

Cloud Certificate & Manager

Service Overview

Issue 09
Date 2026-03-31



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

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 Infographics of Cloud Certificate & Manager (CCM)	1
2 What Is Cloud Certificate & Manager?	3
3 Advantages	5
4 Application Scenarios	7
5 Features	9
6 SSL Certificate Selection	11
6.1 Differences Between SSL Certificate Types.....	11
6.2 Certificate Selection Cases.....	18
7 Security	20
7.1 Identity Authentication and Access Control.....	20
7.2 Personal Data Protection.....	20
7.3 Audit and Logs.....	22
7.4 Monitoring Security Risks.....	22
7.5 Certificates.....	22
8 Permission Management	24
9 Related Services	35
10 Basic Concepts	37
10.1 SSL Certificate Concepts.....	37
10.2 Private CA and Private Certificate Concepts.....	38

1 Infographics of Cloud Certificate & Manager (CCM)



Getting to Know Cloud Certificate & Manager (CCM)



A Platform for Issuing and Managing Massive Certificates

01 What Is Cloud Certificate & Manager?

Cloud Certificate & Manager (CCM) is a service that provides **one-stop certificate lifecycle management**. It integrates **SSL Certificate Manager (SCM)** and **Private Certificate Authority (PCA)**, and provides issuance and unified management of massive certificates in scenarios such as public HTTPS security and intranet identity authentication.

02 Features

Certificate management

Covers the entire process of applying for, issuing, installing, and revoking SSL certificates and private certificates.



One-click deployment

You can deploy SSL certificates to other Huawei Cloud products, such as ELB, CDN, WAF, and VOD.



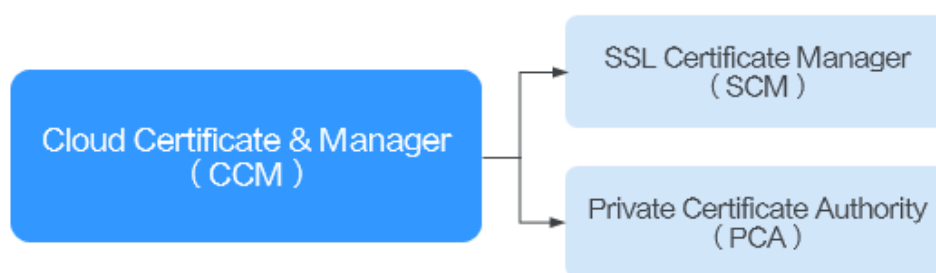
You can set up a complete **CA hierarchy** and issue and manage private certificates for your enterprise.

Domain name certificate **monitoring** monitors the **HTTPS status** of all sites and simplifies certificate maintenance.

2 What Is Cloud Certificate & Manager?

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

Figure 2-1 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.

3 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, VOD, 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.

4 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.

5 Features

With CCM, you can quickly get your SSL certificates 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 200 days. You need to renew the certificate before it expires. For details, see Renewing an SSL Certificate .

Feature	Description
SSL certificates download	<p>After an SSL certificate is issued, you can download it in SCM.</p> <p>You can install a downloaded SSL certificate on a server to establish a secure connection between your server and the client using SSL.</p>

Private Certificate Authority (PCA)

Feature	Description
Hosting CAs on Huawei Cloud	<p>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.</p>
Private certificate lifecycle management	<p>PCA allows you to apply for, download, and revoke private certificates. It can manage more than 10 million certificates.</p>
Key lifecycle management	<p>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.</p>
Certificate Revocation List (CRL) management	<p>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.</p>
Automated API integration	<p>PCA provides APIs to help you efficiently develop and deploy products.</p>

6 SSL Certificate Selection

6.1 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. 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 6-1 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	<ul style="list-style-type: none"> 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's 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.	<ul style="list-style-type: none"> • DigiCert • GeoTrust • GlobalSign 	3 to 5 working days
EV	Highest	CAs will verify the organization's identity and domain name ownership.	Websites of large enterprises, institutions, and organizations with strict security requirements For example, financial institutions, insurance agencies, and banks.	<ul style="list-style-type: none"> • DigiCert • GeoTrust • GlobalSign 	7 to 10 working days

Certificate Authorities

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

Table 6-2 Certificate authorities

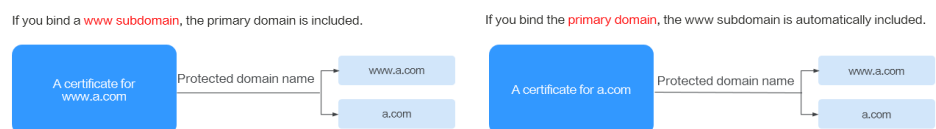
Certificate Authority	Description	SSL DV Certificates Supported	SSL OV Certificates Supported	SSL EV Certificates Supported
DigiCert	<p>DigiCert, formerly Symantec, is the world's largest CA. It provides services for more than 100,000 customers in over 150 countries and regions.</p> <p>Advantages: High security, stability, and compatibility. Suitable for digital transactions with high security requirements and widely used by financial institutions.</p>	<p>Yes</p> <p>Single-domain and wildcard-domain certificates supported</p>	<p>Yes</p> <p>Single-domain, multi-domain, wildcard-domain, and IP-address certificates supported</p>	<p>Yes</p> <p>Single-domain and multi-domain certificates supported</p>
GeoTrust	<p>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.</p> <p>Advantages: Powered by DigiCert. High security, stability, and compatibility, cost-effective, and less know-how required for HTTPS protection</p>	<p>Yes</p> <p>Single-domain and wildcard-domain certificates supported</p>	<p>Yes</p> <p>Single-domain, multi-domain, wildcard-domain, and IP-address certificates supported</p>	<p>Yes</p> <p>Single-domain and multi-domain certificates supported</p>

Certificate Authority	Description	SSL DV Certificates Supported	SSL OV Certificates Supported	SSL EV Certificates Supported
GlobalSign	<p>Founded in 1996, GlobalSign is one of the world's earliest CAs. A trusted CA of SSL digital certificates, they have partnered with many companies around the world.</p> <p>Advantages: Fast issuance and verification Widely used by large e-commerce enterprises (including Huawei Cloud), supported standard RSA+ECC algorithms, less resource required for installation</p>	No	Yes Single-domain, multi-domain, wildcard-domain, and IP-address certificates supported	Yes Single-domain and multi-domain certificates supported

Domain name reward rules:

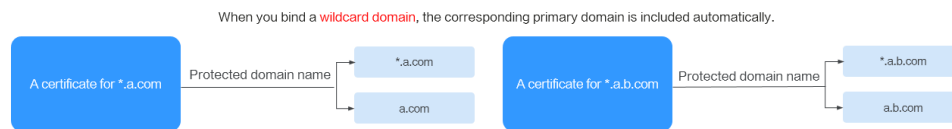
- Single-domain certificate, as shown in **Figure 6-1**:
 - When your certificate is used for the subdomain name www, the certificate can be used for the primary domain name the subdomain name matches. If you purchase a certificate for www.a.com, domain names www.a.com and a.com can be protected.
 - When your certificate is used for primary domain name, the certificate can be used for the subdomain name www the primary domain name matches. If you purchase a certificate for a.com, domain names www.a.com and a.com can be protected.

Figure 6-1 Single-domain reward rules



- Wildcard domain name certificate, as shown in **Figure 6-2**:
When your certificate is used for wildcard domain name, the certificate can be used for the primary domain name the wildcard domain name matches. For example, if you purchase a certificate for *.a.com, the certificate can protect *.a.com and a.com. If you purchase a certificate for *.a.b.com, the certificate can protect *.a.b.com and a.b.com.

Figure 6-2 Wildcard domain name reward rules



Domain Name Types Supported in SCM

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

Table 6-3 Domain types

Domain Type	Description
Single domain	Only a single domain can be associated with an SSL certificate. For example, example.com.
Multiple domains	<p>Multiple domain names can be associated with an SSL certificate.</p> <ul style="list-style-type: none"> 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.
Wildcard domain	<p>Only one wildcard domain can be associated with an SSL certificate. Domain names having multiple wildcard characters, such as *.*.example.com, are not supported.</p> <p>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.</p>
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 6-4 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
		Wildcard domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
	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
		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

Certificate Authority	Certificate Type	Domain Type	Cryptographic Algorithm
	EV Pro	Multiple domains	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		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
	DV	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
		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
	GlobalSign	OV	Single domain
Multiple domains			RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384

Certificate Authority	Certificate Type	Domain Type	Cryptographic Algorithm
		Wildcard domain	RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384
		IP address	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

6.2 Certificate Selection Cases

Table 6-5 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
<ul style="list-style-type: none"> • Agriculture Bank of China • Ping An Insurance 	Finance, banking, and insurance	<ul style="list-style-type: none"> • There are strict requirements for data confidentiality. • They expected to show their company identity information in the address bar of the browser. 	EV

Case	Industry	Scenario	Common Certificate Type
<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • No data transmission service. • Websites are used to present only information or content 	DV

7 Security

7.1 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](#).

7.2 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 7-1](#) lists the personal data generated or collected by CCM.

Table 7-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Tenant ID	<ul style="list-style-type: none"> 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.

Type	Collection Method	Can Be Modified	Mandatory
Name	Contact name entered when applying for an SSL certificate.	Yes	Yes. The contact name is mandatory in the manual verification phase.
Email Address	Email address entered when applying for the SSL certificate or private certificate	<ul style="list-style-type: none"> Email address entered when applying for an SSL certificate: Yes Email address entered when applying for a private certificate: No 	<ul style="list-style-type: none"> 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.

7.3 Audit and Logs

Monitoring is key to ensuring the reliability, availability, and performance of CCM. You can summarize operation logs of Huawei Cloud services for analysis, audit, resource monitoring, and fault locating.

CCM interworks with Cloud Trace Service (CTS). Huawei Cloud CTS collects, stores, and queries resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

For details about how to enable and use CTS, see [Getting Started](#).

7.4 Monitoring Security Risks

CCM interworks with Cloud Eye. Cloud Eye is a multi-dimensional monitoring platform provided by Huawei Cloud for a wide range of cloud resources. With Cloud Eye, you can learn about the resource usage and service running status on the cloud, receive alarms in a timely manner, and respond quickly to exceptions to keep your cloud services stable.

For details about how to enable and use CES, see [Getting Started](#).

7.5 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 7-1 Downloading compliance certificates

Download Compliance Certificates

Please enter a keyword to search

 <p>BS 10012:2017</p> <p>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.</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>	 <p>ENS</p> <p>Mandatory law for companies in the public sector and their technology suppliers</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>	 <p>Singapore Multi Tier Cloud Security (MTCS) Level 3</p> <p>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.</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>
 <p>Trusted Partner Network (TPN)</p> <p>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.</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>	 <p>ISO 27001:2022</p> <p>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.</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>	 <p>ISO 27017:2015</p> <p>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.</p> <p style="text-align: center; border: 1px solid #ccc; border-radius: 10px; width: 60px; margin: 0 auto;">Download</p>

Resource Center





Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 7-2 Resource center

Resource Center

White Papers

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

 <p>Compliance with Argentina PDPL</p> <p style="font-size: x-small;">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</p>	 <p>Compliance with Brazil LGPD</p> <p style="font-size: x-small;">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.</p>	 <p>Compliance with Chile PDPL</p> <p style="font-size: x-small;">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.</p>	 <p>Compliance with PDPO of the HK</p> <p style="font-size: x-small;">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.</p>
--	---	--	--

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

Huawei Cloud IAM is a free service. You only pay for the resources in your account.

With IAM, you can control access to specific Huawei Cloud resources. For example, some developers in your enterprise need to use CCM but you do not want them to have permissions to perform high-risk operations such as deleting CCM. To achieve such purpose, you can use IAM to grant them only the permissions to use CCM, but not delete CCM. With IAM, you can control their usage of CCM resources.

IAM supports role/policy-based authorization and identity policy-based authorization.

The following table describes the differences between these two authorization models.

Table 8-1 Differences between the two types of authorization

Name	Core Relationship	Permission	Authorization Method	Application Scenario
Role/Policy-based Authorization	User-permission-authorization scope	<ul style="list-style-type: none"> • System-defined role • System-defined policy • Custom policy 	Assigning roles or policies to principals	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It provides a limited number of condition keys and cannot meet the requirements of fine-grained permissions control. This method is suitable for small- and medium-sized enterprises.
Identity Policy-based Authorization	User-policy	<ul style="list-style-type: none"> • System-defined identity policies • Custom identity policies 	<ul style="list-style-type: none"> • Assigning identity policies to principals • Attaching identity policies to principals 	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users permission to create the ECS in CN North-Beijing4 and the OBS in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the users or grant the users the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization models are not interoperable. You are advised to use the identity policy-based authorization model. For details about system-defined permissions, see [Role/Policy-based Permissions Management](#) and [Identity Policy-based Permissions Management](#).

For more information about IAM, see [IAM Service Overview](#).

Role/Policy-based Permissions Management

CCM supports role/policy-based authorization. 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. CCM permissions are assigned to IAM users in the global project, so IAM users can access CCM in any region without having to switch over among regions.

Table 8-2 lists all CCM system permissions. System-defined policies in role/policy-based authorization are not interoperable with those in identity policy-based authorization.

Table 8-2 CCM system permissions

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

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

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-defined 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 8-3 describes the common operations supported by each system-defined permission of CCM.

Table 8-3 Common operations for each system-defined policy or role of SCM

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

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
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 certificate	√	√	√
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

Operation	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
Unsubscribing from an SSL certificate	√	√	x

Identity Policy-based Permissions Management

CCM supports identity policy-based authorization. [Table 8-4](#) lists all the system-defined identity policies for CCM. System-defined policies in identity policy-based authorization are not interoperable with those in role/policy-based authorization.

Table 8-4 System-defined identity policies of CCM

Identity Policy Name	Description	Role Type
SCMReadOnlyPolicy	Read-only permissions for SCM.	System-defined identity policies
SCMFullPolicy	Administrator permissions for SCM.	System-defined identity policies
PCAFullAccessPolicy	All permissions for PCA	System-defined identity policies
PCAReadingOnlyPolicy	Read-only permissions for PCA	System-defined identity policies

[Table 8-5](#) and [Table 8-6](#) describe the common operations supported by system-defined identity policies of CCM.

Table 8-5 Common operations for each system-defined policy or role of SCM

Operation	SCMFullPolicy	SCMReadOnlyPolicy
Querying the SSL certificate list	√	√
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

Operation	SCMFullPolicy	SCMReadOnlyPolicy
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 certificate	√	√
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

Operation	SCMFullPolicy	SCMReadOnlyPolicy
Unsubscribing from an SSL certificate	√	x

Table 8-6 Common operations for each system-defined policy or role of PCA

Operation	PCAFullAccessPolicy	PCAReadOnlyPolicy
Querying the CA list	√	√
Creating a CA	√	x
Querying CA quotas	√	x
Querying CA details	√	√
Deleting a CA	√	x
Activating a CA	√	x
Exporting a CSR of a CA	√	x
Disabling a CA	√	x
Enabling a CA	√	x
Exporting a CA certificate	√	x
Importing a CA certificate	√	x
Restoring a CA	√	x
Revoking a CA	√	x
Querying the list of private certificates	√	√
Applying for a certificate	√	x
Issuing a certificate through a CSR	√	x
Parsing a CSR	√	x
Querying the private certificate quota	√	x
Querying details of a certificate	√	√
Deleting a certificate	√	x
Exporting a certificate	√	x

Operation	PCAFullAccessPolicy	PCAReadOnlyPolicy
Revoking a certificate	√	x

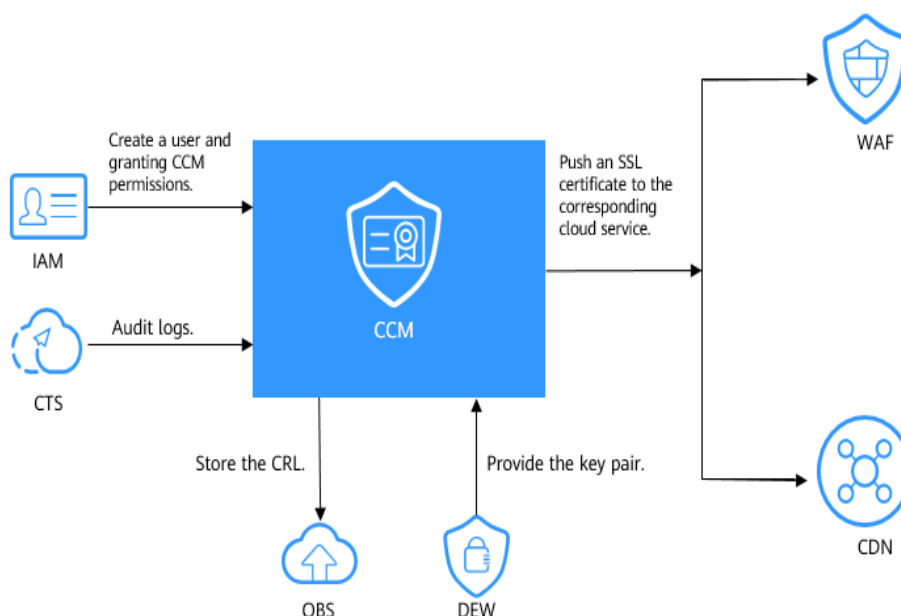
Helpful Links

- [IAM Service Overview](#)
- [Using IAM to Grant Access to SCM](#)
- [Using IAM to Grant Access to PCA](#)
- [Actions Supported by Identity Policy-based Authorization](#)

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.

Video on Demand (VOD)

You can purchase SSL certificates on the SCM console and deploy them on VOD 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 \(DEW\) 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 Basic Concepts

10.1 SSL Certificate Concepts

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

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 contains a public key and a distinguished name (DN). Typically, a CSR is generated by a web server. A pair of public and private keys are created along with the CSR. For details, see [Creating a CSR](#).

SSL Certificate Validity Period

From March 15, 2026, the maximum validity period of SSL certificates issued by global CAs is 200 days. To prevent certificate expiration from affecting service functions, renew the certificate in time. For details, see [Renewing an SSL Certificate](#).

10.2 Private CA and Private Certificate Concepts

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

Private Certificate Authority (PCA) is a private CA and certificate 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 an organization.

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. For details about how to obtain the root CA, see [Activating a Private CA](#).

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. For details about how to obtain a subordinate CA, see [Activating a Private CA](#).

NOTE

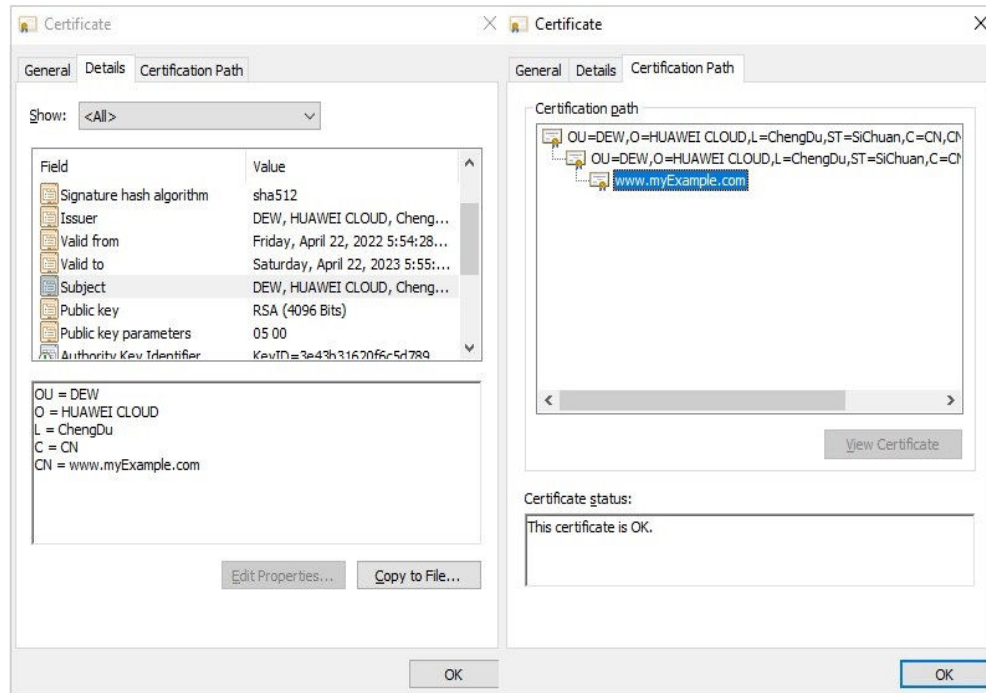
The path depth of a subordinate CA controls how many layers of subordinate CAs the current CA can issue. (The last layer of the certificate chain is a private certificate).

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 10-1](#) shows the content of a private certificate. For details about how to obtain a private certificate, see [Applying for a Private Certificate](#).

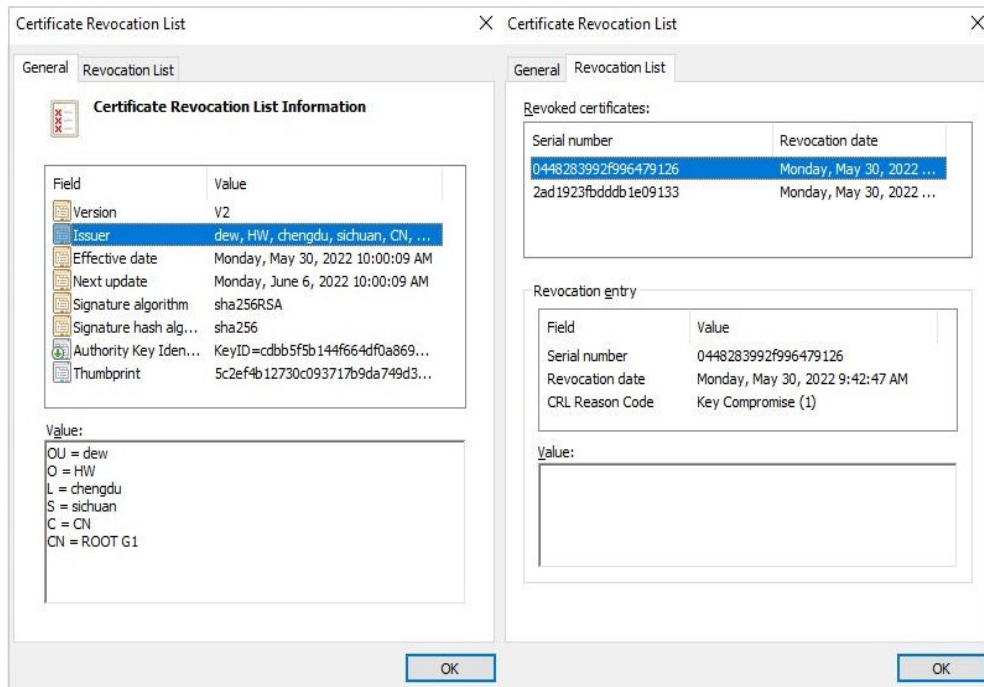
Figure 10-1 Private certificate



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 CAs and 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 10-2](#) provides more details. For details about how to configure a CRL, see [Configuring a CRL](#).

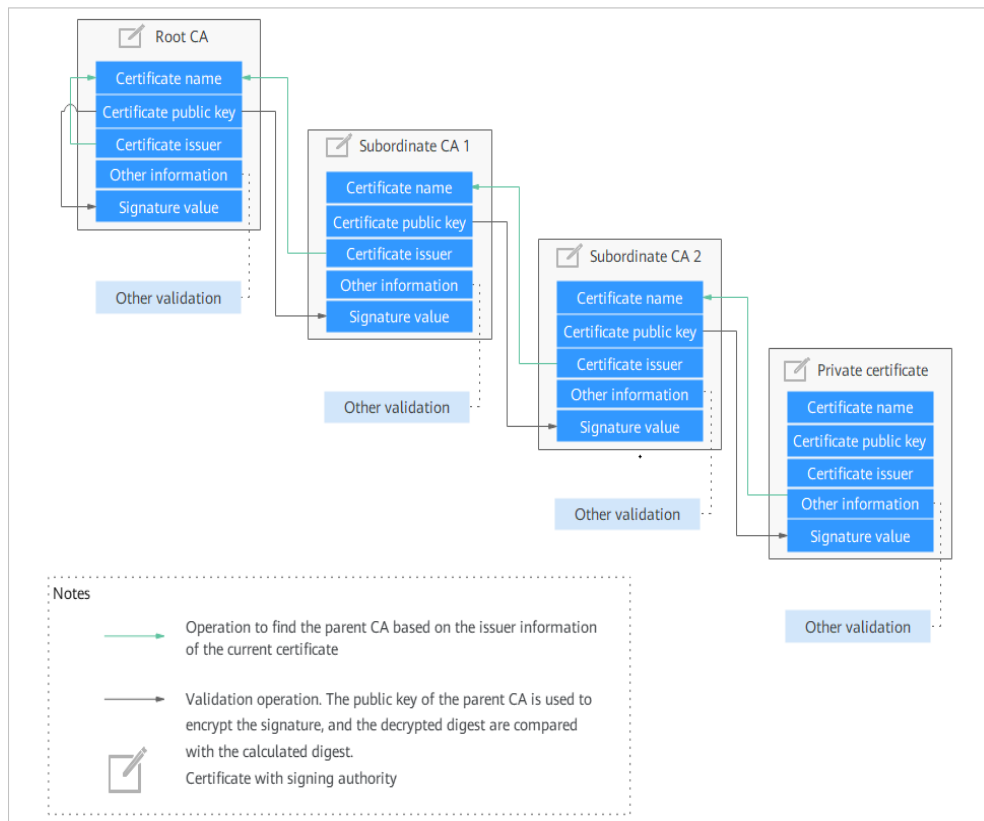
Figure 10-2 Certificate Revocation List (CRL)



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 10-3](#) shows an example certificate chain.

Figure 10-3 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 10-1** 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 10-1 Certificate validity period constraints

CA/ Certificate	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.