SSL 在线工具使用手册

中金金融认证中心

运营中心

2017 年 5 月

文档修订记录

版本	内容	日期	编写	审核
1.0	第一版	2017.5.10	王天昊	

目录

一、 CFCA SSL 在线工具平台介绍

1.1 什么是 SSL 在线工具平台？

CFCA SSL 在线工具平台由 CFCA 自主研发，意在方便客户完成服务器证书制作、检查、格式转换和网站漏洞检测等相关操作。

1.2 SSL 在线工具平台有哪些功能？

SSL 在线工具平台有哪些功能：

CSR 生成：用于生成服务器公钥证书时用到的 CSR（PKCS#10 申请书）文件和私钥。

CSR 查看：查看生成服务器证书填写的相关信息（域名、IP 等）。

证书查看：查看公钥证书信息（域名、密钥算法、颁发机构等）。

证书公私钥匹配检查：查看公钥证书和私钥是否匹配。

证书格式转换：转换各中间件或服务器使用的不同格式证书。

站点认证配置：部署 CFCA EV、OV 服务器证书的网站访客点击该图标即可链接到 CFCA 的站点认证页面，认证该网站的相关信息。

SSL 网站检查：检查开启 https 协议网站的安全性和服务器证书信息。

SSL 漏洞检查：检查网站 HeartBleed、POODLE、FREAK 漏洞是否存在。

证书链下载：下载 CFCA EV、OV 服务器证书证书链文件。

二、 CFCA SSL 在线工具使用方法

2.1 CSR 生成

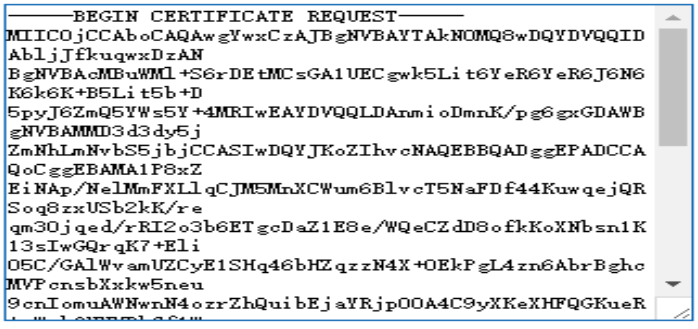
填写办理服务器证书的相关信息（注：SSL 在线平台只支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法的服务器证书）。

CSR生成 | CSR查看 | 证书查看 | 证书公私钥匹配检查 | 证书格式转换 | 站点认证配置 | SSL网站检测 | SSL漏洞检测 | 证书链下载

填写信息

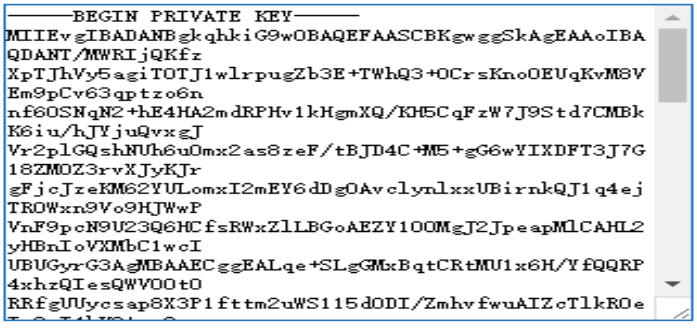
填写完成相关信息后，点击生成 CSR，即可生成相应的 CSR（PKCS#10 申请书，用于申请公钥证书）文件和密钥（key.txt 可以直接保存.key 格式）文件，下载并保存（**注：私钥一定要留存好，之后合成服务器证书时需再次用到**）建议不要输入 KEY 密码。

CSR



保存

KEY



保存

2.2 CSR 查看

上传需要查看的 CSR 文件信息，页面会自动显示出 CSR 文件内容，以便用户查看自己申请服务器证书时填写的信息是否正确。

CSR解析结果

通用名(CN)	www.cfca.com.cn
组织单元(OU)	技术部
组织(O)	中金金融认证中心有限公司
城市(L)	北京
省份(S)	北京
国家(C)	CN
密钥算法	RSA
密钥长度	2048
哈希算法	SHA256

2.3 证书查看

上传需要查看的服务器证书文件，页面会自动显示出证书文件内容，其中包括域名、颁发者、密钥用法、密钥算法等。

证书解析结果

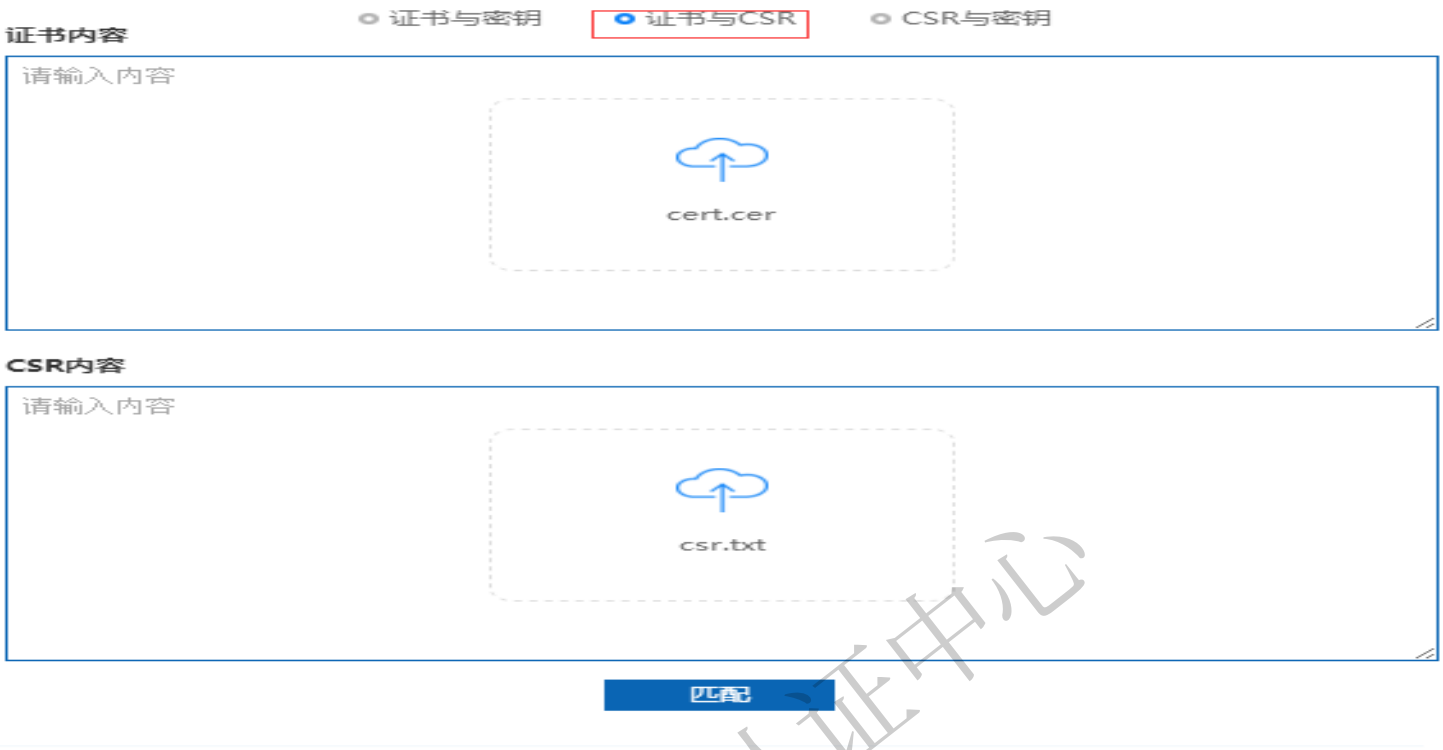
通用名(CN)	www.cfca.com.cn
组织单元(OU)	技术部
组织(O)	中金金融认证中心有限公司
城市(L)	北京
省份(S)	北京
国家(C)	CN
密钥算法	RSA
密钥长度	2048
哈希算法	SHA256
序列号	1003802675
生效日期	2017-02-17 10:47:40
截止日期	2018-02-17 10:47:40
主题备用名	www.cfca.com.cn
颁发者	CN=CFCA TEST OCA1, O=China Financial Certification Authority, C=CN
密钥用法	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
增强密钥用法	

2.4 证书公私钥匹配查询

上传需要查看的公钥证书、私钥、CSR 匹配文件，页面会自动显示出是否匹配，并提示匹配成功或者失败。

公钥证书与秘钥：

公钥证书与 CSR：



CSR 与秘钥：

2.5 证书格式转换

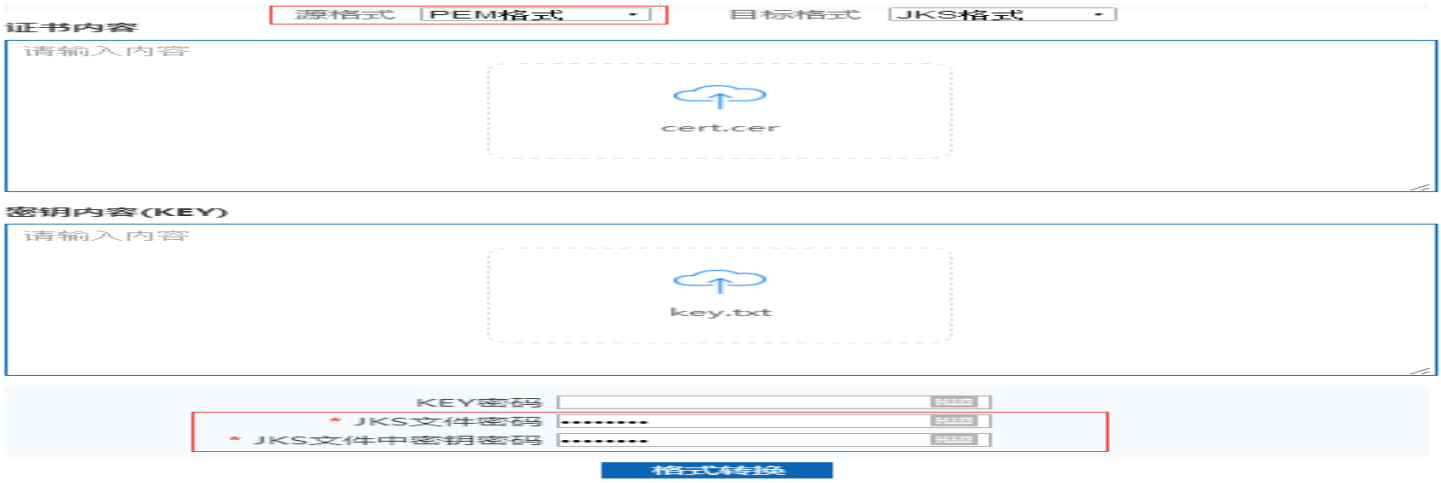
在 CFCA 申请服务器证书，获得序列号和授权码之后，在 CFCA 统一下载平台，提交 CSR(PKCS#10 申请书)，即可下载对应的服务器公钥证书。

PEM 格式为（.key 私钥和.cer 公钥两个文件）

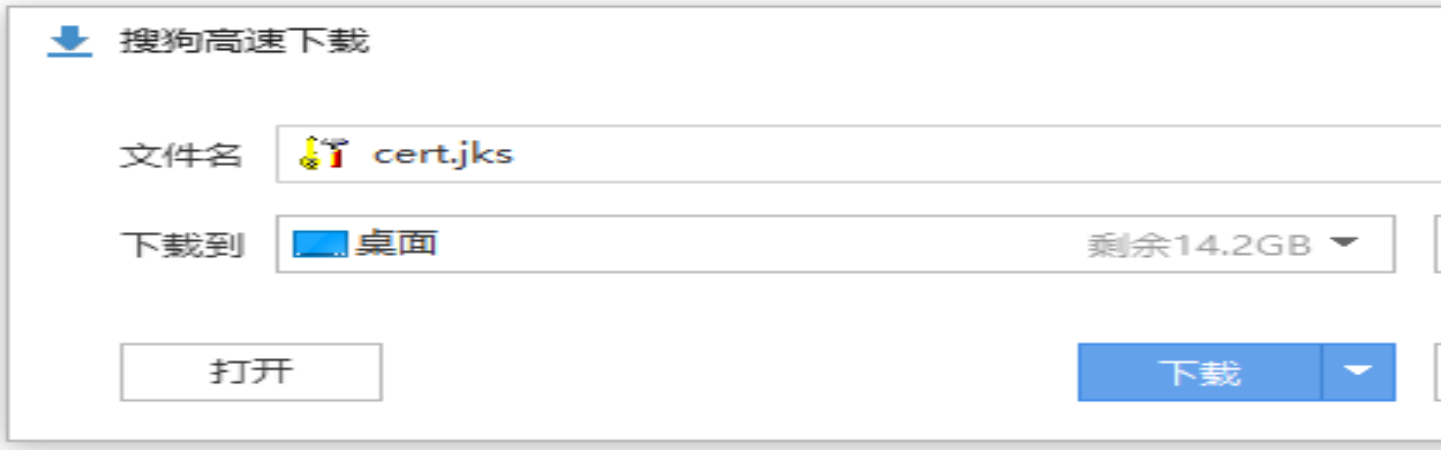
JKS 格式为（.jks 公私钥包含在一个文件，同时含有证书链）

P12 格式为（.pfx 为 windows 系统等可直接安装文件）

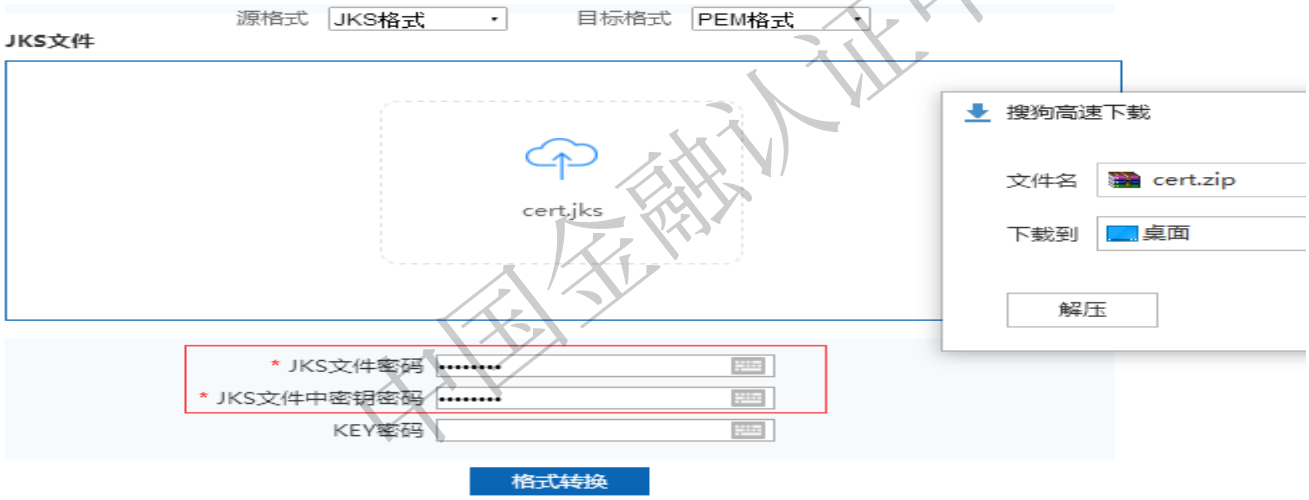
- PEM （用于部署 Apache、Nginx）格式转 JKS（用于部署 Tomcat、Weblogic、JBoss）格式（注：格式转换需要设置 JKS 文件密码）



格式转换后下载 jks 格式文件



- JKS（用于 Tomcat、Weblogic、JBoss）格式转 PEM（用于 Apache、Nginx）格式（注：格式转换需要输入 JKS 文件密码）



- JKS（用于 Tomcat、Weblogic、JBoss）格式转 P12（用于 IIS）格式（注：格式转换需要输入 JKS 文件密码并设置 P12 文件密码）

2.6 站点认证配置

输入需要生成站点信任的域名信息(站点信任只适用于办理 CFCA EV、OV 证书)，点击生成站点信任的.png 图片

2.7 SSL 网站检测

输入需要检测的网站域名信息，检测结果如下：

填写信息

域名 www.cfca.com.cn 端口 443 检测

检测结果

证书信息	
证书主题	CN=www.cfca.com.cn, OU=运行部, O=中金金融认证中心有限公司, L=北京, ST=北京, C=CN, SERIALNUMBER=91110000759626025U, BusinessCategory=Private Organization, 1.3.6.1.4.1.311.60.2.1.1=北京, 1.3.6.1.4.1.311.60.2.1.2=北京, 1.3.6.1.4.1.311.60.2.1.3=CN
主题备用名	www.cfca.com.cn,pboc.cfca.com.cn,cez.cfca.com.cn,cs.cfca.com.cn,webverify.cfca.com.cn,evwebverify.cfca.com.cn,ssl.cfca.com.cn,freessl.cfca.com.cn
序列号	25A0158481680CF85187
颁发者	CN=CFCA EV OCA, O=China Financial Certification Authority, C=CN
生效日期	2016-02-26 10:44:15
截止日期	2018-02-26 10:44:15
密钥算法	RSA
密钥长度	2048
哈希算法	SHA256
密钥用法	Digital Signature, Key Encipherment
增强密钥用法	TLS Web Server Authentication
证书链信息	
证书主题	CN=www.cfca.com.cn, OU=运行部, O=中金金融认证中心有限公司, L=北京, ST=北京, C=CN, SERIALNUMBER=91110000759626025U, BusinessCategory=Private Organization, 1.3.6.1.4.1.311.60.2.1.1=北京, 1.3.6.1.4.1.311.60.2.1.2=北京, 1.3.6.1.4.1.311.60.2.1.3=CN
颁发者	CN=CFCA EV OCA, O=China Financial Certification Authority, C=CN
生效日期	2016-02-26 10:44:15
截止日期	2018-02-26 10:44:15
^^	
证书主题	CN=CFCA EV OCA, O=China Financial Certification Authority, C=CN
颁发者	CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
生效日期	2012-08-08 14:06:31
截止日期	2029-12-29 14:06:31
^^	
证书主题	CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
颁发者	CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
生效日期	2012-08-08 11:07:01
截止日期	2029-12-31 11:07:01

SSL协议	
SSL2.0	不支持
SSL3.0	不支持
TLS1.0	不支持
TLS1.1	支持
TLS1.2	支持
密码套件	
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	
TLS_DHE_RSA_WITH_SEED_CBC_SHA	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	
TLS_RSA_WITH_IDEA_CBC_SHA	
TLS_RSA_WITH_3DES_EDE_CBC_SHA	
TLS_RSA_WITH_SEED_CBC_SHA	
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	

2.8 SSL 漏洞检测

输入需要检测漏洞的网站，选择漏洞类型，进行检测：

CSR生成 CSR查看 证书查看 证书公私钥匹配检查 证书格式转换 站点认证配置 SSL网站检测 SSL漏洞检测 证书链下载

填写信息

漏洞类型 FREAK 域名 www.cfca.com.cn 端口 443 检测

恭喜您, www.cfca.com.cn不受FREAK漏洞影响

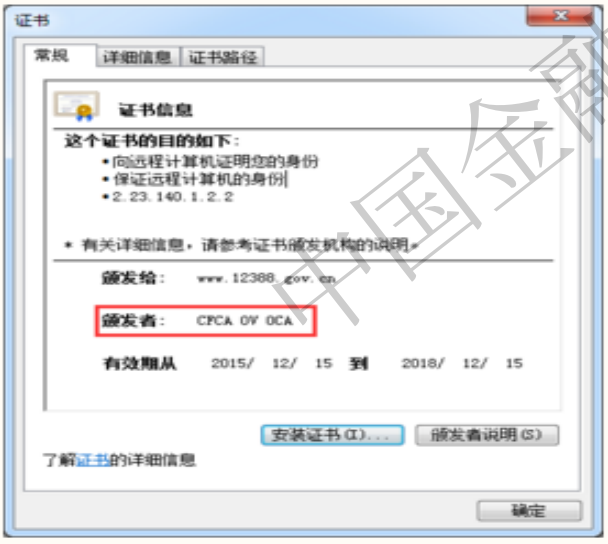
2.9 证书链下载

按照需要下载证书链：说明对应下载 其他证书链下载

证书链下载

OV证书链

如果证书的颁发者是CFCA OV OCA,请下载以下中级证书和根证书。



CFCA OV OCA编码：Base64
CFCA OV ROOT编码：Base64

下载

EV证书链

如果证书的颁发者是CFCA EV OCA,请下载以下中级证书和根证书。

CFCA EV OCA编码：Base64
CFCA EV ROOT编码：Base64

下载

附录:非入根 CFCA 服务器证书制作介绍

服务器证书制作方法:

输入下载证书的两码（参考号，授权码），上传之前生成好的 CSR（PKCS#10 申请书）文件保存即可。