Data Encryption Workshop

Service Overview

Issue 19

Date 2023-06-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

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 provides services such as Key Management Service (KMS), , Key Pair Service (KPS), and Cloud Secret Management Service (CSMS). DEW secures your data and keys, as well as simplifies key management. DEW uses hardware security modules (HSMs) to protect the security of your keys and can be integrated with multiple Huawei Cloud services. Additionally, DEW enables you to develop customized encryption applications.

Figure 1-1 DEW subservices

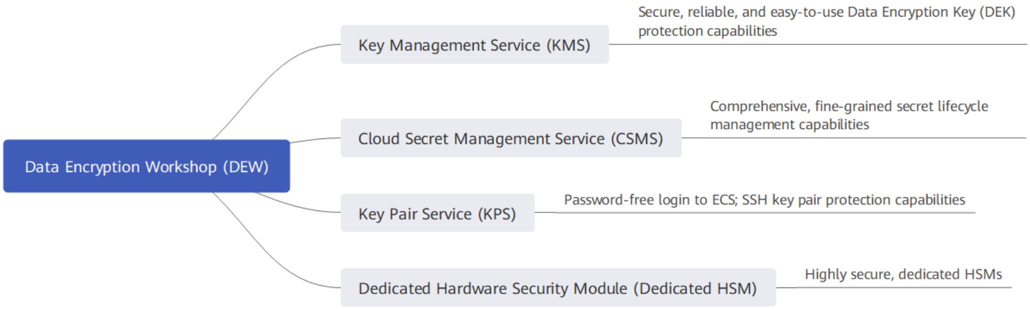

Data Encryption Workshop (DEW)
Key Management Service (KMS)
Secure, reliable, and easy-to-use Data Encryption Key (DEK) protection capabilities
Cloud Secret Management Service (CSMS)
Comprehensive, fine-grained secret lifecycle management capabilities
Key Pair Service (KPS)
Password-free login to ECS; SSH key pair protection capabilities
Dedicated Hardware Security Module (Dedicated HSM)
Highly secure, dedicated HSMs

Table 1-1 Service overview

Service	Description	Reference
Key Management Service (KMS)	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. KMS uses hardware security modules (HSMs) to protect keys. HSM meets the FIPS 140-2 Level 3 security requirements. It helps you create and manage keys. All keys are protected by root keys in HSMs to avoid key leakage.	**Key Types**
Cloud Secret Management Service (CSMS)	CSMS is a secure, reliable, and easy-to-use secret hosting service. Users or applications can use CSMS to create, retrieve, update, and delete credentials in a unified manner throughout the secret lifecycle. CSMS can help you eliminate risks incurred by hardcoding, plaintext configuration, and permission abuse.	**Creating a Secret**
Key Pair Service (KPS)	KPS is a secure, reliable, and easy-to-use cloud service designed to manage and protect your SSH key pairs (key pairs for short). 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.	**Creating a Key Pair**

Service	Description	Reference
Dedicated Hardware Security Module (Dedicated HSM)	Dedicated HSM enables data encryption on the cloud, specifically, encrypting and decrypting data, verifying signature, generating keys, and storing keys. 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.	**Dedicated HSM**

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 keys are protected by root keys in HSMs to avoid key leakage. The HSM module meets the FIPS 140-2 Level 3 security requirements.

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:
  - Create, query, enable, and disable CMKs, as well as schedule and cancel CMK deletion.
  - Modify the alias and descriptions of CMKs.
  - Use the online tool to encrypt and decrypt small-size data.
  - Add, search for, edit, and delete tags.
  - Create, cancel, and query grants.
- You can use the APIs to:
  - Create, encrypt, or decrypt DEKs.
  - Retire grants.
  - Sign or verify the signature of messages or message digests.
  - Generate and verify message authentication codes.

  For details, see the *Data Encryption Workshop API Reference*.
- Generate hardware true random numbers.

  You can generate 512-bit random numbers based on hardware using the KMS API. The 512-bit true random numbers can be used 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 and SM4 algorithms. Asymmetric keys created by KMS support the RSA, SM2, and ECC algorithms.

Table 2-1 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Application Scenario
Symmetric key	AES	AES_256	AES symmetric key	● Data encryption and decryption ● DEKs encryption and decryption **NOTE** You can encrypt and decrypt a small amount of data using the the online tool on the console. You need to call APIs to encrypt and decrypt a large amount of data.
Digest key	SHA	● HMAC_256 ● HMAC_384 ● HMAC_512	Digest key	● Data tampering prevention ● Data integrity verification

Key Type	Algorithm Type	Key Specifications	Description	Application Scenario
Asymmetric key	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA asymmetric password	• Digital signature and signature verification • Data encryption and decryption **NOTE** Asymmetric keys are applicable to signature and signature verification scenarios. Asymmetric keys are not efficient enough for data encryption. Symmetric keys are suitable for encrypting and decrypting data.
	ECC	• EC_P256 • EC_P384	Elliptic curve recommended by NIST	Digital signature and signature verification

Table 2-2 describes the encryption and decryption algorithms supported for user-imported keys.

Table 2-2 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA algorithm that uses OAEP and has the **SHA-256** hash function	Select an algorithm based on your HSM functions. If your HSM supports the **RSAES_OAEP_SHA_256** algorithm, use **RSAES_OAEP_SHA_256** to encrypt key materials.

2.2 Advantages

Extensive Service Integration

- By integrating with OBS, EVS, and IMS, you can use KMS to manage the keys of the services or use KMS APIs to encrypt and decrypt local data.
- By integrating with Cloud Trace Service (CTS), you can use CTS to view recent KMS operation records.

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.

Easy to Use

You can use and manage keys easily using the console or APIs, needless to purchase hardware encryption devices.

2.3 Application Scenarios

Prerequisites

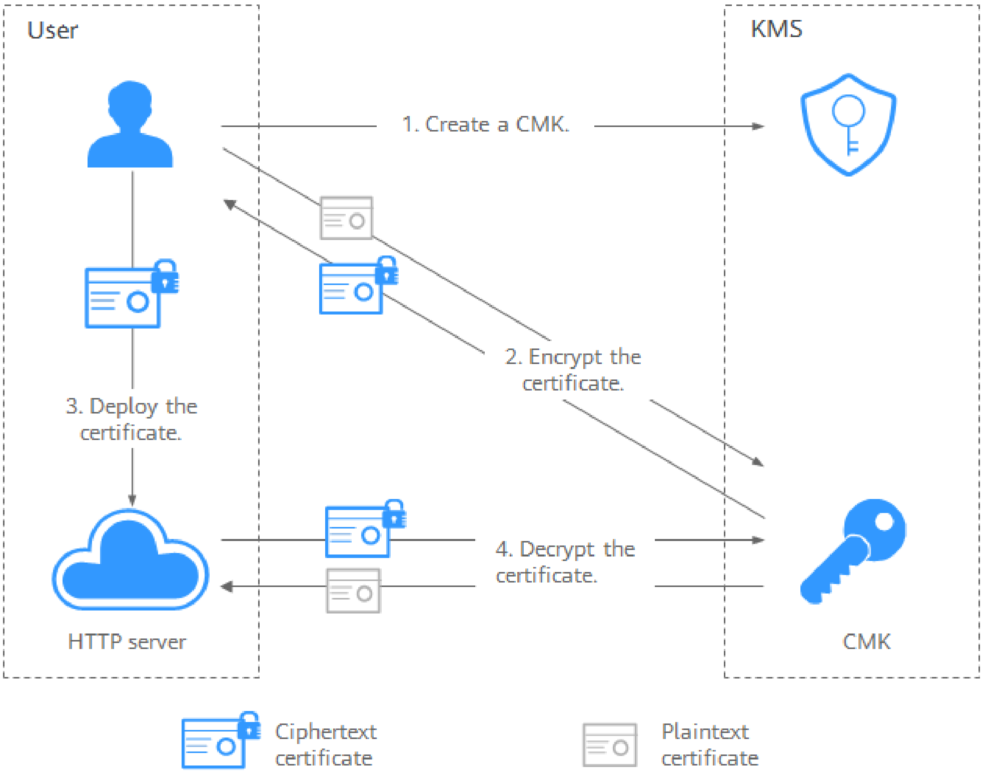
All the custom keys mentioned in this section are symmetric keys. For details about symmetric keys and asymmetric keys, see **Keys Types**.

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


User
KMS
1. Create a CMK.
2. Encrypt the certificate.
3. Deploy the certificate.
4. Decrypt the certificate.
HTTP server
CMK
Ciphertext certificate
Plaintext certificate

The procedure is as follows:

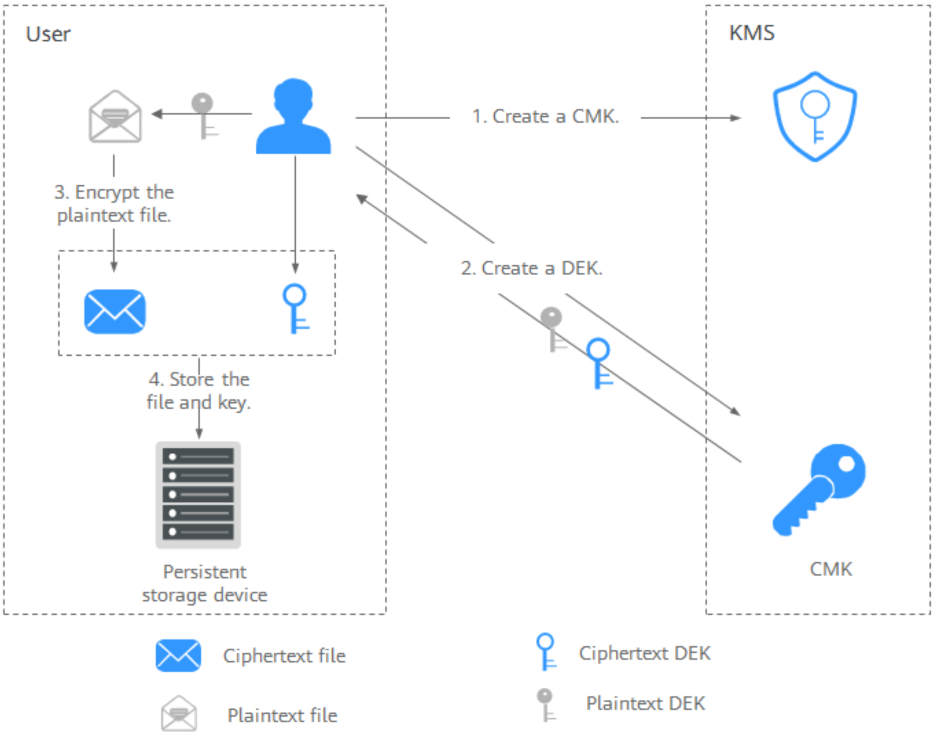
1. Create a CMK on KMS.
2. Call the **encrypt-data** API of KMS and use the CMK to encrypt the plaintext certificate.
3. Deploy the certificate onto a server.
4. The server calls the **decrypt-data** API of KMS to decrypt the ciphertext certificate.

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.

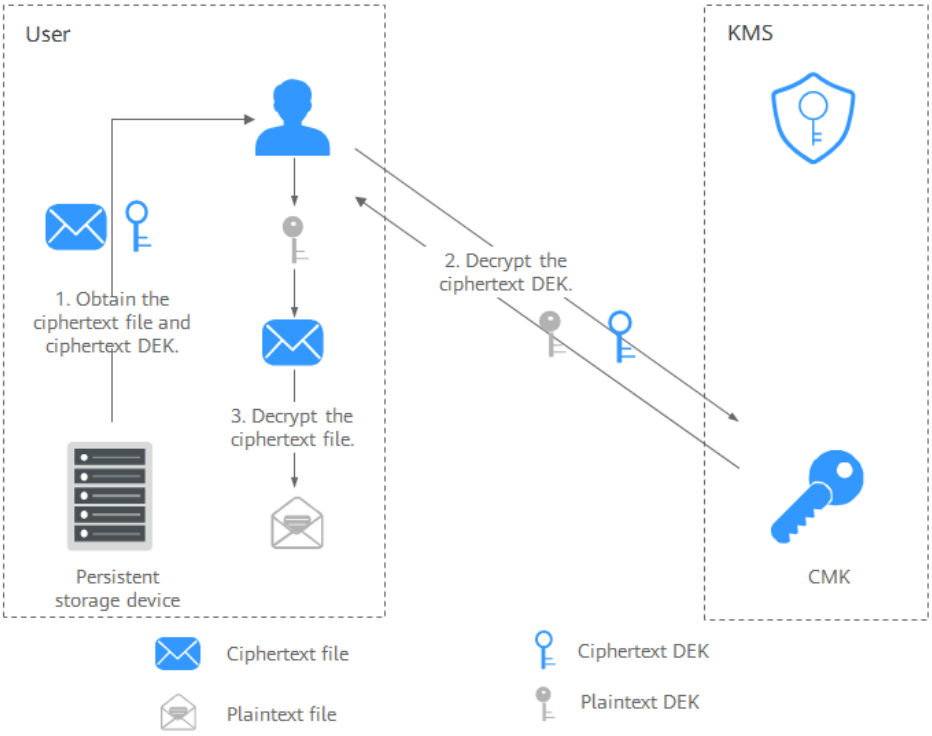
b. Call the **create-datakey** API of KMS to create a DEK. Then you get a plaintext DEK and a ciphertext DEK. The ciphertext DEK was generated by using a custom key to encrypt the plaintext DEK.

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


User
KMS
1. Obtain the ciphertext file and ciphertext DEK.
2. Decrypt the ciphertext DEK.
3. Decrypt the ciphertext file.
Persistent storage device
CMK
Ciphertext file
Plaintext file
Ciphertext DEK
Plaintext DEK

The procedure is as follows:

a. Obtain the ciphertext DEK and file from the persistent storage device or the storage service.

b. 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.

c. Use the plaintext DEK to decrypt the ciphertext file.

Helpful Links

Document	Link
Best Practices	• **Encrypting or Decrypting Small Volumes of Data** • **Encrypting or Decrypting a Large Amount of Data**
API Example	• **Encrypting or Decrypting Small Volumes of Data** • **Encrypting or Decrypting a Large Amount of Data**

2.4 Using KMS

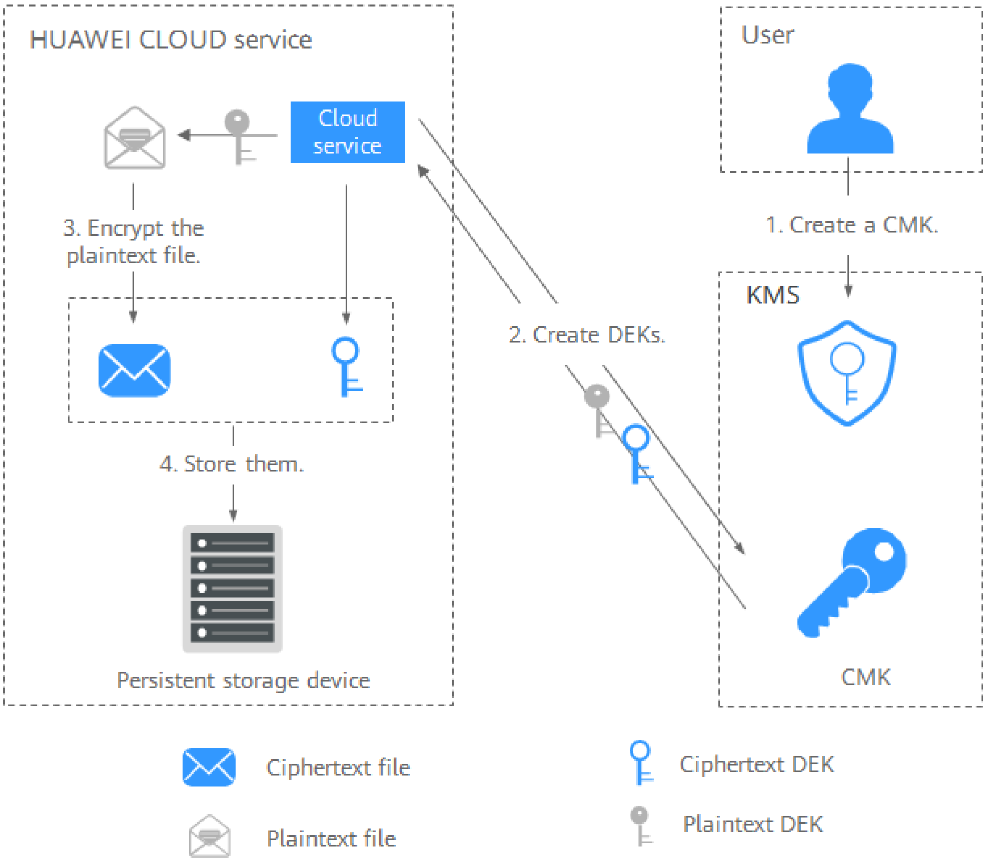
Prerequisites

All the custom keys 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 custom key of yours to encrypt data.

Figure 2-4 How Huawei Cloud uses KMS for encryption



The encryption process is as follows:

1. Create a custom key 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 custom key 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)	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. For details about how to upload objects to OBS in SSE-KMS mode, see the **Object Storage Service Console Operation Guide**.
Elastic Volume Service (EVS)	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. For details about how to use the encryption function of EVS, see **Elastic Volume Service User Guide**.
Image Management Service (IMS)	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. For details about how to use the private image encryption function of Image Management Service (IMS), see **Image Management Service User Guide**.
Scalable File Service (SFS)	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. For details about how to use the file system encryption function of SFS, see **Scalable File Service User Guide**.
Relational Database Service (RDS)	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. For details about how to use the disk encryption function of RDS, see **Relational Database Service User Guide**.

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 **Document Database Service Getting Started**.

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 custom key.
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.

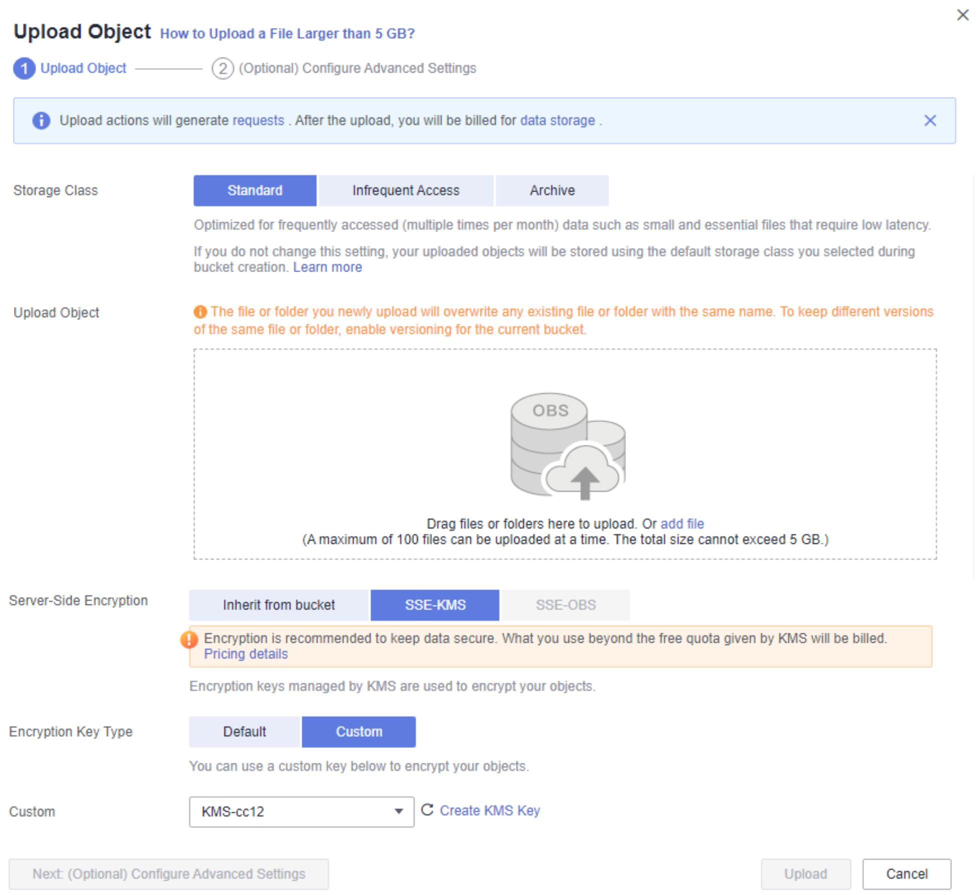
For details, see **Data Encryption Workshop API Overview**.

2.5 Cloud Services with KMS Integrated

2.5.1 Encrypting Data in OBS

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

Figure 2-5 OBS server-side encryption



Upload Object How to Upload a File Larger than 5 GB?

1 Upload Object —— 2 (Optional) Configure Advanced Settings

Upload actions will generate requests . After the upload, you will be billed for data storage .

Storage Class: Standard | Infrequent Access | Archive

Optimized for frequently accessed (multiple times per month) data such as small and essential files that require low latency.

If you do not change this setting, your uploaded objects will be stored using the default storage class you selected during bucket creation. Learn more

Upload Object

The file or folder you newly upload will overwrite any existing file or folder with the same name. To keep different versions of the same file or folder, enable versioning for the current bucket.

Drag files or folders here to upload. Or add file
(A maximum of 100 files can be uploaded at a time. The total size cannot exceed 5 GB.)

Server-Side Encryption: Inherit from bucket | SSE-KMS | SSE-OBS

Encryption is recommended to keep data secure. What you use beyond the free quota given by KMS will be billed. Pricing details

Encryption keys managed by KMS are used to encrypt your objects.

Encryption Key Type: Default | Custom

You can use a custom key below to encrypt your objects.

Custom: KMS-cc12

There are two types of CMKs that can be used:

- The default key **obs/default** created by KMS
- Custom keys that you created on the KMS console

- 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*.

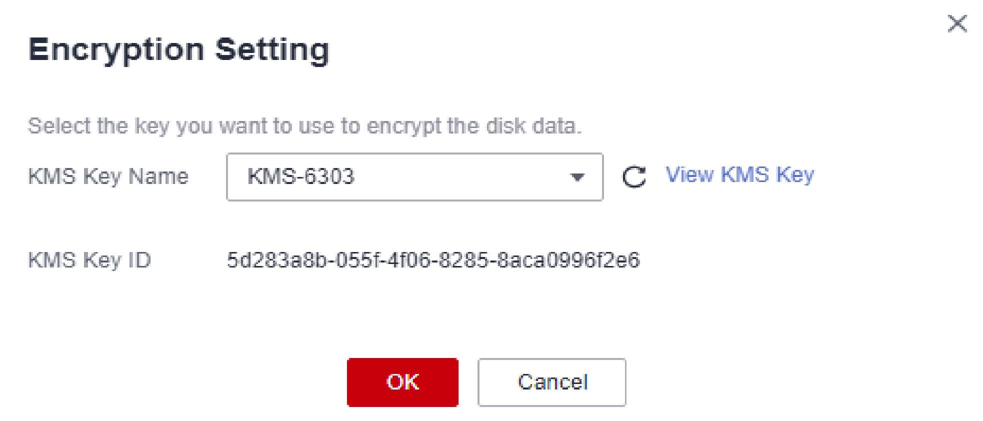
2.5.2 Encrypting Data in EVS

- When purchasing a disk, you can choose **Advanced Settings** > **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



Encryption Setting

Select the key you want to use to encrypt the disk data.

KMS Key Name: KMS-6303

KMS Key ID: 5d283a8b-055f-4f06-8285-8aca0996f2e6

There are two types of CMKs that can be used:

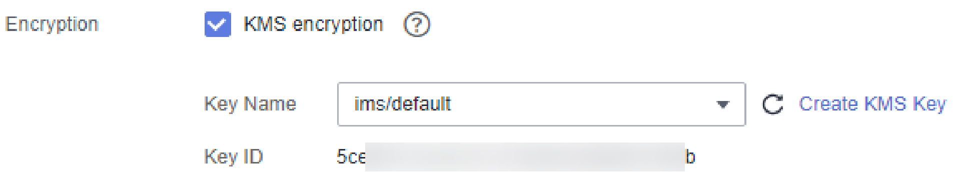
- The default key **evs/default** created by KMS
- Custom keys that you create on the KMS console using KMS-generated key materials

- 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



Encryption ☑ KMS encryption

Key Name: ims/default

Key ID: 5ce[redacted]b

There are two types of CMKs that can be used:

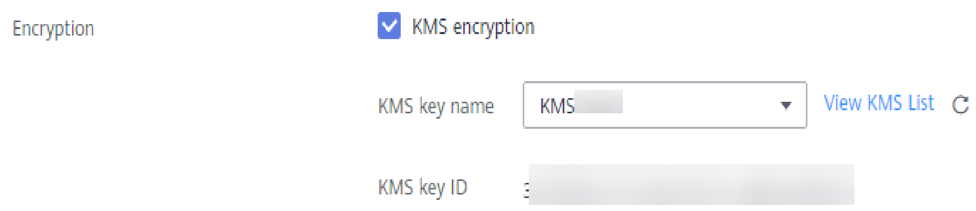
- The default key **ims/default** created by KMS
- Custom keys that you create on the KMS console using KMS-generated key materials

- 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 SFS

- When creating a file system using the Scalable File Service (SFS), you can select **KMS encryption** and use the key provided by the KMS to encrypt the file system.For details, see **Figure 2-8**. For more information, see the *Scalable File Service User Guide*.

Figure 2-8 Encrypting Data in SFS



Encryption ☑ KMS encryption

KMS key name KMS[redacted] View KMS List

KMS key ID [redacted]

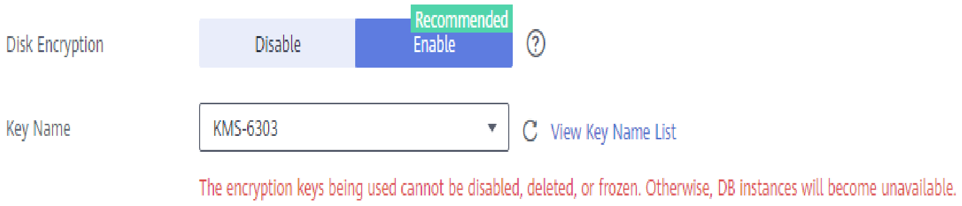
You can use a custom key created on the KMS console for encryption.

- You can use the SFS API to create an encrypted file system. For details, see the *Scalable File Service API Reference*.

2.5.5 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 2-9 Encrypting data in RDS



Disk Encryption Disable [✓ Enable] Recommended

Key Name KMS-6303 View Key Name List

The encryption keys being used cannot be disabled, deleted, or frozen. Otherwise, DB instances will become unavailable.

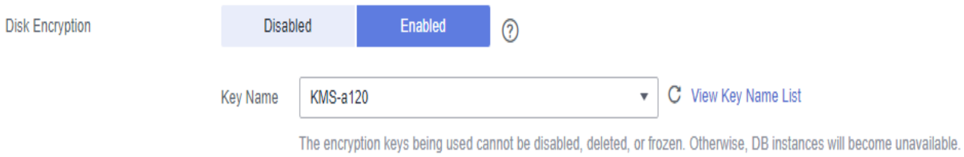
You can use a custom key created on the KMS console for encryption.

- You can also call the RDS APIs to purchase encrypted database instances. For details, see the *Relational Database Service User Guide*.

2.5.6 Encrypting Data in DDS

- When a user purchases a database instance from DDS, 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 *Document Database Service User Guide*.

Figure 2-10 Encrypting data in DDS



Disk Encryption Disabled [✓ Enabled]

Key Name KMS-a120 View Key Name List

The encryption keys being used cannot be disabled, deleted, or frozen. Otherwise, DB instances will become unavailable.

You can use a custom key created on the KMS console for encryption.

- You can also call the required API of DDS to purchase encrypted DB instances. For details, see *Document Database Service API Reference*.

3 CSMS

3.1 Functions

CSMS is a secure, reliable, and easy-to-use secret hosting service. Users or applications can use CSMS to create, retrieve, update, and delete credentials in a unified manner throughout the secret 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.

Secret Event Notification

After you subscribe to an associated event for a secret object, if the event is enabled and a basic event is triggered on the secret object, an event notification is sent to the notification topic specified by the event through Simple Message Notification (SMN). Basic event types include new secret version creation, secret version expiration, secret deletion, and secret rotation. After configuring event notification, you can use event-driven managed functions in FunctionGraph to automatically rotate secrets.

Perform the following operations to manage secrets using CSMS:

1. The administrator adds an event on the CSMS event notification console or by calling the API.

2. When creating or updating a secret, you need to associate the event object required for subscription.

3. You will receive an event notification when the secret status changes. You can configure functions in FunctionGraph to automatically update or rotate secrets.

CSMS Basic Features

Table 3-1 CSMS basic features

Function	Description
Secret lifecycle management	● Create, view, and schedule and cancel the deletion of secrets. ● Change the secret encryption key and description.
Secret version management	● Create and view secret versions. ● View secret values. ● Set secret version expiration configurations.

Function	Description
Secret version status management	Update, query, and delete secret versions.
Secret tag management	Add, search for, edit, and delete tags.
Secret event management	● Create, view, and delete events ● Secret change event types
Secret notification management	View the change event type, event name, and secret name.

3.2 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 secrets. CTS monitors access to secrets. These services prevent unauthorized access to and breach of sensitive information.

Secret change notification

SMN notifies users of basic secret event changes in a timely manner. FunctionGraph is used to configure functions to automatically update or rotate secrets.

Secure secret calling

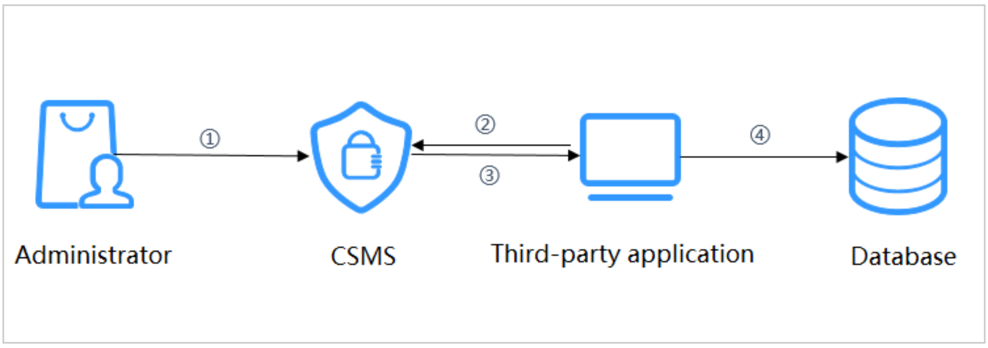
CCE allows users to mount secrets to pods. In this way, sensitive information can be decoupled from the cluster environment, which prevents information leakage caused by program hardcoding or plaintext configuration.

3.3 Application Scenarios

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

The administrator saves and updates secret values. The user obtain the required secret value through third-party application services. For details, see **Figure 3-1**.

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 the administrator created in the last step.

Step 3 CSMS retrieves and decrypts the secret ciphertext, and securely returns the information stored in the secret to the application through the secret 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

Cryptographic Algorithms Supported by KPS

- 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 length can be 2048, 3072, and 4096 bits.

- 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 length can be 2048, 3072, 4096 bits.

4.2 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 ECS runs Linux, you can use a key pair to log in to the ECS. For details, see **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 or imported on 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 or imported on the KPS console.

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

5 Dedicated HSM

5.1 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

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

Dedicated HSM Types

Table 5-2 Dedicated HSM types

HSM Type	Function	Application Scenario
Hardware Security Module (HSM)	● Data encryption and decryption ● Data signature and verification ● Data digest ● Generation and verification of MAC addresses	Basic password calculations in applications of a wide range of industries, such as identity authentication, data protection, SSL keys, and computation offloading.
Finance	● Generation, encryption, conversion, and verification of personal identification number (PIN) ● Generation and verification of Media Access Control (MAC) ● Generation and verification of Card Verification Value (CVV) ● Generation and verification of Type Allocation Code (TAC) ● Typical Racal instruction set ● People's Bank of China (PBOC) 3.0 common instruction set	Cryptographic calculation in financial systems, such as card issuing systems and point of sale (POS) systems
Signature verification server	● Signing and signature verification ● Encoding and decoding of digital envelopes ● Encoding and decoding of signed digital envelopes ● Certificate verification	Signature usage in Certificate Authority (CA) systems, certificate verification, encrypted transmission of a large amount of data, and identity authentication

5.2 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.
  - Dedicated HSM provides reliable backup and hosting solutions for HSM data.

- 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.

5.3 Application Scenarios

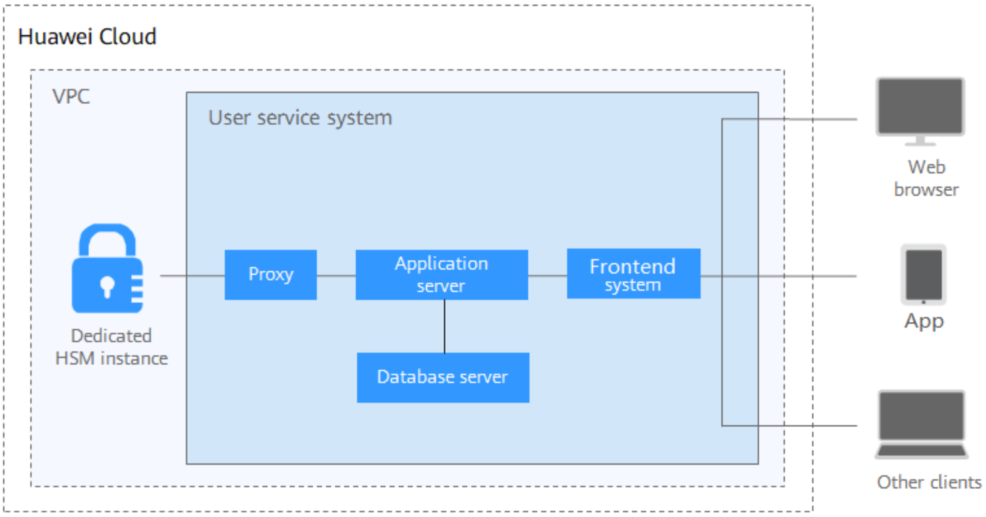
After a Dedicated HSM instance is purchased, you can use the UKey provided by Dedicated HSM to initialize and manage the instance. You can fully control the key generation, storage, and access authentication.

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.

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.

5.4 Editions

Dedicated HSM provides instances of the platinum edition (outside Chinese mainland). For details, see **Table 5-3**.

Table 5-3 Dedicated HSM

Edition	Billing Mode	Service Scope
Platinum edition (outside Chinese mainland)	Yearly/ Monthly	● Exclusive chip for encryption Provides you with exclusive chips for data encryption in the cloud, ensuring hardware isolation while maintaining your service performance. ● Full service support Supports application security, such as financial payment, identity authentication, and digital signature, meeting your stringent requirements for data and system security. ● Scalable Allows you to easily and flexibly add and reduce password computing resources based on your service needs. ● Highly reliable Instances of hardware devices are virtualized into clusters to achieve load balancing and high reliability. ● Compatibility Provides the same functions and API as physical cryptographic devices, facilitating migration to the cloud with support for PKCS#11 and CSP APIs. ● Common algorithms – Symmetric algorithm: DES and AES – Digest algorithm: SHA1, SHA256, and SHA384 – Asymmetric algorithm: RSA, DSA, ECDSA, DH, and ECDH. ● Exclusive subrack and power supply Provides you with exclusive HSM subrack and power supply. ● Dedicated network Provides dedicated network bandwidth and API resources. ● FIPS 140-2 certification Uses FIPS 140-2 level 3 certified HSM to generate encryption keys.

6 Security

6.1 Shared Responsibilities

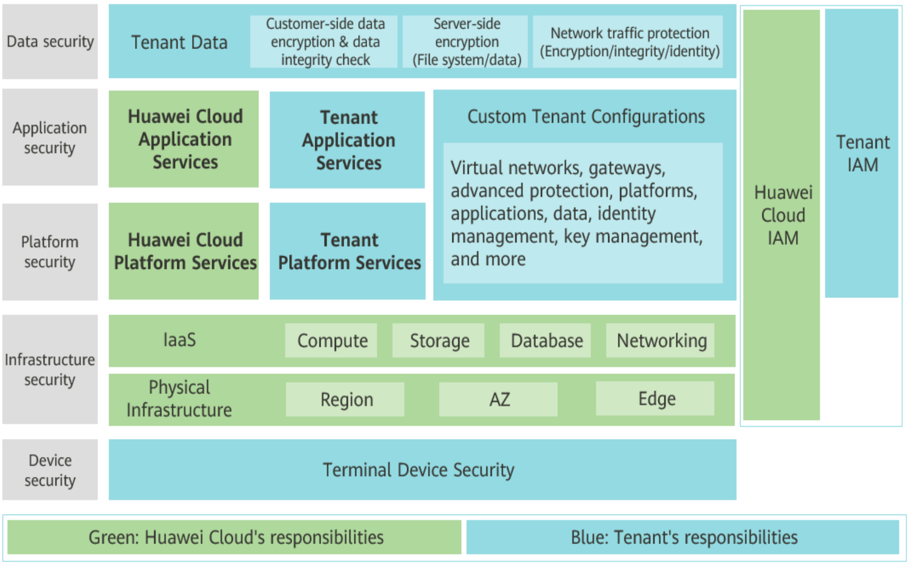
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 6-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

6.2 Asset Identification and Management

The following table lists the main assets managed using DEW and how they are managed.

Subservice	Asset	How to Manage
KMS	Key	Keys are protected by HSMs.
CSMS	Secret	Secrets are protected by HSMs.
KPS	Key pair	Key pairs are protected by HSMs.
Dedicated HSM	Dedicated HSM instance	The permissions of Dedicated HSM instances are controlled by users. HSMs are managed in the equipment rooms of the Huawei Cloud data center in a unified manner.

6.3 Identity Authentication and Access Control

Identity Authentication

You can access DEW through the DEW console, APIs, or SDK. Regardless of the access method, requests are sent through the REST APIs provided by DEW.

DEW APIs support multiple types of authentication requests. Take AK/SK as an example. An authenticated request must contain a signature value. The signature value is calculated based on the requestor's access key as the encryption factor and the specific information carried in the request body. OBS supports authentication using an AK/SK pair. It uses AK/SK-based encryption to authenticate requests. For details, see **Authentication**.

Access Control

- DEW uses Identity and Access Management (IAM) to implement refined access control. By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. After authorization, the user can perform specified operations on cloud services based on the permissions. For details, see **Permission Control**.
- For KMS subservices, you can configure their permissions on the KMS console. You can create grants for other IAM users or accounts to use their CMKs. You can create up to 100 grants on a CMK. For details, see **Managing a Grant**.

6.4 Data Protection Technologies

DEW takes different measures to keep data stored in DEW secure and reliable.

Measure	Description	Reference
Transmission encryption (HTTPS)	DEW uses HTTPS to enhance data transmission security.	**Making an API Request**
Key management	HSMs are used to manage and store key materials to prevent key leakage.	**Functions**
Envelope encryption	In scenarios where a large amount of data needs to be encrypted or decrypted, DEW provides envelope encryption to protect sensitive data in application systems. The data keys used for encryption are stored, transferred, and used with envelopes.	**Encrypting or Decrypting a Large Amount of Data**
Key rotation mechanism	Keys that are widely or repeatedly used are insecure. DEW allows you to periodically rotate keys and change the key materials to comply with encryption best practices.	**About Key Rotation**
Secret management	DEW provides secret lifecycle management and supports secure, convenient application access, helping you reduce secret leakage risks caused by hard coding and improve data and asset security.	**Secret Management**
Secret import	Key materials imported to KMS can be encrypted using the RSAES_OAEP_SHA_256 or SM2_ENCRYPT algorithms.	**Importing Key Materials**

6.5 Audit and Logging

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

For details, see **What Is Cloud Trace Service?**

CTS can track DEW operations. For details, see **Audit Logs**.

6.6 Service Resilience

DEW implements fault isolation, data backup, and traffic control to improve service resilience and enhance user data security.

Fault Isolation

- The inter-region isolation design of DEW ensures that the faults in a region do not affect the DEW services in other regions.
- DEW servers and HSMs adopt the AZ-level DR design, so that the faults in an AZ do not affect DEW availability. In the case of a fault, DEW automatically shields the faulty AZ and switches traffic over to other another AZ, smoothly scheduling workloads.
- DEW servers and HSMs are deployed in cluster mode. If any single-server or single-HSM fault does not affect DEW availability.

Data Backup

DEW keys are replicated among multiple HSMs to avoid permanent key loss in the case of an HSM fault. DEW data (non-sensitive data) is replicated among multiple servers and database instances, and backed up in real time to prevent data loss.

Flow Control

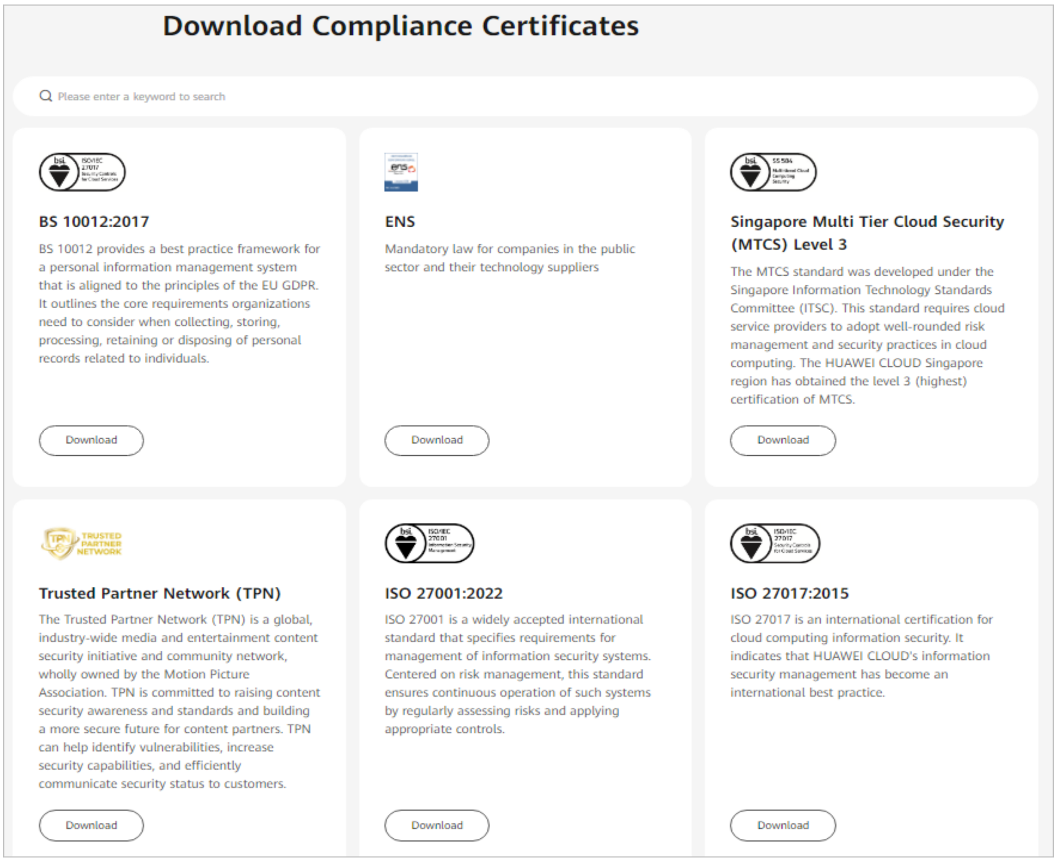
DEW can meet the SLA target of 99.95% availability and provide a large quota of API calls for each user. If a user has used up their quota of API calls, DEW will restrict their subsequent API calls to ensure service availability.

6.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

Figure 6-2 Downloading compliance certificates



Download Compliance Certificates

Please enter a keyword to search

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

ISO 27017:2015

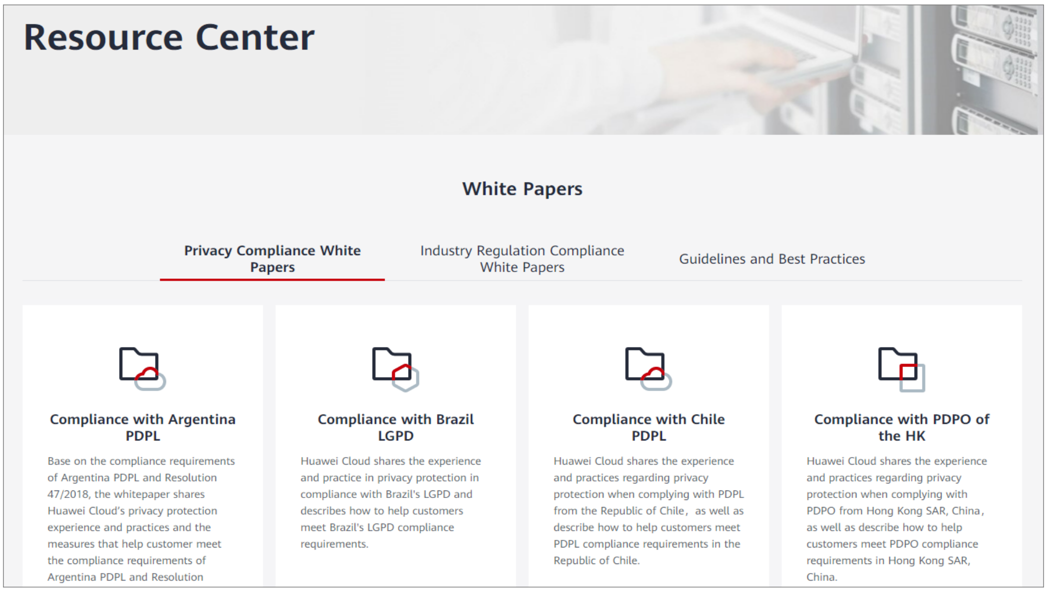
ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 6-3 Resource center



Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile， as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China， as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

7 Billing Description

Billing Item

DEW charges based on your usage and purchased edition.

Table 7-1 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 per use. 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 (outside Chinese mainland) For details, see **Editions**.
	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

  Key instances created or imported during the promotion period from October 1, 2021 to March 31, 2022 are permanently free of charge. Key instances created or imported after March 31, 2022 will be charged.

  KMS is charged per use. No minimum fee is required. Once a key is created, it will be charged . 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.

- CSMS

  You are billed per use. No minimum fee is required. After a secret is created, it is charged by day. You pay for the secrets you created and the API requests that exceed the free-of-charge threshold.

For price details, see **Product Pricing Details**.

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

  If your account is in arrears, you can check the details in the Billing Center. To prevent related resources from being stopped or released, top up your account in time. For details, see **Making Repayments (Prepaid Direct Customers)**.

FAQ

For more billing FAQs, see **DEW FAQs**.

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

IAM is free. You pay only for the resources in your account. For details about IAM, 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. When using roles to grant permissions, you must also assign other roles that the permissions depend on to take effect. 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**.

The following tables list all DEW system permissions.

Table 8-1 KMS system policies

Role/Policy	Description	Type	Dependency
KMS Administrator	All permissions of KMS	Role	None
KMS CMKFullAccess	All permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	Policy	None
KMS CMKReadOnlyAccess	Read-only permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	Policy	None

Table 8-2 KPS system policies

Role/Policy	Description	Type	Dependency
DEW KeypairFullAccess	All permissions for KPS. Users with these permissions can perform all the operations allowed by policies.	Policy	None
DEW KeypairReadOnlyAccess	Read-only permissions for KPS in DEW. Users with this permission can only view KPS data.	Policy	None

Table 8-3 CSMS system policies

Role/Policy	Description	Type	Dependency
CSMS FullAccess	All permissions for CSMS in DEW. Users with these permissions can perform all the operations allowed by policies.	Policy	None
CSMS ReadOnlyAccess	Read-only permissions for CSMS in DEW. Users with these permissions can perform all the operations allowed by policies.	Policy	None

📖 NOTE

The DEW KeypairFullAccess and DEW KeypairReadOnlyAccess policies used for enterprise project authorization do not take effect for individual users.

If you are an individual user and need to use enterprise project authorization, ensure that you are added to a user group, and authorize the user group.

Table 8-4 lists the common operations supported by each system-defined permission of DEW. Select the permissions as needed.

Table 8-4 Common operations supported by each system-defined policy or role of KMS

Operation	KMS Administrator	KMS CMKFullAccess
Create a key	√	√
Enable a key	√	√
Disable a key	√	√
Schedule key deletion	√	√
Cancel scheduled key deletion	√	√
Modify a key alias	√	√
Modify key description	√	√
Generate a random number	√	√
Create a DEK	√	√
Create a plaintext-free DEK	√	√
Encrypt a DEK	√	√
Decrypt a DEK	√	√

Operation	KMS Administrator	KMS CMKFullAccess
Obtain parameters for importing a key	√	√
Import key materials	√	√
Delete key materials	√	√
Create a grant	√	√
Revoke a grant	√	√
Retire a grant	√	√
Query the grant list	√	√
Query retirable grants	√	√
Encrypt data	√	√
Decrypt data	√	√
Send signature messages	√	√
Authenticate signature	√	√
Enable key rotation	√	√
Modify key rotation interval	√	√
Disable key rotation	√	√
Query key rotation status	√	√
Query CMK instances	√	√
Query key tags	√	√
Query project tags	√	√
Batch add or delete key tags	√	√
Add tags to a key	√	√
Delete key tags	√	√
Query the key list	√	√
Query key details	√	√
Query a public key	√	√
Query instance quantity	√	√
Query quotas	√	√
Query the key pair list	x	x

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

Related Links

- **What Is IAM**
- **Creating a User and Authorizing the User the Permission to Access DEW**
- **Permissions Policies and Supported Actions**

9 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*.

10 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.

SFS

Scalable File Service (SFS) provides high-performance file storage (NAS) that can be expanded on demand. KMS provides central management and control capabilities of CMKs for SFS. It is used for file system encryption in SFS.

Relational Database Service (RDS) is a cloud database that is reliable, scalable, easy to manage, and immediately ready for use. KMS provides central management and control capabilities of CMKs for RDS. It is used for disk encryption in cloud databases.

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.

KPS 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 10-1 KMS operations recorded by CTS

Operation	Resource Type	Trace Name
Create a key	cmk	createKey
Create a DEK	cmk	createDataKey
Create a plaintext-free DEK	cmk	createDataKeyWithout-Plaintext
Enable a key	cmk	enableKey
Disable a key	cmk	disableKey
Encrypt a DEK	cmk	encryptDatakey
Decrypt a DEK	cmk	decryptDatakey
Schedule key deletion	cmk	scheduleKeyDeletion
Cancel scheduled key deletion	cmk	cancelKeyDeletion
Generate random numbers	rng	genRandom
Modify a key alias	cmk	updateKeyAlias

Operation	Resource Type	Trace Name
Modify key description	cmk	updateKeyDescription
Prompt risks about CMK deletion	cmk	deleteKeyRiskTips
Import key materials	cmk	importKeyMaterial
Delete key materials	cmk	deleteImportedKeyMaterial
Create a grant	cmk	createGrant
Retire a grant	cmk	retireGrant
Revoke a grant	cmk	revokeGrant
Encrypt data	cmk	encryptData
Decrypt data	cmk	decryptData
Add a tag	cmk	dealUnifiedTags
Delete a tag	cmk	dealUnifiedTags
Add tags in batches	cmk	dealUnifiedTags
Delete tags in batches	cmk	dealUnifiedTags
Enable key rotation	cmk	enableKeyRotation
Modify key rotation interval	cmk	updateKeyRotationInterval

Table 10-2 KMS operations recorded by CSMS

Operation	Resource Type	Trace Name
Create a secret	secret	createSecret
Update a secret	secret	updateSecret
Delete a secret	secret	forceDeleteSecret
Schedule the deletion of a secret	secret	scheduleDelSecret
Cancel the scheduled secret deletion	secret	restoreSecretFromDeletedStatus
Create a secret status	secret	createSecretStage
Update a secret status	secret	updateSecretStage
Delete a secret status	secret	deleteSecretStage
Create a secret version	secret	createSecretVersion

Operation	Resource Type	Trace Name
Download a secret backup	secret	backupSecret
Restore a secret backup	secret	restoreSecretFromBackupBlob
Update the secret version	secret	putSecretVersion
Start the secret rotation	secret	rotateSecret
Create a secret event	secret	createSecretEvent
Update a secret event	secret	updateSecretEvent
Delete a secret event	secret	deleteSecretEvent
Create a resource tag	secret	createResourceTag
Delete a resource tag	secret	deleteResourceTag

Table 10-3 KMS operations recorded by KPS

Operation	Resource Type	Trace Name
Create or import an SSH key pair	keypair	createOrImportKeypair
Delete an SSH key pair	keypair	deleteKeypair
Import a private key	keypair	importPrivateKey
Export a private key	keypair	exportPrivateKey
Bind an SSH key pair	keypair	bindKeypair
Unbind an SSH key pair	keypair	unbindKeypair
Clear private keys	keypair	clearPrivateKey

Table 10-4 KMS operations recorded by Dedicated HSM

Operation	Resource Type	Trace Name
Purchase an HSM instance	hsm	purchaseHsm
Configure an HSM instance	hsm	createHsm
Delete 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*.

11 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 11-1 lists the personal data generated or collected by DEW.

Table 11-1 Personal data

Type	Source	Can Be Modified	Mandatory
Tenant ID	● Tenant ID in the token when an operation is performed on the console. ● Tenant ID in the token when an API is invoked.	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
2023-06-30	This is the nineteenth official release. Added the description of HMAC key algorithm types in section **Functions**. Added the description of secret event notifications in section **Functions**. Added the description of secret change notification in section **Advantages**.
2022-11-22	This is the eighteenth official release. Added **Editions**.
2022-11-15	This is the seventeenth official release. Added **Security**.
2022-08-18	This is the sixteenth official release. Added the concepts about key pairs, private key pairs, and account key pairs in **What Is DEW?**.
2022-03-29	This is the fifteenth official release. Optimized the billing description in 1.8 "Billing Description".
2021-12-27	This is the fourteenth official release. Optimized functions in section **Functions**. Optimized the description in **Application Scenarios**.
2021-10-26	This is the thirteen official release. Added description about secret management in **CSMS**.

Released On	Description
2021-09-30	This is the twelfth official release. ● Added links to related documents in section **Application Scenarios**. ● Optimized the billing description in 1.10 "Billing Description".
2021-07-20	This is the eleventh official release. Optimized functions and features in **Functions**.
2021-06-10	This is the tenth official release. Added the table "Common operations supported by each system-defined policy or role" in **DEW Permission Management**.
2020-12-14	This is the ninth official release. Added **Personal Data Protection Mechanism**.
2020-05-27	This is the eighth official release. Added section 1.10 "Billing Description".
2020-02-10	This is the seventh official release. Modified DEW system policy names in section "Permissions Management" in chapter "Service Overview" based on IAM GUI changes: changed **DEW Keypair Admin** to **DEW KeypairFullAccess**, **DEW Keypair Viewer** to **DEW KeypairReadOnlyAccess**, and **KMS CMK Admin** to **KMS CMKFullAccess**.
2019-12-03	This is the sixth official release. Added section "RDS Server Encryption".
2019-07-04	This is the fifth official release. ● Added the usage process in **Using KMS**. ● Optimized **DEW Permission Management**.
2019-03-30	This is the fourth official release. Optimized the structure of the document to provide users with better reference.
2018-05-30	This is the third official release. ● Modified section "Functions": added description about binding, unbinding, resetting, and replacing a key pair. ● Added description about importing and exporting private keys in **Related Services**.

Released On	Description
2018-01-30	This is the second official release. ● Added section "SSH Key Pair." ● Modified section "Application Scenarios": added part "Authenticating Users Logging In to ECSs." ● Modified section "Functions": added descriptions about creating, importing, and deleting key pairs. ● Modified section **Using KMS**: added description about ECS. ● Modified section **Related Services**: added the description about the relationship with ECS
2017-12-31	This is the first official release.