

证书常见问题解决办法

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

1. 普通证书下载方面的问题

1) 下载普通证书时报错：-3274，安全协议失败

原因：造成此错误的原因通常是由于参考号和授权码没有对应。参考号和授权码颠倒填写还会引起-3290 Invalid Authentication Token 的错误信息。

解决办法：检查用户的参考号授权码的对应是否正确。

2) 下载或者恢复普通证书时，IE 报告包含" 1B6 "的错误提示

原因：1、使用 IE6.0sp1 以前版本的用户得到此错误的原因可能是 IE 缺少必要的补丁，需要打补丁。需要注意：此时下载普通证书的时候只罗列“Microsoft Base Cryptographic Provider v1.0”，就会出现上述错误。

2、IE 禁止了脚本运行，导致不能正常执行页面包含的控件。此时的 CSP 选项的内容只有“Microsoft Base Cryptographic Provider v1.0”。常见于 IE7.0。

解决办法：1、针对原因 1，登录 CFCA 网站

(<http://www.cfca.com.cn/cda-docs/1b6patch.html>) 根据操作系统选择补丁版本，下载并安装该补丁。

2、针对原因 2，需要将下载证书的站点加入受信任的站点，并根据页面的提示选择执行控件。正常的情况下，CSP 选项的内容应为“Microsoft Enhanced Cryptographic Provider v1.0”。

3、个别情况可以通过以下方式解决：点击“开始”->“运行”，输入“regsvr32 xenroll.dll”，注册 xenroll.dll 控件。

3) 下载普通证书，报“No keypair has been created.Please make sure that you using internet Explorer 3.0+,and that the required.DLL is properly installed on the server machine.See your administrator for details.”错

原因：1、IE6 sp1 以前版本的操作系统，没有安装 323172 补丁。

2、IE 禁止了脚本运行，导致不能正常执行页面包含的控件。此时的 CSP 选项的内容只有“Microsoft Base Cryptographic Provider v1.0”。常见于 IE7.0。

解决办法：a、针对原因 1，需要登录 CFCA 网站（

<http://www.cfca.com.cn/cda-docs/1b6patch.html>）根据操作系统选择补丁版本，下载并安装该补丁。

b、针对原因 2，需要将下载证书的站点加入受信任的站点，并根据页面的提示选择执行控件。正常的情况下，CSP 选项的内容应为“Microsoft Enhanced Cryptographic Provider v1.0”。

4) 普通证书下载时报“-1666”错

原因：1、参考号输入错误。

2、选择的是其他 CA 的证书下载中心地址。

3、证书已下载。

解决办法：

对于原因 1 检查参考号是否正确。

对于原因 2 确定是在<http://www.cfca.com.cn/tongyi>输入参考号下载证书。

对于原因 3 证书已下载情况如下：

以民生银行个人网银系统为例(E-01 系统证书，对于 J-01 证书也可用类似方式解决)

第一步：核实下载证书所使用的参考号、授权码是否正确。

注意检查下载证书时录入的参考号、授权码是否正确。

对于 E-01 系统证书：

1) 参考号都是数字

2) 授权码为数字和字母的组合，每四个为一组，共三组，中间以英文输入法下的减号“-”连接。

第二步：检查是否已经下载。

1、在下载证书报错的机器上，打开浏览器，点击“工具”——“Internet 选项”，如下图所示：

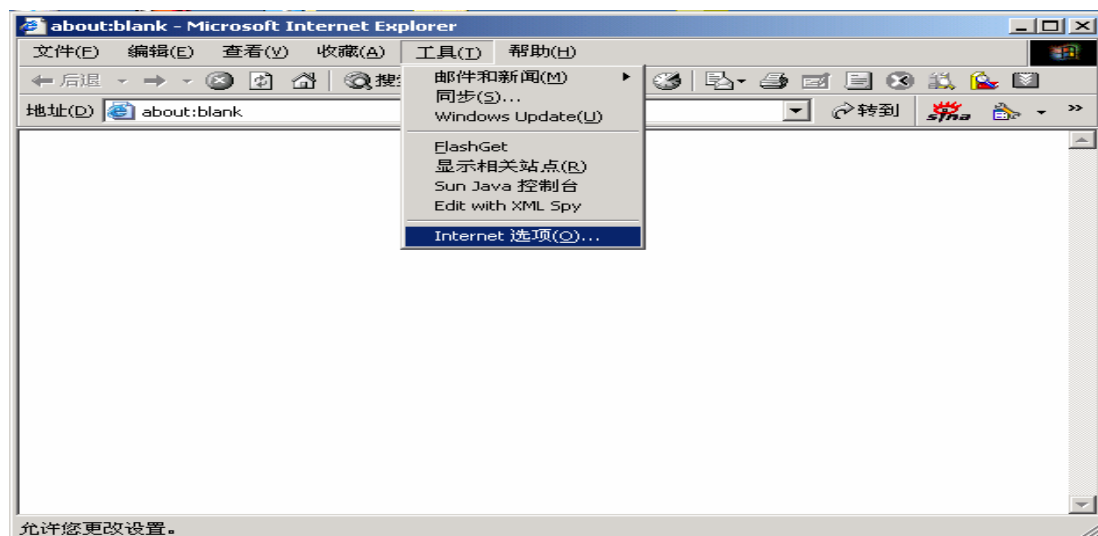


图 2

2、进入“选项”以后，点击“内容”，如下图所示：



图 3

3、点击“证书”，注意查看。

- 1) 如果在“个人”项中如下图所示为空，则表示用户证书没有下载到浏览器中。请参考“[第三步 重新下载证书](#)”中的操作。

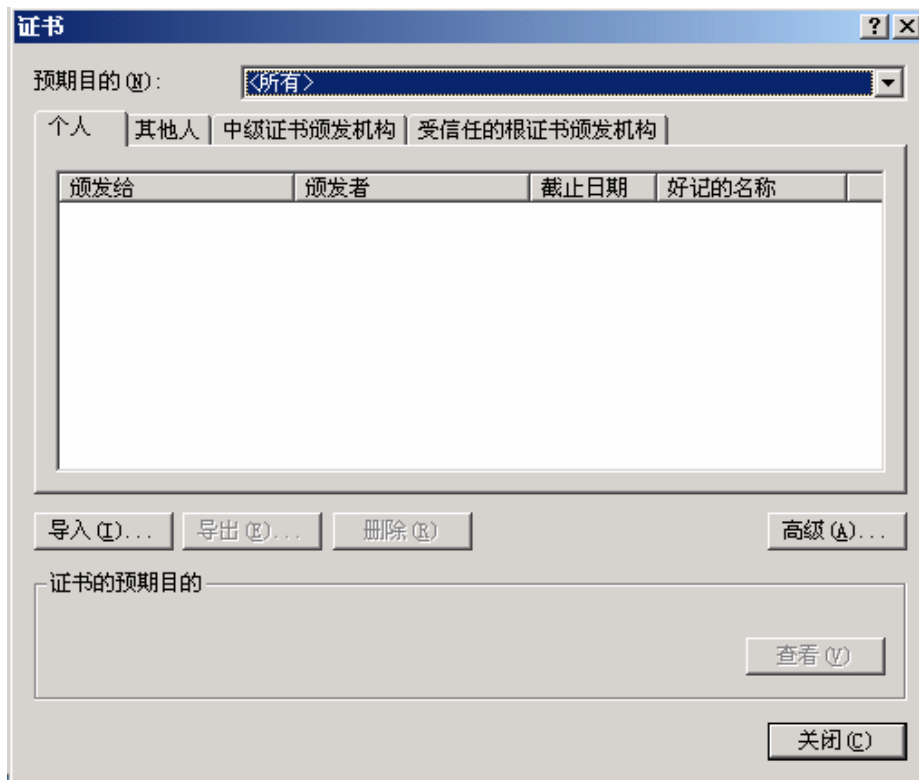


图 4

2) 查看用户证书是否为民生银行的证书：如果在“个人”项中有证书，并且其颁发者为“CFCA Operation CA”如下图所示，则表明用户已经下载了 CFCA 的证书，并请核对“颁发给”中的内容与您的 DN（部分银行会在给用户的印有参考号、授权码的下载凭证中，印有 DN。比如民生银行的下载凭证如下所示：如果用户不知道自己的 DN，则需要用户与银行联系，得到自己的 DN 后再与 4008809888 热线联系。）

民生银行证书下载凭证的大致格式： 操作员号：2002240321301

姓名：王红 授权码：7VHP-SQKB-DC43 参考号：81344314

DN : cn=11234567890test@00000001,ou=Customers,ou=CMBC,o=CFCA Operation CA,C=CN

备注：个人用户证书请在 14 天内下载证书，逾期需重新申请。

核对“颁发给”中的内容与您的 DN 是否一致，如果一致说明您的证书已经下载。

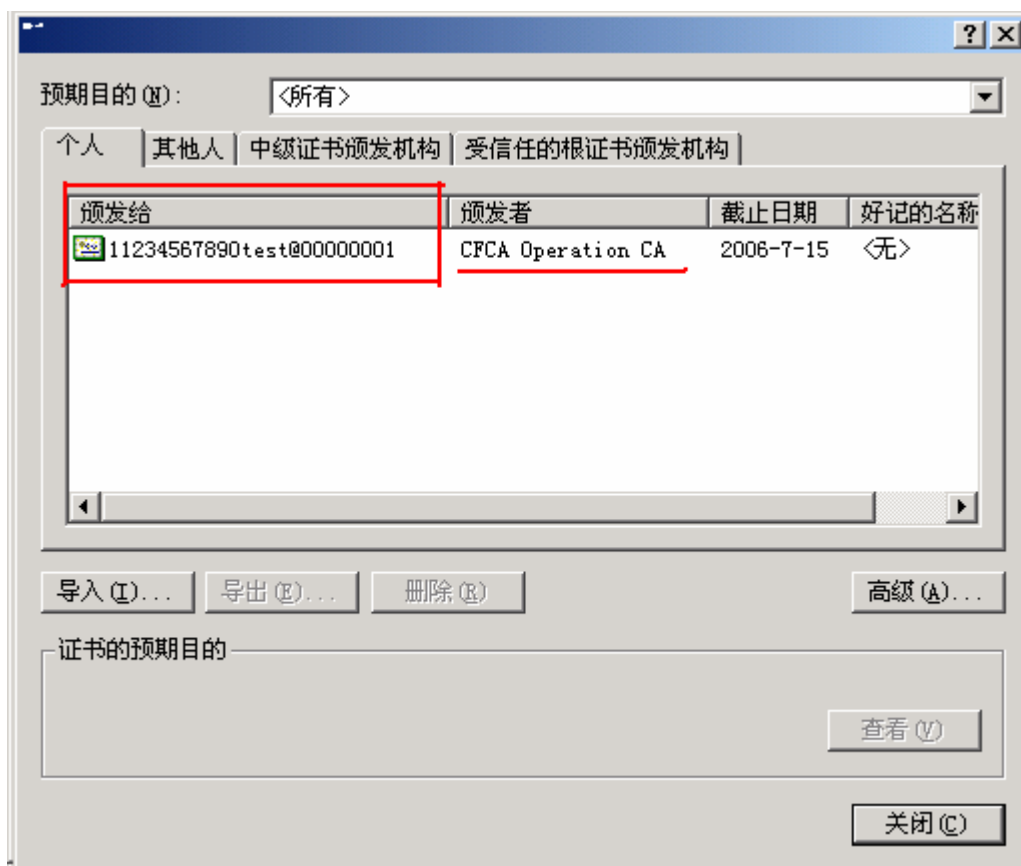


图 5

另外请注意：如果此处显示已经有证书，或者有多张证书，可能是已经使用了一段时间的网银或使用了多家银行的网银，这就需要仔细核对用户的 DN 以及“截止日期”判断存在的证书是否是这次下载的证书。截止日期 = 证书下载日期 + 2 年。

即如图 5 所示，则表明证书已经下载，证书相关的部分已经完成。可以登录相应的网上银行系统。

如：民生银行的个人网银：<https://business.cmbc-online.com.cn:8102/>进行网银的相关操作。

如果不是，则表示证书没有下载，请参考“[第三步 重新下载证书](#)”

第三步：重新下载用户证书。

1、查找证书（这个过程可由 4008809888 热线或银行的支持服务人员完成。）

1) 支持服务人员登录 <http://www.cfca.com.cn/tongyi>，点击“查找证书”，如下图所示：

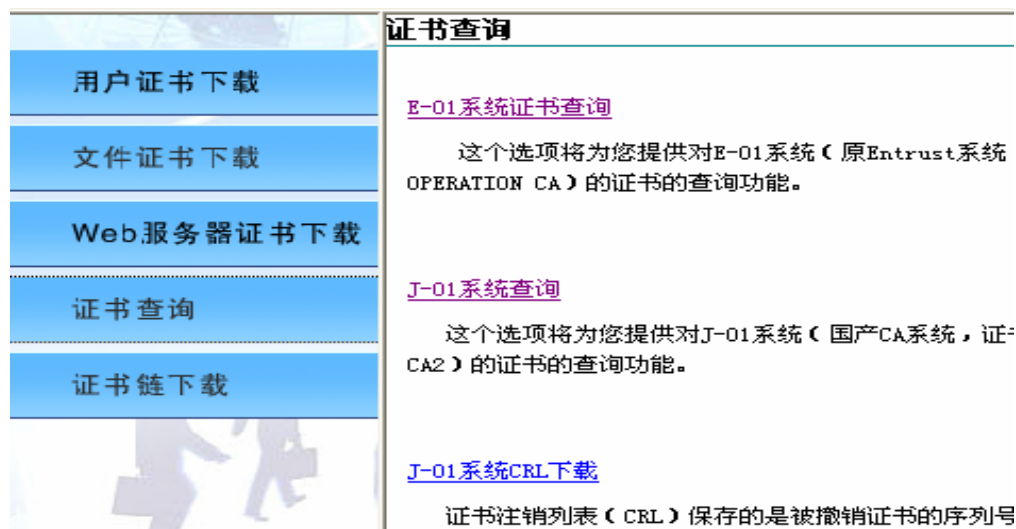


图 8

2) 由于民生银行是使用 E-01 系统，故点“E-01 系统证书查询”如下图：

从目录下载证书—第一步

利用证书搜索器从目录中下载证书共有三步。第一步(此页)，你需要确定你想得到的证书的名称、e-mail地址（任选）。字段之中的星号(*)是让证书搜索器去搜索在DN中包含有这种属性的证书。注意：一次最多只能返回200个用户信息。

姓名：	<input type="text" value="*"/>	(必需)
E-mail地址：	<input type="text"/>	(可选)
搜索条件：	<input type="text" value="ABC"/>	<input type="button" value="v"/>
<input type="button" value="搜索"/> <input type="button" value="重设"/>		

3) 将 DN 中 cn=后面到第一个逗号前面的部分在“姓名”部分输入。在搜索条件中选择“CMBC”，如图 9 所示：

证书下载凭证的大致格式：(注意将红色的部分对应填写到网页中的“姓名”部分)

操作员号：2002240321301

姓名：王红

授权码：7VHP-SQKB-DC43 参考号：81344314

DN：cn=11234567890test@00000001,ou=Customers,
ou=CMBC,o=CFCA Operation CA,C=CN

备注：个人用户证书 请在 14 天内下载证书，逾期需重新申请。

从目录下载证书－第一步

利用证书搜索器从目录中下载证书共有三步。 第一步(此页)，你需要确定你想得到的证书的名称、e-mail地址（任选）。 字段之中的星号（*）是让证书搜索器去搜索在DN中包含有这种属性的证书。 注意：一次最多只能返回200个用户信息。

姓名:	<input type="text" value="11234567890test@000000"/>	(必需)
E-mail地址:	<input type="text"/>	(可选)
搜索条件:	<input type="text" value="CMBC"/>	▼
<input type="button" value="搜索"/> <input type="button" value="重设"/>		

图 9

4) 输入完成后点击“搜索”。出现如下图所示的页面：

从目录下载证书－第二步

证书搜索器查找到以下符合条件的用户。请在以下的超级链接中选择一个

 ou=CMBC,o=CFCA Operation CA,c=CN - 1 entry(ies) found

 [cn=11234567890test@00000001, ou=Customers, ou=CMBC, o=CFCA Operation CA, c=CN](#)

图 10

5) 选中“cn=112345* , ou=Customer,ou=CMBC,o=CFCA Operation CA”，点击进入，选择“displayed as PEM encoding of certificate in PKCS #7”，如图 11 所示。

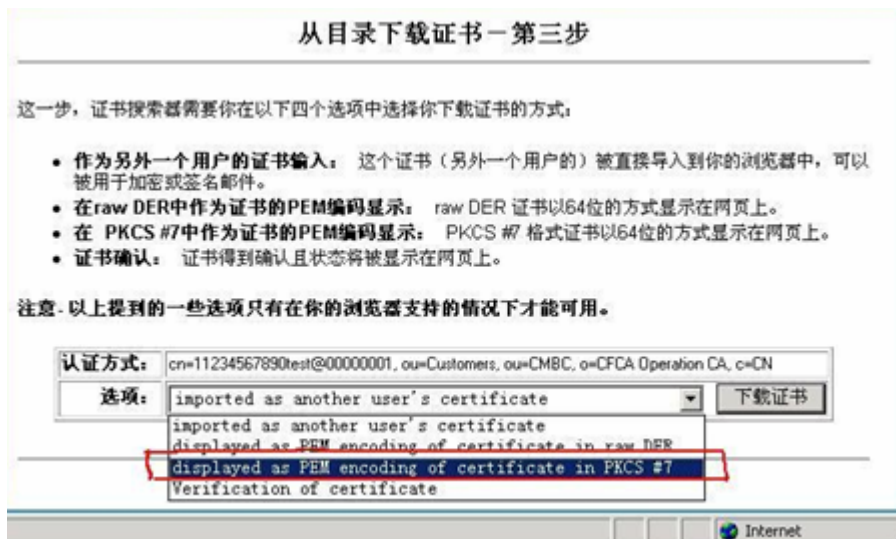


图 11

a) 然后点击“下载证书”，出现如下图所示页面：



图 12

b) 选择“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”之间的部分，进行复制，如图 13 所示：

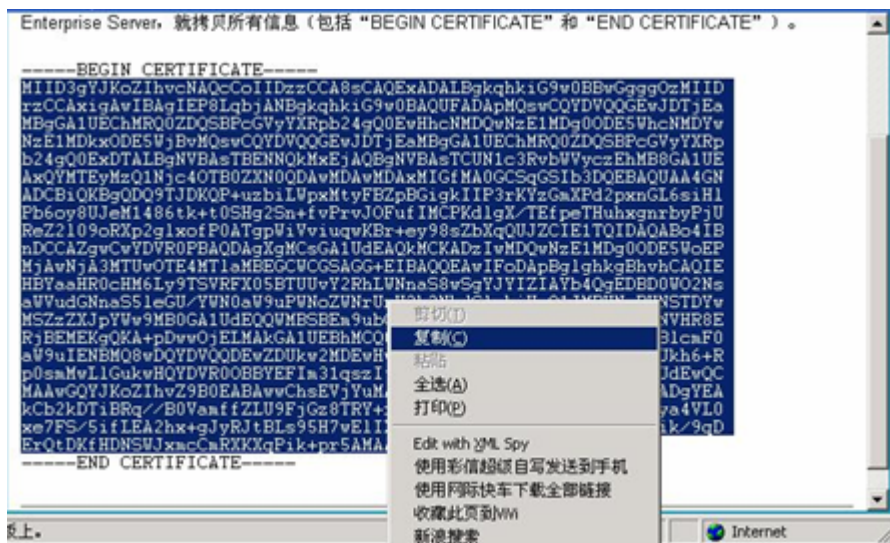


图 13

打开一个记事本，将刚才页面中复制的内容 copy 到记事本中保存为 cert.txt

6) 重新安装用户证书：

在客户端下载证书失败的机器上，使用浏览器访问

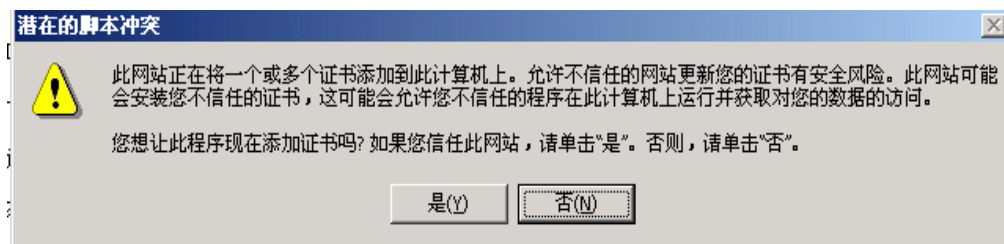
<http://www.cfca.com.cn/cda-docs/installcert.html>，将cert.txt中的内容，

粘贴在提示框内，如下图所示：



图 14

粘贴好以后点击“提交”。会连续出现两个“潜在脚本冲突”的对话框。如下图所示，点击“是”。



如果证书安装成功，会提示“证书安装成功”，可以按照“第二步：检查是否已经下载”中查找证书，并登录民生银行的网银。

如果证书的内容不完整或者格式不正确，会提示下载不成功，如下图所示：



如果您没有在报 1666 错误的机器上重新下载证书，或者查找的证书不是您的证书，会出现提示：



出现以上情况请您仔细检查“[第三步：重新下载用户证书](#)”查找证书和下载证书的过程是否正确。

5) 普通证书下载报错：-11280 General Entrust Error

原因：无法连接 CFCA 生产系统证书下载中心，是域名解析的问题。

解决方法：通过 IP 地址（210.74.41.118-电信；123.127.239.118-网通）连接（除非特别需要，建议还是通过域名访问证书下载中心）。

6) 普通证书下载成功，但是证书有效期不是两年，而是一年。

原因：CFCA 生产系统和对外测试系统默认普通证书有效期都是两年，下载证书有效期只有一年的原因有：

- 1、证书颁发机构设置该证书有效期只有一年；
- 2、下载证书使用的 IE 的密钥长度不是 128 位。

解决方法：

- 1、向证书颁发机构核对是否设置该证书的有效期只有一年；
- 2、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及获得相关补丁见：

http://www.cfca.com.cn/zhengshu/IE_patch.htm。

7) 证书下载报(-2018)证书状态错误，证书已被签发。

原因：证书已经被下载。

解决办法：

第一步：核实下载证书所使用的参考号、授权码是否正确。

注意检查下载证书时录入的参考号、授权码是否正确：参考号、授权码的字母取值范围：a b c d e f，数字取值范围：0 1 2 3 4 5 6 7 8 9。不含有字母“l”，因此所有像字母“l”的应该都是数字“1”，不含有字母“o”，因此所有像字母“o”的应该都是数字“0”。

如果确认参考号、授权码输入没有问题，请参考第二步

第二步：检查是否已经下载。

- 1、在下载证书报错的机器上，打开浏览器，点击“工具”——“Internet 选项”，如下图所示：

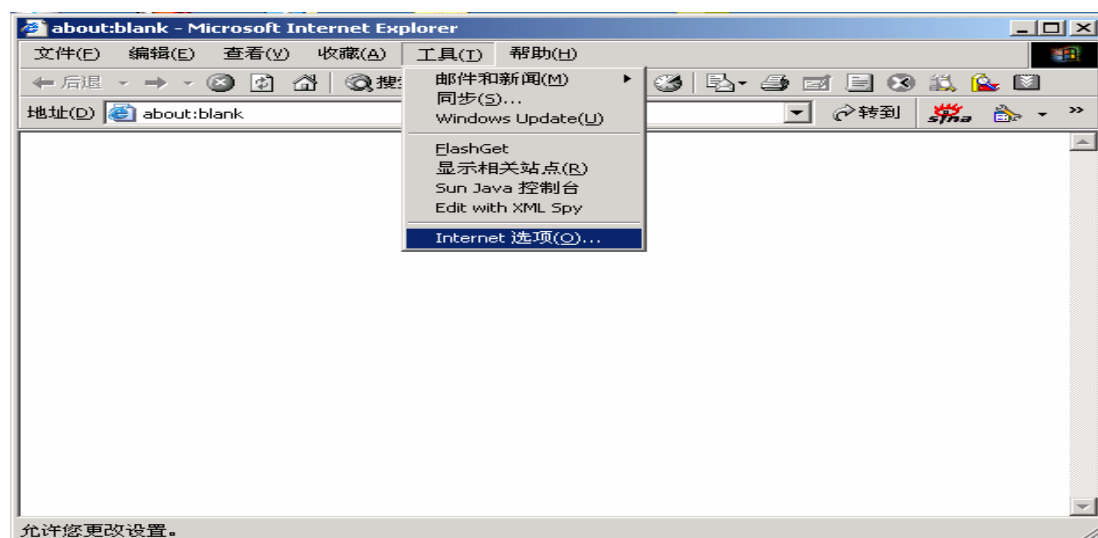


图 2

2、进入“选项”以后，点击“内容”，如下图所示：



图 3

3、点击“证书”，注意查看：

- 1) 如果在“个人”项中如下图所示为空，则表示用户证书没有下载到浏览器中。执行“第三步”。

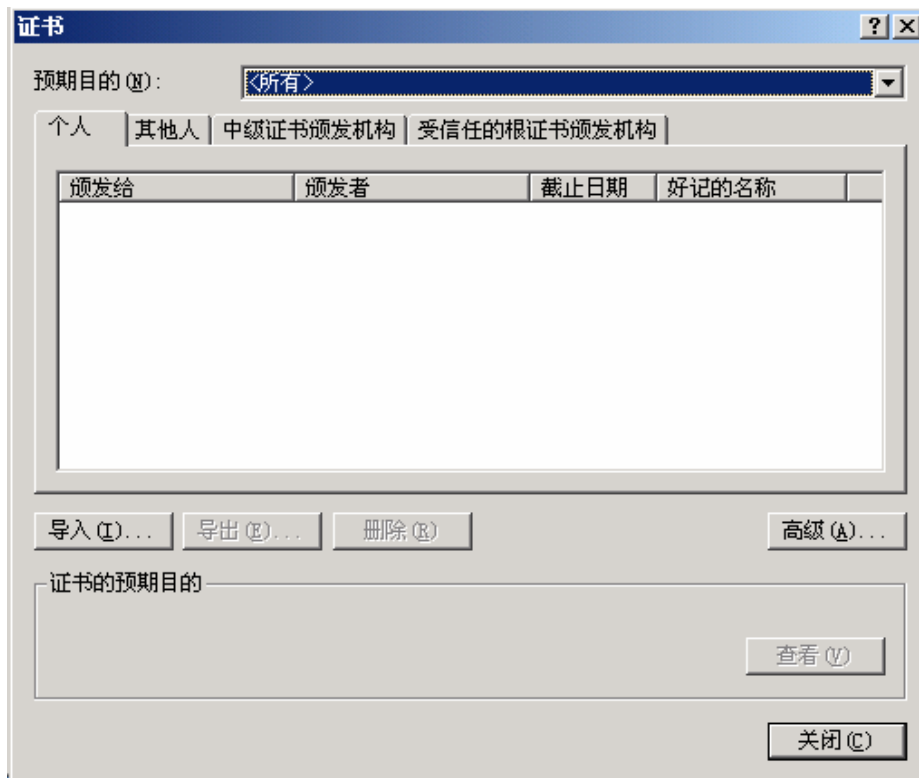


图 4

- 2) 查看用户证书是否为所需的证书：如果在“个人”项中有证书，并且其颁发者为“CFCA Operation CA2”如下图所示，则表明用户已经下载了 CFCA 的证书，并请核对“颁发给”中的内容与您的 DN（部分银行会在给用户的印有参考号、授权码的下载凭证中，印有 DN。比如银行的下载凭证；如果用户不知道自己的 DN，则需要用户与银行联系）。

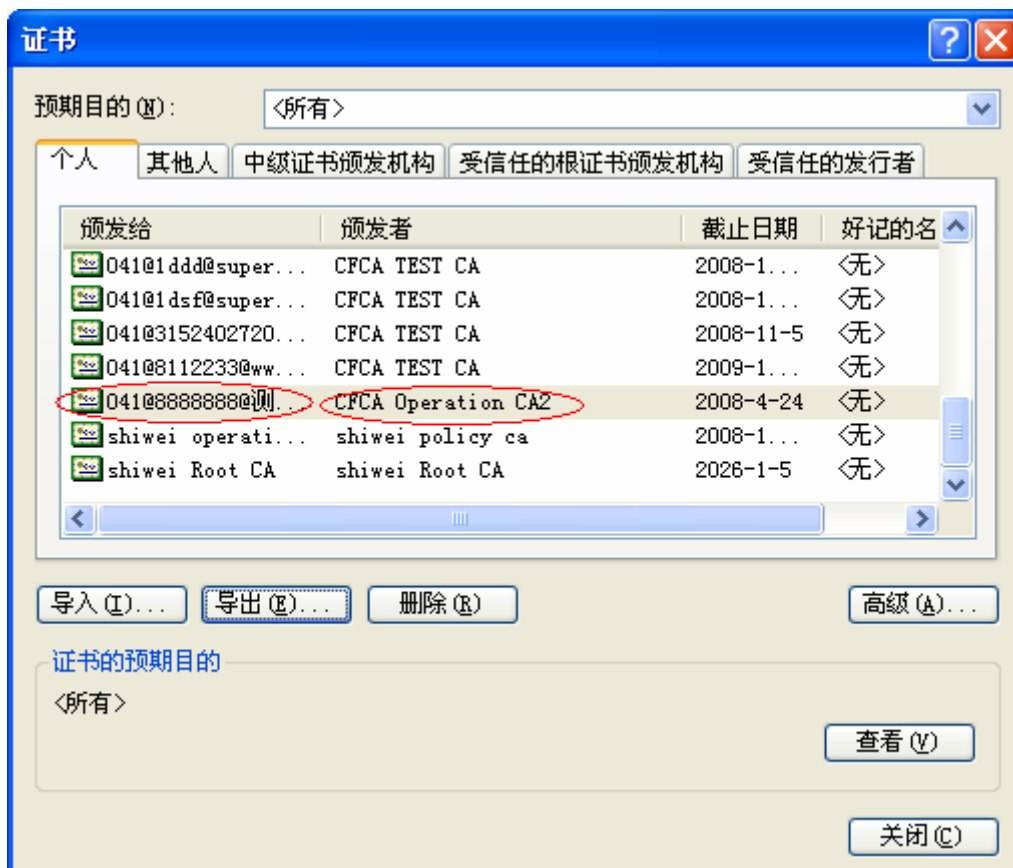


图 5

另外请注意，如果此处显示已经有证书，或者有多张证书，可能是已经使用了一段时间的网银或使用了多家银行的网银，这就需要仔细核对用户的 DN 以及“截止日期”判断存在的证书是否是这次下载的证书。截止日期 = 证书下载日期 + 2 年。

即如图 5 所示，则表明证书已经下载，证书相关的部分已经完成。可以登录相应的网上银行系统。

第三步：查询证书状态。

- 1) 登录<http://www.cfca.com.cn/tongyi>。



2) 选择左侧证书查询。



3) 选择 J-01 系统查询。

请填写查询条件	
用户证书下载	用户名(CN) <input type="text"/>
文件证书下载	电子邮件(EMAIL) <input type="text"/>
Web服务器证书下载	部门(OU) <input type="text" value="中国银联"/>
证书查询	证书类型 <input type="text" value="所有类型"/>
证书链下载	证书状态 <input type="text" value="所有状态"/>
	<input type="button" value="提交"/> <input type="button" value="重填"/>

注意：每次最多查询500条记录，请尽量精确查询条件！

4) 输入查询条件。

请填写查询条件	
用户证书下载	用户名(CN) <input type="text" value="*0345434*"/>
文件证书下载	电子邮件(EMAIL) <input type="text"/>
Web服务器证书下载	部门(OU) <input type="text" value="中国银联"/>
证书查询	证书类型 <input type="text" value="所有类型"/>
证书链下载	证书状态 <input type="text" value="所有状态"/>
	<input type="button" value="提交"/> <input type="button" value="重填"/>

注意：每次最多查询500条记录，请尽量精确查询条件！

5) 点击证书条目查看状态。



6) 看证书状态, 如果是证书使用中, 说明证书已经下载。



7) 然后点击“下载证书”, 下载一个名为 cert.cer 的文件, 用记事本打开, 出现如下图所示:



图 12

8) 选择“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”之间的部分, 进行复制, 如图 13 所示:

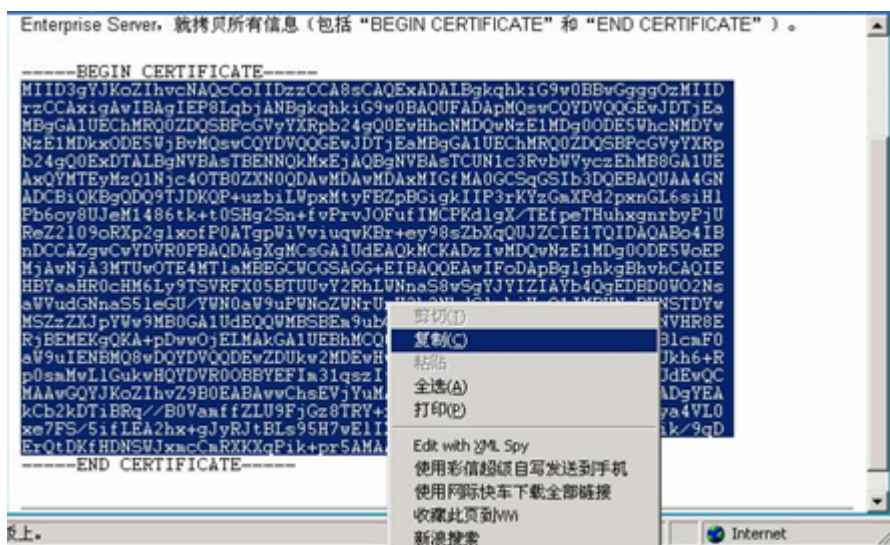


图 13

打开一个记事本，将刚才页面中复制的内容 copy 到记事本中保存为 cert.txt

第四步、重新安装用户证书

9) 在客户端下载证书失败的机器上，使用浏览器访问

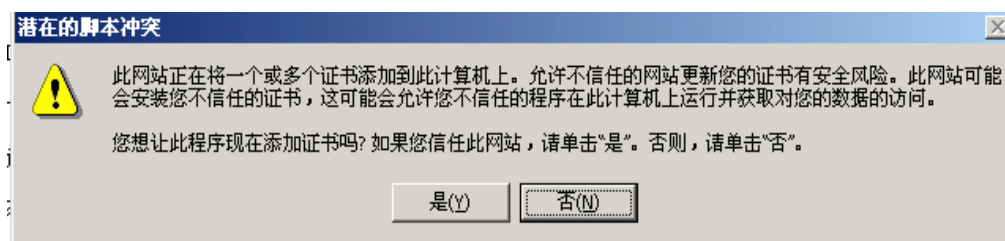
<http://www.cfca.com.cn/cda-docs/installcert.html> ,

将 cert.txt 中的内容，粘贴在提示框内，如下图所示：



图 14

粘贴好以后点击“提交”。会连续出现两个“潜在脚本冲突”的对话框。如下图所示，点击“是”。



如果证书安装成功，会提示“证书安装成功”，可以按照“第二步：检查是否已经下载”中查找证书，并登录银行的网银。

如果证书的内容不完整或者格式不正确，会提示下载不成功，如下图所示：



如果您没有在报错的机器上重新下载证书，或者查找的证书不是您的证书，会出现提示：



出现以上情况请您仔细检查“第三步：查询证书状态”查找证书和下载证书的过程是否正确。

8) 证书下载报“用户不存在”错误。

原因：下载证书的参考码、授权码不正确。

解决办法：

- 1) 首先核对参考码、授权码的位数，参考码、授权码应该都为 32 位。如果不是 32 位，则需要与发证机构管理员联系，获取正确的参考码、授权码。

2) 确认录入的参考码 (码) 授权码是否正确的规则为 :

字母 : a b c d e f

数字 : 0 1 2 3 4 5 6 7 8 9

不含有字母 “ I ”, 因此所有像字母 “ 1 ” 的应该都是数字 “ 1 ”。

不含有字母 “ o ”, 因此所有像字母 “ 0 ” 的应该都是数字 “ 0 ”。

9) 证书下载报“8010001D”错误。

原因 1 : USBKEY 没有插入电脑或者操作系统没有识别 USBKEY。

解决办法 : 确认 USBKEY 已经插入电脑。或者重新安装 USBKEY 驱动程序。

原因 2 : 在下载网页上选择的密钥容器 (或者叫 CSP) 错误。

解决办法 : 选择正确的 CSP , 使用厂商生产的 key 进行证书下载必须选择厂商所指定 CSP。

10) 证书下载报“80090020”错误。

原因 : USBKEY 的的驱动或者硬件有问题或者 USBKEY 没有初始化。

解决办法 : 1. 确认 USBKEY 是否插入电脑。

2. 确认 Key 的驱动是否正确。

3. 确认 USBKEY 本身有没有故障。

4. 初始化 USBKEY。

11) 证书下载报“80070020”错误。

原因 : 瑞星杀毒软件与 USBKEY 驱动冲突。

解决办法 : 关闭瑞星即可正常下载。

12) 下载证书报“ 8009000B”错误。

原因 : 这种情况多发生在用户帐户属于 windows 管理员帐户组里的情况 , 并且修改过帐户的口令。在 WinXP 中 , 私钥是通过 DPAPI 加密保护的 , 由于修改了帐户口令 , 导致私钥无法加密 , 因此无法下载证书。

解决办法 : 重新建立一个新帐户进行证书的下载。

13) 证书下载报“-2409 目录操作错误：更新目录项目”。

原因 1：该证书已经做了 30 次更新操作，CA 中对证书的更新操作的上限次数为 30 次。

解决办法：新发一张证书，重新下载。

原因 2：目录服务器信息发布出问题。

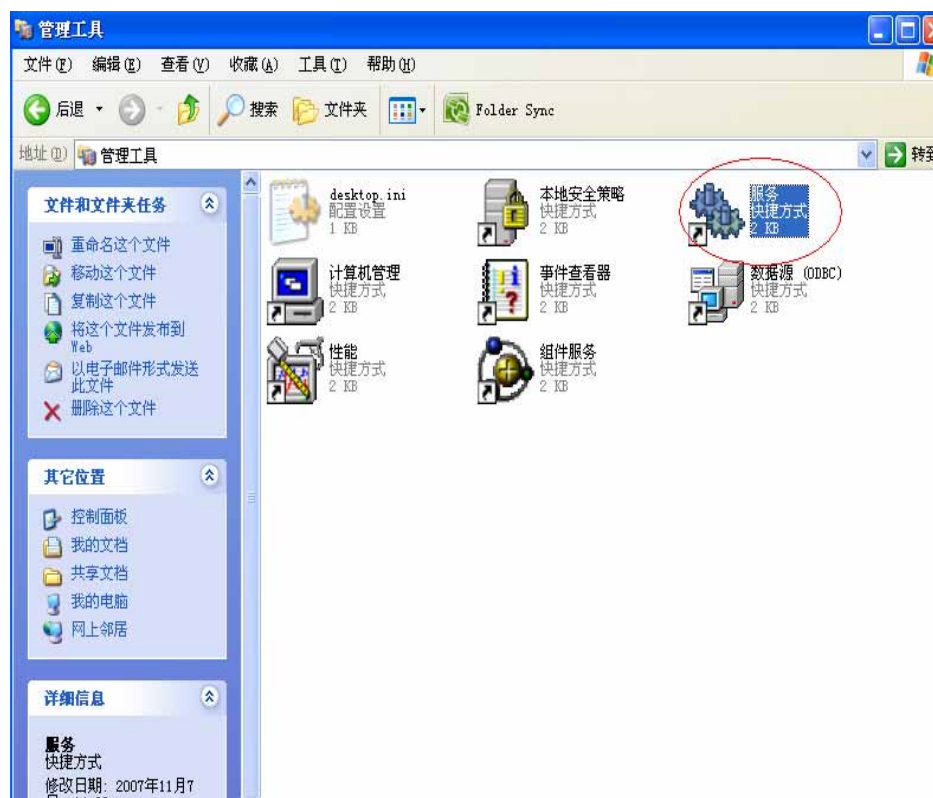
解决办法：可以打 CFCA 热线 4008809888 咨询，CA 重新发布该数据即可正常下载。

14) 下载证书报 p10 请求错误

原因：protected storage 服务未启动。

解决办法：在控制面板-->管理工具-->服务里，将 protected storage 服务开启，即可解决。





此服务
启动此服务

叙述：
提供对敏感数据（如私钥）的保护性存
储，以便防止未授权的服务，过程或
用户对其的非法访问。

IMAPI CD-Burnin...	用...	手动	本地系统
Indexing Service	本...	手动	本地系统
IPSEC Services	管...	已启动 自动	本地系统
Logical Disk Ma...	监...	已启动 自动	本地系统
Logical Disk Ma...	配...	手动	本地系统
Machine Debug M...	Man...	已启动 自动	本地系统
Macromedia Lice...	Pro...	手动	本地系统
Messenger	传...	已禁用	本地系统
Microsoft Offic...	运...	手动	本地系统
Microsoft Offic...		手动	本地服务
MS Software Sha...	管...	手动	本地系统
Multi-user Clea...		已启动 自动	本地系统
Net Logon	支...	手动	本地系统
NetMeeting Remo...	使...	手动	本地系统
Network Connect...	管...	已启动 手动	本地系统
Network DDE	为...	已禁用	本地系统
Network DDE DSDM	管...	已禁用	本地系统
Network Locatio...	收...	已启动 手动	本地系统
Network Provisi...	为...	手动	本地系统
NOTEPAD.EXE	NOT...	已启动 自动	本地系统
NT LM Security ...	为...	手动	本地系统
Office Source E...	保...	手动	本地系统
OracleDBConsole...		自动	本地系统
OracleJobSchedu...		已启动 自动	本地系统
OracleOraDb10g...	iSQ...	已启动 自动	本地系统
OracleOraDb10g...		自动	本地系统
OracleServiceORA10		自动	本地系统
Performance Log...	收...	手动	网络服务
Plug and Play	使...	已启动 自动	本地系统
Portable Media ...	Ret...	手动	本地系统
Print Spooler	按...	已启动 自动	本地系统
Protected Storage	提...	已启动 自动	本地系统
QoS RSVP	为...	手动	本地系统
Remote Access A...	无...	手动	本地系统
Remote Access C...	创...	已启动 手动	本地系统
Remote Desktop ...	管...	手动	本地系统
Remote Procedur...	提...	已启动 自动	网络服务
Remote Procedure...	管...	手动	网络服务

15) 下载证书报“-3290”请求错误。

原因：参考号，授权码不正确。

解决办法：注意检查下载证书时录入的参考号、授权码是否正确：

1) 参考号都是数字。

2) 授权码为数字和字母的组合，每四个为一组，共三组，中间以英文输入法下的减号“-”连接。

16) 下载证书报“-2033”错误。

原因：参考号，授权码过期。

解决办法：需要办理证书的机构重新为您发放两码。

17) 用户在 CFCA 网站下载证书点“证书下载”后页面乱码。

原因：IE 的编码设置不对。

解决办法：将 IE 的编码设置为简体中文再重启 IE 即可。如果查看证书，证书已下载，则可

以忽略这个错误。

2. 普通证书使用方面的问题

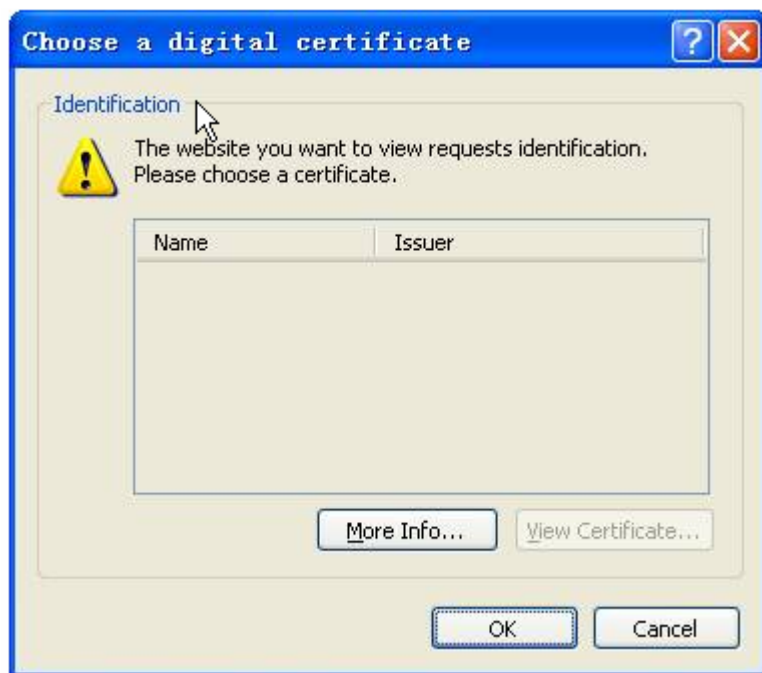
1) 如何获得别人的证书？

解答：可以通过个人普通证书的下载页面 <http://www.cfca.com.cn/tongyi>，在“证书查询”选项中查询得到需要下载的证书，然后就可以下载该证书。查找方式见<<普通证书技术支持手册>>第四章。

2) 卸载 IE 或重新安装操作系统时，已安装的证书会丢失吗？

解答：是的，已安装的浏览器证书会丢失。建议卸载前将需要保存的证书在浏览器中导出备份，在重新安装完浏览器后再行导入恢复。备份恢复方法见<<普通证书技术支持手册>>。

3) 访问 Https://的网站弹出“选择证书”窗口，但是没有证书可以选择，如下图：



原因 1、客户端没有证书。

2、没有安装证书链。

3、用户安装了安全代理软件，如股民用户安装了核新的安全代理软件。

解决办法：

1、 确认客户端证书是有效和完整的。

1) 是否已经插入 USBKey，并正确了安装 USBKey 的管理工具。

2) 在 IE 中检查证书是否存在（见<<普通证书支持手册>>中查看证书部分内容）。

2、 检查证书链。

虽然通过 IE 查看证书信息完整，证书链安装正常，但实际证书链安装不正常，需要通过 Win2000 还需要使用自带的“证书管理单元”安装证书链。

使用自带的“证书管理单元”安装证书链。

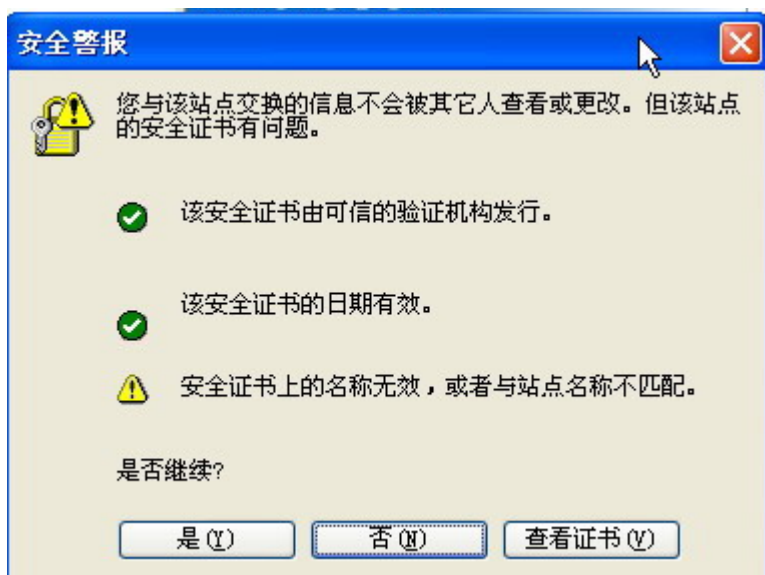
a, 请先在 CFCA 网站获得对应系统的证书链。

b, “证书管理单元”的启用一般需要运行 mmc 进行配置后才能使用。打开“证书管理单元”，可以分别选择“受信任的根证书颁发机构/证书”或“中级证书颁发机构/证书”点右键选择“所有任务/导入...”指向对应的证书进行安装。证书管理单元的使用方法见<<普通证书技术支持手册>>

3、 对原因 3，需要退出相关软件。

4) 用户登录安装过服务器证书的站点出现如下对话框“安全证书上的名称无效”：

对于 IE6 如下图：



对于 IE7 如下图：



原因：对于 IE6 弹出的警告图，惊叹号在第三行，说明浏览器输入的 URL 与服务器证书的名称不符。

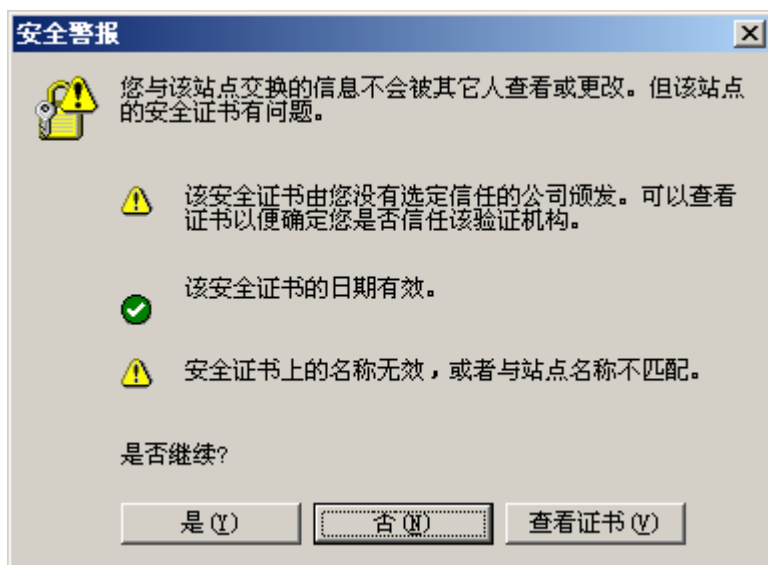
对于 IE7 显示的图，也提示了相应的警告“此网站出具的安全证书是为其他网站地址颁发的”，只是与 IE6 表现形式不同。出现这个警告框的原因可能是：

- a、服务器证书以域名申请，而用户 URL 输入 IP；
- b、或者服务器证书以 IP 申请，而用户 URL 输入域名导致的。

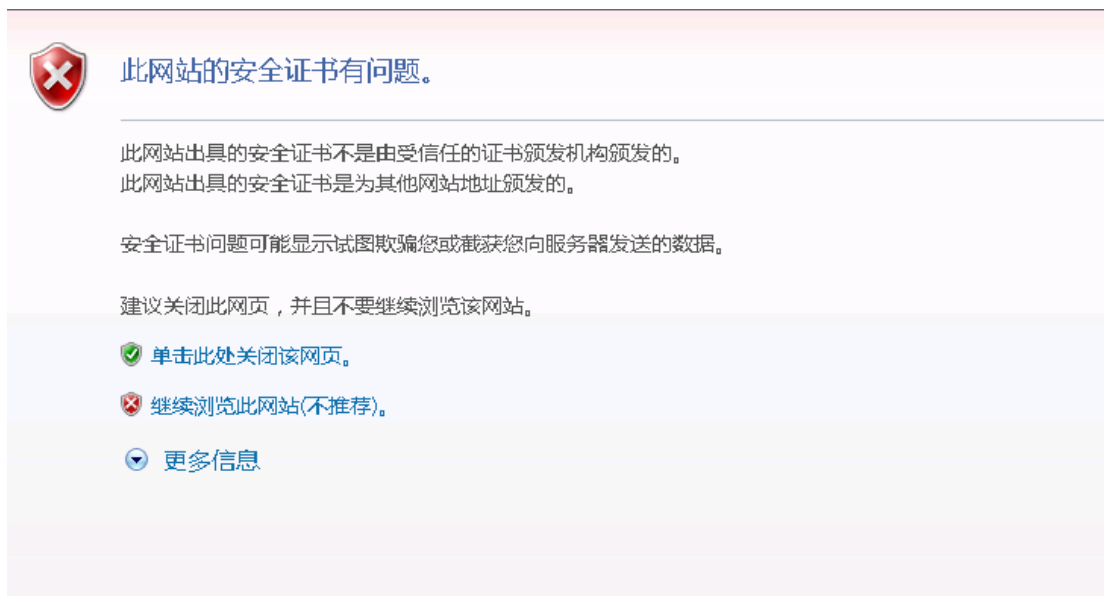
解决办法：建议用户在 URL 中输入相应的域名或者 IP 应该就不会有该警告了。当然，该警告并不影响继续使用。

5) 用户登录安装过服务器证书的站点出现如下对话框：

对于 IE6 如下图：



对于 IE7 如下图：



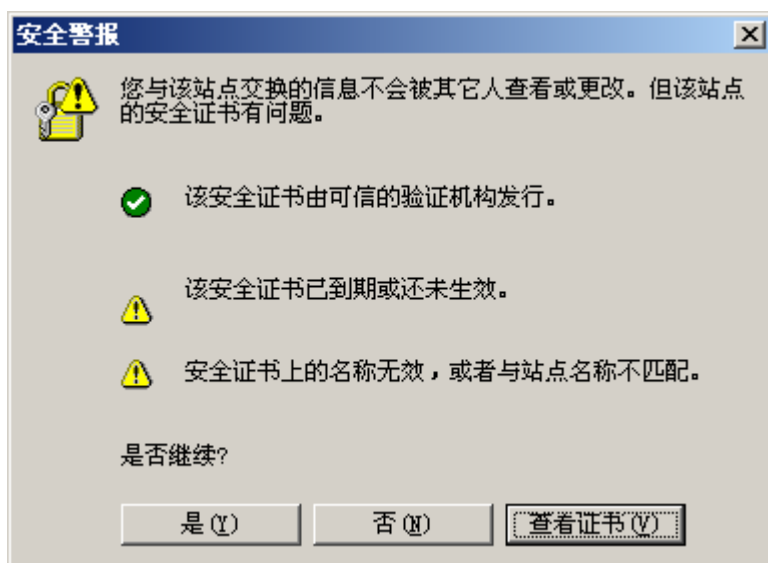
原因：对于 IE6 弹出的警告图，惊叹号除了在第三行有以外(原因已经在前面说明过)，在第一行也有。第一行的惊叹号说明服务器证书是由不受信任的证书颁发机构颁发的。

对于 IE7 显示的图，也提示了相同的警告，提示此安全证书不是由受信任的证书颁发机构颁发的。

解决办法：用户需要安装颁发此服务器证书的 CA 的证书链。当然，该警告并不影响继续使用。

6) 用户登录安装过服务器证书的站点出现如下对话框：

对于 IE6 出现如下图：



对于 IE7 出现如下图：



原因：对于 IE6 弹出的警告图，惊叹号除了在三行有以外（出现原因前面已经解释过了），在第二行也有。第二行的惊叹号说明本机时间不在服务器证书有效期的范围内。

对于 IE7 显示的图，也提示了相同的警告，提示此服务器安全证书已经过期或还未生效。

解决办法：可能本机时间不对，调整本机时间到正常时间，使之在服务器证书有效期的范围内即可。当然，该警告并不影响继续使用。

7) 用户访问 https 网站期间清除 SSL 缓存会产生什么后果？

答：用户在访问 https 网站期间在 IE 里面清除 SSL 缓存后（如下图），则再在此 https 网站进行页面切换的时候，需要用户重新选择登录此网站的证书。



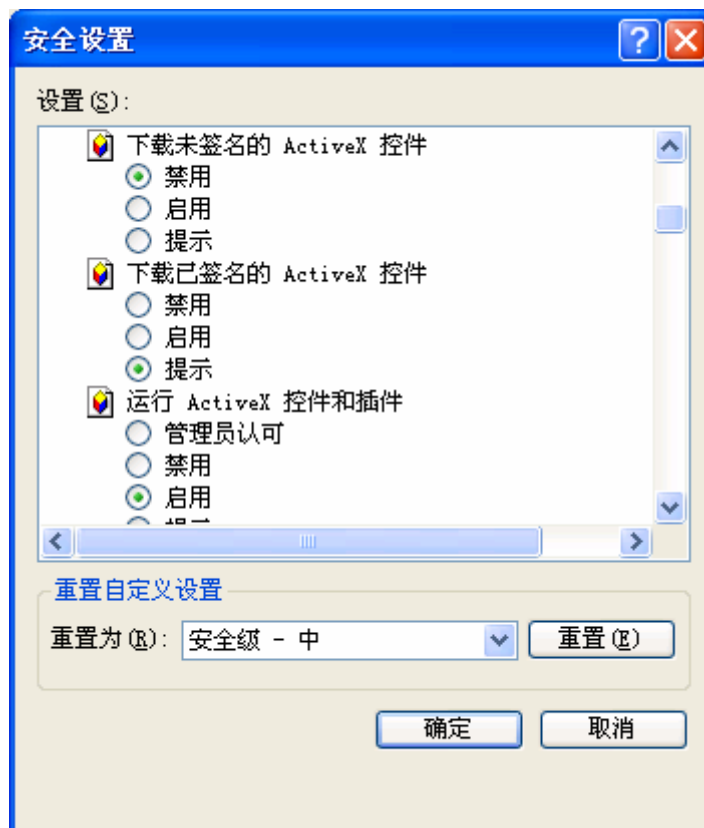
8) 普通证书能自动换发吗？

解答：普通证书不支持自动换发。证书换发首先需要到发证机构获取新的下载凭证，然后像证书下载一样到 CFCA 的证书下载中心(<http://www.cfca.com.cn/tongyi>)完成新证书的下载。

9) 调用证书工具包做业务时，提示“对象不支持属性或方法”

原因 1：IE 禁止下载已签名的安全控件。

解决办法：确认 IE 允许下载已签名的 ActiveX 控件，如下图所示：



原因 2：ActiveX 控件被拦截。

解决办法：检查网页是否有控件安装提示，一般在地址栏下方，如果有，则右键点击安装控件。

原因 3：证书工具包安装没有执行。

解决办法：请重新执行证书工具包安装软件。

10) 证书补发和证书换发的区别？

解答：证书补发：表示证书还在有效期内，证书丢失或者损坏时，需要重新拿到和原来证书通用名一样的证书，就可以申请这种操作。这种操作证书有效期的截止时间不变。

证书换发：表示证书快过期或者已经过期，需要延期证书时，申请该操作。这种操作证书有效期的截至时间会向后推迟一个有效期时间段。

11) 下载证书后发现该证书状态为未生效或已过期。

解答：证书签发时间是以 ca 的时间为准，如果用户的客户端时间与正常时间差别较大，可能会出现未生效状态。

13) 根证书链导入不到“受信任的根证书列表”中。

解答：vista 系统中默认安装证书链是安装不进去的，一定要指定证书链的存储区域。详细操作见<<普通证书技术支持手册>>证书链安装的章节。

14) 普通证书文件导入的时候不能导入成为个人证书，导入的是他人证书。

解答：该证书从浏览器里面导出的时候没有导出私钥，因此证书文件只是一个.cer 的公钥证书文件。再用该文件导入当然导不到个人里面去。需要在导出证书的时候选择“导出私钥”选项才能在用证书文件导入的时候导到个人里面去。

15)、如何备份证书？

解答：可以通过证书导出的方式备份证书。具体见<<普通证书技术支持手册>>。

16)、出现“该页无法显示”页面。

原因 1：没有安装证书链文件。

解决方法：安装 CFCA 证书链，安装方法见<<普通证书技术支持手册>>。

原因 2：Key 的驱动程序没有安装正确，或者 Key 没有插入 USB 接口，或者 Key 与 USB 接口接触不良。

解决方法：要正常的使用系统，要求能够使用 Key 的用户工具或者智能卡管理工具正常的查看到 Key 中的证书。如果不能，说明 Key 不能正常使用。因此，必须确认 Key 正确的插入 USB 接口，并且接触良好，保证 Key 的用户工具或者智能卡管理工具能够正常的查看到 Key 中的证书。如果以上措施不起作用，可能 Key 的驱动程序没安装或者安装的版本不正确，请联系 Key 的厂商进行处理。

原因 3：key 中的证书没有正确的安装到 IE 浏览器中。

解决方法：经常发生在使用握奇 Key 的情况下，使用 Key 的用户工具或者智能卡管理工具将证书安装或者注册到 IE 浏览器中。如果“安装”选项不可用，可以先选用“卸载”，然后再“安装”。直到在 IE 的“工具”->“Internet 选项”->“内容”->“证书”->“个人”页中能够查看到这张证书为止。建议在以上操作前，先的“工具”->“Internet 选项”->“内

容”->“证书”->“个人”页中能够查看到这张证书是否存在，如果存在，可以先手工删除。

原因 4：网络问题（网络不通、端口没开放或者域名解析 DNS 错误）。这种情况下，一般“客户身份验证”的证书选择对话框不会出现。

解决方法：用户检查网络情况。

原因 5：证书已经过期或者损坏、输入的 USB Key 的 PIN 码错误。

解决方法：如果过期，向证书发放机构申请证书换发；如果损坏或者口令遗忘，向证书发放机构申请证书补发。获得参考号和授权码，重新下载证书。

原因 6：USB Key 由于多次输错 PIN 码，导致锁卡。

解决方法：从 USB Key 厂商获得解锁工具，对 USB Key 解锁。

原因 7：可能是系统的 ssl 服务器的系统时间晚于 CA 系统的时间。因此刚下载证书的用户登录时，SSL 服务器认为用户的证书还未生效。

解决方法：稍后或者到第二天再登陆。