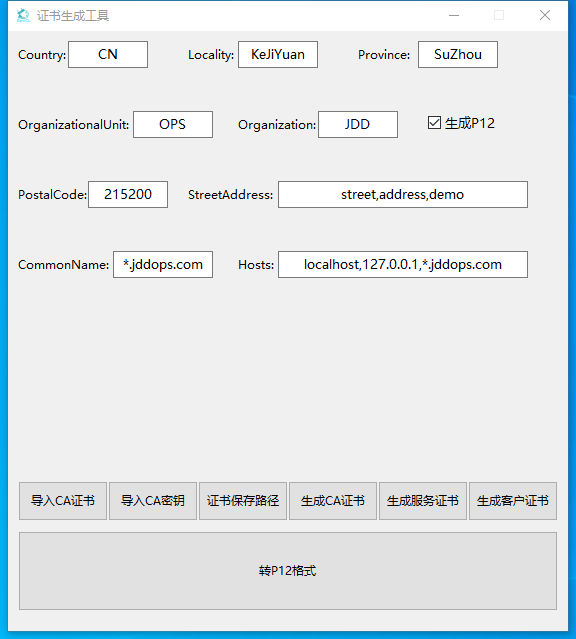
### Nginx与Chrome实现SSL双向认证访问

首先一键部署tengine和openssl以及tengine的一些插件。脚本文件已经附加，

生成ca和服务端以及客户端证书。一般我们使用openssl来生成。我用golang写了一个生成工具来省事。  
工具说明：  
软件界面：

软件使用说明：

1. 软件内置的证书有效期是从生成时间开始10年。
2. 如果不设置证书保存路径，默认在程序运行目录保存证书
3. 默认不生成P12的证书（Windows和Mac系统需要P12导入）。可以通过勾选打开 P12证书生成。
4. 勾选生成P12的证书会内置CA的证书方便导入游览器。
5. Ca根证书与客户端和服务端证书的CommonName不能相同。
6. 客户端和服务端证书会根据系统时间的时间戳生成多个，但是ca只能生成一个 多生成CA根证书会覆盖（注意注意注意）
7. 证书的StreetAddress和Hosts以逗号分割类容

# Chrome导入P12证书步骤：

1. 打开Chrome游览器设置。
2. 在左侧选择隐私设置与安全性
3. 在右侧的隐私设置与安全性分支下的安全
4. 在安全下选择管理证书
5. 在弹出的窗口选择受信任的根证书颁发机构标签卡点击导入
6. 在证书导入向导欢迎页点击下一步
7. 先导入CA根证书
8. 再到个人标签下导入P12客户端证书
9. 在要导入的文件处选择生成的P12格式Client证书点击下一步
10. 输入生成P12证书时设置的证书密码点击下一步
11. 在证书存储选择根据证书类型，自动选择证书存储，点击下一步
12. 点击完成证书导入
13. 弹出警告，点击是确认导入根证书
14. 查看受信任的根证书颁发机构标签下根证书是否导入成功
15. 查看个人标签下Client证书是否导入成功

生成后的P12证书导入游览器截图

