Alibaba Cloud KeyManagementService

プロダクト紹介

Document Version20190704

目次

1 概要

Key Management Service (KMS) は、Alibaba クラウドが提供する安全で使いやすい管理サービスです。 KMS により、キーの機密性、整合性、および可用性を保護に多大な労力を費やすことなく、キーを安全かつ便利に使用し、暗号化および復号化機能の開発に集中できます。

シナリオ

役割	要求	KMS ソリューション
アプリケーション / web サイト開発者	開発者はプログラムにおいて暗号化や署名のためのキーや証明書が必要です。また安全で独立したキー管理を求めています。 アプリケーションがどこにデプロイされていても、安全にキーにアクセス仕組みが必要です。 当然、非常に危険なため、どこにでも平文のキーをデプロイすることはありません。	エンベロープ暗号化テクノロジを使用すると、カスタマーマスターキー (CMK) を KMS に格納し、暗号化されたデータキーのみをデプロイできます。 必要に応じて KMS を呼び出し、データキーを復号化するだけです。
サービス開発者	暗号鍵の管理は、SaaS サービス提供者としては堅実は仕組みを提供しつつ、 責任分担としてはユーザーの範囲としたく考えています。 特定のキーを使用し、その認証でデータを暗号化します。 このようにして、私はサービス機能の開発に集中することができます。	エンベロープ暗号化テクノロジと KMS API に基づいて、サービス開発者は指定された CMK を使用しデータキーを暗号化および復号化することができるため、平文は直接ストレージデバイスに格納されません。 これにより、サービス開発者がユーザーのキーを管理する方法について心配する必要がなくなります。
セキュリティ最高責任者 (CSO)	自社内における暗号鍵の管理運用が、コンプライアンス要件を満たしている必要があります。 暗号鍵の権限設定と、暗号鍵の使用履歴の監査が可能であることも必要です。	KMS を RAM と関連付けて、統合された権限管理を行うことができます。

2 利点

利点	従来のキー管理ソリューション	KMS
コスト効率	安全な物理的環境を構築するために安全なキー管理機器を購入すると、ハードウェアコストが高くなります。 安全なキー管理仕様を設計と実行をするには、ソフトウェアコストが高くなります。	KMS を使えば、支出は必要なものに対してのみであるため、価格は低くなります。
使いやすさ	ハードウェア機器のAPIには標準がないため、使いにくくなっています。 通信チャネルセキュリティのソリューションおよび構成は煩雑です。	統合された、使いやすい API を有し 標準の HTTPS プロトコルを備えています。
信頼性	一般的に、高い信頼性を保証するにはオフラインバックアップソリューションを使用する必要があります。	KMS は、分散システムと暗号化ハードウェアを組み合わせて高い信頼性を実現します。

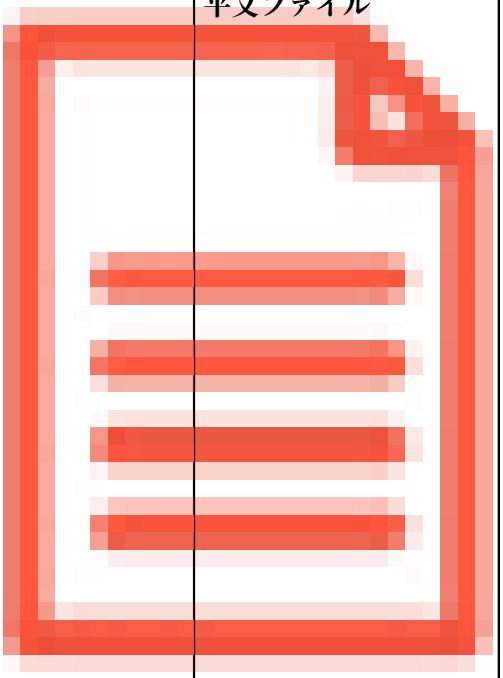
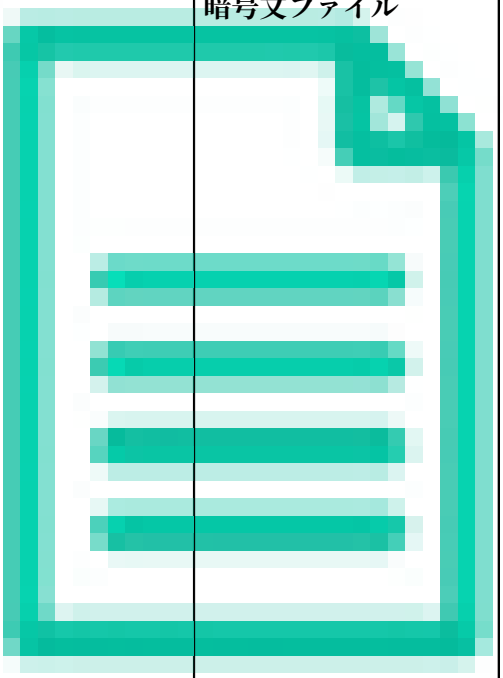
3 シナリオ

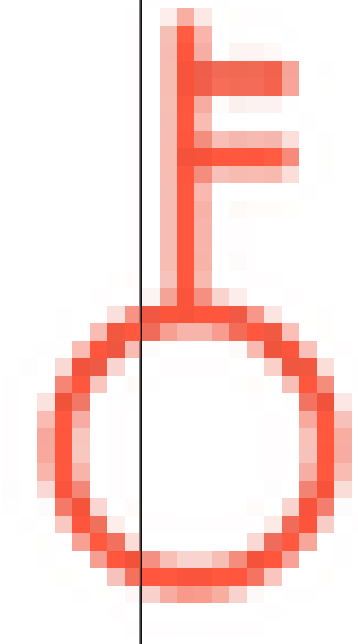
KMS の一般的な使い方:

- CMK を使用してデータを暗号化および復号化します。
- エンベロープ暗号化を使用して、データをローカルで暗号化および復号化します。

表 3-1 : 例

例	意味	例	意味
	CMK		暗号文キー

例	意味	例	意味
	平文証明書		平文ファイル
	暗号文証明書		暗号文ファイル

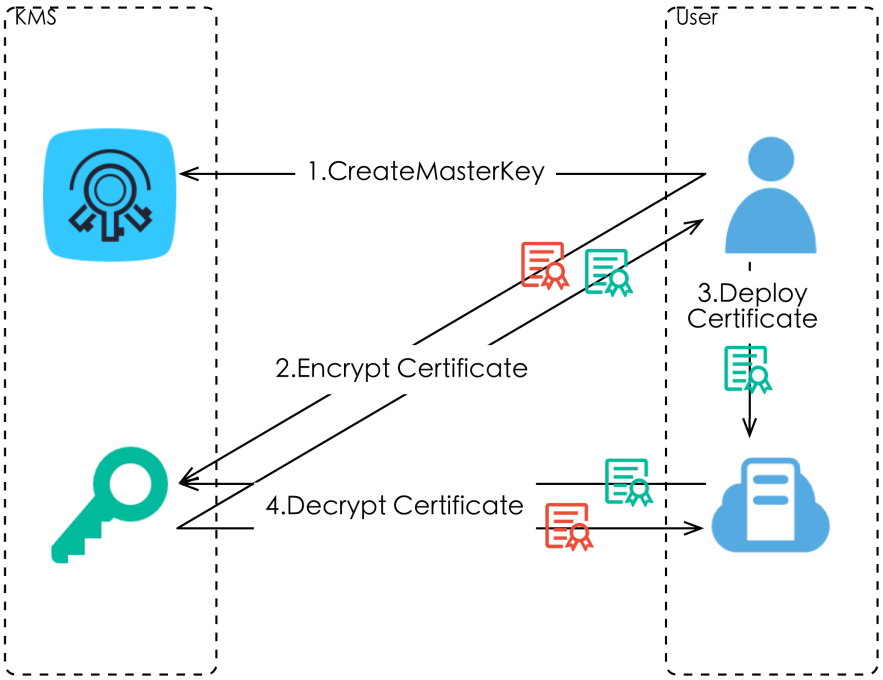
例	意味	例	意味
	平文キー 		

Customer Master Key (CMK) を使用してデータを暗号化および復号化

CMK を使用して少量のデータ (4 KBより小さい) を暗号化および復号化することができます。ユーザーデータは、セキュリティで保護されたチャネル経由で KMS サーバーに渡され、KMS

サーバーはデータの暗号化と復号化を行い、操作結果をセキュリティで保護されたチャネル経由でユーザーに送信します。

図 3-1 : 利用イメージ: サーバーの HTTPS 証明書の暗号化および復号化



手順：

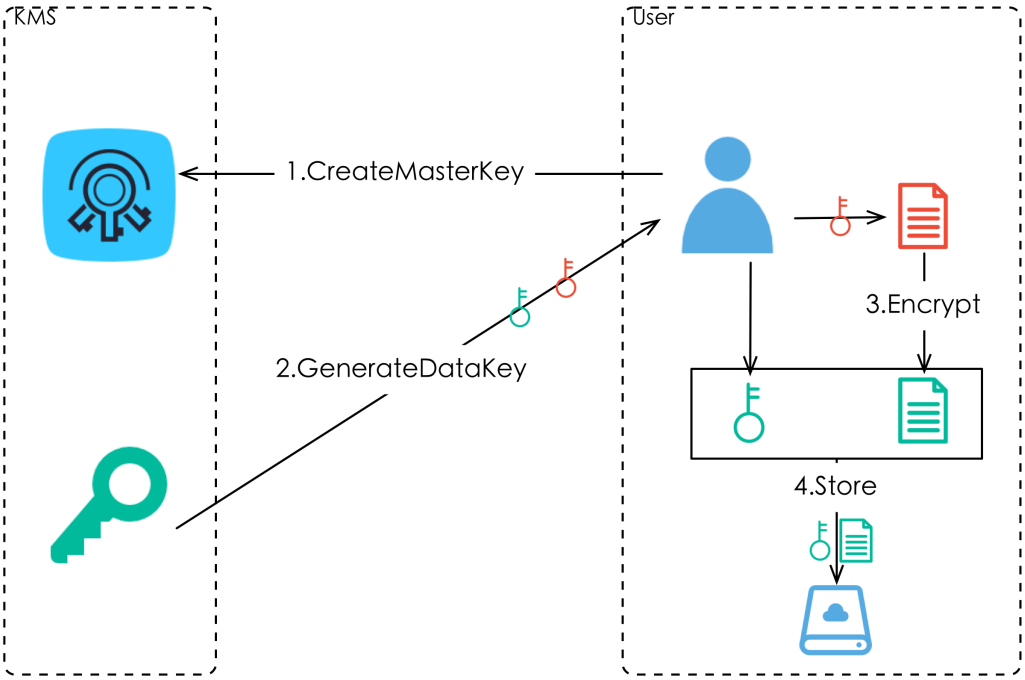
1. CMK を作成するには、KMS コンソールにログインするか、CreateKeyを呼び出す必要があります。
2. Encrypt平文証明書を暗号化するために呼び出します。
3. 暗号化された証明書をサーバーにデプロイします。
4. Decrypt認証のために暗号化された証明書を復号化するために呼び出します。

エンベロープ暗号化を使用して、データをローカルで暗号化および復号化

KMS を使用して CMK を作成し、CMKを使用してデータキーを生成できます。データキーは、大量のデータをローカルで暗号化および復号化するための暗号化キーとして使用されます。 この

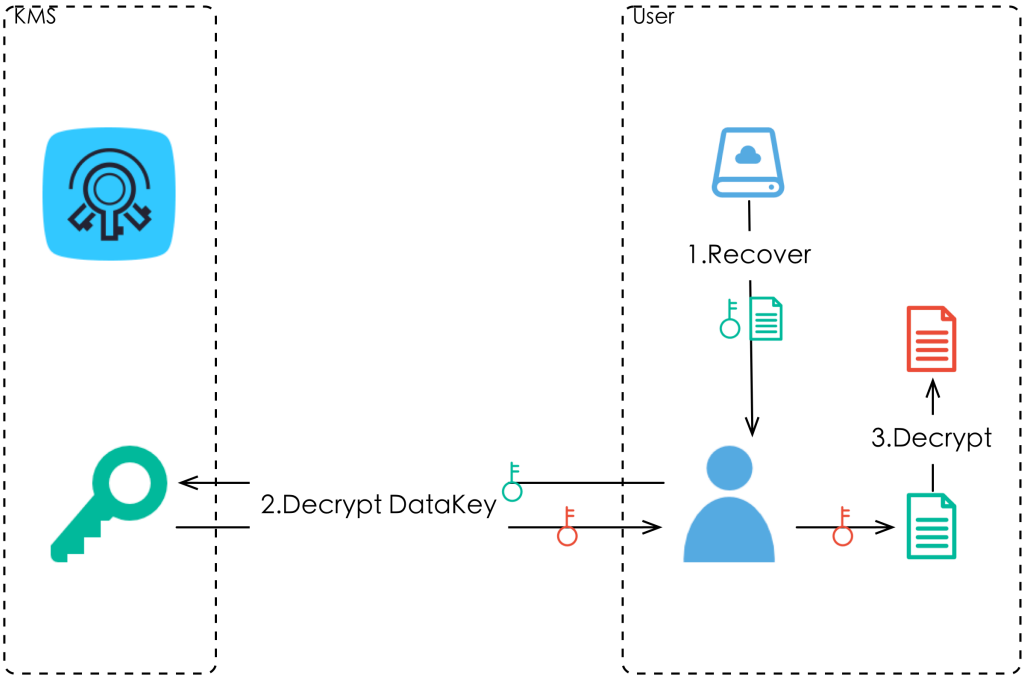
ようにして、暗号化と復号化のためにネットワーク経由でデータを送信するコストが節約されます。

図 3-2 : 利用イメージ: ローカルファイルの暗号化



手順：

1. CMK を作成するには、 KMS コンソールにログインするか、CreateKeyを呼び出す必要があります。
2. GenerateDataKeyデータキーを生成するために呼び出します。 平文データキーと暗号化データキーを返します。
3. 平文データキーを使用してファイルをローカルで暗号化し、その後平文データキーをメモリから消去します。
4. ローカルに暗号化されたデータとともに暗号化データキーを格納します。
5. ローカルにデータを復号化します
   - Decryptを呼び出して、暗号化データキーを平文データキーに復号化します。
   - 平文データキーを使用してデータをローカルで復号化し、その後平文データキーをメモリから消去します。


KMS
User
1.Recover
2.Decrypt DataKey
3.Decrypt

4 履歴

リリース日	バージョン	内容
04/06/2016	1.0	KMS OBT
05/19/2016	1.1	3 リージョンのサポート追加: 中国 (北京)、中国 (上海)、中国 (深セン)。
06/22/2016	1.2	キーの有効化および無効化をサポート。
08/10/2016	1.3	バグ修正により性能を最適化。 EncryptionContext で暗号化および復号化 API をサポート。
09/20/2016	1.4	新しいキーを追加し性能を最適化。 キーを削除する 2 つのAPI を追加: ScheduleKeyDeletion および CancelKeyDeletion.
11/02/2016	1.5	性能の最適化。4 リージョンのサポート追加: 日本 (東京)、オーストラリア (シドニー)、ドイツ (フランクフルト)、UAE (ドバイ)。
01/22/2017	1.6	性能の最適化。1 リージョンのサポート追加: 中国 (香港)。
03/01/2017	1.7	性能の最適化。
05/10/2017	1.8	性能の最適化。1 リージョンのサポート追加: 中国 (張家口)。
06/05/2017	1.9	新しい API: DescribeRegions。SDK を 2.4.0 へ更新。
11/15/2017	1.10	性能の最適化。3 リージョンのサポート追加: 中国 (青島)、中国 (フフホト)、マレーシア (クアラルンプール)。

リリース日	バージョン	内容
03/30/2018	1.11	BYOK (独自のキーを使用) 用の新しい API、エイリアス用の新しいAPI、および 4 リージョンのサポート追加: 米国 (バージニア)、米国 (シリコンバレー)、インド (ムンバイ)、インドネシア (ジャカルタ)。

5 用語集

次の用語は、KMS の主要な概念です。

用語	フルネーム	定義
KMS	Key Management Service	Alibaba クラウドキー管理サービス
Envelope encryption	エンベロープ暗号化	エンベロープ暗号化は、一意のデータキーを使用して平文データを暗号化し、キー暗号化キー (EDK) を使用してデータキーを暗号化する方法です。 EDK を別の EDK で暗号化するように選択することもできますが、最終的にはマスターキーを持っている必要があります。 マスターキーは、暗号化されていない (平文) キーで、他の 1 つ以上のキーを復号化できます。
CMK	Customer Master Key (CMK)	CMK は Alibaba クラウド KMSを使用して生成されたマスターキーです。 データキーを暗号化してエンベロープ暗号化を生成できます。 少量のデータも暗号化できます。
EDK/DK	Enveloped Data Key/Data Key	DK はデータを暗号化するための平文キーで、EDK はエンベロープ暗号化を使用して DK を暗号化するためのキーです。