SMARTCRYPT

PKWARE NEXT GENERATION ENCRYPTION AND KEY MANAGEMENT

Smartcrypt Application と Manager

次世代の暗号化と鍵管理

セキュリティー対策にかかる費用は年々高くなっています。外部からのセキュリティーの脅威はますます高度化し、予測不可能です。内部統制もより複雑になり実装が難しくなってきています。情報漏えいが生じた場合、売上や企業イメージに与える影響は膨大で、信頼の回復に何年もかかることでしょう。

世界中のセキュリティー管理者は、今やネットワークやデバイスの暗号化による保護だけでは十分でないことを認識しています。真の情報セキュリティーは、セキュリティー上の不正アクセスがあっても、情報にはアクセス不可能な状態で、永続的なデータレベルの暗号化による保護が必要です。

従来、組織ではデータレベルの暗号化による保護を実装する際に、次の二つのアプローチを採用してきました：パスワードベースか公開鍵暗号化方式 (PKI)。それぞれのアプローチには欠点があります。

パスワードベースの暗号化は、より一般的なアプローチですが、パスワードを作成し、保存し、交換して、暗号化したデータのセキュリティーを維持し続けるのは非常に困難です。公開鍵暗号化方式は、より強度な暗号化による保護を提供しますが、使い勝手の面で問題があり、鍵管理の方法を実装するのが困難な問題があります。モバイル テクノロジーやクラウド ベースのサービスの普及によって、公開鍵暗号化方式の採用は使い勝手の面で既に下降気味になっています。

PKWARE の Smartcrypt は、エンタープライズ向けのセキュリティー管理にとって、画期的なソリューションです。Smartcrypt のソリューションは、公開鍵暗号化方式の強度と信頼性、パスワードベースの暗号化の使いやすさとシンプルさの両方を組み合わせ、組織で暗号化して保護したデータを完全にコントロールできます。

Smartcrypt は、エンドユーザー向けのアプリケーションと Web ベースの管理コンソールを提供します。Smartcrypt のプラットフォームには、SDK (ソフトウェア開発キット) も含まれ、主要なプログラミング言語で利用可能です。

APPLICATION の特長

- すべての主要なエンタープライズ向けの OS で利用可能なクロスプラットフォーム対応
- 既存の PGP、X.509 公開鍵とシームレスに統合
- ハードウェアの暗号化アクセラレーターを使用して、より高速な暗号化処理を実現
- PKWARE の業界最高レベルの圧縮技術と強度な暗号化を組み合わせることで、必要なストレージ容量やネットワーク帯域幅を大幅に削減
- オプションの Smartcrypt Cloud への統合機能で、社外のお客様やパートナーと安全なデータ交換が可能

Smartcrypt Application:
永続的なデータ暗号化による保護と使いやすさ

データを暗号化する、暗号化したデータを保存する、アクセスするすべてのデバイスに Smartcrypt Application をインストールします。さまざまなプラットフォーム独自のユーザーインターフェースを提供し、Smartcrypt Application はさまざまな暗号化システム、鍵タイプ、鍵インターフェースをサポートします。Smartcrypt はまた、最も煩わしい鍵管理を簡素化し自動化する組込み鍵管理ソリューションである Smartkeys を提供します。

Smartcrypt Application でデータを暗号化すると、データを使用、共有および保存するすべての場所で、データを永続的に暗号化して安全に保護できます。Application は、自動的に鍵を作成し、同期化し、交換し、許可された人のみがデータにアクセスできるようにします。

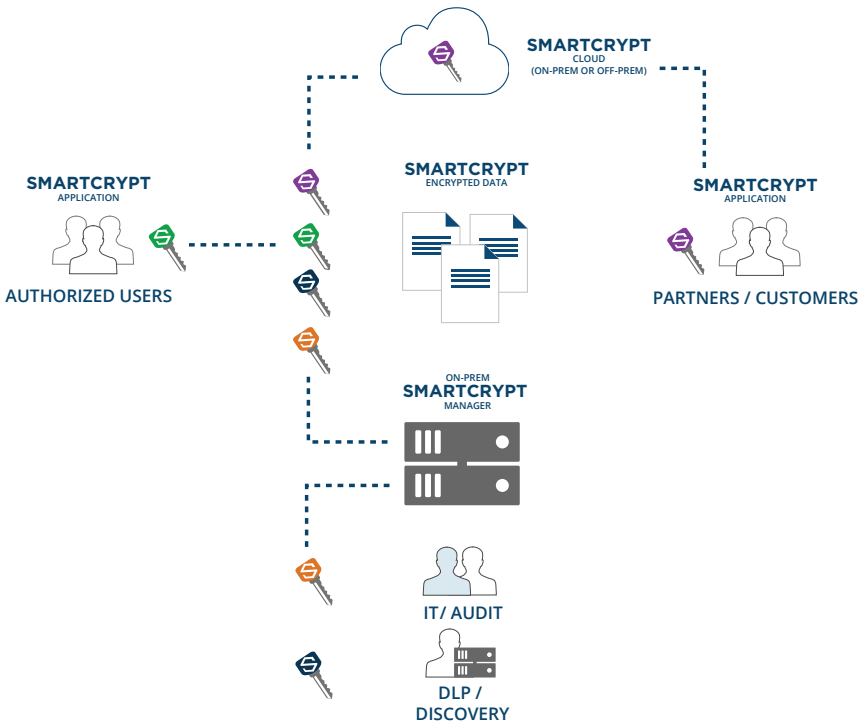
Smartcrypt Manager: エンタープライズ レベルでの管理

Smartcrypt Manager Console は、鍵の集中管理とポリシー管理機能を提供します。Web ベースの管理コンソールには、構成、ポリシー、許可 / 拒否管理など、きめ細かいコンソールが含まれます。Smartcrypt の Data Security Intelligence は、どのファイルが暗号化されているか、どのユーザーがアクセスしたか、どこでイベントが発生したかなど、完全に可視化する機能を提供します。

監査員、IT 管理者、DLP スキャナーが暗号化したデータをレビューする際に、Smartcrypt のポリシー キーが信頼できるアクセスを提供します。すべての暗号化操作には複数の公開鍵を含むようにソリューションを構成可能なので、組織はデータへアクセスできなくなるという問題は起きません。ユーザーは Smartkey を使用するか、サードパーティーが生成した鍵 (X.509 または PGP 形式) を使用するか選択できます。

MANAGER CONSOLE の特長

- Microsoft Active Directory と統合し、シームレスなユーザーインターフェースを提供します。
- 管理者は暗号化したデータへのアクセスを簡単に許可、拒否、期限切れにすることができます。
- ポリシー グループによって、再暗号化の必要性なしに、コンテンツへのアクセスを再度復活できます。
- Data Security Intelligence を使用して、コンソールで直接レポートでき、また SIEM エージェントまたは API を使用して検索もできます。



Smartkeys

Smartcrypt Application と Management Console のコアは、PKWARE の革新的な Smartkey テクノロジーです。Smartkeys を使用して、組織はファイルを復号化し、データを読むユーザーのコントロールが可能です。

Smartkey は、特定のファイル、フォルダー、または他の暗号化して保護した資産に対して、Smartcrypt Application で生成されたユニークな鍵です。
Smartkeys を使用して、いつでもユーザー アクセスを追加したり削除したりできます — ファイルを共有、コピー、名前の変更、転送または Email した場合でもファイルのライフサイクル全体を暗号化して保護します。

ユーザー ワークフローの変更や割り込みなどせずに、許可したデバイス間で Smartkeys を自動的に生成、共有、および同期化します。

Smartcrypt を使用して、ユーザーは社外の組織 (ベンダーやパートナーなど) と暗号化したデータのやり取りも可能です。暗号化した後にアクセス権限を付与した社外のユーザーに対しても、クラウド ベースの鍵サーバーには、組織のセキュリティー ポリシーに基づいた鍵を保存し配布します。

データの暗号化による保護に加え、各 Smartkey 自体をポリシーベースのアクセス リストに基づいて、暗号化し、交換します。この革新的なアプローチによって、セキュリティー マネージャーは、暗号化して保護したデバイスを紛失した場合、個人やグループからアクセスを拒否する場合など、素早い対応ができます。単純に Smartkey で暗号化を変更するだけで、管理者は、大量のデータを再度暗号化することなく、不正なアクセスをブロックできます。

Smartcrypt の利点

安全なデータ交換

Smartcrypt は、社外のパートナーや顧客とファイルを交換する前にファイルを永続的に暗号化します。これによって、組織は、何回でも情報をコピーしたり、バックアップを取ったり、転送しても情報に対するコントロールを維持できます。このアプローチを使用して、セキュリティーの強度が低い Email や FTP などのプロトコルやクラウド サービスを使用しても、機密情報を安全にやり取りできます。

コンプライアンスに準拠

金融機関、医療機関、政府機関のコンプライアンスの標準は、データは保存する際も移動する際も暗号化して保護されている必要があります。Smartcrypt は、義務付けられた職務分離、社内の脅威からの保護、DLP プロセスとの統合を提供します。Manager Console は、機密情報を転送およびアクセスする場所を可視化する機能も提供します。

クロスプラットフォーム対応

メインフレームからモバイルまで、Smartcrypt はクロスプラットフォームの完全な暗号化を提供します。Office や Outlook などの一般的なアプリケーションとの統合で、Smartcrypt を使用して、エンドユーザーのデバイス、ネットワーク共有、ファイル共有サービスでさえ、保存した情報を暗号化して保護します。Smartcrypt はまた back-office や batch 処理などのワークフローにも簡単に統合できます。

拡張 DLP

組織では、DLP 技術と処理を実装する柔軟なデータ セキュリティー ソリューションが必要です。Smartcrypt を既存の DLP 戦略と統合して、機密情報を検出したり、暗号化を復活したりできます。

SMARTCRYPT

PKWARE NEXT GENERATION ENCRYPTION AND KEY MANAGEMENT

エンタープライズ向けのクロスプラットフォーム対応

- IBM z/OS, IBM i, IBM AIX, Oracle Solaris, HP-UX, Linux, Windows, Mac, iOS および Android を含むすべてのエンタープライズ向けの OS で End-to-end の暗号化アプリケーションを利用可能

組込み鍵管理 (Smartkeys)

- 自動公開鍵 / 秘密鍵生成、同期化、交換
- 外部のパートナーとの鍵の交換と管理
- 従業員が組織を去った後もデータのコントロールを維持
- 再暗号化なしでデータへのアクセスを変更
- エンタープライズ IT、監査、DLP 担当と技術へ鍵を配布

高度なプラットフォーム コントロール

- Smartcrypt Manager は可視化、ポリシー、コントロール、検出を提供
- アクセスを簡単に無効にし、自動的に期限切れ

ハイパフォーマンス

- IBM と Intel ハードウェア暗号化アクセラレーターを利用
- 暗号化する前に最大 95% データを圧縮するので、ストレージの容量やネットワークの帯域幅を大幅に削減

既存の PKI をサポート

- OpenPGP 暗号化および鍵形式をサポート
- X.509 証明書ベースの暗号化をサポート
- パスワードベースの暗号化をサポート

技術仕様

OS :

- Microsoft Windows
- Linux: RHEL (.rpm) および SLES (.deb)
- UNIX: Oracle Solaris (Sparc and x86), IBM AIX および HP-UX
- IBM z/OS, IBM i, and Linux for Z Systems
- Apple Mac OS X および iOS
- Google Android

アルゴリズム :

- 暗号化 : 3DES, AES128, AES192, AES256, CAST5, IDEA, AE-x
- 署名 : SHA-1, SHA-256, SHA-384, SHA-512
- 厳密なチェックと失効ステータスの確認 (オプション)

鍵の保存と取得 :

- ハードウェア : PIV / CAC を含む KMIP HSM, Smartcards
- ソフトウェア : PKCS#11, LDAP, KMIP, CAPI/CNG, Keychain, Keystore, ICSF-CKDS, PKDS, Security Server, RACF, ACF2, Top Secret

証明書ベースのファイル暗号化と鍵タイプ :

- Smartkeys
- X.509 Digital Certificates
- OpenPGP

PKWARE について

PKWARE, Inc. は ZIP 標準の発案者で、かつイノベーターとして継続的な地位を確立しており、データ セントリック、クロスプラットフォームのデータ セキュリティと圧縮ソフトウェア製品を提供するグローバル市場およびテクノロジーのリーディング カンパニーです。SecureZIP および PKZIP 製品群は 30,000 社以上の企業と 200 以上の官公庁への導入実績を持ち、組織内および組織外のパートナーとデータ セキュリティ、可搬性、クロスプラットフォームのデータ交換の確保に使用されています。PKWARE 製品は、金融サービス、銀行、小売、ヘルスケア、官公庁、製造業の各分野で、他社製品にはないスケーラビリティ、使いやすさ、そして迅速な導入が評価され、広く導入されています。PKWARE は、ウィスコンシン州ミルウォーキーに本拠を置き、ニューヨーク、イギリスなどに拠点を構える株式非公開の会社です。

XLSOFT エクセルソフト株式会社

〒108-0073
東京都港区三田 3 丁目 9 番 9 号 森伝ビル 6 階
Tel: 03-5440-7875
Fax: 03-5440-7876
Email: xlsoftkk@xlsoft.com
www.xlsoft.com

XLsoft のロゴ、XLsoft は XLsoft Corporation の商標です。※このカタログに記載されている内容・仕様は予告無しに変更する場合がありますので、予めご了承ください。
Copyright © 2016 PKWARE, Inc. and its licensors, All rights reserved. PKWARE、SecureZIP、PKZIP は PKWARE, Inc. の登録商標です。本紙に記載されているその他の企業の登録商標および商標は、それらの所有者を明確にする目的でのみ記載されており、各々の所有者に所有権が属しています。