SSL调研

1. 前言

此次调研是因为微信公众开发平台的设备功能使用时，需要开通https协议，否则某些功能无法完成，而要开通https协议，则需要进行SSL认证。去相应机构认证获取crt文件和密码，然后到tomcat和nginx配置文件配置即可(注：https可以理解为安全加密版的http)

1. 什么叫SSL

安全套接层（Secure Sockets Layer，[缩写](https://zh.wikipedia.org/wiki/%E7%B8%AE%E5%AF%AB)：SSL）是一种[安全协议](https://zh.wikipedia.org/wiki/%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE)，使用https协议才会用到的。

1. SSL的意义

给传输层加密只是SSL的作用之一，SSL 证书更主要的用处其实在于验证网站及其背后企业的真实性以及合法性。

1. SSL认证机构的选择

在SSL认证有的付费，有的免费，有什么区别。其实在认证时，无论收费和免费的，都可以看看他们对SSL认证的相关介绍，就了解区别了。更贵的 SSL 证书的验证过程通常更加严谨，过程更复杂、签发更严谨，价格自然就更高。另外，你购买证书时往往还同时为顾客购买了一份保险，越贵的认证收费，认证机构给非法公司颁发了证书，导致顾客在网站上遭受损失，那么认证机构也需要对顾客进行一定的赔偿，而收费越贵的，一般赔偿会更多。

1. SSL认证

通过调研最后选择国内深圳沃通来进行SSL认证，选择该机构的原因，一是有免费版的，二是在国内知名度很高,国内包括南方电网，武汉大学用的都是这个机构认证

的SSL证书。

链接地址: <https://buy.wosign.com/free/>，可以申请免费的SSL证书

1. SSL配置

注:配置使用到的相关文件，在申请ssl以后，可以下载到。

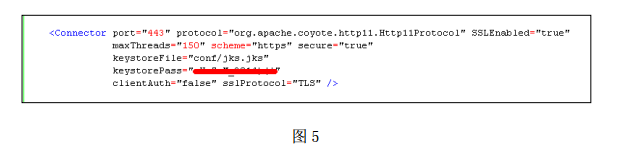
1. 配置tomcat

首先找到安装 Tomcat 目录下该文件“Server.xml”，一般默认路径都是在 Conf 文件夹 中。然后用文本编辑器打开该文件，接着找到如下所示 图 4



（注意：不要直接拷贝所有配置，只需添加 keystoreFile，keystorePass 这两个参数即可！）

默认情况下是被注释的，我们可以把“”去掉， 然后对其节点进行相应的修改，比如：port：端口号；keystoreFile：证书路径(例如：conf/SSL.jks)； keystorePass：证书密码。图 5



最后保存该配置文件，然后重启 Tomcat 后再次访问即可。

1. 配置nginx

打开 Nginx 安装目录下 conf 目录中的 nginx.conf 添加。

server {

listen 443;

server\_name localhost;

ssl on;

ssl\_certificate sslkey/wosign.com.crt; （证书公钥）

ssl\_certificate\_key sslkey/wosign.com.key; （证书私钥）

ssl\_session\_timeout 5m;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL:!eNULL;

ssl\_prefer\_server\_ciphers on;

location / {

root html; index index.html index.htm;

}

} 保存退出，并重启nginx，就可以通过https访问设置的url

1. 总结

整个过程没什么特别的难点，如果不需要配置nginx的话，只需要配置tomcat即可访问。如果需要配置nginx的话，建议先配置tomcat访问成功以后，在配置nginx，不要一步到位去配置，否则出错，找不到原因。