普通证书技术支持手册

版本 2.1
2008 年 2 月 22 日

修 改 记 录

日 期	修 改	修 改 者	审核人	版 本
2004/12/13	建立文档	施威		0.1
2005/1/12	形成正式文档	施威		1.0
2008-1-16	针对统一下载平台及 VISTA 系统进行相关修改	李菲	张昊	2.0
2008-2-20	最后上线前修改	张进	张昊	2.1

目录

前言

普通证书是用户与服务器建立安全连接及签名时所使用的证书。普通证书的密钥对由相应的浏览器或 USB Key 自己产生和管理，下载证书时只需在 CFCA 证书下载中心输入获得的参考号和授权码即可。安装在浏览器证书存储区域或 USB Key 的普通证书除了用于与网站建立安全连接外，还可以用于安全电子邮件由邮件客户端直接应用。为了更好的推广普通证书的应用，CFCA 开发了普通证书工具包帮助开发人员更方便的开发基于普通证书应用的产品。

第一章、普通证书的下载

1.浏览器上CFCA证书链的安装

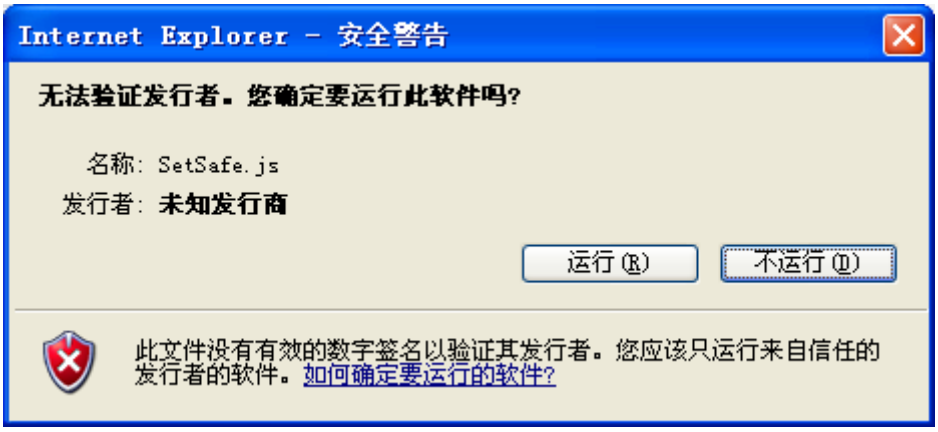
用户在下载普通证书之前，首先要下载相应的 CFCA 证书链。

1. 访问 http://www.cfca.com.cn/tongyi 网站，出现下图：

对于使用 IE7 的用户，或者使用 Vista 操作系统的用户需要做以下操作：

直接执行页面上的 SetSafe.js 脚本文件如下所示：

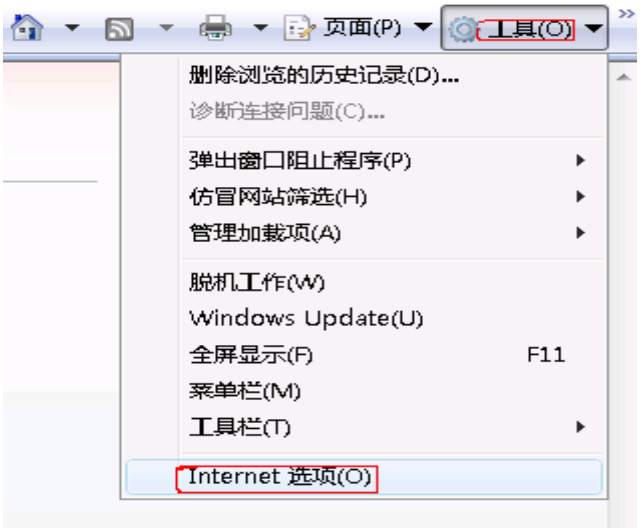
点击“ 打开 ”。

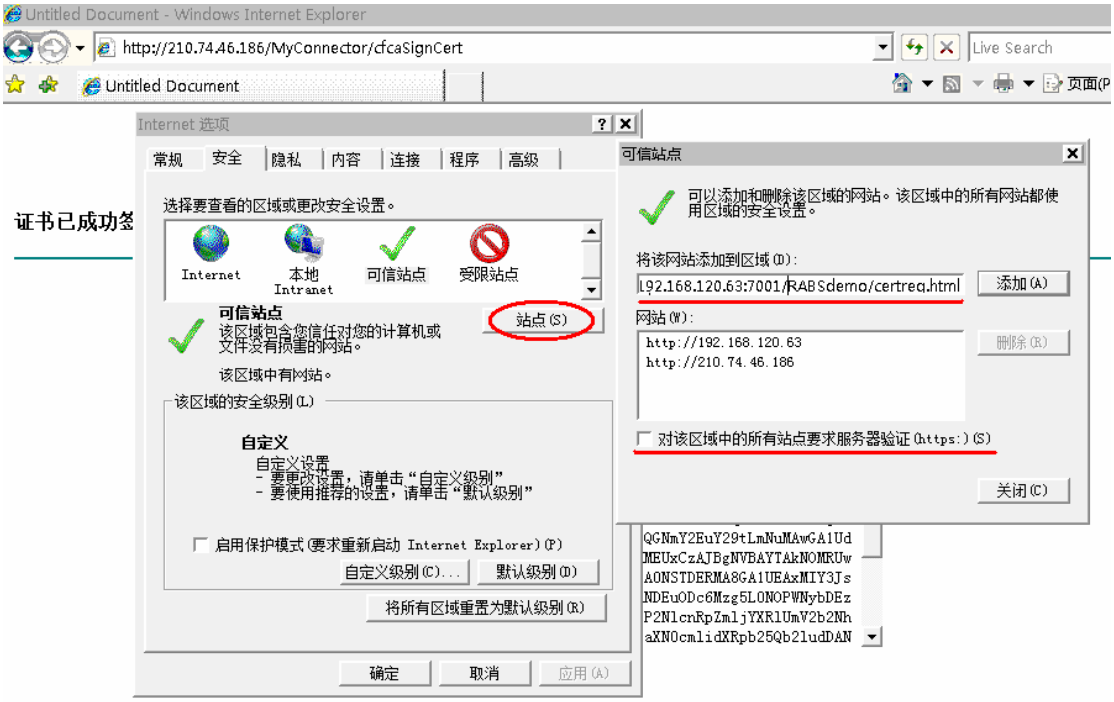


点击“ 运行 ”。

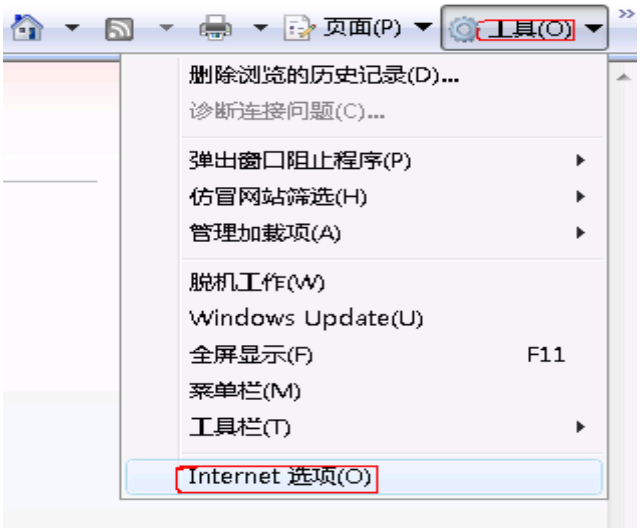
如果没有弹出设置成功，需要使用以下方法进行手工设置：

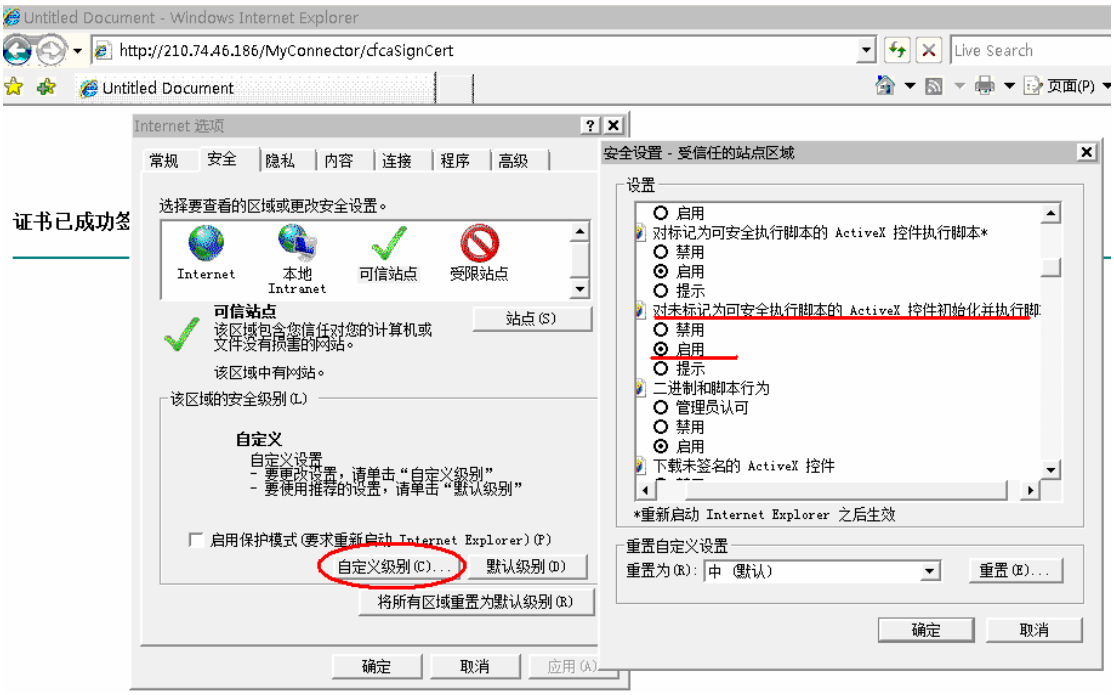
1）将下载证书的站点加入可信站点中，可以通过浏览器的“ 工具→选项→安全→站点 ”，将 CFCA 添加为受信任的站点，如图：



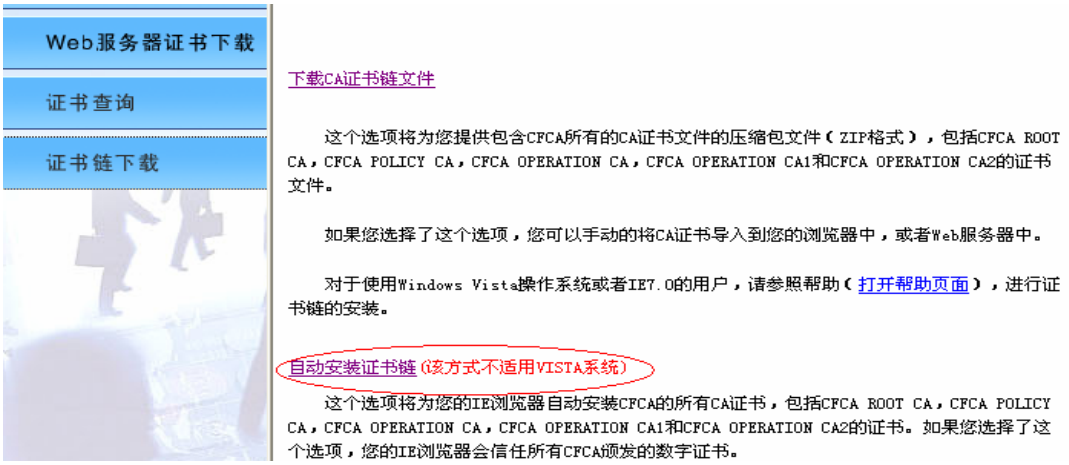


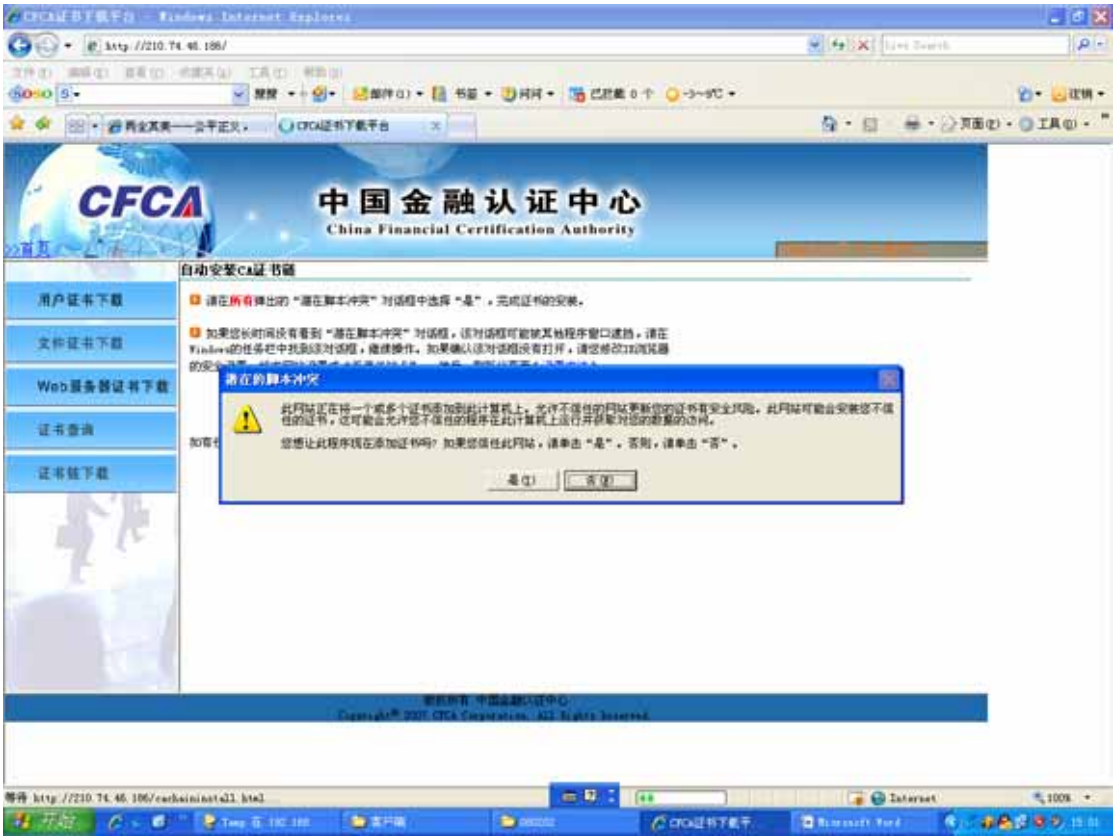
2）手工将受信任站点的【Internet 选项->安全->可信站点->自定义级别->ActiveX 控件和插件->对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本】 必须设置成启用，如图：





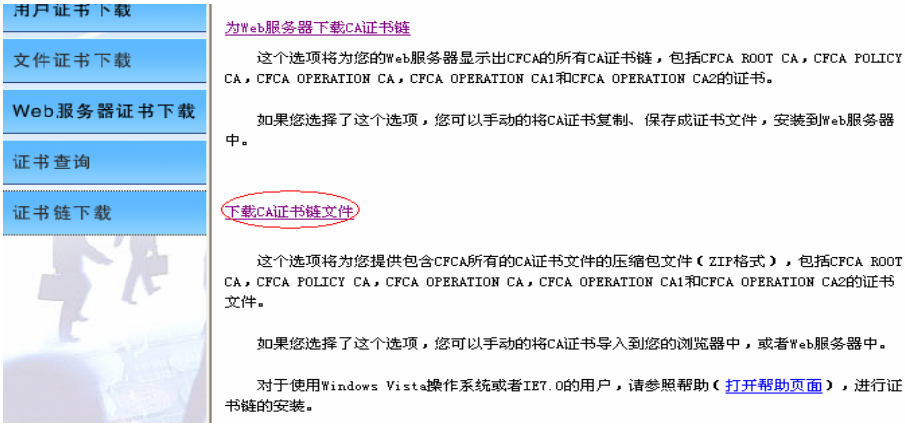
2.非微软 VISTA 系统用户，可以直接点击“ 自动安装证书链 ”，出现下图:





选择“是”，则安装成功，如下图：

3. 对于微软 VISTA 系统用户，可以选择“下载 CA 证书链文件”下载证书链文件，手动安装。

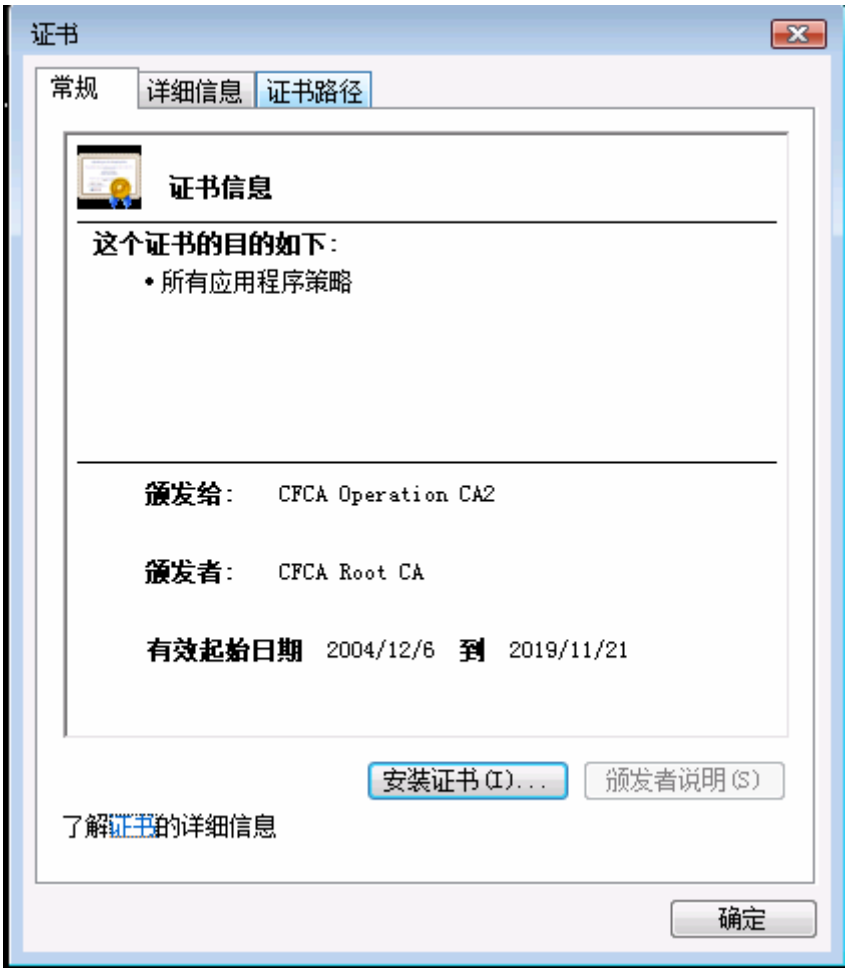


将下载的压缩文件解压缩后，有 5 个 CFCA 的证书链文件，除 Root__CA.cer 文件外，其余文件均可以双击证书链文件，对于出现的对话框都选默认通过，就能安装证书链。

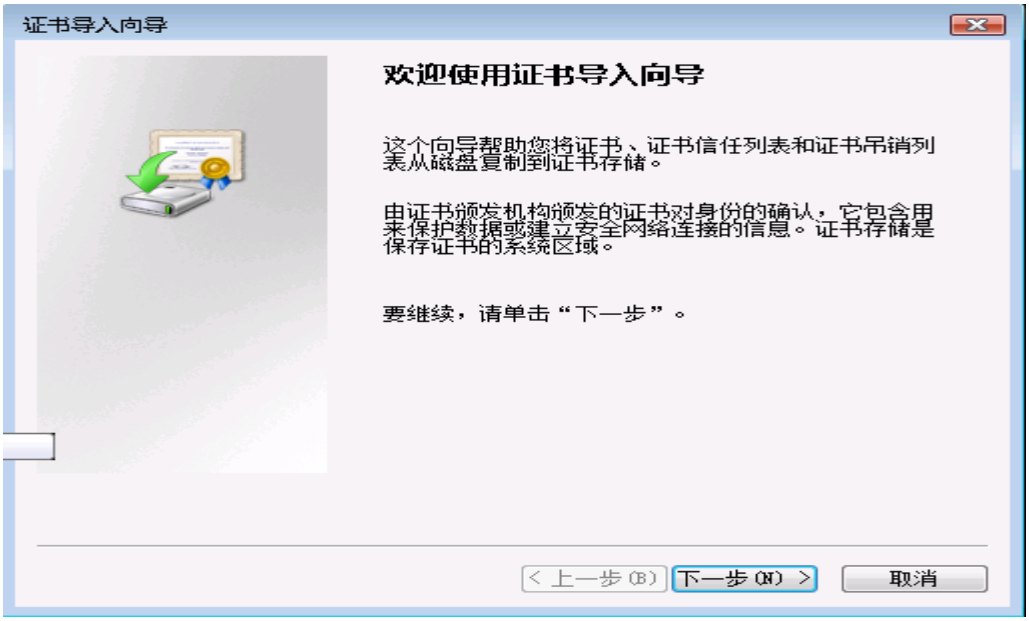
对于非 Root_CA.cer 证书安装步骤如下(以 Operation_CA2.cer 文件为例)：

1) 双击 Operation_CA2.cer 文件，选择“ 打开 ”。

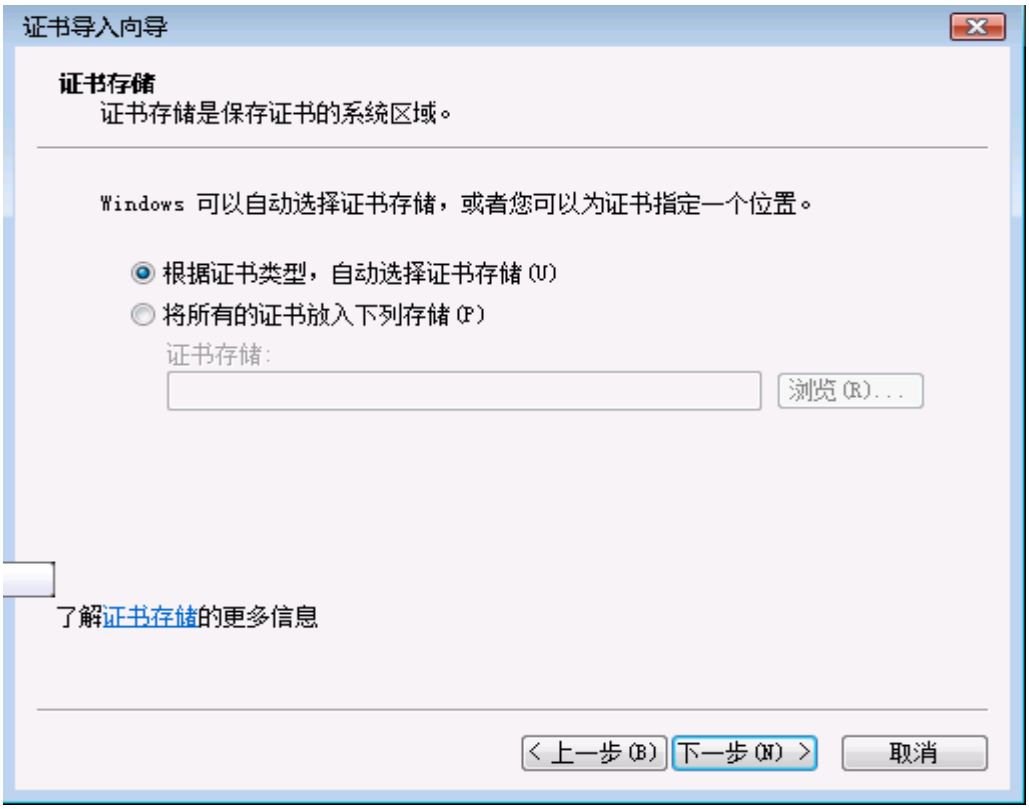
2) 选择“ 安装证书 ”。



3) 选择“下一步”。



4) 选择“下一步”。


证书导入向导
证书存储
证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储，或者您可以为证书指定一个位置。
根据证书类型，自动选择证书存储(U)
将所有的证书放入下列存储(P)
证书存储:
浏览(R)...
了解证书存储的更多信息
< 上一步(B)
下一步(N) >
取消

5) 选择“ 完成 ”。

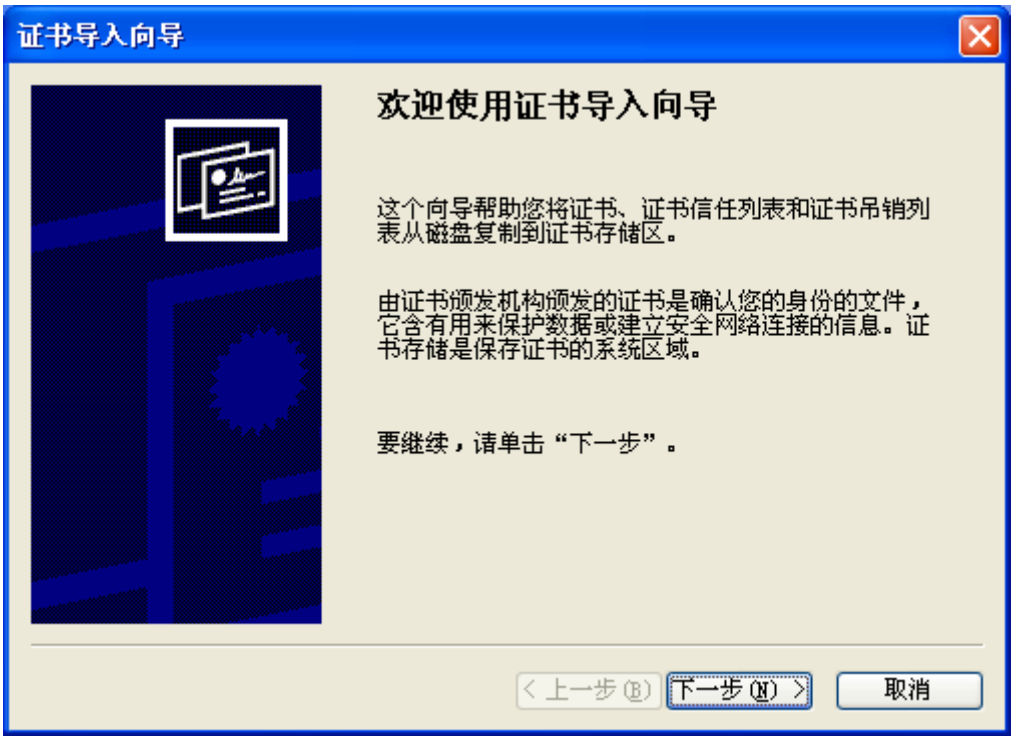

证书导入向导
正在完成证书导入向导
单击“完成”后将导入证书。
您已指定下列设置:
选定的证书存储 由向导自动决定
内容 证书
< 上一步(B)
完成
取消

安装完成，出现导入成功画面。

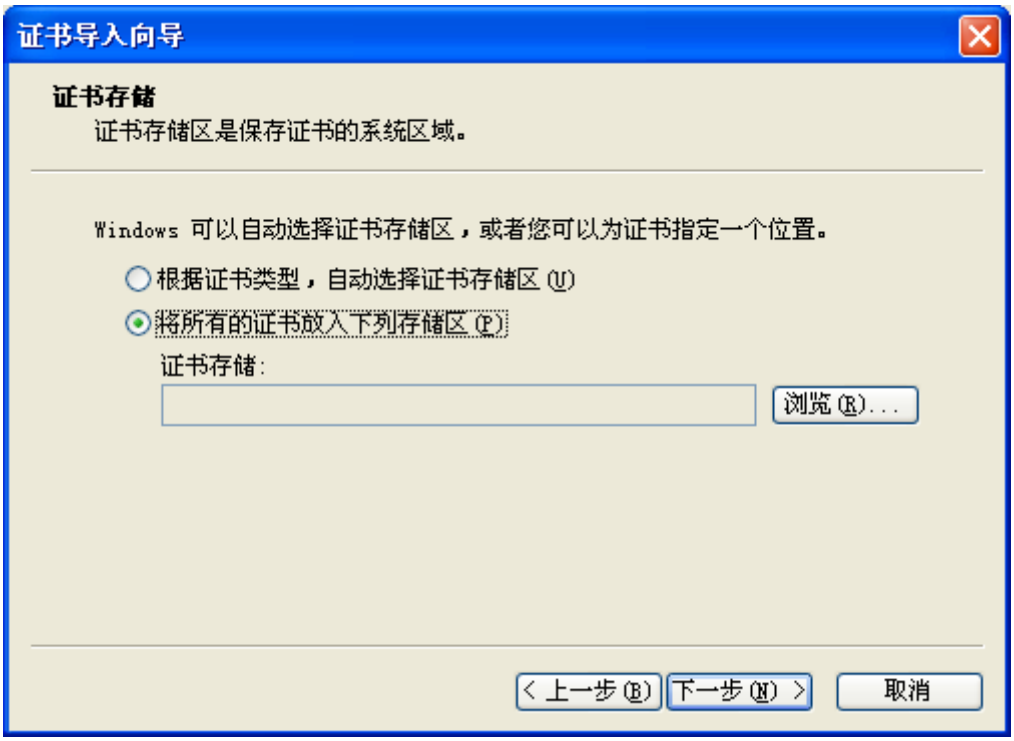
对于 Root_CA.cer 文件安装步骤如下：

1) 双击 Root__CA.cer 文件。

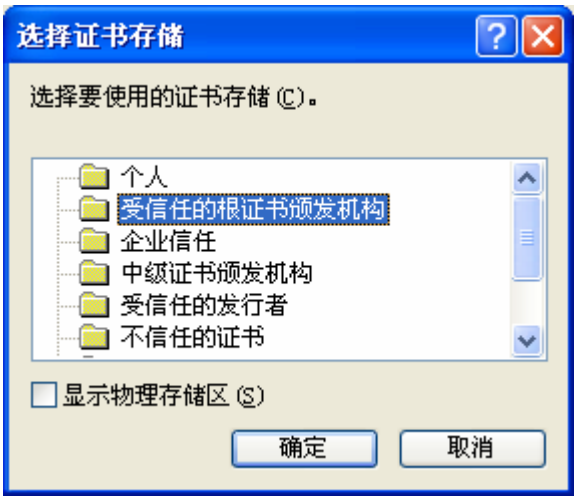
2) 选择“ 下一步 ”。



3)注意要选择“ 将所有的证书放入下列存储区 ”，不能选默认值。



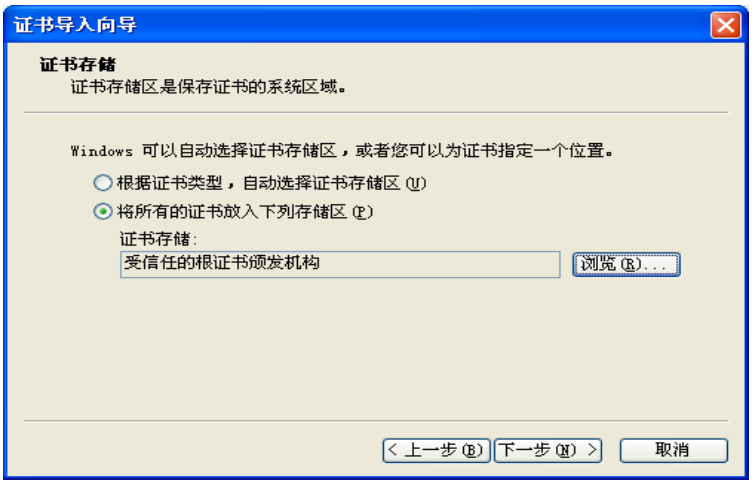
4)点击“ 浏览 ”，选择受信任的根证书颁发机构。



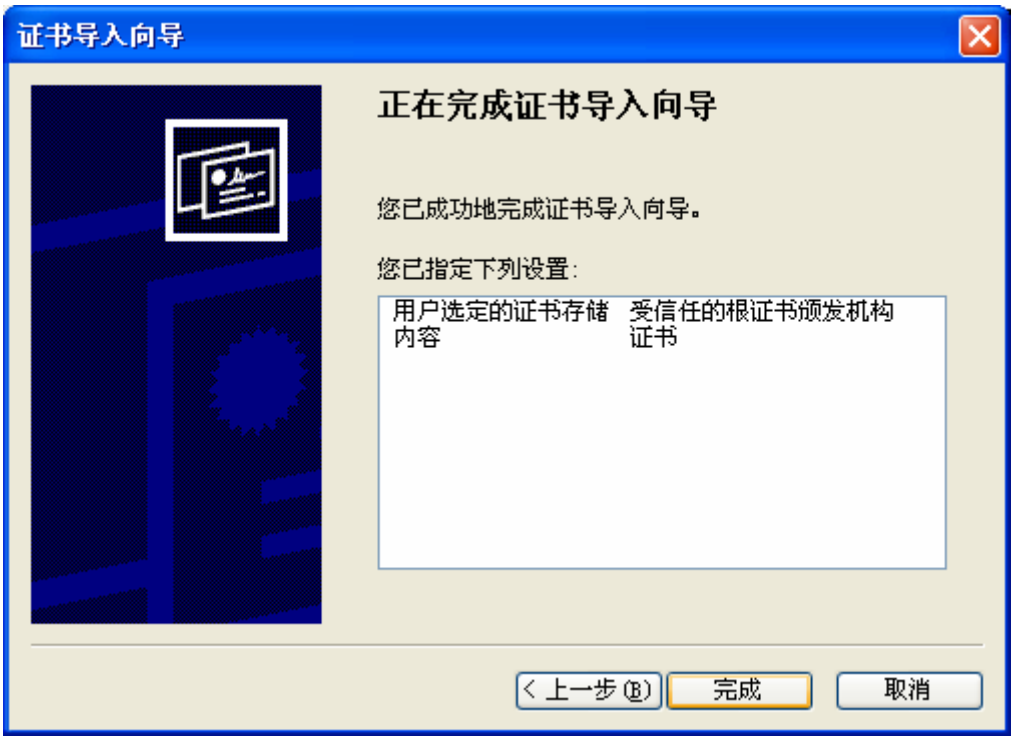
大多数情况上述选择即可。

个别情况下，需要选中“显示物理存储区”，然后选中“受信任的根证书颁发机构”下面的“本地计算机”，选择确定：

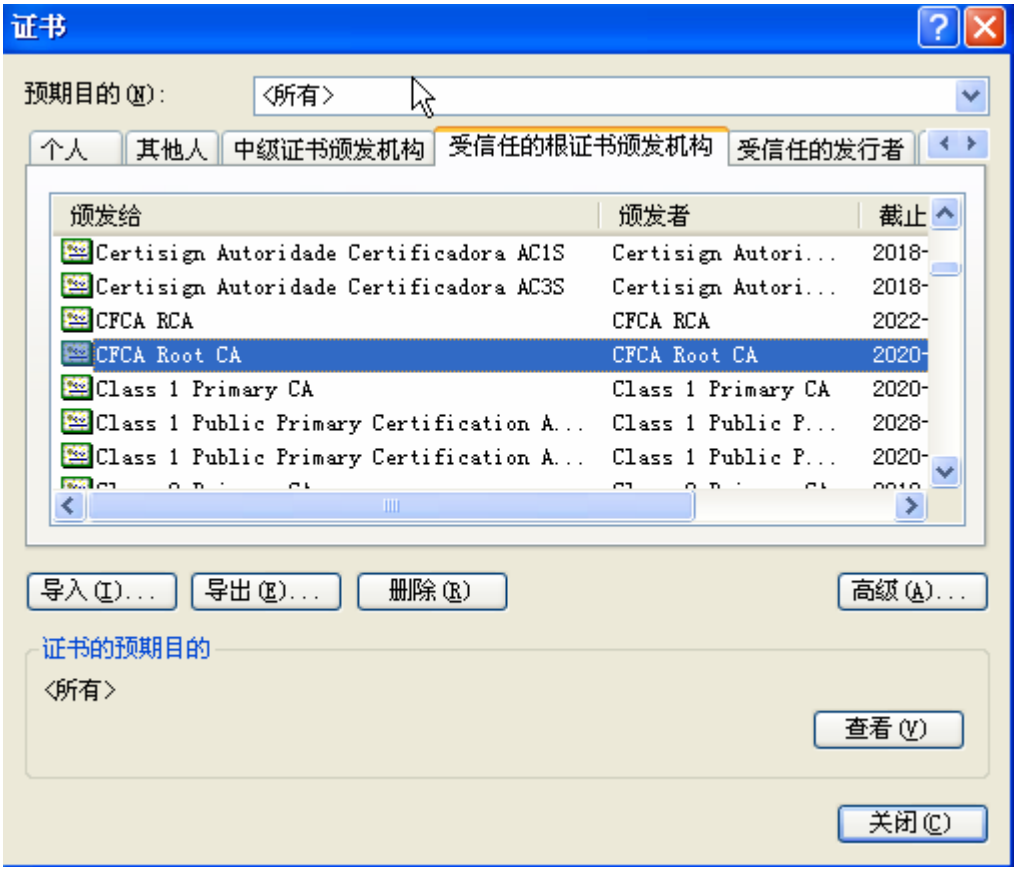
5) 选择“下一步”。



6) 选择“完成”，安装成功。



7) 安装成功后，可以在 IE “ 工具 ” 栏中的 “ INTERNET 选项 ” 中的 “ 内容 ” 一项，看到 “ 证书 ” 信息，在 “ 中级认证机构 ” 及 “ 受信任的根证书 ” 中会出现 CFCA 相关根证书。

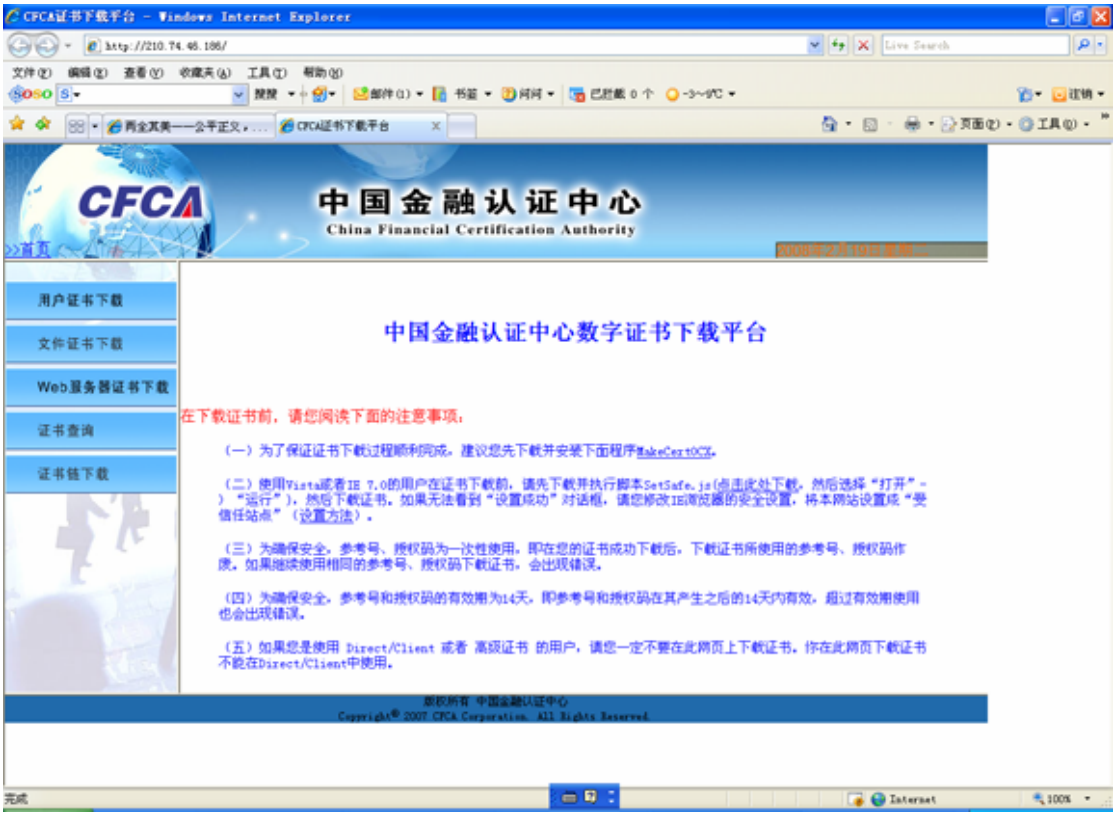


2.普通证书下载

为了您能够正常下载和使用CFCA证书，在IE密钥长度不足 128 位时请根据操作系统选择安装下列补丁。如何查看IE版本和操作系统版本的方法以及获得相关补丁如下：http://www.cfca.com.cn/zhengshu/IE_patch.htm。

用户首先要从发证机构或 CFCA 得到参考号和授权码，然后访问 CFCA 网站下载证书，简单流程如下（以个人普通证书为例）：

1.访问证书下载地址：http://www.cfca.com.cn/tongyi，出现下图：



2.请注意阅读注意事项，避免下载过程中间发生错误。

3.点击左侧菜单“ 用户证书下载 ”，则出现以下图：

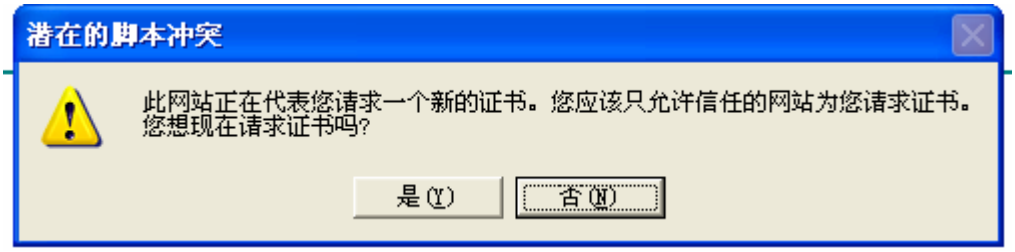
4.在下载证书前，请注意阅读证书服务协议，在该协议中声明了 CFCA 和用户之间的权利和义务。如果用户接受该协议，点击“ 接受此协议 ”，则出现如下图：

5.输入参考号和授权码，选择制证方式,如果证书直接下载到 IE 浏览器中，则选择“ IE 浏览器 ”，如果证书要下载到 USB Key 中，则选择“ USB 智能密码钥匙(CSP 方式) ”。然后选择合适的 CSP（浏览器用户可以选择“ Microsoft Enhanced Cryptographic Provider v1.0 ”，对于 USB Key 用户，根据用户使用 USB Key 的型号选择相应的 CSP）后点击下一步。之后将会弹出一些提示框，按照默认点击确定即可，之后下载证书完成。下面详细介绍一下下载步骤。如下：

2.1 下载到浏览器中

1)在下载页面中填入用户参考号和授权码，同时制证方式选择“ IE 浏览器 ”，软件 CSP 选择“ Microsoft Enhanced Cryptographic Provider v1.0 ”后点击下一步如下图：

2)系统可能弹出“ 潜在脚本冲突 ”对话框（如果按照注意事项的要求，将 CFCA 的网站添加到“ 受信任的站点 ”，则不会出现此对话框），选择“ 是 ”。



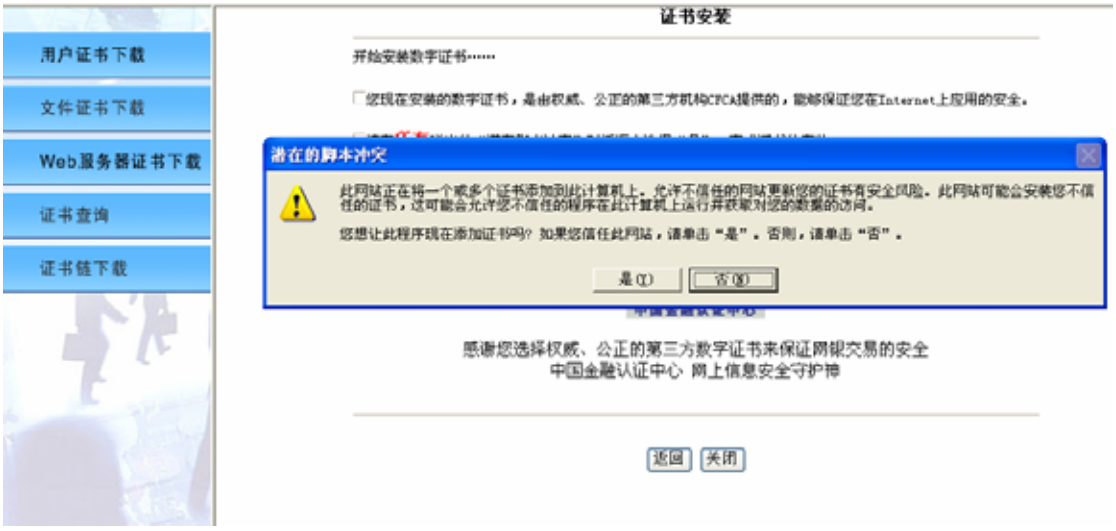
3）此处推荐选择“ 设置安全级别 ”按钮，将安全级别设置为高:这样,使用证书的时候就需要输入密码，可以防止使用你的计算机的其他人在你不知情的情况下滥用你的证书。如果不希望在使用证书时需要输入密码进行确认，可以直接选择“ 确定 ”，进行步骤 4 的操作。

如果选择了“设置安全级别”按钮，可以进行下面操作。选择“高”，点击“下一步”。

输入密码，选择“完成”。请牢记输入的密码，如果你忘记了这个密码，你就无法使用这个证书。为了保证密码不容易被其他人猜测出来，建议不要使用生日、身份证号码或者电话号码等作为密码；建议你选择 8 位以上，由数字、字母以及标点符号共同组成的密码。

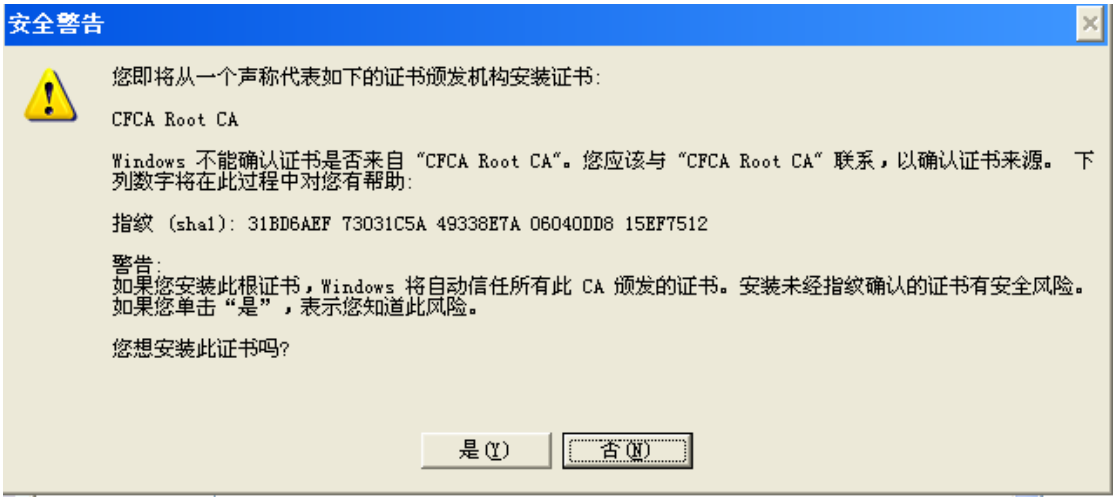
出现下图，表示安全级别已被设成高级，请选择“ 确定 ”，完成安全级别的设置。

选择“ 确定 ”，可能弹出“ 潜在脚本冲突 ”对话框（如果按照注意事项的要求，将 CFCA 的网站添加到“ 受信任的站点 ”，则不会出现此对话框），请选择“ 是 ”：



4）当出现下图，显示“您已经成功完成 CFCA 数字证书的安装”提示时，表明证书安装成功。

5）如果用户浏览器中没有安装 CFCA 的根证书，则会出现如下根证书的安装界面，选择“是”完成。



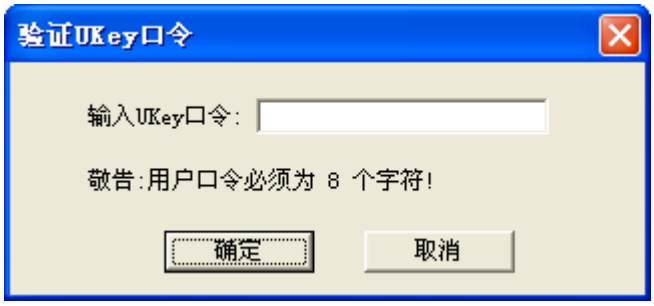
2.2 下载证书到 USB Key 中

USB Key 下载证书过程基本和浏览器下载过程基本相同。

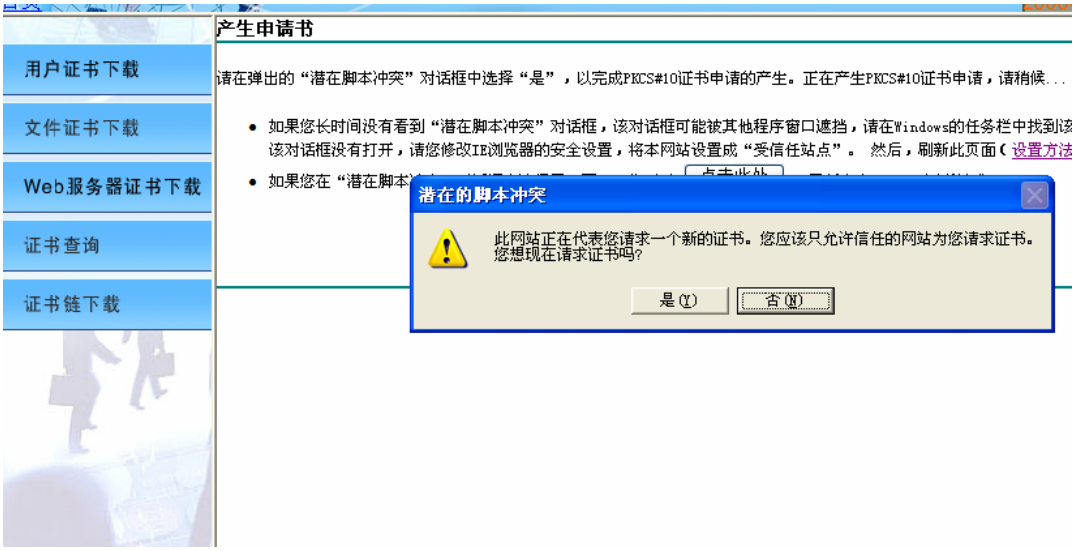
1）在第一个下载页面中，制证方式选择“USB 智能密码钥匙(CSP 方式)”，根据用户使用 USB Key 的型号选择相应的 CSP,如下图：

2）在使用 USB Key 下载时会出现要求输入 USB KEY 用户口令的对话窗口，输入已经获得的 USB Key 管理密码(即 pin 码)即可，如下图（某 USB Key 密码输入窗口为例，不同的

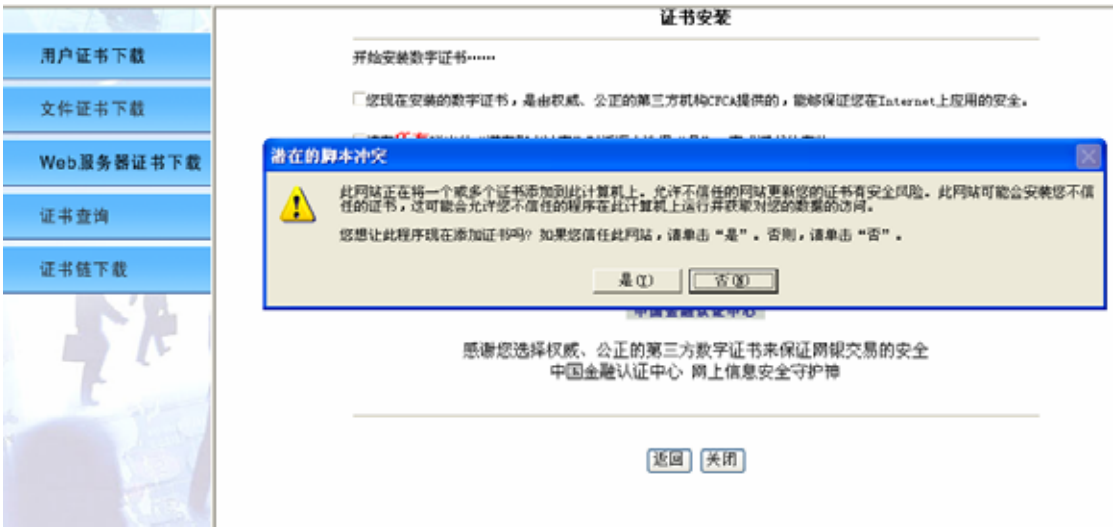
USB Key 的密码输入窗口是不同的）：



3）选择“ 确定 ”，产生证书请求，可能弹出“ 潜在脚本冲突 ”对话框（如果按照注意事项的要求，将 CFCA 的网站添加到“ 受信任的站点 ”，则不会出现此对话框），如图：



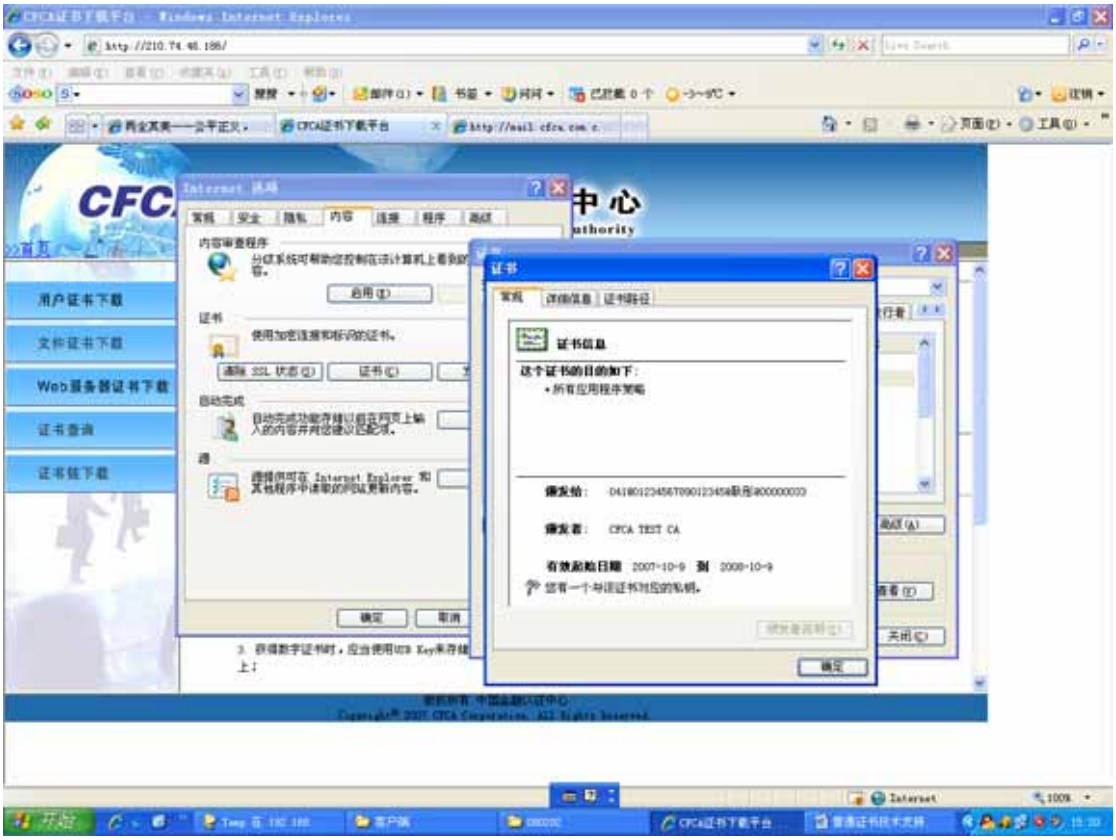
4）选择“ 是 ”，证书开始安装，可能弹出“ 潜在脚本冲突 ”对话框（如果按照注意事项的要求，将 CFCA 的网站添加到“ 受信任的站点 ”，则不会出现此对话框），如图：



5）选择“是”，当出现下图，显示“您已经成功完成 CFCA 数字证书安装”提示时，表明证书安装成功。

3 .证书查看

可以通过查看浏览器查看已经下载的证书：点击浏览器菜单“工具”->“选项”->“内容”->“证书”，选择要查看的证书点击查看按钮。如下图：



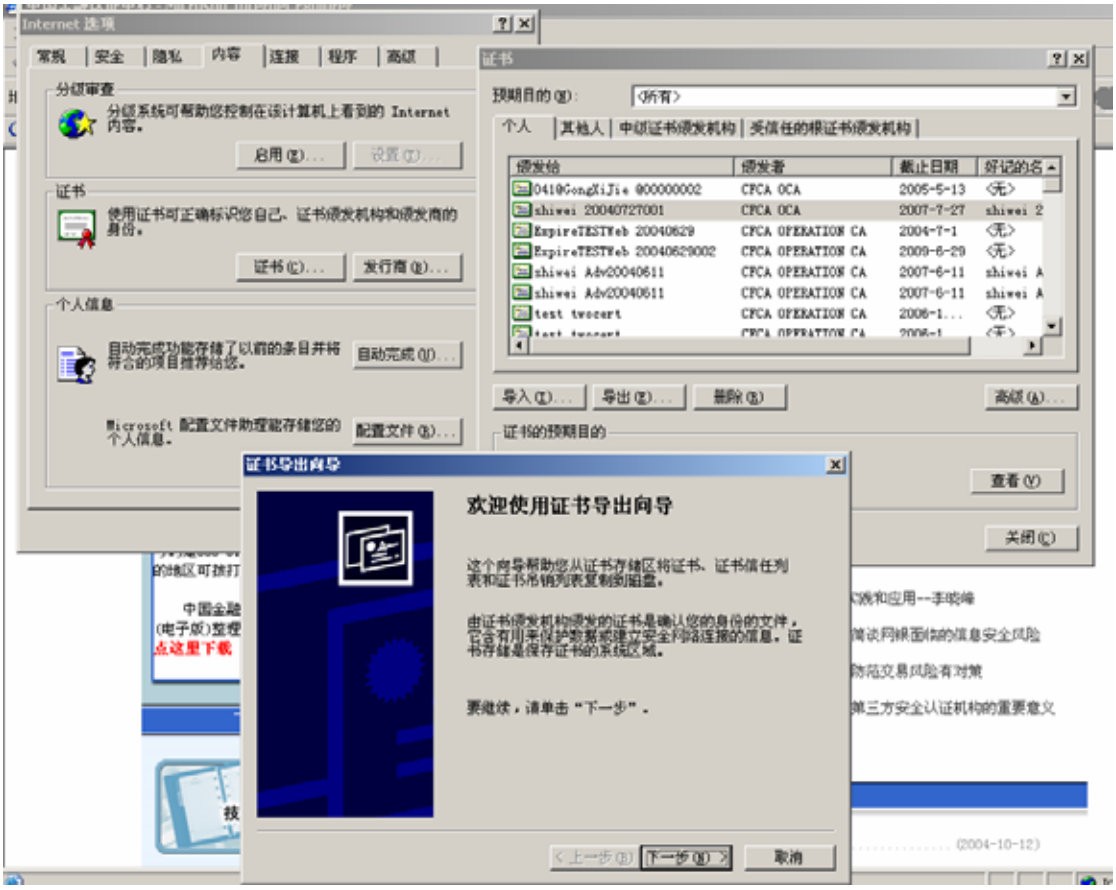
第二章、普通证书的使用

1.文件证书的备份和恢复

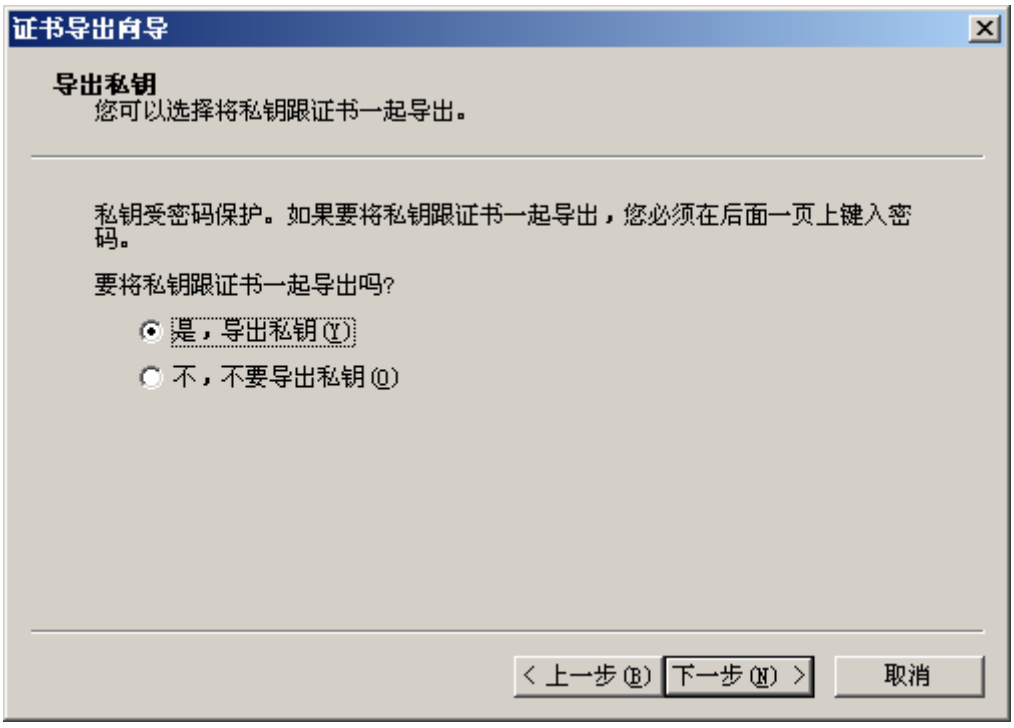
对于将证书下载到浏览器中的用户来说，很可能由于系统损坏或者浏览器软件损坏等情况导致证书丢失或损坏，所以需要做好证书的备份工作，并在需要的时候进行证书的恢复。下面详细介绍一下如何进行证书的备份与恢复。对于 USB Key 用户没有这个操作。

1.1 证书备份：

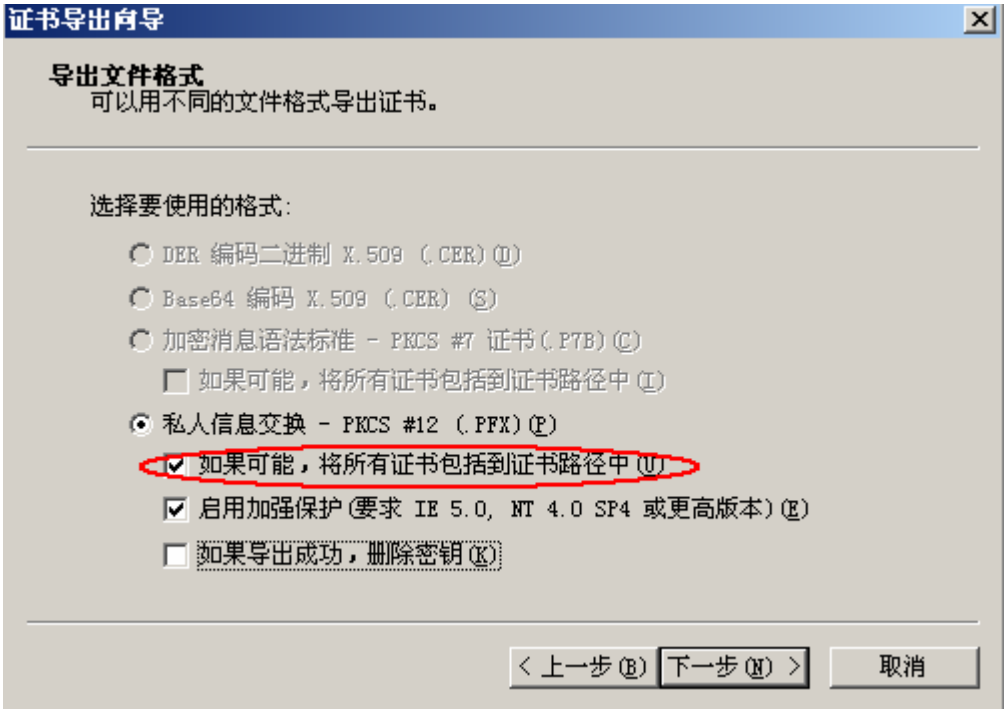
1) 首先打开 IE 浏览器，选择工具菜单->internet 选项->内容->证书，选择需要备份的证书，点击“ 导出 ”按钮，并选择下一步：



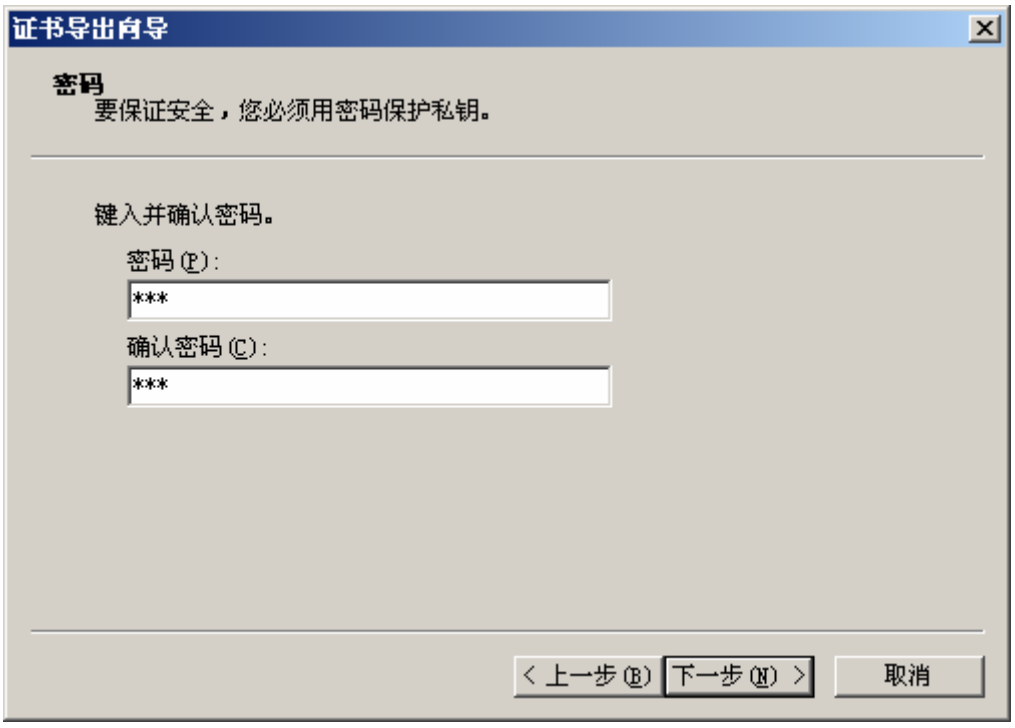
2)选择导出私钥选项，因为只有私钥跟证书一起导出，才能在安装此证书的机器上完成签名和解密工作,若导出私钥选项为灰色，不能选择，说明该证书无法被导出。然后选择下一步：



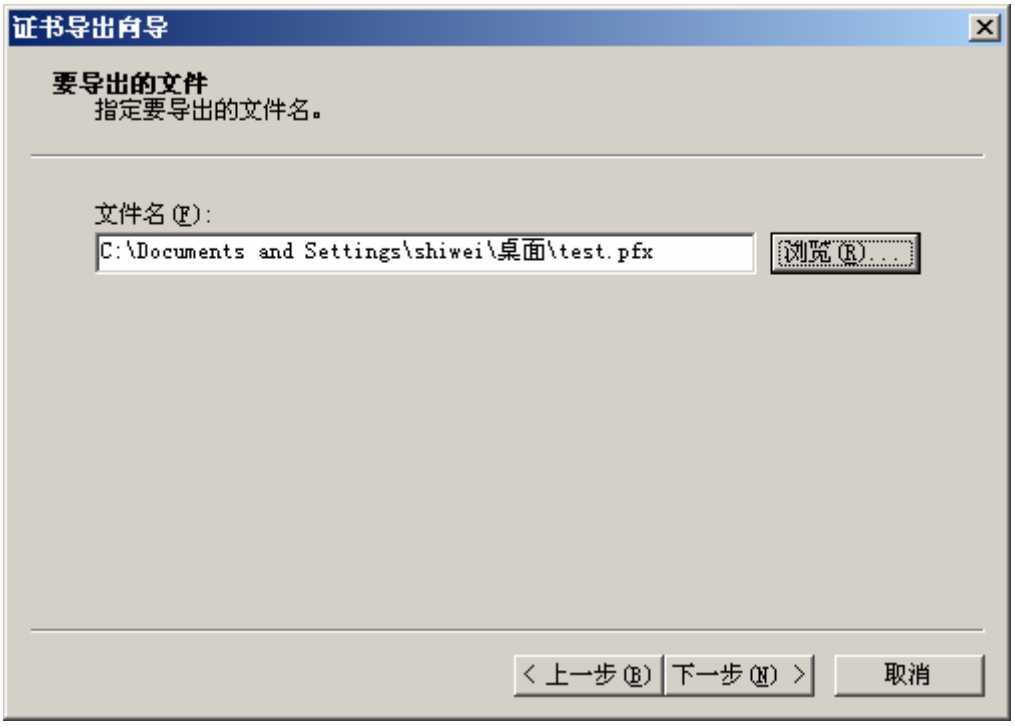
3)请将证书链随同证书导出，如同下面红圈的选择。这样可以使得安装此证书的机器无需单独安装证书链，其余选项如下图所示，然后选择下一步：



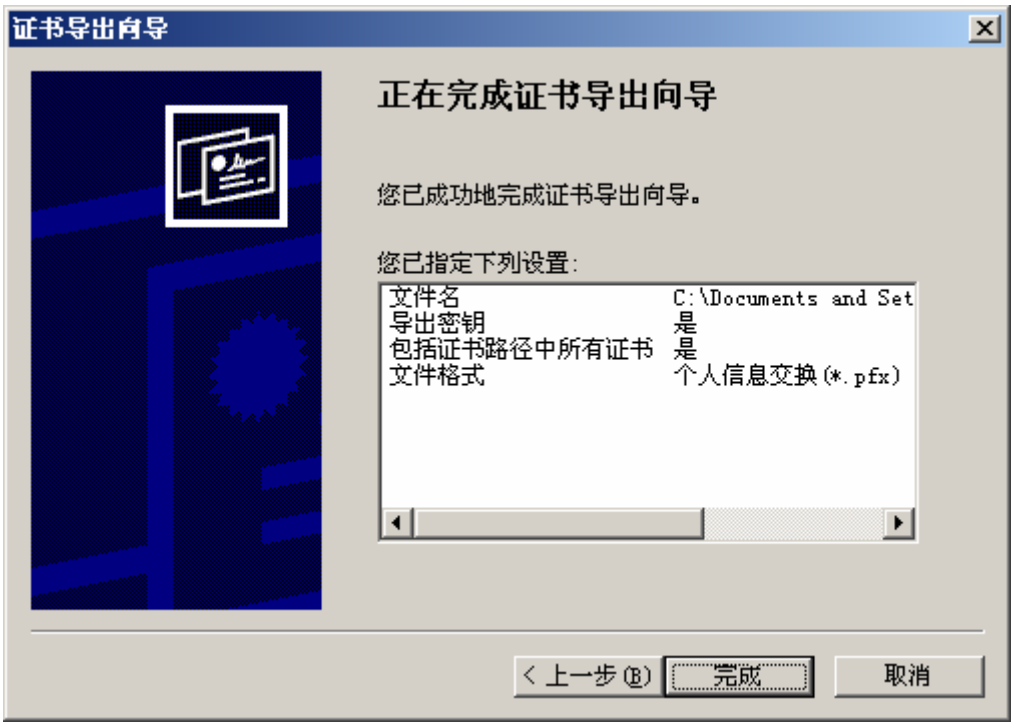
4)在证书密码设置对话框中设置密码，该密码是保护导出后的证书备份文件的，在做证书恢复时，需要使用该密码才能完成。设置完密码后选择下一步：



5)指定导出证书的名称和存放路径，选择下一步：

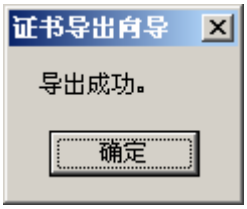


6)信息确认，选择完成：



7)点击 “ 完成 ”可能出现如下对话框，表明正在访问安全级别设置为中级以上的证书：

8)点击上面对话框的“ 确定 ”，出现如下对话框，则表明导出证书成功：

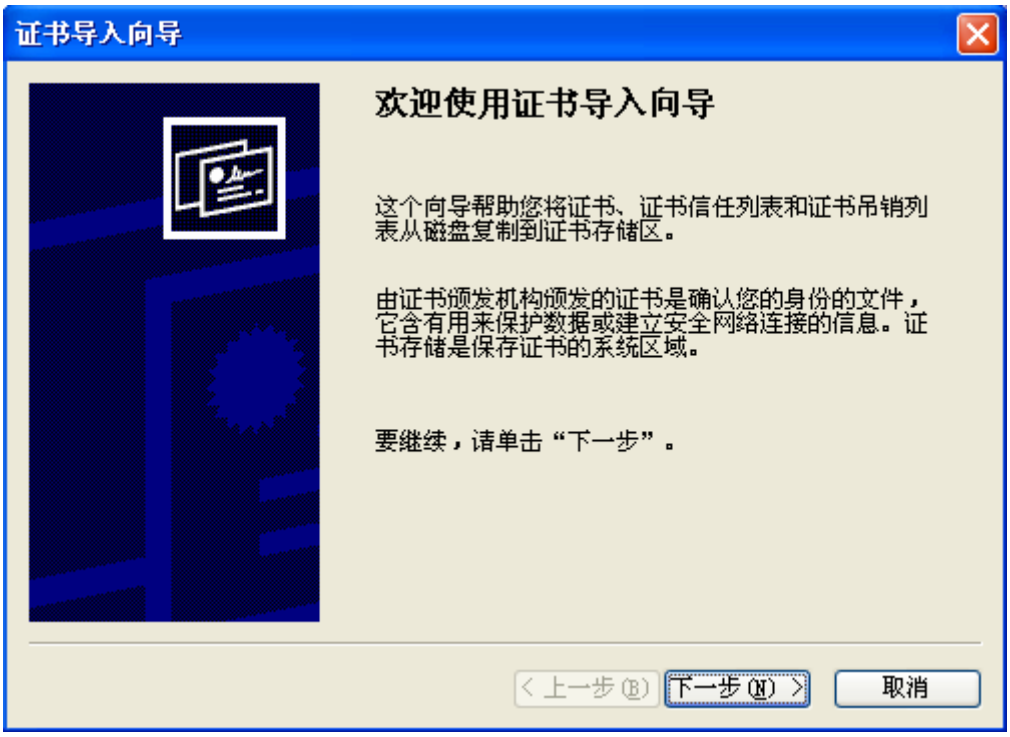


得到上述导出过程完成后的.pfx 文件，就可以在其它 PC 机上安装使用这张证书了。

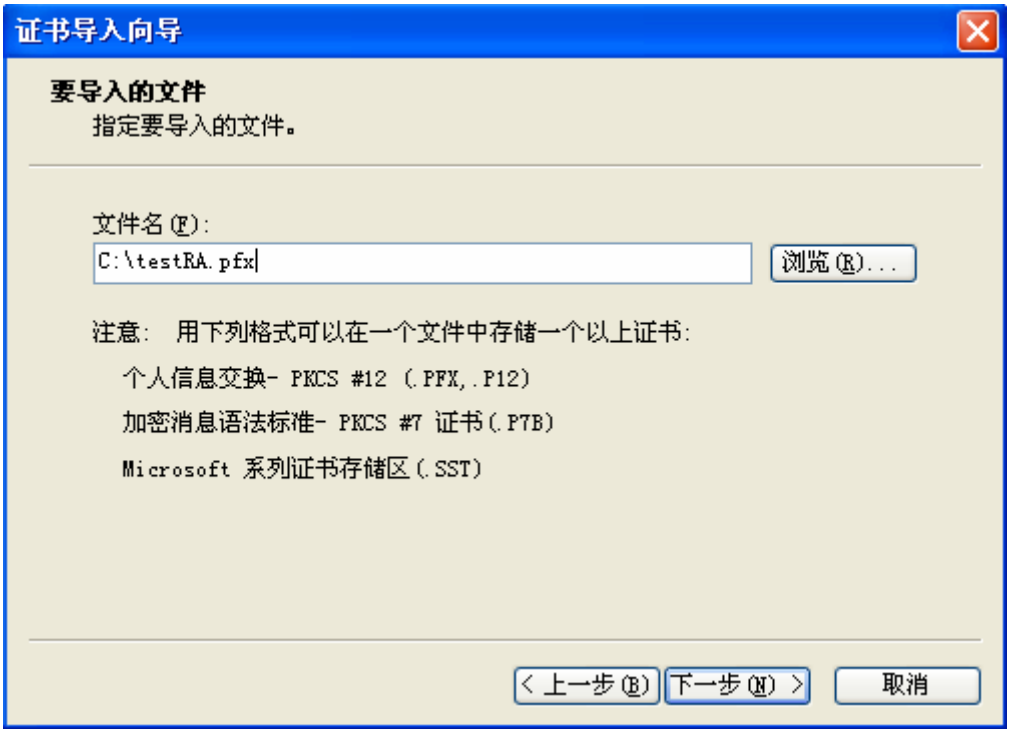
1.2 证书恢复

双击文件证书备份时得到的.pfx 文件或者点击右键选择“安装 pfx”，启动证书导入向导。不含私钥的 cer 文件安装见前面证书链安装一节。下面详细介绍一下证书恢复操作：

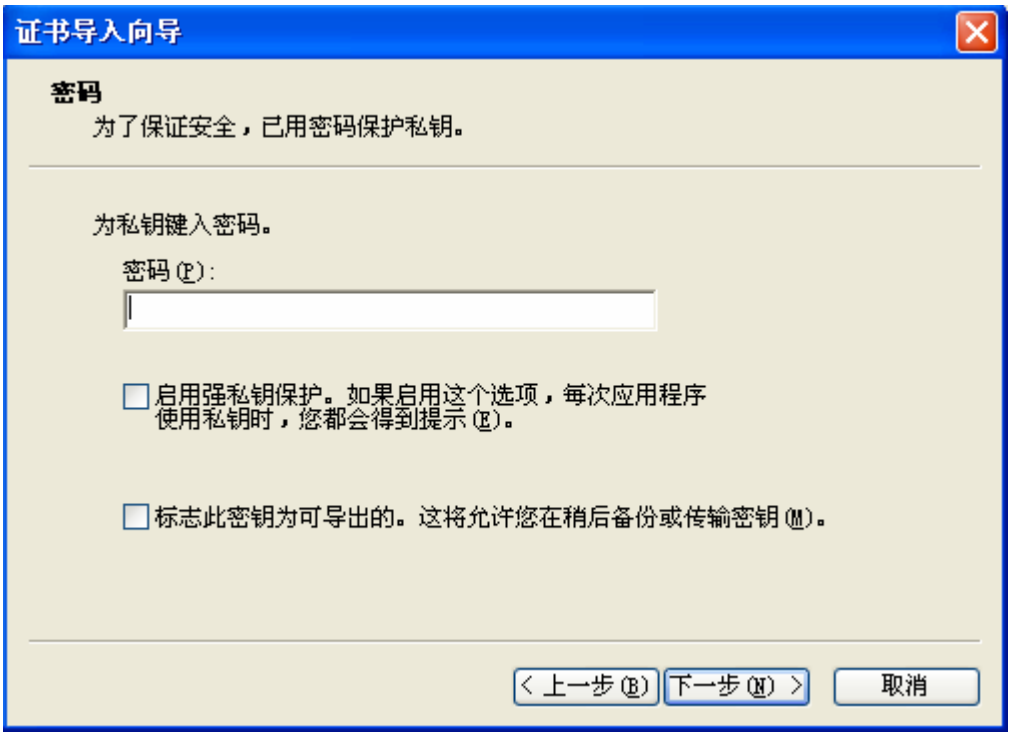
1)双击文件证书备份时得到的 pfx 文件或者点击右键选择“安装 pfx”，启动证书导入向导如下图，选择下一步：



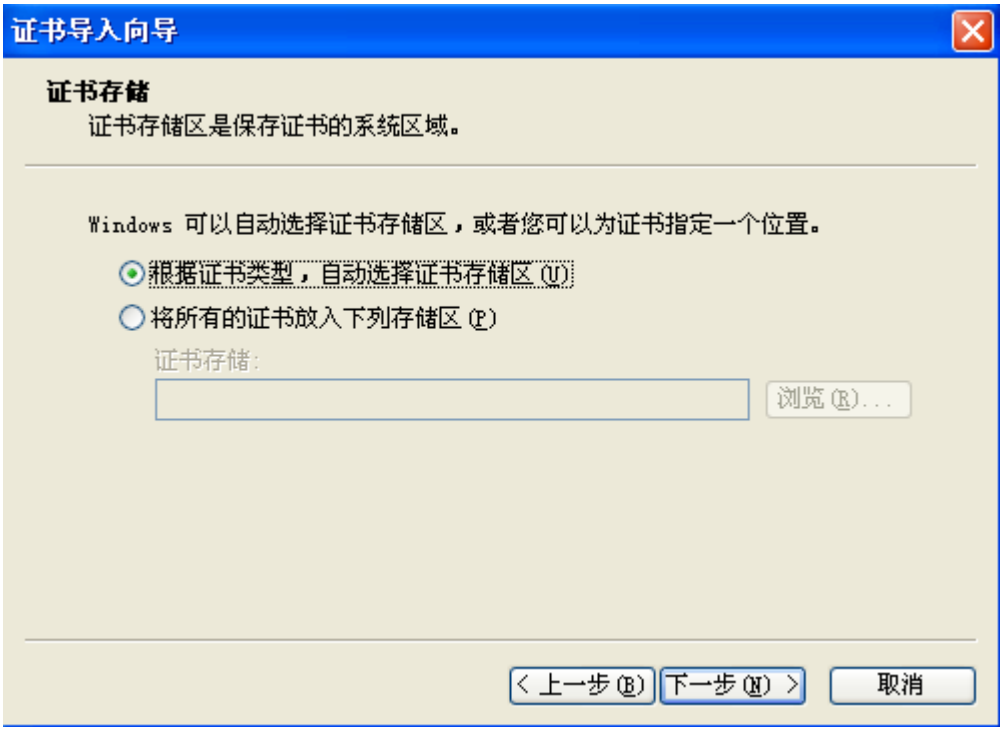
2)选择下一步：



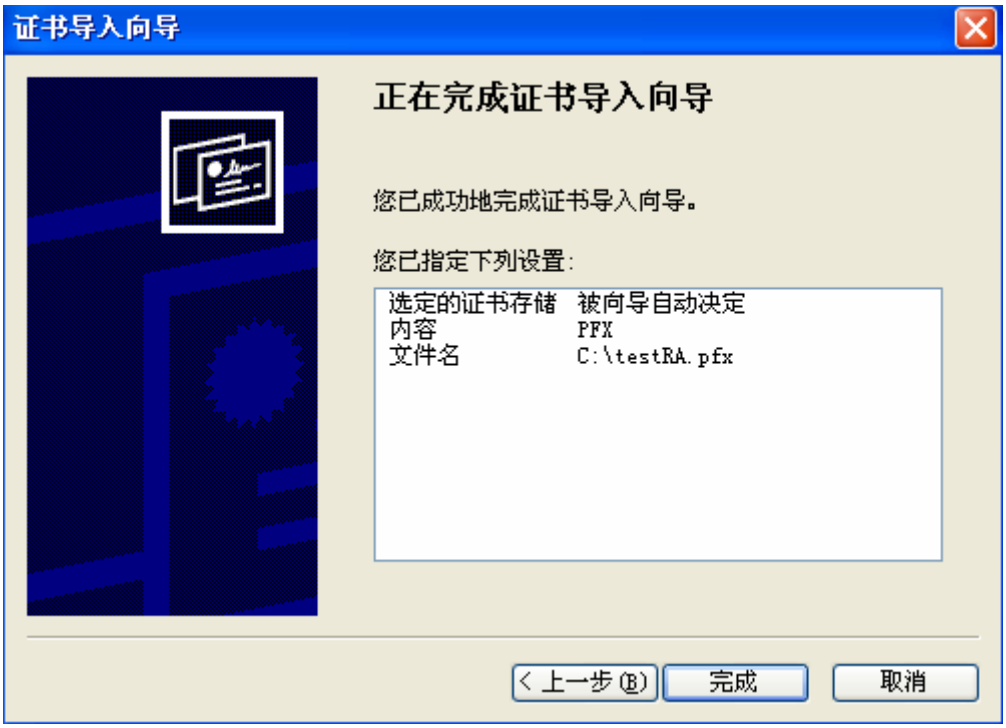
3) 在密码对话框输入证书备份时设置的密码，若希望证书导入到浏览器中能被再次导出，则可以选中“标志此密钥为可导出的”选项，然后点击下一步：



4) 选择下一步：

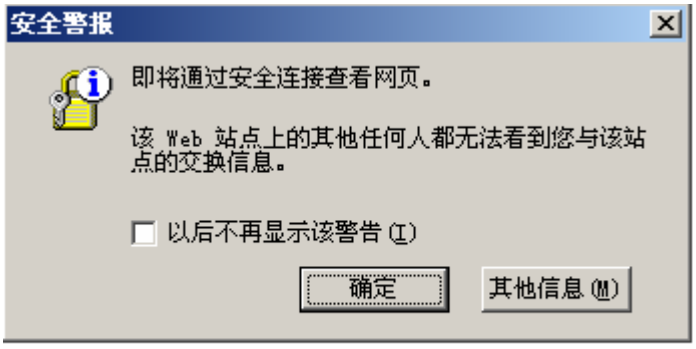


5) 选择完成，则安装结束。



2.关于普通证书应用中对话框的简单说明

一、用户访问 https 的网站过程中，在输入网站地址后，通常会弹出如下对话框：



这是 IE 本身的设置造成的。如果用户不希望每次访问 https 的站点都有这样的提示，只要勾中“ 以后不再显示该警告 ”即可。

二、用户访问 https 站点后将首先选择证书，选择证书之后以及每次使用证书都可能出现如下对话框：

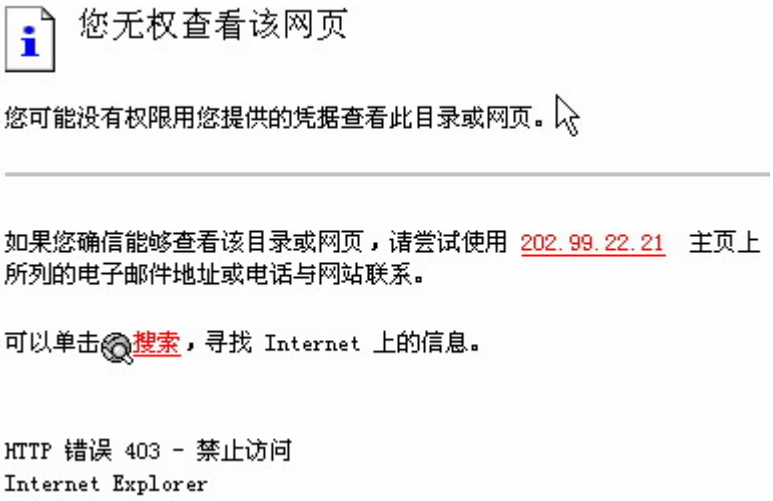
此对话框是提醒用户某应用程序将使用证书。

此对话框的产生是在下载证书过程中设置的安全级别决定的。默认是中级，还有高级、低级

可以选择。有关安全级别的设置请参考下图：
如果选择“ 高 ”，则每次使用证书都会弹出对话框要求输入密码：

输入密码错误则会有如下提示：

最终导致无法访问页面：



第三章、普通证书的管理

对于普通证书来说经常会有以下相关管理操作：

1）证书换发

当用户证书快过期或已经过期时，为用户重新生成一张证书操作称为证书换发。证书 DN 不变。如果证书还没过期，则新换发证书的失效时间在旧证书失效时间基础上加有效期；如果证书已经过期，则新换发证书的失效时间在当前时间基础上加有效期。原证书会被自动撤销。

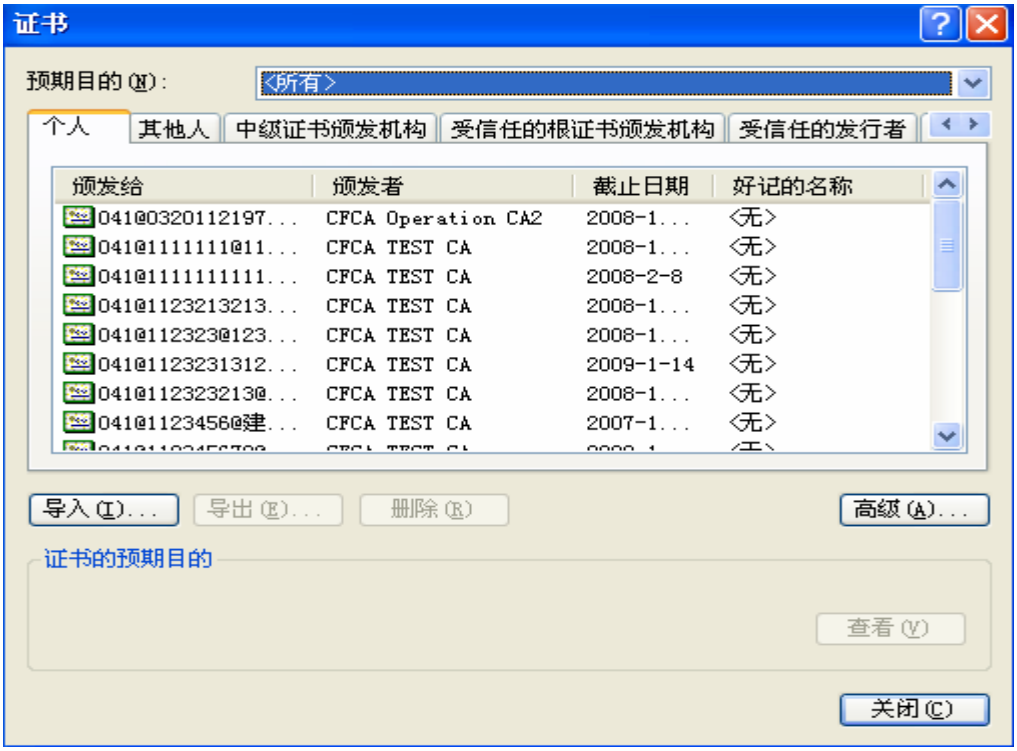
2）证书补发

当用户的证书丢失或者装载证书的介质损坏后，需要重新发放证书的操作称为证书补发。证书 DN 不变，证书的生效时间和失效时间都不变。原证书会被自动撤销。

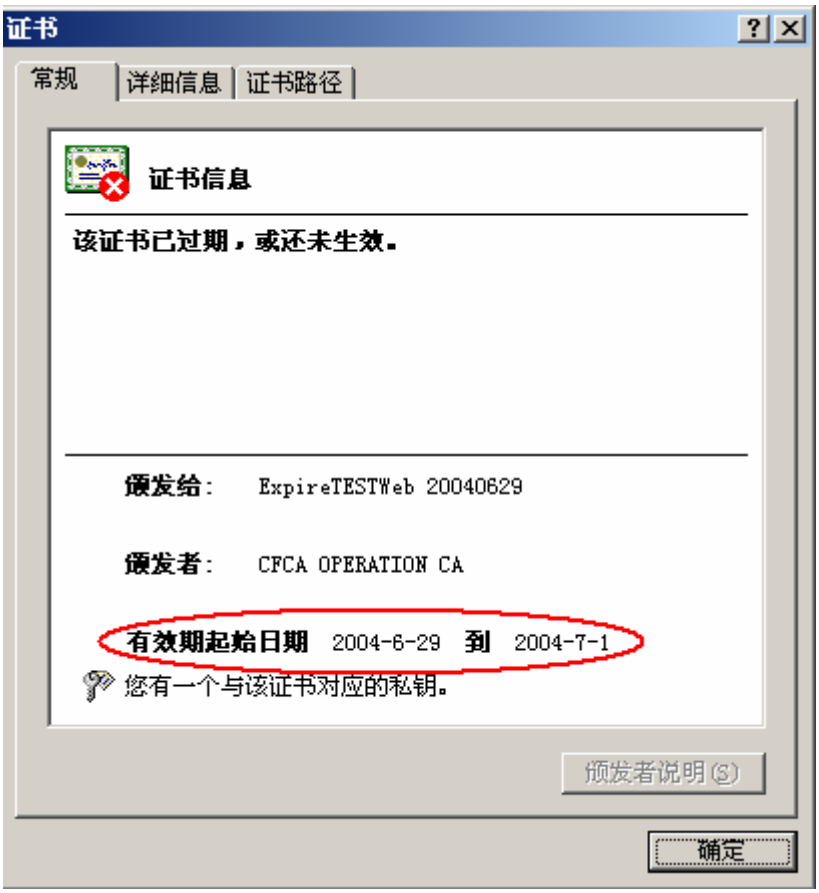
3）证书吊销

如果用户证书失秘或者用户不想继续使用该证书了，则可以做证书吊销操作。被吊销证书将放到 CA 的 CRL 列表里面。

对于普通证书来说，我们还可以通过浏览器提供的功能来查看普通证书的相关信息比如证书有效期等。打开浏览器，打开工具菜单->internet 选项->内容->证书如下图：

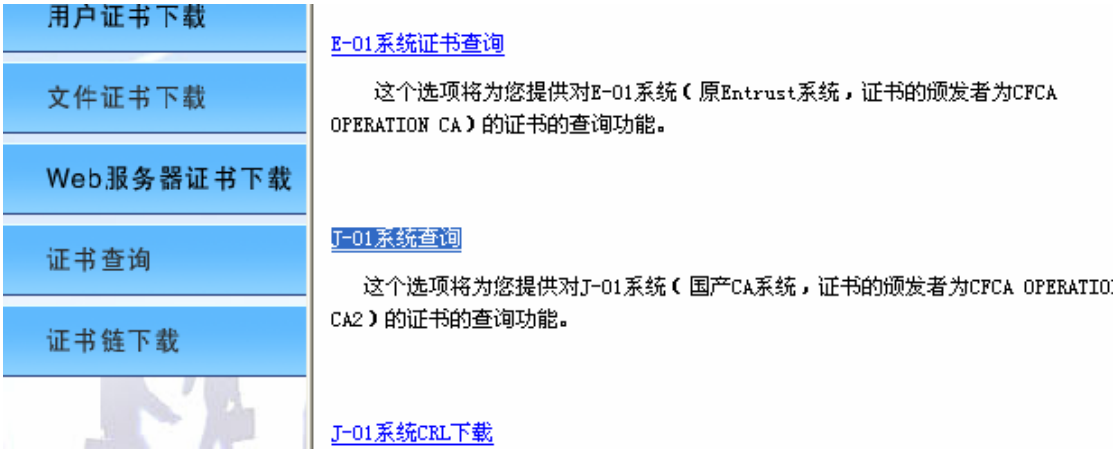


选择需要的证书选择如下图：

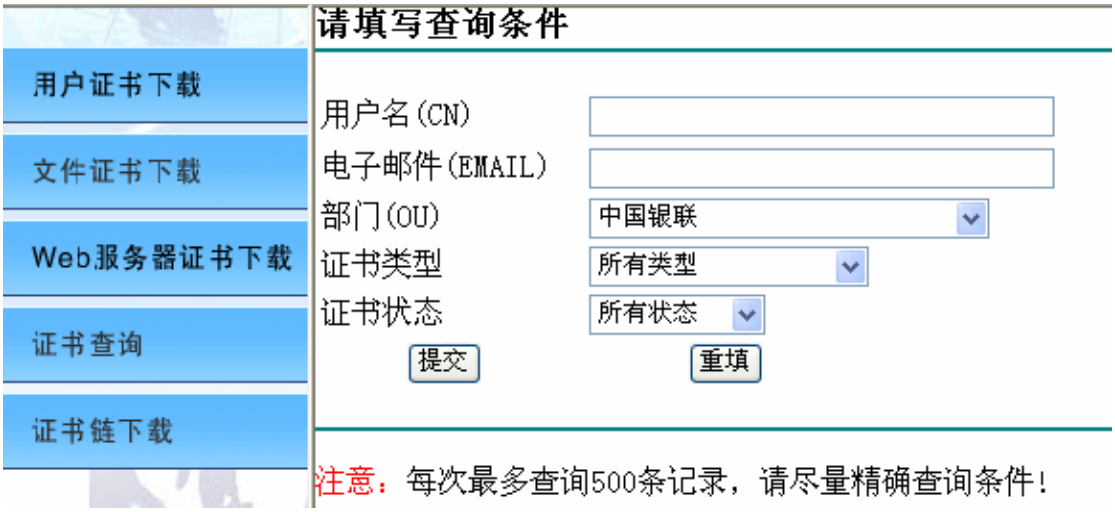


第四章、普通证书的查找

CFCA所发放的所有公钥证书都公布在CFCA的目录服务器上，并对外提供查询。具体查询网址为：http://www.cfca.com.cn/tongyi，选择左侧“证书查询”链接，如下图：



用户的证书所属系统需要用户咨询自己证书的发放机构，下面以 J-01 系统的用户为例，演示如何查找别人的证书。点击“ J-01 系统查询 ”链接，如下图：



填入相应的查询条件，点击提交后如下图：

证书查询结果：

共查到500条，本次查到20条，剩余480条。点击查看详细内容。

1. 041@01111111111111111111@ccb_admin@00000015
2. 041@03333333333333333333@koal@10000019
3. 041@01111111111111111111@ccb_admintest@00000036
4. 041@0123456789012345@yang1@00000001
5. 041@01111111111111111111@uuuuu@00000037
6. 041@01111111111111111111@koal001@00000001
7. 041@02222222222222222222@koal002@00000002
8. 041@03333333333333333333@koal003@00000003
9. 041@04444444444444444444@koal004@00000004
10. 041@05555555555555555555@koal005@00000005
11. 041@06666666666666666666@koal006@00000006
12. 041@07777777777777777777@koal007@00000007
13. 041@08888888888888888888@koal008@00000008

选择自己需要查看的证书，点击相应链接，如下图：

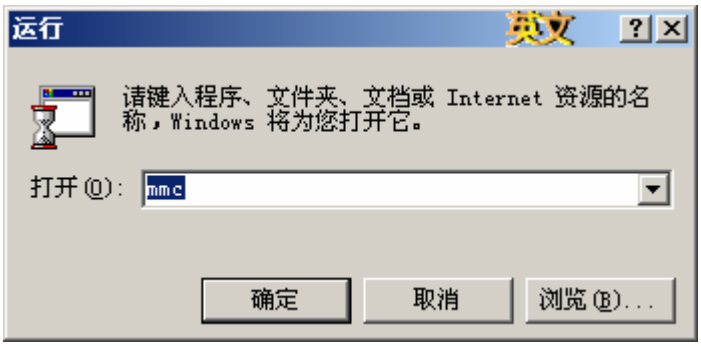
用户信息摘要

甄别名	cn=041@01111111111111111111@ccb_admin@00000015, ou=Customers, ou=ccb, o=CFCA TEST CA, c=CN		
证书类型	**证书状态**	**证书**	**CRL**
未知	证书使用中	下载证书	下载CRL

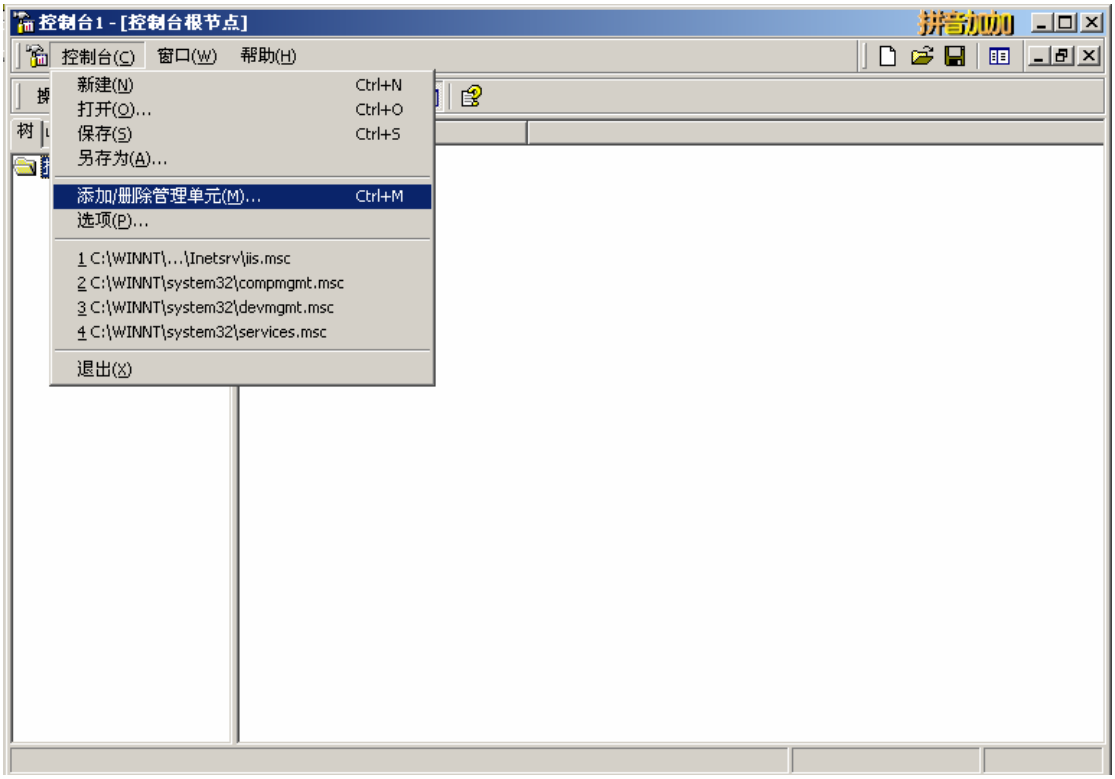
附录

在某些情况下，我们还可以通过证书管理单元来管理证书：

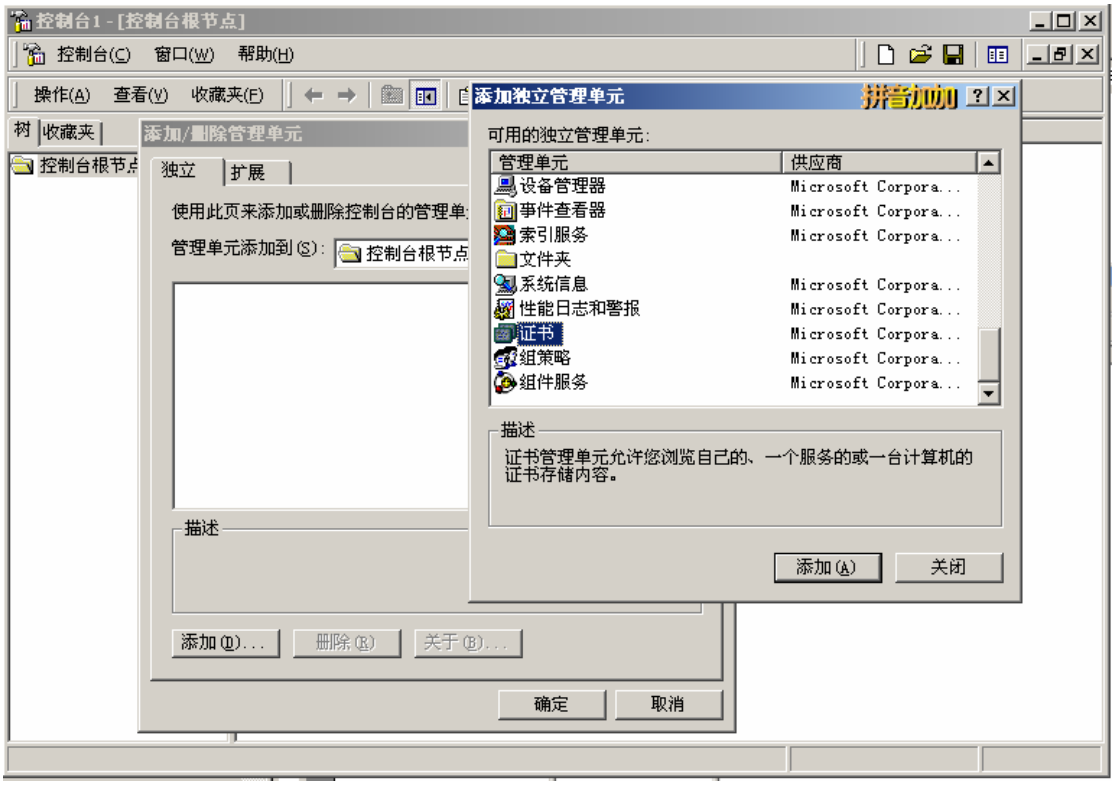
1)点击“开始”→运行，输入 mmc，打开控制台界面如下图：



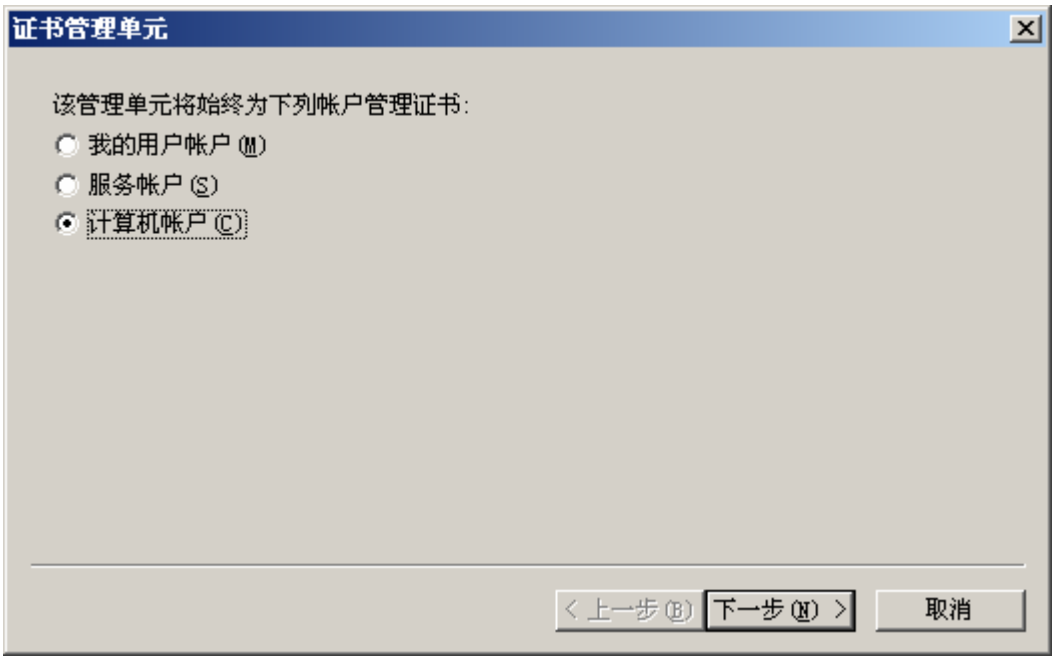
2)添加证书管理单元



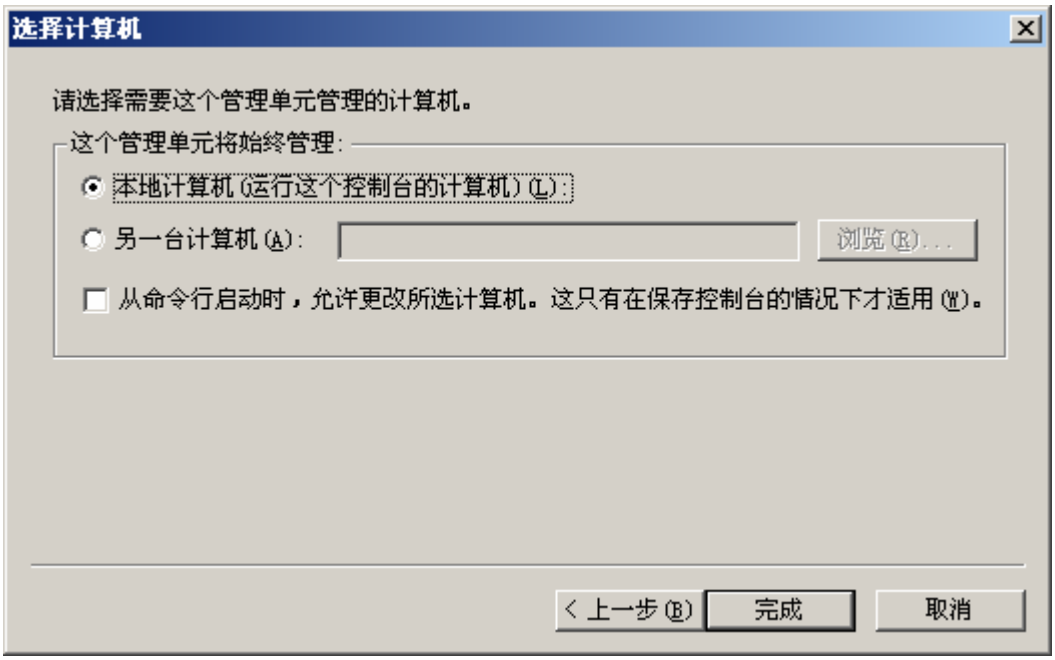
3)点击添加，选择“证书”



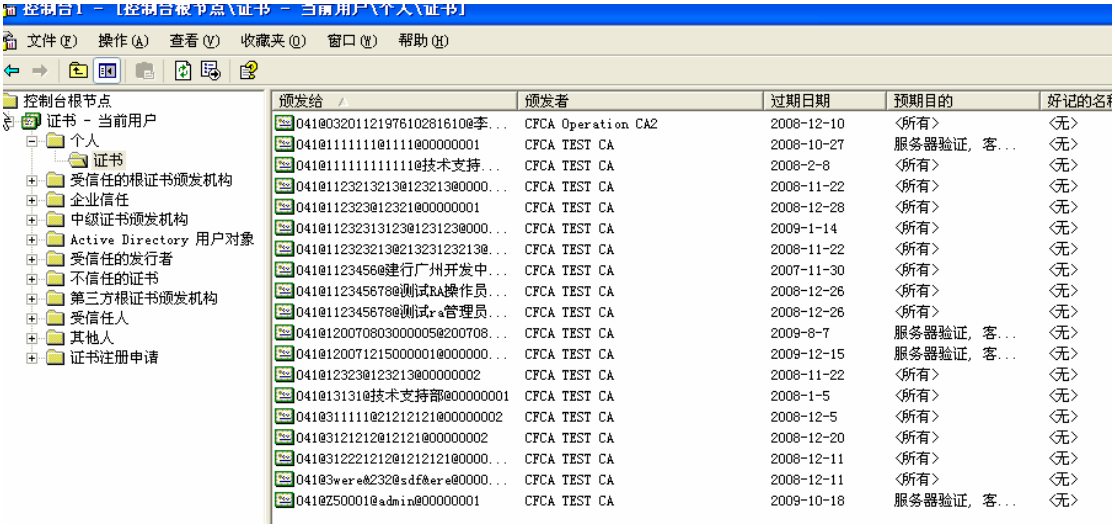
4)根据需要，可以选择“我的用户账户”或者“计算机账户”，选择下一步：



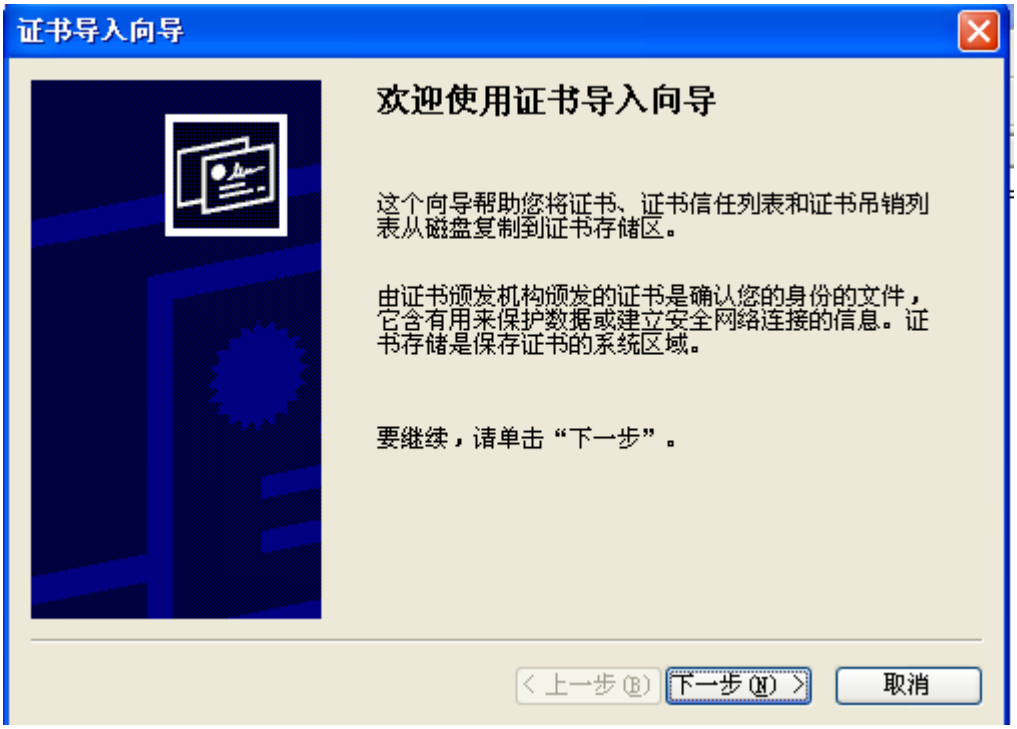
5)选择完成。



现在就可以通过证书管理单元来管理查看本机证书了：



我们也可以通过该工具导入一个证书，选择“ 操作 ”→“ 所有任务 ”→“ 导入 ”如下图：



下面的导入操作和前面证书备份中介绍的是一样的。