# Data Encryption Workshop

# Getting Started

**Issue** 01

**Date** 2023-07-14

HUAWEI

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

# Contents

# 1 Getting Started with Common Practices

After completing basic operations such as creating keys, key pairs, and secrets, you can get started with common Data Encryption Workshop (DEW) practices as needed.

**Table 1-1** Common practices

| Practice | | Description |
| --- | --- | --- |
| Data protection | **Encrypting and Decrypting Small Amounts of Data** | You can use online tools on the Key Management Service (KMS) console or call the necessary KMS APIs to directly encrypt or decrypt small-size data with a Customer Master Key (CMK), such as passwords, certificates, or phone numbers. |
| | **Encrypting and Decrypting Large Amounts of Data** | If you want to encrypt or decrypt large volumes of data, such as pictures, videos, and database files, you can use envelope encryption, which allows you to encrypt and decrypt files without having to transfer a large amount of data over the network. |
| | **Using the Encryption SDK to Encrypt and Decrypt Local Files** | Encryption Software Development Kit (SDK) can encrypt and decrypt data and file streams. You can easily encrypt and decrypt massive amounts of data simply by calling APIs. If large files and images are sent to KMS through HTTPS for encryption, a large number of network resources will be consumed and the encryption will be slow. You can use the encryption SDK to encrypt and decrypt local files. |
| | **Encrypting and Decrypting Data Through Cross-region DR** | If a fault occurs during encryption or decryption in a region, you can use KMS to implement cross-region DR encryption and decryption, ensuring service continuity. |

  

| Practice | | Description |
| --- | --- | --- |
| Cloud services use KMS for encryption | **Encryption in ECS** | KMS supports one-click encryption for Elastic Cloud Server (ECS). The images and data disks of ECS can be encrypted.<br>• When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, with its encryption mode same as the image encryption mode.<br>• When creating an ECS, you can encrypt added data disks. |
| | **Encryption in OBS** | When you enable server-side encryption in Object Storage Service (OBS):<br>• An object uploaded to OBS is encrypted on the server before being stored.<br>• When the object is downloaded, data is decrypted on the server first.<br>Server-side encryption with KMS-managed keys (SSE-KMS) can be implemented for the objects to be uploaded. |
| | **Encryption in EVS** | In case your services require encryption for the data stored on disks, KMS is integrated with Elastic Volume Service (EVS). You can use the key provided by KMS to encrypt the disk. |
| | **Encryption in IMS** | When creating a private image, you can select KMS encryption and use the key provided by KMS to encrypt the image, ensuring image data security. |
| | **Encrypting an RDS Database** | After encryption is enabled, disk data will be encrypted and stored on the server when you create a Relational Database Service (RDS) database instance or expand disk capacity. When you download encrypted objects, the encrypted data will be decrypted on the server and displayed in plaintext. |
| | **Encrypting a DDS Database** | After encryption is enabled, disk data will be encrypted and stored on the server when you create a Document Database Service (DDS) database instance or expand disk capacity. When you download encrypted objects, the encrypted data will be decrypted on the server first. |

  

| Practice | | Description |
| --- | --- | --- |
| Secret encryption | **Using CSMS to Change Hard-coded Database Account Passwords** | Generally, the secrets used for access are embedded in applications. To update a secret, you need to create a new secret and spend time updating your applications. CSMS is required to manage credentials more conveniently, efficiently, and securely. |
| | **Using CSMS to Prevent AK and SK Leakage** | You can use Identity and Access Management (IAM) to obtain temporary access keys for ECS to protect AKs and SKs. |
| | **Rotating a Secret for a User** | You can update the information of a user in a secret. This is the most commonly used secret rotation policy. |
| | **Rotating a Secret for Two Users** | You can update the information of two users in a secret. To prevent access failures when changing the user password and updating the secret content, use the multi-user secret rotation policy to ensure high availability of applications. |
| API calling | **Retrying Failed DEW Requests by Using Exponential Backoff** | If you receive an error message when calling an API, you can use exponential backoff to retry the request. |

  

# A Change History

| Released On | Description |
| --- | --- |
| 2023-07-14 | This issue is the first official release. |

  