Data Encryption Workshop

Service Overview

Issue 07
Date 2020-02-10
## Contents

1 What Is DEW? ........................................................................................................................... 1

2 KMS ............................................................................................................................................. 3
   2.1 Functions ............................................................................................................................. 3
   2.2 Product Advantages .......................................................................................................... 4
   2.3 Application Scenarios ...................................................................................................... 4
   2.4 Using KMS ....................................................................................................................... 7
   2.5 Cloud Services with KMS Integrated .............................................................................. 10
      2.5.1 Encrypting Data in OBS .......................................................................................... 10
      2.5.2 Encrypting Data in EVS .......................................................................................... 11
      2.5.3 Encrypting Data in IMS .......................................................................................... 11
      2.5.4 Encrypting Data in RDS ......................................................................................... 12

3 KPS ........................................................................................................................................... 13
   3.1 Functions .......................................................................................................................... 13
   3.2 Product Advantages .......................................................................................................... 14
   3.3 Application Scenarios ...................................................................................................... 14

4 Dedicated HSM ..................................................................................................................... 15
   4.1 Functions .......................................................................................................................... 15
   4.2 Product Advantages .......................................................................................................... 16
   4.3 Application Scenarios ...................................................................................................... 16

5 Permissions Management .................................................................................................... 19

6 How to Access ....................................................................................................................... 21

7 Related Services ................................................................................................................... 22

A Change History .................................................................................................................... 25
1 What Is 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 covers Key Management Service (KMS), Key Pair Service (KPS), and Dedicated Hardware Security Module (Dedicated HSM). 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.

KMS

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

KPS

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).

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.

Dedicated HSM

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 certified by China State Cryptography Administration (CSCA), 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.
2.1 Functions

Key Management Service (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
- You can use the API to perform the following operations:
  - Creating, encrypting, or decrypting data encryption keys (DEKs)
  - Retiring grants
  
  For 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.

KMS supported cryptographic algorithms

Keys created on the KMS console use the AES-256 algorithm.
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

Small Data Encryption and Decryption

You can use the online tool on the KMS console or call the KMS APIs to directly encrypt or decrypt a small-size 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.
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.
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.
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.

2.4 Using KMS

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.
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 2-1 List of cloud services that use KMS encryption

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Storage Service (OBS)</td>
<td>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 <em>Object Storage Service Console Operation Guide</em>.</td>
</tr>
<tr>
<td>Elastic Volume Service (EVS)</td>
<td>If you enable the encryption function when creating an EVS disk and select a CMK provided by KMS to encrypt the EVS disk, data stored to the EVS disk is automatically encrypted. For details about how to use the encryption function of EVS, see the <em>Elastic Volume Service User Guide</em>.</td>
</tr>
<tr>
<td>Image Management Service (IMS)</td>
<td>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 the <em>Image Management Service User Guide</em>.</td>
</tr>
<tr>
<td>Relational Database Service (RDS)</td>
<td>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 the <em>Relational Database Service User Guide</em>.</td>
</tr>
</tbody>
</table>

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. Figure 2-5 describes details. For more information, see *Object Storage Service User Guide*.

**Figure 2-5 OBS server-side encryption**

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, 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 details, 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 the 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](image)

- You can also call the RDS APIs to purchase encrypted database instances. For details, see the Relational Database Service User Guide.
3.1 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
an encryption 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. As you do not need to enter a password, the
password will not be intercepted, cracked, and leaked, and the server becomes
more secure.

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.

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
- SSH-2 key pairs created on the KPS console support only the **RSA-2048**
cryptography algorithms.
Keys imported to the KPS console support the following cryptographic algorithms:
- RSA-1024
- RSA-2048
- RSA-4096

### 3.2 Product Advantages

- **Reinforced Login Security**
  You can log in to a Linux ECS without entering a password, effectively preventing account from being disclosed due to password interception and cracking. As a result, the security of Linux ECSs is greatly improved.

- **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.

### 3.3 Application Scenarios

When purchasing an ECS running a Linux OS, 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 a Windows OS, 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 a Linux OS, 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

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

If your Elastic Cloud Server (ECS) runs a Windows OS, 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
4.1 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 certified by China State Cryptography Administration (CSCA), 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.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Common Cryptographic Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric Encryption Algorithm</td>
<td>AES, DES, and 3DES</td>
</tr>
<tr>
<td>Category</td>
<td>Common Cryptographic Algorithm</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>RSA, DSA, ECDSA, DH, and ECDH</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>SHA1, SHA256, and SHA384</td>
</tr>
</tbody>
</table>

### 4.2 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 has 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 China State Cryptography Administration (CSCA) certified and FIPS 140-2 validated level 3 HSMs for protection of your keys, guaranteeing high-performance encryption services to meet your stringent security requirements.
  - Dedicated HSM chips are exclusively used by each instance. Even if some hardware chips are damaged, the service are not affected.

- **Security compliance**
  Dedicated HSM provides the CSCA validated HSM instances, helping 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.

### 4.3 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 customer service.

**Figure 4-1 Architecture**

![Architecture Diagram](image)

**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.

Video Surveillance

Safe city and smart campus

Dedicated HSM can ensure the confidentiality of videos, facial images, vehicles, tracks, and personal data during storage, preventing data leakage.
5 Permissions 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 the access to your HUAWEI CLOUD resources.

With IAM, you can use your HUAWEI CLOUD account to create IAM users for your employees, and assign 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 information 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. Policies are currently under open beta testing. You can apply to use policies for fine-grained access control free of charge. For more information, see Applying for Policy-based Access Control.

- 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 also need to 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 define permissions based on APIs.

Table 5-1 lists all the system policies of DEW.

### Table 5-1 System-defined roles and policies supported by DEW

<table>
<thead>
<tr>
<th>Role/Policy Name</th>
<th>Description</th>
<th>Type</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMS Administrator</td>
<td>Users with this set of permissions can perform administrator operations on DEW.</td>
<td>System role</td>
<td>None</td>
</tr>
<tr>
<td>KMS CMKFullAccess</td>
<td>Users with this set of permissions have full permissions for encryption keys in DEW.</td>
<td>System policy</td>
<td>None</td>
</tr>
<tr>
<td>DEW KeypairFullAccess</td>
<td>Users with this set of permissions have full permissions for key pairs in DEW.</td>
<td>System policy</td>
<td>None</td>
</tr>
<tr>
<td>DEW KeypairReadOnlyAccess</td>
<td>Users with this set of permissions can view key pairs in DEW.</td>
<td>System policy</td>
<td>None</td>
</tr>
</tbody>
</table>

Helpful Links

- [IAM Service Overview](#)
- [Creating a User Group, a User, and Granting Permissions for DEW](#)
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 > Data Encryption Workshop.](image)

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

OBS

KMS provides central management and control capabilities of CMKs for Object Storage Service (OBS). It is applied to the function of server-side encryption with KMS-managed keys (SSE-KMS) on OBS.

EVS

KMS provides central management and control capabilities of CMKs for Elastic Volume Service (EVS). It is applied to the encryption function of EVS.

IMS

KMS provides central management and control capabilities of CMKs for Image Management Service (IMS). It is applied to the private image encryption function of IMS.

ECS

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.

CTS

Cloud Trace Service (CTS) provides you with a history of KMS 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 7-1 DEW operations supported by CTS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Resource Type</th>
<th>Trace Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a CMK</td>
<td>cmk</td>
<td>createKey</td>
</tr>
<tr>
<td>Operation</td>
<td>Resource Type</td>
<td>Trace Name</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Creating a DEK</td>
<td>cmk</td>
<td>createDataKey</td>
</tr>
<tr>
<td>Creating a plaintext-free DEK</td>
<td>cmk</td>
<td>createDataKeyWithoutPlaintext</td>
</tr>
<tr>
<td>Enabling a CMK</td>
<td>cmk</td>
<td>enableKey</td>
</tr>
<tr>
<td>Disabling a CMK</td>
<td>cmk</td>
<td>disableKey</td>
</tr>
<tr>
<td>Encrypting a DEK</td>
<td>cmk</td>
<td>encryptDataKey</td>
</tr>
<tr>
<td>Decrypting a DEK</td>
<td>cmk</td>
<td>decryptDataKey</td>
</tr>
<tr>
<td>Scheduling the deletion of a CMK</td>
<td>cmk</td>
<td>scheduleKeyDeletion</td>
</tr>
<tr>
<td>Canceling the scheduled deletion of a CMK</td>
<td>cmk</td>
<td>cancelKeyDeletion</td>
</tr>
<tr>
<td>Generating random numbers</td>
<td>rng</td>
<td>genRandom</td>
</tr>
<tr>
<td>Changing the alias of a CMK</td>
<td>cmk</td>
<td>updateKeyAlias</td>
</tr>
<tr>
<td>Changing the description of a CMK</td>
<td>cmk</td>
<td>updateKeyDescription</td>
</tr>
<tr>
<td>Prompting risks about CMK deletion</td>
<td>cmk</td>
<td>deleteKeyRiskTips</td>
</tr>
<tr>
<td>Importing key material</td>
<td>cmk</td>
<td>importKeyMaterial</td>
</tr>
<tr>
<td>Deleting key material</td>
<td>cmk</td>
<td>deleteImportedKeyMaterial</td>
</tr>
<tr>
<td>Creating a grant</td>
<td>cmk</td>
<td>createGrant</td>
</tr>
<tr>
<td>Retiring a grant</td>
<td>cmk</td>
<td>retireGrant</td>
</tr>
<tr>
<td>Revoking a grant</td>
<td>cmk</td>
<td>revokeGrant</td>
</tr>
<tr>
<td>Encrypting data</td>
<td>cmk</td>
<td>encryptData</td>
</tr>
<tr>
<td>Decrypting data</td>
<td>cmk</td>
<td>decryptData</td>
</tr>
<tr>
<td>Adding a tag</td>
<td>cmk</td>
<td>createKeyTag</td>
</tr>
<tr>
<td>Deleting a tag</td>
<td>cmk</td>
<td>deleteKeyTag</td>
</tr>
<tr>
<td>Adding or deleting tags in batches</td>
<td>cmk</td>
<td>batchCreateKeyTags</td>
</tr>
<tr>
<td>Batch deleting tags</td>
<td>cmk</td>
<td>batchDeleteKeyTags</td>
</tr>
<tr>
<td>Creating or importing an SSH key pair</td>
<td>keypair</td>
<td>createOrImportKeypair</td>
</tr>
<tr>
<td>Deleting an SSH key pair</td>
<td>keypair</td>
<td>deleteKeypair</td>
</tr>
<tr>
<td>Operation</td>
<td>Resource Type</td>
<td>Trace Name</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Importing a private key</td>
<td>keypair</td>
<td>importPrivateKey</td>
</tr>
<tr>
<td>Exporting a private key</td>
<td>keypair</td>
<td>exportPrivateKey</td>
</tr>
<tr>
<td>Purchasing an HSM instance</td>
<td>hsm</td>
<td>purchaseHsm</td>
</tr>
<tr>
<td>Configuring an HSM instance</td>
<td>hsm</td>
<td>createHsm</td>
</tr>
<tr>
<td>Deleting an HSM instance</td>
<td>hsm</td>
<td>deleteHsm</td>
</tr>
</tbody>
</table>

**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*.
## Change History

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-02-10</td>
<td>This is the seventh official release. Modified DEW system policy names in section &quot;Permissions Management&quot; in chapter &quot;Service Overview&quot; 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.</td>
</tr>
<tr>
<td>2019-12-03</td>
<td>This is the sixth official release. Added section &quot;RDS Server Encryption&quot;.</td>
</tr>
<tr>
<td>2019-07-04</td>
<td>This is the fifth official release. • Added the usage process in Using KMS. • Optimized Permissions Management.</td>
</tr>
<tr>
<td>2019-03-30</td>
<td>This is the fourth official release. Optimized the structure of the document to provide users with better reference.</td>
</tr>
<tr>
<td>2018-05-30</td>
<td>This is the third official release. • Modified section &quot;Functions&quot;: added description about binding, unbinding, resetting, and replacing a key pair. • Added description about importing and exporting private keys in Related Services.</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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. |