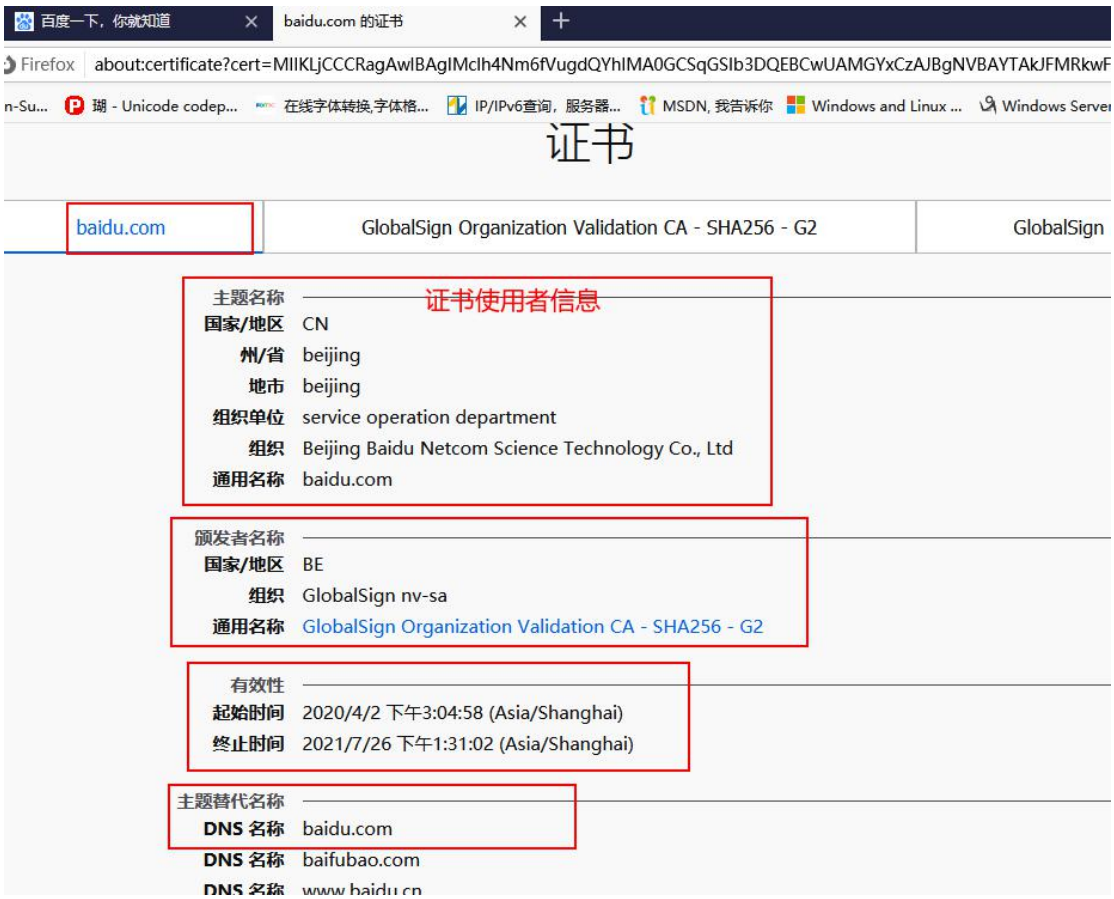
# XCA 密钥及证书管理工具的使用

## 一、ssl 证书的查看

ssl 证书的主要用途是身份认证和数据加密，在 https 里常用于网站服务端的身份认证
在浏览器地址栏左侧可看到当前网站的 ssl 证书相关信息，显示“已安全连接到此网站”则说明此网站的 ssl 证书通过了验证，浏览器认为它是可信的。

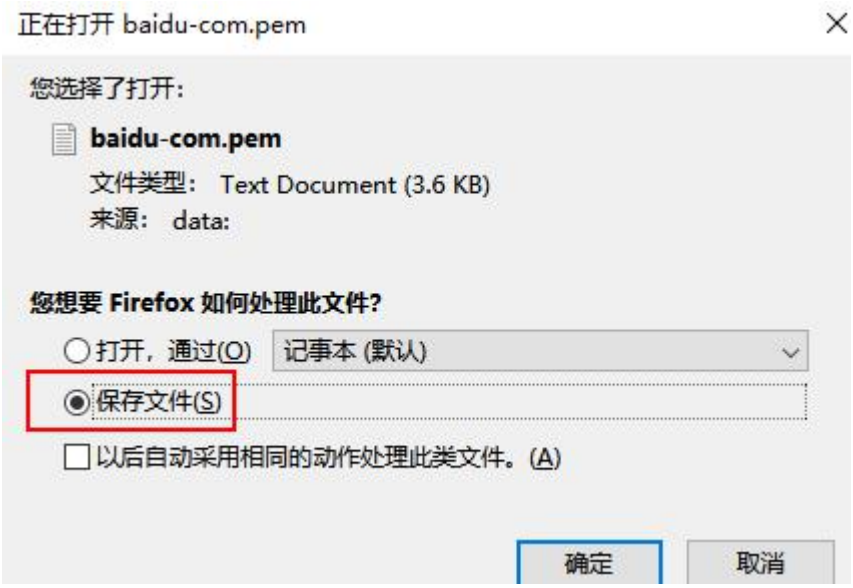


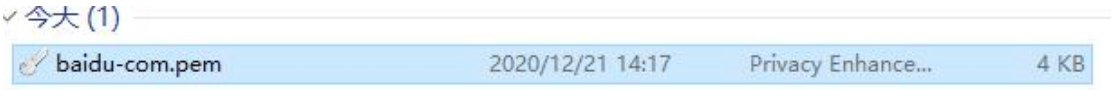
可以在浏览器里查看网站的证书：


百度一下，你就知道
baidu.com 的证书
Firefox
about:certificate?cert=MIIKLjCCCRagAwIBAgIMcIh4Nm6fVugdQYhIMA0GCSqGSIb3DQEBCwUAMGYxCzAJBgNVBAYTAkJFMRkwF
证书
baidu.com
GlobalSign Organization Validation CA - SHA256 - G2
GlobalSign
证书使用者信息
主题名称
国家/地区 CN
州/省 beijing
地市 beijing
组织单位 service operation department
组织 Beijing Baidu Netcom Science Technology Co., Ltd
通用名称 baidu.com
颁发者名称
国家/地区 BE
组织 GlobalSign nv-sa
通用名称 GlobalSign Organization Validation CA - SHA256 - G2
有效性
起始时间 2020/4/2 下午3:04:58 (Asia/Shanghai)
终止时间 2021/7/26 下午1:31:02 (Asia/Shanghai)
主题替代名称
DNS 名称 baidu.com
DNS 名称 baifubao.com


百度一下，你就知道
baidu.com 的证书
Firefox
about:certificate?cert=MIIKLjCCCRagAwIBAgIMcIh4Nm6fVugdQYhIMA0
指数 65537
模块 C1:A9:B0:AE:47:1A:D2:57:EB:1D:15:1F:6E:5C
杂项
序列号 72:58:78:36:6E:9F:56:E8:1D:41:88:48
签名算法 SHA-256 with RSA Encryption
版本 3
下载 PEM（证书） PEM（证书链）

也可以下载证书到本地，



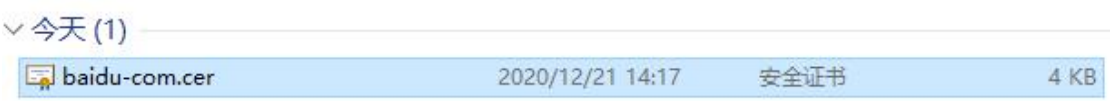

这个 ssl 证书文件本身不大，大概 2 到 6KB 左右，证书内容本身是二进制的，有时为了方便复制粘贴，也可转为 base64 编码。下图为 baidu.com 网站 ssl 证书的内容（base64 编码格式）

baidu-com.pem

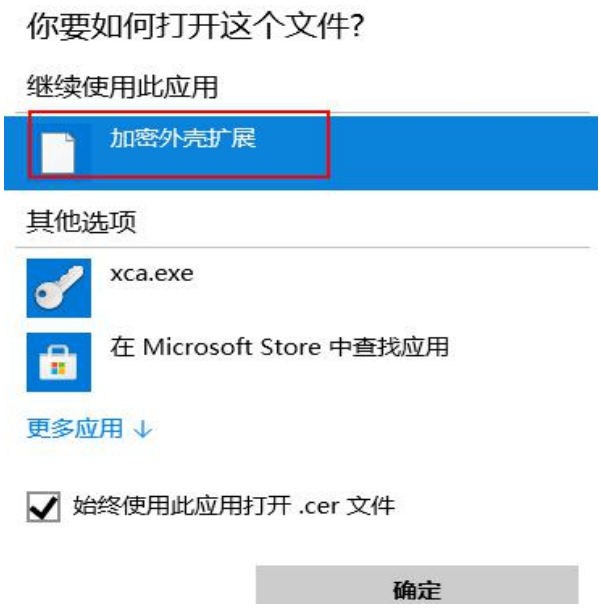
```
-----BEGIN CERTIFICATE-----
MIIKLjCCCRagAwIBAgIMclh4Nm6fVugdQYhIMA0GCSqGSIb3DQEBCwUAMGYxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMTwwOgYDVQQDEzNH
bG9iYWxTaWduIE9yZ2FuaXphdGlvbiBWYWxpZGF0aW9uIENBIC0gU0hBMjU2IC0g
RzIwHhcNMjAwNDAyMDcwNDU4WhcNMjEwNzI2MDUzMTAyWjCBpzELMAkGA1UEBhMC
Q04xEDAOBgNVBAgTB2JlaWppbmcxEDAOBgNVBAcTB2JlaWppbmcxJTAjBgNVBAsT
HHNlcnZpY2Ugb3BlcmF0aW9uIGRlcGFydG1lbnQxOTA3BgNVBAoTMEJlaWppbmcg
QmFpZHUgTmV0Y29tIFNjaWVuY2UgVGVjaG5vbG9neSBDby4sIEx0ZDESMBAGA1UE
AxMJYmFpZHUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwamw
rkca0lfrHRUfblyy5PgLINvqAN8p/6RriSZLnyMv7FewirhGQCp+vNxaRZdPrUEO
vCCGSwxdVSFH4jE8V6fsmUfrRw1y18gWVHXv00URD0vOYHpGXCh0ro4bvthwZnuo
k0ko0qN2lFXefCfyD/eYDK2G2sau/Z/w2YEympfjIe4EkpbkeBHlxBAOEDF6Speg
68ebxNqJN6nDN9dWsX9Sx9kmCtavOBaxbftzebFoeQOQ64h7jEiRmFGlB5SGpXhG
eY9Ym+k1Wafxe1cxCpDPJM4NJOeSsmrp5pY3Crh8hy900lzoSwpfZhinQYbPJqYI
jqVJF5JTs5Glz1OwMQIDAQABo4IGmDCCBpQwDgYDVR0PAQH/BAQDAgWgMIGgBggr
BgEFBQcBAQSBkzCBkDBNBggrBgEFBQcwAoZBaHR0cDovL3NlY3VyZS5nbG9iYWxz
aWduLmNvbS9jYWNlcnQvZ3Nvcmdhbml6YXRpb252YWxzaGEyZzJyMS5jcnQwPwYI
KwYBBQUHMAGGM2h0dHA6Ly9vY3NwMi5nbG9iYWxzaWduLmNvbS9nc29yZ2FuaXph
qwzch98lINQYzLAV52+C8GXZPXFZNfhfpM4tQ6xbMA0GCSqGSIb3DQEBCwUAA4IB
AQC83ALQ2d6MxeLZ/k3vutEiizRCWYSSMYLVCrxANdsGshNuyM8B8V/A57c0Nzqo
CPKfMtX5IICfv9P/bUecdtHL8cfx24MzN+U/GKcA4r3a/k8pRVeHeF9ThQ2zo1xj
k/7gJl75koztdqNfOeYiBTbFMnPQzVGqyMMfqKxbJrfZlGAIgYHT9bd6T985IVgz
tRVjAoy4IurZenTsWkG7PafJ4kAh6jQaSu1zYEbHljuZ5PXlkhPO9DwW1WIPug6Z
rlylLTTYmlW3WETOATi70HYsZN6NACuZ4t1hEO3AsF7lqjdA2HwTN10FX2HuaUvf
5OzP+PKupV9VKw8x8mQKU6vr
-----END CERTIFICATE-----
```

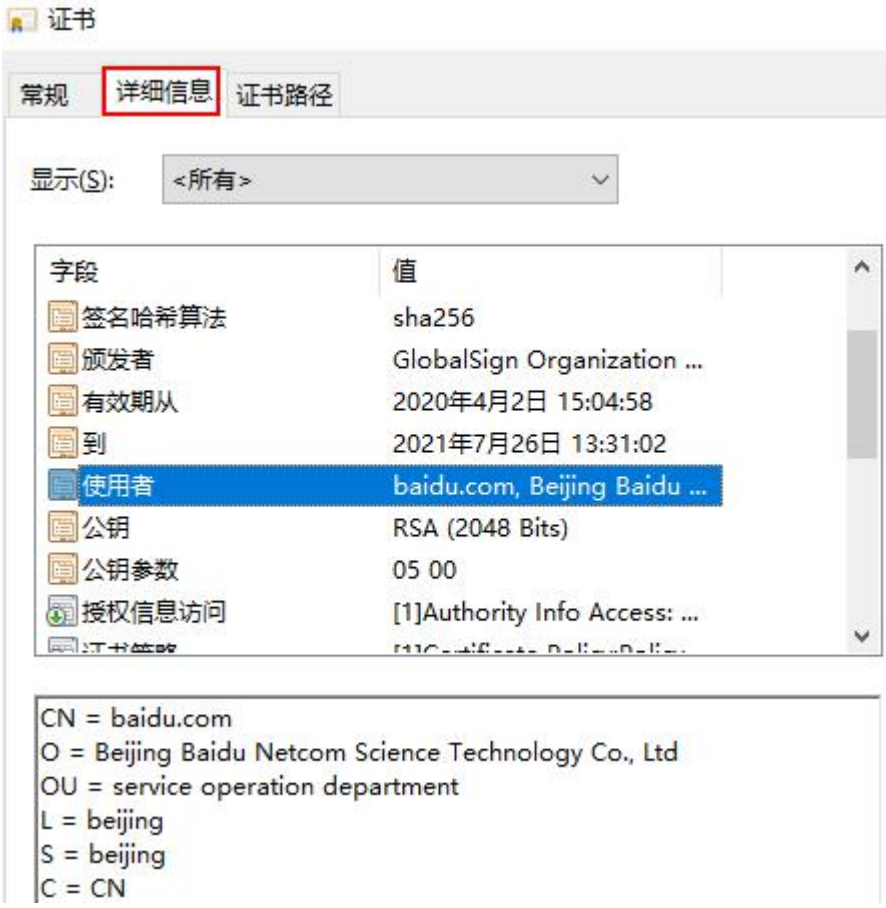
内容以“-----BEGIN CERTIFICATE-----”开始，以“-----END CERTIFICATE-----”结束，中间是正式内容的 base64 编码。

从浏览器上下载得到的证书一般为 x.509 标准的证书，默认以.pem 为后缀，可改为.cer，



然后在 windows 系统上可直接双击此证书文件 查看证书的详细信息，如果已经安装了 xca 工具，则可能无法直接双击查看了，这时使用“加密外壳扩展”打开





证书
常规
详细信息
证书路径
显示(S):
<所有>
字段
值
签名哈希算法
sha256
颁发者
GlobalSign Organization ...
有效期从
2020年4月2日 15:04:58
到
2021年7月26日 13:31:02
使用者
baidu.com, Beijing Baidu ...
公钥
RSA (2048 Bits)
公钥参数
05 00
授权信息访问
[1]Authority Info Access: ...
CN = baidu.com
O = Beijing Baidu Netcom Science Technology Co., Ltd
OU = service operation department
L = beijing
S = beijing
C = CN


证书
常规
详细信息
证书路径
证书路径(P)
GlobalSign Root CA
GlobalSign Organization Validation CA - SHA256 - G2
baidu.com

# 二、ssl 证书内容及验证原理

**① ssl 证书里主要包含的内容有：**

版本号（version）：v3
证书序列号（serial number）：xxxxxx
签发者（issuer）：某 ca 机构
签名算法（signature algorithm）：sha256Rsa
有效期始（valid from）：生效时间
有效期至（valid to）：截止时间
主题（subject）：证书拥有者/使用者的相关信息
公钥（public key）：rsa 公钥
……

在“主题/主体”里一共有 7 个字段，用以表明使用者的身份信息




countryName（**C**）：国家或地区，只能是 2 个大写字母
state or province（**S**）：省/州
locality（**L**）：市
organizationalUnit（**OU**）：组织/公司的 某单位/部门，如 it-dept（IT 部）
organizatoin（**O**）：组织名/公司名称
commonName（**CN**）：通用名称，一般为网站的域名或组织名，必需字段
email address（**E**）：邮件地址，可选字段
（括号里的为字段的缩写）

在签发者信息里也有上面的 7 个字段，用以表明签发者的身份信息。

当浏览器收到服务器发来的证书后，会对此证书进行验证，

**②ssl 证书验证流程**是：

1.查看网站证书的 通用名称或扩展字段 SAN 里的域名是否和网站的域名相同，相同则说明此证书是给这个网站用的

2.查看证书里的签发者名称，再去找签发者的证书，签发者的证书可在系统预安装的证书里查找，也可由浏览器去它自己官网找，找到后，再用签发者的 rsa 公钥去解开网站的 ssl 证书里的签名信息，解开后再和网站的证书一比对，对得上就说明 此网站的 ssl 证书确实由此签发者签名的。

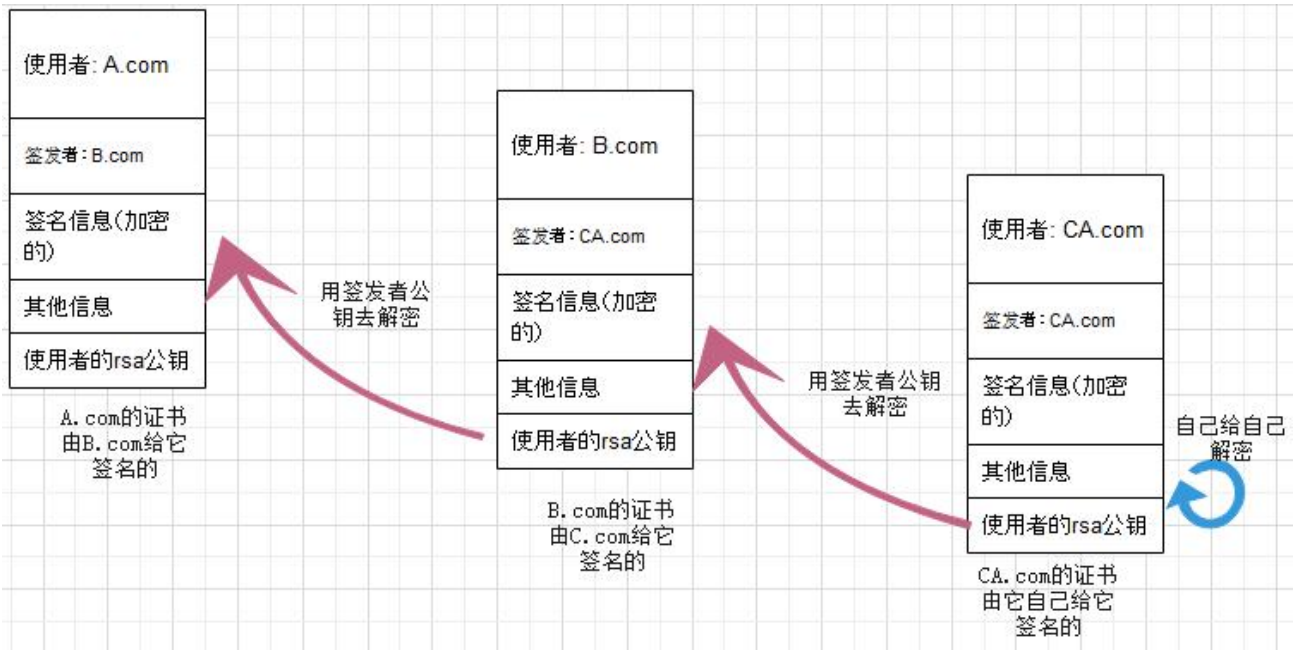
3.对签发者的证书也如上步骤进行验证，直到最终的签发者为可信的 CA，即最终的签发者证书为可信的根证书，一般预安装在操作系统里。

根证书的签名信息是由自己进行签名生成的（是自签名证书）,即签发者和使用者为同一组织。

**签名**：B 给 A 签名就是指 B 使用自己的 rsa 私钥去给 A 的相关身份信息的 hash 值进行加密，再把加密后的信息放入 A 的证书里

**验证**：要验证 A 的证书是否为 B 所签名，需要用到 B 的证书里的公钥，用 B 的公钥去给 A 的证书里的签名信息进行解密，解密后再和 A 的相关身份信息的 hash 值比对，一致则说明 A 证书确实是由 B 签名的，即 A 证书可信，要验证 B 证书的可信度，也是一样的过程（去找 B 的签发者）。

验证时，最顶级的证书一定是自签名的，且为受信任的根证书，验证时，从底层证书一直到最高层都要验证通过才能说明最底层证书可信。




这一串证书构成了一条信任链，称为**证书链**

可把要用到的证书内容都放在一起，直接用文本处理工具把它们的 base64 编码内容都复制在一个文件里，这个新的文件就是证书链文件，后缀也可为.pem 或.crt


st.com.csr.pem
baidu-com-chain.pem
-----BEGIN CERTIFICATE-----
证书1
MIIKLjCCCRagAwIBAgIMclh4Nm6fVugdQYhIMA0GCSqGSIb3DQEBCwUAMGYxC
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
中间证书
MIIEYjCCA0qgAwIBAgILBAAAAAABMYnGRMkwDQYJKoZIhvcNAQELBQAwTDEg
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
顶级证书
MIIDXzCCAkegAwIBAgILBAAAAAABIVhTCKIwDQYJKoZIhvcNAQELBQAwTDEgM
-----END CERTIFICATE-----

## 三、ssl 证书安全级别

ssl 证书根据受信任的程度可分为 3 种级别：域名型、机构验证型、严格身份验证型
区别如下表：

| ssl 证书级别类型 | **DV 域名型**<br>Domain Validation | **OV 机构验证型**<br>Organization Valid | **EV 严格身份验证型**<br>Extended Validation |
|---|---|---|---|
| 商业上的称呼 | 超快 SSL 证书 | 超真 SSL 证书 | 超安 SSL 证书 |
| 证书用途 | 个人站点，简单的 Https 加密需要 | 中小企业，电子商务站点 | 大型金融平台，政府机构站点 |
| 审核内容 | 域名所有权验证 | 域名所有权验证及企业身份信息 | 最高等级的企业身份信息验证和域名所有权验证 |
| 证书颁发需要时长 | 10 分钟至 1 小时 | 2 至 5 个工作日 | 2 至 5 个工作日 |
| 首次申请年限 | 1 年 | 1 至 2 年 | 1 至 2 年 |
| 价格参考（2020 年 | 1k 或免费 | 5k | 12k |
| 证书内容差异 | 主体信息里仅含有 CN 通用名称（一般为域名） | 主体信息里含有更多的信息，可以 7 个字段都有（域名及公司名称等） | 主体信息和 OV 证书一样多，更多的体现在证书的扩展字段里 |

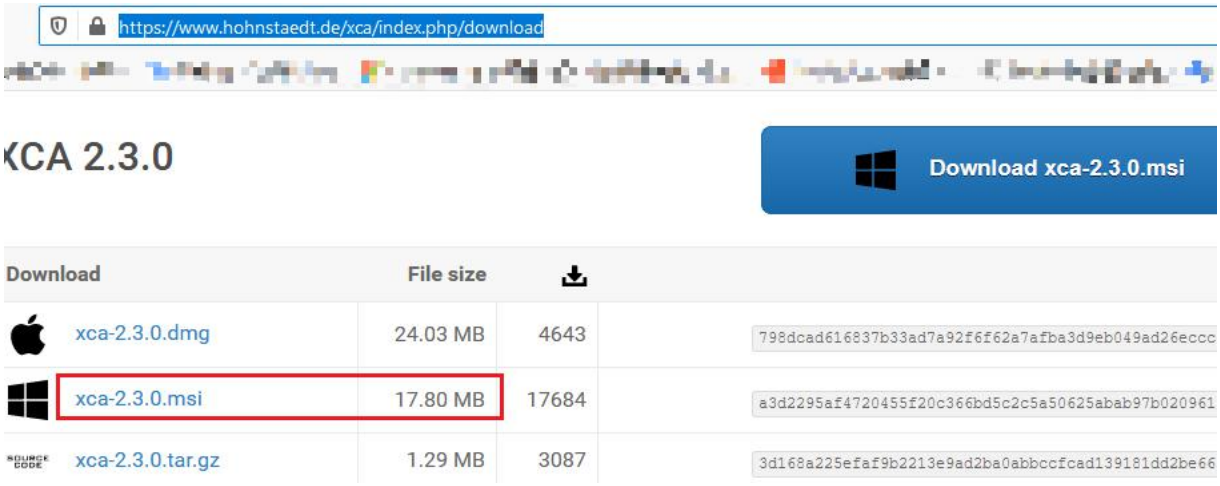
这三种证书有什么本质的区别吗？
没有

# 四、向 ca 机构申请自己的证书

**①安装 XCA 工具**

首先 ssl 证书是基于 rsa 加密算法的，得先生成 rsa 密钥，本例使用 XCA 密钥及证书管理工具

下载地址：https://www.hohnstaedt.de/xca/index.php/download




选择一个较新版本，如果是 windows 系统就下载.msi 后缀的安装包，下载后双击安装


安装完成后，双击运行


**②新建数据库**用以保存密钥及证书等文件

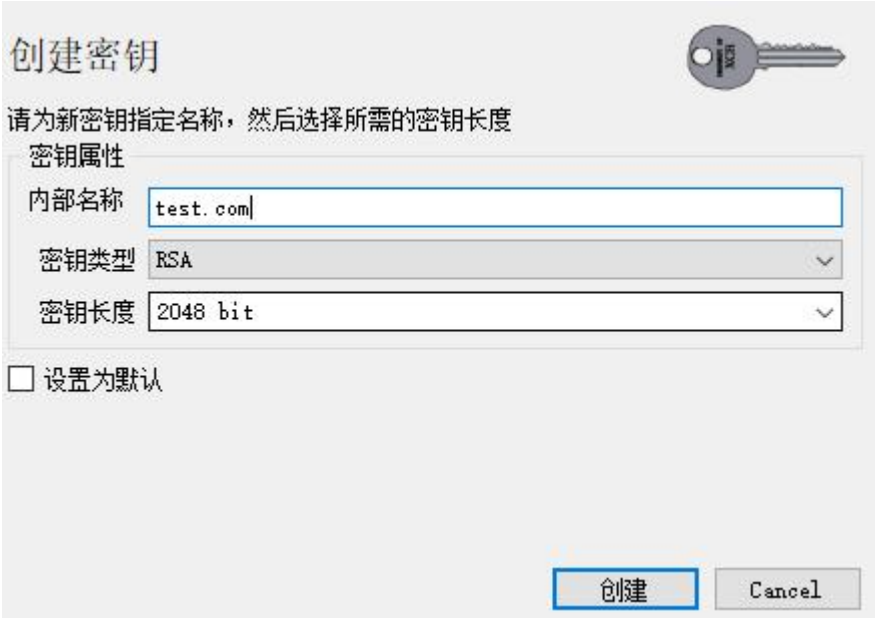
在主界面上，点击左上角菜单栏的“文件”→“新建数据库”

选择保存到某个目录下，名为 test.xdb

确定后，要求输入数据库的密码


**③在此数据库里创建 rsa 密钥**


点击主界面左上角的“私钥”，再点击右边的“创建密钥”

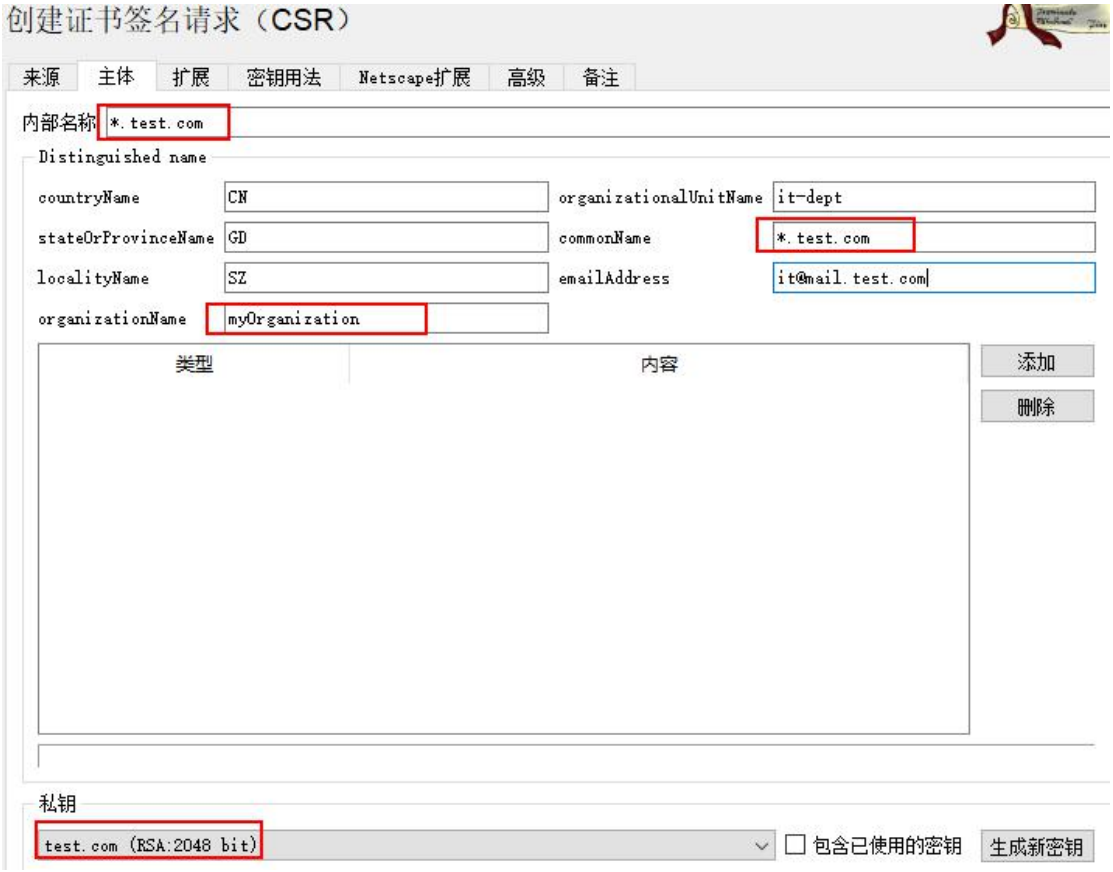



内部名称可随便写，比如就以自己的网站域名为名，其他参数自己设定

点击“创建”后就 ok 了

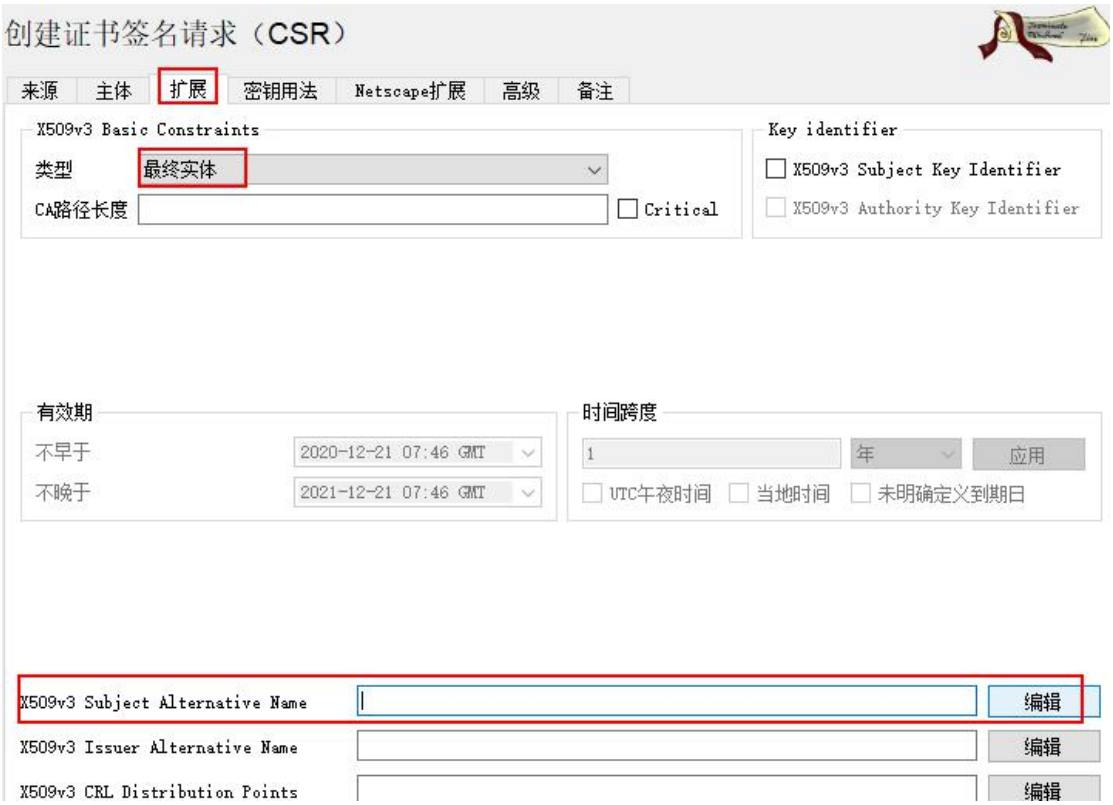

然后在主界面的“私钥”框里，就有了刚刚创建的密钥对，rsa 密钥是一对一对的，虽然在这个 xca 软件里显示的是私钥，但私钥里也是包含有公钥的。（私钥文件里一定包含有公钥）


**④创建证书签名请求**，点击“证书签名请求”→“创建请求”




在主体里，内部名称也可随便写，一般写域名，本次我们要申请一个泛域名证书，所以就写 *.test.com，其他的如国家/省/市就写 大写字母简称，O 组织名称为 公司名称，OU 组织单

位一般写 IT-dept，cN 通用名称一般写域名或泛域名*.test.com，邮件可写/可不写
再确认此签名请求文件使用的 rsa 密钥为要使用的那个密钥。（密钥名称和域名无必然联系）

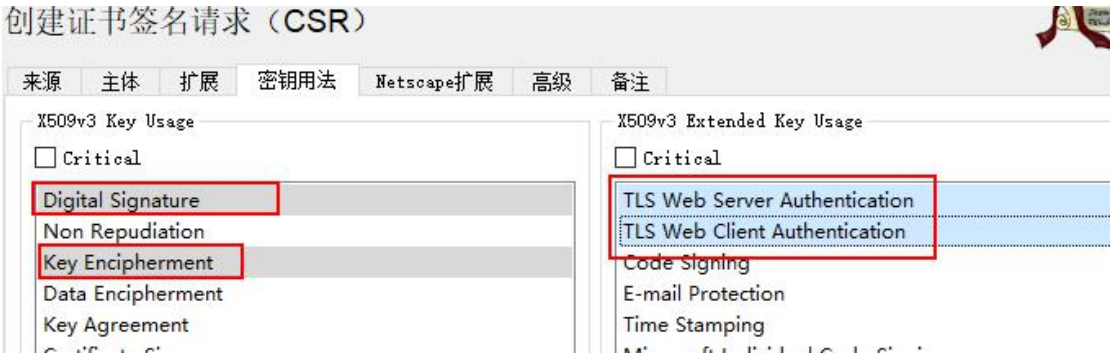



然后在“扩展”框里，“类型”选择为“最终实体”，现代的证书一般都需要有 x.509v3 的扩展字段 SAN（Subject Alternative Name）使用者可选名称：
点击“x509v3Subject Alternative Name”右边的“编辑”


添加 2 条记录，第 0 条一定要和 cN 通用名称一致，即必须为前面的 *.test.com
第 1 条则写 test.com 二级域名本身，还可有其他的子域名，一般不加了，点击“应用”

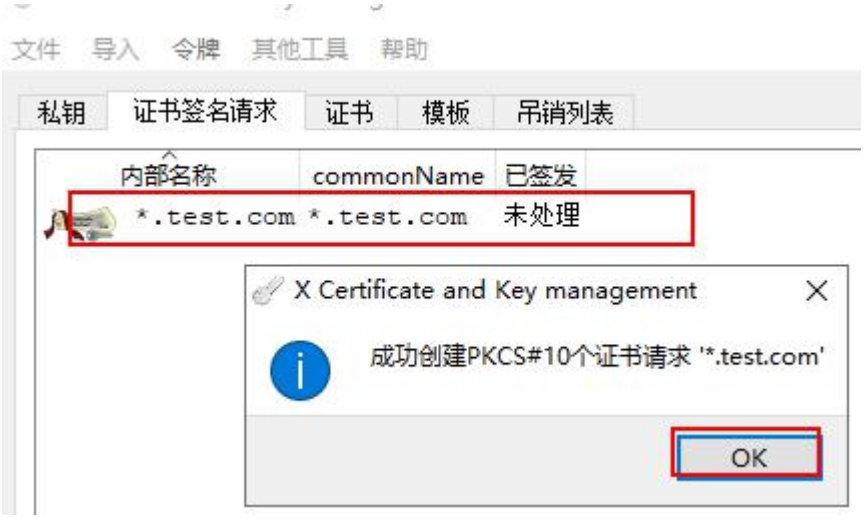

最后添加证书的用途信息：


点击“密钥用法”，左边基础用法点击 Digital Signature 和 Key Encipherment 这 2 个就行了



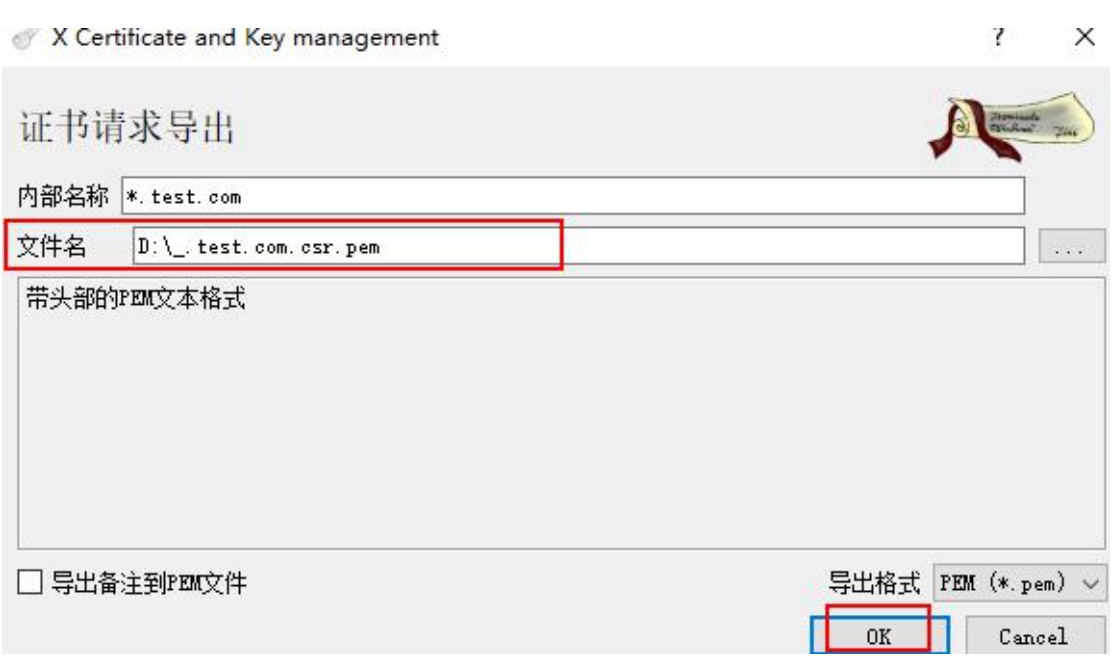

右边扩展用法点击 TLS web SERVER Authentication 和 CLIENT Authentication 就可以了

最后确认所有信息无误后，点击最右下方的 OK 就行了，




提示创建成功，在“证书签名请求”框里多了一个*.test.com 的证书签名请求

**⑤接下来要导出此请求文件**


导出到 D 盘，文件名可随便取，一般为_.test.com.csr.pem 之类的名字，也可直接以.csr 为后缀

_.test.com.csr.pem

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDNzCCAh8CAQAwgYgxCzAJBgNVBAYTAkNOMQswCQYDVQQIEwJHRDELMAkGA1UE
BxMCU1oxFzAVBgNVBAoTDm15T3JnYW5pemF0aW9uMRAwDgYDVQQLEwdpdC1kZXB0
MRMwEQYDVQQDDAoqLnRlc3QuY29tMR8wHQYJKoZIhvcNAQkBFhBpdEBtYWlsLnRl
c3QuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvmdlJtl7JSev
Q53CZUNB6ixC4iAmbezogiR2Af7sg0vo770/U7vOROdQjXqGJE8bP543TNIaO4YI
cEBYSk3dagooNhEj+3pU3ljYy72QAa25N9QK5faMreTH9UTFp0a3MZ2AhvU2Udbv
MHHB/JIPIbd5hOUPYPizKTcyyPyS25mbJwqcKjSzAsmfQrbydKYuHNlYVOcl4Y8O
Lnt3epq8EoZIt8dqmGiH+nonXPgacgRRLj5CeYVIqXkiHN6od+i6tZZN6Qi2MoV1
98E1vKF8/9VgPE8c2byOl8vQjs2rUGW4M0jEat+Ll6RFhrhU1E1UJ+mB+mgfJd1S
0J9cOrIiRwIDAQABoGkwZwYJKoZIhvcNAQkOMVowWDAJBgNVHRMEAjAAMAsGA1Ud
DwQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0RBBgw
FoIKKi50ZXN0LmNvbYIIdGVzdC5jb20wDQYJKoZIhvcNAQELBQADggEBAES0Cg96
RmOMNRWrSTZ7NYUuVcf4tpBSlP9FaUT72xEea1G4LUnqObES4M4FI0+H+c6iuuiS
BQU8i07RrDX6hdSV/mEBRAKZT9hMwR/gL6ausGZQ/TQA9bH1B1saCN9+PMP6KW4/
dlrGZ64cmPGinOBK2PINkD8clCeiYzX2ZIFAcp5VT5YSqvQQfjvRQNXe7ZBHX9r0
Rw2ntszHle02Y6nQQ/LY+LRCWDHW3jtTlt/3Lfj8GjZZr6a4xE8uHR1fiQLqflYG
4juXDpyD9IvfIb8mwX2jUi8aHKmdHWB69+GddtRw++DZzIgAFKv/rumtEyxKY7Sd
DZvnKXJ7BAD8Boo=
-----END CERTIFICATE REQUEST-----
```

证书签名请求文件内容也是 base64 编码的

⑥之后可把此文件交给**证书签发商**的工作人员或在他们的 **ssl 证书申请网站**上复制进去就行，等待验证通过后，就会收到他们发来的已签名了的 ssl 证书。

我们收到的 ssl 证书一般有多种格式的，常见的是 x.509 编码的，后缀为.cer 或.crt 或.pem 之类的。

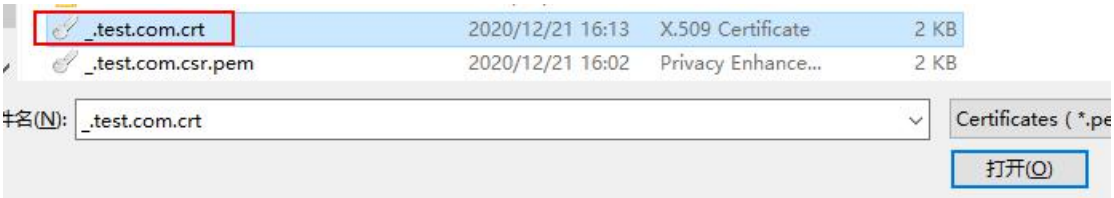
# 五、转换 ssl 证书格式

我们向 ca 机构（Certificate Authority）提交证书签名请求文件后，他们会验证我们的目标域名及公司身份等信息，验证通过后会得到有签名的 ssl 证书，不过此证书一般为 x.509 的编码格式，后缀为.cer 或.crt 或.pem，而我们的 web 服务器可能要其他的格式的证书

可用 XCA 工具进行转换，千万不要在网上在线转换，因为转换时可能要用到 rsa 的私钥，如果私钥给了第三方网站，则此 ssl 证书可以算是作废了。

**①导入收到的已签名的 ssl 证书**

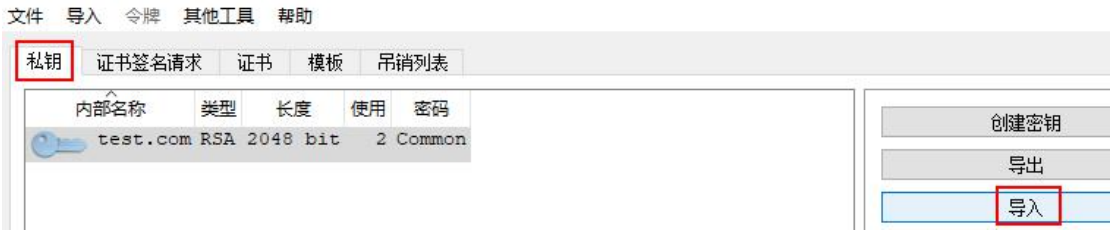

点击“证书”→“导入”




选择目标证书，点击“打开”，导入成功后，在“证书”框里有刚导入的证书信息

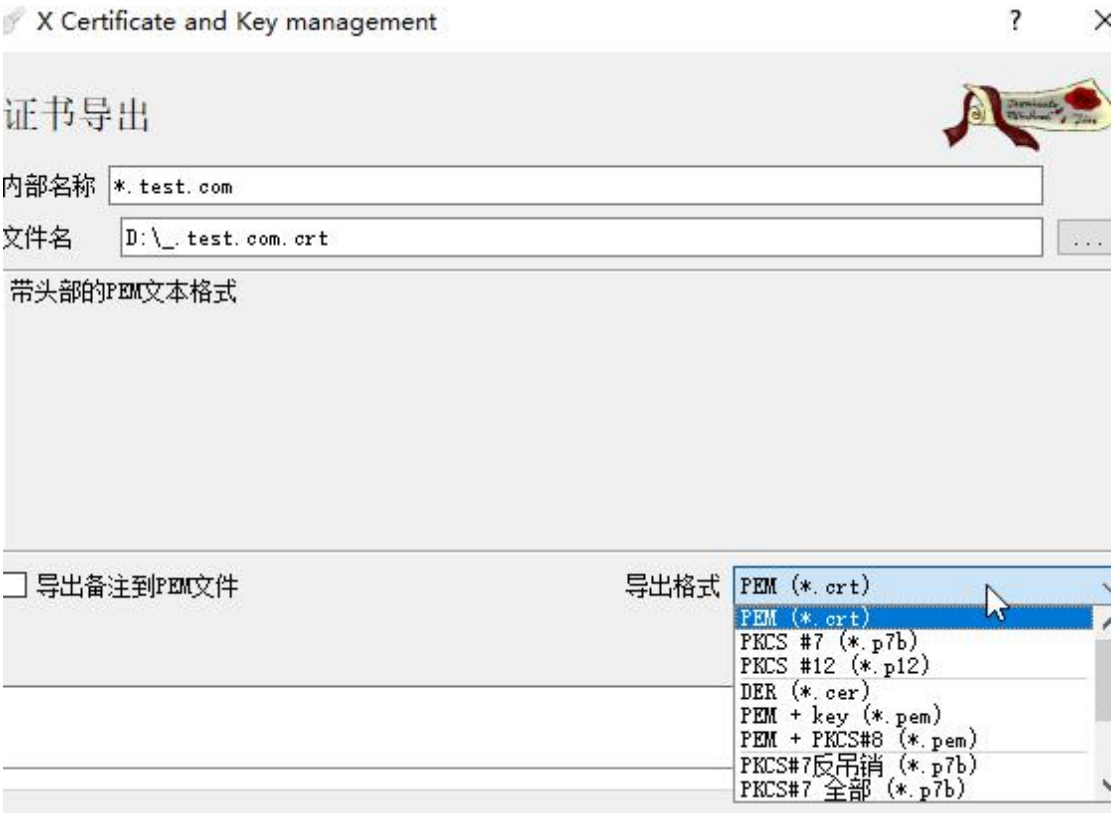

默认是导入 x.509 的格式证书，要导入其他格式的证书，请点击下面的“导入 pcks#xx”

导入后就可直接再导出为其他格式的证书了，因为它的 rsa 私钥本来就在我们的这个 xca 数据库里，如果是从其他的地方发来的证书，其 rsa 密钥不在本 xca 数据库里，则要导入此证书对应的私钥：




**②导出证书为其他格式**


选中目标证书，点击“导出”

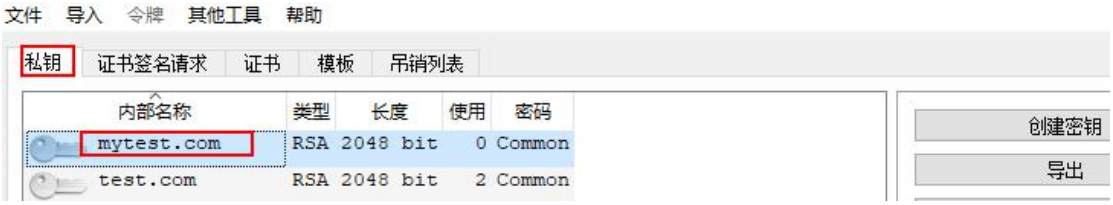



选择目标类型就行了，如：导出为.p7b 的格式，或者导出为.p12 的格式
（.p12 的格式就是.pfx，导出后把后缀改为.pfx 就能直接给 IIS web 服务器使用）

# 六、创建自签名证书

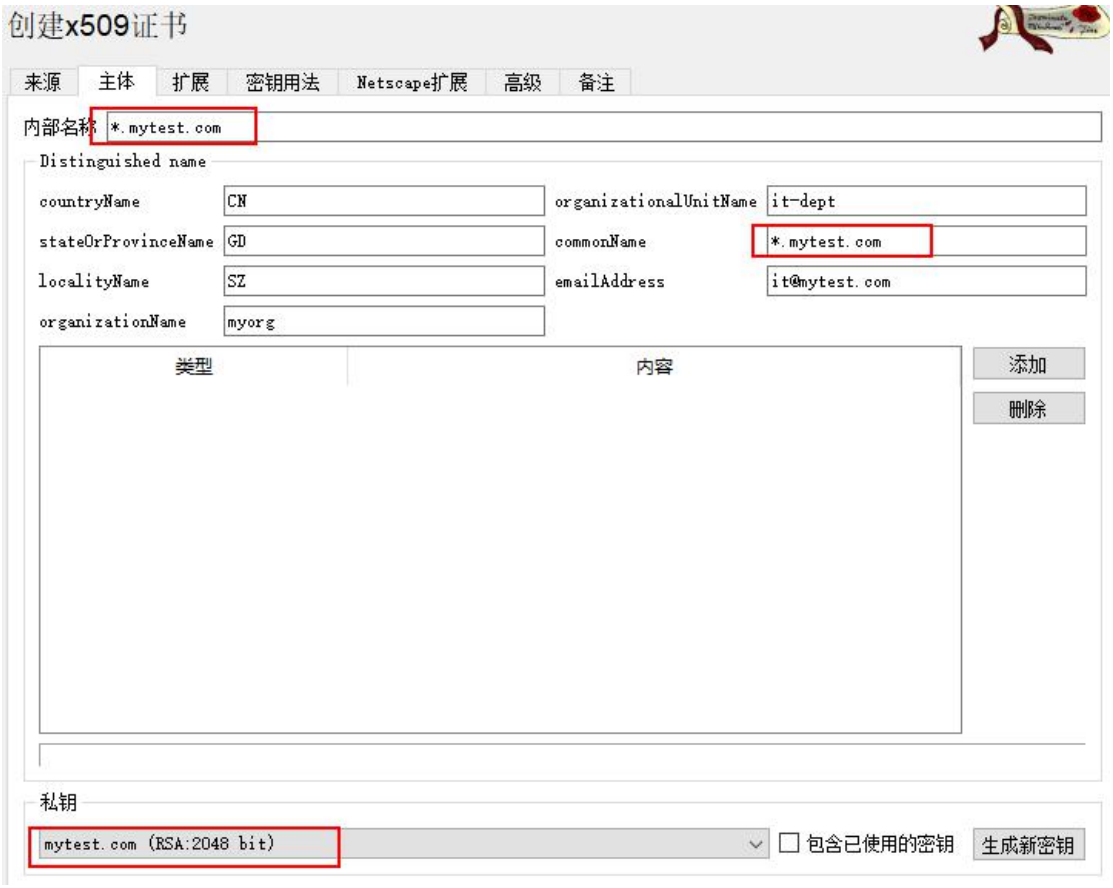
如果我们的网站是给广大客户用的，则一定要用 CA 权威机构签名了的 ssl 证书，别人才信得过我们，而如果是自己做实验或一般内部使用的环境下，可用自签名 ssl 证书，就是不给 CA 机构去签名了，自己签名就行，自己信任自己即可。

**①同样也是要先创建 rsa 密钥对**

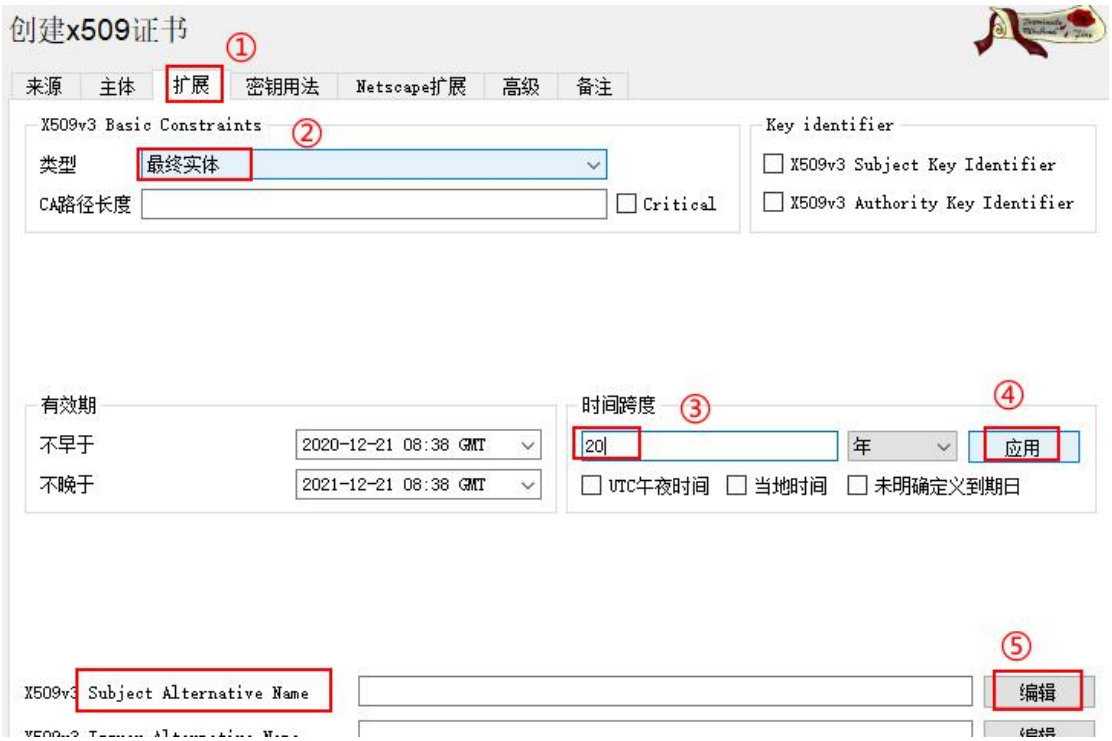



**②可直接创建证书**，不用先创建请求文件了


“来源”下面的“签名”选择“创建自签名证书”




其他的信息和之前创建 CSR 证书签名请求时一样，随便写，合理即可




在“扩展”里，选择“最终实体”类型，证书有效时间随便写，1 到几十年都行，点击“应用”后这个时间才生效，最后添加 SAN 主体可选名称，点击右下的“编辑”


添加以上信息，第 0 个一定是和 cN 通用名称一致，记录类型都是 DNS

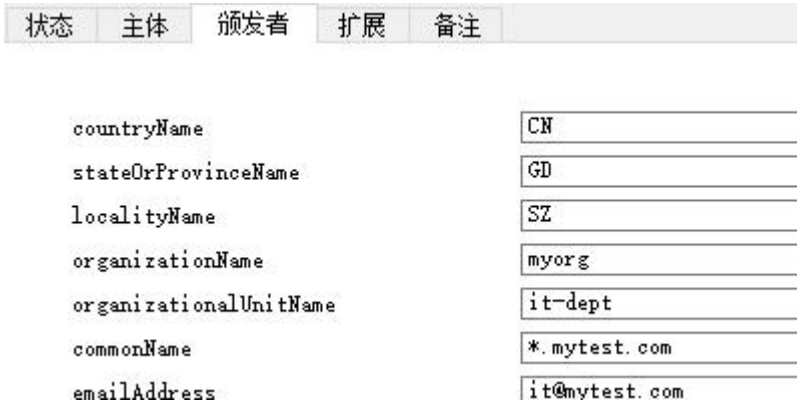

“密钥用法”一般选择以上 4 个，确认无误后，点击右下方的 OK



创建成功

双击此证书可查看详细信息






主体和颁发者都是自己，这就是自签名证书。

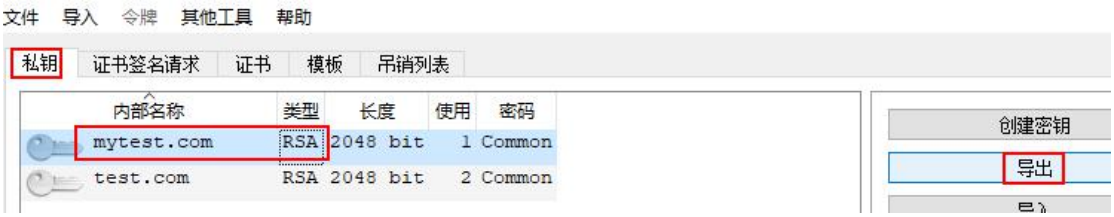
之后导出证书和对应的密钥 就能拿去使用了。

# 七、导出 RSA 密钥

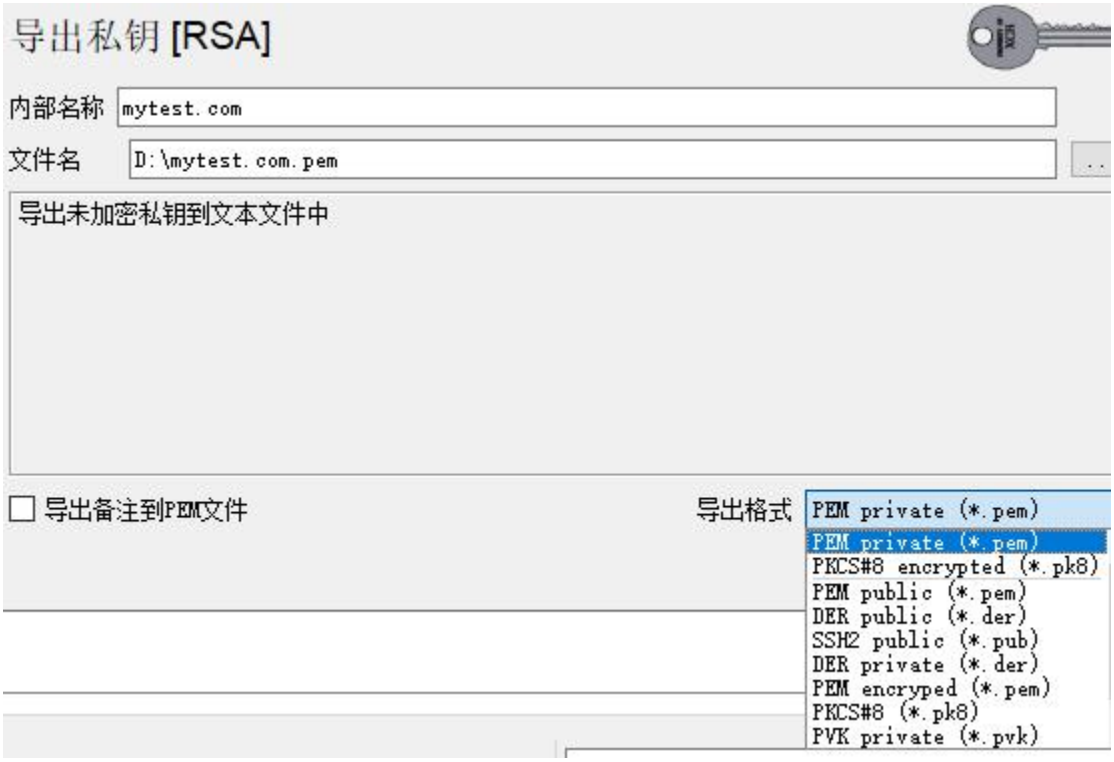

当我们再次打开 XCA 工具时，之前创建的东西好像都没了，
不要慌，只是默认没有打开上次的数据库而已，


点击菜单栏的“文件”→“打开数据库”


选择之前的 test.xdb 数据库文件，输入密码即可

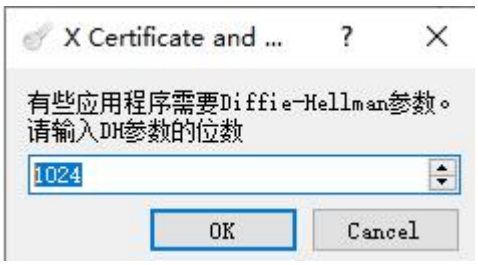
选中目标 RSA 密钥，点击“导出”




可导出的格式非常多，根据实际需求来选择格式类型。一般就选择 pem private 以.pem 结尾的未加密的私钥，（私钥文件一定是包含有公钥的，如果导出的是公钥，则它就只有公钥）我们也可把导出的文件名改为*.key.pem，这样便于我们的理解。
导出 rsa 密钥后可以和证书一起用，也用单独用在其他地方，比如导出为 ssh2 public 的密钥，则可用于 ssh 的连接验证，即使用密钥登录 Linux 服务器。

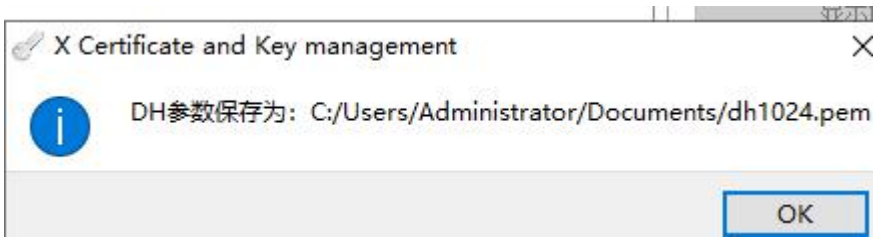
**②生成 DH 参数**
生成 DH 密钥交换算法的“材料”，有的服务可能要这个东西（比如 openvpn）


点击“其他工具”→“生成 DH 参数”



材料长度可根据自己的需求去写，如 1024，2048 之类的


点击 OK 后，保存到目标目录下即可




出现上图提示说明生成成功了

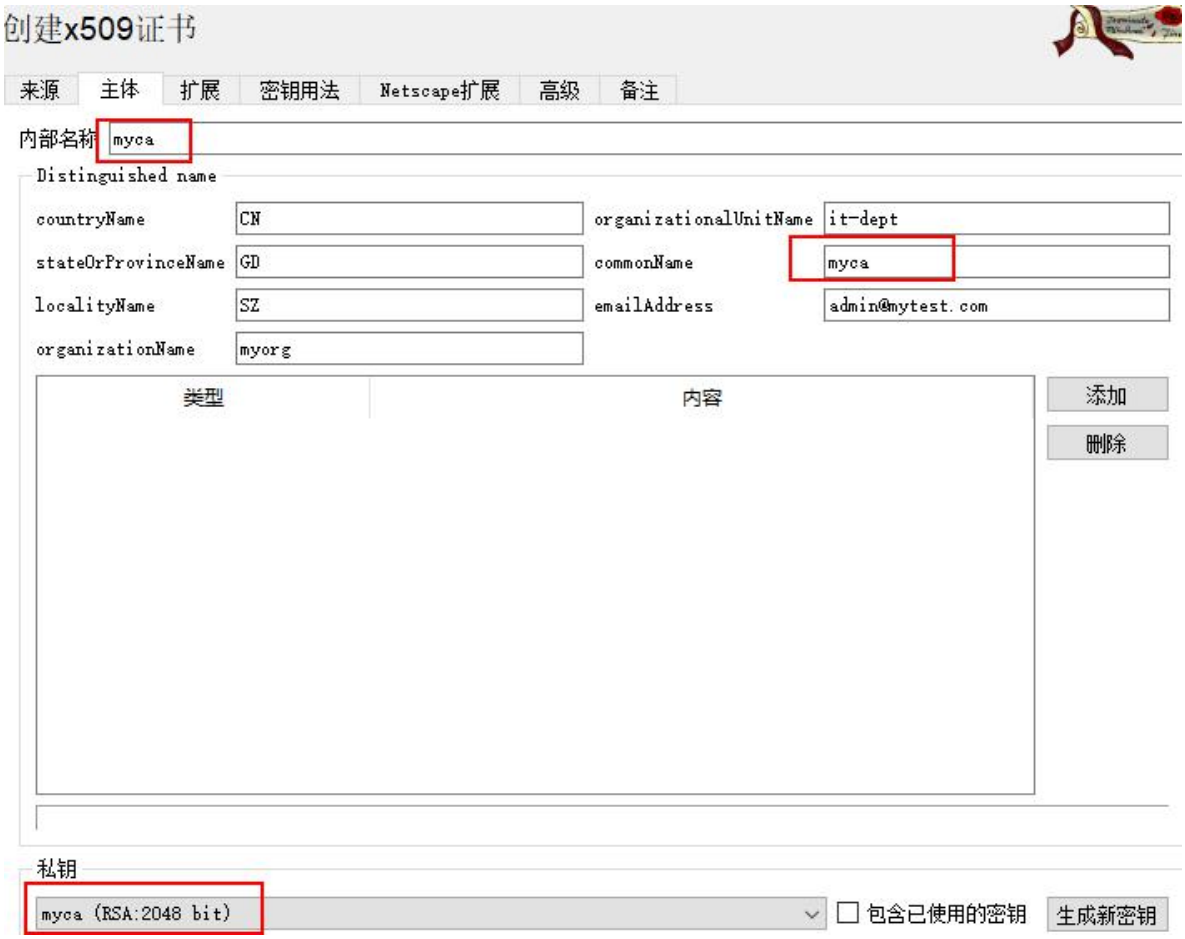
dh 参数文件内容也是 base64 编码的：

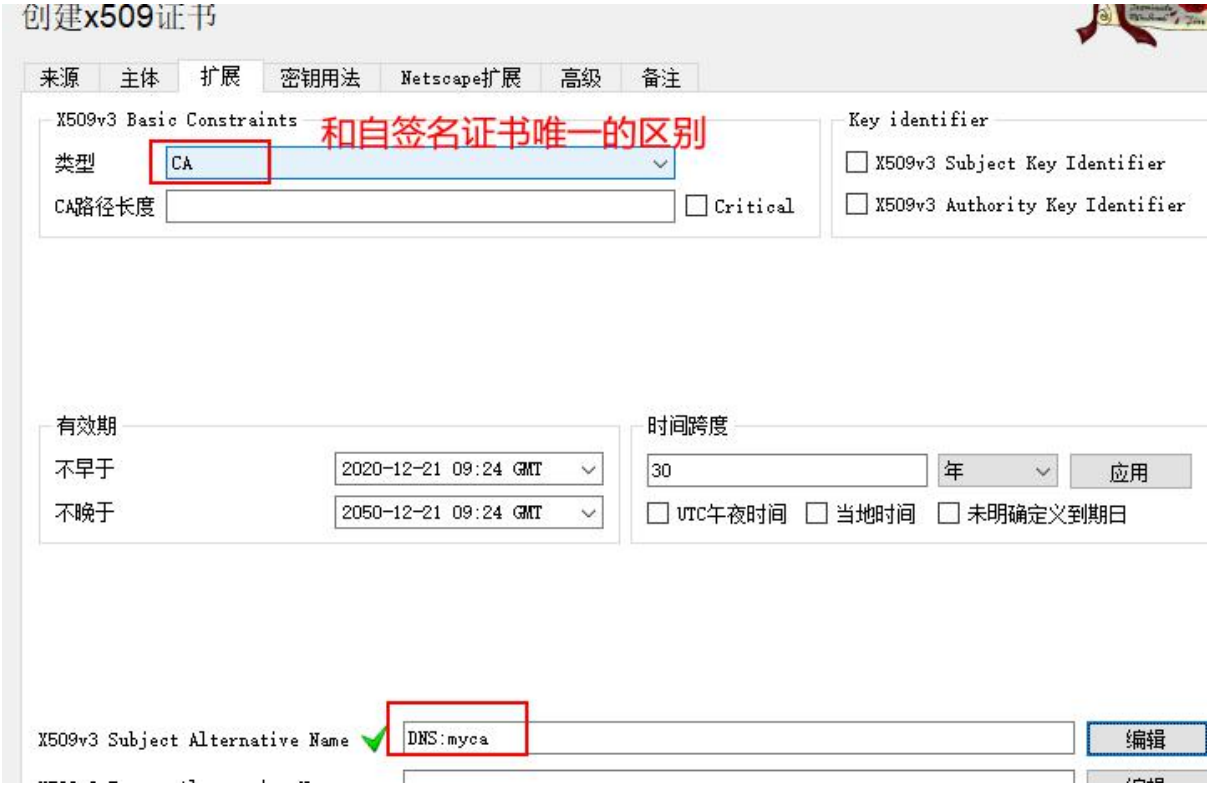
# 八、创建 CA 证书

自己可以生成自签名证书，也可以给其他的 CSR 文件进行签名，即自己作为一个 CA 给别人签名。

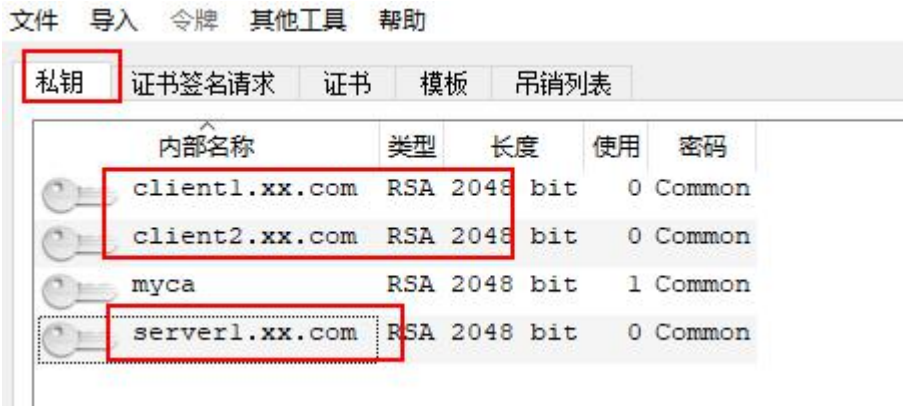
**①生成 CA 证书**

和创建自签名证书过程一样（先创密钥对，再创证书）唯一不同的是在证书类型那里，选择 **CA**

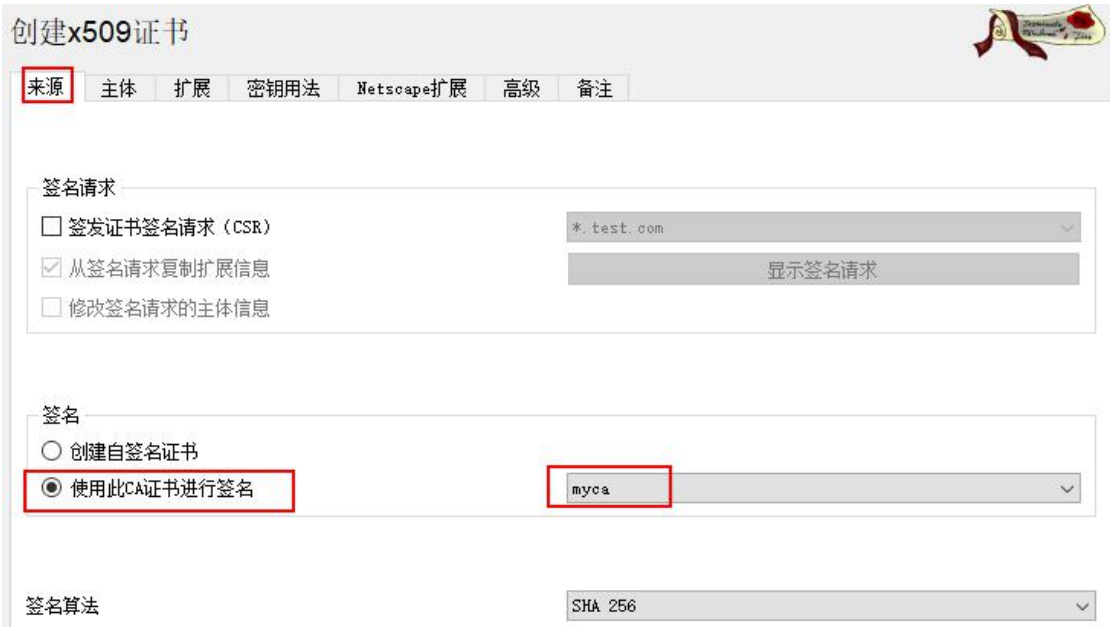


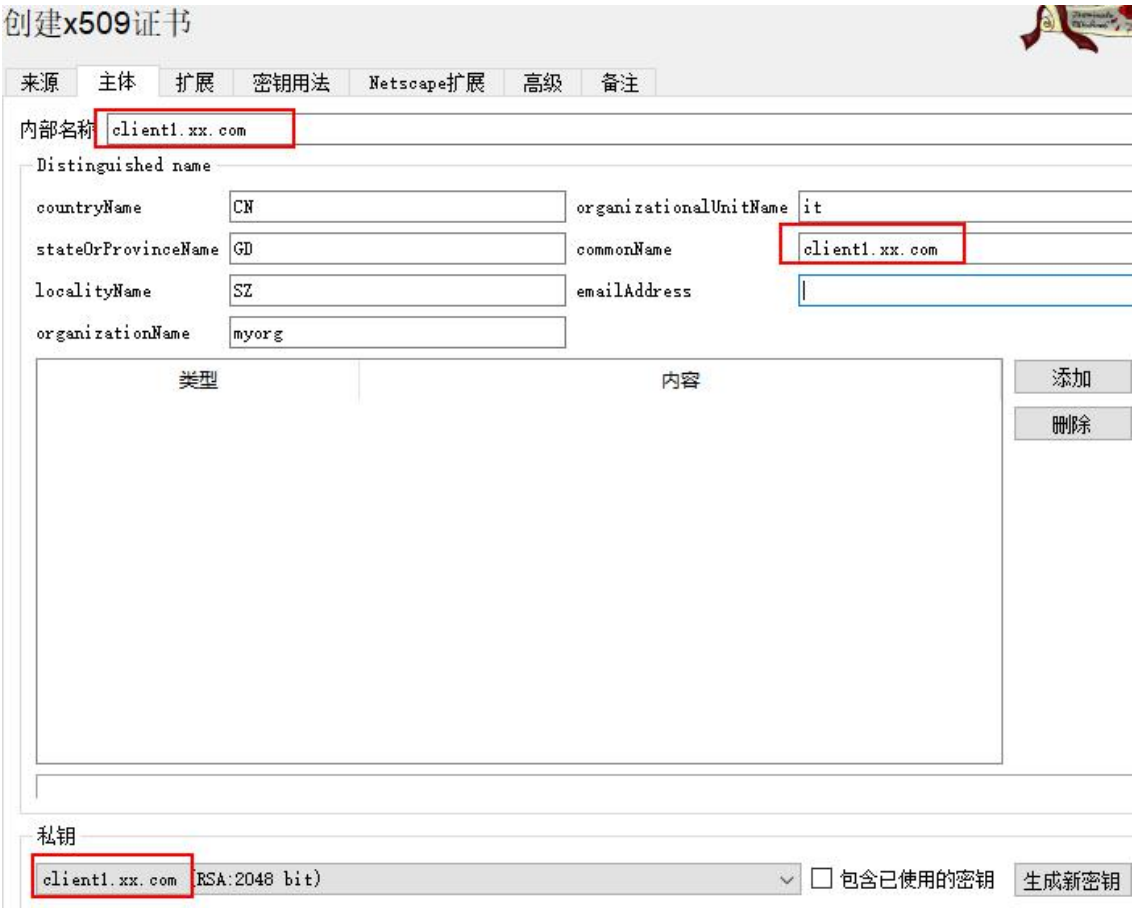


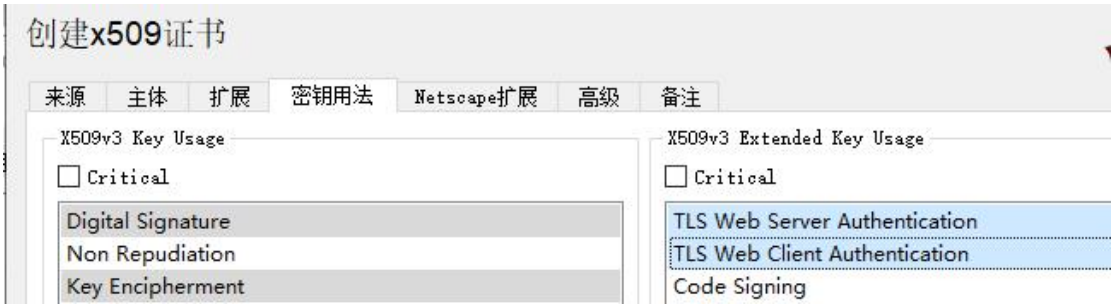

②然后也可直接在本数据库里创建若干客户的 rsa 密钥，再用此 CA 去给它们签名，生成客户的 ssl 证书（这些客户的 CA 是同一个）；也可让客户自己去创建 CSR 证书签名请求文件




③用自签名的 CA 给客户们签名


创建x509证书
来源
主体
扩展
密钥用法
Netscape扩展
高级
备注
签名请求
签发证书签名请求（CSR）
*.test.com
从签名请求复制扩展信息
显示签名请求
修改签名请求的主体信息
签名
创建自签名证书
使用此CA证书进行签名
myca
签名算法
SHA 256


创建x509证书
来源
主体
扩展
密钥用法
Netscape扩展
高级
备注
内部名称
client1.xx.com
Distinguished name
countryName
CN
organizationalUnitName
it
stateOrProvinceName
GD
commonName
client1.xx.com
localityName
SZ
emailAddress
organizationName
myorg
类型
内容
添加
删除
私钥
client1.xx.com
(RSA:2048 bit)
包含已使用的密钥
生成新密钥


创建x509证书
来源
主体
扩展
密钥用法
Netscape扩展
高级
备注
X509v3 Key Usage
Critical
Digital Signature
Non Repudiation
Key Encipherment
X509v3 Extended Key Usage
Critical
TLS Web Server Authentication
TLS Web Client Authentication
Code Signing



点击 ok 后，就生成了客户 1 的证书了，它是用我们自签名的 CA（myca）去签名的

同以上步骤创建其他客户的证书… …


如上图，myca 给三个客户签名了，生成的 3 个客户证书都位于 myca 证书下方

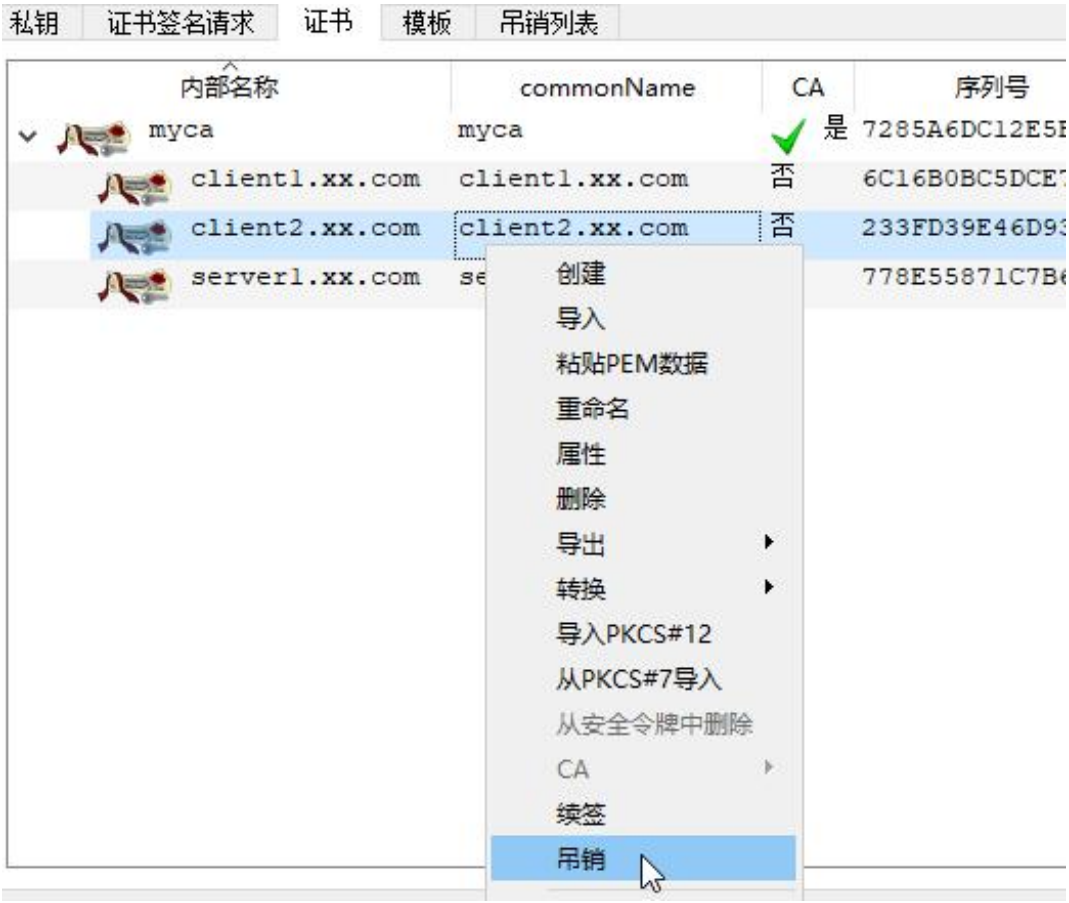
# 九、吊销客户证书

当用 myca 这个 CA 给其他客户签名证书之后，默认客户的证书作废时间为证书时写的到期时间，如果未到此时间而此证书又由于其他原因作废了，怎么办？

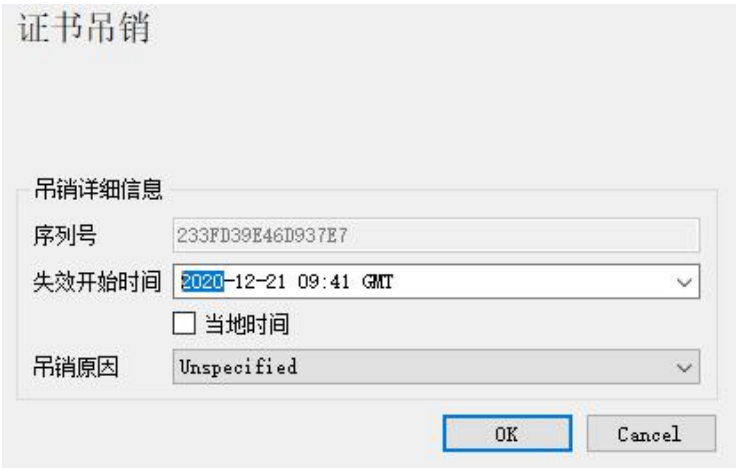
需要吊销此客户证书，并生成 CRL 证书吊销列表文件（Certificate Revocation List）

**①吊销某客户证书**

假如 client2.xx.com 由于密钥被窃，告知我们（我们是 CA 认证机构），我们需要宣告它的证书作废，




右键点击目标客户的证书，点击“吊销”



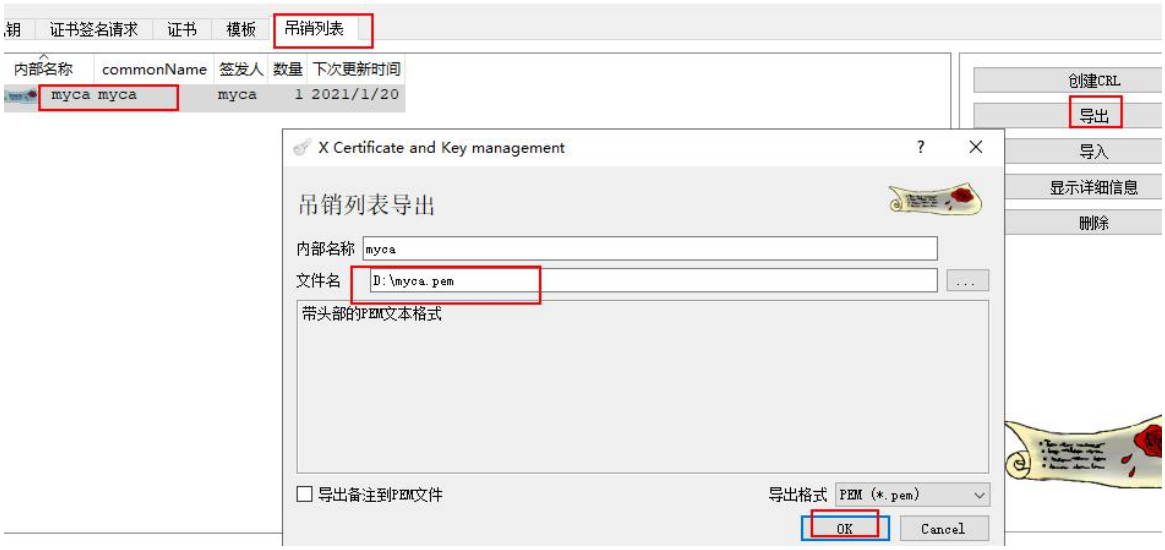

吊销原因随便选，点击 OK


在此客户的证书上就出现了一个红色的叉号

**②然后要生成 CRL 证书吊销列表文件**

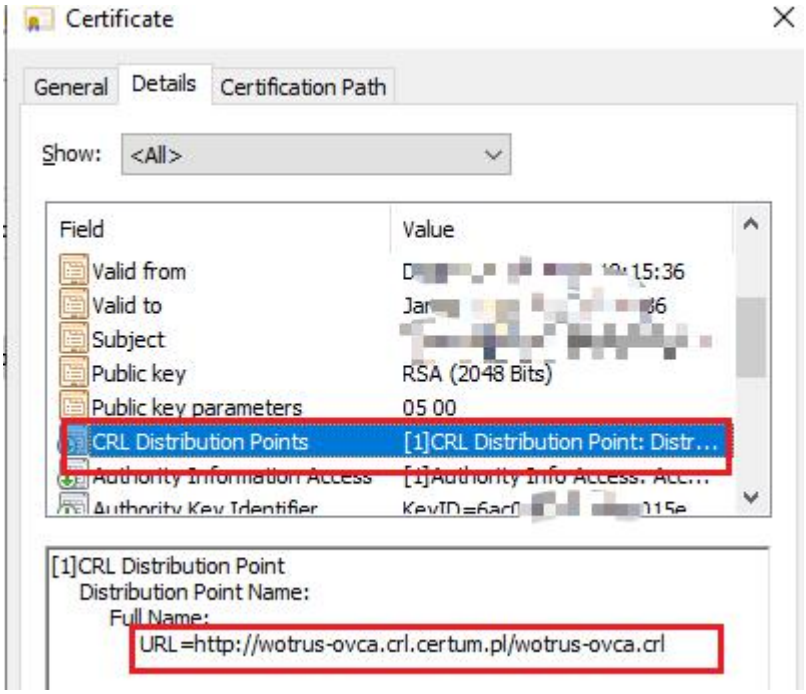

点击“吊销列表”→“创建 CRL”


点击 OK 即可，



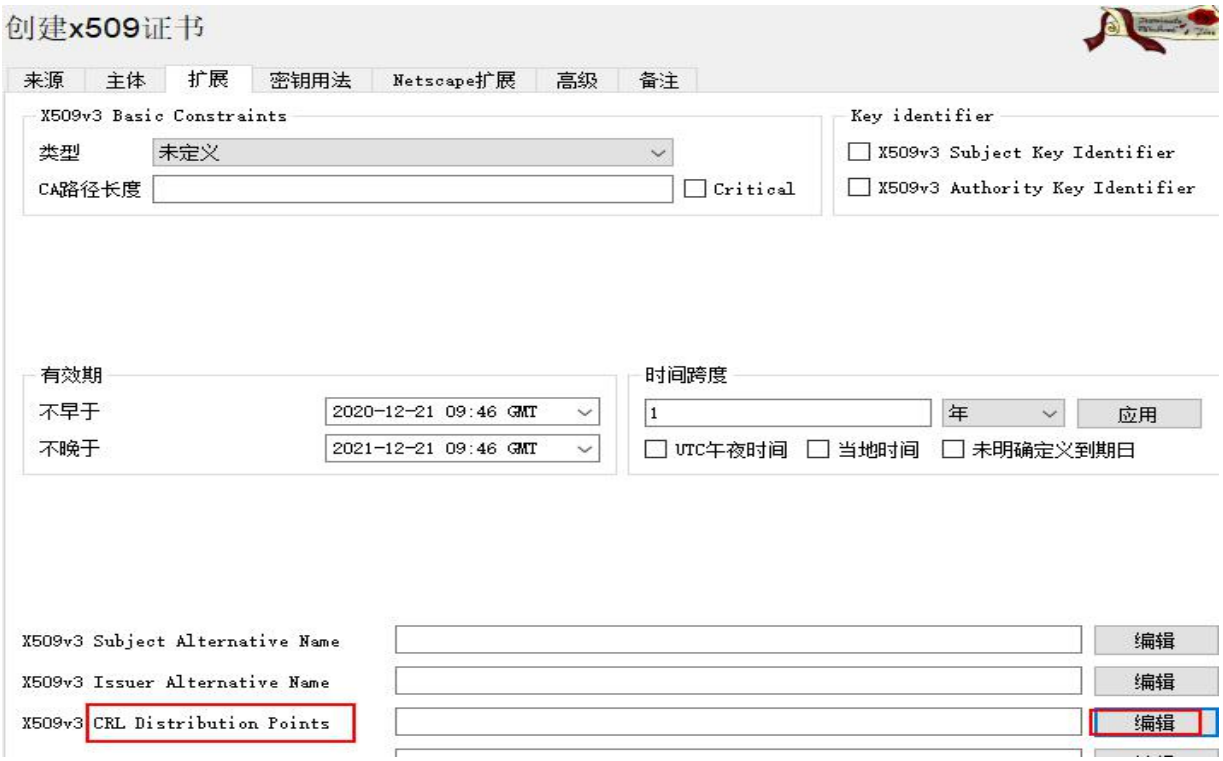

最后导出此 crl 文件，文件名改为.crl 后缀，最后发布到自己的 crl 发布网站上就行了

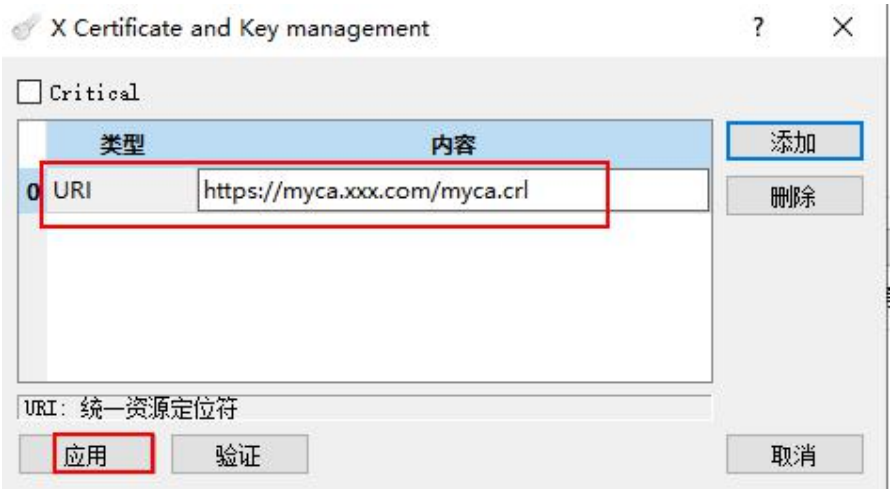
③那么客户端是怎么知道此证书已被吊销了呢？
因为浏览器在验证客户的 ssl 证书时，会查看它的扩展字段里的 CRL 端点/分发点，如下图：

浏览器再去 crl 分发点的地址下载 CA 的 crl 文件，并查看里面是否有此目标客户 ssl 证书的记录，如果有则说明此证书已被吊销，就不可信了，没有则再进一步验证。

④所以我们在给客户签名证书时，要多添加一个扩展字段：CRL distribution points




这样生成的客户证书就有“crl 分发点地址”扩展字段了，
我们定时更新 crl 文件并上传到此站点就行了（我们这时是 CA）

作者：cof-lee
日期：2020-12-21