Every month, it seems, another prominent company suffers a catastrophic data breach. In some cases, the fault lies with employees or contractors who failed to observe proper security procedures. In others, the company’s network or device defenses were simply not strong enough to withstand an attack from a skilled hacker or hostile government.

No matter how these breaches occur, one fact inevitably surfaces in the aftermath: the compromised data was not protected by persistent encryption, so whoever stole it will be able to access and use it. Corporations already dealing with consumer and shareholder backlash find themselves paying millions in fines and legal settlements, in addition to paying for long-term identity theft protection for individuals whose personal data was stolen.

Given the abundance of these examples in recent years, why would any company, organization, or government agency fail to encrypt their data?

The answer is simple. Implementing persistent encryption is difficult for any employer, and becomes almost impossible as the size of the organization increases. Each of the two predominant approaches to data encryption—passphrase-based symmetric key encryption and PKI-based asymmetric key encryption—creates a set of challenges that most organizations would prefer to avoid.
Option #1: Passphrases

Symmetric key encryption, the oldest form of data protection, still accounts for 80% of the encryption in use today. Organizations that use encryption typically choose a passphrase-based approach because it is simpler to implement and easier for end users to understand.

Despite its initial appeal, symmetric key encryption has several significant drawbacks:

- **Insufficient key strength:** Data protection is only as strong as its weakest element. Users often believe they have created an unbreakable passphrase, only to learn that hackers were able to discover it through a brute-force attack or other computational strategy.

- **Insecure key exchange:** Even when users create strong passphrases, they are faced with the problem of exchanging those passphrases with the people who need them. Passphrases are easily compromised when shared through email or other insecure channels.

- **Irrevocability:** Passphrase-based encryption provides no mechanism for revoking access to protected data. When a passphrase is compromised, the data remains accessible to anyone who has the key.

- **Potential for lockout:** When end users apply their own passphrase-based encryption, they give themselves control over the data. Encrypted files are inaccessible to auditors, security personnel, and data leakage prevention technology unless the user shares the key. Employees or contractors who depart without providing their encryption keys can leave a company permanently locked out of its own data.

Option #2: PKI

A stronger alternative to symmetric key encryption, public key infrastructure represents only 20% of the data encryption in use today. PKI provides excellent protection when used correctly, but few organizations have the resources and technical savvy to implement and support an enterprise-wide PKI solution.

Whether companies rely on the PGP web of trust or a 3rd party backed rigorous X.509 standard, PKI encryption involves an assortment of difficulties:

- **Identity creation requirements:** In order to use PKI-based encryption, users must establish an identity by satisfying potentially cumbersome validation requirements from their chosen certificate authority. PKI does not allow users to encrypt data for individuals who have not yet established an identity.

- **Insecure private key transfer:** Users need copies of their private keys on every device they will use to access encrypted data. Moving keys to other systems, and especially to mobile devices, can be impossible without relying on email or other insecure channels.

- **Unfamiliar workflows:** Exchanging public keys can be difficult and time-consuming, especially for users who have not used PKI in the past.

- **Key escrow requirements:** As with passphrase-based encryption, keys need to be available to IT and other departments to facilitate audits and data loss prevention scanning. Key escrow, however, often creates difficulties in determining which keys are associated with which sets of data.

- **Irrevocability:** While PKI gives administrators the ability to revoke a digital certificate when a key is compromised, this does nothing to prevent anyone with the key from accessing stolen data.

- **Heavy resource demands:** Key rotation, necessary for long-term security, requires that organizations replace encryption keys for all protected data, which can take weeks or months and consume massive amounts of resources.
Option #3: No Encryption

Unfortunately, the problems inherent in traditional encryption methods leave most organizations where they started, without company-wide data-level protection. This exposes them to massive financial and legal consequences, and often creates a second set of issues as employees try to fix the problem themselves. When a company lacks a consistent encryption policy, employees often take matters into their own hands and apply end-user encryption to sensitive files. This effectively blocks access by auditors and data leakage prevention scanners, and raises the potential for the company to lose access to its own data.

In addition to the problems with existing encryption methods, a second cause has contributed to the slow rate of adoption for data-level protection: a failure by companies to appreciate the true value of their data. While corporations assign a value to every physical asset they own, including their mainframes, laptops, and mobile devices, their general ledgers do not include a single line item for the value of the data on those devices. This perceived lack of value can bias business decisions and create the illusion that data-level encryption is unnecessary. In many security managers’ minds, a company-wide implementation of either PKI or passphrase-based encryption is guaranteed to be costly and difficult, while the cost of going without encryption is undefined and the risk of a breach is unknown.

A sea change is under way. As hackers grow more sophisticated and breaches become more common, more companies will begin to see the true value of their data and the insupportable risk of leaving it unprotected.

The Key Management Challenge

When companies weigh the relative advantages and disadvantages of passphrases and PKI, the analysis typically comes down to a single consideration: encryption key management.

Generally considered the most challenging aspect of enterprise-wide encryption, key management involves a variety of functions, including key generation, key storage, key exchange, and key rotation. While reliable encryption algorithms and hash functions have existed for decades, an optimal approach to key management has remained elusive.

To meet the needs of large, complex organizations, an encryption solution must include key management methodology that addresses a wide variety of challenges:

- Private key creation and synchronization to authorized devices
- Public key creation, synchronization and exchange
- Encrypting data for entities that have no published public key
- Adding or removing access to shared data without the need to re-encrypt the actual data
- Allowing administrative functions such as IT review, audits, and data loss prevention scanning to remain operational
- Rotating keys to minimize the risk of theft or compromise
- Eliminating usability issues and obstacles for end users
Neither passphrases nor PKI can solve all of these challenges, and some challenges remain no matter which encryption strategy a company chooses. This is likely the reason so many organizations choose to go without data-level protection, despite the obvious risks of their position.

Today, companies no longer need to choose between problematic encryption and no encryption at all. PKWARE’s new Smartcrypt solution, built on revolutionary Smartkey technology, overcomes the challenges posed by key management by combining the best aspects of traditional encryption methods.

Bridging the Gap Between Passphrases and PKI

PKWARE’s innovative Smartcrypt platform delivers persistent end-to-end data encryption, without the vulnerabilities or administrative burdens of passphrases and PKI.

The Smartcrypt platform supports a wide variety of encryption systems, key types, and key interfaces. Smartcrypt also features Smartkeys, a proprietary encryption key management solution that simplifies and automates key generation, storage, and exchange.

Smartkey technology allows for complete control over who can decrypt files and read data, even when encrypted data has been copied or shared. Security administrators can use Smartcrypt to grant and revoke access to encrypted material at any time, including providing keys for use by IT, audit and DLP teams.

From an end user perspective, Smartcrypt is almost completely transparent. Using Smartkeys, the application automatically creates public and private keys for users, syncs them with their devices, delivers them to IT for escrow, and performs seamless public key exchanges with external partners and customers. Encryption can be incorporated into existing workflows, eliminating the difficulties associated with other encryption methods.

Smartkey Technology

PKWARE’s Smartcrypt platform is based on Smartkey technology, which delivers a previously unavailable combination of strength, control, and usability.

A Smartkey consists of one or more encryption keys and a corresponding access control list that defines which individuals can use the keys. Smartkeys can be applied to one file or to several files at once, and take the place of PKI or passphrases in older encryption methodologies.

Smartcrypt software agents installed on user devices and network assets encrypt data at the file level using a Smartkey, in accordance with the organization’s security policy. The encrypted data can be used, shared, or stored in multiple ways, either within the company’s systems or on external networks and devices.

Smartcrypt is compatible with all enterprise operating systems, so authorized users can access protected data using any device on which the Smartcrypt application is installed.
Encrypt sensitive data using Smartcrypt software agents on protected devices and file servers.

Administrators use the Smartcrypt Enterprise Manager to define and apply the organization’s encryption policies. Policy keys can be included in any encryption operation to facilitate access by audit personnel or DLP technology.

Smartcrypt automatically delivers and synchronizes encryption keys, making the key management process transparent for end users.

PARTNERS / CUSTOMERS
Can decrypt and read files for which they have been granted access. Administrators can revoke access to encrypted data at any time.
Inside a Smartkey

Each Smartkey has three components: the session key, the asset key, and the access control list (ACL).

- The Session Key is a symmetric key generated by the Smartcrypt application and used to encrypt the data. The session key is an AES256 key, providing strong protection for the underlying data.

- The Asset Key is a second AES256 key generated by the Smartcrypt application. The asset key is used to encrypt all session keys associated with files controlled by the Smartkey.

- The Access Control List (ACL) is a list of one or more users (designated by email addresses) that are allowed to use the Smartkey. User accounts can be integrated with Active Directory, and individual user devices can be managed via the Smartcrypt Enterprise Manager. Smartkeys are synchronized through Smartcrypt to all user devices defined by the ACL. When the ACL changes (for example, when an authorized user is removed from the list), the asset key is re-encrypted and redistributed to the remaining users on the list. This process, in which only the key material needs to be re-encrypted, saves the time and resources that would otherwise be dedicated to re-encrypting the underlying data. Although Smartcrypt supports a variety of encryption key types, this type of zero-impact re-encryption is only available with Smartkeys.

Smartkey technology solves the problems that have limited the adoption and use of strong encryption. Functions that once involved risk and manual intervention are now simple and automatic:

- Synchronizing private keys to all devices that need them
- Exchanging public keys with all users who need them
- Creating identities through integration with existing identity access management solutions
- Providing access to encrypted data for use in data loss prevention and auditing
- Revoking access from individuals without the need to re-encrypt data
- Enabling access for additional individuals after data has been encrypted

Flexibility and Control

Key exchange is one of the most troublesome aspects of PKI or passphrase encryption. With Smartkey technology, however, key exchange happens automatically, based on the configuration of the Smartcrypt manager console and the users listed in each ACL.

Smartkey access can be defined by system administrators, simplifying the process for end users and allowing administrators to ensure compliance with the company’s existing IT security policies. Where appropriate, end users can also define Smartkey access for their encrypted data, removing the burden from IT.

Access to Smartkeys can even be defined for users who don’t yet exist within the ecosystem. Once new users take the steps to create or register their accounts, any Smartkeys to which they have access will automatically be delivered to their devices.
Opportunities for Implementation

Smartkey technology has applicability for dozens of industries and business models. The strength and simple administration provided by Smartcrypt has value for any company that wants to protect its intellectual property, or that needs to ensure compliance with data security regulations. Smartkey technology is especially well suited to meet the needs of government contractors and businesses in the financial services and healthcare sectors.

Financial Services

Banks and other organizations in the heavily-regulated financial services industry are subject to a variety of data security requirements. Some of these requirements (Gramm-Leach-Bliley, Sarbanes-Oxley) are imposed by the federal government, while others (PCI DSS) are imposed by industry councils. As the threats to financial data grow and multiply, both government and industry authorities are likely to continue to increase their requirements for strong protection of data at rest, in motion, and in use.

Government Contractors

Companies that do business with the government must meet strict requirements related to data security. Federal government agencies and their vendors are subject to Federal Information Processing Standards (FIPS 140) requirements, which include specific mandates related to which encryption algorithms must be used and how keys are to be maintained. Companies whose systems fail to meet the applicable FIPS-140 requirements for their product or industry are unable to compete for government contracts. PKWARE’s Smartcrypt solution meets or exceeds all FIPS-140 standards for key management.

Healthcare

Hospitals, medical groups, insurance companies, and other organizations in the healthcare industry must ensure the security of patients’ personal data. The data security requirements included in laws such as HIPAA and HITECH will likely be supplemented by additional mandates in coming years. Smartkey technology is ideally suited to help healthcare organizations protect their data as they share and exchange it with multiple external partners.
Benefits of Adoption

With complete cross-platform functionality and a software development kit in all major programming languages, the Smartcrypt platform is ideal for even the largest and most complex organizations. Companies that adopt data-level encryption based on Smartkey technology can expect to see multiple long-term benefits:

- Simpler administration: Smartkey technology streamlines and automates encryption key management, including critical processes such as key generation, key synchronization, key exchange, and key escrow.

- More reliable protection: Smartkeys are generated and exchanged by Smartcrypt software agents, removing opportunities for human errors that could compromise an organization’s data.

- Simplified end user training: When implementing other encryption solutions, organizations need to devote considerable resources for end user training. Companies using passphrase-based encryption need to educate employees on why and how they should create strong passphrases, while companies using PKI need to provide extensive training on identity creation and key exchange. Smartcrypt implementations, however, typically require little to no end-user training, as the application handles most aspects of key management automatically.

- Higher performance: Smartcrypt applies PKWARE’s advanced compression technology before encrypting data, resulting in significant improvements in processing time and lower storage requirements. Smartcrypt is also one of the few encryption technologies that utilizes customers’ available IBM or Intel hardware accelerators, further reducing processing times.

- Cross-platform functionality: Smartcrypt is compatible with every enterprise operating system, enabling customers to protect their data on everything from mainframes to mobile devices. The Smartcrypt software development kit is available in every major programming language and allows Smartkey technology to be incorporated into existing applications with only a few lines of code.

- Scalability: Smartcrypt is a software-defined solution, requiring no new hardware or infrastructure, so implementations can be easily scaled up as needs change and customers grow. The application and management console run as fast as the customer’s existing applications and processes.

- Data Security Intelligence: Smartcrypt administrators have complete visibility into what data has been encrypted and who has access to it. Security data can be included in reports from the manager console or exported via an API or SIEM agent.

- Lower total cost of ownership: By streamlining workflows and eliminating manual tasks, Smartkey technology greatly reduces the time and effort needed to support a company’s encryption solution. Reduced demands on IT staff and computing resources result in lower costs and greater value for the company’s security investment.

Most significantly of all, Smartkey technology removes the barriers which have prevented many companies from protecting their critical information. Organizations that may have considered and rejected enterprise-wide encryption in the past can now move forward with a solution that allows them to protect their data everywhere it is used, shared, or stored.
About PKWARE

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.