PKWARE

pkware.com

Building Seamless Key Management Strategies

How To Achieve the Complex Combination of Flexibility, Strength, Control, and Usability for Encryption.

Contents

Executive Summary

Encryption key management is the cornerstone of any enterprise encryption solution. The National Institute of Standards and Technology (NIST) provided October 2019 guidelines on best practices for key management in NIST SP 800-57 PART 1. These guidelines are recognized by federal and industry standards as critical steps to building and implementing 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.

Encryption keys are analogous to the combination of a safe.

PK Encryption's strong algorithms and smart management of encryption keys are **essential** to sensitive data protection.

However, these best practices do not allow storing encryption keys along with encrypted data, which puts them at odds with meeting 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.

"Strengthening cryptographic standards and validation has long been a mainstay of NIST's cybersecurity efforts, and 2021 will be no different, examining new approaches to encryption and data protection."

2021: What's Ahead from NIST in Cybersecurity and Privacy
NIST, February 2, 2021

Challenges with Key Management

- In large enterprises, multiple, separate, and possibly even incompatible encryption tools can be used unwittingly. The result can be thousands of encryption keys which all must be securely and reliably stored, protected, and retrieved.
- Each encryption implementation requires the establishment of a shared key in advance.
- Sensitive data resides in multiple storage and device locations throughout an organization. This means keys must be managed in a practical, automated, and risk-mitigated way throughout their lifecycle, with only credentialed entities accessing them.
- Keys grow exponentially as companies manage the data encryption lifecycle. Companies have to understand how to best control and protect access to keys to ensure they do not get into the wrong hands.
- Lack of unified tools increases management overhead. Keys and key management software from different vendors are not interoperable, and encryption is implemented in different ways.

Introducing PK Encryption for Enterprise

PK Encryption is an innovative platform providing an otherwise unavailable combination of flexibility, strength, control, and usability. Because PK Encryption was built to utilize both PKWARE key management as well as partners' and other third-party key management systems flawlessly, your company has an array of choices to select from. At the enterprise level, it is critical to choose technology that works in your environment and meets all the challenges described above.

PK Encryption software is built on Smartkey technology and provides seamless key management capabilities, allowing you to avoid direct user access to keys, key-rings, and public or private key files. It authorizes encryption to be managed on an owner or recipient level, which avoids common issues in key sharing and access that occur with traditional PKI systems today. All keys are stored securely on each device of that platform's native encryption key storage mechanism. Encrypted copies of those keys are maintained and managed utilizing PK Encryption Manager.

PK Encryption Manager

- Windows application that runs in the customer private cloud, backed by an application layer mode (if external key exchange is not required) 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 PK Encryption and 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 and users within an organization

PK Encryption Application

- Installs on mobile, desktop, and server endpoints
- Integrates with Microsoft Outlook for encrypted email (attachments and body) and Microsoft Office
- Offers a rich command-line interface for batch processing
- Integrates with Windows Explorer / Mac Finder
- Delivers full encryption and decryption support on iOS and Android
- Supports multiple encryption systems including OpenPGP, X.509, and passphrases

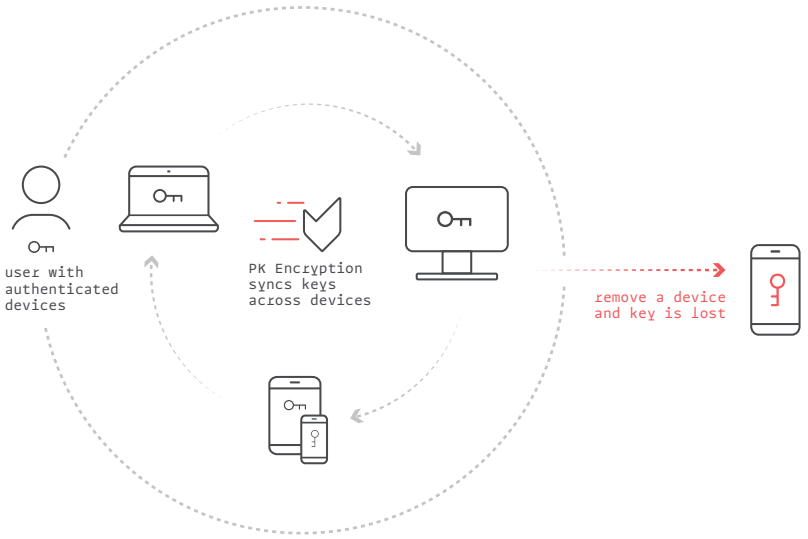
PK Encryption Smartkeys

What Are They?

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

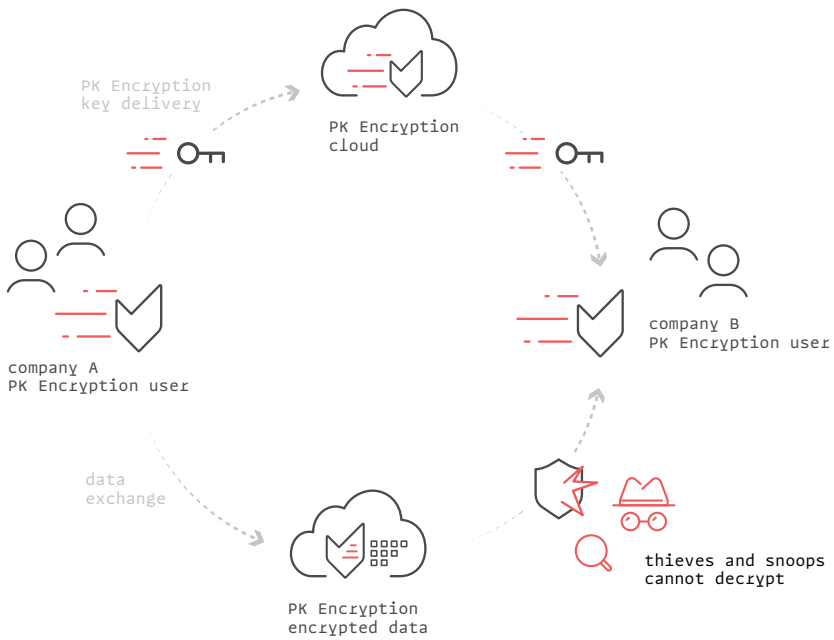
PK Encryption Key Synchronization

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



PK Encryption Key Storage and Exchange

PK Encryption Smartkeys are exchanged through PK Encryption Managers, and each key is encrypted for the public keys of the authorized user(s). Smartkey access lists can contain PK Encryption 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 user's authenticated devices, ensuring they can access secure content immediately. If the user is outside of the organization, the PK Encryption Cloud facilitates secure external delivery. Data secured with PK Encryption Smartkeys follows whichever path it is currently being used in.



Access Control and Usability

Bundling encryption and key management together in PK Encryption solves many of the identity and access related workflows found in traditional PKI solutions. PK Encryption access is defined by user identities rather than by actual keys (passwords, common names, and PGP keys), removing IT complexity and improving end-user experience.

Smartkeys can be created and assigned by email 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 Smartkeys which grant 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 any users having to update the data files themselves. This zero-impact re-encryption is only available with Smartkeys.

Enterprise IT, Audit, and DLP

Users and Administrators encrypt data using PK Encryption Smartkeys defined by their organization's security policy. This data can be used, shared, or stored in a variety of places, including network drives, email, cloud storage, and on-premises repositories. Persistent data level PK Encryption keeps thieves and misusers from exposing data, as only authorized users can decrypt it.

Persistent encryption at the file and element level can often present access problems for IT and Audit teams as well as discovery problems for DLP and Legal teams. By utlizing PK Discovery and PK Encryption, all team members with appropriately defined roles can readily discover, view, and encrypt sensitive data at both the element and file levels, according to the company's policies. PK Encryption 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 Third-Party Public Key Infrastructure

PK Encryption also supports passphrases, OpenPGP keys, and X.509 certificates for strong encryption operations. These systems are able to co-exist due to PK Encryption's hybrid-crypto-system, which combines 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 breach 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 decades, PKWARE has focused on data. From our compression heritage to strong PK Encryption, PKWARE protects data for both enterprise customers and 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 and in data stores from on-premises repositories to all major cloud platforms.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

Enterprise-Wide Policy Management

The PKWARE Enterprise Manager provides a single point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification, and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204