CFCA 全球信任证书

(SSL 证书)

中国金融认证中心

技术支持部

2016 年 10 月

文档修订记录

版本	内容	日期	编写	审核
1.0	第一版	2013.3.7	张诚	
2.0	增加证书格式转换	2013.12.2	张诚	
2.1	增加应用服务证书配置	2014.1.9	张诚	
2.2	修改部分应用服务证书配置	2014.1.20	张诚	
2.3	修改证书 DN 生成规则	2014.4.16	张诚	
2.4	增加 SSLv3 禁用方式	2014.11.6	张诚	
2.5	增加 Nginx 双向 SSL 配置	2015.4.13	张诚	
3.0	完善证书介绍	2015.5.18	张诚	
3.1	完善证书介绍	2015.7.7	张诚	
3.2	完善证书介绍	2015.7.13	张诚	
4.0	完善证书介绍、办理流程等	2015.12.3	张诚	
4.1	增加域名或者公网 IP 的证明示例和常见问题	2016.2.5	胡俊燕	
4.2	修改服务器证书支持范围（增加 MAC OS 和 IOS 系统），根据业务部的新申请表更新本文申请表	2016.10.28	王瑞萍	

目　　录

一、CFCA 全球信任 SSL 证书介绍.....1
1.1 什么是 SSL 证书？.....1
1.2 什么是 CFCA 全球信任 SSL 证书？.....1
1.3 CFCA 全球信任 SSL 证书有哪些优势？.....2
1.4 CFCA 全球信任 SSL 证书有哪些产品？.....2
1.4.1 CFCA EV SSL 证书.....3
1.4.2 CFCA EV 多域名 SSL 证书.....4
1.4.3 CFCA OV SSL 证书.....4
1.4.4 CFCA OV 多域名 SSL 证书.....5
1.4.5 CFCA OV 通配符 SSL 证书.....6
二、CFCA 全球信任 SSL 证书办理.....7
2.1 机构申请.....7
2.2 CFCA 审核.....9
2.3 证书签发.....9
2.4 证书更新、延期、吊销.....9
三、CFCA 全球信任 SSL 证书制作.....10
3.1 证书制作说明.....10
3.2 密钥和证书请求文件 CSR.....10
3.3 证书文件格式.....11
3.4 证书制作.....11
3.4.1 使用 Keytool 工具制作证书.....11
3.4.2 使用 OpenSSL 工具制作证书.....15
3.4.3 使用 iKeyman 工具制作证书.....17
3.5 证书格式转换.....21
3.5.1 JKS 转换为 PFX.....21
3.5.2 PFX 转换为 JKS.....21
3.5.3 KEY&CRT 转换为 PFX.....21
3.5.4 PFX 转换为 KEY&CRT.....22
3.5.5 KDB 转换为 PFX.....22
3.5.6 PFX 转换为 KDB.....23
3.6 证书部署.....28
3.6.1 Apache 证书配置.....28
3.6.2 Tomcat 证书配置.....30
3.6.3 Nginx 证书配置.....30
3.6.4 Weblogic 证书配置.....32
3.6.5 IBM Http Server 证书配置.....35
3.6.6 JBoss 证书配置.....36
3.6.7 IIS 证书配置.....36

附录一、CFCA 全球信任证书（SSL 证书）申请表.....43
附录二、CFCA 全球信任根证书获取方式.....46
附录三、CFCA 全球信任证书链.....47
附录四、SHA 摘要算法介绍.....52
附录五、常见问题.....53

一、CFCA 全球信任 SSL 证书介绍

1.1 什么是 SSL 证书？

随着信息技术的发展，互联网站以及基于互联网的应用系统面临越来越严重的安全威胁。其中，网站面临的两个最基本的问题是：

1、网站身份的真实性

用户访问网站时需要确认网站的真实性。由于互联网的开放和共享，互联网上存在很多虚假的网站。如何让用户信任自己访问的网站是真实的？

2、信息传输的保密性

大量的网上应用需要用户向网站应用系统提交一些隐私或者机密信息，同时网站应用系统也可能向用户返回一些隐私或者机密信息。如何确保信息传输过程中的安全？

SSL 证书，是由权威的、可信的第三方数字证书认证机构（CA）签发的，用来标记网站身份的数字证书。因其通常部署在网站服务器上，也称为网站证书或者服务器证书。SSL 证书通过在客户端浏览器和网站服务器之间建立一条 SSL 安全通道（Secure Socket Layer），对传输的数据进行加密，确保数据在传输过程中不被窃听、篡改和伪造。有效地解决了网站身份的真实性和信息传输的保密性问题。

1.2 什么是 CFCA 全球信任 SSL 证书？

中国金融认证中心（China Financial Certification Authority，简称 CFCA）是经中国人民银行和国家信息安全管理机构批准成立的国家级权威安全认证机构，是国家重要的金融信息安全基础设施之一。在《中华人民共和国电子签名法》颁布后，CFCA 成为首批获得电子认证服务许可的电子认证服务机构。

中国金融认证中心全球信任证书（Global Trust Certificate）是发放给全球范围的数字证书，通过微软根证书项目认证、Mozilla 根证书认证和苹果根证书认证，其根证书已经预埋在微软所有系统、设备，Mozilla 所有产品以及苹果所有产

品中。

CFCA 全球服务器证书（SSL 证书）由 CFCA 自主研发。CFCA 作为国内第一家与国外 SSL 服务器证书厂商媲美的电子认证服务机构，严格按照国际标准提供电子认证服务，并结合我国国情，在密码算法、安全技术服务等方面兼容国际和国产算法。目前已通过第三方审计公司按照国内、国际双重标准进行的审计。

CFCA 全球服务器证书（SSL 证书）相当于 Web 站点的网络身份证，可为 Web 站点提供身份鉴定，并为 Web 站点提供高强度安全加密传输，保证信息在传输过程中的安全，能够有效地防止信息传输过程中的网络钓鱼、窃听、篡改等安全问题。

1.3 CFCA 全球信任 SSL 证书有哪些优势？

CFCA 全球信任 SSL 证书的优势：

- ✓ 由中国权威数字证书认证机构 CFCA 签发；
- ✓ CFCA 是国际 CA 浏览器联盟组织（CA/Browser Forum）成员，是国际证书标准的参与者；
- ✓ CFCA 通过国际 WebTrust 认证，遵循全球统一鉴证标准；
- ✓ 根系统、吊销列表、证书管理、鉴证资料、服务支持本地化；
- ✓ 金融级的安全保障服务；
- ✓ 完善的风险承保计划，确保理赔的可行性和便捷性；
- ✓ 中文版 CPS（全球信任体系电子认证业务规则）便于用户理解双方权利和义务。

1.4 CFCA 全球信任 SSL 证书有哪些产品？

CFCA 全球信任 SSL 证书包括：

CFCA EV SSL 证书

CFCA EV 多域名 SSL 证书

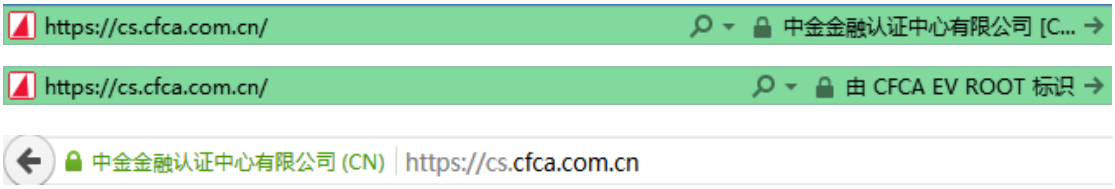
CFCA OV SSL 证书

CFCA OV 多域名 SSL 证书

CFCA OV 通配符 SSL 证书

1.4.1 CFCA EV SSL 证书

CFCA EV SSL 服务器证书相当于网站的身份证，可为网站提供身份鉴定和高强度安全加密服务。CFCA EV SSL 证书遵循全球统一认证标准中最严格的 Webtrust EV 标准。部署 CFCA EV SSL 证书的网站，浏览器地址栏自动变成绿色，循环显示公司名称（支持中文）和 CFCA 认证机构标识。访客浏览器和网站服务器之间建立起 SSL 安全加密通道（Secure Sockets Layer），有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。



- ✓ 有效期 1 至 2 年；
- ✓ 2 至 5 个工作日快速签发；
- ✓ 有效期内免费重新签发；
- ✓ 证书到期前自动提醒；
- ✓ 提供安全站点签章；
- ✓ 支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法；
- ✓ Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；
- ✓ Windows Phone 平台浏览器 100%支持；
- ✓ Andriod（Android 6.0 Marshmallow）平台 100%支持；
- ✓ Linux 平台浏览器 100%支持；
- ✓ Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；
- ✓ IOS（10.1 及更新版本）平台浏览器 100%支持；
- ✓ 支持 128 位至 256 位加密强度；

- ✓ 最高人民币 50 万元赔付保障。

1.4.2 CFCA EV 多域名 SSL 证书

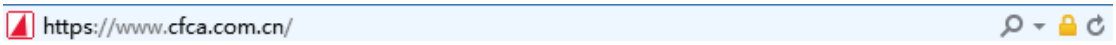
CFCA EV 多域名 SSL 证书，将有限多个域名写入一个证书文件中，可以同时保护多个域名的 EV SSL 证书。部署 CFCA EV 多域名 SSL 证书的多个网站，浏览器地址栏自动变成绿色，循环显示公司名称（支持中文）和 CFCA 认证机构标识。访客浏览器和网站服务器之间建立起 SSL 安全加密通道（Secure Sockets Layer），有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期 1 至 2 年；
- ✓ 2 至 5 个工作日快速签发；
- ✓ 有效期内免费重新签发；
- ✓ 证书到期前自动提醒；
- ✓ 提供安全站点签章；
- ✓ 支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法；
- ✓ Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；
- ✓ Windows Phone 平台浏览器 100%支持；
- ✓ Andriod（Android 6.0 Marshmallow）平台 100%支持；
- ✓ Linux 平台浏览器 100%支持；
- ✓ Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；
- ✓ IOS（10.1 及更新版本）平台浏览器 100%支持；
- ✓ 支持 128 位至 256 位加密强度；
- ✓ 最高人民币 50 万元赔付保障。

1.4.3 CFCA OV SSL 证书

CFCA OV SSL 服务器证书相当于网站的身份证，可为网站提供身份鉴定和高

强度安全加密服务。部署 CFCA 标准 SSL 证书的网站，浏览器地址栏有锁的标志，可以查看证书颁发机构名称，增加客户信赖度。访客浏览器和网站服务器之间建立起 SSL 安全加密通道（Secure Sockets Layer），有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。



- ✓ 有效期 1 至 3 年；
- ✓ 2 至 5 个工作日快速签发；
- ✓ 有效期内免费重新签发；
- ✓ 证书到期前自动提醒；
- ✓ 提供安全站点签章；
- ✓ 支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法；
- ✓ Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；
- ✓ Windows Phone 平台浏览器 100%支持；
- ✓ Andriod（Android 6.0 Marshmallow）平台 100%支持；
- ✓ Linux 平台浏览器 100%支持；
- ✓ Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；
- ✓ IOS（10.1 及更新版本）平台浏览器 100%支持；
- ✓ 支持 128 位至 256 位加密强度；
- ✓ 最高人民币 50 万元赔付保障。

1.4.4 CFCA OV 多域名 SSL 证书

CFCA OV 多域名 SSL 证书，将有限多个域名写入一个证书文件中，可以同时保护多个域名的 SSL 证书。部署 CFCA 标准多域名 SSL 证书的多个网站，浏览器地址栏有锁的标志，可以查看证书颁发机构名称，增加客户信赖度。访客浏览器和网站服务器之间建立起 SSL 安全加密通道（Secure Sockets Layer），有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期 1 至 3 年；
- ✓ 2 至 5 个工作日快速签发；
- ✓ 有效期内免费重新签发；
- ✓ 证书到期前自动提醒；
- ✓ 提供安全站点签章；
- ✓ 支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法；
- ✓ Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；
- ✓ Windows Phone 平台浏览器 100%支持；
- ✓ Andriod（Android 6.0 Marshmallow）平台 100%支持；
- ✓ Linux 平台浏览器 100%支持；
- ✓ Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；
- ✓ IOS（10.1 及更新版本）平台浏览器 100%支持；
- ✓ 支持 128 位至 256 位加密强度；
- ✓ 最高人民币 50 万元赔付保障。

1.4.5 CFCA OV 通配符 SSL 证书

CFCA OV 通配符 SSL 证书适用于网站主域名（www.domain.com）以及子域名（*.domain.com），不限制子域名数量。部署 CFCA 标准通配符 SSL 证书的多个网站，浏览器地址栏有锁的标志，可以查看证书颁发机构名称，增加客户信赖度。访客浏览器和网站服务器之间建立起 SSL 安全加密通道（Secure Sockets Layer），有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期 1 至 3 年；
- ✓ 2 至 5 个工作日快速签发；
- ✓ 有效期内免费重新签发；
- ✓ 证书到期前自动提醒；
- ✓ 提供安全站点签章；

- ✓ 支持 RSA 算法，2048 位密钥强度，SHA256 摘要算法；
- ✓ Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；
- ✓ Windows Phone 平台浏览器 100%支持；
- ✓ Andriod（Android 6.0 Marshmallow）平台 100%支持；
- ✓ Linux 平台浏览器 100%支持；
- ✓ Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；
- ✓ IOS（10.1 及更新版本）平台浏览器 100%支持；
- ✓ 支持 128 位至 256 位加密强度；
- ✓ 最高人民币 50 万元赔付保障。

二、CFCA 全球信任 SSL 证书办理

CFCA 全球信任 SSL 证书办理过程，申请机构必须提供真实的材料，以证明机构的真实身份、申请人的真实身份、机构对网站域名的所有权等。CFCA 将对机构提供的材料进行严格审查。

2.1 机构申请

申请机构需要向 CFCA 提供如下材料：

1、证书申请表（详见附录一、附录二）；

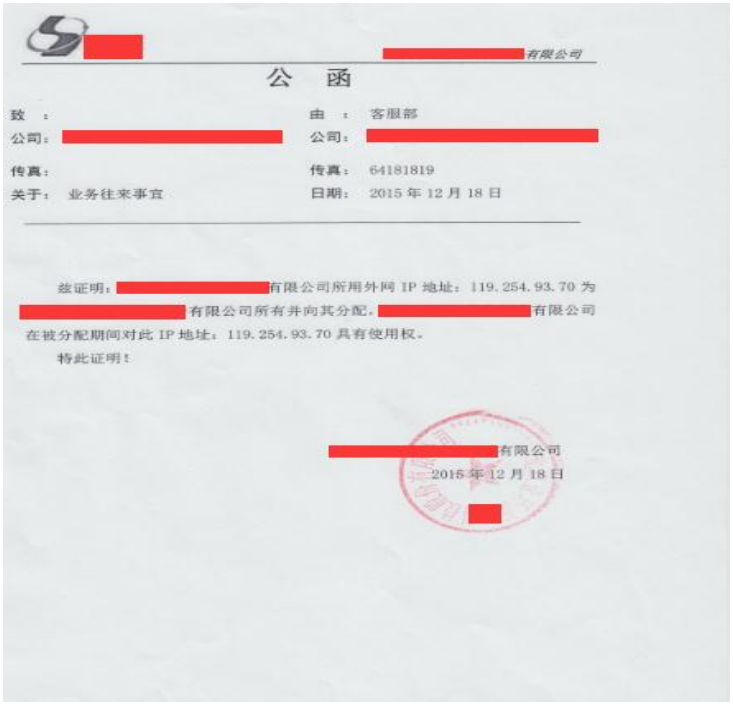
2、至少一种机构身份证件（如，企业营业执照副本复印件）；

3、申请人的个人身份证件（如，申请人身份证复印件）；

4、机构授予申请人的授权证明；

5、域名或者公网 IP 的证明（内网 IP 不能申请）；

IP 分配权证明示例如下：



[redacted] [redacted]有限公司

公 函

致 ： 由 ： 客服部

公司： [redacted] 公司： [redacted]

传真： 传真： 64181819

关于： 业务往来事宜 日期： 2015 年 12 月 18 日

兹证明：[redacted]有限公司所用外网 IP 地址：119.254.93.70 为[redacted]有限公司所有并向其分配，[redacted]有限公司在被分配期间对此 IP 地址：119.254.93.70 具有使用权。

特此证明！

[redacted]有限公司

2015 年 12 月 18 日

[redacted]

域名证书示例如下：

ICANN

顶级国际域名证书

Certification of Global Top Level Domain Name

域名[redacted] 已由 [redacted] 注册，并已在国内顶级域名数据库中记录。

This is to certify that the domain name gdnybank.com has been registered by zhongshanguzhennanyuecunzhenyinhanggufenyouxiangongsi .And the registration has been put on records in the database of gTLD(Generic Top Level Domain) and ccTLD(Country Code Top Level Domain).

域名：[redacted]

域名持有者：[redacted]股份有限公司

Registrant：[redacted]

域名所属注册机构：北京万网志成科技有限公司

域名注册日期：2011-7-07

域名到期日期：2021-7-07

北京万网志成科技有限公司

以下说明与本证书主文一起构成本证书统一整体，不可分割

1. 本证书表明证书上列出的组织或者个人是列出的域名的合法注册人，该注册人依法享有该域名项下之各项权利。
2. 本证书并不表明北京万网志成科技有限公司对本证书所列域名是否贬斥、侵害或毁损任何第三人之合法权利或利益作出任何明示或默示之评判、确认、担保，或作出其它任何形式之意思表示。北京万网志成科技有限公司亦无任何责任或义务作出上述之评判、确认、担保，或作出其它任何形式之意思表示。
3. 因本证书中所列域名之注册或使用而可能引发与任何第三人之纠纷或冲突，均由该域名注册人本人承担，北京万网志成科技有限公司不承担任何法律责任。北京万网志成科技有限公司亦不在此类纠纷或冲突中充当证人、调停人或其它形式之参与人。
4. 本证书不得用于非法目的，北京万网志成科技有限公司不承担任何由此而发生或可能发生之法律责任。
5. 本证书仅用于证明域名注册当时的域名状态和持有人情况，若域名被转让、转出万网、被删除或发生其他改变域名状态及持有人信息的情况，则本证书不再具有证明效力。当本证书持有、出具、展示或以其它任何形式使用时，即表明本证书之持有人或接触人已审读、理解并同意以上各条款之规定。

6、证书请求文件 CSR（什么是 CSR？请参考 3.3 章节）。

以上材料除第 6 项外，均需加盖公章。所盖公章为机构公章，不可使用部门章、业务章等，并且公章的名称要与机构名称一致。

申请机构需要将上述所有材料提供给 CFCA 商务经理，申请机构必须保证所提供材料的真实性，CFCA 商务经理将协助机构办理证书。

2.2 CFCA 审核

CFCA 业务部门将对申请机构提供的材料进行审查，主要内容包括：

1、检查证书申请表中机构信息与提供的机构身份证件是否相符。

2、检查证书申请表中申请人信息与提供的申请人身份证件是否相符，与机构授予申请人的授权证明是否一致。

3、检查证书申请表中域名与提供的域名证明是否相符。如检查域名非申请机构所有，则需要申请机构提供该域名所有者出具的唯一使用该域名的授权证明材料。如使用公网 IP，需提供网络运营商出具的 IP 授权使用证明。

4、CSR 文件，DN 规则要求符合如下规范：

（1）DN 中各项顺序依次为：CN、OU、O、L、ST、C；

（2）CN 项必须是域名，与证书申请表中域名一致；

（3）O 项必须是真实的、完整的机构名称，与证书申请表中机构名称一致；

（4）L 项、ST 项、C 项是必须是机构所在地区，与机构身份证件中的注册地区一致。

2.3 证书签发

CFCA 审核通过后，将由 CFCA 证书管理员签发证书。证书公钥及证书链将发送到证书申请表中的申请人电子邮件地址。

2.4 证书更新、延期、吊销

机构使用证书过程中，如果出现证书遗失、损坏、密钥泄露等问题，需要重新签发证书的，机构应按照 2.1 章节重新提供材料办理证书更新。证书有效期内 CFCA 免费进行证书更新。

证书到期前三个月内，CFCA 商务经理会主动提醒机构申请人办理证书延期。机构应按照 2.1 章节重新提供材料办理证书延期。

机构如果不再使用证书，可以联系 CFCA 商务经理办理证书吊销，并将该证书从网站服务器上移除。

三、CFCA 全球信任 SSL 证书制作

3.1 证书制作说明

CFCA 全球信任 SSL 证书需要部署在网站 Web 服务上，制作证书之前请先了解网站 Web 服务所使用的软件或者硬件。

1、如果网站使用网关、负载均衡等硬件设备提供 Web 服务，请咨询相应的硬件厂商制作和部署 SSL 证书的方法。

2、如果网站使用 IBM Http Server（IHS）、Internet Information Services（IIS）、Oracle Weblogic 等商业软件提供 Web 服务，请优先咨询软件厂商制作和部署 SSL 证书的方法。本章节也提供了部分商业软件制作 SSL 证书方法，仅供参考。

3、如果网站使用 Nginx、Apache、Tomcat 等开源软件，请优先通过开源软件的技术文档了解制作和部署 SSL 证书的方法。本章节也提供了部分开源软件制作 SSL 证书方法，仅供参考。

4、部署 SSL 证书时，必须部署相应的证书链。办理 CFCA EV SSL 证书、EV SSL 多域名证书，需要部署根证书 CFCA EV Root 和中级证书 CFCA EV OCA；办理 CFCA OV SSL 证书、OV SSL 多域名证书、OV SSL 通配符证书，需要部署根证书 CFCA EV Root 和中级证书 CFCA OV OCA。证书链文件会与证书文件一起发送到证书申请表中的申请人电子邮件地址。关于证书链的详细信息可参考“附录四、CFCA 全球信任证书链”。

3.2 密钥和证书请求文件 CSR

SSL 证书中含有一套非对称密钥，用于客户端浏览器和网站服务器之间的数据加密。证书申请机构应当在安全的服务器或者设备上生成密钥和证书请求文件 CSR（Cerificate Signing Request）。其中，CSR 提交给 CFCA 用于签发证书（详见 2.1 章节），密钥由证书申请机构保管。

特别注意，任何机构或者个人如果拥有该密钥，即可通过技术手段解密客户端浏览器和网站服务器之间的加密数据，给网站和网站用户造成极大的安全威胁。

因此，证书申请机构务必妥善保管密钥！一旦密钥泄露，请证书申请机构重新生成密钥和 CSR，并立即联系 CFCA 进行证书更新（参考 2.4 章节）。CFCA 将使用新提供的 CSR 签发证书，并将已泄露密钥的证书吊销。

此外，证书申请机构只需将 CSR 提交给 CFCA，CFCA 使用 CSR 签发证书。即 CFCA 并不拥有证书申请机构的密钥，也无法解密客户端浏览器和网站服务器之间的加密数据。

3.3 证书文件格式

一般来说，主流的 Web 服务软件，通常都基于两种基础密码库：OpenSSL 和 Java。

Tomcat、Weblogic、JBoss 等，使用 Java 提供的密码库。通过 Java 的 Keytool 工具，生成 Java Keystore（JKS）格式的证书文件。

Apache、Nginx 等，使用 OpenSSL 提供的密码库，生成 PEM、KEY、CRT 等格式的证书文件。

此外，IBM 的产品，如 Websphere、IBM Http Server（IHS）等，使用 IBM 产品自带的 iKeyman 工具，生成 KDB 格式的证书文件。微软 Windows Server 中的 Internet Information Services（IIS），使用 Windows 自带的证书库生成 PFX 格式的证书文件。

3.4 章节提供了部分主流的 Web 服务软件生成密钥、CSR、证书文件的方法，3.5 章节提供了常用证书文件格式相互转换的方法，仅供参考。

3.4 证书制作

3.4.1 使用 Keytool 工具制作证书

Keytool 是 JDK 中自带的密钥管理工具，可以制作 Keystore（jks）格式的证书文件。下载并安装 JDK 后，可以通过相关命令制作服务器证书。

以下地址可以下载 JDK：

http://www.oracle.com/technetwork/java/javase/downloads/index.html

以下以 Windows 平台为例，介绍制作证书的方法。

1、进入 Keytool 目录；

```
cd C:\Program Files\java\jdk1.6.0_39\bin
```

2、生成证书文件 Keystore，文件后缀名可以是 jks、keystore，证书文件中包含密钥；

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore D:\server.jks
```

其中，keyalg 是密钥类型，必须为 RSA；keysize 是密钥长度，必须是 2048，alias 是证书别名，可自定义；keystore 是证书文件保存的路径。

而后，输入证书文件的密码：

```
输入 keystore 密码：

再次输入新密码：
```

而后，输入名称（CN），即证书申请表中的域名；

```
您的名字与姓氏是什么？

  [Unknown]：  www.cfca.com.cn
```

而后，输入组织单位（OU），即证书申请表中申请人的部门名称；

```
您的组织单位名称是什么？

  [Unknown]：  技术支持部
```

而后，输入组织（O），即机构身份证件中机构名称全称；

```
您的组织名称是什么？

  [Unknown]：  中金金融认证中心有限公司
```

而后，输入城市（L），即机构身份证件中机构所在市级地区；

```
您所在的城市或区域名称是什么？

  [Unknown]：  北京
```

而后，输入省份（ST），即机构身份证件中机构所在省级地区；

```
您所在的州或省份名称是什么？

  [Unknown]：  北京
```

而后，输入机构身份证件中机构所在的国家或者行政区（C），限定两位字母，如中国输入 CN，美国输入 US 等；

```
该单位的两字母国家代码是什么？
```

```
[Unknown]:  CN
```

输入完成后，确认输入内容是否正确；

```
CN=www.cfca.com.cn, OU=技术支持部, O=中金金融认证中心有限公司, L=北京, ST=北京, C=CN
正确吗？
  [否]:  Y
```

而后，提示输入密钥（Key）密码，可以与证书（Keystore）密码一致；

```
输入<mykey>的主密码
        （如果和 keystore 密码相同，按回车）：
```

确认后，即在 keystore 保存的路径下，生成证书文件（server.jks）。

3、通过证书文件，生成证书请求；

```
keytool -certreq -sigalg SHA256withRSA -alias server -keystore d:\server.jks -file d:\certreq.csr
```

其中，sigalg 是摘要算法，推荐 SHA256withRSA；alias 是别名，必须与第 2 步生成证书文件时定义的别名一致；keystore 是证书文件的路径，file 是产生证书请求（CSR）的路径。

而后，提示输入 keystore 的密码；

```
输入 keystore 密码：
```

确认后，即产生证书请求（CSR）文件（certreq.csr）。

4、证书申请机构将证书请求文件（certreq.csr）连同相关材料（详见 2.1）提供给 CFCA，并妥善保管证书文件（server.jks）。

5、CFCA 审核资料后，将公钥证书和证书链反馈给证书申请机构。

6、证书申请机构将收到的公钥证书和证书链（包括根证书和中级证书）装回到证书文件（server.jks）中。

其中，证书文件一般以申请单位全称命名；EV SSL 证书、EV 多域名 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是 CFCA_EV_OCA.cer；OV SSL 证书、OV 多域名 SSL 证书、OV 通配符 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是 CFCA_OV_OCA.cer（详见附录四）。

7、导入根证书（以 EV 证书为例，OV 证书请导入 OV 的根证书，下同）；

```
keytool -import -alias evca -keystore d:\server.jks -trustcacerts -file d:\CFCA_EV_CA.cer
```

而后，输入证书文件密码；

```
输入 keystore 密码：
```

而后，会显示根证书的属性；

```
所有者: CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
发布者: CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
序列号: 184accd6
有效期开始日期: Wed Aug 08 11:07:01 CST 2012，截止日期: Mon Dec 31 11:07:01 CST 2029
证书指纹:
        MD5: 74:E1:B6:ED:26:7A:7A:44:30:33:94:AB:7B:27:81:30
        SHA1: E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83
        SHA256:
5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:7
0:FD
        签名算法名称: SHA256withRSA
……
```

而后，确认信任认证，导入完成。

```
信任这个认证？ [否]：  Y
认证已添加至 keystore 中
```

8、导入中级证书；

```
keytool -import -alias evoca -keystore d:\server.jks -trustcacerts -file d:\CFCA_EV_OCA.cer
```

而后，输入证书文件密码；

```
输入 keystore 密码：
```

导入完成。

```
认证已添加至 keystore 中
```

9、导入服务器证书（证书文件一般以申请单位的全称命名）；

```
keytool -import –alias server -keystore d:\server.jks -trustcacerts -file d:\中金金融认证中心有限
公司.cer
```

其中，别名（alias）必须是生成证书文件时设置的别名，必须与第 2 步生成证书文件时定义的别名一致；

而后，输入证书文件密码；

```
输入 keystore 密码：
```

导入完成。

```
认证已添加至 keystore 中
```

完成上述操作后，生成完整的证书文件（server.jks），可以部署在 Tomcat、Weblogic 等 Web 应用中。

3.4.2 使用 OpenSSL 工具制作证书

使用 OpenSSL 工具可以制作 KEY 和 CRT 格式的证书文件，OpenSSL 工具可以从以下地址下载：

http://www.openssl.org/

以下以 Windows 平台为例，介绍制作证书的方法。

1、进入 OpenSSL 目录；

```
cd D:\OpenSSL\bin
```

2、生成证书文件 key 和证书请求文件 csr；

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

其中，newkey 必须是 rsa:2048，key 为密钥文件，csr 为证书请求文件，默认都在 OpenSSL 目录下；

```
Generating a 2048 bit RSA private key
.....................................................................+++
.....................+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
```

而后，输入机构身份证件中机构所在的国家或者行政区（C），限定两位字母，如中国输入 CN，美国输入 US 等；

```
Country Name (2 letter code) [AU]:CN
```

而后，输入省份（ST），即机构身份证件中机构所在省级地区；

```
State or Province Name (full name) [Some-State]:Beijing
```

而后，输入城市（L），即机构身份证件中机构所在市级地区；

```
Locality Name (eg, city) []:Beijing
```

而后，输入组织（O），即机构身份证件中机构名称全称；

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:China Financial Certification Authority
```

而后，输入组织单位（OU），即证书申请表中申请人的部门名称；

```
Organizational Unit Name (eg, section) []:Technology Department
```

而后，输入名称（CN），即证书申请表中的域名；

```
Common Name (e.g. server FQDN or YOUR name) []:www.cfca.com.cn
```

而后，以下几项均可不填写；

```
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Please enter the following 'extra' attributes
```

而后，将在 OpenSSL 目录下，产生证书文件 key 和证书请求文件 csr。

3、证书申请机构将证书请求文件（server.csr）连同相关材料（详见 2.1 章节）提供给 CFCA，并妥善保管密钥文件（server.key）。

4、CFCA 审核订户资料后，将公钥证书和证书链反馈给订户。

其中，证书文件一般以申请单位全称命名；EV SSL 证书、EV 多域名 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是 CFCA_EV_OCA.cer；OV SSL 证书、OV 多域名 SSL 证书、OV 通配符 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是

CFCA_OV_OCA.cer。

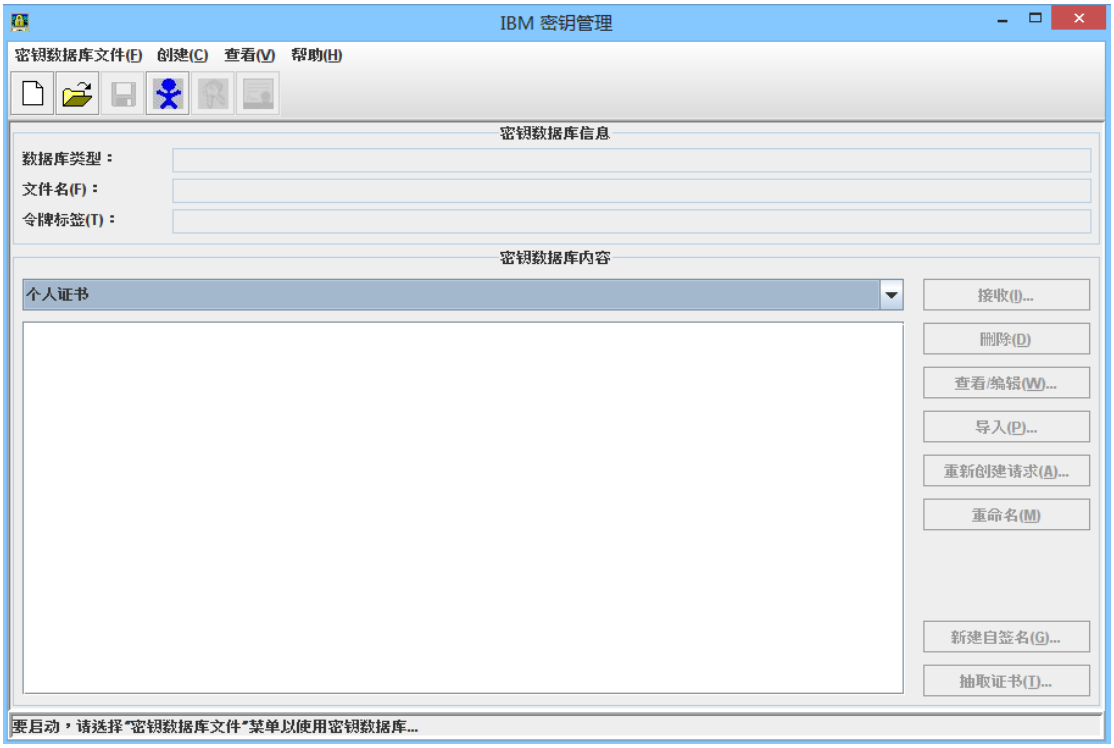
5、将服务器证书公钥另存为 server.crt。

完成上述操作后，server.key 为密钥文件、server.crt 为服务器证书文件，和证书链文件一起，可以部署在 Apache、Nginx 等 Web 应用中。

3.4.3 使用 iKeyman 工具制作证书

IBM HTTP Server 含有 iKeyman，可以制作证书。

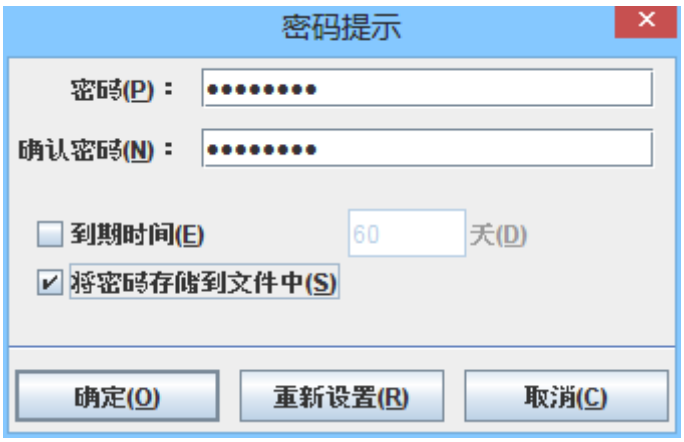
1、执行 IHS7 安装目录下，“bin”目录下的“ikeyman”命令，进入 iKeyman 界面。



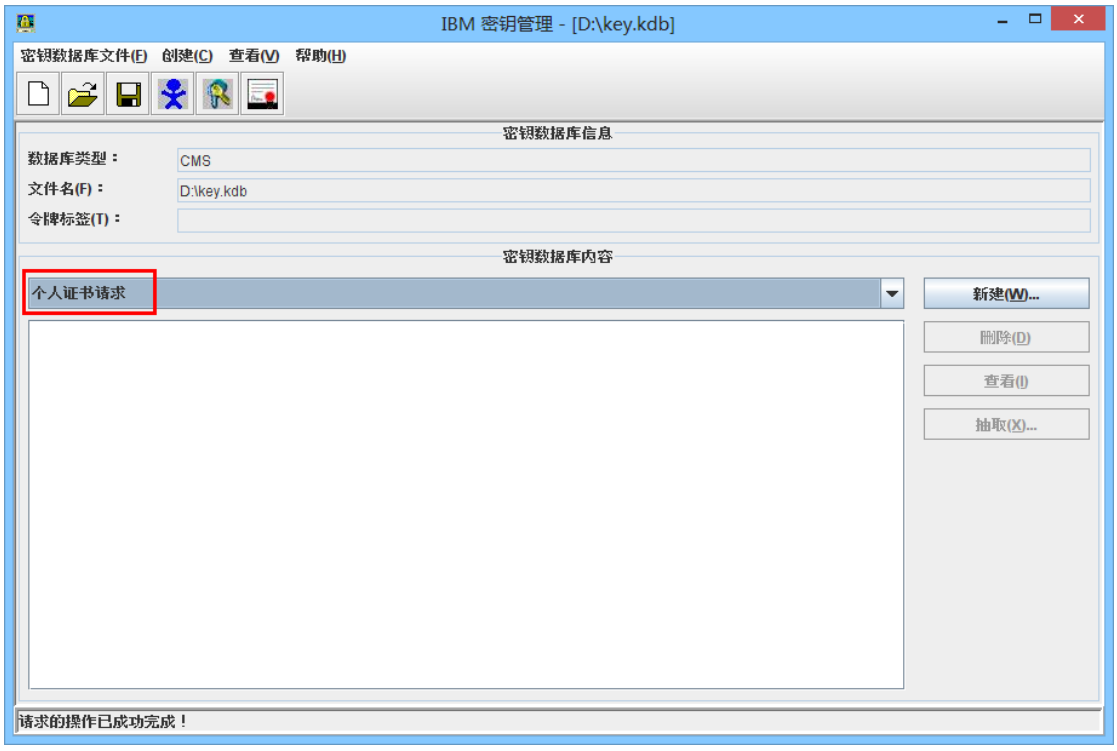
2、选择“密钥数据库文件——新建”，弹出以下对话框。

3、在密钥数据库类型中选择“CMS”。点击“浏览”选择密钥数据库文件所

在路径，默认情况下应该在执行 ikeyman 的 bin 目录下。点击确定进入如下界面：



4、输入密钥数据库的密码，选择“将密码存储到文件中”点击“确定”进入如下界面，同时生成密码存储文件“key.sth”。该密码存储文件必须和密码数据库文件放在同一目录下。



5、切换到“个人证书请求”，选择界面上方的“创建——新建证书请求”进入如下界面。其中：

密钥大小必须为 2048；

公用名（CN），即证书申请表中的域名；

组织（O），即机构身份证件中机构名称全称；

组织单元（OU），即证书申请表中申请人的部门名称；

市、县、区（L），即机构身份证件中机构所在市级地区；

省、直辖市（ST），即机构身份证件中机构所在省级地区；

国家或地区（C），输入机构身份证件中机构所在的国家或者行政区，限定两位字母，如中国输入 CN，美国输入 US 等。

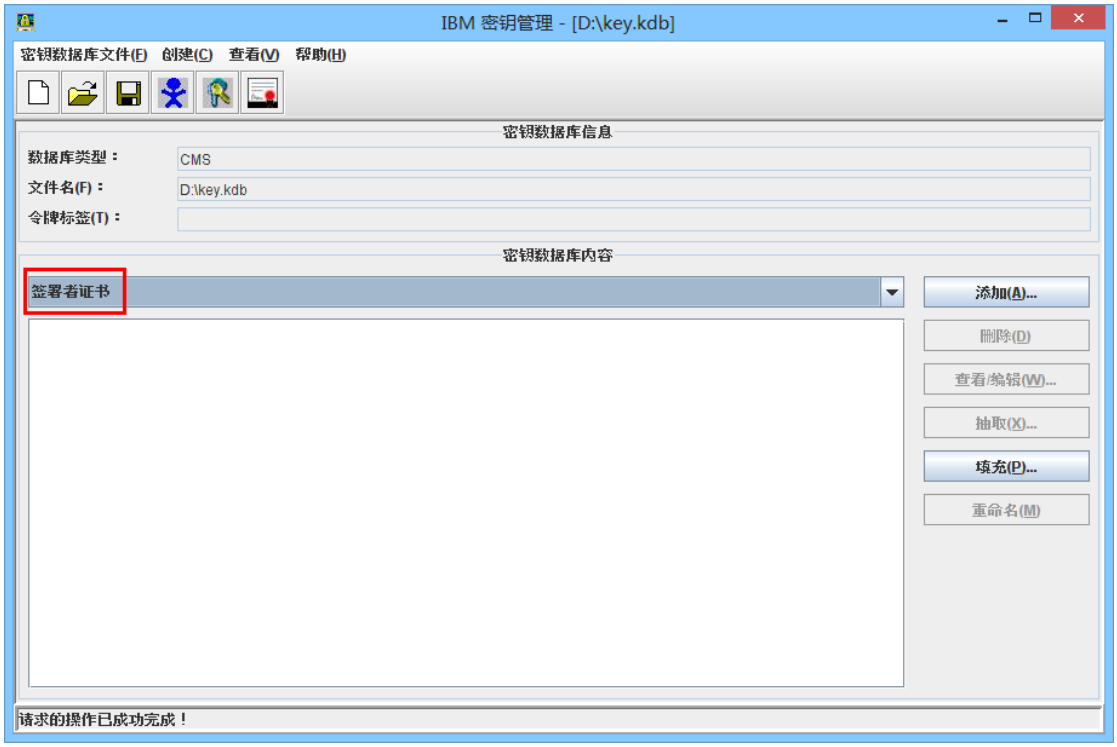
6、点击确定后，即在该路径下生成证书请求文件 certreq.arm。证书申请机构将证书请求文件提供给 CFCA，并妥善保管证书文件（key.kdb）和证书密码文件（key.sth）。

7、CFCA 审核订户资料后，将公钥证书和证书链反馈给订户。

8、证书申请机构将收到的公钥证书和证书链装回到证书文件（key.kdb）中。

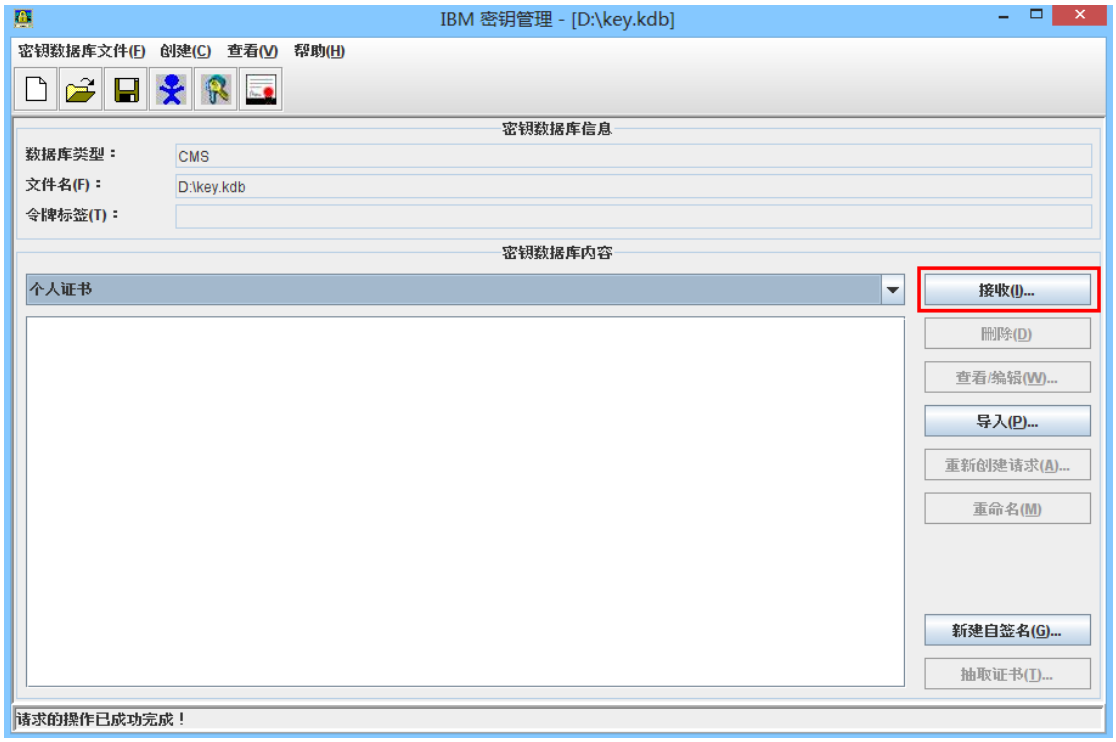
其中，证书文件一般以申请单位全称命名；EV SSL 证书、EV 多域名 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是 CFCA_EV_OCA.cer；OV SSL 证书、OV 多域名 SSL 证书、OV 通配符 SSL 证书的根证书是 CFCA_EV_CA.cer；中级证书是 CFCA_OV_OCA.cer。

9、选择“签署人证书”，进入如下界面。

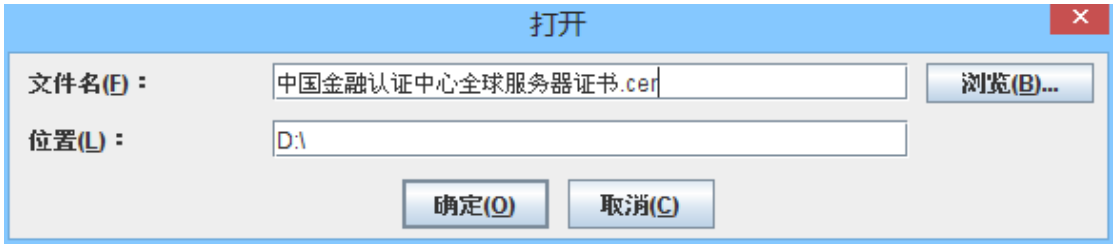


10、选择“添加”，弹出选择证书对话框，选择根证书，点击确定，导入完成。同样，将中级证书也导入到 key.kdb 中。

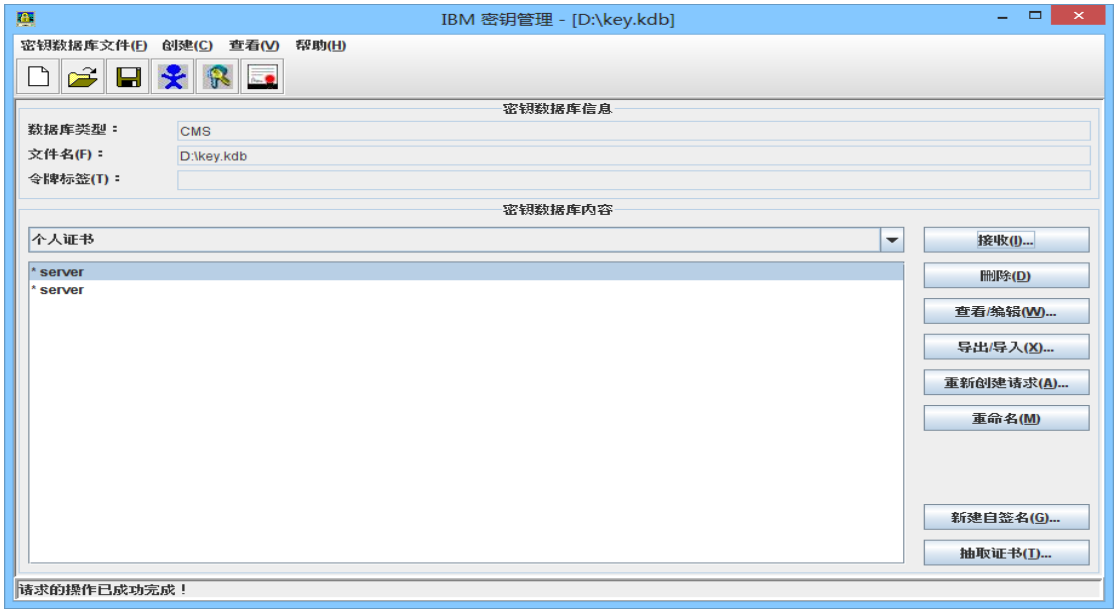
11、在密钥数据库中选择“个人证书”，进入下面的界面。



14、点击“接收”，弹出如下对话框。



15、选择服务器证书公钥文件，点击“确定”，导入完成。



3.5 证书格式转换

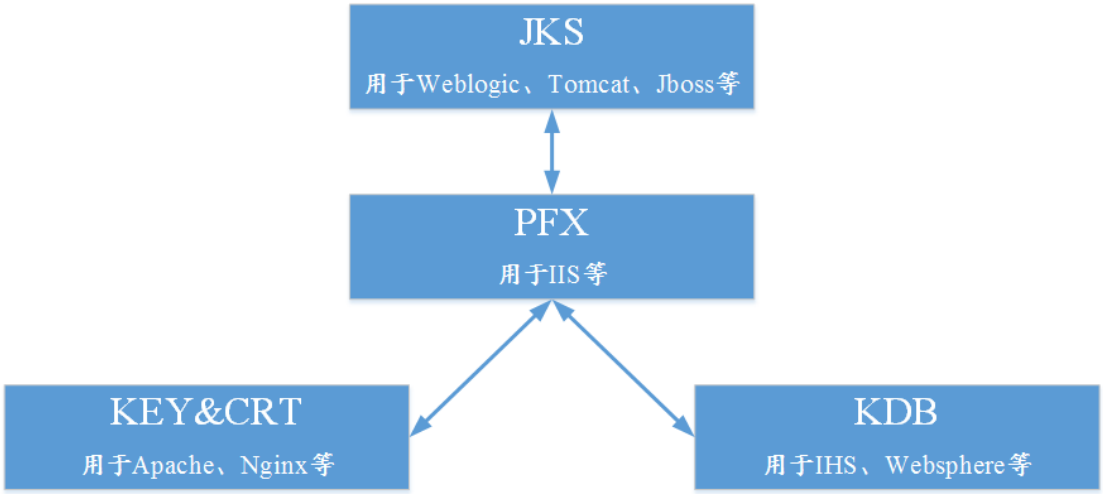
Tomcat、Weblogic、JBoss 等，使用 Java Keystore（JKS）格式的证书文件；

Apache、Nginx 等，使用 KEY、CRT 格式的证书文件；

IBM Websphere、IBM Http Server 等，使用 KDB 格式的证书文件；

IIS 等，使用 PFX（P12）格式的证书文件；

JKS、KEY&CRT、KDB、PFX 等格式的证书文件可以相互转换。如下图所示：



3.5.1 JKS 转换为 PFX

可以使用 Keytool 工具，将 JKS 格式转换为 PFX 格式。

keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -srcstoretype JKS -deststoretype PKCS12

3.5.2 PFX 转换为 JKS

可以使用 Keytool 工具，将 PFX 格式转换为 JKS 格式。

keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks -srcstoretype PKCS12 -deststoretype JKS

3.5.3 KEY&CRT 转换为 PFX

使用 OpenSSL 工具，可以将密钥文件 KEY 和公钥文件 CRT 转化为 PFX 文件。

将密钥文件 KEY 和公钥文件 CRT 放到 OpenSSL 目录下，打开 OpenSSL 执行以下命令：

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt

3.5.4 PFX 转换为 KEY&CRT

使用 OpenSSL 工具，可以将 PFX 文件转化为密钥文件 KEY 和公钥文件 CRT。

将 PFX 文件放到 OpenSSL 目录下，打开 OpenSSL 执行以下命令：

openssl pkcs12 -in server.pfx -nodes -out server.pem

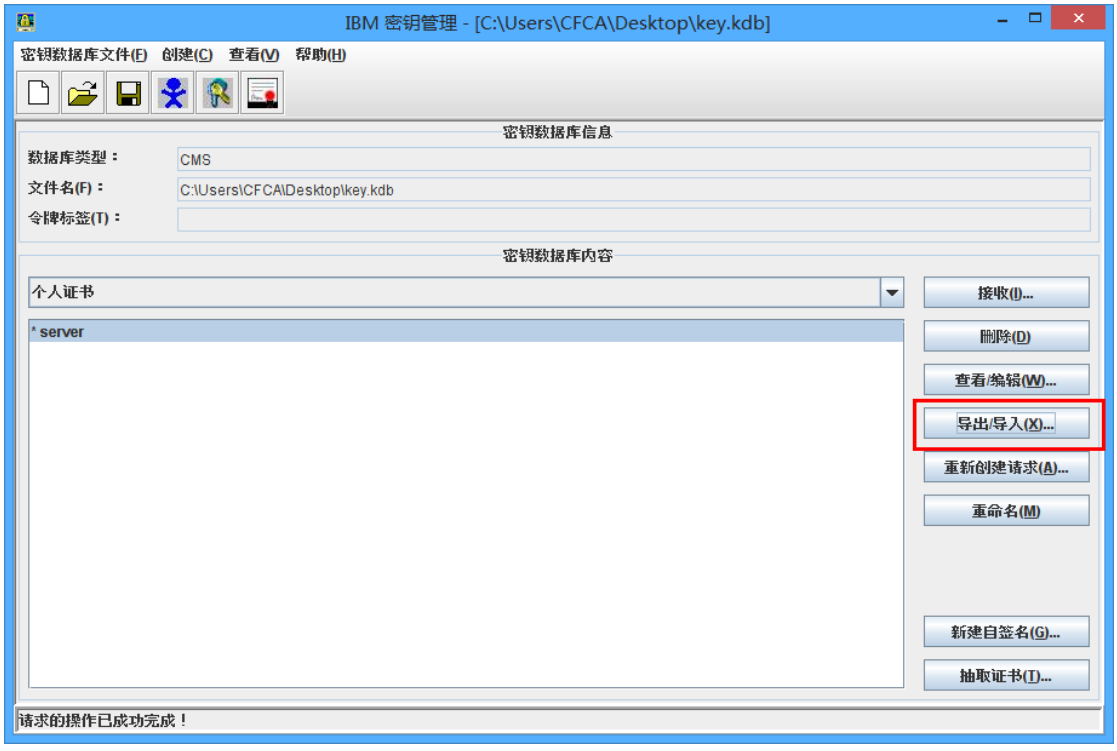
openssl rsa -in server.pem -out server.key

openssl x509 -in server.pem -out server.crt

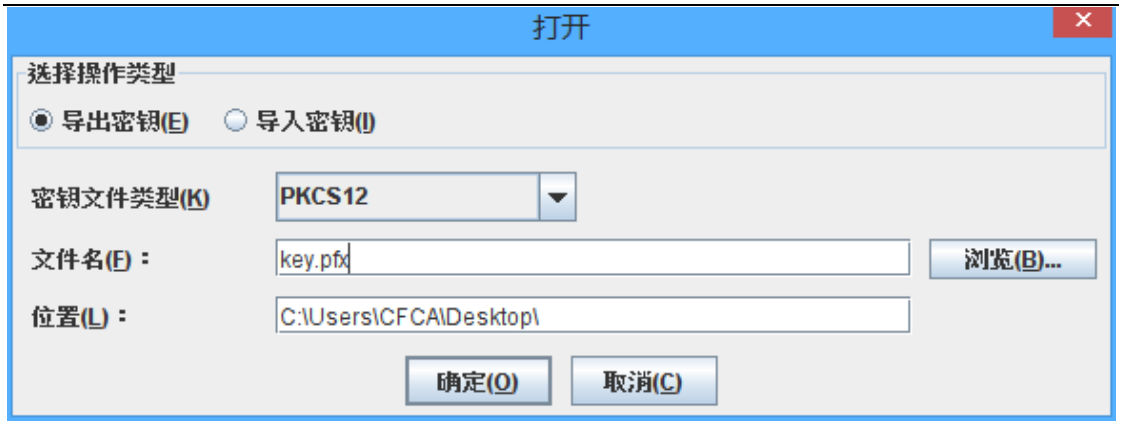
3.5.5 KDB 转换为 PFX

使用 iKeyman 工具，可以将 KDB 文件转化为 PFX 文件。

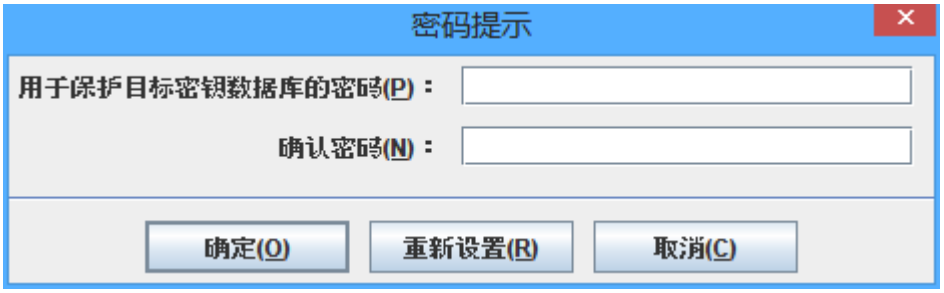
打开 KDB 文件，点击“导出”按钮。



选择“导出密钥”，选择 PKCS12 格式。



设置 PFX 密码。

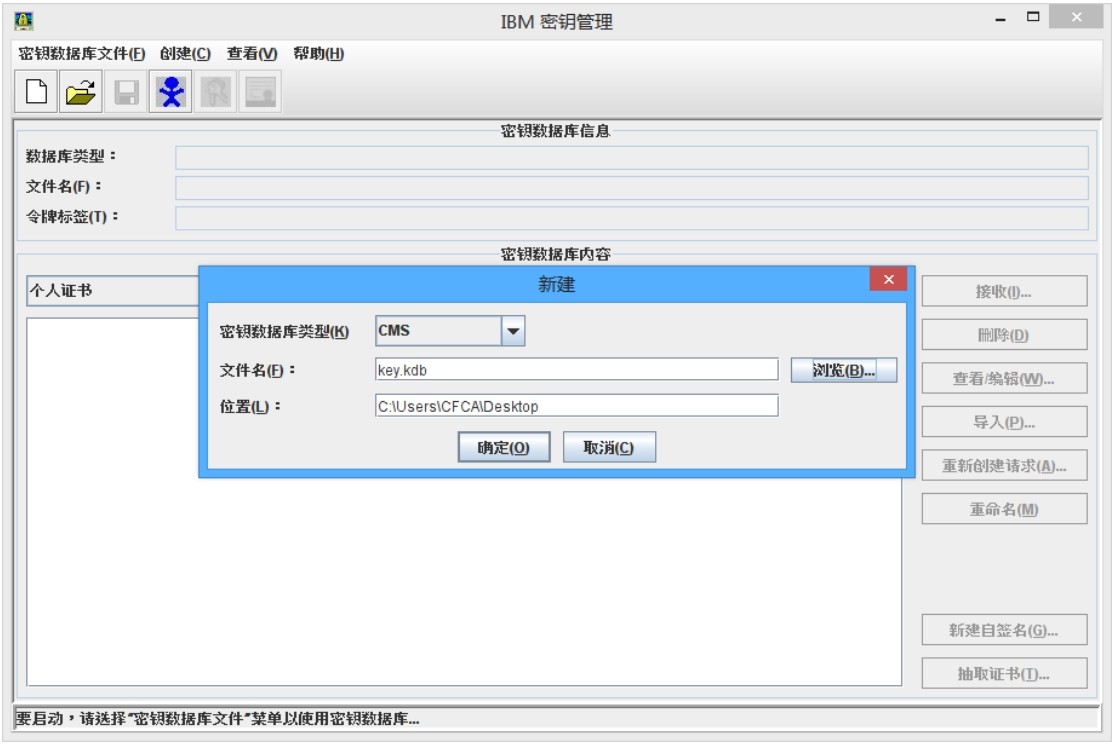


即可导出 PFX 文件。

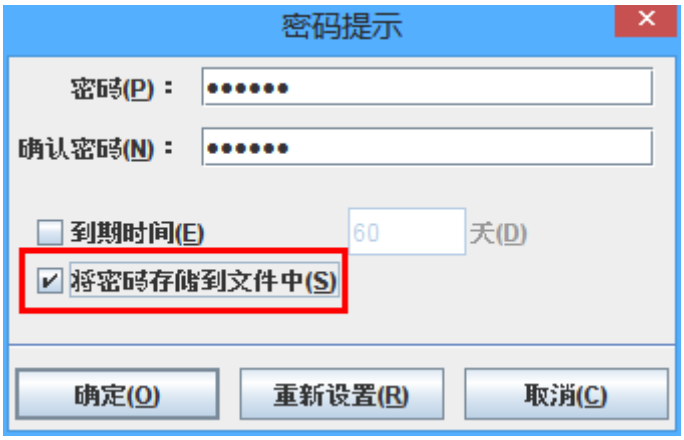
3.5.6 PFX 转换为 KDB

使用 iKeyman 工具，可以将 PFX 文件转化为 KDB 文件。

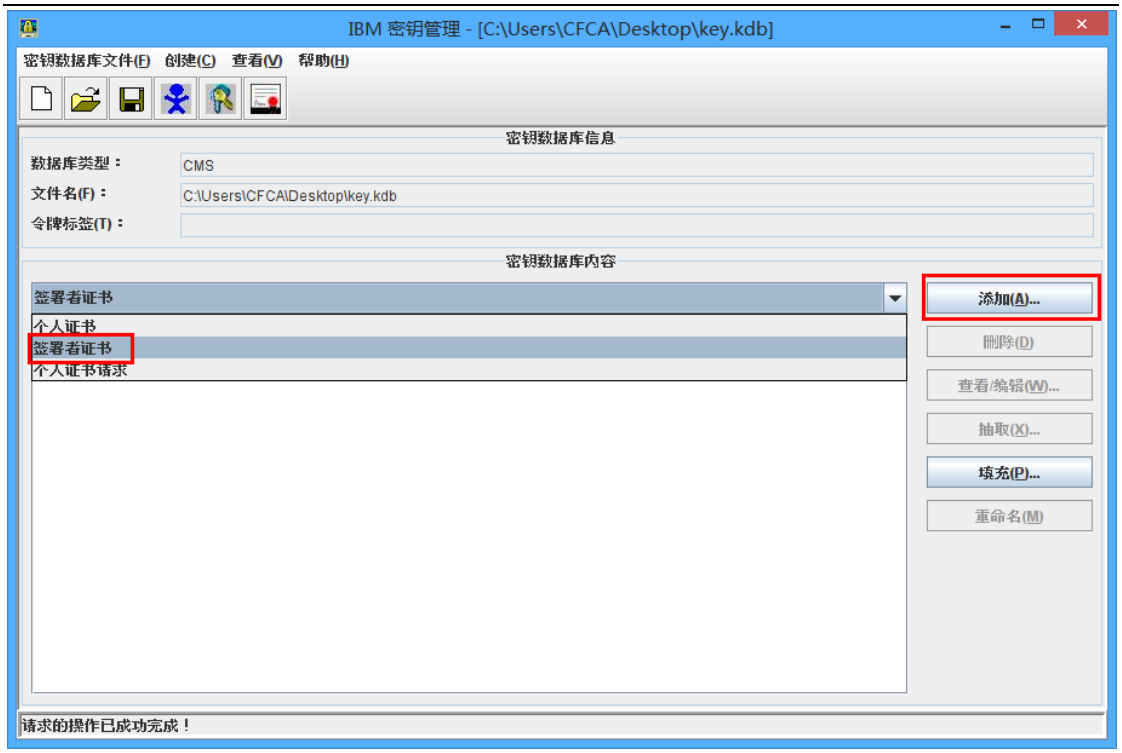
打开 iKeyman，新建一个 KDB 文件。



输入密码，可将密码存储到文件中。

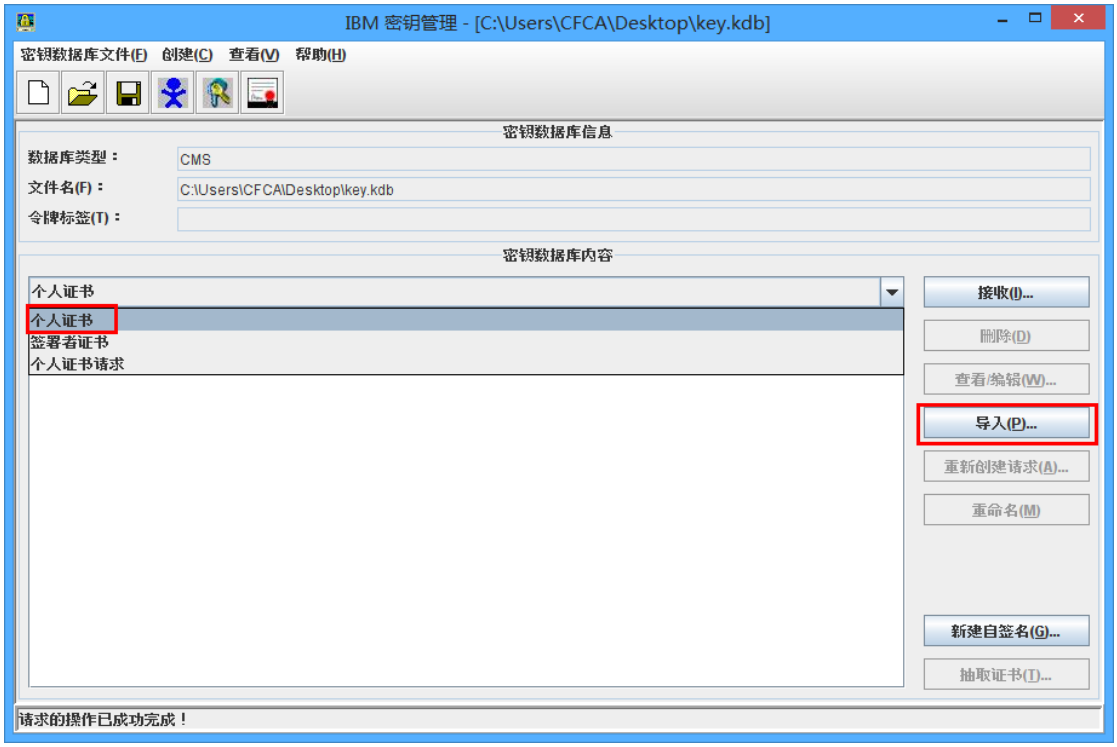


选择签署者证书，点击“添加”按钮。

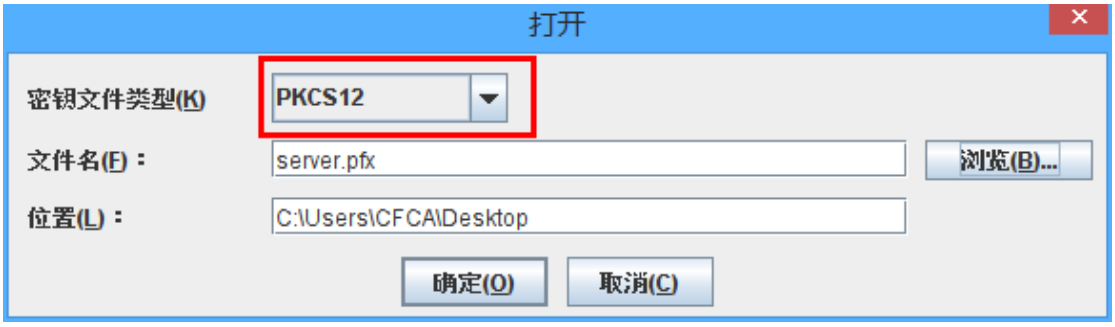


依次将根证书和中级证书导入。

选择个人证书，点击“导入”按钮。



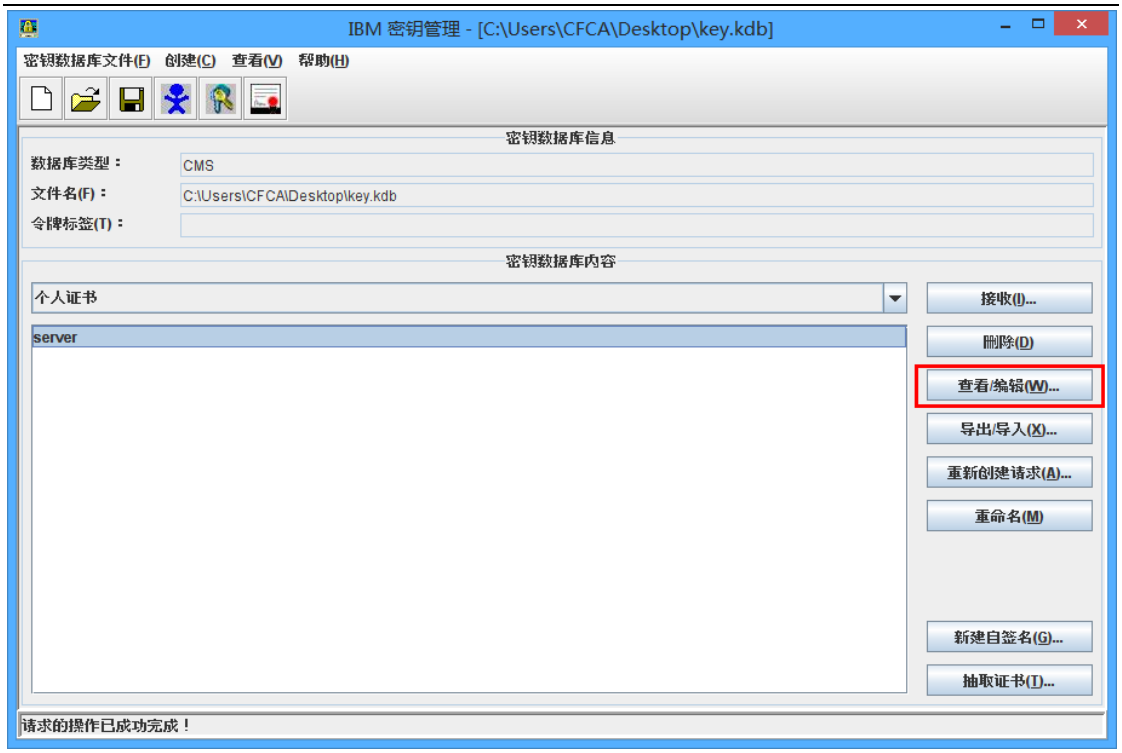
选择 PKCS12 类型，选择 PFX 文件。



输入 PFX 密码。

输入标签名称。

导入成功后，查看个人证书。



证书信息中，勾选“将此证书设置为缺省证书”。

而后保存 KDB 文件即可。

3.6 证书部署

证书部署方式，请优先咨询提供 Web 应用软件的软件或者硬件厂商，本章节也提供了部分 Web 应用软件部署证书的方式，仅供参考。

3.6.1 Apache 证书配置

Apache 使用 KEY 和 CRT 格式的证书，证书制作方式请参考“3.4 使用 OpenSSL 工具制作证书”。

将中级证书和根证书打开，依次将其代码复制到文本文件中（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），并保存成 cfca.crt。如下：

```
-----BEGIN CERTIFICATE-----
中级证书编码
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
根证书编码
-----END CERTIFICATE-----
```

将服务器证书文件 server.key 和 server.crt，以及证书链文件 cfca.crt，配置在 Apache 中。

用文本编辑器打开 Apache 根目录下的 conf/httpd.conf 文件，去掉下述两行的注释符号#。

#LoadModule ssl_module modules/mod_ssl.so

#Include conf/extra/httpd-ssl.conf

用文本编辑器打开 Apache 根目录下的 conf/extra/httpd-ssl.conf 文件，修改以下内容：

```
<VirtualHost 127.0.0.1:443>
    DocumentRoot "/var/www/html"
    ServerName
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3
    SSLCertificateFile server.crt 路径
    SSLCertificateKeyFile server.key 路径
    SSLCertificateChainFile cfca.crt 路径
</VirtualHost>
```

其中：

启用 SSL 功能：SSLEngine on

禁用 SSLv2、SSLv3 协议：SSLProtocol all -SSLv2 -SSLv3

公钥文件：SSLCertificateFile server.crt 路径

私钥文件：SSLCertificateKeyFile server.key 路径

证书链文件：SSLCertificateChainFile cfca.crt 路径

上述设置完成过后，重新启动 Apache。

3.6.2 Tomcat 证书配置

Tomcat 使用 JKS 格式的证书，证书制作方式请参考“3.3 使用 Keytool 工具制作证书”。

将服务器证书文件（server.jks），配置在 Tomcat 中。

文本编辑器打开 Tomcat 安装目录下 conf 目录中的 server.xml 文件，更新以下内容。

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="jks 路径"
    keystorePass="jks 密码"
    truststoreFile="jks 路径"
    truststorePass="jks 密码" />
```

其中：

SSL 访问端口：port="443"

禁用 SSLv2、SSLv3 协议：sslProtocol="TLS"

证书文件：keystoreFile="jks 路径"

证书密码：keystorePass="jks 密码"

信任证书链文件：truststoreFile="jks 路径"

信任证书链密码：truststorePass="jks 密码"

配置完成后，重新启动 Tomcat。

3.6.3 Nginx 证书配置

Nginx 使用 KEY 和 CRT 格式的证书，证书制作方式请参考“3.4 使用 OpenSSL

工具制作证书”。

将服务器证书、中级证书和根证书打开，依次将其代码复制到文本文件中（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），并保存成 server.crt。如下：

```
-----BEGIN CERTIFICATE-----
服务器证书编码
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
中级证书编码
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
根证书编码
-----END CERTIFICATE-----
```

将服务器证书文件 server.key 和 server.crt，配置在 Nginx 中。

如果是单向 SSL，用文本编辑器打开 Nginx 根目录下 conf/nginx.conf 文件，更新以下内容：

```
server {
    listen 443;
    server_name 127.0.0.1;
    ssl on;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate server.crt;
    ssl_certificate_key server.key;
    }
```

其中：

启用 SSL 功能：ssl on

禁用 SSLv2、SSLv3 协议：ssl_protocols TLSv1 TLSv1.1 TLSv1.2

公钥文件：ssl_certificate server.crt 路径

私钥文件：ssl_certificate_key server.key 路径

上述设置完成过后，重新启动 Nginx。

如果是双向 SSL，用文本编辑器打开 Nginx 根目录下 conf/nginx.conf 文件，更新以下内容：

```
server {
    listen 443;
    server_name 127.0.0.1;
    ssl on;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate server.crt;
    ssl_certificate_key server.key;
    ssl_client_certificate ca.crt;
    ssl_verify_client on;
    ssl_verify_depth 2;
    }
```

其中：

启用 SSL 功能：ssl on

禁用 SSLv2、SSLv3 协议：ssl_protocols TLSv1 TLSv1.1 TLSv1.2

公钥文件：ssl_certificate server.crt 路径

私钥文件：ssl_certificate_key server.key 路径

证书链文件：ssl_client_certificate ca.crt 路径

启用双向 SSL：ssl_verify_client on

证书链深度：ssl_verify_depth 2 如果客户端使用 CFCA 证书，则该项必须为 2

上述设置完成过后，重新启动 Nginx。

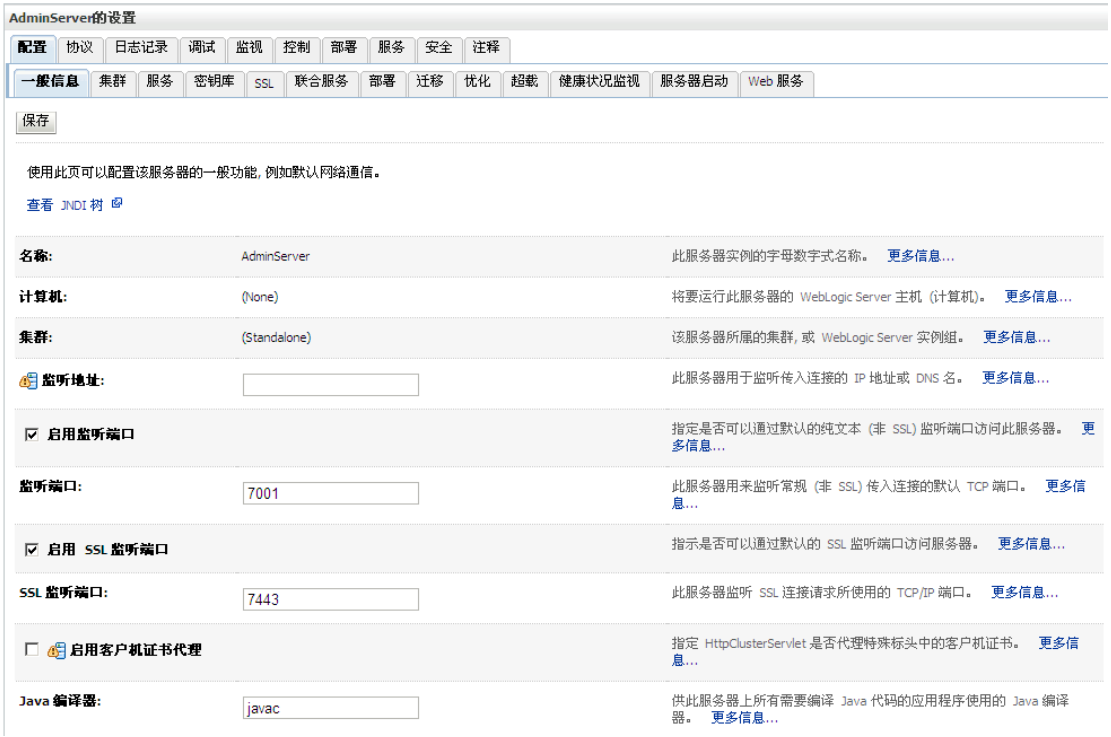
3.6.4 Weblogic 证书配置

Weblogic 使用 JKS 格式的证书，证书制作方式请参考“3.3 使用 Keytool 工具制作证书”。

打开 Weblogic 控制台，进入“服务器”。

选择部署的服务器。

在“一般信息”中，“启用 SSL 监听端口”。



在“密钥库”页面，配置服务器证书（server.jks）。其中：

密钥库选择“定制标识和定制信任”；

密钥库输入 server. jks 的路径和密码；

信任密钥库输入 server. jks 的路径和密码；

输入完成后，保存。

在“SSL”页签，配置 SSL 选项。其中：

标识和信任设置，选择“密钥库”；

私有密钥输入密钥别名和密码；

输入完成后，保存。

配置完成后，激活 Weblogic 更改，重新启动 Weblogic 服务。

3.6.5 IBM Http Server 证书配置

IBM Http Server 使用 KDB 格式的证书，证书制作方式请参考“3.5 使用 iKeyman 工具制作证书”。

将制作好的 kdb、rdb、sth 文件放在同一个目录下，而后在 httpd.conf 文件中配置。

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
    <VirtualHost 127.0.0.1:443>
    ServerName 127.0.0.1
    SSLEnable
    SSLClientAuth required
    Keyfile "key.kdb 路径"
    SSLStashfile "key.sth 路径"
    </VirtualHost>
   SSLDisable
```

其中，KeyFile 所指定的为证书数据库路径，SSLStashfile 为密码文件路径。

配置完成后，重启启动 IBM HTTP Server。

3.6.6 JBoss 证书配置

JBoss 使用 JKS 格式的证书，证书制作方式请参考“3.3 使用 Keytool 工具制作证书”。

将服务器证书文件（server.jks），配置在 JBoss 中。

用文本编辑器打开 Jboss 安装目录下 server/default/deploy/jbossweb.sar 目录中的 server.xml 文件，更新以下内容。

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
    port="443" address="${jboss.bind.address}"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="jks 路径"
    keystorePass="jks 密码"
    truststoreFile="jks 路径"
    truststorePass="jks 密码"
    sslProtocol = "TLS"/>
```

其中：

SSL 访问端口：port="443"

证书文件：keystoreFile="jks 路径"

证书密码：keystorePass="jks 密码"

信任证书链文件：truststoreFile="jks 路径"

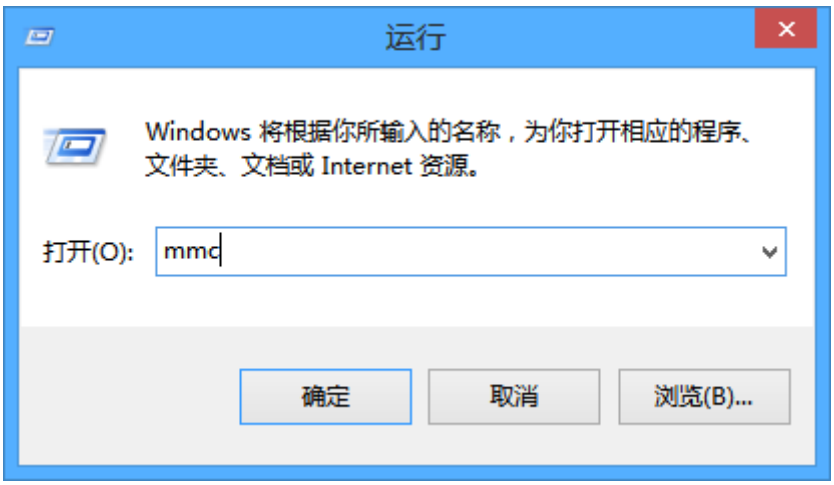
信任证书链密码：truststorePass="jks 密码"

配置完成后，重新启动 JBoss。

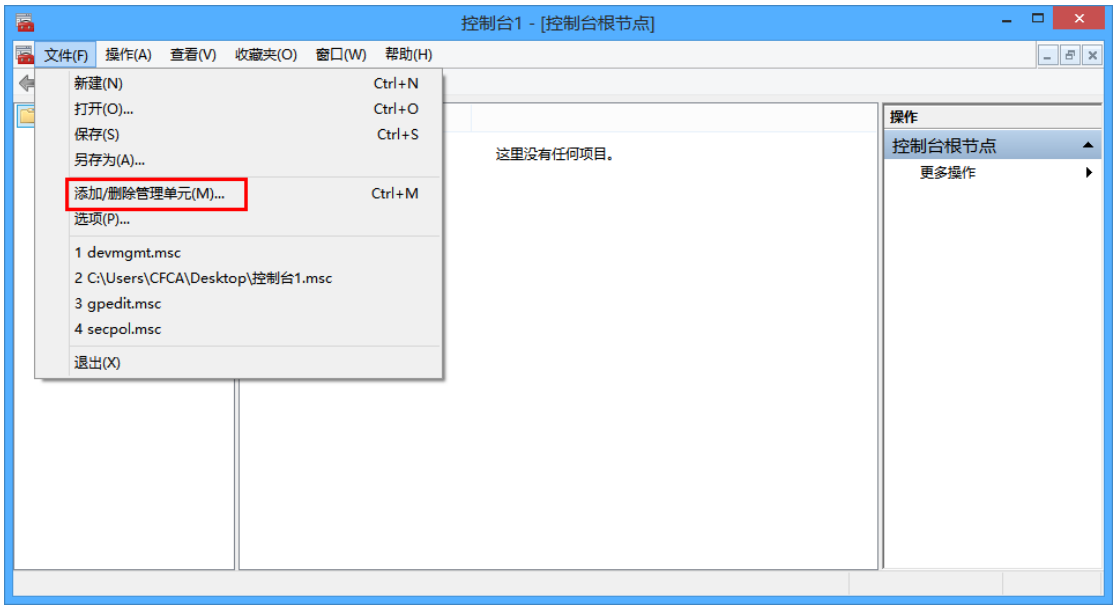
3.6.7 IIS 证书配置

IIS 可以直接使用 PFX 格式的证书文件，PFX 证书制作方式请参考“3.6 证书格式转换”。

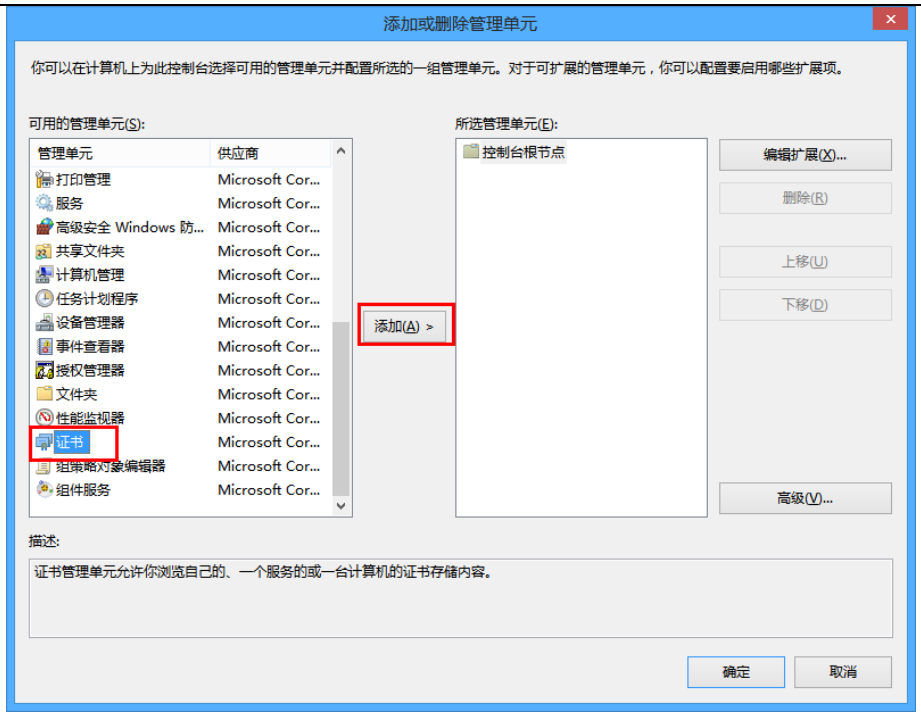
在运行框中输入 MMC，进入管理控制台。



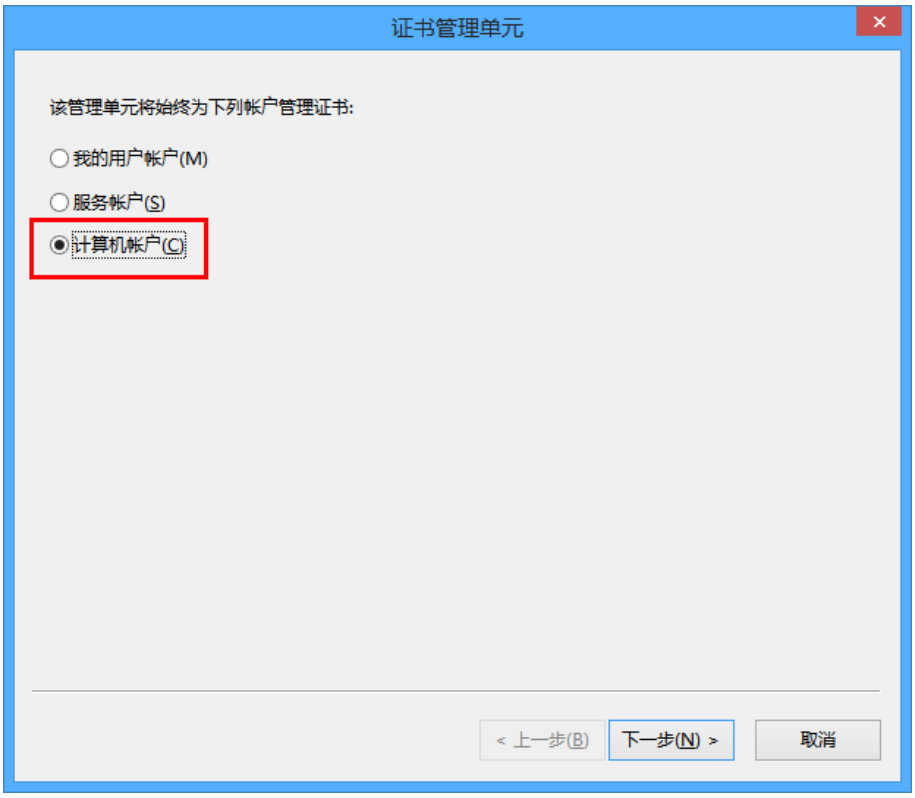
添加删除管理单元。



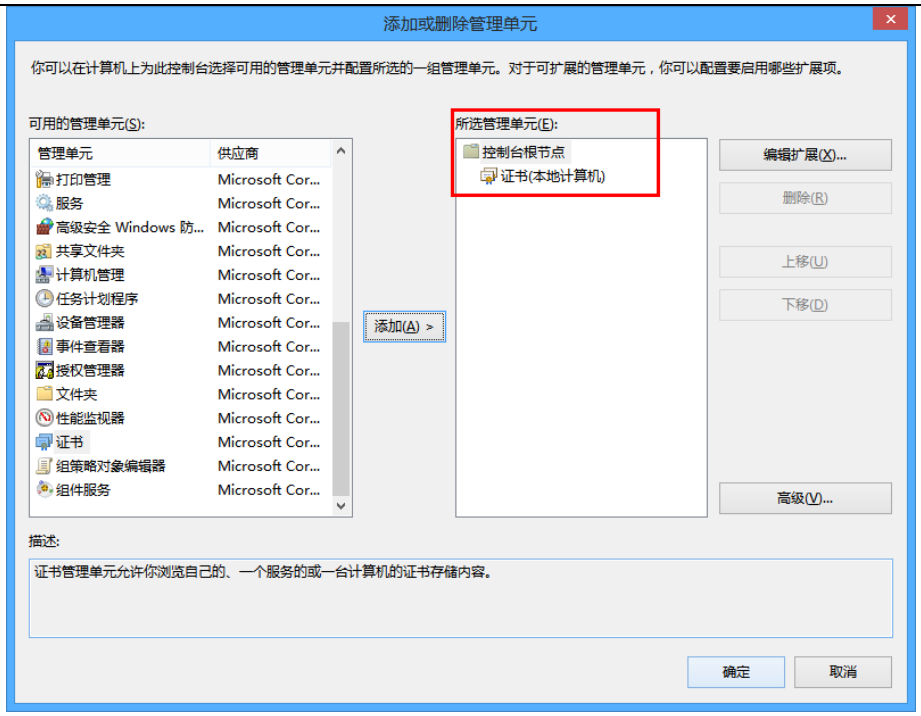
添加证书。



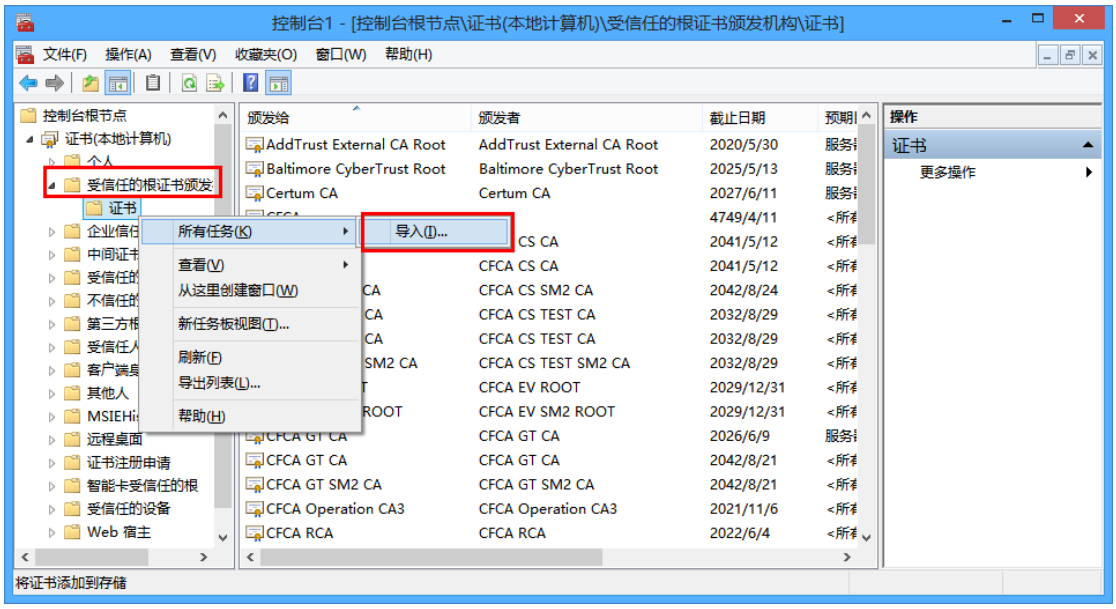
选择计算机账户。



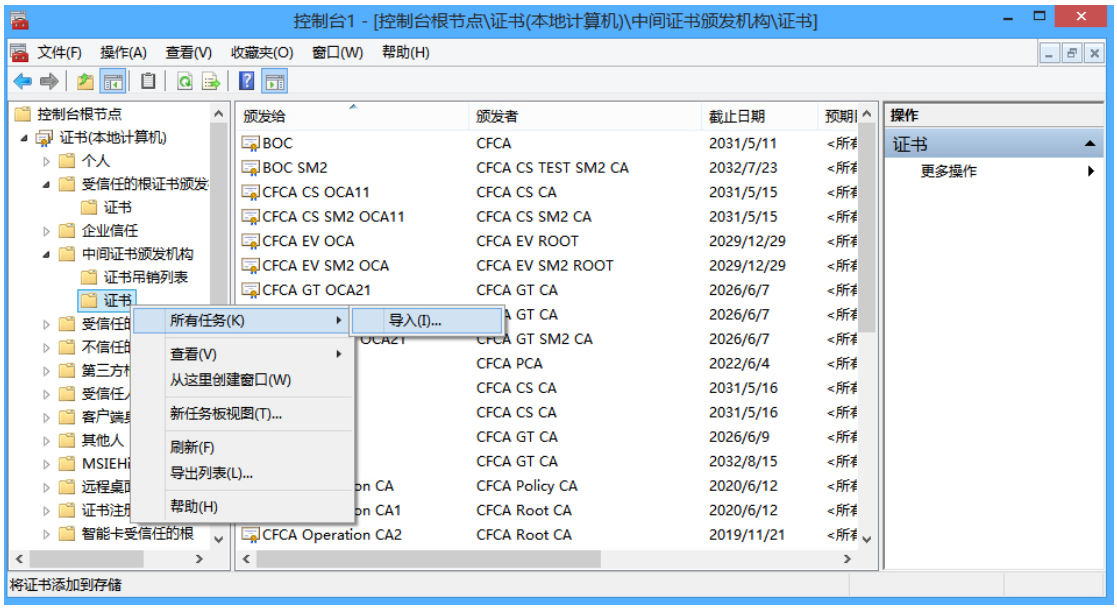
添加之后，确定。



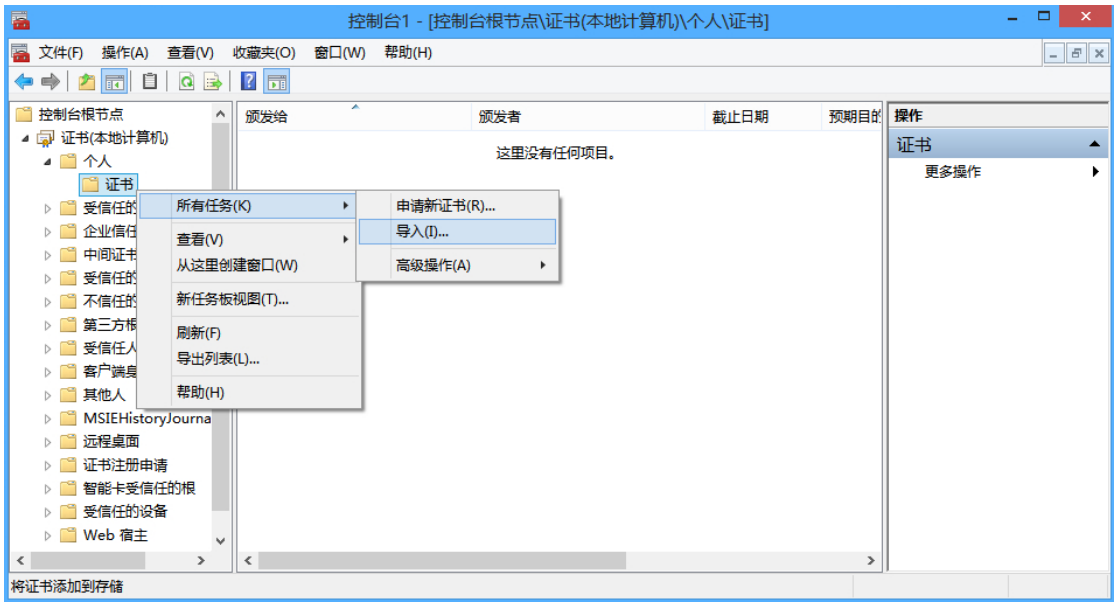
在受信任的根证书颁发机构中，导入根证书。



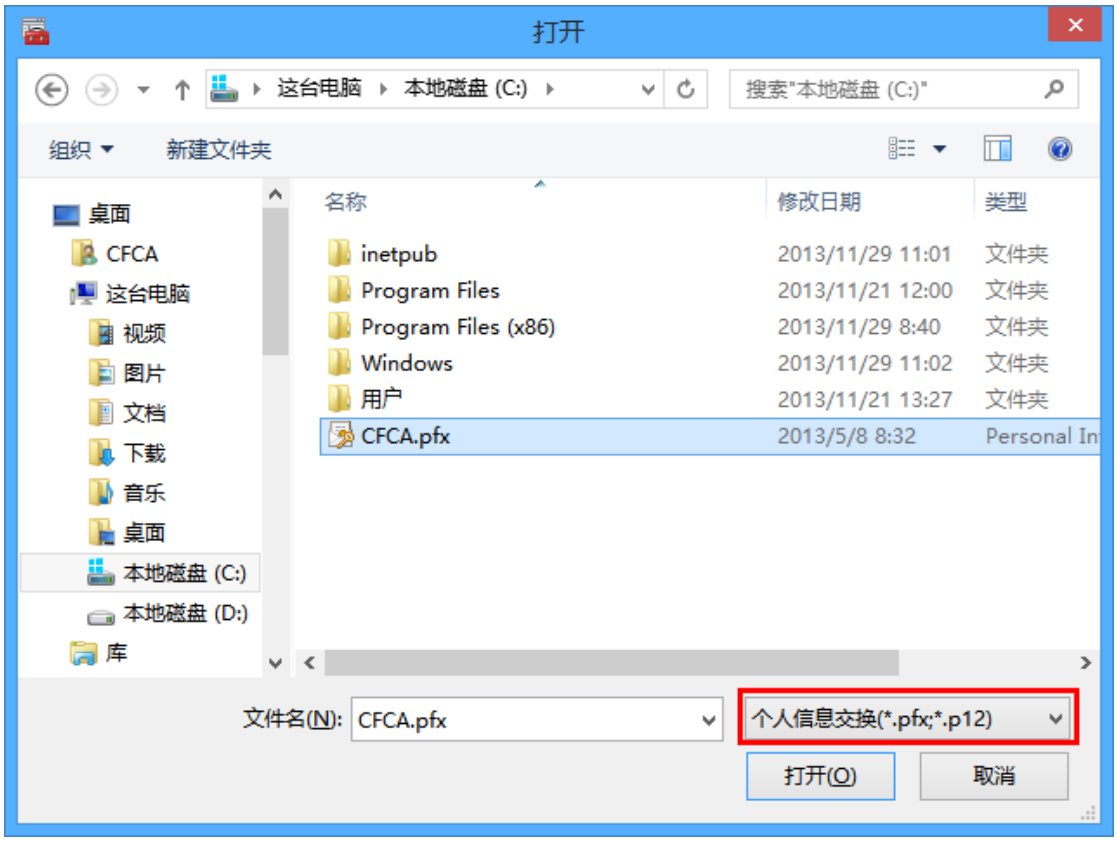
在中级证书颁发机构中，导入中级证书。



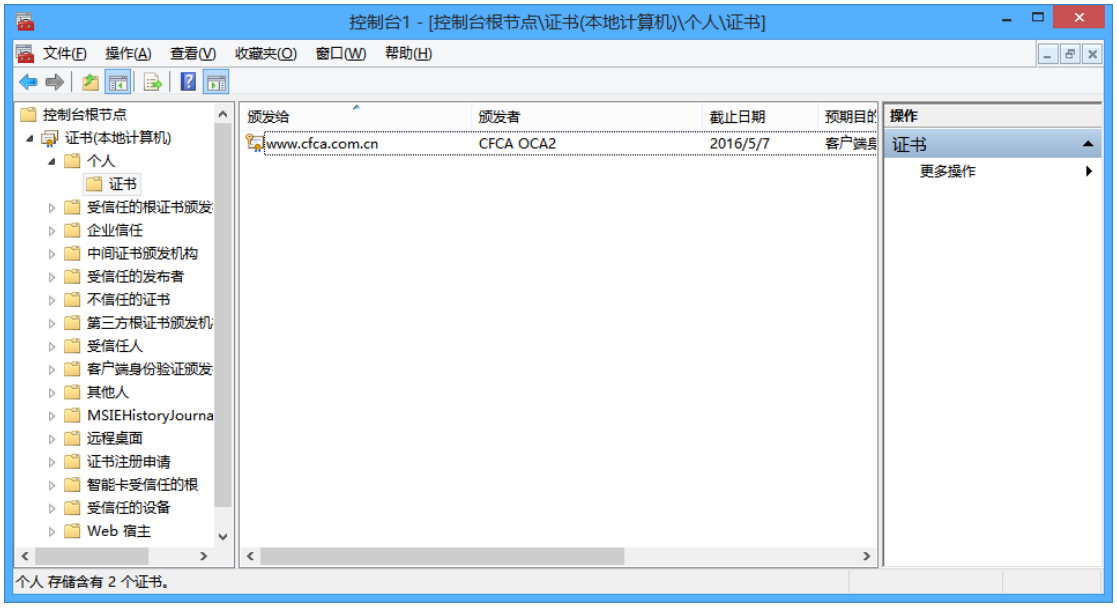
在个人证书中，导入 PFX 证书文件。



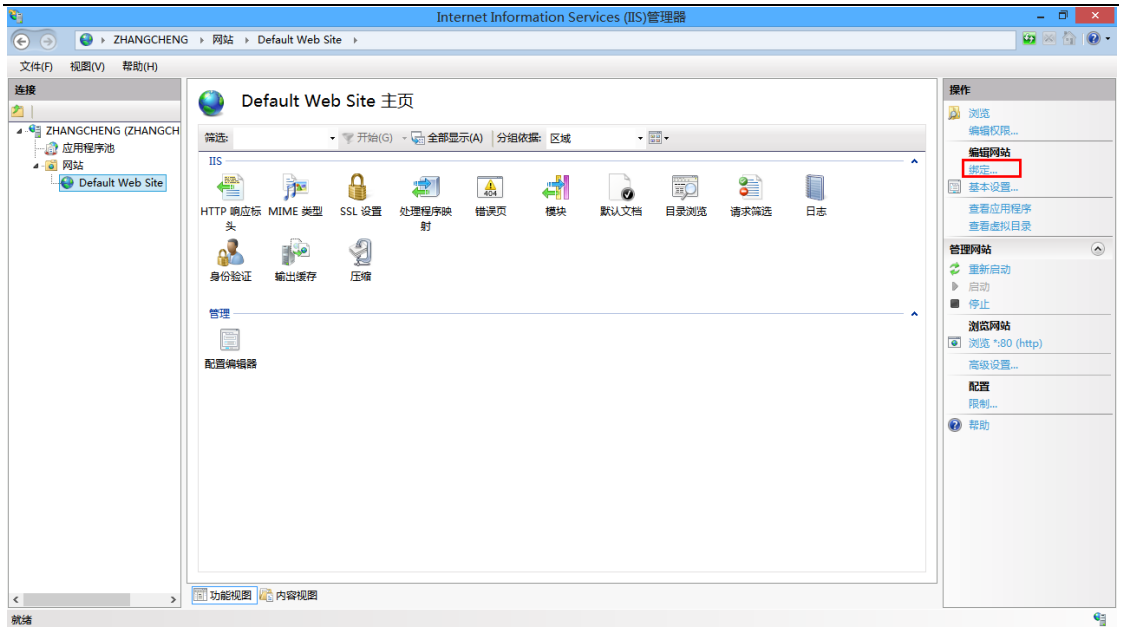
导入时，选择个人信息交换（PFX、P12）。



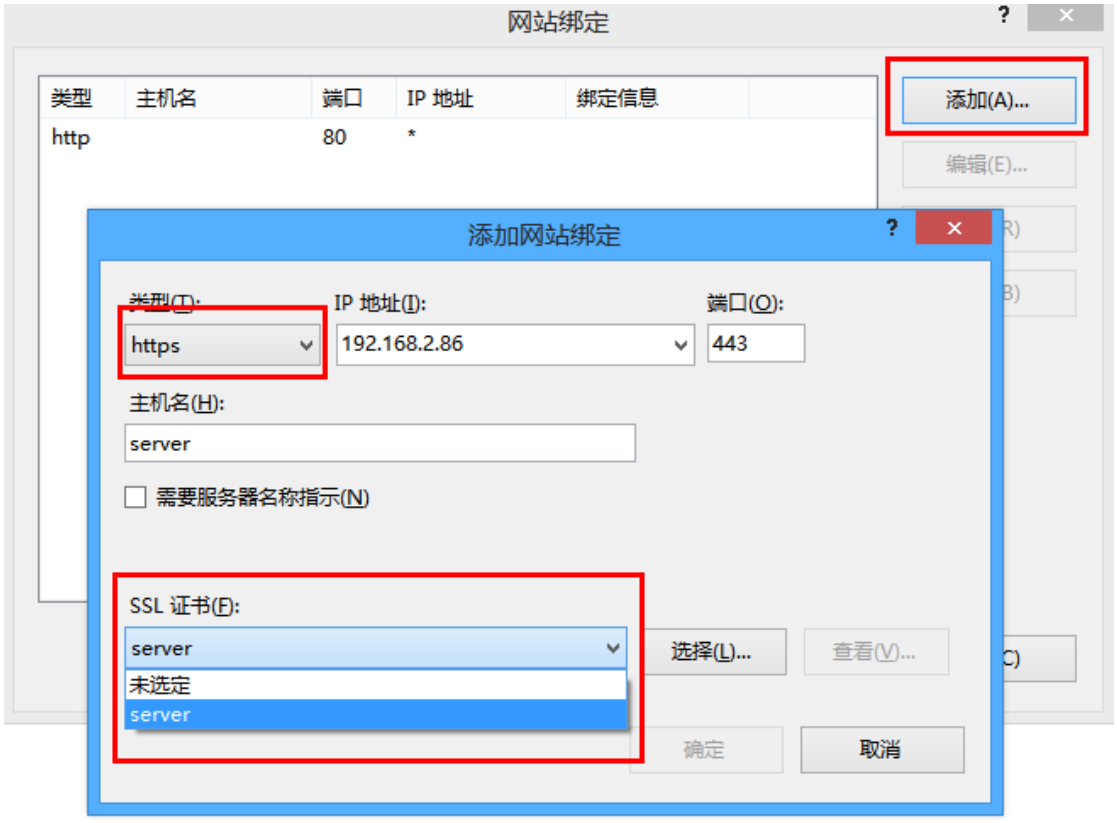
导入完成。



在 IIS 管理控制台，选择站点，点击“绑定”。



点击“添加”，选择“https”，选择 SSL 证书，点击确定。



重新启动 IIS 即可。

附录一、CFCA 全球信任证书（SSL 证书）申请表

CFCA 全球信任体系证书申请表							
证书申请信息	申请日期		证书数量		证书期限		
	业务类型	☐新申请 ☐更新 ☐吊销					
	证书类型（单选）	OV证书	☐单域名OV服务器证书	☐OV代码签名证书			
			☐多域名OV服务器证书	☐通配符OV服务器证书			
		EV证书	☐单域名EV服务器证书	☐EV代码签名证书			
			☐多域名EV服务器证书				
		文档签名	☐个人普通文档签名证书	☐企业/机构普通文档签名证书			
			☐个人高级文档签名证书	☐企业/机构高级文档签名证书			
	站点认证	☐站点认证 （申请服务器证书选填）					
	域名	（申请服务器证书需填）					
	证书存储介质	☐用户自备，设备名称与型号： ☐CFCA提供 （申请EV代码签名证书与高级文档签名证书需填）					
个人证书信息区（申请个人证书时填写）							
申请人信息	姓名(中文)			姓名(拼音)			
	证件类型	☐身份证 ☐护照					
	证件号码						
	联系电话		传真		电子邮件		
	联系地址					邮政编码	
	公司名称					公司审批人	
	审批人邮箱					审批人电话	
企业/机构信息区（申请企业/机构证书时填写）							
申请机构信息	机构名称（中文）						
	机构证件类型	☐企业营业执照 ☐组织机构代码证 ☐其它，请注明：					
	证件颁发机构						
	机构证件号码					联系电话	
	联系地址					邮政编码	
申请机构审批人	姓名				职务		
	联系电话				电子邮件		
	签名						
经办人1	姓名		职务		电子邮件		
	证件类型		证件号			联系电话	
经办人2	姓名		职务		电子邮件		
	证件类型		证件号			联系电话	
人力资源负责人		姓名				联系电话	
申请声明	本人/机构承诺以上信息资料真实、有效。本机构已认真阅读并同意遵守中金金融认证中心有限公司（CFCA）网站（http://www.cfca.com.cn)发布的《数字证书服务协议》、《全球信任体系电子认证业务规则（CPS））》中规定的相关义务。						
	申请人签字/申请机构盖章					日期	
	备注						

CFCA Global-Trust Certificate Application Form							
Certificate Application Information	Application Date			Unit		Period	
	Application Type	☐New Application ☐ Renewal ☐ Revocation					
	Certificate Type	OV	☐Single-Domain OV SSL		☐OV CodeSign		
			☐Mutli-Domain OV SSL		☐Wildcard OV SSL		
		EV	☐Single-Domain EV SSL		☐EV CodeSign		
			☐Mutli-Domain EV SSL				
		Document	☐Personal standard		☐Organization standard		
			☐Personal Advanced		☐Organization Advanced		
	Site Auth	☐Site Auth Addition （SSL Certificate required）					
	Domain Name	（SSL Certificate required）					
	Hardware Device	☐Subscriber provide Device ☐CFCA provide device (EV CodeSign and Document Signing Required)					
Personal Certificate Information（Applicable for personal certificate application）							
Applicant Information	Name						
	Credential type	☐ID Card ☐Passport					
	Credential Num.						
	Telephone		Fax		E-mail		
	Address					Postcode	
	Company name					Approver	
	Approver E-mail					Approver Telephone	
Organization Certificate Information（Applicable for Organization certificate application）							
Organization Information	Legal Name					Abbreviation Name	
	Identity File Name	☐Business License ☐Organization code Certificate ☐others，please note:					
	Registration Authority						
	Registration Number					Telephone	
	Address					Postcode	
Higher Authority Information	Name				Title		
	Telephone				E-mail		
	Seal/Signature						
No.1 Contact Information	Name		Title		E-mail		
	Credential type		Number			Telephone	
No.2 Contact Information	Name		Title		E-mail		
	Credential type		Number			Telephone	
HR Information		Name				Telephone	
Applicant Statement	I commit that the above information is true and effective. I have read and agreed to the related obligations of the "Digital Certificate Services Agreement" and "CFCA's Certification Practice Statement (CPS))" published on CFCA website (www.cfca.com.cn).						
	Signature / Seal					Date	
	Remark						

"注①： 个人证书

申请个人证书时，此表经申请人签名后方可有效。申请人须同时提供身份证件复印件。单位中的个人需提供加盖公章的单位授权证明。"

"注②： 企业、机构证书（包括文档签名，OV 证书）

1、申请机构须同时提供机构证件复印件、经办人身份证件复印件、机构授

予经办人的授权书原件，以上资料均需加盖公章

2、申请机构在正式申请前须与 CFCA 技术人员进行充分沟通，确认该证书能够满足本机构需求。此申请表一经申请机构盖章确认后，就表明其申请的全球信任体系已满足本机构的需求。

3、文档签名证书和 OV 证书申请中，经办人即为申请人本人，只需填写 1 人。"

"注③：企业、机构证书（EV 证书）

1、申请机构须同时提供机构证件复印件、经办人身份证件复印件、机构授予经办人的授权书原件，以上需加盖公章。同时需要提供律师函及律师证。

2、经办人需两人，且第一人应为部门领导，第二人可为普通员工，两者之间应有授权关系，订户申请中共需要以下角色：证书负责人，证书申请人，合同签署人，申请代表人（可选，仅适用于申请者是 CFCA 附属机构或关联方时）这几个角色，需由至少 2 人担任（可由经办人或者负责人担任），且至少有一人应为部门领导，一个人可以担任多个角色。 "

附录二、CFCA 全球信任根证书获取方式

Windows Vista、Windows 7

Windows Vista 以及更高版本的操作系统，Windows 通过根证书自动更新机制分发 CFCA 全球信任根证书。即，用户访问含有 CFCA 全球信任证书的网站、读取含有 CFCA 全球信任证书的安全电子邮件、执行含有 CFCA 全球信任证书代码签名的 ActiveX 控件及可执行程序时，Windows 证书链验证程序访问 Microsoft 根证书信任列表，自动下载 CFCA 全球信任根证书，并将其安装在用户 Windows 受信任根证书颁发机构存储区。整个过程自动完成，用户不会看到任何安全性对话框或警告。有关 Windows Vista、Windows 7 根证书更新的详细技术信息，请访问以下网站：

http://technet.microsoft.com/en-us/library/cc749331(WS.10).aspx

Windows XP

Windows XP 含有更新根证书组件（控制面板——添加或删除程序——添加/删除 Windows 组件），当用户访问含有 CFCA 全球信任证书的网站、读取含有 CFCA 全球信任证书的安全电子邮件、执行含有 CFCA 全球信任证书代码签名的 ActiveX 控件及可执行程序时，更新根证书组件将联系的微软 Windows Update 站点检查根证书信任列表，自动下载 CFCA 全球信任根证书，并将其安装在用户 Windows 受信任根证书颁发机构存储区。有关 Windows XP 根证书更新的详细技术信息，请访问以下网站：

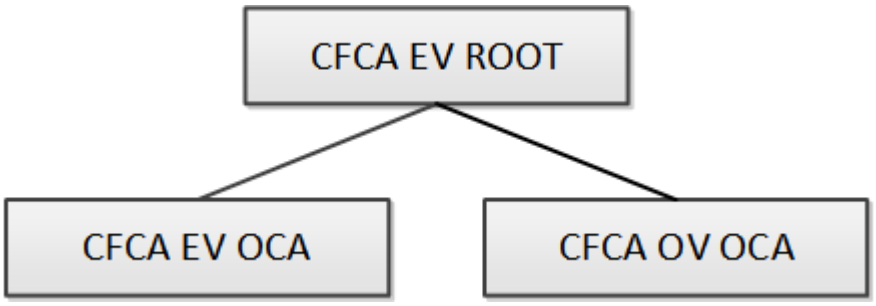
http://technet.microsoft.com/en-us/library/bb457160.aspx

Firefox 浏览器

CFCA EV 根证书已经内置在 Firefox 浏览器中，包括 Windows、Linux、Mac OS X、Andriod 等平台。用户升级到 Firefox v38.0 及以上版本，即可获取 CFCA EV 根证书。

附录三、CFCA 全球信任证书链

CFCA 全球服务器证书体系如下：



主题：CN = CFCA EV ROOT

O = China Financial Certification Authority

C = CN

序列号：18 4a cc d6

有效期：2012 年 8 月 8 日 11:07:01——2029 年 12 月 31 日 11:07:01

摘要算法：SHA256

密钥长度：RSA（4096Bits）

-----BEGIN CERTIFICATE-----

MIIFjTCCA3WgAwIBAgIEGErM1jANBgkqhkiG9w0BAQsFADBWMQswCQYDVQQGEwJD

TjEwMC4GA1UECgwnQ2hpbmEgRmluYW5jaWFsIENlcnRpZmljYXRpb24gQXV0aG9y

aXR5MRUwEwYDVQQDDAxDRkNBIEVWIFJPT1QwHhcNMTIwODA4MDMwNzAxWhcNMjkx

MjMxMDMwNzAxWjBWMQswCQYDVQQGEwJDTjEwMC4GA1UECgwnQ2hpbmEgRmluYW5j

aWFsIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MRUwEwYDVQQDDAxDRkNBIEVWIFJP

T1QwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDXXWvNED8fBVnVBU03

sQ7smCuOFR36k0sXgiFxEFLXUWRwFsJVaU2OFW2fvwwbwuCjZ9YMrM8irq93VCpL

TIpTUnrD7i7es3ElweldPe6hL6P3KjzJIx1qqx2hp/Hz7KDVRM8Vz3IvHWOX6Jn5

/ZOkVIBMUtRSqy5J35DNuF++P96hyk0g1CXohClTt7GIH//62pCfCqktQT+x8Rgp

7hZZLDRJGqgG16iIOgNyejLi6mhNbiyWZXvKWfry4t3uMCz7zEasxGPrb382KzRz

EpR/38wmnvFyXVBlWY9ps4deMm/DGIq11Y+wejfeWkU7xzbh72fROdOXW3NiGUgt

hxwG+3SYIElz8AXSG7Ggo7cbcNOIabla1jj0Ytwli3i/+Oh+uFzJlU9fpy25IGvP
a931DfSCt/SyZi4QKPaXWnuWFo8BGS1sbn85WAZkgwGDg8NNkt0yxoekN+kWzqot
aK8KgWU6cMGbrU1tVMoqLUuFG7OA5nBFDWteNfB/O7ic5ARwiRIlk9oKmSJgamNg
TnYGmE69g60dWIolhdLHZR4tjsbftsbhf4oEIRUpdPA+nJCdDC7xij5aqgwJHsfV
PKPtl8MeNPo4+QgO48BdK4PRVmrJtqhUUy54Mmc9gn900PvhtgVguXDbjgv5E1hv
cWAQUhC5wUEJ73IfZzF4/5YFjQIDAQABo2MwYTAfBgNVHSMEGDAWgBTj/i39KNAL
tbq2osS/BqoFjJP7LzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAd
BgNVHQ4EFgQU4/4t/SjQC7W6tqLEvwaqBYyT+y8wDQYJKoZIhvcNAQELBQADggIB
ACXGumvrh8vegjmWPfBEp2uEcwPenStPuiB/vHiyz5ewG5zz13ku9Ui20vsXiObT
ej/tUxPQ4i9qecsAIyjmHjdXNYmEwnZPNDatZ8POQQaIxffu2Bq41gt/UP+TqhdL
jOztUmCypAbqTuv0axn96/Ua4CUqmtzHQTb3yHQFhDmVOdYLO6Qn+gjYXB74BGBS
ESgoA//vU2YApUoOFmZ8/Qmkrp5nGm9BC2sGE5uPhnEFtC+NiWYzKXZUmhH4J/qy
P5Hgzg0b8zAarb8iXRvTvyUFTeGSGn+ZnzxEk8rUQElsgIfXBDrDMlI1Dlb4pd19
xIsNER9Tyx6yF7Zod1rg1MvIB6710i6ON7fQAUtDKXeMOZePglr4UeWJoBjnaH9d
Ci77o0c0PaYjesYBx4/IXr9tgFa+iiS6M+qf4TIRnvHST4D2G0CvOJ4RUHlzEhLN
5mydLIhyPDCBBpEi6lmt2hkuIsKNuYyH4Ga8cyNfIWRjgEj1oDwYPZTISEEdQLpe
/v5WOaHIz16eGWRGENoXkbcFgKyLmZJ956LYBws2J+dIeWCKw9cTXPhyQN9Ky8+Z
AAoACxGV21ZFA4gKn2fQ1XmxqI1AbQ3CekD6819kR5LLU7m7Wc5P/dAVUwHY3+vZ
5nbv0CO70615s9UCKc2Jo5YPSjXnTkLAdc0Hz+Ys63su

-----END CERTIFICATE-----

主题：CN = CFCA EV OCA

O = China Financial Certification Authority

C = CN

序列号：00 b4 cf 94 32 66

有效期：2012 年 8 月 8 日 14:06:31——2029 年 12 月 29 日 14:06:31

摘要算法：SHA256

密钥长度：RSA（2048Bits）

-----BEGIN CERTIFICATE-----

MIIFTjCCAzagAwIBAgIGALTP1DJmMA0GCSqGSIb3DQEBCwUAMFYxCzAJBgNVBAYT
AkNOMTAwLgYDVQQKDCdDaGluYSBGaW5hbmNpYWwgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkxFTATBgNVBAMMDENGQ0EgRVYgUk9PVDAeFw0xMjA4MDgwNjA2MzFaFw0y
OTEyMjkwNjA2MzFaMFUxCzAJBgNVBAYTAkNOMTAwLgYDVQQKDCdDaGluYSBGaW5h
bmNpYWwgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFDASBgNVBAMMC0NGQ0EgRVYg
T0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA02OMsGFxFQIPMKVP
oRaO9rHNX41xbq8jhnbdK0MDVbxfGa3b8QTKxMcmxlRlULfsaie0cIlaRl0AUcJP
QH9ftekzh4T287xqsEAydYQHf77arWQ5nY3fR9RcoBq9pTCQbqw49S6/jHA5oPQa
EoKbF0G8zfVKp5PrcKSufHMQyKo/Ez2UYT+gut36j4GYpAABuV6PbusPpjufsN9B
r9+xqgyz8ubSp1W11qSlvQUQBhAJAH+a3NMhD0illaGfTdWbF485a5NilMFGqJBa
/kLVEYwG4aoKdV9vG/NFS0LKz3QVnB7bkrLjTkuGN/zQJP0daJ3CGAzmN+Cr2ujt
XOfAYwIDAQABo4IBITCCAR0wOAYIKwYBBQUHAQEELDAqMCgGCCsGAQUFBzABhhxo
dHRwOi8vb2NzcC5jZmNhLmNvbS5jbi9vY3NwMB8GA1UdIwQYMBaAFOP+Lf0o0Au1
uraixL8GqgWMk/svMA8GA1UdEwEB/wQFMAMBAf8wRAYDVR0gBD0wOzA5BgRVHSAA
MDEwLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cuY2ZjYS5jb20uY24vdXMvdXMtMTIu
aHRtMDoGA1UdHwQzMDEwL6AtoCuGKWh0dHA6Ly9jcmwuY2ZjYS5jb20uY24vZXZy
Y2EvUlNBL2NybDEuY3JsMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUVQji3MyV
bR9d3rNH6OkWxsBFd8QwDQYJKoZIhvcNAQELBQADggIBAMmFEIoCE9UNmb2BYYhT
RV12kNVucP6t683BaFTgJizIJw/ebvvTdWNTycyP5MQFlHKrIYwjvFO9Rfw8+yIs
sT3JFYiqsLBswvaMr3AIuA2mTnmasvZFe6P19qitzTRkz+TL6TFailrtnzudsvn2
SeVbRiX+6CsyNNMoPsRHTeZAEpkB7J3vh+ZAiv3gsIXtjtz5Y1iWWRZipemJ/qEf
W2hDONB+T61GcEXHDi9dIkWcC/jFT4XPM64pagAz9gEGZg1PzFBE8QMxiwaDAOea
GOlOe/HW4wJlo4ZzOELqZGJL1YhQ8AkBYR95NEtR9j5bWK98Lznykldk2MDLBD2m
rIfMkVjMwEj4A8ElMXsLnWXXg41NN6gjUm2/IudKOaGqniPs5SZrN36O4B3NzsaZ
dLznHH5HO+aksurjgme8RAGOA2OAnRG3VXBWrxud7tOKDINLs+mxY7IR+xVZ2cw6
Cer8HnAVfKPJrbdq7vyJJkIpCll+mLHaGgvv3IqiU4rrrllE3NYjKG4Fk2MiYvZg
1OKXA8tlYsLt8I/RcNmC2TvjZHYVE3tanbGw53TRGFk2Vq68XOkvooOardihwRkg
qcOgUvouORuvSqTlkQizTFH6FTUt3xuuED4dnn5N/1ijcDtON3l5ovoyHOVcYiO4
drCN96LHiUoiSfYODmpXG2tl

-----END CERTIFICATE-----

主题：CN = CFCA OV OCA

O = China Financial Certification Authority

C = CN

序列号：00 f9 df 6a df f5 64 be a6 8b 82

有效期：2015 年 3 月 25 日 10:02:56——2029 年 12 月 25 日 10:02:56

摘要算法：SHA256

密钥长度：RSA（2048Bits）

-----BEGIN CERTIFICATE-----

MIIFfDCCA2SgAwIBAgILAPnfat/1ZL6mi4IwDQYJKoZIhvcNAQELBQAwVjELMAkG

A1UEBhMCQ04xMDAuBgNVBAoMJ0NoaW5hIEZpbmFuY2lhbCBDZXJ0aWZpY2F0aW9u

IEF1dGhvcml0eTEVMBMGA1UEAwwMQ0ZDQSBFViBST09UMB4XDTE1MDMyNTAyMDI1

NloXDTI5MTIyNTAyMDI1NlowVTELMAkGA1UEBhMCQ04xMDAuBgNVBAoMJ0NoaW5h

IEZpbmFuY2lhbCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEUMBIGA1UEAwwLQ0ZD

QSBPViBPQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDn14xTy0bH

zkaeyACeq6ryfxxG5zZT1fCL4lmw7sk6SVmOKNfE60Gf7W6orksrFVIbIMK+VrYp

+aYyhScq8EJT9xXBgXK2HqtpaDGOeclspJvcs+rXn9tlT789NBp3i5U+nLE9M1bR

CHSx3Hzu8p7Aeqllou+8nZ2egaVbWFL1zC1JENupSSI9Yjbefhb06y/TVxQ0x4Zt

zwPwLcd8NUtSruldolxPbhQeCZNJMPq1GKMxhd5pDwY4mCKxDeraqhTNXui9Aef3

qyi2Ic9EXmdNPARkZJU2XTJ9FJ+DE+ChaIvfJ/VwQfM0eGlBn/SAaav54jBmRnec

PeD6YfpuiJ8vAgMBAAGjggFKMIIBRjA4BggrBgEFBQcBAQQsMCowKAYIKwYBBQUH

MAGGHGh0dHA6Ly9vY3NwLmNmY2EuY29tLmNuL29jc3AwHwYDVR0jBBgwFoAU4/4t

/SjQC7W6tqLEvwaqBYyT+y8wDwYDVR0TAQH/BAUwAwEB/zBEBgNVHSAEPTA7MDkG

BFUdIAAwMTAvBggrBgEFBQcCARYjaHR0cDovL3d3dy5jZmNhLmNvbS5jbi91cy91

cy0xMi5odG0wOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybC5jZmNhLmNvbS5j

bi9ldnJjYS9SU0EvY3JsMS5jcmwwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRm

s+/7VJWH6aylllau5n3tOtBDOTAnBgNVHSUEIDAeBggrBgEFBQcDAgYIKwYBBQUH

AwQGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4ICAQDKER8qcBmZGOG8GOJ670VW

OSg3UovOoc7/xz2mE+enyEcSwn/OQrL8C5DSA6nMvBMrCWEytYPofGQUXTwtlu78
GLxYNn3A/RtzczJ+/BXIhoe3aOT4tQ+2s9vrFRfIXs4CkmqHhfYSvArokdayYmBd
78psIwS5LCUzGKSn7y8UmAgoxiy7RtrVt5c1wvJyeuYk1Z1l8MN1szPrmAb4HS/D
qnB+OqdhFGvfOyv7lg6/wlIAkN84cHlKNC3JvyFHaCIAyhTPgjUayUvBKFK7XwN9
utIXl2L3IZX7zfxGS/J9+ZeNwyblQKmd/MKydJu9Ak6+ZMLLgjlCFkihJIn9Ur8M
2KQigz7YPDVIJjOtS7ljOQVGh88LPUnQ1fBY7RwagficS/xclIOnaXhoyWzg7EcQ
/T1/O4FkpMqKuOreaI5NExjAT8cKizyY2wcOOXKIYri3Ewnbm+OOIaYYaiQRGUR6
pzFFKxdFMbStCtI4ObN+A9tB7cnBCW4vz3sAJd/OgmLF38XTa+/km3c1nQOfhCGs
6kx2heN/DgFAc+P71dObo/kgGQtR6tr02gyXCFWnLMtTO+CoNOYOo3T+LbEqYeKL
W7p29G9sgHgoqLFibWNMSKG1QvevkhjUMOD/g48f/nMSYsbU++yEaLvjvRHbb5ON
IPkcE28TRhQQKmDKI+DRIg==
-----END CERTIFICATE-----

附录四、SHA 摘要算法介绍

安全哈希算法（Secure Hash Algorithm）主要适用于数字签名标准 （Digital Signature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。对于长度小于 2^64 位的消息，产生一个消息摘要。消息摘要可以用来验证数据的完整性。

SHA 家族的五个算法，分别是 SHA-1、SHA-224、SHA-256、SHA-384，和 SHA-512，后四者并称为 SHA-2。支持 SHA2 的操作系统包括：Windows 8.1、Windows 8、Windows 7、Windows Server 2012 R2、Windows Server 2012、Windows Server 2008 R2、Windows Server 2008、Windows Vista、Windows Server 2003 R2、Windows 2003 Server SP2、32 位 Windows XP SP3、64 位 Windows XP SP2。

由于 SHA1 摘要算法存在杂凑冲撞攻击，随着计算机运算能力越来越强，其安全性受到越来越严重的威胁。微软、谷歌等陆续发布了弃用 SHA1 摘要算法的时间表。微软方面，要求 CA 机构 2016 年之后不能再签发新的 SHA1 摘要算法的 SSL 站点证书。2017 年之后，Windows Vista、Windows Server 2008 及以上版本操作系统将无法访问 SHA1 摘要算法 SSL 证书的网站。谷歌方面，Chrome 浏览器将对 SHA1 摘要算法 SSL 证书的站点提示安全警告。

附录五、常见问题

1、CFCA 全球信任 SSL 证书支持的操作系统和浏览器

Windows 平台浏览器 100%支持，包括但不限于：Internet Explorer、Google Chrome、Mozilla Firefox、Opera，以及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器；

Windows Phone 平台浏览器 100%支持；

Andriod（Android 6.0 Marshmallow）平台 100%支持；

Linux 平台浏览器 100%支持；

Mac OS（10.12.1 及更新版本）平台浏览器 100%支持，包括但不限于：Safari、Google Chrome、Mozilla Firefox 等；

IOS（10.1 及更新版本）平台浏览器 100%支持；

浏览器 操作系统	Internet Explorer	Mozilla Firefox	Google Chrome	Apple Safari
Windows	√	√	√	——
Unix/Linux	——	√	√	——
Mac OS 10.12.1 及更新版本	——	√	√	√
iOS 10.1 及更新版本	——	√	√	√
Andriod 6.0 Marshmallow	——	√	√	——
Windows Phone	√	√	√	——

√：表示该浏览器完全支持 CFCA 全球信任 SSL 证书；

×；表示该浏览器不完全支持 CFCA 全球信任 SSL 证书，当浏览器访问含有 CFCA 全球信任 SSL 证书的网站时，会有不受信任提示；

——：表示该浏览器不支持此操作系统。

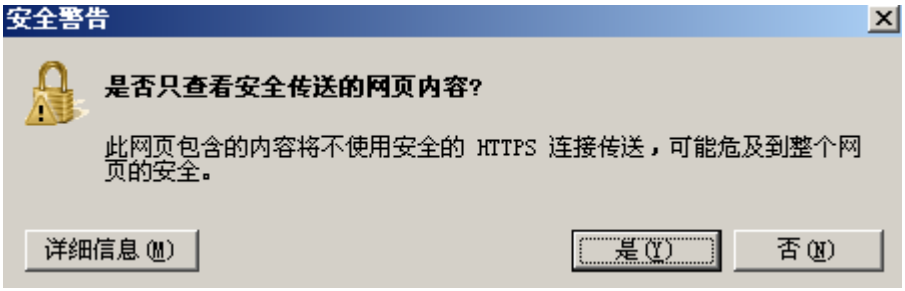
2、Windows XP SP2 操作系统使用 CFCA EV SSL 证书

CFCA EV SSL 证书采用 SHA256 摘要算法，而 Windows XP SP2 操作系统并不支持该算法。在 Windows XP SP2 操作系统中，使用 IE 浏览器无法访问含有 CFCA EV SSL 证书的网站（包括使用其他 CA 机构 SHA256 摘要算法 SSL 证书的网站）。可以将操作系统升级到 Windows XP SP3 及以上版本，即可正常访问。

此外，火狐（Firefox）、谷歌（Chrome）等浏览器不依赖操作系统，浏览器本身支持 SHA256 摘要算法。因而可以在 Windows XP SP2 操作系统上使用这些浏览器访问含有 CFCA EV SSL 证书的网站。

3、通过 HTTPS 访问，页面弹出警告“是否只查看安全传送的网页内容”

当网页包括经加密传送的 HTTPS 内容和未经加密传送的 HTTP 内容时，IE 会弹出警告询问用户是否允许接受未经加密的内容。



可以在“工具”——“Internet 选项”——“安全”——“自定义级别”——“显示混合内容”设置为“启用”，即可不再弹出该提示。

一般来说，当 HTTPS 页面引用外部 HTTP 链接时，会提示此内容不安全。可以通过 Firefox 的 Web 控制台，或者 Chrome 的 JavaScript 控制台查看到具体的报错代码行，并可以参考相关提示修改页面代码。

4、部署 CFCA 站点认证标识

办理 CFCA EV SSL 证书、CFCA OV SSL 证书的网站均可以在其网站页面上嵌入 CFCA 站点认证标识，用户点击该标识，可以跳转到 CFCA 站点认证页面，CFCA 将对网站的相关信息予以认证说明，增强网站的可信度。

部署 CFCA 站点认证标识，需将站点认证图标和以下链接嵌入网站页面上。

https://evwebverify.cfca.com.cn/WebVerify/webVerifyServlet?domain=网站域名

注意：1、网站域名必须为完整的域名，如：www.cfca.com.cn

2、该 URL 和图标必须放在对应域名的页面上，如果 URL 中的域名和网页的域名不一致则会认证失败；

3、如果网站既有 https 页面，也有 http 页面，则 https 页面嵌入的 URL 为“https://”，http 页面嵌入的 URL 为“http://”。

5、Chrome、Firefox 提示“SSL 收到了一个弱临时 Diffie-Hellman 密钥”

Chrome、Firefox 等最新版本的浏览器，对客户端浏览器和网站服务器之间的密钥算法有较高要求，不允许客户端浏览器和网站服务器之间使用相对较弱的密钥算法。该问题需要调整 Web 应用服务器的相关配置，限定客户端浏览器和网站服务器之间使用较高强度的密钥。

常用的 Web 应用服务器配置密钥算法的方式如下：

Apache：

在 httpd-ssl.conf 配置文件中增加如下内容：

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

Nginx：

在 conf/nginx.conf 配置文件中增加如下内容：

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

Tomcat：

在 conf/server.xml 配置文件中增加如下内容：

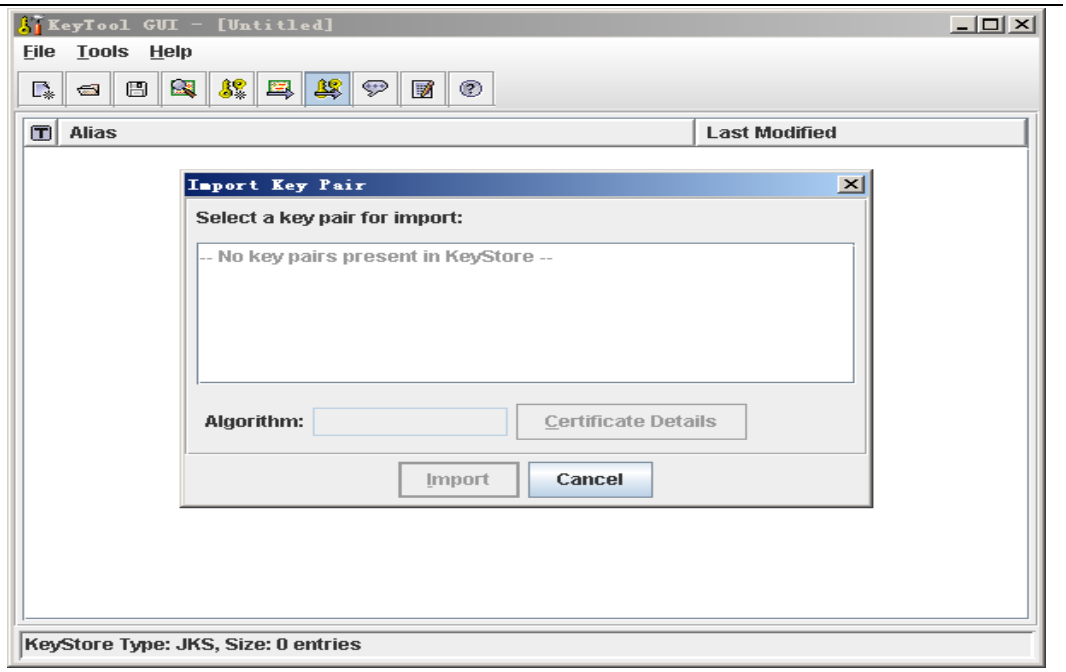
<Connector

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_SHA256,TLS_ECDHE_RSA_WITH_AES_128_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_SHA,TLS_ECDHE_RSA_WITH_AES_256_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_SHA384,TLS_ECDHE_RSA_WITH_AES_256_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_SHA,TLS_DHE_RSA_WITH_AES_128_SHA256,TLS_DHE_RSA_WITH_AES_128_SHA,TLS_DHE_DSS_WITH_AES_128_SHA256,TLS_DHE_RSA_WITH_AES_256_SHA256,TLS_DHE_DSS_WITH_AES_256_SHA,TLS_DHE_RSA_WITH_AES_256_SHA" />

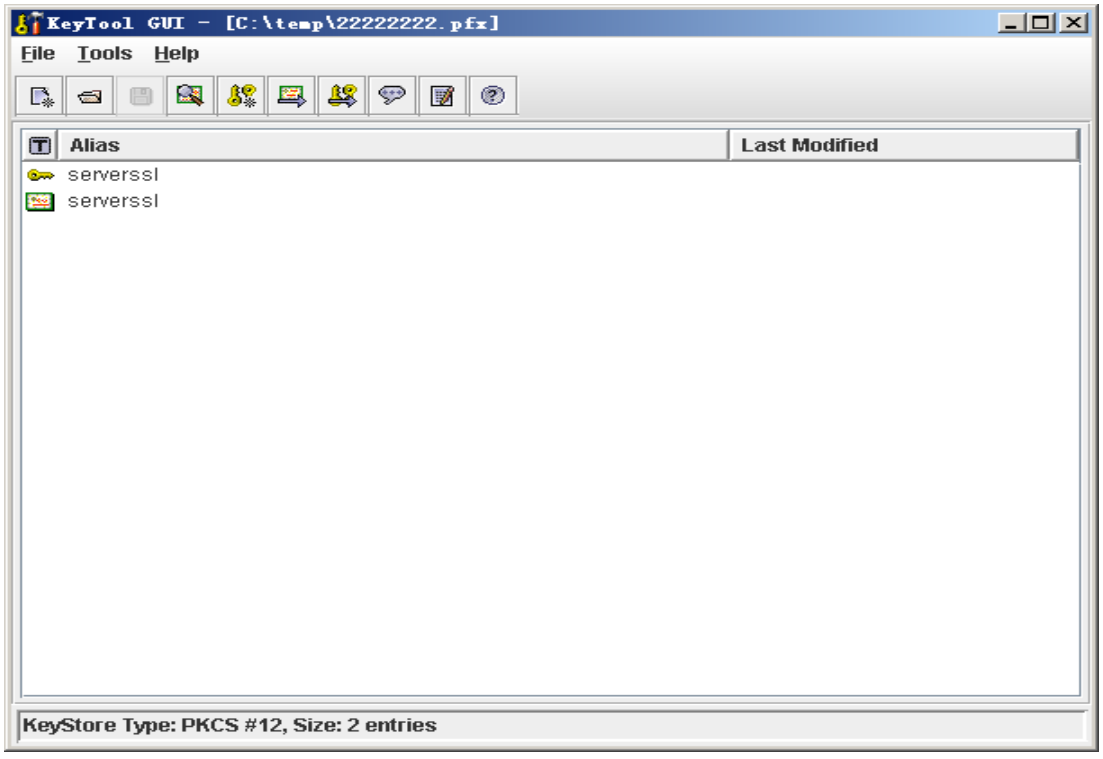
6. 客户反馈下载的服务器公钥证书总是在导入 jks 文件的时候报错无法安装认证回复

- 确认 JKS 文件是否是当初生成 CSR 文件的证书文件;
- 确认证书链是否已经导入：注意要先后导入根证书、中级证书
- 确认证书链是否与公钥证书的证书路径一致。
- 如是不相符的证书文件，只能重新办理，即重新产生 CSR 并且补发证书

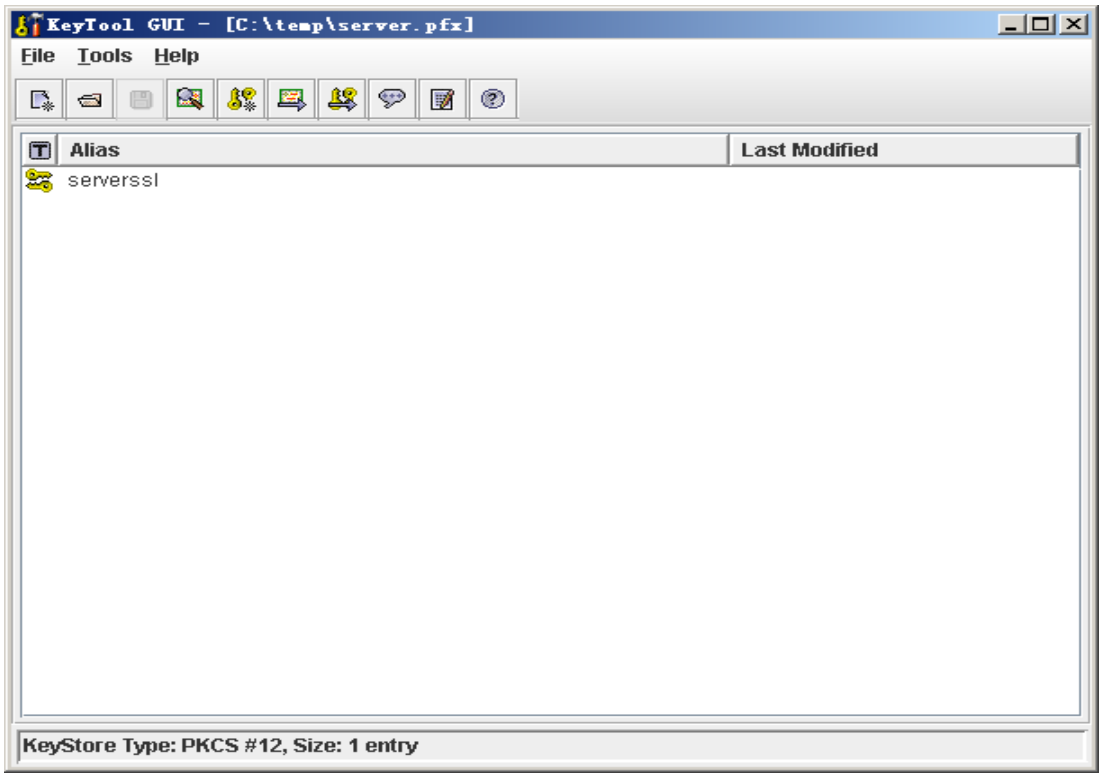
7. pfx 导入 jks 出现如下问题“No key pairs present in KeyStore ”



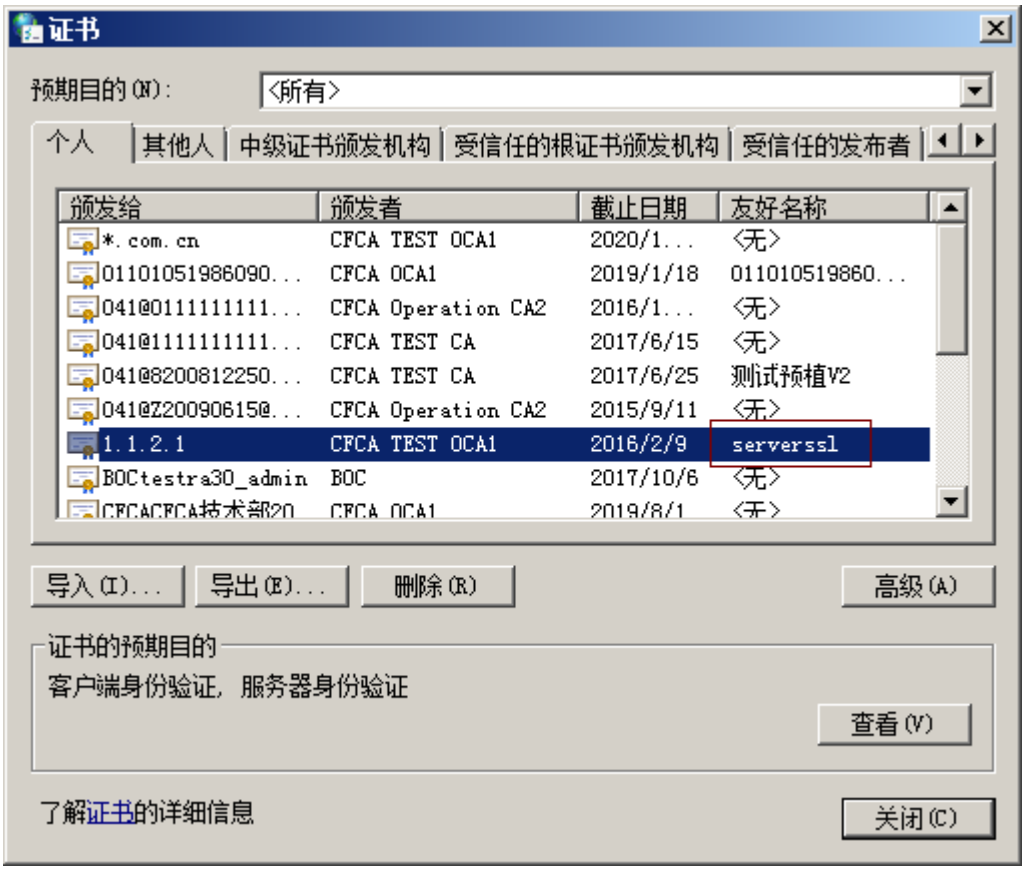
问题原因：造成此问题的原因是 pfx 出现问题，在 keytool 工具打开 pfx 文件时，现象如图



如果 pfx 文件正常，那么 keytool 工具打开时，效果如下图：



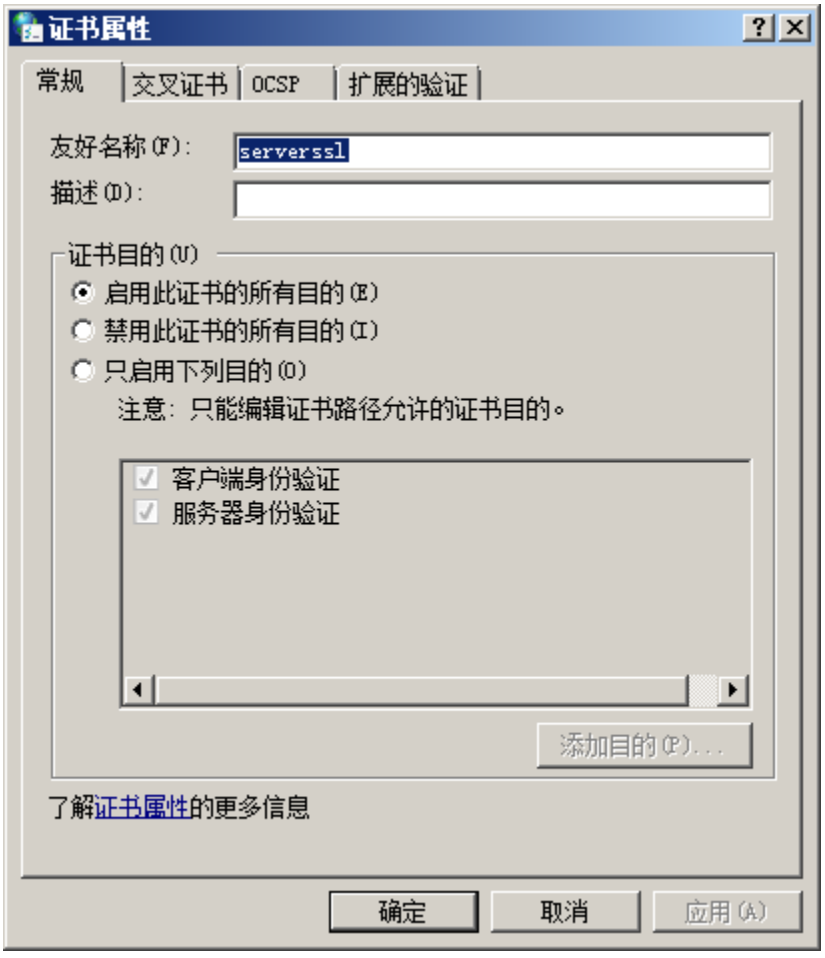
造成 pfx 出现上面另种情况的原因在于，ie 中看到的友好名称：



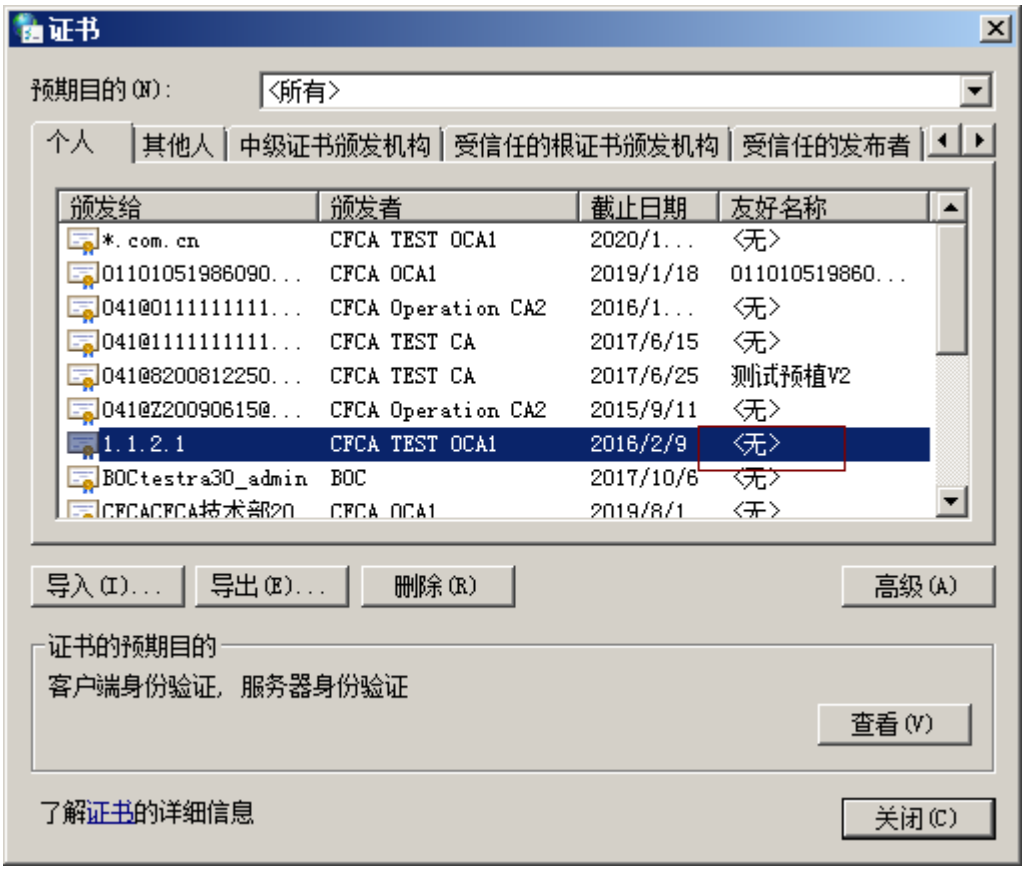
解决方法：删除友好名称

1. 双击证书，查看详细信息：

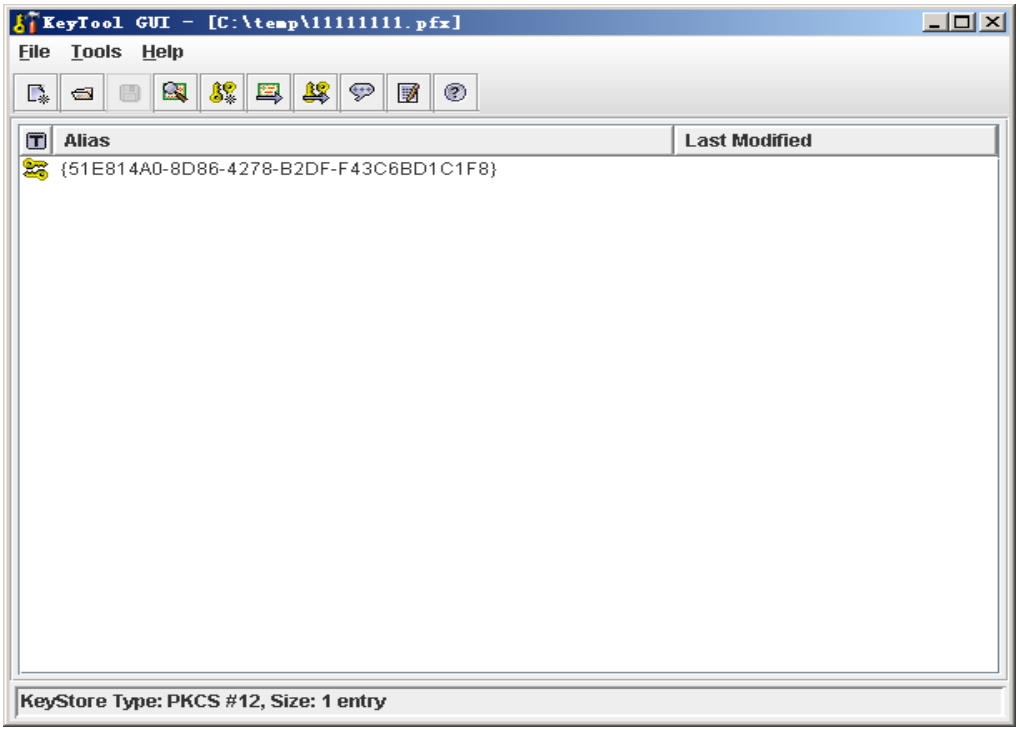
2. 点击“编译属性”



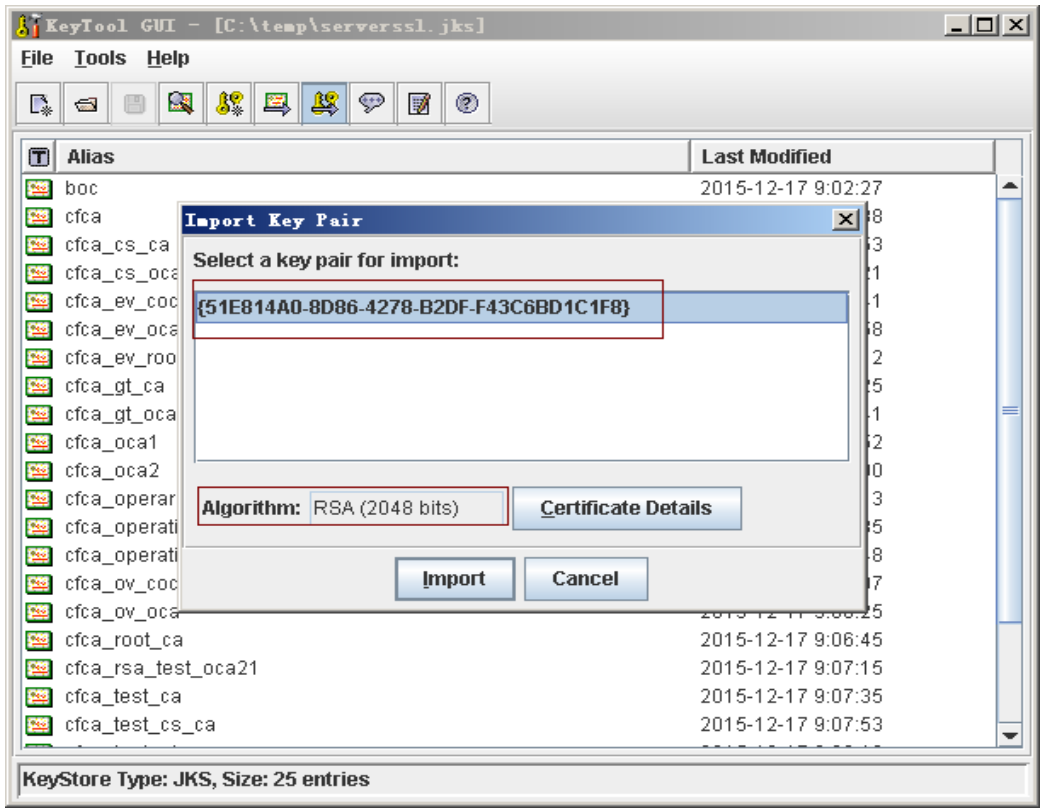
3. 将友好名称删除

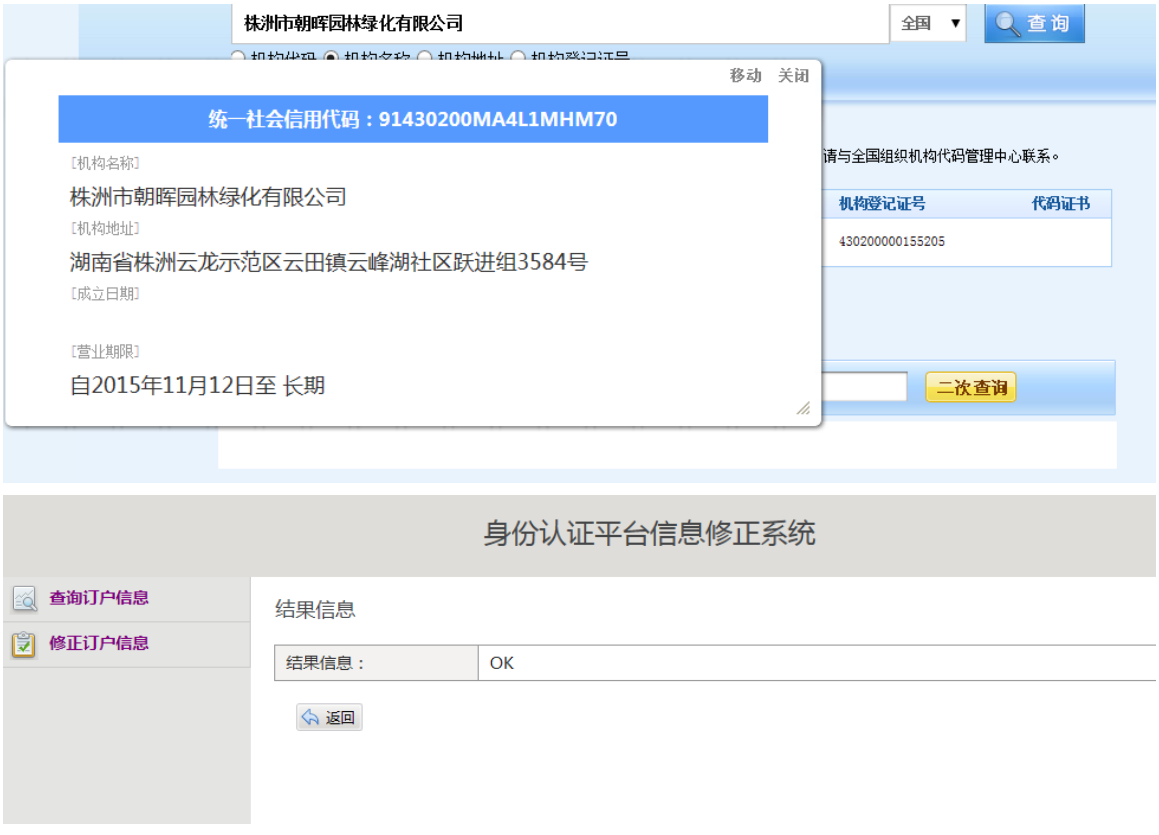


4. 之后再导出成 pfx。Jks 查看，pfx 文件正常：



5. 导入 jks 时可以正常选中密钥空间





身份认证平台信息修正系统
结果信息
状态：
证书有效
订户名：
株洲市朝晖园林绿化有限公司
证件类型：
统一社会信用代码
证件号码：
91430200MA41L1MHM70
修正
返回