**实 验 报 告**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |
| --- | --- |
| **课程名称：** | **信息系统安全** |
| **学生姓名：** | **吴双** |
| **学生学号：** | **201436614018** |
| **学生专业：** | **软件工程** |
| **开课学期：** | **2016-2017 第二学期** |

**XXXX单位**

**2016年5月**

**实验3-数字证书及其应用**

**（安全协议）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **地 点：** | B7 楼 | 133 房； | **实验台号：** |  |
| **实验日期与时间：** | 2017年3月21号 | | **评 分：** |  |
| **预习检查纪录：** | 良好 | | **实验教师：** | 陈春华 |

**实验过程与结果**

使用文件与图片方式，详细展现实验过程与内容等。

请合理划分章节！

## 了解实验原理：

PKI是由公钥密码技术、数字证书、证书认证中心和关于公开密钥的安全策略等基本成分共同组成，管理密钥和证书的系统或平台。一个完整的PKI系统必须具备证书认证机构（Certificate Authority、CA）、数字证书库、密钥备份及恢复系统、证书作废系统和应用接口（API）等基本组成部分。

## 具体过程

### 搭建pki

本次实验在腾讯云服务器上搭建pki体系。

云服务器系统：



先下载easy-rsa：

yum install easy-rsa

把下载的easy-rsa拷到新的目录以防不当操作。

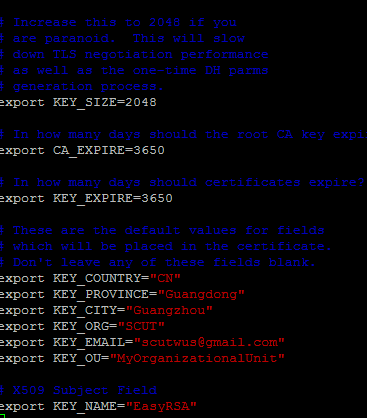
cp -R /usr/share/easy-rsa/ /etc/ easy-rsa/

从库里下载的easy-rsa为2.0版本

从github上找到文档说明：

https://github.com/OpenVPN/easy-rsa-old/blob/master/doc/README-2.0#L87

配置vars文件：



KEY\_SIZE=2048**#默认密钥长度为1024，建议为2048**

CA\_EXPIRE=3650 **#默认CA证书和私钥有效期为3650天**

KEY\_EXPIRE=3650 **#默认服务器/客户端证书和私钥有效期为3650天**

修改完成后，

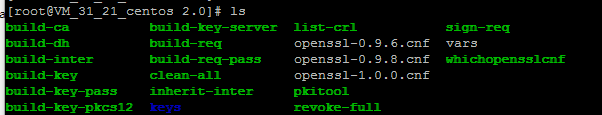
执行：

**#source ./vars #加载配置参数**

**#./clean-all #清空以前生成的keys**

**#./build-ca#构建CA私钥和自签发证书**

此时会生成一个keys文件夹。



#cd keys 可以发现生成了如下文件：



ca证书和密钥生成完成。

PKI体系构建完成

### 签发证书

easy-rsa2.0无法通过给定的公钥来生成证书，只能自己生成一对公私密钥并签发对应的证书。

对于签发证书有两个命令

#./build-key client #该命令生成客户端主机所需的证书，其CN字段默认值为client

#./build-key-server server#该命令生成OpenVPN服务器所需的证书，其CN字段默认值为server

生成原理上两者并无不同。

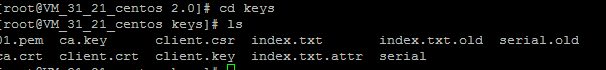
由于实验要做的是电子邮件证书，故选择#./build-key client  
将vars的使用者邮件字段改为需要发邮件的邮箱

[我用的是scutwus@gmail.com](mailto:我用的是scutwus@gmail.com) 故：



运行 ./build-key client

keys文件：



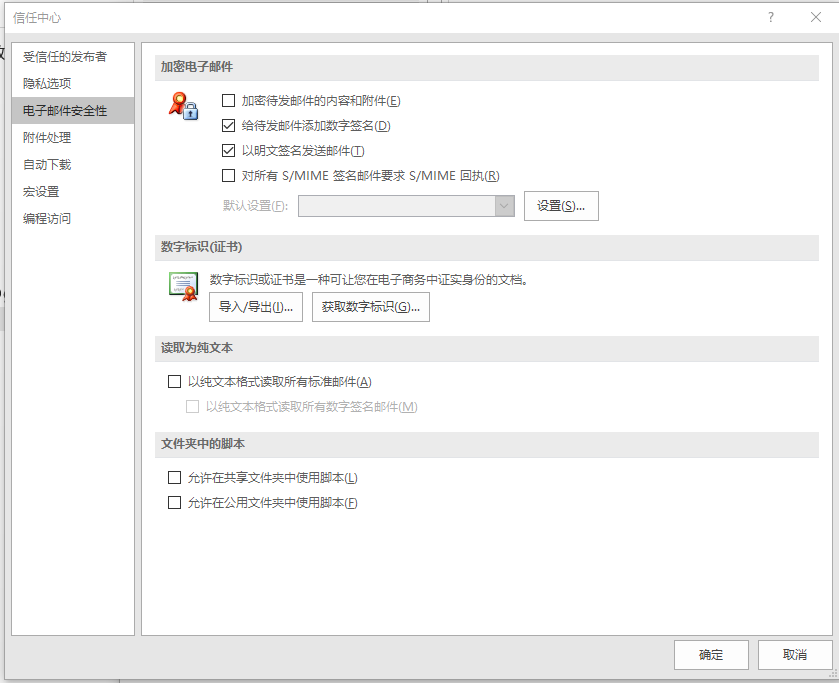
可以发现已经生成完成。

利用winSCP将生成的keys拷到本地。

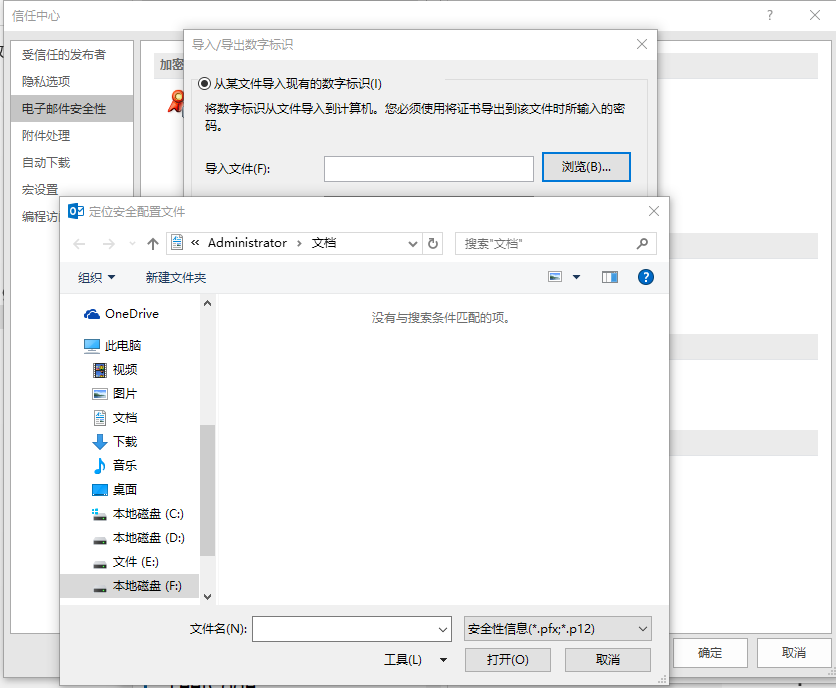
### 对电子邮件进行数字签名

打开outlook2016

文件-选项-信任中心-信任中心设置-电子邮件安全性-数字标识。



导入、



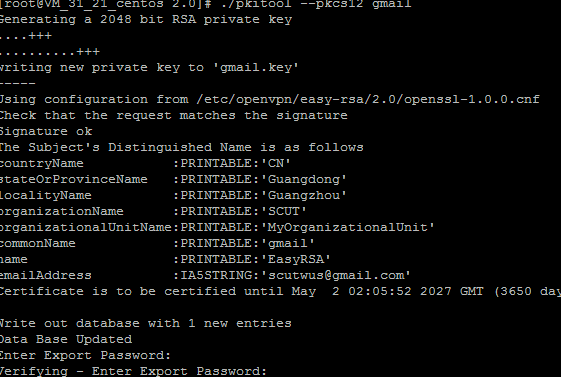
发现需要P12后缀的签名。此证书包含使用者公私钥。

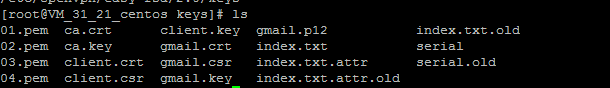
查阅文档发现easy-rsa有直接生成p12证书的命令

pkitool --pkcs12 client

键入

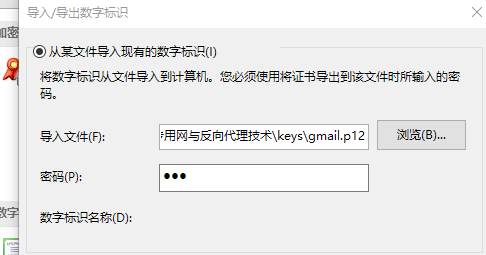
因为P12证书有私钥，所以需要设置密码。



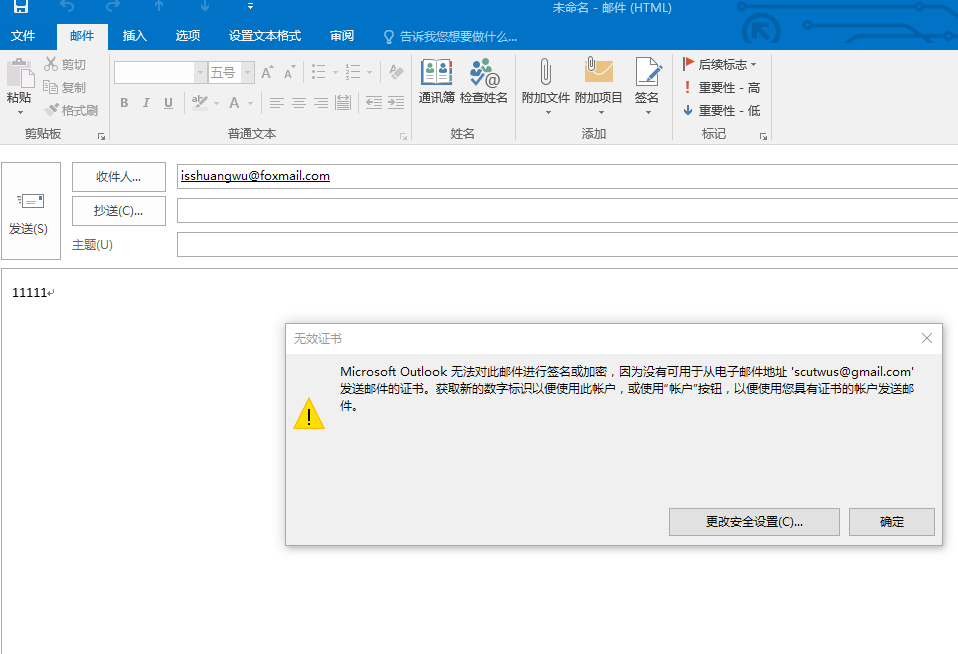


成功生成

导入outlook



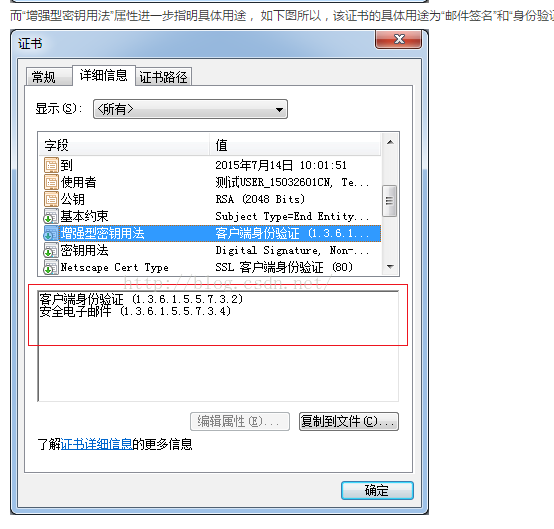
导入成功



报错无法找到，查阅资料，

在<http://blog.csdn.net/yyfzy/article/details/48343295>

证书必须有安全电子邮件用法的证书才能用于电子邮件发送。



easy-rsa无法找到生成此类证书的命令。

于是转用openssl。

编辑openssl.cnf



一定要注意[ policy\_match ]中的设定的匹配规则，是有可能因为证书使用的工具不一样，导致即使设置了csr中看起来有相同的countryName,stateOrProvinceName等，但在最终生成证书时会报错。

在CA目录下创建两个初始文件：

# touch index.txt serial

# echo 01 > serial

生成根证书

# cd /etc/pki/CA/

# openssl genrsa -out private/cakey.pem 2048

为客户端密钥生成证书签署请求。

openssl req -new -key private/client.key -out client.csr

注意邮件选项需要与发送邮件的邮箱一致。

用ca签署证书

openssl ca -in client.csr -out client.crt

将ca和生成的csr，key文件从服务器上拷到电脑上。

由于邮件需要pfx格式证书。

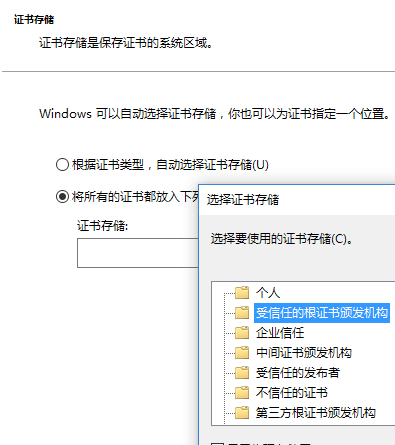
在命令提示符下,输入openssl 回车

看到openssl>;

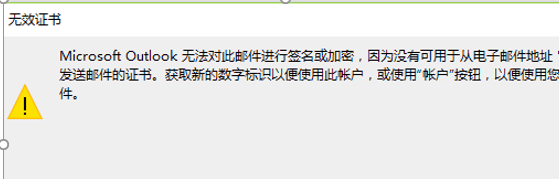
再输入

pkcs12 -export –in client.crt -inkey client.key -out client.pfx

安装根证书，切记不能选择自动，要如下图选择，



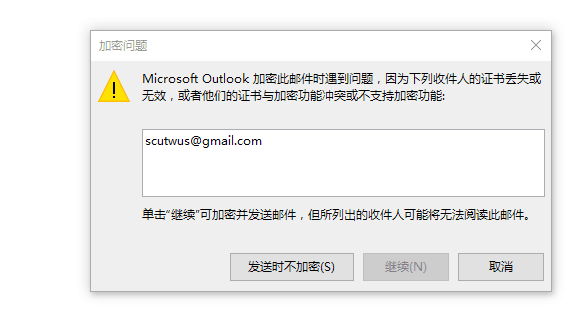
否则pfx证书安装了outlook也不会用。猜测直接安装把ca当成了一般的证书.会一直报下图的错误：



给outlook里添加pfx，并勾选加密选项。



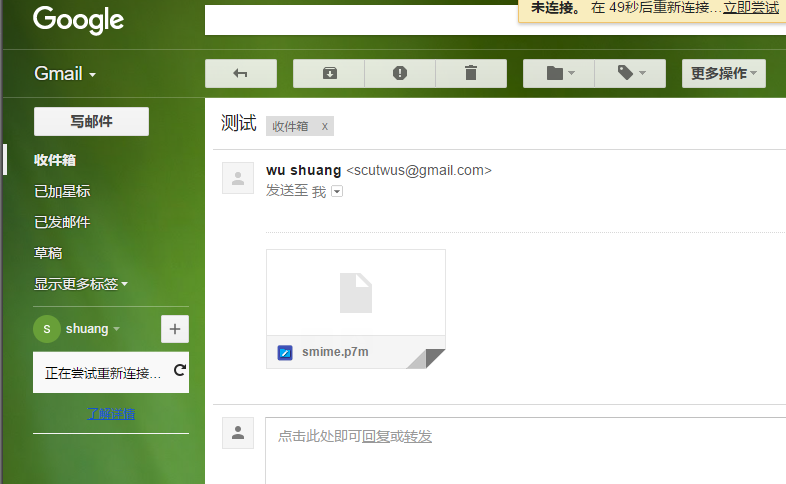
由于发送加密邮件是用发送者的公钥加密，需要发送者的证书，所以选择给自己发邮件来认证。直接发加密邮件会有错误：

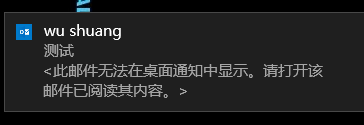


先发送一封带签名的邮件给自己，不加密内容。然后添加为常用联系人。这样outlook就能识别出证书。此时在发加密邮件则成功。

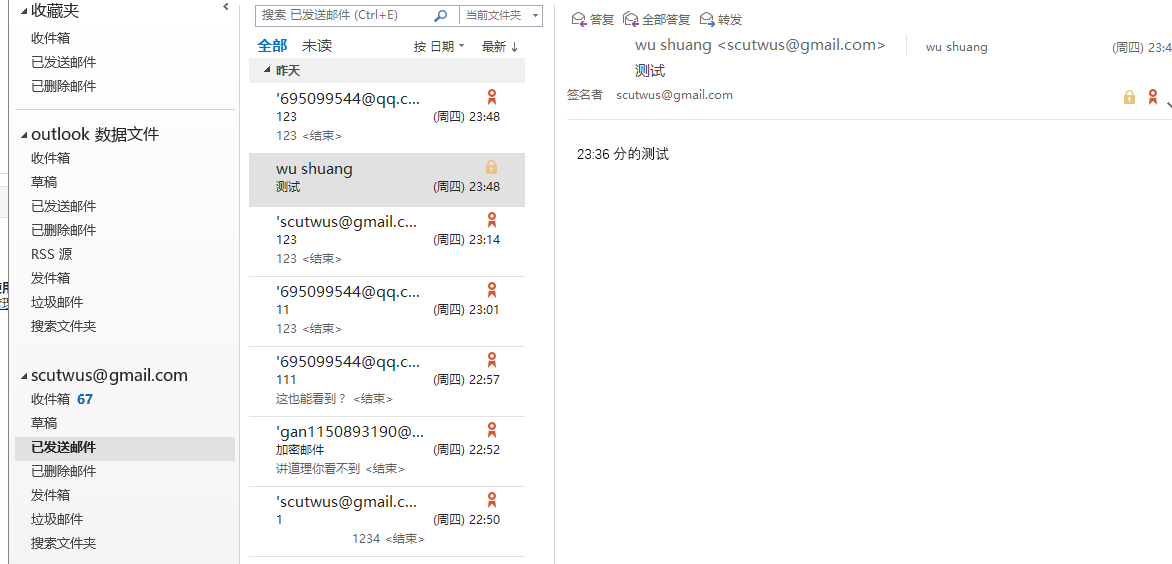


网页端显示：





客户端显示：



实验成功。

**实验结论与思考题**

对实验做出总结，并回答思考题等

## 实验总结

公钥证书的管理是个复杂的系统。一个典型、完整、有效的CA系统应具有以下部分：公钥密码证书管理；黑名单的发布和管理；密钥的备份和恢复；自动更新密钥；历史密钥管理；支持交叉认证，等等。本次实验只完成了一部分，密钥管理部分还可以完善。由于CA证书获得麻烦，交换繁琐，因此这种电子邮件加密模式一直很难普及。

## 思考题：

1. 加密邮件与签名邮件有什么区别？

加密邮件用收件者公钥加密邮件，对方收到后用自己的私钥解密。保证内容的机密性

签名邮件是把要发送的内容取hash值，用发送者的私钥把hash值加密以防被中间人修改，同时把数字证书随邮件一起发送，收件人收到后用证书里的公钥对加密后的hash值（即数字签名）解密，与接收者重新计算的hash值对比，验证邮件没有被修改。但内容是明文。

1. 随着中华人民共和国电子签名法的颁布实施，你认为签名电子邮件具有法律效力吗？

有，数字签名具有不可否认性，故可靠的电子签名与手写签名或者盖章具有同等的法律效力。

3、为什么发送加密邮件需要对方的数字证书？其加密原理是什么？真的是使用接收方的公钥直接对邮件的内容进行加密吗？

如果加密邮件用的是发送者的私钥，那所有知道公钥的人都能知道邮件内容，而公钥是公开的，所以没有意义，需要用接收者的公钥加密，

加密邮件用收件者公钥加密邮件内容，对方收到后用自己的私钥解密。

不是直接对内容加密，因为公钥加密时间代价高，采用的应该是对称加密，把加密的密钥用收件者的公钥加密，减少加密成本。（如果有误，希望老师告之）

4、能用他人的证书发送签名邮件吗？为什么？

不行，因为其他人的证书时公开的，任意人都可以伪造一封邮件并用其证书里的公钥进行签名，没有安全性。