ALIBABA CLOUD

# Alibaba Cloud

## SSL Certificates

## Product Introduction

Document Version: 20220622

Alibaba Cloud

# Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
| Danger | A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results. | **Danger:** Resetting will result in the loss of user configuration data. |
| Warning | A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results. | **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance. |
| Notice | A caution notice indicates warning information, supplementary instructions, and other content that the user must understand. | **Notice:** If the weight is set to 0, the server no longer receives new requests. |
| Note | A note indicates supplemental instructions, best practices, tips, and other content. | **Note:** You can use Ctrl + A to select all files. |
| > | Closing angle brackets are used to indicate a multi-level menu cascade. | Click **Settings**> **Network**> **Set network type**. |
| **Bold** | Bold formatting is used for buttons , menus, page names, and other UI elements. | Click **OK**. |
| `Courier font` | Courier font is used for commands | Run the `cd /d C:/window` command to enter the Windows system folder. |
| *Italic* | Italic formatting is used for parameters and variables. | `bae log list --instanceid` *Instance_ID* |
| [] or [a\|b] | This format is used for an optional value, where only one item can be selected. | `ipconfig [-all\|-t]` |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | `switch {active\|stand}` |

# Table of Contents

# 1.What is Certificate Management Service?

Certificate Management Service is a digital certificate service provided by Alibaba Cloud in cooperation with certificate authorities (CAs) across the world. This service allows you to purchase and manage certificates in the Certificate Management Service console. Certificate Management Service allows you to manage your SSL certificates throughout their entire lifecycles at lower costs and helps ensure the security of data transmission for your websites and apps.

## Relationship between Certificate Management Service and HTTPS

You can purchase a certificate in the Certificate Management Service console and submit a certificate application to the CA for review. After the certificate is issued, you can install the certificate on your web server. This way, the web service transmits data over HTTPS.

If HTTPS is used, an encrypted channel over SSL is used to transmit data from a client browser to the web server. This enables unidirectional encrypted transmission and prevents data in transmission from being tampered with or intercepted.

## Benefits of HTTPS for websites

- Security compliance: App Stores and application ecosystems require that applications and mini programs can be released only after the apps and mini programs meet the requirements of security compliance.
- Data encryption in transmission: SSL certificates allow you to enable end-to-end HTTPS encryption on your website. This way, data is encrypted when users interact with your website. This prevents data hijacking, tampering, and eavesdropping, and ensures secure data transmission.
- Protection against website hijacking: SSL certificates help prevent hijacking events, such as traffic hijacking and your mobile phone being hijacked by ads.
- High website security: SSL certificates help prevent phishing events. SSL certificates allow you to enable end-to-end HTTPS encryption on your website. When users access your website, the browsers prompt that connections to the website are secure. Your website is trustworthy for users to access. This improves the credibility and search ranking of your website, and increases the traffic to your website.

## Use scenarios of HTTPS

- A message that indicates an unsecure connection appears when users access your website.
- Apps, mini programs, programs, and controls to be published in App Stores or application ecosystems.
- Data encryption in transmission is required between servers.

## Features

The following table describes the features supported by Certificate Management Service.

| Module | Feature | Description | References |
| --- | --- | --- | --- |

| Module | Feature | Description | References |
| --- | --- | --- | --- |
| SSL certificate issuance and use | Purchase certificate instances | You can purchase domain validated (DV), organization validated (OV), and extended validation (EV) certificate instances in the Certificate Management Service console. Then, you can use the certificate instances to apply for certificates.<br>For more information, see Supported certificate types. | 选择购买方式<br>Purchase an SSL certificate instance |
| | Apply for certificates | You can use the certificate instances that you purchase to apply for certificates and wait until the certificates are issued by CAs. | Submit a certificate application |
| | Install certificates | You can download issued certificates to your computer and install the certificates on your web servers. | Installation overview |
| | Revoke certificates | You can revoke certificates in the Certificate Management Service console after your revocation requests are approved by CAs. The process to revoke certificates is secure and fast. | Revoke an SSL certificate |
| | Request refunds for certificates | If your certificate meets the refund conditions, you can submit a to request a refund in offline mode. | None |
| Certificate renewal | Manually renew certificates | You can manually renew and update your certificates in the Certificate Management Service console within 30 calendar days before the certificates expire. | Renew a certificate |
| PCA | Issue private certificates | Private Certificate Authority (PCA) allows you to build a private CA for your enterprise in the Certificate Management Service console. The private CA can issue and manage self-signed private certificates within your enterprise. Then, you can use the private certificates to authenticate the identities of applications and encrypt and decrypt data within your enterprise. | Overview |
| Application information management | Manage contact information | Certificate Management Service automatically saves the contact information that is used to apply for certificates as contacts. Alternatively, you can manually create contacts. This way, you can directly select existing contacts when you apply for certificates. | Manage contacts |
| | Manage company information | Certificate Management Service automatically saves the company information that is used to apply for certificates as company profiles. Alternatively, you can manually create company profiles. This way, you can directly select existing company profiles when you apply for certificates. | Manage company profiles |

| Module | Feature | Description | References |
| --- | --- | --- | --- |
| Centralized certificate management | Upload certificates | You can upload existing certificates to the Certificate Management Service console for centralized management. | Upload a certificate |
| Domain name management | Append domain names to certificates | You can append domain names to the certificates that are in the **Issued** state and issued by GlobalSign. | |
| | Change the domain names that are bound to certificates | You can change the domain names that are bound to certificates only when the certificates are in the **Issued** state and issued by GlobalSign for more than 30 calendar days. | Change a domain name |

## Supported certificate types

Alibaba Cloud Certificate Management Service allows you to purchase the following types of certificate instances: DV, OV, and EV. Different types of certificates provide different levels of security and are suitable for different types of websites.

For more information, see Certificate brands supported by Alibaba Cloud and Supported encryption algorithms.

## Related information

- Benefits
- 选择购买方式Purchase an SSL certificate instance
-
-

# 2.Benefits

Alibaba Cloud supports multiple certificate brands and provides you with different types of SSL certificates.

## Cooperation with famous brands

Alibaba Cloud cooperates with the most trusted third-party certification authorities (CAs) both in and outside China to ensure the certification credibility, encryption strength, and data security for website users.

## Quick issuance of SSL certificates

You can purchase and issue SSL certificates of different brands in the Alibaba Cloud Management Console, without the need to switch between different CA systems. Alibaba Cloud accelerates the approval and issuance of SSL certificates.

## Deployment of SSL certificates to Alibaba Cloud services with a few clicks

SSL Certificates Service is deeply integrated with Alibaba Cloud services. It allows you to deploy SSL certificates to activated Alibaba Cloud services, such as Server Load Balancer (SLB) and Alibaba Cloud CDN with a few clicks. In this situation, you can maintain and manage a large number of certificates at minimal costs.

## Easy-to-use API operations

SSL Certificates Service allows you to purchase, apply for, download, and deploy multiple certificates at a time by calling API operations.

## Refund

SSL Certificates Service supports a 5-day money-back guarantee.

# 3.Scenarios

SSL Certificates Service applies to the following scenarios:

## Encrypt website data

The HTTP protocol does not support data encryption. This may cause problems such as data leaks, data tampering, and phishing attacks. After you install an SSL certificate on your website, this website encrypts website data over the HTTPS protocol during data transmission. This can effectively protect the transmission of sensitive data. The website data includes enterprise application data, government affairs information, and payment data on your website.

## Convert website services from HTTP to HTTPS

To convert website services from HTTP to HTTPS, you can use SSL Certificates Service to apply for a digital certificate issued by a trusted certification authority (CA). Then you can deploy this digital certificate on your cloud website to convert from HTTP to HTTPS and provide authentication and encryption for website access.

## Improve website security

If your website is not installed with an SSL certificate and the website URL starts with HTTP, your browser will mark this website as a website that is not secure.

If your website is installed with an SSL certificate, your browser marks this website as a secure website so that your website users can securely access your website.

If a website is installed with an EV or OV SSL certificate, the real identity of the enterprise to which this website belongs appears in the address bar of the browser. This helps enhance website users' trust in this website and increase the business turnover rate on this website.

## Deploy HTTPS on Alibaba Cloud CDN, SCDN, DCDN, and SLB

If you have purchased Alibaba Cloud CDN, Secure Content Delivery Network (SCDN), Dynamic Route for CDN (DCDN) or Server Load Balancer (SLB), you can use SSL Certificates Service to deploy your digital certificates to these products with just one click. SSL Certificates Service enables the HTTPS protocol for these cloud products.

# 4.SSL certificate concepts

## 4.1. What is a public key and a private key?

A public key and a private key are a key pair that is obtained by using an encryption algorithm. The public key and private key are used for asymmetric encryption. The public key is used to encrypt sessions and verify digital signatures, whereas the matching private key is used to decrypt the session data to ensure secure data transmission. The public key is the public part of a key pair, whereas the private key is the private part managed by users.

A key pair that is generated by using an encryption algorithm is unique worldwide. If you use a key in a key pair to encrypt a piece of data, the data can be decrypted only by using the other key in this key pair. For example, data encrypted with a public key must be decrypted with the matching private key. Data encrypted with a private key must be decrypted with the matching public key.

### How does an SSL certificate work?

An SSL certificate adopts a public-key encryption system that uses a matching key pair to encrypt and decrypt data. Each user creates a private key that is highly secured and not disclosed to anyone for decryption and signature. The user also creates a public key and discloses this key to a group of users for encryption and signature verification.

Only the key owner can use the matching private key to encrypt a document, and therefore generate a digital signature.

An SSL certificate is a document digitally signed by a certificate authority (CA). This document contains information about a public key and the owner of the public key. A certificate must contain a public key, a certificate name, and a digital signature of the corresponding CA. Digital certificates are valid for only a specific period of time.

For more information about private keys, see How does Certificate Management Service protect private keys?.

### Create a private key

SSL Certificates Service has the following requirements for the private key length and the encryption algorithm that is used to generate a private key:

- The Rivest-Shamir-Adleman (RSA) algorithm is used.
- The private key length must be at least 2,048 bits.

You can use one of the following methods to create your private key:

- **Use OpenSSL to generate a private key**
  i. You can download the latest OpenSSL installation package from the OpenSSL official website.

  > **Note** The version of OpenSSL must be 1.0.1g or later.

  ii. After OpenSSL is installed, run the `openssl genrsa -out myprivate.pem 2048` command on the command line to generate your private key file. *myprivate.pem* is the generated private key file. 2,048 represents the private key length.
- **Use Keytool to generate and export a private key**

Keytool is a key management tool installed with JDK. This tool can create keystore files in JKS format for SSL certificates. You can obtain Keytool when you download JDK from the official website.

By default, the public key and private key that are created by using Keytool are not exported. You must export the private key from a *.keystore* file that has been created. For more information about how to export a private key from a *.keystore* file, see Certificate format conversion.

In the exported file, your private key is visible if a section of the file is similar to one of the following examples:

```
-----BEGIN RSA PRIVATE KEY-----
......
-----END RSA PRIVATE KEY-----
```

or

```
-----BEGIN PRIVATE KEY-----
......
-----END PRIVATE KEY-----
```

**Note** We recommend that you keep your private key confidential. If the private key is lost or becomes corrupt, you cannot use the matching public key or digital certificate that you have requested.

# 4.2. How does Certificate Management Service protect private keys?

Certificate Management Service encrypts private keys before it stores the private keys for certificates by using Key Management Service (KMS). This ensures the security of private keys.

Certificate Management Service uses accredited KMS to encrypt and store the private keys that are uploaded with your certificates and the private keys that are generated by using certificate signing requests (CSRs) during your certificate application.

KMS is a security management service that is provided by Alibaba Cloud to ensure the security, integrity, and availability of keys for certificates. KMS allows you to manage keys for multiple applications and services and meets regulatory and classified protection requirements. For more information about KMS, see What is Key Management Service?

Certificate Management Service stores private keys for certificates by using various asymmetric encryption methods. A private key is not stored in plaintext in disks. The plaintext appears in application memory only when necessary. For example, when you download a certificate, Certificate Management Service decrypts the ciphertext of the private key for the certificate. The plaintext appears in your server memory. This way, you can download the plaintext to your local computer over HTTPS.

# 4.3. What is the difference between HTTPS and HTTP?

HTTPS is an SSL-based communication protocol for encrypted transmission over a network. After an SSL certificate is installed on your server, it gets deployed to your website. Visiting the website with HTTPS activates the "SSL encryption channel" (SSL protocol) between the client-side browser and the web server.

This provides intensive bidirectional encryption of communications between the client and server, and prevents the contents of the communication from being divulged or tampered with. HTTPS is a combination of HTTP and SSL.

# 4.4. What formats are used for mainstream digital certificates?

Typically, the mainstream web services are mostly based on the following cryptographic libraries:

- Java cryptographic libraries are generally used for Tomcat, Weblogic, and JBoss web services. By using Keytool included in the Java Development Kit (JDK), you can generate certificates in the Java Keystore (JKS) format.
- OpenSSL cryptographic libraries are generally used for Apache and Nginx web services to generate certificates in the PEM, KEY, and CRT formats.
- For IBM web services such as Websphere and IBM HTTP Server (IHS), the built-in iKeyman tool is generally used to generate certificates in the KDB format.
- For Internet information Services (IIS) in Microsoft Windows Server, cryptographic libraries built in Windows are used to generate certificates in the PFX format.

## How do I determine whether a certificate is in text or binary format?

You can determine the format of a certificate with a suffix extension using the following methods:

- *. DER or *.CER: These two certificates are both in binary format. They contain only certificate information and not the private key.
- *. *.CRT: This certificate can be in either text or binary format (commonly in text format). It has the same functions as *.DER and *. CER certificates. DER and *.
- *. *.PEM: This file is generally in text format, and includes either the certificate, or private key, or both. *. If a *.PEM file only contains the private key, it is generally replaced by the *.KEY extension.
- *. *.PFX or *. P12: These two certificates are both in binary format and contain both the certificate and private key. They are generally password-protected.

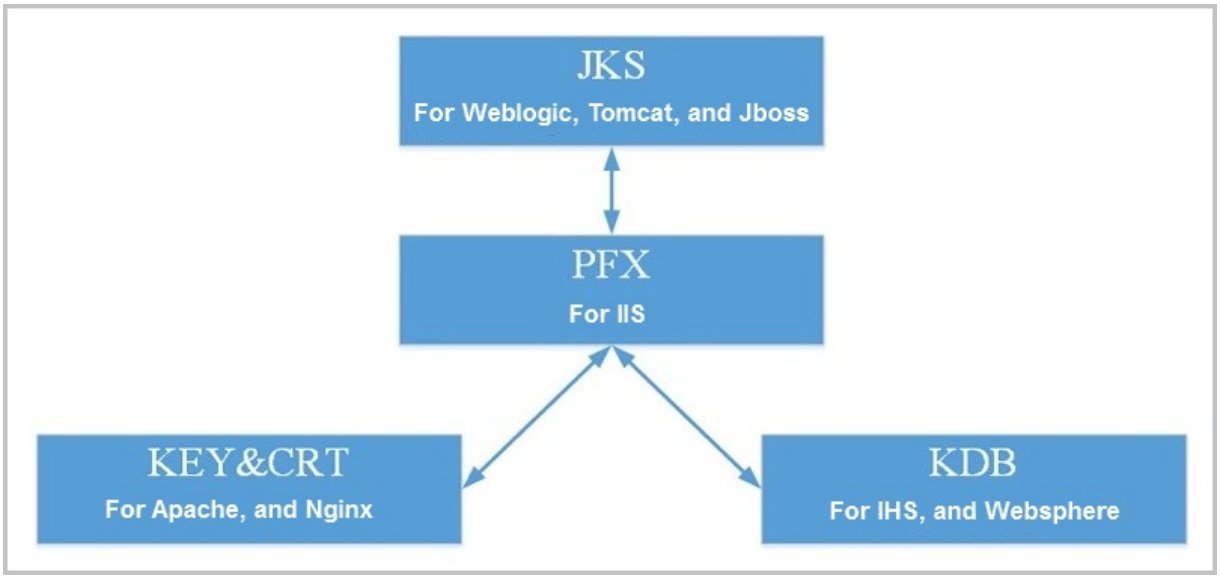
You can also use Notepad to open a certificate file to determine the format of the certificate. A text format example is as follows:

```
-- Begin certificate --
MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh……
-- END CERTIFICATE --
```

- If you see `-- BEGIN CERTIFICATE --`, it indicates a certificate file.
- If you see `-- BEGIN RSA PRIVATE KEY --`, it indicates a private key file.

## Certificate format conversion

The following flowchart demonstrates which certificate formats are interchangeable.




You can convert certificates between different formats using the following methods:

> **Note** Alibaba Cloud Certificates Service uses the PEM format for all digital certificates.

- Convert from JKS to PFX

  You can use the built-in JDK tool Keytool to convert a certificate from JKS to PFX For example, you can convert *server.jks* to *server.pfx* by running the following command:

  ```
  keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx
          -srcstoretype JKS -deststoretype PKCS12
  ```

- Convert from PFX to JKS

  You can use the built-in JDK tool Keytool to convert a certificate from PFX to JKS. For example, you can convert *server.pfx* to *server.jks* by running the following command:

  ```
  keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks
          -srcstoretype PKCS12 -deststoretype JKS
  ```

- Convert from PEM/KEY/CRT to PFX

  You can use the OpenSSL tool to convert a .key private key file and a .crt public key file to a PFX certificate file. For example, you can copy the .key file (server.key) and the .crt file (server.crt) to the OpenSSL installation directory, and convert the files to *server.pfx* by running the following command in the OpenSSL tool:

  ```
  openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
  ```

- Convert from PFX to PEM/KEY/CRT

  You can use the OpenSSL tool to convert a PFX certificate to a .key private key file For example, you can copy the PFX certificate file to the OpenSSL installation directory, and convert the file to a *server .pem* certificate file, a .key private key file (server.key) and a.crt public key file (server.crt) by running the following command in the OpenSSL tool:

  - `openssl pkcs12 -in server.pfx -nodes -out server.pem`

- `openssl rsa -in server.pem -out server.key`
- `openssl x509 -in server.pem -out server.crt`

> **Note** This conversion method is specific to the situation where the private keys and CSR files are generated by Keytool. This method also allows you to extract the private key when you have received the PEM public key. In actual environments, we recommend that you combine the private key that you have extracted, and the public key certificate you have received, to deploy your digital certificate.

# 4.5. What are differences between a renewed certificate and a purchased certificate?

Alibaba Cloud SSL Certificates Service allows you to renew a certificate before it expires. The remaining validity period of the original certificate is added to the validity period of the renewed certificate. This prevents the website that is bound to the certificate from being identified as insecure if the certificate is not updated in time. You can renew a certificate that is due to expire in the SSL Certificates Service console. For more information, see

You can purchase a new certificate on the Alibaba Cloud Certificates Service page in the SSL Certificates Service console. For more information, see

A renewed certificate differs from a purchased certificate in the following aspects:

- The remaining validity period of the original certificate is added to the validity period of the renewed certificate.

  > **Note**

- A renewed certificate is issued faster than a purchased certificate.
- When you apply for a purchased certificate, you must enter application information, but you do not need to do so for a renewed certificate.

  > **Note** Alibaba Cloud SSL Certificates Service stores your information about certificate application. When you apply for a certificate after it is renewed, the system automatically fills in the historical information that you entered when you previously applied for the certificate.

# 4.6. What kind of domain names are supported by wildcard domain certificates?

Alibaba Cloud SSL Certificates Service supports wildcard domain certificates. You can install a wildcard domain certificate on a server to protect a parent domain name and all its subdomains of the same level. Both the Domain Validation (DV) and Organization Validation (OV) certificates of the professional version support wildcard domain names.

If your server hosts multiple subdomain names of the same level, you do not need to purchase and install a certificate for each subdomain.

If you want to purchase a **wildcard domain** certificate, take note of the following rules to match the subdomains of the **wildcard domain name**:

- A wildcard domain certificate supports only the subdomains of the same level.

  For example, if a wildcard domain certificate is bound with the domain name *.example.com, it supports subdomains of the same level, such as abc.example.com, sport.example.com, and good.example.com. However, it does not support subdomains that reside at different levels, such as mycard.good.example.com and mycalc.good.example.com.

  If a wildcard domain certificate is bound with the domain name *.good.example.com, it supports subdomains such as mycard.good.example.com and mycalc.good.example.com.
- A wildcard domain certificate can be bound with a second-level domain name.
- A wildcard domain certificate can be bound with only one wildcard domain name.
- A wildcard domain certificate supports only wildcard domain names but not common domain names.

  For more information about how to use one certificate to protect multiple wildcard domain names and one or more common domain names, see How do I apply for multi-domain certificates or hybrid certificates?

# 4.7. What websites must have HTTPS encryption enabled?

Currently, HTTPS encryption must be enabled for the following websites:

- E-commerce platforms and associated online payment systems
- Websites for banks and financial institutions
- Websites for governments, colleges and universities, and research institutions
- Websites of which traffic is mostly driven by search engines
- Email-dominated enterprise communication platforms

In the long run, the HTTPS protocol website is an inevitable trend. Enabling HTTPS protocol encryption is the key point of today's Web site construction. Not only is it limited to the above-mentioned web site types, but HTTPS is enabled Protocol encryption is not only the inevitable need of website security, but also the advanced layout of the company's development.

# 5.Terms

This topic introduces the basic concepts related to Alibaba Cloud Certificate Management Service.

## digital certificate

A digital certificate is a document signed by a certificate authority (CA). The certificate contains information about the public key owner and the public key. It is a trusted credential that is issued by a CA to a website. A certificate must contain a public key, a certificate name, and a digital signature provided by a CA.

Digital certificates are valid only for a specific period of time.

## CA

CA stands for certificate authority.

A CA is a trusted third party in e-commerce transactions. A CA is responsible for verifying the validity of public keys.

## validity period

From September 1, 2020, certificates issued by CAs are valid for up to one year. Therefore, the certificates that you apply for by using Certificate Management Service are valid for one year.

## SSL

SSL is a protocol that is used for data encryption in transmission between browsers and websites. It prevents data tampering and data theft during data transmission.

## SSL certificate

An SSL certificate is a trusted credential that is issued by a CA to a website. It uses the SSL protocol for communications and implements website identity authentication and encrypted transmission.

SSL provides an encryption mechanism for application data transmission on a TCP/IP network. The protocols of the applications include HTTP, Telnet, and FTP. SSL uses public keys to encrypt data transmitted over TCP/IP connections, ensure message integrity, and authenticate servers and clients. Client authentication is optional.

An SSL certificate adopts public key cryptography, which uses a pair of keys to encrypt and decrypt data. Each user creates a private key that is not disclosed to anyone for decryption and signature. The user also creates a public key and discloses this key to a group of users for encryption and signature verification.

After you install an SSL certificate on a web server, HTTPS is enabled for the web server. Your website will transmit data over HTTPS, which helps establish trusted and encrypted connections between your website and the web server. This ensures the security of data during transmission.

For more information about the private keys of certificates, see What is a public key and a private key?

## HTTPS

HTTPS is a combination of HTTP and SSL. It is a secure version of HTTP and encrypts website communications based on SSL.

After you install an SSL certificate on the server of your website, HTTPS is enabled to activate the SSL-encrypted channel between browsers and the web server. This enables bidirectional encrypted transmission and prevents data tampering and data leak during transmission.

## domain name

A domain name is a representation of an IP address. A domain name consists of a string of names separated by periods (.) and is used to identify a server or a group of servers during data transmission.

Single domain names are in the simplest structure. Example: *www.aliyundoc.com*.

A wildcard domain name can match its parent domain name and all the subdomains of the parent domain name. Example: **.aliyundoc.com*. The domain name **.aliyundoc.com* can match its parent domain name *aliyundoc.com* and the first-level subdomains such as *www.aliyundoc.com* and *example.aliyundoc.com*. The domain name *.aliyundoc.com cannot match *www.example.aliyundoc.com*.

## wildcard certificate

A wildcard certificate is also called a wildcard domain certificate. If a wildcard domain name, such as **.aliyundoc.com*, is bound to a certificate, the certificate is a wildcard certificate.

A multi-domain wildcard certificate is a certificate to which multiple wildcard domain names are bound. Certificate Management Service allows you to apply for only a wildcard certificate to which a single wildcard domain name is bound. You cannot apply for a multi-domain wildcard certificate. To obtain a multi-domain wildcard certificate, you can combine multiple certificates of the same brand and type. For more information, see Combine certificate instances.

## hybrid certificate

A hybrid certificate is a certificate whose bound domain names include both single and wildcard domain names. For example, if a certificate is bound to the **.aliyundoc.com* and *demo.example.com* domain names, the certificate is a hybrid certificate.

Certificate Management Service does not allow you to apply for a hybrid certificate. To obtain a hybrid certificate, you can combine multiple certificates of the same brand and type. For more information, see Combine certificate instances.

## Nginx

NGINX is a lightweight web server and processes highly concurrent connections. You can configure it as a reverse proxy server or an email proxy server that complies with Internet Message Access Protocol (IMAP) or Post Office Protocol version 3 (POP3). NGINX is based on BSD-like licenses. NGINX runs on different operating systems, such as Linux, Windows, FreeBSD, Solaris, AIX, and macOS. It can be used for reverse proxy, load balancing, and dynamic and static separation.

## Tengine

Tengine is a web server project initiated by Taobao. It supports all the features of NGINX and is compatible with NGINX configurations.

## PuTTY

PuTTY is a piece of connection software that allows you to perform operations by using Telnet, SSH, rlogin, pure TCP, and serial interfaces. It can remotely manage Linux and Windows operating systems.

## Xshell

Xshell is a powerful terminal emulator. It supports Telnet on SSH1 and SSH2 clients and also in Windows. XShell can remotely manage servers that run different operating systems from Windows. Xshell supports VT100, VT220, VT320, Xterm, Linux, SCO ANSI, and ANSI terminals and provides a variety of terminal screen views to replace traditional Telnet clients.

## CentOS

Community Enterprise Operating System (CentOS) is an enterprise-grade Linux distribution and is derived from the sources of Red Hat Enterprise Linux. CentOS is open source and free of charge.

## CSR

A certificate signing request (CSR) file contains the information about your server and company. When you apply for an SSL certificate, you must submit the CSR file to the CA. The CA signs the CSR file by using the private key of the root certificate and generates a public key file to issue your certificate.

# 6.Supported certificate brands

This topic describes the certificate brands that are supported by Alibaba Cloud SSL Certificates Service. This topic also describes the types of certificates that each brand can issue. Certificate brands are also known as certificate authorities (CAs).

The following table describes the supported certificate brands and the types of certificates that each brand can issue. The following symbols are used in the table:

- Tick (√): indicates that the type of certificate can be issued by the brand.
- Cross (×): indicates that the type of certificate cannot be issued by the brand.

> **Note** For more information about certificate types, see Supported certificate types.

| Certificate brand | Description | Certificate type | | |
|---|---|---|---|---|
| | | DV SSL certificate | OV SSL certificate | EV SSL certificate |
| **DigiCert** | DigiCert is the largest CA and the most trusted SSL certificate brand in the industry. All DigiCert certificates use industry-leading encryption technologies to provide enhanced security solutions for different websites and servers. DigiCert is formerly known as Symantec. | √ Supports single-domain certificates and wildcard-domain certificates. | √ Supports single-domain certificates and wildcard-domain certificates. | √ Supports only single-domain certificates. |
| **Entrust** | Entrust is a world-renowned CA that has established a trusted virtual environment. It allows users to conduct secure digital transactions and communication from all locations.<br>Entrust provides trust services for websites, software developers, and individuals. The services include issuing SSL certificates that are used for website authentication and encryption. More than 83% of the Fortune Global 500 companies use Entrust SSL certificates. | × | √ Supports single-domain certificates, wildcard-domain certificates, and multi-domain certificates. | √ Supports single domain names and multiple domain names. |

| Certificate brand | Description | Certificate type | | |
|---|---|---|---|---|
| | | DV SSL certificate | OV SSL certificate | EV SSL certificate |
| **GlobalSign** | GlobalSign is one of the earliest CAs in the industry. It has been committed to network security authentication and digital certificate services. GlobalSign is a trusted CA and SSL certificate provider. | √<br>Supports single-domain certificates and wildcard-domain certificates. | √<br>Supports single-domain certificates, wildcard-domain certificates, and multi-domain certificates. | × |

# 7.Supported encryption algorithms

Alibaba Cloud SSL Certificates Service supports the RSA, ECC, and SM2 encryption algorithms. This topic describes the encryption algorithms that are supported by different certificate brands.

The following list describes the RSA, ECC, and SM2 encryption algorithms:

- **RSA**: The RSA algorithm is an asymmetric algorithm that is widely used and provides high compatibility.
- **ECC**: The ECC algorithm is a public key encryption algorithm based on elliptic curves. Compared with the RSA algorithm, the ECC algorithm is more advanced and secure. The ECC algorithm provides faster encryption and higher efficiency at lower server resource consumption. The ECC algorithm is promoted among mainstream browsers.
- **SM2**: The SM2 algorithm is developed and approved by the State Cryptography Administration of China based on the ECC algorithm. The SM2 algorithm is used to replace the RSA algorithm in Chinese commercial cryptography systems.

The following table describes the certificate brands that are supported by SSL Certificates Service and the types of encryption algorithms that are supported by the brands. The following symbols are used in the table:

- Tick (√): indicates that the encryption algorithm type is supported by the brand.
- Cross (×): indicates that the encryption algorithm type is not supported by the brand.

| Certificate brand | Certificate type | RSA | ECC | SM2 |
| --- | --- | --- | --- | --- |
| **DigiCert** | DV | √ | × | × |
| | OV | √ | √ | × |
| | EV | √ | × | × |
| **Entrust** | OV | √ | × | × |
| | EV | √ | × | × |
| **GlobalSign** | DV | √ | × | × |
| | OV | √ | √ | × |