SSL常见密钥及证书格式

一、SSL中常见密钥格式与证书格式

## **1.1 密钥库文件格式（Keystore）**

在keystore里，包含两种数据：

1. 密钥实体（Key entity）——密钥（secret key）又或者是私钥和配对公钥（采用非对称加密）
2. 可信任的证书实体（trusted certificate entries）——只包含公钥

### **1) JKS 拓展名：.jks/.ks**

JKS (Java KeyStore): 密钥库的Java实现版本，provider为SUN，java的密钥存储文件,二进制格式,是一种 Java 特定的密钥文件格式， JKS的密钥库和私钥用不同的密码进行保护。

### **2) JCEKS 拓展名：.jce**

JCEKS （JCE[Java Cryptography Extension] Keystore）：密钥库的JCE实现版本，provider为SUN JCE，java的密钥存储文件，在JCEKS中存储和装载不同条目的过程类似于JKS，相对于JKS安全级别更高，JDK1.4版本后可直接使用，保护Keystore私钥时采用TripleDES。

### **3) PKCS12 拓展名：.p12/.pfx**

PKCS12：是公钥加密标准，它规定了可包含所有私钥、公钥和证书。其以二进制格式存储，也称为 PFX 文件，在windows中可以直接导入到密钥区，密钥库和私钥用相同密码进行保护

### **4) BKS 拓展名：.bks**

BKS（Bouncycastle Keystore）：密钥库的BC实现版本，provider为BC，保护Keystore私钥时采用TripleDES，它能够防止证书库被不小心修改（Keystore的keyentry改掉1个bit都会产生错误），BKS能够跟JKS互操作。

### **5) BUER 拓展名：.ubr**

BUDER（Bouncycastle UBER Keystore）：密钥库的BC更安全实现版本，provider为BC，当密码是通过命令行提供的时候，它只能跟keytool交互。整个keystore是通过PBE/SHA1/Twofish加密，因此 keystore能够防止被误改、察看以及校验。SunJDK允许你在不提供密码的情况下直接加载一个Keystore，类似cacerts，UBER不 允许这种情况。

## **1.2 证书文件格式（Certificate）**

### **1) DER 拓展名：.cer/.crt/.rsa**

DER（ASN .1 DER）：用于存放证书，不含私钥，为二进制。

.DER =扩展名.DER用于二进制DER编码的证书。这些证书也可以用CER或者CRT作为扩展名。

.CRT = 扩展名CRT用于证书。证书可以是DER编码，也可以是PEM编码。扩展名CER和CRT几乎是同义词。这种情况在各种unix/linux系统中很常见。

.CER = CRT证书的微软型式。可以用微软的工具把CRT文件转换为CER文件（CRT和CER必须是相同编码的，DER或者PEM）。扩展名为CER的文件可以被IE识别并作为命令调用微软的cryptoAPI（具体点就是rudll32.exe cryptext.dll, CyrptExtOpenCER），进而弹出一个对话框来导入并/或查看证书内容。

### **2) PKCS7 拓展名：.p7b/.p7r**

PKCS#7,也叫做加密消息的语法标准，由RSA安全体系在公钥加密系统中交换数字证书产生的一种加密标准。 其中p7b以树状展示证书链，不含私钥；p7r为CA对证书请求签名的回复，只能用于导入

### **3) CMS 拓展名：.p7c/.p7m/,p7s**

CMS(Cryptographic Message Syntax):

p7c：只保存证书；

p7m：signature with enveloped data；

p7s：时间戳签名文件

### **4) PEM 拓展名：.pem**

PEM（Privacy nhanced Mail）：该编码格式在RFC1421中定义，但他也同样广泛运用于密钥管理，实质上是 Base64 编码的二进制内容。

### **5) PKCS10 拓展名：.p10/.csr**

CSR：证书签发请求(Certificate Signing Request)，或者叫做认证申请，是一个发送到CA的请求认证信息。有两种格式，应用最广泛的是由PKCS#10定义的，另一个用的少的是由SPKAC定义的，主要应用于网景浏览器。 P10：证书请求文件，类似于CSR文件。

### **6) SPC 拓展名：.pvk/.spc**

SPC(Software Publishing Certificate)：微软公司特有的双证书文件格式，经常用于代码签名，其中.pvk用于保存私钥、.spc用于保存公钥。

# 二、CSR文件生成方法

在申请证书前，用户需要提交CSR文件，以完成身份校验并生成证书公钥文件。生成CSR文件时会同时生成私钥文件，请妥善保管和备份。

## **2.1 使用OpenSSL工具生成CSR文件**

1. 安装OpenSSL工具。
2. 执行以下指令生成CSR文件。

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

1. 按提示输入以下信息，此处填写的信息要和补全证书信息时填写的内容一致。

| **字段** | **解释** | **示例** | **约束** |
| --- | --- | --- | --- |
| Country Name | ISO国家代码 | CN | 英文大写，两位字符 |
| State or Province Name | 所在省份 | 北京 | 中英文均可 |
| Locality Name | 所在城市 | 北京 | 中英文均可 |
| Organization Name | 公司名称 | 北京金山云网络技术有限公司 | 中英文均可 |
| Organizational Unit Name | 部门名称 | 产品部 | 中英文均可 |
| Common Name | 申请证书的域名 | www.ksyun.com |  |
| Email Address | 无需输入 |  |  |
| A challenge password | 无需输入 |  |  |
| An optional company name | 无需输入 |  |  |

[root@xxxx ~]# openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout myprivate.key -out mydomain.csr

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) [XX]:CN

State or Province Name (full name) []:Beijing

Locality Name (eg, city) [Default City]:Beijing

Organization Name (eg, company) [Default Company Ltd]:Beijing xxx Technologies.Inc.

Organizational Unit Name (eg, section) []:IT Dept

Common Name (eg, your name or your server's hostname) []:www.myhost.com

Email Address []:

Please enter the following 'extra' attributes

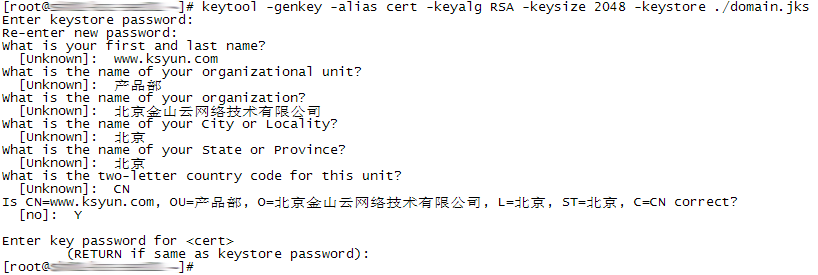
to be sent with your certificate request

A challenge password []:

1. 完成后，会在当前目录下生成 private.key（私钥文件）和 domain.csr（证书请求文件）。

## **2.2 使用Keytool工具生成CSR文件**

1.输入指令 **keytool -genkey -alias cert -keyalg RSA -keysize 2048 -keystore ./domain.jks**



2.输入证书保护密码，并按提示输入以下信息，**注意：此处填写的信息要和补全证书信息时填写的内容一致**

| **问题** | **解释** | **示例** | **约束** |
| --- | --- | --- | --- |
| What is your first and last name? | 申请证书的域名 | www.ksyun.com |  |
| What is the name of your organizational unit? | 部门名称 | 产品部 | 中英文均可 |
| What is the name of your organization? | 公司名称 | 北京金山云网络技术有限公司 | 中英文均可 |
| What is the name of your City or Locality? | 所在城市 | 北京 | 中英文均可 |
| What is the name of your State or Province? | 所在省份 | 北京 | 中英文均可 |
| What is the two-letter country code for this unit? | ISO国家代码 | CN | 英文大写，两位字符 |

4.完成后确认信息无误，[no]:Y 输入

5.输入密钥密码

6.通过证书文件生成证书请求

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

CSR文件生成方法

完成