Cloud Certificate Manager

Service Overview

Issue 08

Date 2024-10-11

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

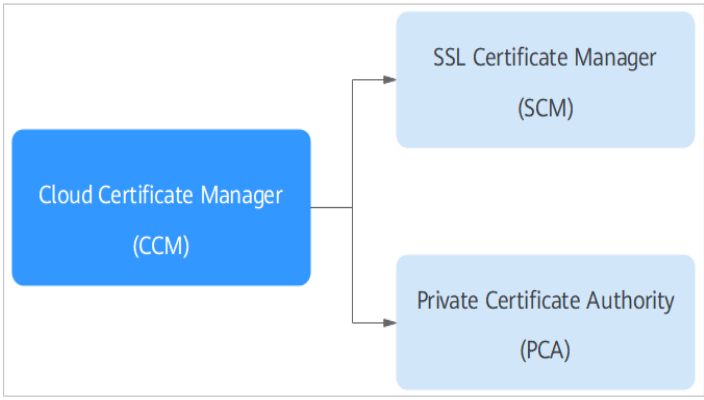
Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is Cloud Certificate Manager?

Cloud Certificate Manager (CCM) is a service that issues certificates and manages the lifecycle of certificates in the cloud. CCM includes the SSL Certificate Manager (SCM) and Private Certificate Authority (PCA) services.

Figure 1-1 CCM



What Is SCM?

SCM is a platform to centrally manage your Secure Sockets Layer (SSL) certificates. Working with trusted Certificate Authorities (CAs) around the world, SCM enables one-stop SSL certificate lifecycle management and helps you improve trust and secure data transmission for your websites.

- What Is an SSL Certificate?

  An SSL certificate is an SSL-compliant digital certificate issued by a trusted CA.

  After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.

- Huawei Cloud SCM and HTTPS

  You can purchase an SSL certificate on Huawei Cloud SCM and submit an application to the corresponding CA. After the CA approves the application, it issues the SSL certificate you request. Then, you can download the SSL certificate and deploy it on your web server or directly use it for other Huawei

Cloud products. After this, data transfer between your customers and your web server or cloud service is encrypted over HTTPS.

- SSL certificates can help you:
  - Authenticate websites and ensure that data is sent to the correct clients and servers.
  - Set up encrypted connections between clients and servers, preventing data from being stolen or tampered with during transmission.

What Is PCA?

Private Certificate Authority (PCA) is a private certificate and CA management platform. You can use CCM to set up a complete CA hierarchy and use it to issue and manage private certificates for your organization. It is used to authenticate application identities and encrypt and decrypt data within your organization.

Certificates issued by a private CA are trusted only within your organization, but not the Internet.

2 Advantages

Quick SSL certificate issuance

One-click certificate request. You can purchase multiple SSL certificates of different CAs in one place.

Varied SSL certificate types from world-renowned CAs

A wealth of certificates issued by the world's leading digital CAs are available, such as OV, OV Pro, EV, EV Pro, and DV (Basic) certificates.

One-Stop SSL certificate management

SCM lets you easily apply for, manage, query, and verify certificates for use with other Huawei Cloud services. You can upload SSL certificates you have bought from third parties to CCM and manage all your certificates in one place. For those external certificates, you can query them, quickly use them for other cloud products, and enable expiration notifications.

Identity authentication

Using an SSL certificate to authenticate your website outperforms other encryption methods as visitors can view information about website owners and verify website identity. This builds trust between your website and visitors and guarantee them that they are not visiting a phishing website.

Quickly Deploying Certificates to Cloud Products

You can deploy an SSL certificate to other Huawei Cloud services (such as CDN, ELB, and WAF) you subscribe in just a few clicks.

Private CA Hosting

You can easily manage CAs and certificates on Huawei Cloud in pay-per-use billing mode without having to build or maintain complex CA infrastructures.

Complete CA Hierarchy

You can create a flexible CA hierarchy, including root CAs and subordinate CAs. External CAs are also supported to meet the deployment requirements of more applications.

Managing the Private Certificate Lifecycle

PCA allows you to centrally manage certificates and keys. It can manage millions of certificates, and quickly notify tenants of certificate status using the CRL to prevent certificate expiration.

Varied Key Algorithms for Private Certificates

PCA supports different key algorithms, such as RSA_2048, RSA_4096, EC_P256, and EC_P384. It supports the x.509 v3 certificate format and complies with the PKI and CA international standards.

Secure and Reliable Storage of Private Certificate Keys

PCA uses Key Management Service (KMS) and hardware security modules (HSMs) to store keys securely.

Flexible Integration of Private Certificate APIs

PCA provides you with great flexibility through abundant APIs that allow you to efficiently integrate and deploy products in the development environment.

3 Application Scenarios

Authenticating Websites

An SSL certificate validates the identity of a website on the Internet. If a website is not installed with an SSL certificate, the browser considers the website as insecure so that the website is hardly trusted by users and have few visitors. Visitors are more likely to explore a website secured with an SSL certificate because they believe the website is secure enough. Especially the websites that use OV or EV certificates, the CA validates the domain name ownership and enterprise identity before issuing a certificate, which effectively improves the website credibility.

Website Data Encryption

The data transmitted over HTTP always faces high risks of being disclosed, eavesdropped, or tampered with as HTTP cannot encrypt data in transit. SSL certificates covert your HTTP website to an HTTPS one. An HTTPS-secured website enables encrypted communication and effectively improves data transmission security.

Enabling of HTTPS on Huawei Cloud Services such as WAF, ELB, and CDN

CCM enables you to quickly deploy SSL certificates to your Huawei Cloud services, such as WAF, ELB, and CDN.

Accelerating Website Loading Speed

SSL certificates are compatible with HTTP/2 and can be used to quickly and dynamically load web page content.

Internal Application Data Security Control

You can use PCA to establish an internal certificate management system for your enterprise and issue and manage self-signed private certificates to authenticate identities, encrypt and decrypt data, and secure data transmission within the enterprise.

IoV

Telematics Service Providers (TSPs) can use PCA to issue a certificate to each vehicle terminal, thereby providing security capabilities such as authentication and encryption during vehicle-vehicle, vehicle-cloud, and vehicle-road interaction.

IoT

The Internet of Things (IoT) platform can use PCA to issue a certificate to each IoT device to implement IoT device identity verification and authentication, ensuring device access security in IoT scenarios.

4 Features

With CCM, you can quickly get your SSL certificate and use them to keep your website more secure and trustworthy.

SSL Certificate Manager (SCM)

Feature	Description
SSL certificate application and purchase	CCM provides six types of SSL certificates, including OV, professional OV (OV Pro), EV, professional EV (EV Pro), and DV (Basic) SSL certificates issued by trusted Certificate Authorities (CA) DigiCert, or GeoTrust.
Centralized SSL certificate management	CCM provides you with a one-stop management platform. You can upload certificates and private keys to our platform to centrally manage certificates, apply for review, view the domain names bound to certificates and certificate expiration time, change certificate names, and delete expired certificates, helping you improve certificate O&M efficiency. For details, see **Uploading an External Certificate**.
One-click SSL certificate deployment	You can deploy an SSL certificate to other Huawei Cloud products, such as CDN, ELB, and WAF, in just a few clicks.
SSL certificate revocation	CCM follows the standard certificate revocation process. After the CA approves your revocation request, the SSL certificates will be revoked securely.
Refund policies supported for SSL certificates	SCM supports seven-day unconditional full refund. For details, see **Unsubscribing from an SSL Certificate**.
Renewing an SSL Certificate	SSL certificates have a validity period. An SSL certificate issued by a CA is valid for one year. You need to renew the certificate before it expires. For details, see **Renewing an SSL Certificate**.

Private Certificate Authority (PCA)

Feature	Description
Hosting CAs on Huawei Cloud	PCA provides CAs and supports multiple key algorithms, including RSA_2048, RSA_4096, EC_P256, and EC_P384. It supports X.509 v3 certificates, as well as multi-level extension and multi-level authentication of CAs. It uses symmetric and asymmetric algorithms which are internationally used and comply with the PKI and CA international standards.
Private certificate lifecycle management	PCA allows you to apply for, download, and revoke private certificates. It can manage more than 10 million certificates.
Key lifecycle management	PCA uses Huawei Cloud Key Management Service (KMS) and Hardware Security Modules (HSMs) to protect CA keys. It supports the generation, update, deletion, and restoration of key pairs for software and hardware.
Certificate Revocation List (CRL) management	PCA periodically releases and updates a private certificate revocation list (CRL) to your OBS buckets for downloading. Applications, services, and devices can use CRLs to periodically check certificate status.
Automated API integration	PCA provides APIs to help you efficiently develop and deploy products.

5 Security

5.1 Shared Responsibilities

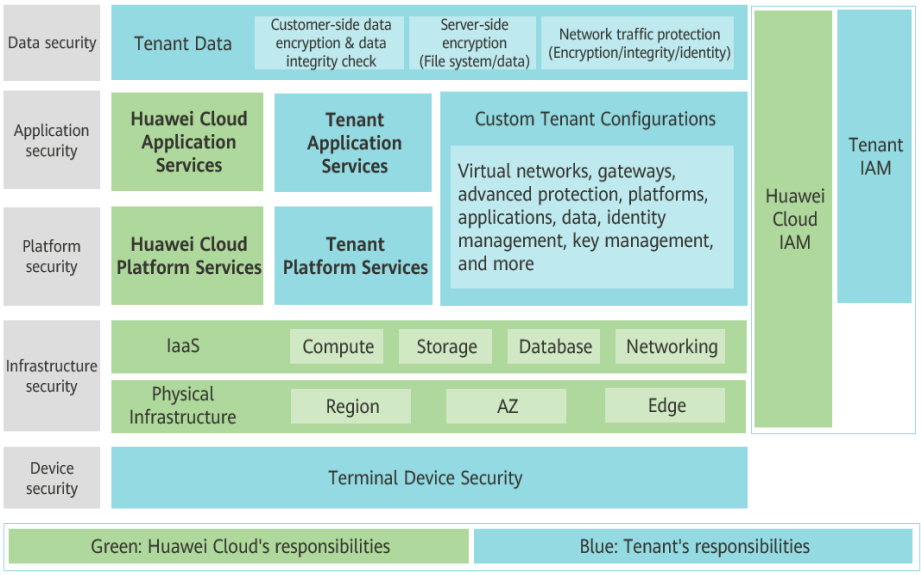
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 5-1 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 5-1 Huawei Cloud shared security responsibility model



5.2 Identity Authentication and Access Control

CCM works with Identity and Access Management (IAM). IAM permissions define which actions on your cloud resources are allowed and which actions are denied, to control access to your resources. With IAM, you can add users to a user group and configure policies to control their access to Huawei Cloud resources.

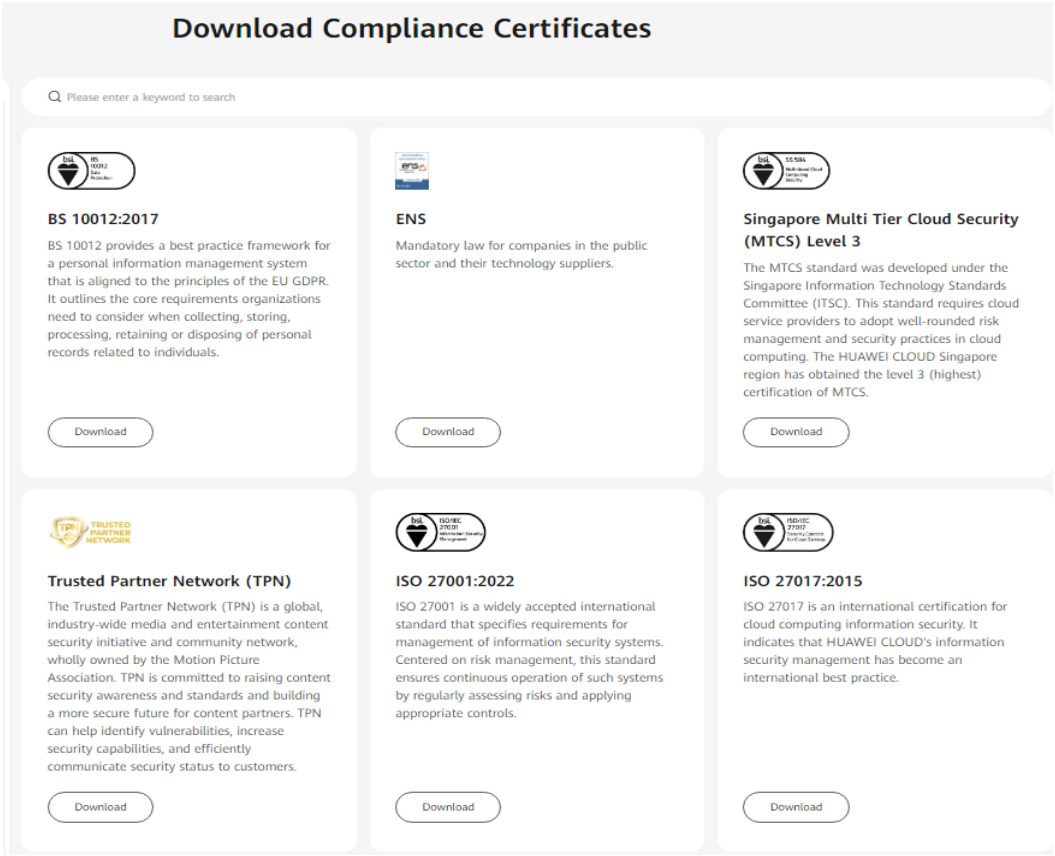
For details about CCM resource access permissions, see **Permissions Management**.

5.3 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.

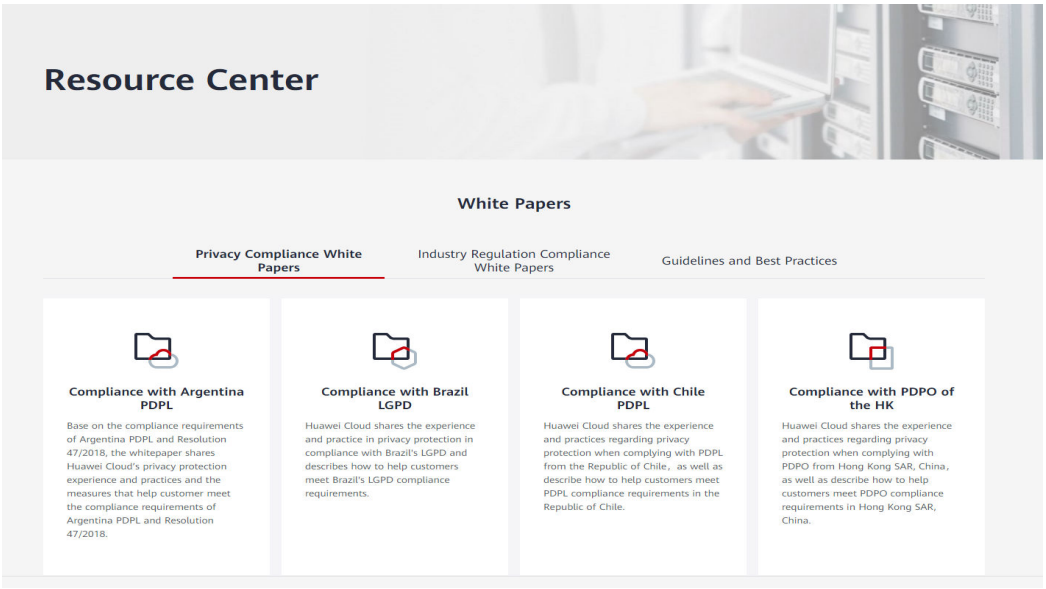
Figure 5-2 Downloading compliance certificates



Resource Center

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

Figure 5-3 Resource center



6 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your CCM resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage 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 CCM but not to delete CCM or its resources, then you can create an IAM policy to assign the developers the permission to access CCM but prevent them from deleting CCM related data.

If your Huawei Cloud account does not need individual IAM users for permissions management, you may skip over this topic.

IAM is free. You pay only for the resources in your account. For more information about IAM, see **What Is IAM**.

CCM 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 the groups to which they are added and can perform specified operations on cloud services based on the permissions.

CCM is a global service deployed for all physical regions. Therefore, CCM permissions are assigned to users in the Global project, and the users do not need to switch regions when accessing CCM.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. This mechanism provides a limited number of service-level roles for authorization. If one role has a dependency role required for accessing CCM, assign both roles to the users. Roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: A 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 and meets secure access control requirements. For example, you can grant CCM users the permissions to manage only a certain type of resources. Most policies define permissions based on APIs. For the API actions supported by CCM, see **Permissions Policies and Supported Actions**.

Table 6-1 lists the system-defined roles of CCM.

Table 6-1 System role supported by CCM

Role/Policy	Description	Type	Dependency
SCM Administrator	SCM administrator permissions. Users with SCM administrator permissions have all the permissions for the SCM service.	System-defined policy	The **Server Administrator** and **Tenant Guest** roles need to be assigned in the same project. BSS Administrator role is required for purchasing a certificate. BSS Administrator: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service. WAF FullAccess: system policy, which is the Web Application Firewall (WAF) administrator. ELB FullAccess: a system policy that has all permissions for Elastic Load Balance (ELB). CDN FullAccess: a system policy that has the permission to operate all fine-grained authentication interfaces of the Content Delivery Network (CDN). EPS FullAccess: a system-defined policy that has all Enterprise Project Management Service (EPS) permissions. OBS Administrator: a system policy, which is the Object Storage Service (OBS) administrator. DNS FullAccess: a system policy that has all permissions for Domain Name Service (DNS), including creating, deleting, querying, and modifying DNS resources.

Role/Policy	Description	Type	Dependency
SCM FullAccess	All permissions for SCM	System-defined policy	BSS Administrator role is required for purchasing a certificate. BSS Administrator: a system role, which is the administrator of the billing center (BSS) and has all permissions for the service. WAF FullAccess: system policy, which is the WAF administrator. ELB FullAccess: a system policy that has all permissions for Elastic Load Balance (ELB). CDN FullAccess: a system policy that has the permission to operate all fine-grained authentication interfaces of the Content Delivery Network (CDN). EPS FullAccess: a system-defined policy that has all Enterprise Project Management Service (EPS) permissions. OBS Administrator: a system policy, which is the Object Storage Service (OBS) administrator. DNS FullAccess: a system policy that has all permissions for Domain Name Service (DNS), including creating, deleting, querying, and modifying DNS resources.

Role/Policy	Description	Type	Dependency
SCM ReadOnlyAccess	Read-only permission for SCM. Users with the read-only permission can only query certificate information but cannot add, delete, or modify certificates.	System-defined policy	None.
PCA FullAccess	All permissions for PCA	System policy	BSS Administrator role is required for creating a private CA or private certificate. EPS FullAccess: a system-defined policy that has all Enterprise Project Management Service (EPS) permissions. OBS Administrator: a system policy, which is the Object Storage Service (OBS) administrator.

Table 6-2 lists the common operations supported by each system-defined policy of SCM. Select the proper system-defined policies as required.

NOTICE

To purchase a certificate, your account must have the BSS Administrator permission in addition to the SCM Administrator or SCM FullAccess permission.

BSS Administrator: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.

Table 6-2 Common operations for each system-defined policy or role of SCM

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
Querying the SSL certificate list	√	√	√

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
Querying the details of an SSL certificate	√	√	√
Querying the SSL certificate type	√	√	√
Querying details about SSL certificates of CAs	√	√	√
Withdrawing an SSL certificate application	√	√	x
Purchasing an SSL certificate	√	√	x
Applying for an SSL certificate	√	√	x
Restoring the information provided when applying for an SSL certificate	√	√	x
Obtaining the information provided when applying for an SSL certificates	√	√	√
Modifying an SSL certificate	√	√	x
Deleting an SSL certificate	√	√	x
Downloading an SSL certificate	√	√	x
Uploading authentication information	√	√	x
Revoking an SSL certificate	√	√	x
Pushing an SSL certificate to other services	√	√	x
Querying the record of SSL certificates pushed to other services	√	√	√
Uploading an SSL certificate	√	√	x
Verifying a CSR	√	√	x
Adding an additional domain name	√	√	x
Canceling privacy authorization	√	√	x
Reissuing an SSL certificate	√	√	x
Unsubscribing from an SSL certificate	√	√	x

Helpful Links

- What Is IAM?
- Creating a User Group, a User, and Granting SCM Permissions
- Creating a User Group, a User, and Granting PCA Permissions
- Supported Actions

7 SSL Certificate Selection

7.1 Differences Between SSL Certificate Types

SCM provides DV, OV, and EV SSL certificates.

This topic describes the differences between different types of certificates.

NOTE

Special enterprises cannot apply for OV or EV certificates. For example, military units, some government agencies, and national security departments.

To apply for OV and EV certificates, organizations must verify their identity through unified social credit code published on the national official website. While, special enterprises cannot verify their organization identity because there is no related details on that website.

Certificate Types

On SCM console, you can buy DV, OV, and EV SSL certificates. Different types of certificates are recommended for different scenarios to meet varied trust and security strength requirements. For details, see **Differences between certificate types**

Table 7-1 Differences between certificate types

Certificate Type	Security	Validation Requirements	Application Scenario	Supported Certificate Authority	Review Duration
DV	General	The CA verifies the domain name ownership only.	Testing websites of individuals or enterprises	• DigiCert • GeoTrust	Several hours

Certificate Type	Security	Validation Requirements	Application Scenario	Supported Certificate Authority	Review Duration
OV	High	The CA follows a standard process to validate the organization identity and the domain name ownership.	Service websites of education agencies, government departments, Internet companies, applications of small and medium-sized enterprises, and e-commerce platforms For example, Apple Store and WeChat applet.	• DigiCert • GeoTrust	3 to 5 working days
EV	Highest	CAs will verify the organization identity and the domain name ownership.	Websites of large enterprises, institutions, and organizations with strict security requirements For example, financial institutions, insurance agencies, and banks.	• DigiCert	7 to 10 working days

Certificate Authorities

The following table lists the CAs supported by SCM and the certificate types each CA provides.

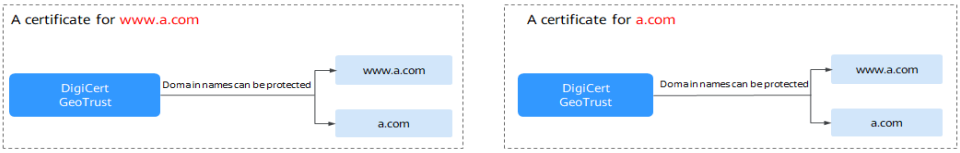
Table 7-2 Certificate authorities

Certificate Authority	Description	SSL DV Certificates Supported	SSL OV Certificates Supported	SSL EV Certificates Supported
DigiCert	DigiCert, formerly Symantec, is the world's largest CA. It provides services for more than 100,000 customers in over 150 countries and regions. Advantages: High security, stability, and compatibility. Suitable for digital transactions with high security requirements and widely used by financial institutions.	Yes Single-domain certificates supported	Yes Single-domain, multiple-domain, and wildcard-domain certificates supported	Yes Single-domain and multi-domain certificates supported
GeoTrust	GeoTrust, the world's second largest CA, is an industry-leading provider of identity and trust validation. It is committed to offering the best service at the lowest price possible to enterprises of all sizes. Advantages: Powered by DigiCert. High security, stability, and compatibility, cost-effective, and less know-how required for HTTPS protection	Yes Single-domain and wildcard-domain certificates supported	Yes Single-domain and wildcard-domain certificates supported	Yes Single-domain and multi-domain certificates supported

Promotion activities

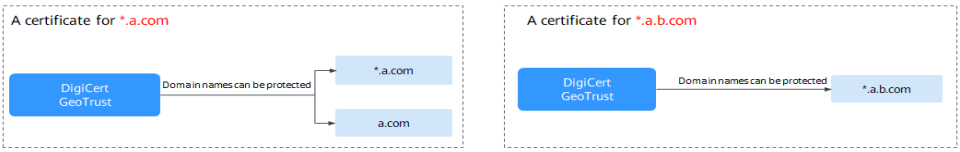
- Single domain names (using domain name www.a.com and root domain name a.com as an example)

Figure 7-1 Promotion activities



- Wildcard domain name (using domain names *.a.com and *.a.b.com as an example)

Figure 7-2 Promotion activities



Domain Name Types Supported in SCM

The following table describes how different types of SSL certificates are used for domain names.

Table 7-3 Domain type

Domain type	Description
Single domain	Only a single domain can be associated with an SSL certificate. For example, example.com.
Multiple domains	Multiple domain names can be associated with an SSL certificate. • You can associate a multi-domain certificate with up to 250 domain names. • A wildcard domain name is allowed only by OV or OV pro multi-domain certificates. Other types of multi-domain certificates can only associate with multiple single domain names • You can associate a multi-domain certificate with multiple domain names at different time points. For example, if you purchase a multi-domain certificate with three domain names, you can associate it with two domain names when applying for the certificate, and associate it with the last domain name after the certificate is issued. • The number of domain names a multi-domain certificate can protect depends on the domain quantity you configure when you buy the certificate. If you have more domain names to protect after the purchase completes, purchase another certificate for them.

Domain type	Description
Wildcard domain	Only one wildcard domain can be associated with an SSL certificate. Domain names having multiple wildcard characters, such as *.*.example.com, are not supported. Only one wildcard character is allowed in a wildcard domain name, for example, *.example.com, which may include domain names a.example.com, b.example.com, and more, but does not include a.a.example.com.
For details about how to select a domain type, see **How Do I Select an SSL Certificate?**	

Cryptographic Algorithms Supported in SCM

SSL certificates issued by CAs in CCM support RSA and ECC algorithms.

- **Rivest–Shamir–Adleman (RSA)** is an asymmetric cryptographic algorithm that is widely used around the world. It has the best compatibility among the three algorithms and supports mainstream browsers and all-platform OSs. Generally, RSA uses a 2048-bit or 3072-bit key.
- **Elliptical curve cryptography (ECC)** features faster encryption, higher efficiency, and lower server resource consumption compared with RSA. ECC is being promoted in mainstream browsers and is becoming a next-generation mainstream algorithm. Generally, ECC uses a 256-bit key.

For more details, see **Cryptographic algorithms supported**.

Table 7-4 Cryptographic Algorithms Supported in SCM

Certificate Authority	Certificate Type	Domain Type	Cryptographic Algorithm
DigiCert	DV (Basic)	Single domain	RSA_2048, RSA_3072, and RSA_4096
	OV	Single domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Multiple domains	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Wildcard domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
	OV Pro	Single domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384

Certificate Authority	Certificate Type	Domain Type	Cryptographic Algorithm
		Multiple domains	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Wildcard domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
	EV	Single domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Multiple domains	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
	EV Pro	Single domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Multiple domains	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
GeoTrust	DV (Basic)	Single domain	RSA_2048, RSA_3072, and RSA_4096
		Wildcard domain	RSA_2048, RSA_3072, and RSA_4096
	OV	Single domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		Wildcard domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384

7.2 Certificate Selection Cases

Table 7-5 The following are some typical certificate selection cases in the industry. You can refer to these cases when purchasing certificates.

Case	Industry	Scenario	Common Certificate Type
• Agriculture Bank of China • Ping An Insurance	Finance, banking, and insurance	• There are strict requirements for data confidentiality. • They expected to show their company identity information in the address bar of the browser.	EV
• Ministry of Education • Taobao and JD • Baidu, Sina, and Toutiao • Shanghai Stock Exchange • State Grid • Ministry of Foreign Affairs • Huawei Cloud	Education, government, and Internet	• There are strict requirements for data confidentiality. • They need to show their company identity information in the address bar of the browser. • Multiple new sites will be added to their websites.	OV wildcard-domain certificate
Personal websites	Individual service	• No data transmission service. • Websites are used to present only information or content	DV

8 Basic Concepts

8.1 Related Concepts in SCM

This topic describes the concepts related to Huawei Cloud SSL Certificate Manager (SCM).

Digital Certificate

A digital certificate is a file digitally signed by a CA and contains information about the owner of a public key and the public key. It is a trusted certificate issued by an authority to a website. The simplest certificate contains a public key, name, and digital signature of the CA. Another important feature of a digital certificate is that it is valid only within a specific period of time.

SSL Protocol

SSL is an encryption protocol that secures communication over a computer network. It establishes an encrypted channel between the browser and website to prevent information from being stolen or tampered with during transmission.

Certificate Authority

A Certificate Authority (CA) is an authority responsible for issuing and managing digital certificates. As a trusted third party in e-commerce transactions, the CA verifies the validity of public keys in the public key system.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a website encryption transmission protocol based on the SSL protocol. HTTPS activates an SSL encrypted channel between a web browser and a website server for a user to visit the website where an SSL certificate has been installed. The channel enables high-strength bidirectional encrypted transmission to prevent leakage or tampering of the data in transit. HTTPS is the secure version of HTTP.

CSR

A certificate signing request (CSR) is a message sent from an applicant to a CA to apply for an SSL certificate. A CSR file contains a public key and a distinguished name (DN). Typically, a CSR file is generated by a web server, and a pair of public and private keys are created along with the CSR file.

SSL Certificate Validity Period

From September 1, 2020, only one-year SSL certificates can be issued by CAs around the world. Therefore, the validity period of an SSL certificate you apply for through Huawei Cloud CCM is one year.

8.2 PCA-related Concepts

This topic describes the concepts related to Huawei Cloud Private Certificate Authority (PCA) service.

Root CA

The public key certificate of a CA. A root certificate is the trust anchor in the public key infrastructure (PKI) system. It can issue subordinate CAs, private certificates, and certificate revocation lists (CRLs). After a root CA is imported into the client trust list, the certificates issued by it can be validated as trusted.

Subordinate CA

A subordinate CA, or intermediate CA or child CA, is used to isolate the root CA from the private certificates. It is the key to divide the CA hierarchy. A subordinate CA validates certificates at the next layer in the certificate chain. If the path length of a subordinate CA is greater than 0, it can issue lower-layer subordinate CAs.

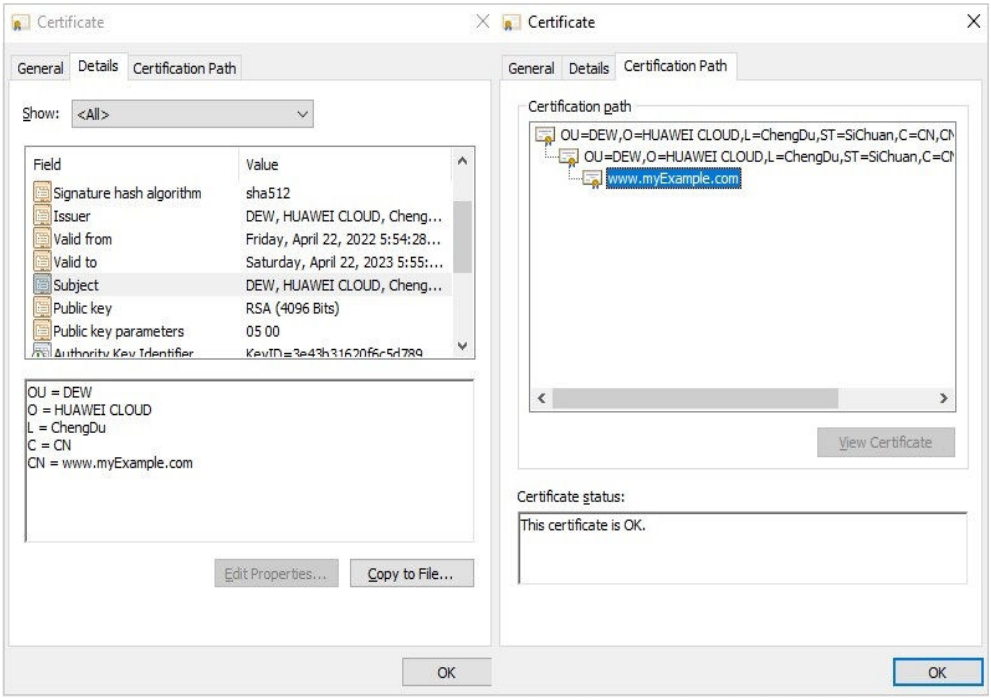
NOTE

The path depth of a subordinate CA controls how many layers of subordinate CAs the current CA can issue. (The last layer of the certificate chain is a private certificate).

Private certificate

A private certificate is an end-entity certificate, which is installed on an end entity, including certificates used for the client (or client certificates) and certificates used for the server (or server certificates). An end-entity certificate is at the bottom layer of a certificate chain and is used to authenticate an entity. It cannot be used to issue a certificate and is a credential for HTTPS communication between the entity that owns the certificate and other entities. **Figure 8-1** shows the content of a private certificate.

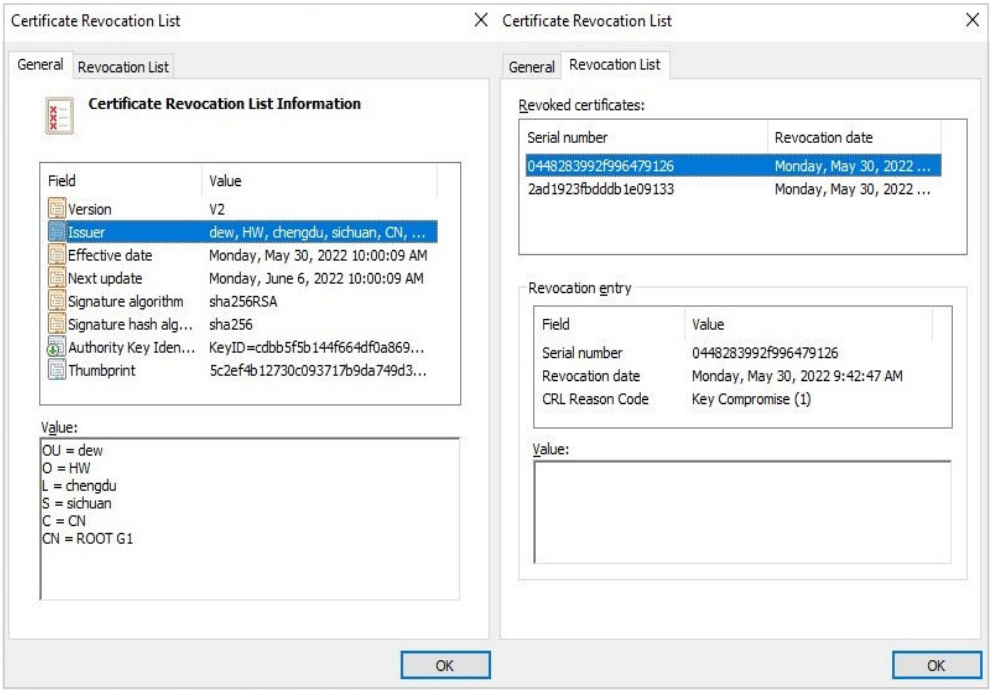
Figure 8-1 Private certificate



Certificate Revocation List (CRL)

A certificate revocation list (CRL) is a list of certificates revoked by the parent CA when they are still valid. The revoked certificates include subordinate CAs and private certificates. A CRL is a structured data file in a fixed format. It contains the issuer information, time when the CRL takes effect, time when the CRL is updated next time, issuing algorithm, fingerprint, as well as the serial number, revocation time, and revocation reason code of a revoked certificate. **Figure 8-2** provides more details.

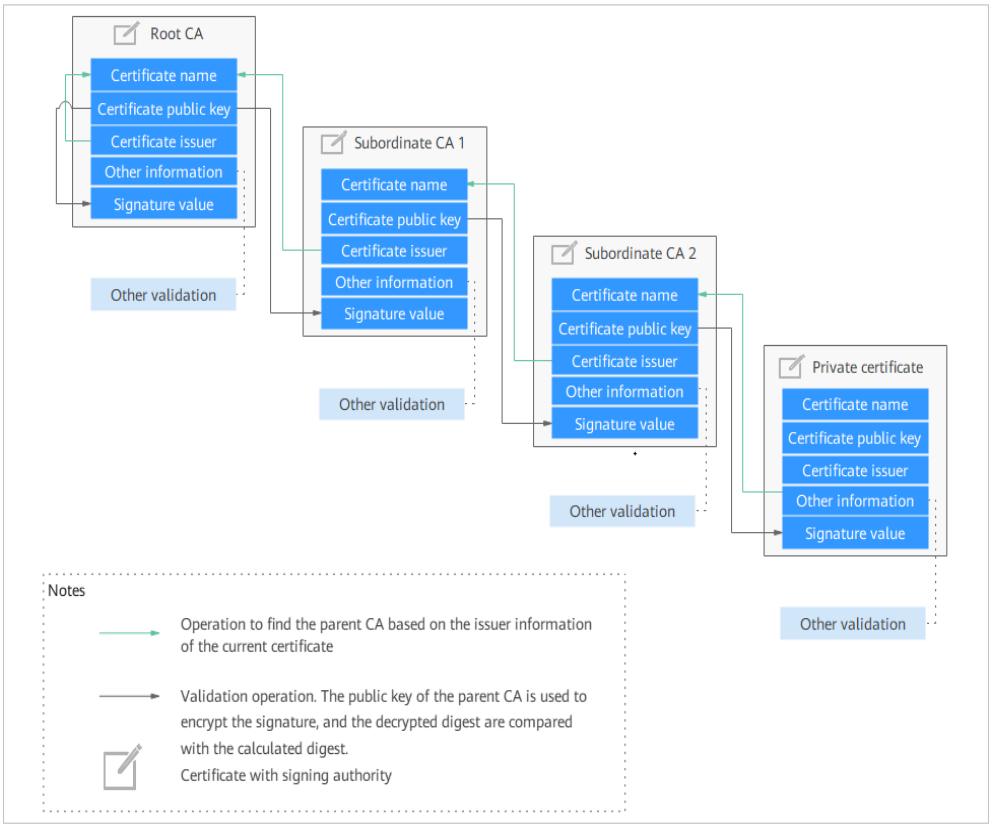
Figure 8-2 Certificate Revocation List (CRL)



Certificate chain

A certificate chain is a file that combines all certificates from the root CA to the private certificates in a fixed sequence. A certificate chain is used to validate certificates layer by layer. **Figure 8-3** shows an example certificate chain.

Figure 8-3 Certificate chain



Certificate validation involves the following aspects:

- Integrity of the certificate chain and validity of certificates
- Validity of the root CA, which is preinstalled in its trust store.

The following information is validated during the validation process:

- Subject the certificate owner claims, such as the domain name of the server
- Certificate validity period
- Key usage, such as key negotiation and digital signatures.
- Digital signature
- Whether the certificate has been revoked.

> **NOTE**
>
> Not all validation items are listed here. The X.509 certificate allows users to add multiple customized extension items. For details, see related international standards.

PCA Certificate Validity Period

In a certificate chain, the root CA is the trust anchor for all of the subordinate CAs and the end-entity certificates below it. Once the root CA expires, all certificates issued by the root CA and its subordinate CAs are no longer trusted. The validity period of the root CA is the upper limit of the validity period of all lower-layer certificates. Even if the validity period of a lower-layer certificate can be set to a value greater than that of the root CA (if not mandated), the certificate chain validation fails as long as the root CA in the chain expires.

In the PCA service, the validity period of a certificate cannot be longer than that of its parent CA. This ensures that the validity periods decrease gradually in the certificate chain from the root CA to the private certificate. **Table 8-1** lists the restrictions PCA places on validity periods of certificates.

The validity periods of different types of certificates vary depending on their roles. The more frequently a certificate is used, the higher the risk of key leakage is. Therefore, the validity period of frequently used certificate should be as short as possible. A root CA is used only to issue subordinate CAs. Root CAs are infrequently used, and the tightest protection measures are used for them. (KMS is used for CA key management in PCA). The validity period of a root CA is about 10 to 30 years. The lower the layer of a subordinate CA, the shorter the validity period. The subordinate CA at the lowest layer is used to issue private certificates, so its validity period is usually set to 2 to 5 years. A private certificate is frequently used during communications. The validity period of a private certificate can be set to several hours, months, or one or two years based on the security requirements of application scenarios.

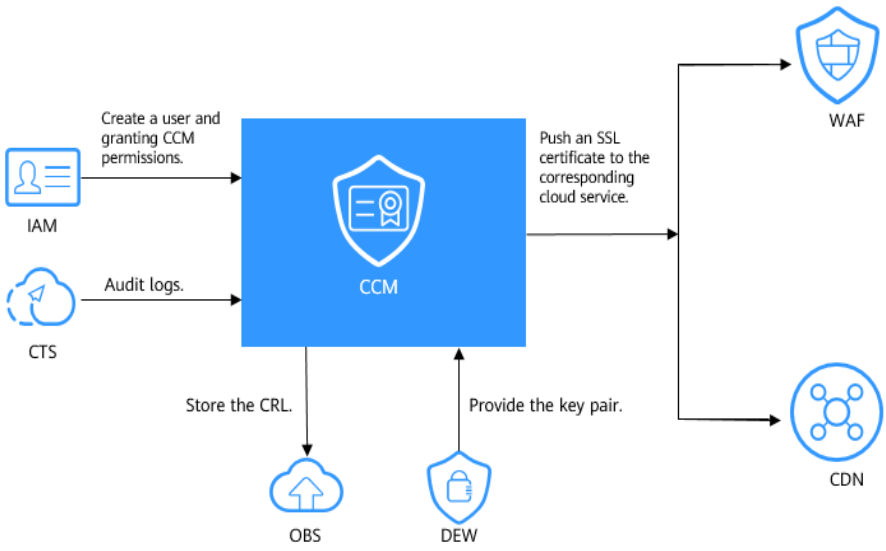
Table 8-1 Certificate validity period constraints

Certificate Type	Min. Validity Period	Max. Validity Period	Extension Supported	Remarks
Root CA	1 hour	30 years	No	None
Subordinate CA	1 hour	20 years	No	The root CA must within the validity period.
Private certificate	1 hour	20 years	No	The root CA must within the validity period.

9 Related Services

[Figure 9-1](#) shows the dependencies between CCM and other services.

Figure 9-1 CCM and related services



Web Application Firewall (WAF)

You can purchase SSL certificates on the SCM console and deploy them on WAF in just a few clicks.

Content Delivery Network (CDN)

You can purchase SSL certificates on the SCM console and deploy them on CDN in just a few clicks.

Object Storage Service (OBS)

OBS is an object-based cloud storage service. It provides massive, secure, highly reliable, and low-cost data storage capabilities. When you revoke a certificate in CCM, the CRL of the revoked certificate is stored in your OBS bucket for query.

Data Encryption Workshop (DEW)

DEW provides key pair generation and protection for CCM. For details, see **Data Encryption Workshop User Guide**.

Cloud Trace Service (CTS)

You can use CTS to record CCM operations for querying, auditing, or backtracking later. For details, see **Cloud Trace Service User Guide**.

Identity and Access Management (IAM)

IAM provides the permission management function for CCM.

Only users who have PCA FullAccess and SCM FullAccess permissions can use CCM.

To obtain the permissions, contact the users who have the Security Administrator permissions. For details, see **Identity and Access Management User Guide**.

10 Personal Data Protection

To ensure that your personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, CCM encrypts your personal data before storing it to control access to the data and records logs for operations performed on the data.

Personal Data

Table 10-1 lists the personal data generated or collected by CCM.

Table 10-1 Personal data

Type	Collection Method	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. The tenant ID is the certificate resource ID.
Name	Contact name entered when applying for an SSL certificate.	Yes	Yes. The contact name is mandatory in the manual verification phase.

Type	Collection Method	Can Be Modified	Mandatory
Email Address	Email address entered when applying for the SSL certificate or private certificate	• Email address entered when applying for an SSL certificate: Yes • Email address entered when applying for a private certificate: No	• Email address entered when applying for an SSL certificate: Yes. This parameter is mandatory in the manual review phase. • Email address entered when applying for a private certificate: No
Mobile number	Contact mobile number entered when applying for an SSL certificate.	Yes	Yes. The contact name is mandatory in the manual verification phase.
Enterprise's business license	When applying for an SSL certificate, you can upload the enterprise's business license.	Yes	No
Bank account opening permit	You can upload the bank account opening permit when applying for an SSL certificate.	Yes	No
Enterprise project ID	When applying for or using an SSL certificate or private certificate, you can assign an enterprise project to the certificate.	Yes	Enterprise project enabled: Yes Enterprise project enabled: No

Storage

CCM uses encryption algorithms to encrypt your sensitive data and stores encrypted data.

- Tenant IDs: Tenant IDs are not sensitive data and are stored in plaintext.
- Name, email address, and mobile number: encrypted for storage

Access Control

Token authentication is required for accessing your personal data in the CCM database.

Logging

CCM logs all operations involving personal data, such as editing, querying, and deleting personal data. The logs are uploaded to Cloud Trace Service (CTS). You can view only the logs for your operations.

