# openssl 安装配置

OpenSSL\_Home

D:\DevelopmentTool\openssl-0.9.8k\_X64

Path追加

;D:\DevelopmentTool\openssl-0.9.8k\_X64\bin

修改openssl.cnf：

dir = D:\\DevelopmentTool\\openssl-0.9.8k\_X64\\demoCA # ./demoCA Where everything is kept

# echo 构建目录

mkdir certs

mkdir crl

mkdir newcerts

mkdir private

echo 构建文件

echo 0>index.txt

echo 01>serial

echo 构建随机数

openssl rand -out private/.rand 1000

# ===A.构建根证书===

1.构建根证书私钥

openssl genrsa -aes256 -out private/ca.key.pem 2048

2.生成根证书签发申请

openssl req -config ../openssl.cnf -new -key private/ca.key.pem -out private/ca.csr -subj "/C=CN/ST=HUBEI/L=WUHAN/O=cas/OU=cas/CN=\*.cas.org"

3.签发根证书

openssl x509 -req -days 10000 -sha1 -extensions v3\_ca -signkey private/ca.key.pem -in private/ca.csr -out certs/ca.cer

4.根证书转换

openssl pkcs12 -export -cacerts -inkey private/ca.key.pem -in certs/ca.cer -out certs/ca.p12

5.查看密钥库信息

keytool -list -keystore D:\DevelopmentTool\openssl-0.9.8k\_X64\demoCA\certs\ca.p12 -storetype pkcs12 -v -storepass 678789

# ===B.构建服务器证书===

1.构建服务器私钥

openssl genrsa -aes256 -out private/server.key.pem 2048

2.生成服务器证书签发申请

openssl req -config ../openssl.cnf -new -key private/server.key.pem -out private/server.csr -subj "/C=CN/ST=HUBEI/L=WUHAN/O=cas/OU=cas/CN=www.cas.org"

3.签发服务器证书

openssl x509 -req -days 3650 -sha1 -extensions v3\_req -CA certs/ca.cer -CAkey private/ca.key.pem -CAserial ca.srl -CAcreateserial -in private/server.csr -out certs/server.cer

4.服务器证书转换

openssl pkcs12 -export -clcerts -inkey private/server.key.pem -in certs/server.cer -out certs/server.p12

# ===C.构建客户端证书===

1.产生客户私钥

openssl genrsa -aes256 -out private/client.key.pem 2048

2.生成客户端签发申请

openssl req -config ../openssl.cnf -new -key private/client.key.pem -out private/client.csr -subj "/C=CN/ST=HUBEI/L=WUHAN/O=cas/OU=cas/CN=cas"

3.签发客户证书

openssl ca -config ../openssl.cnf -days 3650 -in private/client.csr -out certs/client.cer -cert certs/ca.cer -keyfile private/ca.key.pem

4.客户证书转换

openssl pkcs12 -export -inkey private/client.key.pem -in certs/client.cer -out certs/client.p12

## C->3报错：

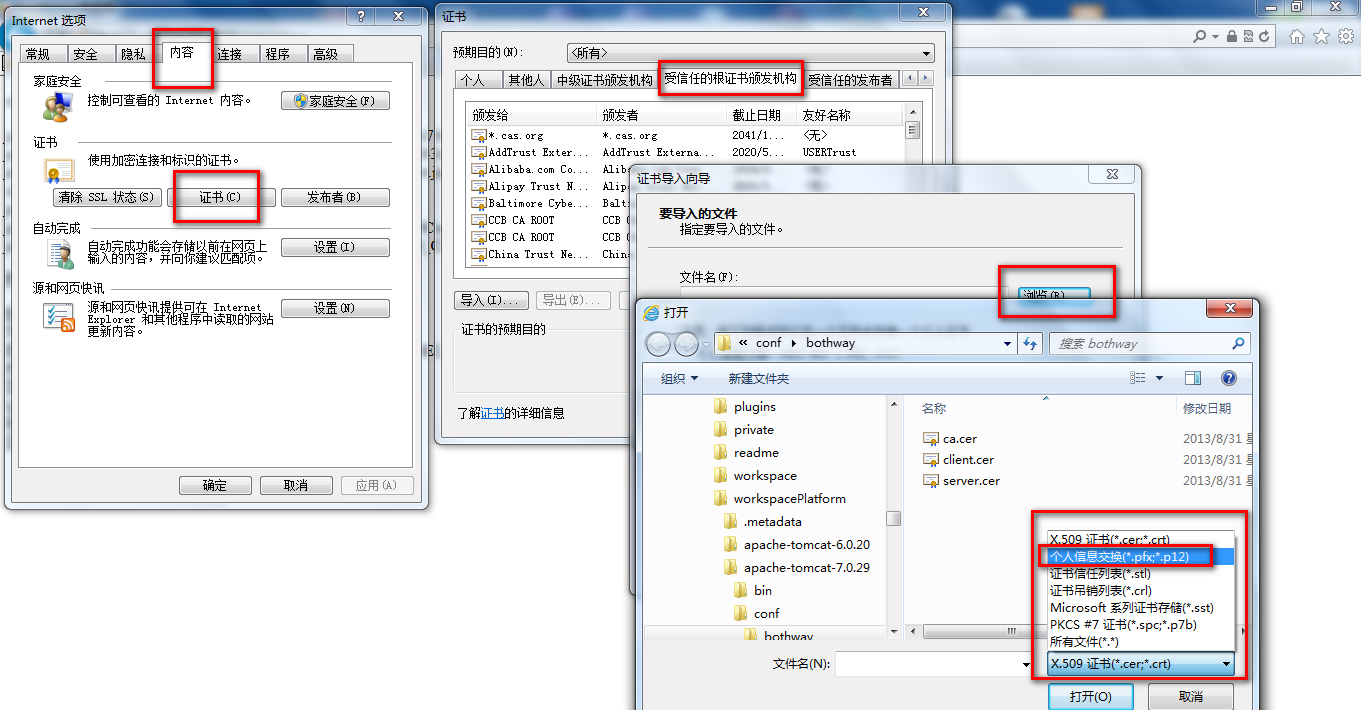
I am unable to access the ./demoCA/newcerts directory

./demoCA/newcerts: No such file or directory

修改openssl.cnf：

dir = D:\\DevelopmentTool\\openssl-0.9.8k\_X64\\demoCA # ./demoCA Where everything is kept

# 导入根证书ca.p12



# 导入客户端证书client.p12

