

# Data Encryption Workshop

## Service Overview

**Issue** 02  
**Date** 2023-01-30



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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.

---

# Contents

---

<b>1 What Is DEW?</b>	<b>1</b>
<b>2 KMS</b>	<b>5</b>
2.1 Functions	5
2.2 Product Advantages	6
2.3 Application Scenarios	7
2.4 Using KMS	10
2.5 Cloud Services with KMS Integrated	12
2.5.1 Encrypting Data in OBS	12
2.5.2 Encrypting Data in EVS	13
2.5.3 Encrypting Data in IMS	14
2.5.4 Encrypting Data in RDS	14
<b>3 CSMS</b>	<b>16</b>
3.1 Functions	16
3.2 Product Advantages	17
3.3 Application Scenarios	18
<b>4 KPS</b>	<b>19</b>
4.1 Functions	19
4.2 Product Advantages	20
4.3 Application Scenarios	20
<b>5 Dedicated HSM</b>	<b>21</b>
5.1 Illustration of Dedicated Encryption Workshop	22
5.2 Functions	24
5.3 Product Advantages	24
5.4 Application Scenarios	25
5.5 Editions	26
<b>6 Billing Description</b>	<b>28</b>
<b>7 DEW Permission Management</b>	<b>31</b>
<b>8 How to Access</b>	<b>36</b>
<b>9 Related Services</b>	<b>37</b>
<b>10 Personal Data Protection Mechanism</b>	<b>41</b>

---

**A Change History..... 42**

# 1 What Is DEW?

## DEW

Data is the core asset of an enterprise. Each enterprise has its core sensitive data, which needs to be encrypted and protected from breach.

Data Encryption Workshop (DEW) is a cloud data encryption service. It consists of the following services: Key Management Service (KMS), Cloud Secret Management Service (CSMS), Key Pair Service (KPS), and Dedicated Hardware Security Module (Dedicated HSM). It helps you secure your data and keys, simplifying key management. DEW uses HSMs to protect the security of your keys, and can be integrated with other Huawei Cloud services to address data security, key security, and key management issues. Additionally, DEW enables you to develop customized encryption applications.

**Figure 1-1** DEW subservices



**Table 1-1** Service overview

Service	Description	Reference
Key Management Service (KMS)	<p>KMS is a secure, reliable, and easy-to-use service for managing your keys on the cloud. It helps you easily create, manage, and protect keys.</p> <p>KMS uses Hardware Security Modules (HSMs) to protect keys, helping you create and control customer master keys (CMKs) with ease. All CMKs are protected by root keys in HSMs to avoid key leakage.</p>	<a href="#">Key Types</a>
Cloud Secret Management Service (CSMS)	<p>CSMS is a secure, reliable, and easy-to-use secret hosting service.</p> <p>Users or applications can use CSMS to create, retrieve, update, and delete credentials in a unified manner throughout the credential lifecycle. CSMS can help you eliminate risks incurred by hardcoding, plaintext configuration, and permission abuse.</p>	<a href="#">Creating a Secret</a>
Key Pair Service (KPS)	<p>KPS is a secure, reliable, and easy-to-use cloud service designed to manage and protect your SSH key pairs (key pairs for short).</p> <p>KPS uses HSMs to generate true random numbers which are then used to produce key pairs. In addition, it adopts a complete and reliable key pair management solution to help users create, import, and manage key pairs with ease. The public key of a generated key pair is stored in KPS while the private key can be downloaded and saved separately, which ensures the privacy and security of the key pair.</p>	<a href="#">Creating a Key Pair</a>
Dedicated Hardware Security Module (Dedicated HSM)	<p>Dedicated HSM enables data encryption on the cloud, specifically, encrypting and decrypting data, verifying signature, generating keys, and storing keys.</p> <p>Dedicated HSM provides encryption hardware, guaranteeing data security and integrity on Elastic Cloud Servers (ECSs) and meeting compliance requirements. Dedicated HSM offers you a secure and reliable management for the keys generated by your instances, and uses multiple algorithms for data encryption and decryption.</p>	<a href="#">Dedicated HSM</a>

## Concepts

This section describes the basic concepts in DEW.

**Table 1-2** Basic concepts

Item	Definition	Reference
Hardware Security Module (HSM)	An HSM is a type of computer hardware that protects and manages the keys used by strong authentication systems and provides related cryptographic operations.	-
Customer Master Key (CMK)	A CMK is a Key Encryption Key (KEK) created by a user or cloud service using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or more DEKs.  CMKs are categorized into custom keys and default keys.	<a href="#">What Is a Customer Master Key?</a>
Default Master Key (DMK)	A Default Master Key is automatically created by another cloud service using KMS, such as Object Storage Service (OBS). The alias of a Default Master Key ends with <b>/default</b> .	<a href="#">What Is a Default Master Key?</a>
Key material	Key materials are important input for cryptographic operations. A CMK consists of a key ID, metadata, and a key material.	-
Envelope encryption	Envelope encryption is the practice of encrypting data with a DEK and then encrypting the DEK with a root key that you can fully manage. In this case, CMKs are not required for encryption or decryption.	<a href="#">What Are the Benefits of Envelope Encryption?</a>
Data Encryption Key (DEK)	A DEK is used to encrypt data.	<a href="#">What Is a Data Encryption Key?</a>

Item	Definition	Reference
Symmetric key encryption	<p>Symmetric key encryption is also called dedicated key encryption. The sender and receiver use the same key to encrypt and decrypt data.</p> <p>Advantage: Encryption and decryption are fast.</p> <p>Disadvantage: Each pair of keys must be unique. Key management is difficult if there are a large number of users.</p> <p>Scenario: Encrypt a large amount of data.</p>	<a href="#">Key Types</a>
Asymmetric key encryption	<p>Asymmetric key encryption is also called public key encryption. A key pair is used for encryption and decryption. One is a public key, and the other is a private key.</p> <p>Advantage: Different keys are used for encryption and decryption, enhancing security.</p> <p>Disadvantage: Encryption and decryption are slow.</p> <p>Scenario: Encrypt sensitive information.</p>	<a href="#">Key Types</a>
Key pair	A key pair is a pair of asymmetric public key and private key. By default, RSA-2048 is used for cryptography.	<a href="#">Key Pair Service</a>
Private key pair	A private key pair can be viewed or used only by the current account.	<a href="#">Creating a Key Pair</a>
Account key pair	An account key pair can be viewed or used by all users under the account.	<a href="#">Upgrading a Key Pair</a>



# 2 KMS

---

## 2.1 Functions

KMS is a secure, reliable, and easy-to-use cloud service that helps users create, manage, and protect keys in a centralized manner.

It uses Hardware Security Modules (HSMs) to protect keys. All CMKs are protected by root keys in HSMs to avoid key leakage.

It also controls access to keys and records all operations on keys with traceable logs. In addition, it provides use records of all keys, meeting your audit and regulatory compliance requirements.

### Functions

- On the KMS console, you can perform the following operations on CMKs:
  - Creating, querying, enabling, disabling, scheduling the deletion of, and canceling the deletion of CMKs
  - Modifying the alias and description of CMKs
  - Using the online tool to encrypt and decrypt small volumes of data
  - Adding, searching for, editing, and deleting tags
  - Creating, canceling, and querying grants
- You can use the API to perform the following operations:
  - Creating, encrypting, or decrypting data encryption keys (DEKs)
  - Retiring grants
  - Signing or verifying the signature of messages or message digestsFor details, see the *Data Encryption Workshop API Reference*.
- Generate hardware true random number.

You can generate 512-bit random numbers using the KMS API. The 512-bit hardware true random numbers can be used as or serve as basis for key materials and encryption parameters. For details, see the *Data Encryption Workshop API Reference*.

## Key Algorithms Supported by KMS

Symmetric keys created on the KMS console use the AES-256 algorithm. Asymmetric keys created by KMS support the RSA and ECC algorithms.

**Table 2-1** Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Asymmetric keys	RSA	<ul style="list-style-type: none"> <li>RSA_2048</li> <li>RSA_3072</li> <li>RSA_4096</li> </ul>	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none"> <li>EC_P256</li> <li>EC_P384</li> </ul>	Elliptic curve recommended by NIST	Digital signature

**Table 2-2** describes the key wrapping encryption and decryption algorithms supported by imported keys.

**Table 2-2** Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA algorithm that uses OAEP and has the <b>SHA-256</b> hash function	Select an algorithm based on your HSM functions.
RSAES_OAEP_SHA_1	RSA algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the <b>SHA-1</b> hash function	If the HSMs support the <b>RSAES_OAEP_SHA_256</b> algorithm, use <b>RSAES_OAEP_SHA_256</b> to encrypt key materials. <b>NOTICE</b> The <b>RSAES_OAEP_SHA_1</b> algorithm is no longer secure. Exercise caution when performing this operation.

## 2.2 Product Advantages

- Extensive Service Integration

KMS can be integrated with Object Storage Service (OBS), Elastic Volume Service (EVS), and Image Management Service (IMS), to manage keys of these services on the KMS console, and encrypt and decrypt your local data by making the KMS API calls.

- Regulatory Compliance

Keys are generated by third-party validated HSMs. Access to keys is controlled and all operations involving keys are traceable by logs, compliant with Chinese and international laws and regulations.

## 2.3 Application Scenarios

### Prerequisites

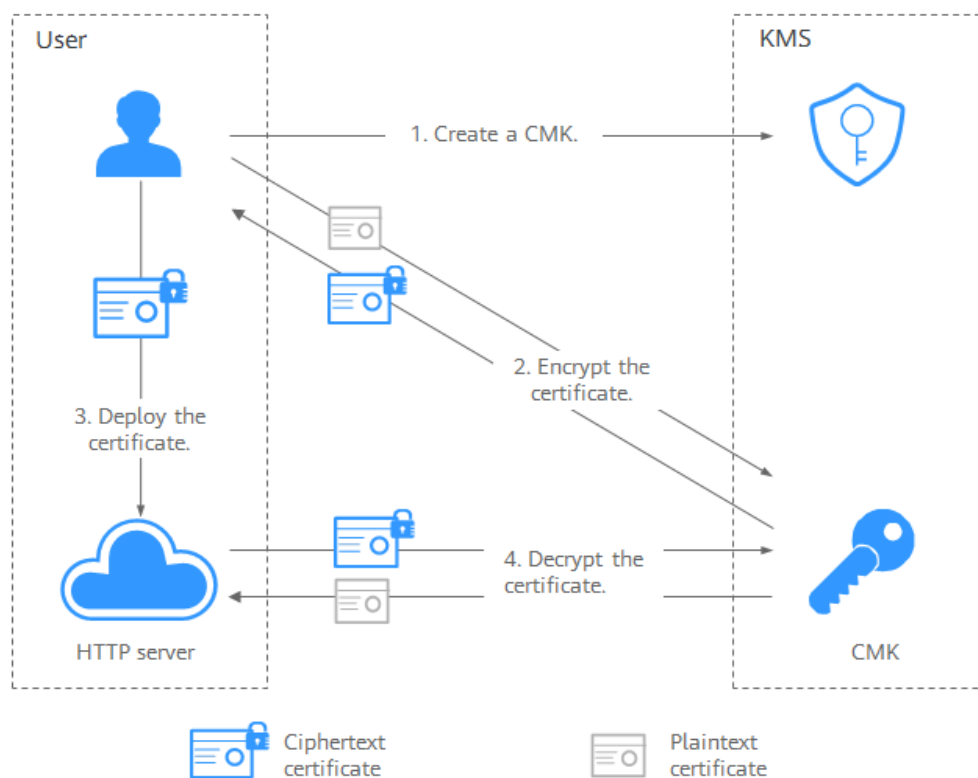
All the CMKs mentioned in this section are symmetric keys. For details about symmetric keys and asymmetric keys, see [Keys Types](#).

### Small Data Encryption and Decryption

You can use the online tool on the KMS console or call KMS APIs to directly encrypt or decrypt a small amount of data, such as passwords, certificates, or phone numbers. Currently, a maximum of 4 KB of data can be encrypted or decrypted in this way.

[Figure 2-1](#) shows an example about how to call the APIs to encrypt and decrypt an HTTPS certificate.

**Figure 2-1** Encrypting and decrypting an HTTPS certificate



The procedure is as follows:

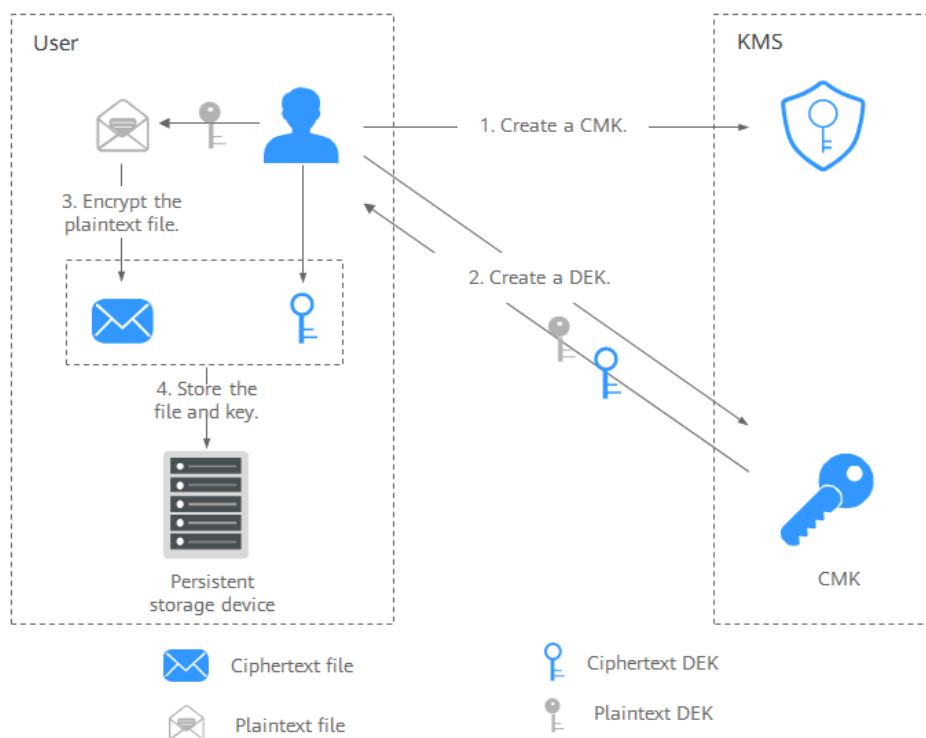
1. Create a CMK on KMS.
2. Call the **encrypt-data** API of KMS and use the CMK to encrypt the plaintext certificate.
3. Deploy the certificate onto a server.
4. The server calls the **decrypt-data** API of KMS to decrypt the ciphertext certificate.

## Large Data Encryption and Decryption

If you want to encrypt or decrypt large volumes of data, such as pictures, videos, and database files, you can use the envelope encryption method, where the data does not need to be transferred over the network.

- **Figure 2-2** illustrates the process for encrypting a local file.

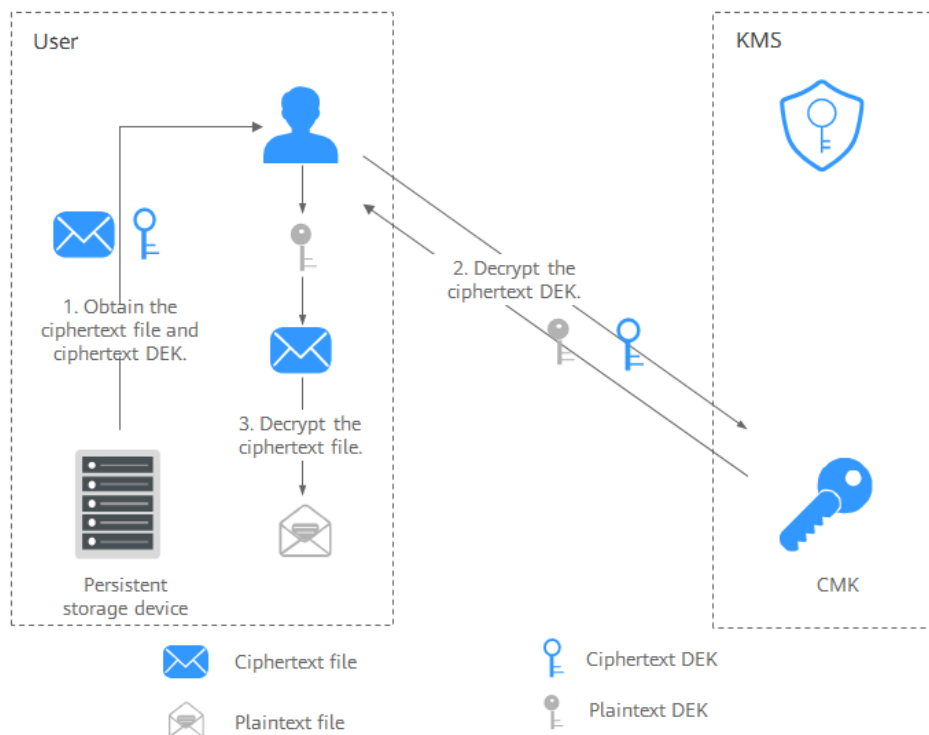
**Figure 2-2** Encrypting a local file



The procedure is as follows:

- a. Create a CMK on KMS.
  - b. Call the **create-datakey** API of KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK. The ciphertext DEK is generated when you use a CMK to encrypt the plaintext DEK.
  - c. Use the plaintext DEK to encrypt the file. A ciphertext file is generated.
  - d. Save the ciphertext DEK and the ciphertext file together in a persistent storage device or a storage service.
- **Figure 2-3** illustrates the process for decrypting a local file.

**Figure 2-3** Decrypting a local file



The procedure is as follows:

- Obtain the ciphertext DEK and file from the persistent storage device or the storage service.
- Call the **decrypt-datakey** API of KMS and use the corresponding CMK (the one used for encrypting the DEK) to decrypt the ciphertext DEK. Then you get the plaintext DEK.  
If the CMK is deleted, the decryption fails. Therefore, properly keep your CMKs.
- Use the plaintext DEK to decrypt the ciphertext file.

## Helpful Links

Document	Link
Best Practices	<ul style="list-style-type: none"> <li><a href="#">Encrypting or Decrypting Small Volumes of Data</a></li> <li><a href="#">Encrypting or Decrypting a Large Amount of Data</a></li> </ul>
API Example	<ul style="list-style-type: none"> <li><a href="#">Encrypting or Decrypting Small Volumes of Data</a></li> <li><a href="#">Encrypting or Decrypting a Large Amount of Data</a></li> </ul>

## 2.4 Using KMS

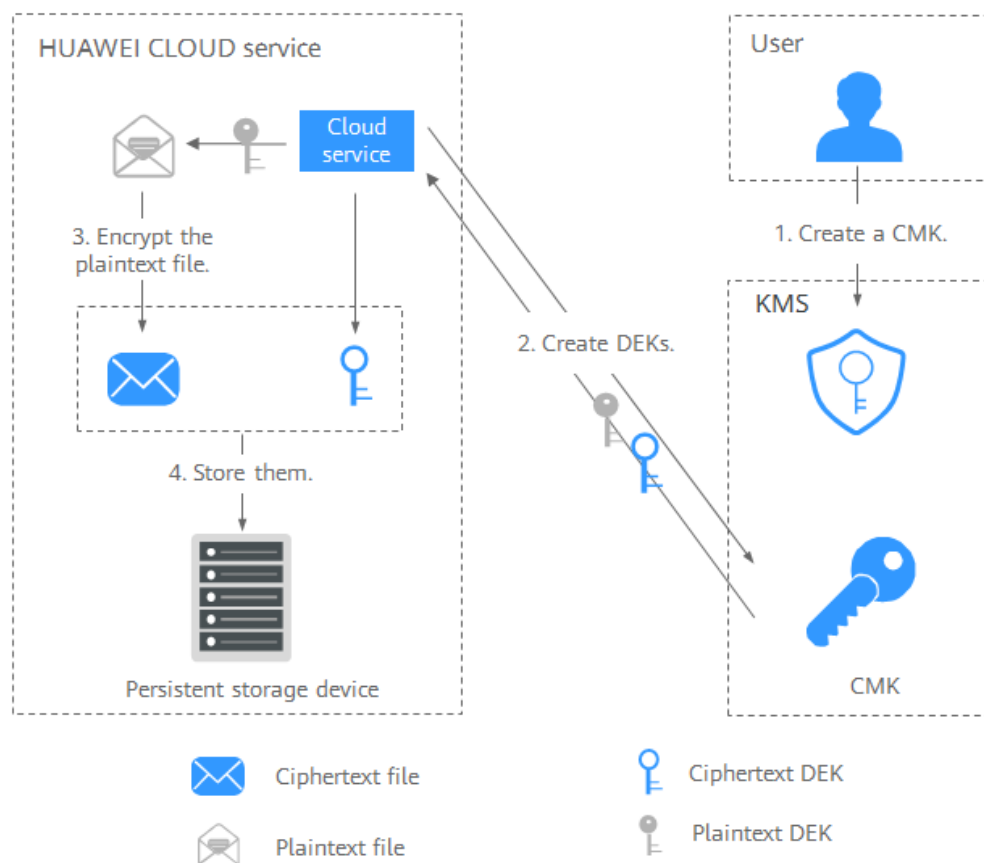
### Prerequisites

All the CMKs mentioned in this section are symmetric keys. For details about symmetric keys and asymmetric keys, see [Keys Types](#).

### Interacting with Huawei Cloud Services

Huawei Cloud services use the envelope encryption technology and call KMS APIs to encrypt service resources. Your CMKs are under your own management. With your grant, Huawei Cloud services use a specific CMK of yours to encrypt data.

**Figure 2-4** How Huawei Cloud uses KMS for encryption



The encryption process is as follows:

1. Create a CMK on KMS.
2. Huawei Cloud services call the **create-datakey** API of the KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK.

#### **NOTE**

Ciphertext DEKs are generated when you use a CMK to encrypt the plaintext DEKs.

3. Huawei Cloud services use the plaintext DEK to encrypt a plaintext file, generating a ciphertext file.
4. Huawei Cloud services store the ciphertext DEK and ciphertext file in a persistent storage device or a storage service.

 **NOTE**

When users download the data from a Huawei Cloud service, the service uses the CMK specified by KMS to decrypt the ciphertext DEK, uses the decrypted DEK to decrypt data, and then provides the decrypted data for users to download.

**Table 2-3** List of cloud services that use KMS encryption

Service Name	Description
Object Storage Service (OBS)	<p>You can upload objects to and download them from Object Storage Service (OBS) in common mode or server-side encryption mode. When you upload objects in encryption mode, data is encrypted at the server side and then securely stored on OBS in ciphertext. When you download encrypted objects, the data in ciphertext is decrypted at the server side and then provided to you in plaintext. OBS supports the server-side encryption with KMS-managed keys (SSE-KMS) mode. In SSE-KMS mode, OBS uses the keys provided by KMS for server-side encryption.</p> <p>For details about how to upload objects to OBS in SSE-KMS mode, see the <a href="#">Object Storage Service Console Operation Guide</a>.</p>
Elastic Volume Service (EVS)	<p>If you enable the encryption function when creating an EVS disk, the disk will be encrypted with the DEK generated by using your CMK. Data stored in the EVS disk will be automatically encrypted.</p> <p>For details about how to use the encryption function of EVS, see <a href="#">Elastic Volume Service User Guide</a>.</p>
Image Management Service (IMS)	<p>When creating a private image using an external image file, you can enable the private image encryption function and select a CMK provided by KMS to encrypt the image.</p> <p>For details about how to use the private image encryption function of Image Management Service (IMS), see <a href="#">Image Management Service User Guide</a>.</p>
Scalable File Service (SFS)	<p>When creating a file system on SFS, the CMK provided by KMS can be selected to encrypt the file system, so that files stored in the file system are automatically encrypted.</p> <p>For details about how to use the file system encryption function of SFS, see <a href="#">Scalable File Service User Guide</a>.</p>
Relational Database Service (RDS)	<p>When purchasing a database instance, you can enable the disk encryption function of the database instance and select a CMK created on KMS to encrypt the disk of the database instance. Enabling the disk encryption function will enhance data security.</p> <p>For details about how to use the disk encryption function of RDS, see <a href="#">Relational Database Service User Guide</a>.</p>

Service Name	Description
Document Database Service (DDS)	When purchasing a DDS instance, you can enable the disk encryption function of the instance and select a CMK created on KMS to encrypt the disk of the instance. Enabling the disk encryption function will enhance data security.  For details about how to use the disk encryption function of DDS, see <a href="#">Document Database Service Getting Started</a> .

## Working with User Applications

To encrypt plaintext data, a user application can call the necessary KMS API to create a DEK. The DEK can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the KMS API to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs.

Envelope encryption is implemented, with CMKs stored in KMS and ciphertext DEKs in user applications. KMS is called to decrypt a ciphertext DEK only when necessary.

The encryption process is as follows:

1. The application calls the **create-key** API of KMS to create a CMK.
2. The application calls the **create-datakey** API of KMS to create a DEK. A plaintext DEK and a ciphertext DEK are generated.

### NOTE

Ciphertext DEKs are generated when you use a CMK to encrypt the plaintext DEKs in [1](#).

3. The application uses the plaintext DEK to encrypt a plaintext file. A ciphertext file is generated.
4. The application saves the ciphertext DEK and the ciphertext file together in a persistent storage device or a storage service.

For details, see the *Data Encryption Workshop API Reference*.

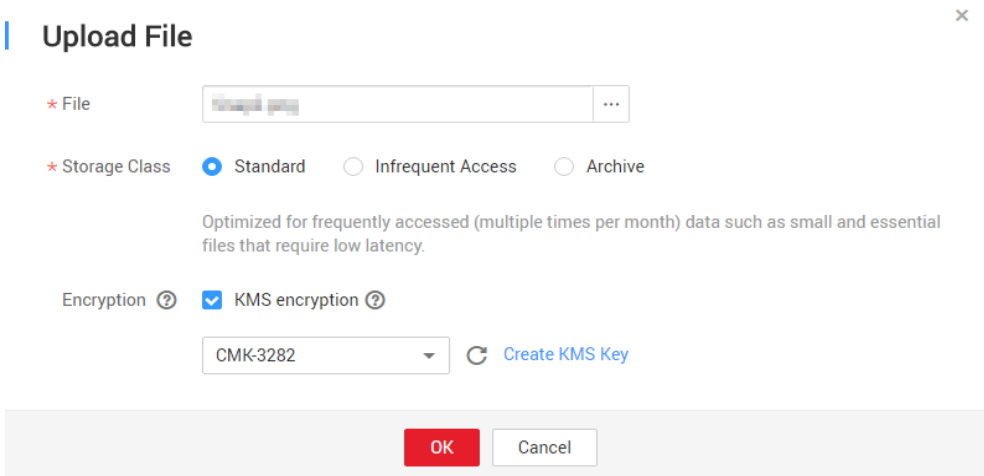
## 2.5 Cloud Services with KMS Integrated

### 2.5.1 Encrypting Data in OBS

- When using Object Storage Service (OBS) to upload files with server-side encryption, you can select KMS encryption and use the key provided by KMS to encrypt the files to be uploaded. For details, see [Figure 2-5](#). For more information, see *Object Storage Service Console Operation Guide*.



Figure 2-5 OBS server-side encryption



The screenshot shows the 'Upload File' dialog box in OBS. It includes a file selection field, storage class options (Standard, Infrequent Access, Archive), and encryption settings. The 'KMS encryption' checkbox is checked, and a CMK ID 'CMK-3282' is selected from a dropdown menu. There are 'OK' and 'Cancel' buttons at the bottom.

There are two types of CMKs that can be used:

- The default master key **obs/default** created by KMS
- CMKs that you create on the KMS console using KMS-generated key materials
- Alternatively, you can call OBS APIs to upload a file with server-side encryption using KMS-managed keys (SSE-KMS). For details, see the *Object Storage Service API Reference*.

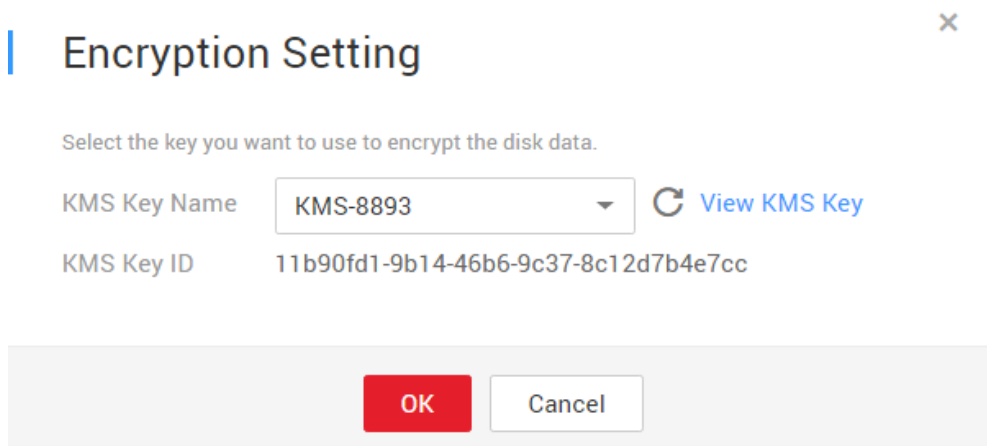
## 2.5.2 Encrypting Data in EVS

- When purchasing a disk, you can choose **Advanced Settings > Configure > Encryption** to encrypt the disk using the key provided by KMS. For details, see [Figure 2-6](#). For more information about EVS, see the *Elastic Volume Service User Guide*.

### NOTE

Before you use the encryption function, EVS must be granted the permission to access KMS. If you have the right to grant the permission, you can grant the permission directly. If you do not have the permission, contact a user with the security administrator permissions to add the security administrator permission for you. Then, you can grant the permission. For more information about EVS, see the *Elastic Volume Service User Guide*.

Figure 2-6 Encrypting data in EVS



There are two types of CMKs that can be used:

- The default master key **evs/default** created by KMS
- CMKs that you create on the KMS console using KMS-generated key materials
- You can also call EVS APIs to create encrypted EVS disks. For details, see the *Elastic Volume Service API Reference*.

### 2.5.3 Encrypting Data in IMS

- When uploading an image file to Image Management Service (IMS), you can choose to encrypt the image file using a key provided by KMS to protect the file. **Figure 2-7** describes details. For details, see the *Image Management Service User Guide*.

Figure 2-7 Encrypting data in IMS



There are two types of CMKs that can be used:

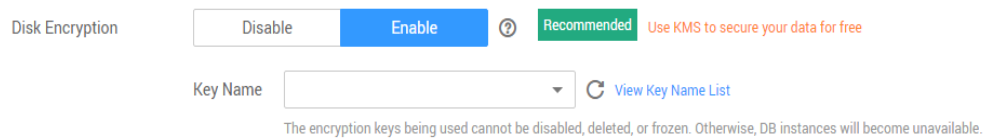
- The default master key **ims/default** created by KMS
- CMKs that you create on the KMS console using KMS-generated key materials
- You can also call IMS APIs to create encrypted image files. For details, see *Image Management Service API Reference*.

### 2.5.4 Encrypting Data in RDS

- When a user purchases a database instance from Relational Database Service (RDS), the user can select **Disk encryption** and use the key provided by KMS

to encrypt the disk of the database instance. For more information, see the *Relational Database Service User Guide*.

**Figure 2-8** Encrypting data in RDS



There are two types of CMKs that can be used:

- The default master key **rds/default** created by KMS
- CMKs that you create on the KMS console using KMS-generated key materials
- You can also call the RDS APIs to purchase encrypted database instances. For details, see the *Relational Database Service User Guide*.

# 3 CSMS

---

## 3.1 Functions

CSMS is a secure, reliable, and easy-to-use credential hosting service. Users or applications can use CSMS to create, retrieve, update, and delete credentials in a unified manner throughout the credential lifecycle. CSMS can help you eliminate risks incurred by hardcoding, plaintext configuration, and permission abuse.

### Unified Secret Management

Applications and business systems have a large number of secrets and are difficult to manage.

CSMS can store, retrieve, and use secrets in a unified manner throughout their lifecycles.

Perform the following operations to manage secrets using CSMS:

1. Collect secrets.
2. Upload the secrets to CSMS.
3. Configure fine-grained access and usage permissions for each secret by using IAM.

### Secure Secret Retrieval

Many applications store plaintext secrets, such as passwords, tokens, certificates, SSH keys, and API keys, in their configuration files to be used for authentication when they access databases or other services. Plaintext and hardcoded secrets are prone to breach and incur security risks.

CSMS allows users to dynamically query secrets via APIs instead of hardcoding the secrets, greatly reducing breach risks.

Perform the following operations to manage secrets using CSMS:

When an application reads its configurations, it calls CSMS APIs to retrieve secrets. Neither hardcoded nor plaintext secrets are required.

## Rotating Credentials and Keys

Secrets need to be periodically updated to enhance security. To rotate a secret, you need to update the secret in all the applications and configurations using it, which is time-consuming, error-prone, and may cause service interruption.

CSMS enables convenient multi-version secret management. Applications can call CSMS APIs or SDKs to securely update secrets without making mistakes.

Perform the following operations to manage secrets using CSMS:

1. An administrator adds a secret version on the CSMS console or via APIs to and update the secret.
2. Applications call CSMS APIs or SDKs to obtain the latest or a specified version of the secret, and perform full or grayscale update.
3. Regularly repeat steps **1** and **2** to rotate secrets.
4. Enable rotation for encryption keys to improve storage security.

## CSMS Basic Features

**Table 3-1** CSMS basic features

Function	Description
Secret lifecycle management	<ul style="list-style-type: none"><li>• Create, view, and schedule and cancel the deletion of secrets.</li><li>• Change the secret encryption key and description.</li></ul>
Secret version management	<ul style="list-style-type: none"><li>• Create and view secret versions.</li><li>• View secret values.</li></ul>
Secret version status management	Update, query, and delete credential versions.
Secret tag management	Add, search for, edit, and delete tags.

## 3.2 Product Advantages

### Secret encryption

Secrets are encrypted by KMS before storage. Encryption keys are generated and protected by authenticated third-party HSM. When you retrieve secrets, they are transferred to local servers via TLS.

### Secure secret retrieval

CSMS calls secret APIs instead of hard-coded secrets in applications. Secrets can be dynamically retrieved and managed. CSMS manages application secrets in a centralized manner to reduce breach risks.

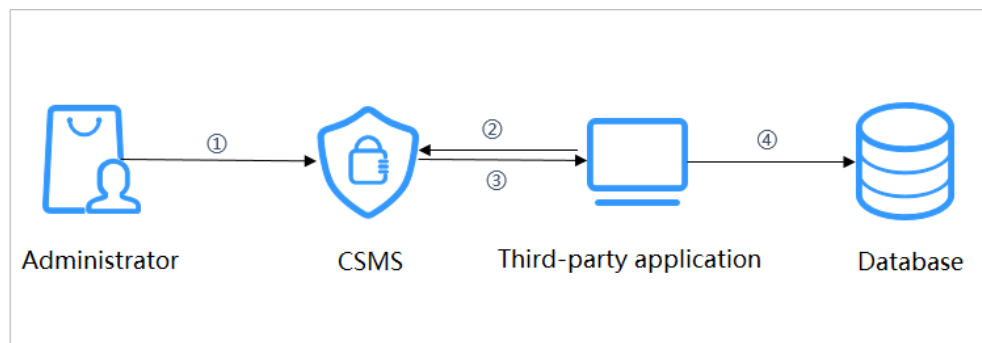
## Centralized secret management and control

IAM identity and permission management ensure only authorized users can retrieve and modify credentials. CTS monitors access to credentials. These services prevent unauthorized access to and breach of sensitive information.

### 3.3 Application Scenarios

This section uses a basic database username and its password as an example to describe how CSMS works.

**Figure 3-1** Secret-based login process



The procedure is as follows:

- Step 1** Create a secret on the **console** or via an API to store database information (such as the database address, port, and password).
- Step 2** Use an application to access the database. CSMS will query the secret you created.
- Step 3** CSMS retrieves and decrypts the credential ciphertext, and securely returns the information stored in the credential to the application through the credential management API.
- Step 4** The application obtains the decrypted plaintext secret and uses it to access the database.

----End

# 4 KPS

---

## 4.1 Functions

Key Pair Service (KPS) is a secure, reliable, and easy-to-use cloud service designed to manage and protect your SSH key pairs (key pairs for short).

As an alternative to the traditional username+password authentication method, key pairs allow you to remotely log in to Linux ECSs.

A key pair, including one public key and one private key, are generated based on a cryptographic algorithm. The public key is automatically saved in KPS, while the private key can be saved to the user's local host. You can also save your private keys in KPS and manage them with KPS based on your needs. If you have configured the public key in a Linux ECS, you can use the private key to log in to the ECS without a password. Therefore, you do not need to worry about password interception, cracking, or leakage.

### Functions

Using the KPS console or APIs, you can perform the following operations on key pairs:

- Creating, importing, viewing, and deleting key pairs
- Resetting, replacing, binding, and unbinding key pairs
- Managing, importing, exporting, and clearing private keys

### KPS supported cryptography algorithms

- The SSH key pairs created on the management console support the following cryptographic algorithms:
  - ssh-ed25519
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521
  - ssh-rsa. The maximum valid length is 2048,3072,4096.

- The SSH keys imported to the KPS console support the following cryptographic algorithms:
  - ssh-dss
  - ssh-ed25519
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521
  - ssh-rsa. The maximum valid length is 2048,3072,4096.

## 4.2 Product Advantages

- Reinforced Login Security  
You can log in to a Linux ECS without entering a password, effectively preventing password interception, cracking, or leakage and improving the Linux ECS security.
- Regulatory Compliance  
Random numbers are generated by third-party validated HSMs. Access to key pairs is controlled and all operations involving key pairs are traceable by logs, compliant with Chinese and international laws and regulations.

## 4.3 Application Scenarios

When purchasing an ECS running Linux, you can choose to authenticate users trying to log in to your ECS with the SSH key pair provided by KPS. When purchasing an ECS running Windows, you can choose to obtain the password used to log in to your ECS from the key file provided by KPS.

### Logging In to a Linux ECS

If your Elastic Cloud Server (ECS) runs Linux, you can use a key pair to log in to the ECS. For details, see the [Elastic Cloud Server User Guide](#).

When purchasing an ECS, you can choose either of the following key pairs:

- Key pairs created or imported on the ECS console
- Key pairs created on or imported to the KPS console

The two types of key pairs only differ in the ways they are imported.

### Obtaining the Password for Logging In to a Windows ECS

If your ECS runs Windows, you need to obtain the login password using the private key of a key pair. For details, see the [Elastic Cloud Server User Guide](#).

When purchasing an ECS, you can choose either of the following key pairs:

- Key pairs created on or imported to the ECS console
- Key pairs created on or imported to the KPS console

The two types of key pairs only differ in the ways they are imported.



# 5 Dedicated HSM

---

## 5.1 Illustration of Dedicated Encryption Workshop

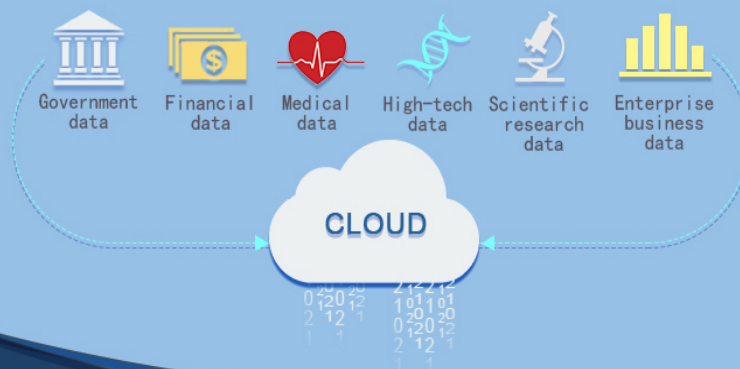


# Data Encryption Workshop Dedicated HSM

Secure and Effective  
Protect Data and Prevent Leakage

## 1.Data Leakage – Always a Threat

More and more people are migrating their data and applications to the cloud, calling for encryption to an increasing amount of **critical, personal, and privacy data**. However, inappropriate protection may result in data leakage, with serious consequences such as reputation damage and economic penalties.



## 2.Dedicated HSM – Emerges for Better Security

Dedicated Hardware Security Module (Dedicated HSM) is a **data encryption service** provided by HUAWEI CLOUD. It is one of the mandatory measures for **level 3 protection of network security**, which effectively **prevent data leakage**.

## 5.2 Functions

Dedicated HSM is a cloud service used for encryption, decryption, signature, signature verification, key generation, and the secure storage of keys.

Dedicated HSM provides encryption hardware, guaranteeing data security and integrity on Elastic Cloud Servers (ECSs) and meeting FIPS 140-2 requirements. Dedicated HSM offers you a secure and reliable management for the keys generated by your instances, and uses multiple algorithms for data encryption and decryption.

### Functions

Dedicated HSM provides the following capabilities:

- Generation, storage, import, export, and management of encryption keys (both symmetric and asymmetric keys)
- Data encryption and decryption by using symmetric and asymmetric algorithms
- Using cryptographic hash functions to calculate message digests and hash-based message authentication code
- Signing data and code in encrypted mode and verifying signature
- Random data generation in encrypted mode

### Supported Cryptography Algorithms

You can use Chinese cryptographic algorithms and certain international common cryptographic algorithms to meet various user requirements.

**Table 5-1** Supported cryptography algorithms

Category	Common Cryptographic Algorithm
Symmetric cryptographic algorithm	AES
Asymmetric cryptographic algorithm	RSA, DSA, ECDSA, DH, and ECDH
Digest algorithm	SHA1, SHA256, and SHA384

## 5.3 Product Advantages

- Cloud Applicable  
Dedicated HSM is the optimal choice for transferring offline encryption capabilities to the cloud, reducing your O&M costs.
- Elastic Scaling  
You can flexibly increase or decrease the number of HSM instances according to your service needs.

- Security management  
Dedicated HSM separates device management from the management of content (sensitive information). As a user of the device, you can control the generation, storage, and access of keys. Dedicated HSM is only responsible for monitoring and managing devices and related network facilities. Even the O&M personnel have no access to customer keys.
- Permission authentication
  - Sensitive instructions are classified for hierarchical authorization, which effectively prevents unauthorized access.
  - Several authentication types are supported, such as username/password and digital certificate.
- Reliable
  - Dedicated HSM provides FIPS 140-2 validated level 3 HSMs for protection of your keys, guaranteeing high-performance encryption services to meet your stringent security requirements.
  - Each Dedicated HSM has its own chips. The service is not affected even if some chips are damaged.
- Security compliance  
Dedicated HSM instances can help you protect your data on ECSs and meet compliance requirements.
- Wide application  
Dedicated HSM offers finance HSM, server HSM, and signature server HSM instances for use in various service scenarios.

## 5.4 Application Scenarios

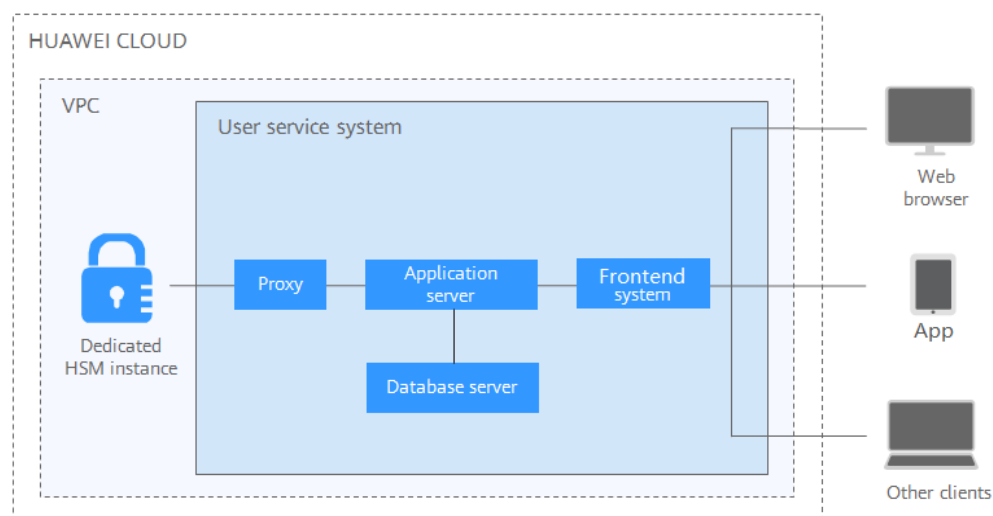
After a Dedicated HSM instance is purchased, you can use the UKey provided by Dedicated HSM to initialize and manage the instance. You can fully control the key generation, storage, and access authentication.

You can use Dedicated HSM to encrypt your service systems (including encryption of sensitive data, payment, and electronic tickets). Dedicated HSM helps you encrypt enterprise sensitive data (such as contracts, transactions, and SNs) and user sensitive data (such as user ID numbers and mobile numbers), to prevent hackers from cracking the network and dragging the database, which may cause data leakage, and prevent illegal access to or tampering with data by internal users.

### NOTE

You need to deploy the Dedicated HSM instance and service system in the same VPC and select proper security group rules. If you have any questions, contact technical support personnel.

**Figure 5-1 Architecture**



## Sensitive Data Encryption

Government public services, Internet enterprises, and system applications that contain immense sensitive information

Data is the core asset of an enterprise. Each enterprise has its core sensitive data. Dedicated HSM provides integrity check and encrypted storage for sensitive data, which effectively prevents sensitive data from being stolen or tampered with, and prevents unauthorized access.

## Finance

System applications for payment and prepayment with transportation card, on e-commerce platforms, and through other means

Dedicated HSM can ensure the integrity and confidentiality of payment data during transmission and storage, and ensure the payment identity authentication and the non-repudiation of payment process.

## Verification

Transportation, manufacturing, and healthcare

Dedicated HSM can ensure the confidentiality and integrity of electronic contracts, invoices, insurance policies, and medical records during transmission and storage.

## 5.5 Editions

Dedicated HSM provides instances of the platinum edition. For details, see [Table 5-2](#).

**Table 5-2** Dedicated HSM

Edition	Billing Mode	Service Scope
Platinum	Yearly/ Monthly	<ul style="list-style-type: none"> <li>● Exclusive chip for encryption Provides you with exclusive chips for data encryption in the cloud, ensuring hardware isolation while maintaining your service performance.</li> <li>● Full service support Supports application security, such as financial payment, identity authentication, and digital signature, meeting your stringent requirements for data and system security.</li> <li>● Scalable Allows you to easily and flexibly add and reduce password computing resources based on your service needs.</li> <li>● Highly reliable Instances of hardware devices are virtualized into clusters to achieve load balancing and high reliability.</li> <li>● Compatibility Provides the same functions and API as physical cryptographic devices, facilitating migration to the cloud with support for PKCS#11 and CSP APIs.</li> <li>● Common algorithms                         <ul style="list-style-type: none"> <li>- Symmetric algorithm: DES and AES</li> <li>- Digest algorithm: SHA1, SHA256, and SHA384</li> <li>- Asymmetric algorithm: RSA, DSA, ECDSA, DH, and ECDH.</li> </ul> </li> <li>● Exclusive subrack and power supply Provides you with exclusive HSM subrack and power supply.</li> <li>● Dedicated network Provides dedicated network bandwidth and API resources.</li> <li>● FIPS 140-2 certification Uses FIPS 140-2 level 3 certified HSM to generate encryption keys.</li> </ul>

# 6 Billing Description

## Billing Item

DEW charges based on your usage and purchased edition.

**Table 6-1** Billing items

Service Name	Billing Mode	Billing Item	Description
Key Management Service (KMS)	Pay-per-use	Number of keys	Key instances that have been successfully created or imported are billed on a pay-per-use basis. Prices are calculated by hour, and no minimum fee is required.
	Pay-per-use	API requests	The first 20,000 API requests are free of charge. Additional API calls are charged. The unit is 10,000 calls.
KPS	Pay-per-use	Number of key pairs	Free of charge
	Pay-per-use	API requests	Free of charge
Dedicated HSM	Yearly/Monthly	Edition	Platinum edition For details, see <a href="#">Editions</a> .
	Pay-per-use	API requests	Free of charge



Service Name	Billing Mode	Billing Item	Description
Cloud Secret Management Service (CSMS)	Pay-per-use	Number of credentials	CSMS instances that have been successfully created or imported are billed on a pay-per-use basis. Prices are calculated by day, and no minimum fee is required.
	Pay-per-use	API requests	Billed by the number of requests. The unit is 10,000 requests.

## Billing

- KMS  
KMS is charged per use. No minimum fee is required. Once a key is created, it will be charged by hour. You pay for the keys you created and the API requests that are beyond the free-of-charge range.
- KPS
  - If you do not choose to let Huawei Cloud manage your private keys when creating or importing them, no cost will be incurred.
  - If you choose to let Huawei Cloud manage your private keys after importing them, KPS is charged by hour. In the current version, it is free of charge.
- Dedicated HSM  
Dedicated HSM offers monthly and yearly packages based on the edition and device models of instances you have purchased.
- Secret management  
You are charged based on the number of secrets, usage duration, and number of API requests.

For price details, see [Product Pricing Details](#).

## Changing Billing Mode

DEW does not support unsubscription currently.

## Renewal

If you do not renew the yearly/monthly-billed DEW service upon its expiration, a retention period is available for you.

For details about the retention period, see [Retention Period](#).

To avoid unnecessary loss caused by security issues, renew your subscription before the retention period expires.

You can renew your resources on the management console. For details, see [Manually Renewing a Resource](#).

## Expiration and Overdue Payment

- Expiration  
If you do not renew your subscription upon the expiration, a retention period is available for you. For details, see [Retention Period](#).
- Overdue Payment

## FAQ

For more billing FAQs, see [DEW FAQs](#).

# 7 DEW Permission Management

---

If you want to assign different access permissions to employees in an enterprise for the DEW resources purchased on Huawei Cloud, you can use Identity and Access Management (IAM) to perform refined permission management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and grant permissions to the users to control their access to specific resource types. For example, if you have software developers and you want to assign them the permission to access DEW but not to delete DEW or its resources, then you can create an IAM policy to assign the developers the permission to access DEW but prevent them from deleting DEW related data.

If the Huawei Cloud account has met your requirements and you do not need to create an independent IAM user for permission control, then you can skip this section. This will not affect other functions of DEW.

IAM is offered for free, and you pay only for the billable resources in your account. For more details, see [IAM Service Overview](#).

## DEW Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services based on the permissions.

DEW is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. Users need to switch to the authorized region when accessing DEW.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. Some roles depend other roles to take effect. When you assign such roles to users, remember to

assign the roles they depend on. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant DEW users only the permissions for managing a certain type of cloud servers. Most policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by DEW, see [Permissions Policies and Supported Actions](#).

**Table 7-1** lists all the system policies of DEW.

**Table 7-1** System-defined roles and policies supported by DEW

Role/Policy Name	Description	Type	De pen den cy
KMS Administrator	Administrator permissions for KMS	System role	No ne
KMS CMKFullAccess	Full permissions for KMS. Users with these permissions can perform all the operations allowed by policies.	System policy	No ne
DEW KeypairFullAccess	Full permissions for KPS. Users with these permissions can perform all the operations allowed by policies.	System policy	No ne
DEW KeypairReadOnlyAccess	Read-only permissions for KPS. Users with this permission can only view KPS data.	System policy	No ne

**Table 7-2** lists the common operations supported by each system-defined permission of DEW. Select the permissions as needed.

**Table 7-2** Common operations supported by each system-defined policy or role

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Create a key	√	√	x	x
Enable a key	√	√	x	x
Disable a key	√	√	x	x
Schedule key deletion	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Cancel scheduled key deletion	√	√	x	x
Modify a key alias	√	√	x	x
Modify key description	√	√	x	x
Generate a random number	√	√	x	x
Create a DEK	√	√	x	x
Create a plaintext-free DEK	√	√	x	x
Encrypt a DEK	√	√	x	x
Decrypt a DEK	√	√	x	x
Obtain parameters for importing a key	√	√	x	x
Import key materials	√	√	x	x
Delete key materials	√	√	x	x
Create a grant	√	√	x	x
Revoke a grant	√	√	x	x
Retire a grant	√	√	x	x
Query the grant list	√	√	x	x
Query retirable grants	√	√	x	x
Encrypt data	√	√	x	x
Decrypt data	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Send signature messages	√	√	x	x
Authenticate signature	√	√	x	x
Enable key rotation	√	√	x	x
Modify key rotation interval	√	√	x	x
Disable key rotation	√	√	x	x
Query key rotation status	√	√	x	x
Query CMK instances	√	√	x	x
Query key tags	√	√	x	x
Query project tags	√	√	x	x
Batch add or delete key tags	√	√	x	x
Add tags to a key	√	√	x	x
Delete key tags	√	√	x	x
Query the key list	√	√	x	x
Query key details	√	√	x	x
Query public key	√	√	x	x
Query instance quantity	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Query quotas	√	√	x	x
Query the key pair list	x	x	√	√
Create or import a key pair	x	x	√	x
Query key pairs	x	x	√	√
Delete a key pair	x	x	√	x
Update key pair description	x	x	√	x
Bind a key pair	x	x	√	x
Unbind a key pair	x	x	√	x
Query a binding task	x	x	√	√
Query failed tasks	x	x	√	√
Delete all failed tasks	x	x	√	x
Delete a failed task	x	x	√	x
Query running tasks	x	x	√	√

## Helpful Links

- [What Is IAM](#)
- [Creating a User and Authorizing the User the Permission to Access DEW](#)
- [Permissions Policies and Supported Actions](#)

# 8 How to Access

---

Huawei Cloud provides a web-based service management platform. You can access DEW using the API over the HTTPS or on the management console.

- Management console

If you have registered with the public cloud, you can log in to the management console directly. In the upper left corner of the console, click



. Choose **Security & Compliance > Data Encryption Workshop**.

- API

You can access DEW using the API. For details, see the *Data Encryption Workshop API Reference*.



# 9 Related Services

---

## OBS

Object Storage Service (OBS) is a scalable service that provides secure, reliable, and cost-effective cloud storage for massive amounts of data. KMS provides central management and control capabilities of CMKs for OBS. It is used for server-side encryption with KMS-managed keys (SSE-KMS) on OBS.

## EVS

Elastic Volume Service (EVS) offers scalable block storage for cloud servers. With high reliability, high performance, and rich specifications, EVS disks can be used for distributed file systems, development and test environments, data warehouse applications, and high-performance computing (HPC) scenarios to meet diverse service requirements. KMS provides central management and control capabilities of CMKs for EVS. It is used for encryption in EVS.

## IMS

Image Management Service (IMS) allows you to manage the entire lifecycle of your images. KMS provides central management and control capabilities of CMKs for Image Management Service (IMS). It is used for private image encryption in IMS.

## ECS

An ECS is a basic computing component that consists of CPUs, memory, OS, and elastic volume service (EVS). After creating an ECS, you can use it like your local computer or physical server.

KMS manages key pairs of ECSs. The key pairs are used to authenticate users logging in to the ECSs.

Dedicated HSM can encrypt sensitive data in the service systems on your ECS. You can control the generation, storage, and access authorization of keys to ensure the integrity and confidentiality of data during transmission and storage.

## DDS

Document Database Service (DDS) is a MongoDB-compatible database service that is secure, highly available, reliable, scalable, and easy to use. It provides DB

instance creation, scaling, redundancy, backup, restoration, monitoring, and alarm reporting functions with just a few clicks on the DDS console. KMS provides central management and control capabilities of CMKs for DDS. It is used for disk encryption in DDS.

## CTS

Cloud Trace Service (CTS) provides you with a history of DEW operations. After the CTS service is enabled, you can view all generated traces to review and audit performed KMS operations. For details, see the *Cloud Trace Service User Guide*.

**Table 9-1** DEW operations supported by CTS

Operation	Resource Type	Trace Name
Creating a CMK	cmk	createKey
Creating a DEK	cmk	createDataKey
Creating a plaintext-free DEK	cmk	createDataKeyWithoutPlaintext
Enabling a CMK	cmk	enableKey
Disabling a CMK	cmk	disableKey
Encrypting a DEK	cmk	encryptDatakey
Decrypting a DEK	cmk	decryptDatakey
Scheduling the deletion of a CMK	cmk	scheduleKeyDeletion
Canceling the scheduled deletion of a CMK	cmk	cancelKeyDeletion
Generating random numbers	rng	genRandom
Changing the alias of a CMK	cmk	updateKeyAlias
Changing the description of a CMK	cmk	updateKeyDescription
Prompting risks about CMK deletion	cmk	deleteKeyRiskTips
Importing key material	cmk	importKeyMaterial
Deleting key material	cmk	deleteImportedKeyMaterial
Creating a grant	cmk	createGrant
Retiring a grant	cmk	retireGrant
Revoking a grant	cmk	revokeGrant

Operation	Resource Type	Trace Name
Encrypting data	cmk	encryptData
Decrypting data	cmk	decryptData
Adding a tag	cmk	createKeyTag
Deleting a tag	cmk	deleteKeyTag
Adding or deleting tags in batches	cmk	batchCreateKeyTags
Batch deleting tags	cmk	batchDeleteKeyTags
Enabling key rotation	cmk	enableKeyRotation
Modifying key rotation interval	cmk	updateKeyRotationInterval
Disabling key rotation	cmk	disableKeyRotation
Creating a secret	csms	createSecret
Updating a secret	csms	updateSecret
Deleting a secret	csms	forceDeleteSecret
Schedule the deletion of a secret	csms	scheduleDelSecret
Canceling the scheduled deletion of a secret	csms	restoreSecretFromDeletedStatus
Creating a secret status	csms	createSecretStage
Updating a secret status	csms	updateSecretStage
Deleting a secret status	csms	deleteSecretStage
Creating a secret version	csms	createSecretVersion
Downloading secret backup	csms	backupSecret
Restoring secret backup	csms	restoreSecretFromBackupBlob
Creating or importing an SSH key pair	keypair	createOrImportKeypair
Deleting an SSH key pair	keypair	deleteKeypair
Importing a private key	keypair	importPrivateKey
Exporting a private key	keypair	exportPrivateKey
Purchasing an HSM instance	hsm	purchaseHsm

Operation	Resource Type	Trace Name
Configuring an HSM instance	hsm	createHsm
Deleting an HSM instance	hsm	deleteHsm

## IAM

Identity and Access Management (IAM) provides the permission management function for DEW.

Only users who have KMS Administrator permissions can use DEW.

Only users who have the KMS Administrator and Server Administrator permissions can use the key pair function.

To apply for permissions, contact a user with Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

# 10 Personal Data Protection Mechanism

To ensure that your personal data, such as the username, password, and mobile phone number, will not be leaked or obtained by unauthorized or unauthenticated entities or people, DEW controls access to the data and records logs for operations performed on the data.

## Personal Data to Be Collected

[Table 10-1](#) lists the personal data generated or collected by DEW.

**Table 10-1** Personal data

Type	Source	Can Be Modified	Mandatory
Tenant ID	<ul style="list-style-type: none"><li>Tenant ID in the token when an operation is performed on the console.</li><li>Tenant ID in the token when an API is invoked.</li></ul>	No	Yes

## Storage Mode

Tenant IDs are not sensitive data and are stored in plaintext.

## Access Permission Control

Users can view only logs related to their own services.

## Log Records

DEW records logs for all operations, such as editing, querying, and deleting, performed on personal data. The logs are uploaded to Cloud Trace Service (CTS). You can view only the logs generated for operations you performed.

# A Change History

---

Released On	Description
2023-01-30	This is the second official release. Added: <b>CSMS</b> <b>KPS</b> <b>Dedicated HSM</b>
2022-09-30	This is the first official release.