ALIBABA CLOUD

Alibaba Cloud

SSL Certificates

Product Introduction

Document Version: 20210120

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 SSL Certificates Service?

SSL Certificates Service is a digital certificate service that is provided by Alibaba Cloud in cooperation with certificate authorities (CAs) inside and outside China. This service allows you to purchase and deploy certificates in the SSL Certificates Service console. SSL Certificates Service allows you to redirect traffic to your website or mobile applications from HTTP to HTTPS at minimal costs. You can use SSL certificates to authenticate users and encrypt data.

Benefits of HTTPS support for websites

- Prevents data hijacking, tampering, and eavesdropping. SSL certificates allow you to enable HTTPS encryption on your websites. Then, data is encrypted when users interact with your website.
- Improves search engine rankings. If HTTPS encryption is enabled on your website, your website gains a higher ranking on the search engine result page. This improves the credibility of your website.
- Increases web traffic. If HTTPS encryption is enabled on your website, your website is more trustworthy for users to access. This increases the traffic to your website.

Features

The following table describes the features that SSL Certificates Service provides.

Module	Feature	Description	Documentation
HTTPS websites	Purchase certificate instances	You can purchase certificate instances in the SSL Certificate Service console. Then, you can use the certificate instances to apply for Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV) certificates. For more information, see Supported certificate types.	Select and purchase certificates
	Apply for certificates	You can use the certificate instances that you purchase to apply for and issue certificates. If errors are returned by CAs, you must fix the errors in a timely manner.	Apply for and validate certificates
	Download certificates	You can download issued certificates to your computer and install them on your web servers.	Download certificates
	Deploy certificates	You can deploy issued certificates to Alibaba Cloud services with a few clicks. For more information, see Related services.	Deploy certificates on Alibaba Cloud services
Centralized certificate	Upload certificates	You can upload existing certificates to the SSL Certificates Service console for centralized management. For example, you can deploy the certificates to Alibaba Cloud services with a few clicks.	Upload certificates

management Module	Feature	Description	Documentation
	Revoke certificates	You can revoke certificates in the SSL Certificates Service console after your revocation requests are approved by CAs. The process to revoke certificates is secure and fast.	Revoke certificates

Supported certificate types

SSL Certificates Service supports DV, OV, and EV certificates. Different types of certificates provide different levels of security and are applicable to different websites.

Certificate type	Applicable website	Credibility level	Authentication strength	Security	Available certificate brand
Domain Validation (DV) SSL	Websites of individuals	Moderate	CAs verify the authenticity of a website, instead of an enterprise.	Moderate	GlobalSign
Organization Validation (OV) SSL	Websites of organizations such as governments, enterprises, and educational institutions	High	CAs verify the authenticity of an organization or an enterprise.	High	GlobalSign and Entrust
Extended Validation (EV) SSL	Websites of organizations such as large-sized enterprises and financial institutions	Highest	CAs perform strict authentication.	Highest (The address bar is in green.)	Entrust

For more information about certificate brands, see Brands of certificates supported by Alibaba Cloud.

Related services

- Anti-DDoS Pro and Anti-DDoS Premium: proxy-based services provided by Alibaba Cloud to mitigate volumetric DDoS attacks.

  For more information, see What are Anti-DDoS Pro and Anti-DDoS Premium?

- Web Application Firewall (WAF): a security service provided by Alibaba Cloud to protect web applications against common attacks defined by the Open Web Application Security Project (OWASP) and mitigate HTTP flood attacks. This service protects your website assets against data leaks and ensures the security and availability of website services.

For more information, see What is WAF?

- Alibaba Cloud CDN: a content delivery network provided by Alibaba Cloud to offload network traffic from origin servers and prevent network congestion. You can use Alibaba Cloud CDN to accelerate website content delivery in different regions and scenarios.

  For more information, see What is Alibaba Cloud CDN?

- Secure CDN (SCDN): a branch of Alibaba Cloud CDN that provides security protection capabilities. SCDN stabilizes the acceleration of content delivery and protects resources against DDoS and HTTP flood attacks.

  For more information, see SCDN.

- Dynamic Route for CDN (DCDN): a CDN service developed by Alibaba Cloud to accelerate static and dynamic content delivery. This service provides a solution to resolve issues of high latency, packet loss, and instability. These issues may occur for various reasons, such as unstable networks, unexpected traffic spikes, and network congestion. These issues may also occur if your website contains both static and dynamic content, content is delivered across network providers, or only one origin server is used. You can use DCDN to improve the overall performance of your website and accelerate content delivery to improve user experience.

  For more information, see What is Dynamic Route for CDN?

- ApsaraVideo Live: an audio and video streaming platform provided by Alibaba Cloud. The platform is based on the next-generation content access and delivery network and large-scale, distributed, and real-time transcoding technology. The platform provides a live streaming service with quick access, high resolution, high fluency, low latency, and high concurrency.

  For more information, see What is ApsaraVideo Live.

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 inside 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 in 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 in a few clicks. In this situation, you can easily 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 unconditional refund within five days of purchase.

3.Scenarios

Alibaba Cloud Certificates Service applies to the following scenarios:

Convert websites from HTTP to HTTPS

Alibaba Cloud Certificates Service helps convert your website service from HTTP to HTTPS for better authentication and encryption support. You can purchase digital certificates issued by the trusted Certificate Authorities and deploy these certificates to your website by using this service.

Deploy HTTPS together with Alibaba Cloud CDN, Anti-DDoS Pro, WAF, and Server Load Balancer

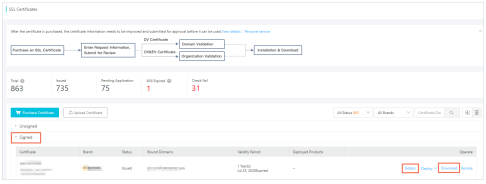
Alibaba Cloud Certificate Service facilitates the HTTPS configuration for Alibaba Cloud CDN, Anti-DDoS Pro, WAF, and Server Load Balancer. This service enables you to deploy digital certificates to these products with just one-click.

4.Features

Alibaba Cloud SSL Certificates offers certificates issued by various CAs. Alibaba Cloud SSL Certificates helps you build HTTPS-based websites to achieve secure and effective access. The SSL Certificates service supports quick deployment, certificate management, and certificate revocation.

- Purchase certificates: Alibaba Cloud SSL Certificates provides digital certificates issued by trusted CAs. Different levels of digital certificates are issued after they are verified by the CAs.
- Manage certificates: SSL Certificates allows you to upload certificates and private keys to achieve unified management of digital certificates on the Alibaba Cloud platform. You can also submit certificates for verification, view the domain names bound to certificates, view the certificate expiration date, modify the certificate name, and delete expired certificates.
- Deploy certificates: SSL Certificates allows you to deploy digital certificates to other Alibaba Cloud products on the Alibaba Cloud platform with minimal costs.
- Upload certificates: you can use the Alibaba Cloud SSL Certificates console to upload your own certificates, so that you can manage all certificates in the console.
- Revoke certificates: provides a standard procedure for you to revoke digital server certificates that are verified and issued by CAs.

You can view the details of your certificate on the **Issued** tag page in the SSL Certificates console.



5.Supported certificate brands

This topic describes the certificate brands that Alibaba Cloud SSL Certificates Service supports. Certificate brands are also known as certificate authorities (CAs).

The following table lists the supported certificate brands and the types of certificates that each brand can issue. Symbol description:

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

For more information about certificate types, see Supported certificate types.

Certificate brand	Description	Certificate type		
		DV	OV	EV
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.	√	√	×
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. Entrust provides trust services for websites, software developers, and individuals, including issuing SSL certificates that are used for website authentication and encryption. More than 83% of the Fortune Global 500 companies use Entrust SSL certificates.	×	√	√

6.Terms

This topic introduces basic concepts and terms used in Alibaba Cloud SSL Certificates Service.

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 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

CentOS is an enterprise-grade Linux distribution and is derived from the sources of Red Hat Enterprise Linux. It is open source and free of charge.

CSR

A certificate signing request (CSR) file contains your server and company information. When you apply for an SSL certificate, you must submit the CSR file to a certificate authority (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 SSL certificate.

7.SSL certificate concepts

7.1. What are the advantages of SSL certificates?

SSL certificates offer the following advantages over traditional encryption methods:

- Simplified operations: You only need to apply for a certificate and deploy it on your web server. No further actions are required within the validity of the certificate.
- Intuitive display: After the SSL certificate is deployed, an encryption lock icon is displayed in, or to the right of, the address bar when you access your website over HTTPS, indicating you website is encrypted. If an EV certificate is deployed, you will be able to view the company name.
- Authentication: Visitors can conveniently see the website owner information from the certificate details, enhancing user trust in your website.
- Quick issue: One-click quick issue. You can issue SSL certificates of different brands here. Alibaba Cloud speeds up the review of these SSL certificates.
- One-click deploy: You can deploy the issued certificates to Alibaba Cloud products (SLB, CDN, SCDN and DCDN) in one click. The cost of cloud application is minimized.

7.2. 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 corresponding 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 SSL Certificates Service work?

SSL Certificates Service uses 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. Meanwhile, the user 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 key to encrypt a document, and therefore generate a digital signature.

An SSL certificate is a document digitally signed by a certification authority (CA). This document contains information about a public key and the owner of the public key. The simplest certificate contains 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.

How can I 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 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 OpenSSL.

  > **Note** OpenSSL version 1.0.1g or later is required.

  ii. After OpenSSL is installed, run `openssl genrsa -out myprivate.pem 2048` in command line mode 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 Java SE Downloads.

  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 safe. If the private key is lost or becomes corrupt, you cannot use the matching public key and digital certificate that you have requested.

7.3. How does SSL Certificates Service protect private keys?

SSL Certificates Service encrypts and stores private keys for SSL certificates by using Alibaba Cloud Key Management Service (KMS) to protect the security of your private keys.

Alibaba Cloud SSL Certificates Service Private key protection
SSL Certificates Service uses accredited KMS to encrypt and store the private keys uploaded with your SSL certificates and the private keys generated with certificate signing requests (CSRs) during your certificate application.

KMS is a security management service that ensures the security, integrity, and availability of keys for certificates. This service allows you to manage keys for multiple applications and services while meeting regulatory and cybersecurity classified protection requirements. For more information about KMS, see What is Key Management Service?.

SSL Certificates Service stores private keys for certificates by using various asymmetric encryption methods. The plaintext of a private key is never stored in disks, and appears in the application memory only when necessary. For example, when you download a certificate, SSL Certificates Service decrypts the ciphertext of the private key for this certificate. In this way, the decrypted ciphertext appears as plaintext in your server memory and can be downloaded to your local computer over HTTPS.

7.4. 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.

7.5. 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.

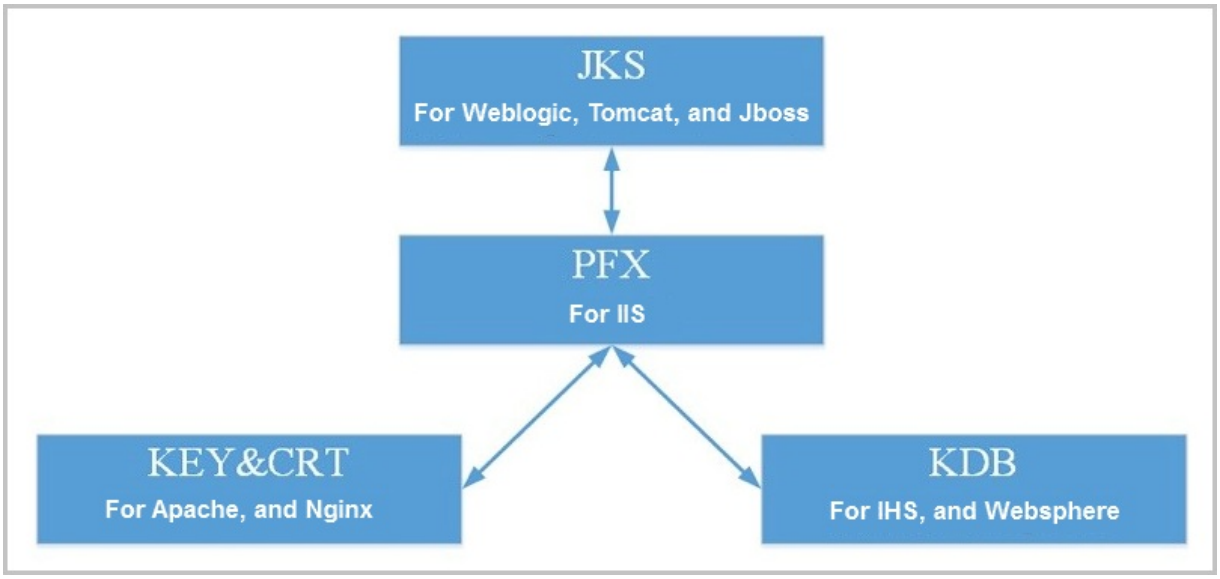
You can also use Notepad to open a certificate file to determine the format of the certificate. A text format example is as follows:

```
-- 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.

7.6. 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** If your existing certificate is due to expire and you purchase a new certificate instead of renewing the existing certificate, you cannot add the remaining validity period of the existing certificate to the new certificate.

- 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.

7.7. 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.

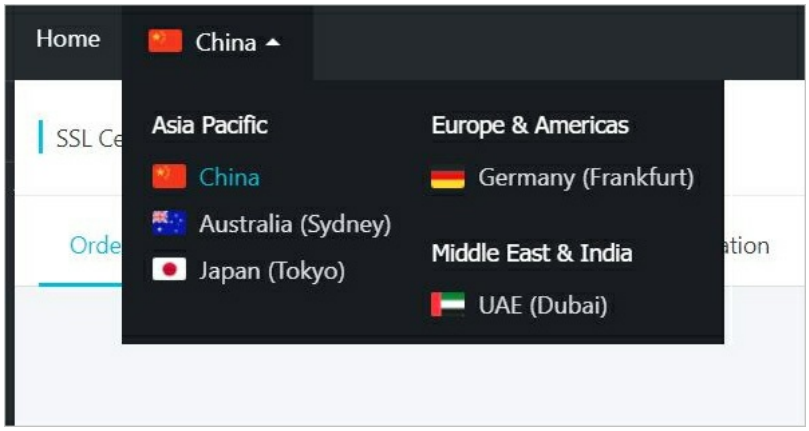
  For example, if a wildcard domain certificate is bound with the domain name *.example.com, it supports subdomains of the same level, such as abc.example.com, sport.example.com, and good.example.com. However, it does not support subdomains that reside at different levels, such as mycard.good.example.com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

7.8. Can I switch the region of the server where my SSL certificate is installed?

You can switch the region of the server where your SSL certificate is installed in the Alibaba Cloud SSL Certificates console, and your SSL certificate data is saved in the corresponding region.



The deployment of purchased and issued certificates is not limited by regions.

You need to select regions when purchasing SSL certificates. You can use SSL certificates only when you switch to the regions where you purchased the certificates.

7.9. 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.