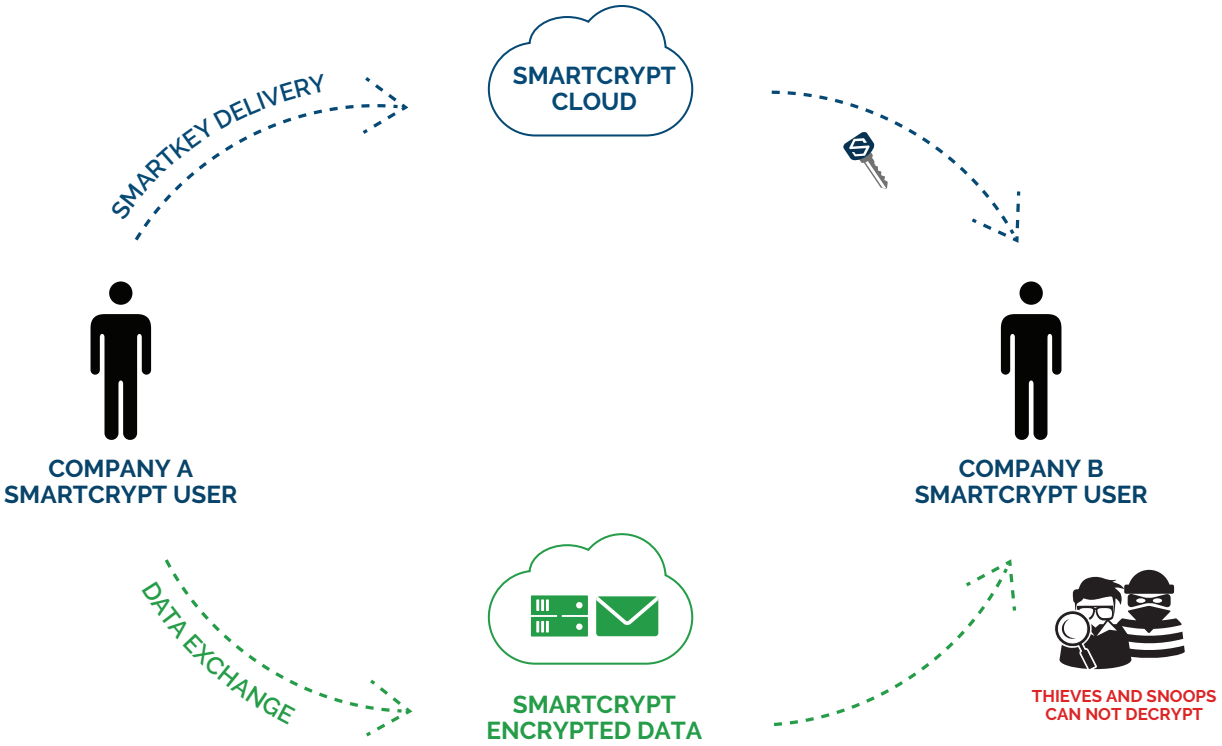
Key Synchronization

When a user authenticates a new device, their public/private keys and any Smartkeys they have access to are automatically synchronized. When a device is lost or stolen, it can be unlinked causing all of keys to get purged.



Key storage and exchange

Smartkeys are exchanged through Smartcrypt Managers and each key is encrypted for the public keys of those authorized to use it. Smartkey access lists can contain Smartcrypt users both inside and outside of the organization. When a user is added to a Smartkey, that key is instantly delivered to all of that users authenticated devices, ensuring they can access secure content immediately. If the user is outside of the organization, the Smartcrypt Cloud facilitates secure external delivery. Data secured with Smartkeys follows whichever path it is currently being used in.



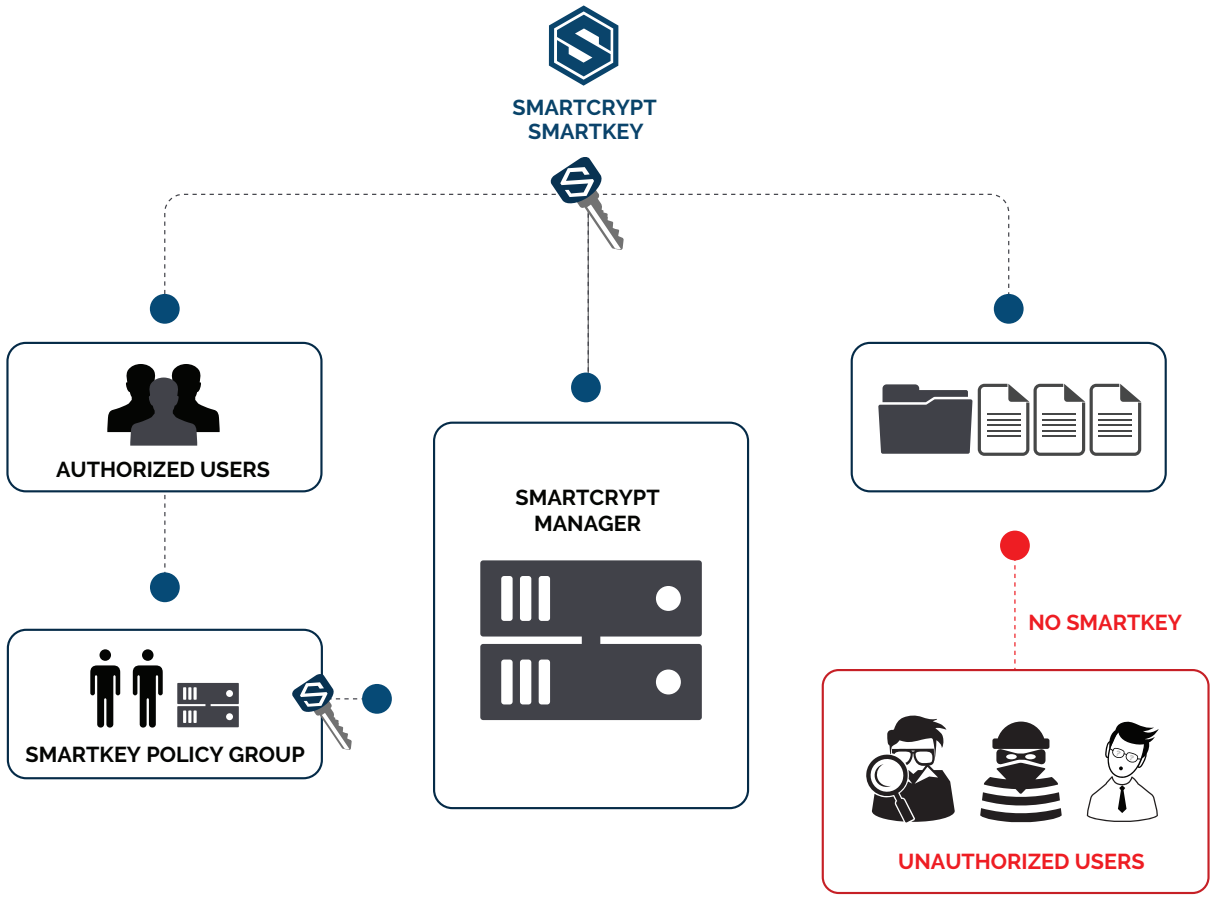
Access Control and Usability

Bundling encryption and key management together solves many of the identity and access related workflows found in traditional PKI solutions. Encryption access is defined by user identities rather than by actual keys (passwords, common names, PGP keys, etc.), removing IT complexity and improving end-user experience. Smartkeys can be created and assigned by e-mail address to users that don't even exist within the ecosystem yet. As soon as their account is created, Smartkeys are automatically delivered to all of their authenticated devices.

Individuals can be added or removed from a Smartkey at any time without ever needing to re-encrypt the data associated with the key. This approach allows organizations to apply persistent, data level encryption to files in shared workspaces like network shares, cloud drives and even removable media. For example, when a user joins a team, they can be issued the team Smartkey(s) which grants them instant access to all data encrypted with those keys. When they leave the team, access can be revoked. Any time access changes, all key material is re-encrypted and redistributed to the remaining authorized users without having to update the data files themselves. Note: this type of zero-impact re-encryption is only available with Smartkeys.

Enterprise IT, Audit and DLP

Users and Administrators encrypt data using Smartkeys defined by their organizations security policy. This data can be used, shared or stored in a variety of places including network drives, e-mail, cloud storage, etc. Persistent data level encryption keeps Thieves, Snoops and Idiots from exposing data as only authorized users can decrypt it. Persistent encryption at the file level can often present access problems for IT and Audit as well as discovery problems for DLP and Legal. Smartkeys can also be silently applied to encryption operations insuring that these individuals and technology systems never lose accesss or visibility into the organizations sensitive information.



Passphrases and 3rd party Public Key Infrastructure

Smartcrypt also supports passphrases, OpenPGP keys and X.509 certificates for strong encryption operations. These systems can be together because Smartcrypt is a hybrid-crypto-system combining the speed of symmetric encryption for actual data encryption with the security of asymmetric encryption for protecting key material. Recipients can access data using whichever type of key they have access to. This approach is flexible enough to support decryption by non-Smartcrypt clients that also support ZIP strong encryption.

Conclusion

As data breaches become more commonplace and increasingly more complex, it is no longer a matter of "if" a may occur, but rather a matter of "when" one will occur.

Regulatory compliance is not the solution, but provides a solid starting point for securing data. No defense-in-depth strategy is complete without a data focused security solution. Persistent data protection provides this and when combined with embedded, flexible key management a solution can be delivered that is easy for architects to embed, IT administrators to control and end users to operate.

For 29 years PKWARE has focused on data. From our compression heritage to strong encryption PKWARE protects data for over 30,000 enterprise customers and 200 government agencies. Our all-software approach provides cost effective usable security that is easy to implement on every enterprise operating system from mainframe to mobile.

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