PKWARE | SMARTCRYPT

POLICY-DRIVEN SOLUTIONS FOR SECURE DATA EXCHANGE

Sending and receiving data is a fundamental part of daily business for nearly every organization. Companies need to share financial transaction details, customer information, employee data, intellectual property, and other forms of sensitive information with a wide range of external parties.

However, each time an organization sends sensitive data outside its own network, it exposes itself to risks. Data can be intercepted en route, stolen from recipients, or passed along to unauthorized parties. The financial and public relations consequences of these types of data breach grow more severe each year.

OBSTACLES TO SECURE DATA EXCHANGE

Strong encryption is the only reliable method for protecting data as is shared between individuals or organizations. When implemented correctly, encryption makes it impossible for anyone to read protected data without a valid decryption key. A growing number of industry and governmental mandates require the use of encryption for certain forms of sensitive data.

While more and more organizations have begun to adopt encryption, the problem of sharing sensitive information with external parties has remained difficult to solve for a variety of reasons:

- **Incomplete Coverage:** most encryption solutions only address a handful of use cases, leaving security gaps where data is stored or sent in unencrypted form. These gaps are easy for sophisticated attackers to identify and exploit.
- **Passphrase Exchange:** when files are protected with symmetric encryption, the sender must somehow provide the passphrase to the intended recipient. This often results logistical difficulties or in passphrases being sent through insecure channels.
- **Uncontrolled Encryption:** when users encrypt files using tools and passwords they have chosen themselves, they create the possibility that the organization could lose access to its own data.
- **Operational Complexity:** data exchange using public-key infrastructure is notoriously difficult to implement, requiring extensive user training and support commitments that large organizations cannot afford to take on.

These challenges leave many organizations with a difficult choice: limiting the amount of data they exchange, or accepting the risk that their data may be compromised and exploited by competitors, criminals, or other hostile groups.

EVERY ORGANIZATION NEEDS TO SHARE SENSITIVE INFORMATION WITH EXTERNAL COMPANIES AND INDIVIDUALS. AS DATA VOLUMES AND DATA TRAFFIC CONTINUE TO INCREASE, DATA EXCHANGE BECOMES A GREATER NECESSITY AND A GREATER RISK EACH YEAR.

SECURE DATA EXCHANGE WITH SMARTCRYPT

PKWARE's Smartcrypt solves the problem of secure data exchange. Smartcrypt detects and classifies sensitive data, and can apply persistent encryption on every enterprise operating system. Smartcrypt's automated key management technology allows administrators to control access to protected data even after files have traveled outside the organization's network, no matter how the data was shared.

Smartcrypt facilitates policy-based secure data exchange, without security gaps and without disrupting user workflows. Organizations can use Smartcrypt to protect data automatically whether data is shared via email, cloud, FTP, or other mechanisms.

With Smartcrypt, even the most sensitive information can be shared with vendors and partners without exposing data to unauthorized access. Encrypted files remain protected no matter how many times they are copied, moved, or shared.

PERSISTENT ENCRYPTION

Smartcrypt applies persistent strong encryption, the most effective form of data protection, before files are sent, shared, or copied. This prevents unauthorized users from accessing sensitive information no matter where files are located.

Unlike other forms of encryption, persistent encryption is applied to data itself, rather than to a storage location or transmission system. Information protected by persistent encryption remains secure throughout the entire data lifecycle, whether files are saved on servers, endpoint devices, removable storage, or in the cloud.

Data-Centric Protection

Data-centric security—security that protects data itself, rather than focusing on perimeter or device protection—is the best way to manage the risks associated with large volumes of sensitive data and increasingly complex IT environments.

Smartcrypt's automated data-centric security workflow provides the capabilities organizations need in order to take control of sensitive data and meet their information security goals.

- **Policy** is defined by administrators and applied to users, groups, or locations
- **Data Discovery** happens continuously as files are created or modified
- **Classification** indicates what data a file contains and how it should be handled
- **Encryption** keeps sensitive data safe from unauthorized access
- **Reporting** allows the organization to demonstrate compliance

Smartkey Technology

Smartkeys, PKWARE's innovative key management technology, can be used to manage access control at the folder or individual file level, even after a file has left the organization.

Smartkeys take the place of passphrases and public-key infrastructure, allowing organizations to implement a secure, manageable solution for data protection across the enterprise. With Smartkeys, an organization can ensure that its sensitive data is protected against theft or misuse, while eliminating the risk that the company will ever lose access to its own data.

Smartkeys use the strongest, most widely-accepted encryption algorithms available to encrypt sensitive data. They can be used to encrypt and decrypt data on user devices, file servers, and other locations, including cloud storage services.

Access to Smartkeys is determined by the organization's encryption policies and the user's role within the organization. Users may have access to several Smartkeys, and (depending on the organization's policies) may also have the ability to create and share new Smartkeys.

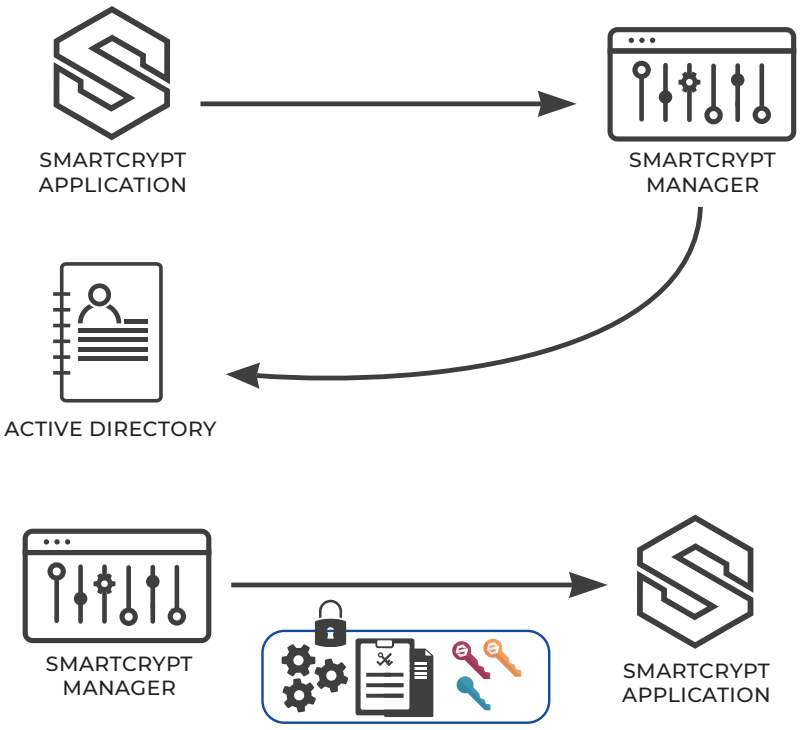
Smartcrypt also supports encryption and decryption using other key types, including traditional passphrases and OpenPGP or X.509 certificates.

SMARTKEY MANAGEMENT

1. After user logs in, Smartcrypt agent sends credentials to Smartcrypt Enterprise Manager (via TLS)

2. Smartcrypt Manager validates identity with Active Directory

3. After user authentication, Smartcrypt Manager delivers encrypted configuration, policy, and allowed Smartkeys

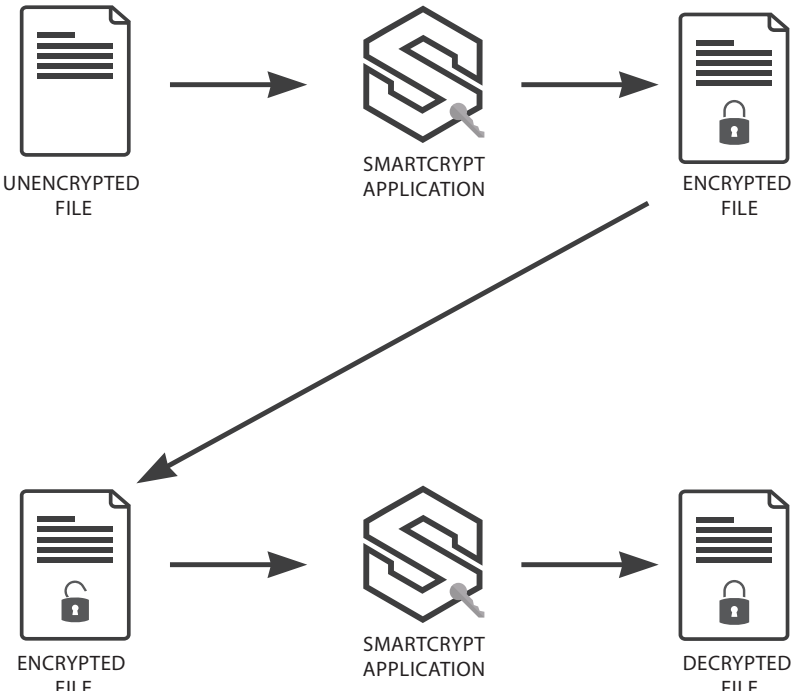


ENCRYPTION & DECRYPTION WITH SMARTKEYS

1. When a user creates or modifies a file containing sensitive information, the Smartcrypt agent encrypts the file according to organizational policy

2. Smartcrypt's persistent encryption travels with data when it is exchanged via email, cloud, ftp, or removable media

3. When a user receives an encrypted file, the Smartcrypt agent will decrypt the file only if the recipient is authorized to use the Smartkey that was used for encryption.



SECURE EXCHANGE: EMAIL

Email is an inherently insecure form of communication. Messages often pass through unsecured systems on the way from sender to recipient, creating multiple opportunities for sensitive data to be compromised in the process.

Even if a message remains safe while in transit, it remains vulnerable indefinitely. Messagess sent to an external recipient can be saved to an unsecure location, forwarded to unauthorized users, or otherwise mishandled at any time, without the knowledge of the organization that owns the data.

Smartcrypt provides persistent data-level encryption for email attachments as well as for the message text itself.

With Smartcrypt, organizations can ensure that documents, spreadsheets, and other sensitive files remain safe from unauthorized access, even when saved to a message recipient's computer or shared in the cloud. Organizations have several options for giving external users access to encrypted information (see "Options for External Recipients" below).

Smartcrypt Plugin for Outlook

The Smartcrypt Microsoft Outlook plugin allows users to encrypt and decrypt email messages and attachments without changing the way they work. Encryption keys are controlled by the Smartcrypt Enterprise Manager, ensuring that the organization always has access to its own data.

Automated email encryption

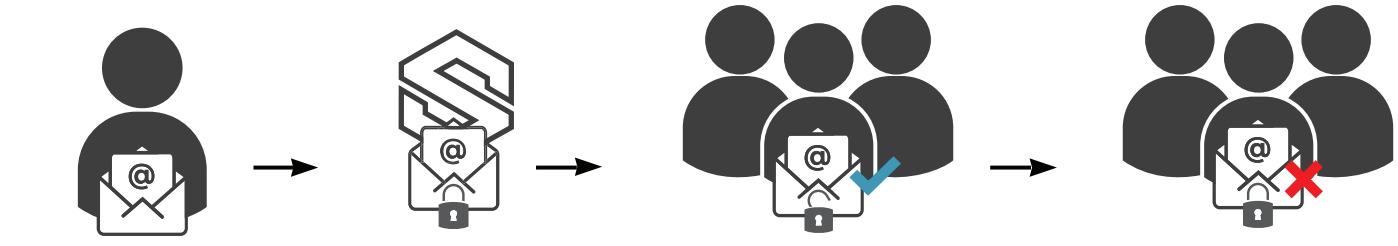
Smartcrypt provides an automated data protection workflow that secures email messages and attachments without disrupting the typical user experience.

Administrators use the Smartcrypt Enterprise Manager to define email encryption policies and apply them to the organization as a whole, or to specific users and groups. The Smartcrypt Outlook plugin then applies the appropriate policy on each user device.

Depending on the organization's needs, Smartcrypt can take a variety of actions when users send email through Outlook:

- Encrypting all outgoing messages with pre-defined encryption keys
- Encrypting only messages that contain sensitive information (as defined in the organization's data discovery policy)
- Encrypting message attachments, body text, or both
- Re-encrypting attachments that were previously encrypted with a different key

When a user receives an encrypted message that they are authorized to read (meaning that they have access to the Smartkey that was used to encrypt the message), the Outlook plugin automatically decrypts the message with no additional action by the user.



Smartcrypt Plugin for Outlook

Manual email encryption

As an alternative to the automated workflow, organizations can configure Smartcrypt to open an encryption dialog box before an email is sent. The dialog box allows users to choose from a variety of email encryption options:

- Encryption method: Smartcrypt can encrypt the message body, attachments, or both
- Encryption key: users can select from available Smartkeys or digital certificates, or create a passphrase for each outgoing message
- Encryption algorithm: available options include AES-256, AES-192, AE-2, and 3DES
- Re-encryption: decrypts attachments that were already encrypted, and re-encrypts them to ensure that authorized recipients will be able to access them
- Auto-search for recipients: automatically searches for Smartkeys or certificates for each of a message's recipients

The manual workflow simply allows users to choose which emails will be encrypted and which encryption keys will be used. The organization retains complete control over its encryption keys and can grant or revoke access to manually-encrypted email messages at any time.

DLP INTEGRATION

Encryption often makes data loss prevention (DLP) technology less effective, especially when the encryption is applied by end users without organizational control. When encrypted email messages or files are submitted for inspection, the encryption renders the data unreadable to DLP scanners.

Smartcrypt integrates with existing data loss prevention solutions, allowing DLP scanners to decrypt and inspect message contents before they leave the organization's network.

SECURE EXCHANGE: CLOUD

Cloud services have become one of the most popular mechanisms for exchanging data between organizations, and for facilitating collaboration between coworkers. However, cloud locations—unprotected by firewalls or other network safeguards—are easy targets for hackers who have stolen employee credentials. Files in the cloud are also vulnerable to unauthorized use by insiders with access to the cloud location, as well as attacks against the cloud provider itself.

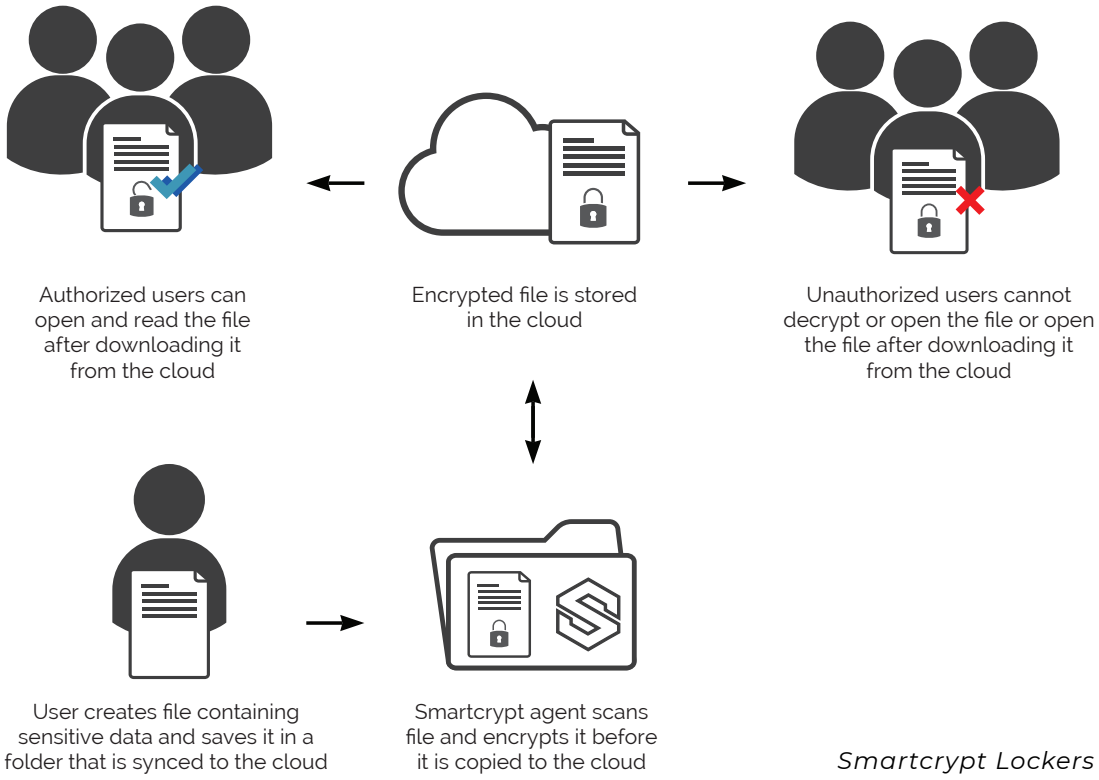
Personal cloud accounts represent an even greater risk. Many employees sync their work computers to their personal storage accounts, copying hundreds or thousands of files to locations that their employers cannot see or control.

Organizations can use Smartcrypt to ensure that files on servers and employee computers are encrypted before they are moved or synced to the cloud. Once in the cloud, encrypted files remain protected whether they are downloaded, copied, or shared through other means.

Smartcrypt Lockers

Using the Smartcrypt Enterprise Manager, administrators create "lockers," or protected locations, on file servers or user devices. When folders that are synced to the cloud are designated as lockers, Smartcrypt applies the organization's data protection policies to all files within the folders. Smartcrypt can be configured to encrypt all files in a locker, or only the files that contain sensitive data.

When employees or external users download encrypted files from the cloud, the encryption remains with the downloaded copies. Smartcrypt will automatically decrypt files for users who have access to the appropriate Smartkey (see



Smartcrypt Lockers

SECURE EXCHANGE: FTP

FTP remains one of the most common methods for data exchange at the enterprise level. While secure FTP provides some measure of protection for data in transit, the organization that owns the data cannot control what happens once files are downloaded by a partner, vendor, or customer.

Smartcrypt gives organizations the ability to encrypt files before an FTP upload, ensuring that only authorized users will be able to decrypt and access the data, even in the event that files are moved or shared inappropriately after download.

User-Initiated FTP

Depending on the organization's security policies, users may need to encrypt files manually before uploading them to FTP sites, or else upload files that have been encrypted automatically through Smartcrypt's data discovery feature.

To encrypt files manually, users can access Smartcrypt's encryption dialog by right-clicking on the file or by opening the Smartcrypt application. The encryption dialog gives users the same options that are available in the email encryption dialog, including key type, certificate selection, passphrase creation, and encryption algorithm.

After encrypting files, users can upload them to the destination FTP site. Only users who have been granted access to the encrypted files (see "Options for External Recipients" below) will be able to open them, even if unauthorized users are able to access the FTP directory.

Integrating Encryption With Existing FTP Processes

If an organization uses a standard FTP program to transfer files, the process can call Smartcrypt's command-line interface and initiate encryption before files are uploaded to an FTP server.

Building automated encryption into FTP workflows ensures that all files are protected according to the organization's security policies before being exposed to potential misuse after they are retrieved by external users.

OPTIONS FOR EXTERNAL RECIPIENTS

Smartcrypt provides two simple methods for allowing external users to access emails or files that have been encrypted by a Smartcrypt user: guest accounts and the free Smartcrypt Reader.

Guest accounts are an ideal solution when an organization needs to share sensitive data with certain external users on an ongoing basis. For short-term needs or less frequent data sharing, the free Smartcrypt Reader allows any external user to decrypt data they are authorized to access.

Guest Accounts

Organizations can extend their Smartcrypt implementation to users at external organizations by creating guest accounts. A guest account allows a user to encrypt and decrypt files and email messages using the Smartcrypt Outlook plugin just like an organization's internal users.

To create a guest account, an organization simply adds the external user in Active Directory, grants the appropriate permission using the Smartcrypt Enterprise Manager, and provides a Smartcrypt license for use on the external user's laptop, desktop, or mobile device.

Smartcrypt Reader

The Smartcrypt Reader is a free, no-install app that allows anyone to decrypt files, provided that they have been granted access to the appropriate Smartkey or other encryption key.

To access an encrypted file or email, the external recipient simply downloads the Smartcrypt Reader and registers using the app's simple interface. After verifying their credentials, users can open files and email messages with just a few clicks

SMARTCRYPT AND OPEN PGP

Organizations that use OpenPGP to share sensitive data with external users can integrate their PGP implementations with Smartcrypt's automated data protection workflow.

When encrypting email messages or files with OpenPGP, administrators or users simply indicate the location of OpenPGP digital certificates and configure Smartcrypt to perform encryption and decryption using those certificates.

Smartcrypt supports a variety of OpenPGP algorithms:

- AES: The standard algorithm adopted for use in government, banking, and other high-security environments.
- 3DES: A stronger, updated variant of the older DES algorithm.
- TCAST5: The default algorithm for many popular OpenPGP clients.
- IDEA: An optional algorithm used in some older OpenPGP clients.

Encrypting With Multiple OpenPGP Keys

Users can enable both passphrase and key-based encryption to expand the list of recipients who can access and encrypted file. In this case, encrypted files can be decrypted by anyone who either has the passphrase or whose private OpenPGP key matches the certificate used in the encryption process.

Recipients without matching keys will need to enter the passphrase in order to decrypt the file, while recipients with matching keys will not.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

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