查看证书内容

openssl x509 -in ssl.crt -noout -text

openssl x509 -in ssl.cer -noout –text

openssl pkcs12 -info -in cert.pfx

1. 证书签发商提供的文件

CACertificate-ROOT-2.cer

发行商自己的**根证书**，所有其他证书都由该根证书签发或派生

CACertificate-INTERMEDIATE-1.cer

发行商自己生成的**中级证书**，以根证书签发。中间证书用于向我们签发域名证书

ServerCertificate.cer

发行商通过中级证书签发给我们的**域名证书**，里面有我们的域名

star.yaofangwang.com.csr

\*.yaofangwang.com 域名的证书请求文件

star.yaofangwang.com.key

\*.yaofangwang.com 域名证书的私匙

Key.pem

集成了 域名证书私匙、域名证书、中级证书 的文件

PKCS7.p7b

PKCS #7 Certificate File， Base64格式的存储域名证书、中级证书、根证书文件

1. Nginx需要的证书

ssl\_certificate: 证书文件(后缀名crt的文件)

制作过程如下

1. 新建一个文本文件
2. 依次将：域名证书、中级证书、跟证书 三个文件里的内容copy到新建文件中
3. 保存该文件为证书文件，如 star.yaofangwang.com.crt

ssl\_certificate\_key: 域名证书私匙文件，即 star.yaofangwang.com.key

3 Java服务器需要的证书

我们的Java服务器需要 pfx 格式的证书文件

PFX证书 == CRT证书（域名证书、中级证书、根证书） + 域名私匙 + 自定义密码

制作过程如下

1. 使用 pwgen 产生一个16位随机密码, 命令行： pwgen 16; 也可以使用其他方式生成一个随机密码，该密码用于加密 pfx文件; (pwgen需要安装)
2. 生成cert.pfx文件

openssl pkcs12 -export -in star.yaofangwang.com.crt -inkey star.yaofangwang.com.key -out cert.pfx

注意，该命令行执行后需要输入上一步生成的密码

1. 将密码写入文件 pfx-password.txt 中
2. 将 cert.pfx，pfx-password.txt 两个文件copy到java服务器的 cert 目录，替换其中的文件