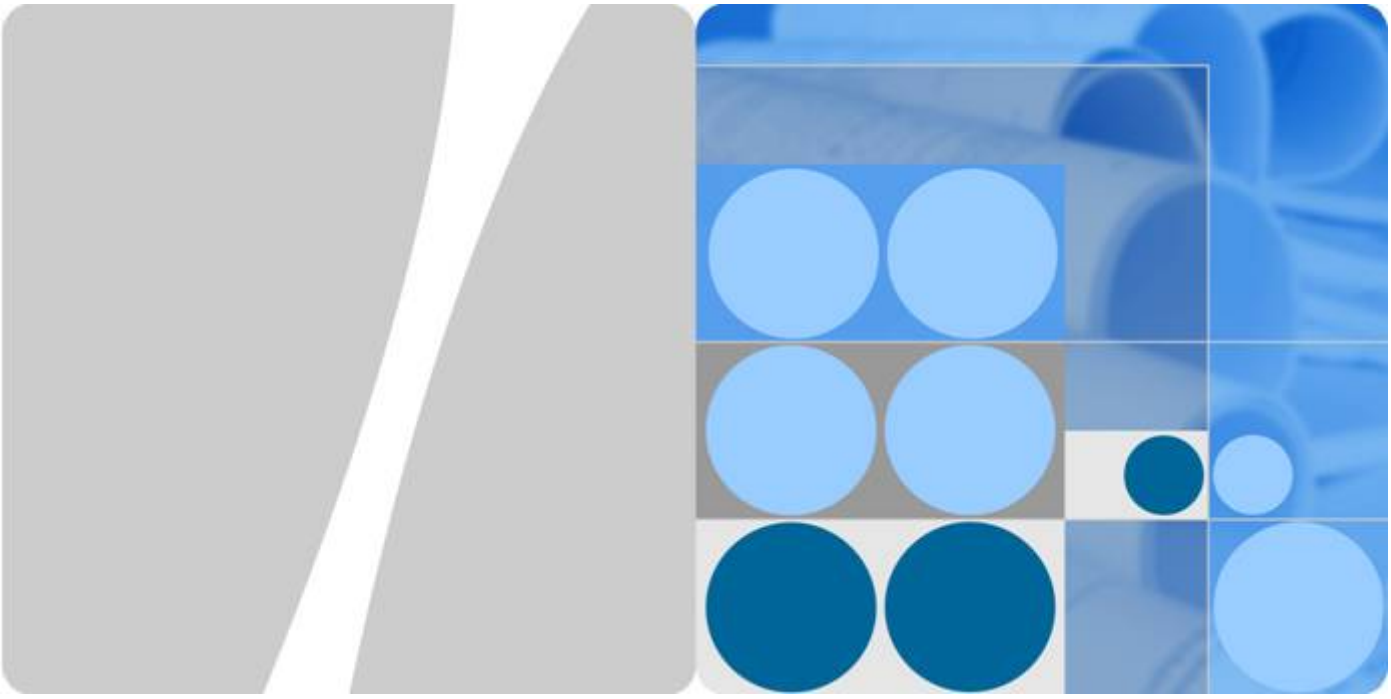


云证书管理服务

用户指南

发布日期　2023-03-30

目 录

1 常见问题

1.1 什么是公钥和私钥?

公钥和私钥就是俗称的不对称加密方式。公钥（Public Key）与私钥（Private Key）是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。

通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，则必须用另一个密钥才能解密。比如用公钥加密的数据就必须用私钥才能解密，如果用私钥进行加密也必须用公钥才能解密，否则将无法成功解密。

说明

由于私钥的非公开属性，建议在证书申请过程中，由客户自己生成私钥，并妥善保管。一旦发生证书私钥丢失的事件，请立刻吊销已有证书并对相关域名重新申购证书。以避免因私钥丢失导致网站信息泄露等恶性事件的发生。

数字证书的原理

数字证书采用公钥体制，即利用一对互相匹配的密钥对进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。

数字证书是一个经证书授权中心（CA）数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书还有一个重要的特征就是只在特定的时间段内有效。

创建私钥

云证书管理对您的私有密钥的加密算法和长度有如下要求：

- 加密算法使用RSA算法
- 加密长度至少2048位

说明

建议您使用2048位加密长度的SHA256摘要算法。

您可以通过以下两种方式创建您的私钥：

- 使用OpenSSL工具生成私钥

  OpenSSL是一个强大且应用广泛的安全基础库工具，您可以从“http://www.openssl.org/source/”下载最新的OpenSSL工具安装包。

  说明

  要求OpenSSL版本必须是1.0.1g或以上版本。

  安装OpenSSL工具后，在命令行模式下运行**openssl genrsa -out myprivate.pem 2048**即可生成您的私钥文件。

  - “myprivate.pem”即为您的私钥文件。
  - “2048”指定加密长度。

- 使用Keytool工具导出私钥

  Keytool工具是JDK中自带的密钥管理工具，可以制作Keystore（jks）格式的证书文件，您可以从“http://www.oracle.com/technetwork/java/javase/downloads/index.html”下载JDK工具包来获取Keytool工具。

  由于使用Keytool工具制作的公钥和私钥默认是不可以导出的，需要您从已经创建好的“.keystore”文件中导出私钥。

  在导出的文件中，以下部分的内容即是您的私钥：

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

  或者

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

须知

无论您通过哪种方式生成密钥，请您完善地保管好您的私钥文件，私钥文件一旦丢失或者损坏，您申请的对应的公钥、及数字证书都将无法使用。

1.2 为什么要使用无密码保护的私钥?

因为私钥是加载密码保护的，且其他云产品在使用数字证书的过程中需要使用您提供的私钥，所以如果您的私钥是加载密码保护的，那么其它云产品在加载您的数字证书时将无法使用您的私钥，可能导致数字证书解密失败，HTTPS服务失效。因此，需要您提供无密码保护的私钥。

在您生成私钥时，请去掉密码保护后再进行上传。

如何去除私钥密码保护

如果您的密钥已经加载密码保护，可以通过OpenSSL工具运行以下命令去掉密码保护：

openssl rsa -in encryedprivate.key -out unencryed.key

其中，“encryedprivate.key”是带密码保护的私钥文件；“unencryed.key”是去掉了密码保护的私钥文件，扩展名为key或pem均可。

如果您的证书使用的是除密码保护的私钥，当需要将该证书部署给CDN时，需要检查证书文件的格式。因为CDN要求证书文件必须是RSA加密的，即私钥是以“-----BEGIN RSA PRIVATE KEY-----”开头并以“-----END RSA PRIVATE KEY-----”结尾的格式。如果证书文件不是此格式，则需要使用工具转换证书的格式。具体转换方式，请参考**主流数字证书有哪些格式？**。

什么样的私钥是有密码保护的

使用文本编辑器打开您的私钥文件，如果私钥文件是如下样式，则说明您的私钥是已加载密码保护的：

- PKCS#8私钥加密格式
```
-----BEGIN ENCRYPTED PRIVATE KEY-----
.....BASE64 私钥内容.....
-----END ENCRYPTED PRIVATE KEY-----
```
- Openssl ASN格式
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,4D5D1AF13367D726
.....BASE64 私钥内容.....
-----END RSA PRIVATE KEY-----
```

说明

用Keytool工具生成的密钥都是带有密码保护的，您可以转换成无密码的密钥文件。关于具体转换方式，请参考**主流数字证书有哪些格式？**。

1.3 主流数字证书有哪些格式？

主流的Web服务软件，通常都基于OpenSSL和Java两种基础密码库。

- Tomcat、Weblogic、JBoss等Web服务软件，一般使用Java提供的密码库。通过Java Development Kit（JDK）工具包中的Keytool工具，生成Java Keystore（JKS）格式的证书文件。
- Apache、Nginx等Web服务软件，一般使用OpenSSL工具提供的密码库，生成PEM、KEY、CRT等格式的证书文件。
- IBM的Web服务产品，如Websphere、IBM Http Server（IHS）等，一般使用IBM产品自带的iKeyman工具，生成KDB格式的证书文件。
- 微软Windows Server中的Internet Information Services（IIS）服务，使用Windows自带的证书库生成PFX格式的证书文件。

查看证书文件的格式

- 您可以使用以下方法简单区分带有后缀扩展名的证书文件：
  - *.DER或*.CER文件：这样的证书文件是二进制格式，只含有证书信息，不包含私钥。
  - *.CRT文件：这样的证书文件可以是二进制格式，也可以是文本格式，一般均为文本格式，功能与*.DER及*.CER证书文件相同。
  - *.PEM文件：这样的证书文件一般是文本格式，可以存放证书或私钥，或者两者都包含。*.PEM文件如果只包含私钥，一般用*.KEY文件代替。

  - *.PFX或*.P12文件：这样的证书文件是二进制格式，同时包含证书和私钥，且一般有密码保护。
- 您也可以使用记事本直接打开证书文件。如果显示的是规则的数字和字母，则表示该证书文件是文本格式。

  举例：

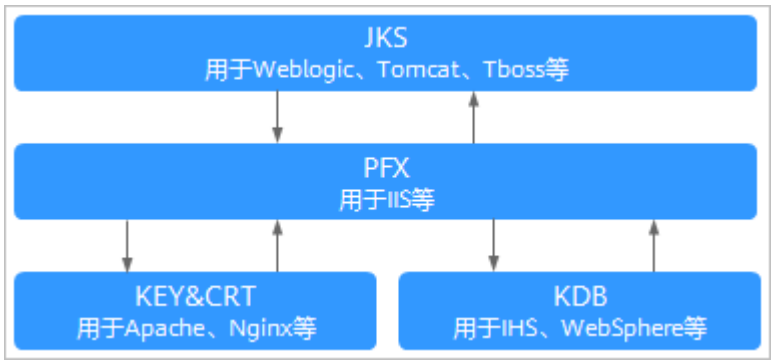
  ```
  —–BEGIN CERTIFICATE—–
  MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
  —–END CERTIFICATE—–
  ```

  - 如果存在“——BEGIN CERTIFICATE——”，则说明这是一个证书文件。
  - 如果存在“—–BEGIN RSA PRIVATE KEY—–”，则说明这是一个私钥文件。

证书格式转换

证书格式之间是可以互相转换的，如图1-1所示。

图 1-1 证书格式转换



您可使用以下方式实现证书格式之间的转换：

- 将JKS格式证书转换为PFX格式

  您可以使用JDK中自带的Keytool工具，将JKS格式证书文件转换成PFX格式。

  例如，您可以执行以下命令将“server.jks”证书文件转换成“server.pfx”证书文件：

  keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -srcstoretype JKS -deststoretype PKCS12
- 将PFX格式证书转换为JKS格式

  您可以使用JDK中自带的Keytool工具，将PFX格式证书文件转换成JKS格式。

  例如，您可以执行以下命令将“server.pfx”证书文件转换成“server.jks”证书文件：

  keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks -srcstoretype PKCS12 -deststoretype JKS
- 将PEM/KEY/CRT格式证书转换为PFX格式

  您可以使用OpenSSL工具，将KEY格式密钥文件和CRT格式公钥文件转换成PFX格式证书文件。

  例如，将您的KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）复制至OpenSSL工具安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pfx”证书文件：

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

- 将PFX格式证书转换为PEM/KEY/CRT格式

  您可以使用OpenSSL工具，将PFX格式证书文件转化为PEM格式证书文件、KEY格式密钥文件和CRT格式公钥文件。

  例如，将您的PFX格式证书文件复制至OpenSSL安装目录，使用OpenSSL工具执行以下命令将证书转换成“server.pem”证书文件、KEY格式密钥文件（server.key）和CRT格式公钥文件（server.crt）：

  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

须知

此转换步骤是专用于通过OpenSSL工具生成私钥和CSR申请证书文件，并且通过此方法您还可以在获取到PEM格式证书公钥的情况下，分离出私钥。在您实际部署数字证书时，请使用通过此转换步骤分离出来的私钥和您申请得到的公钥证书匹配进行部署。

1.4 如何制作 CSR 文件?

在申请数字证书之前，您必须先生成证书私钥和证书请求文件（Cerificate Signing Request，简称CSR）。CSR文件是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给CA认证中心进行审核。

说明

建议您使用系统提供的创建CSR功能，避免出现内容不正确而导致的审核失败。

手动生成CSR文件的同时会生成私钥文件，请务必妥善保管和备份您的私钥。

此处提供2种制作方法，请根据您的需要进行选择：

- **使用OpenSSL工具生成CSR文件**

  如果您需要输入中文信息，建议您使用Keytool工具生成CSR文件。
- **使用Keytool工具生成CSR文件**

说明

证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。

使用 OpenSSL 工具生成 CSR 文件

步骤1 安装OpenSSL工具。

步骤2 执行以下命令生成CSR文件。

openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout *myprivate.key* -out *mydomain.csr*

- -new：指定生成一个新的CSR。
- -nodes：指定私钥文件不被加密。

- -sha256：指定摘要算法。
- -newkey rsa:2048：指定私钥类型和长度。
- -keyout：生成私钥文件，名称可自定义。
- -out：生成CSR文件，名称可自定义。

步骤3 生成CSR文件“mydomain.csr”。

图 1-2 生成 CSR 文件

```
Generating a 2048 bit RSA private key
....+++
.....................................................................+++
writing new private key to 'myprivate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
[Country Name (2 letter code) [CN]:CN
[State or Province Name (full name) []:ZheJiang
[Locality Name (eg, city) [Default City]:HangZhou
[Organization Name (eg, company) [Default Company Ltd]:HangZhou xxx Technologies,Inc.
[Organizational Unit Name (eg, section) []:IT Dept.
[Common Name (eg, your name or your server's hostname) []:www.example.com
[Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
[A challenge password []:
[An optional company name []:
```

需要输入的信息说明如下：

字段	说明	示例
Country Name	申请单位所属国家，只能是两个字母的国家码。例如，中国只能是CN。	CN
State or Province Name	申请单位所在省名或州名，可以是中文或英文。	ZheJiang
Locality Name	申请单位所在城市名，可以是中文或英文。	HangZhou
Organization Name	申请单位名称法定名称，可以是中文或英文。	HangZhou xxx Technologies, Inc.
Organizational Unit Name	申请单位的所在部门，可以是中文或英文。	IT Dept.
Common Name	申请证书的具体网站域名。 **说明** • 多域名类型的证书，请填写需要绑定的主域名。 • 泛域名类型的证书，请填写泛域名。示例：*.example.com	www.example.com

字段	说明	示例
Email Address	申请单位的邮箱。 无需输入，请直接按“Enter”。	-
A challenge password	设置CSR文件密码。 无需输入，请直接按“Enter”。	-

说明

- 在使用OpenSSL工具生成中文证书时，需要注意中文编码格式必须使用UTF8编码格式。同时，需要在编译OpenSSL工具时指定支持UTF8编码格式。
- 证书服务系统对CSR文件的密钥长度有严格要求，密钥长度必须是2,048位，密钥类型必须为RSA。

完成命令提示的输入后，会在当前目录下生成myprivate.key（私钥文件）和mydomain.csr（CSR，证书请求文件）两个文件。

----结束

使用 Keytool 工具生成 CSR 文件

步骤1 安装Keytool工具，Keytool工具一般包含在Java Development Kit（JDK）工具包中。

步骤2 使用Keytool工具生成keystore证书文件。

说明

Keystore证书文件中包含密钥，导出密钥方式请参考**主流数字证书有哪些格式？**。

1. 执行以下命令生成keystore证书文件。

   keytool -genkey -alias mycert -keyalg RSA -keysize 2048 -keystore ./mydomain.jks

   - -keyalg：指定密钥类型，必须是RSA。
   - -keysize：指定密钥长度为2,048。
   - -alias：指定证书别名，可自定义。
   - -keystore：指定证书文件保存路径，证书文件名称可自定义。

   图 1-3 生成 keystore 证书文件

```
[Enter keystore password:
[Re-enter new password:
What is your first and last name?
[  [Unknown]:  www.example.com
What is the name of your organizational unit?
[  [Unknown]:  IT Dept.
What is the name of your organization?
[  [Unknown]:  HangZhou xxx Technologies,Inc.
What is the name of your City or Locality?
[  [Unknown]:  HangZhou
What is the name of your State or Province?
[  [Unknown]:  ZheJiang
What is the two-letter country code for this unit?
[  [Unknown]:  CN
Is CN=www.example.com, OU=IT Dept., O="HangZhou xxx Technologies,Inc.", L=HangZhou, ST=Zhe
Jiang, C=CN correct?
[  [no]:  Y

Enter key password for <mycert>
[        (RETURN if same as keystore password):
```

2. 输入证书保护密码，然后根据下表依次输入所需信息：

问题	说明	示例
What is your first and last name?	申请证书的域名。 **说明** – 多域名类型的证书，请填写需要绑定的主域名。 – 泛域名类型的证书，请填写泛域名。示例：*.example.com	www.example.com
What is the name of your organizational unit?	申请单位的所在部门名称。	IT Dept
What is the name of your organization?	申请单位的所在公司名称。	HangZhou xxx Technologies,Ltd
What is the name of your City or Locality?	申请单位的所在城市。	HangZhou
What is the name of your State or Province?	申请单位的所在省份。	ZheJiang
What is the two-letter country code for this unit?	申请单位所属国家，ISO国家代码（两位字符）。	CN

输入完成后，确认输入内容是否正确，输入Y表示正确。

3. 根据提示输入密钥密码。可以与证书密码一致，如果一致直接按回车键即可。

步骤3 通过证书文件生成证书请求。

1. 执行以下命令生成CSR文件。

   keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr

   – -sigalg：指定摘要算法，使用SHA256withRSA。
   – -alias：指定别名，必须与**•-alias**中keystore文件中的证书别名一致。
   – -keystore：指定证书文件。
   – -file：指定证书请求文件（CSR），名称可自定义。

2. 根据提示输入证书密码即可以生成“mydomain.csr”。

----结束

1.5 如何解决“审核失败 - 主域名不能为空”的问题?

问题描述

如果您在申请数字证书时选择自己上传CSR文件，可能收到“审核失败 – 主域名不能为空”的返回结果。

问题原因

在创建CSR文件时，未正确填写Common Name字段。

解决方法

重新制作并上传CSR文件，确保正确填写Common Name字段。

须知

Common Name字段必须是证书绑定的主域名。

为保证CSR文件内容正确，强烈建议您使用系统提供的系统生成CSR文件功能。同时，使用系统自动生成CSR文件功能，在数字证书颁发后还可支持不同格式的证书下载。

1.6 私有证书有效期相关问题

私有证书的有效期是多久?

私有证书的有效期是您根据申请证书时设置的有效期而定的。

说明

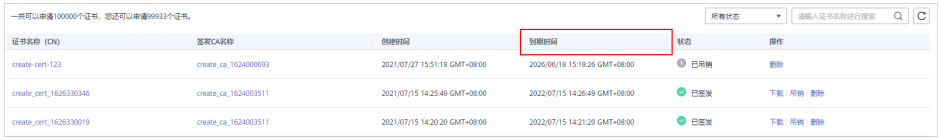
私有证书由处于激活状态的CA进行签发，所以，私有证书有效期设置时须满足：私有证书有效期≤签发的私有CA有效期。

图 1-4 设置有效期

私有证书由处于激活状态的CA进行签发

证书申请成功后，可在私有证书列表页面查看证书到期时间，如图1-5所示。私有证书到期后，需重新申请。

图 1-5 到期时间



私有证书的有效期快到了，怎么避免业务中断?

为了避免证书过期，导致业务中断，您需要提前轮换证书。在旧证书过期前，用新签发的证书进行替换。

1.7 私有证书管理服务是如何收费的?

私有CA和私有证书都是按需计费，将根据您的私有CA数量、私有证书数量进行收费。具体收费情况以购买页面显示为准。

如何停止私有 CA 或私有证书的计费?

私有CA和私有证书支持按需计费。其中，根CA创建后即开始计费；从属CA创建后不收费，激活后才开始计费。

如需停止计费，删除申请的私有CA和私有证书即可。

⚠ 注意

- 私有CA禁用期间也将保持收费。
- 用户执行删除私有CA操作后，私有CA不会立即删除。计划删除最快7天生效（根据您设置的推迟时间为准）。在此期间收费情况说明如下：
  - 如果用户未取消计划删除，私有CA被删除了，则在计划删除期间的私有CA不会收费；
  - 如果用户在计划删除期间，取消了计划删除，私有CA未被删除，则在计划删除期间的私有CA将保持收费。

  例如：您在2022年01月01日00:00执行了删除私有CA的操作，且设置的私有CA计划删除推迟时间为7天，7天后私有CA被删除，那么，PCA服务将不收取这7天的费用；如果您在2022年01月04日00:00取消了计划删除，私有CA未被删除，那么，PCA服务将补齐2022年01月01日00:00至2022年01月04日00:00期间的费用。