

# BJCA 证书应用环境用户手册



北京数字证书认证中心有限公司

北京市海淀区北四环西路 68 号双桥大厦 15 层



## 主要功能

BJCA 证书应用环境用于管理和维护 BJCA 颁发给您的数字证书。

BJCA 证书应用环境为您提供如下几大功能：

- **为您的数字证书应用准备好软件环境** – 为正常读取您的数字证书介质里的证书信息，准备好硬件驱动程序、证书应用所需控件等。
- **安装数字证书** – 将您的数字证书信息导入到系统中。
- **读取您的数字证书信息** – 读取并显示您的数字证书信息，以窗口形式清晰展现。
- **修改您数字证书密码**– 修改您的数字证书密码，确保您的证书安全。



## 硬件及软件要求

运行 **BJCA 证书应用环境安装程序**，计算机必须满足如下要求：

基本要求：

1. 至少 50MB 的剩余硬盘空间
2. Microsoft Internet Explorer 6.0 或更高版本浏览器

产品支持以下 Windows 操作系统：

Windows XP

Windows Vista

Windows 7(32 位和 64 位)

Windows 2000

Windows Server 2003

登录要求：

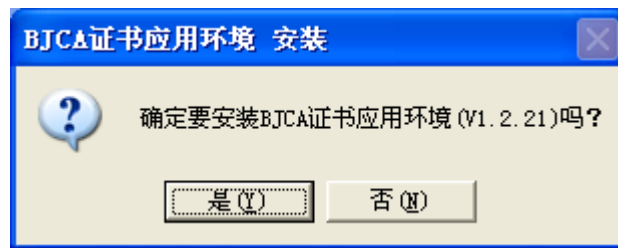
必须以管理员权限登录操作系统

## 安装和卸载

以下为程序卸载安装说明

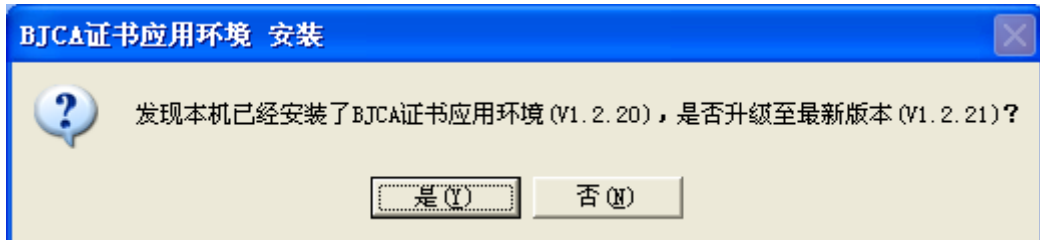
### 安装

双击 **BJCA 证书应用环境安装程序** 运行证书应用环境安装程序，若您首次进行安装，则首先会出现如下界面：



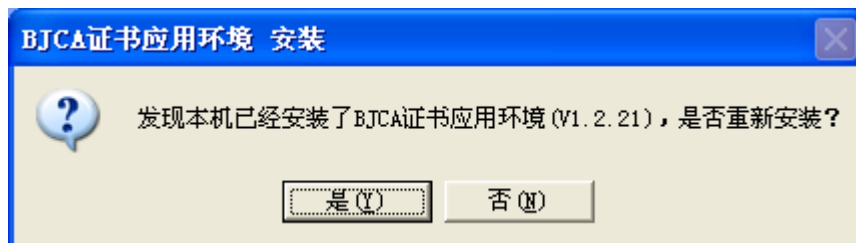
点击“是”开始程序安装，点击“否”退出安装程序。

若您已安装过 BJCA 证书管理工具（1.2.20 版本以上），则会询问您是否重新安装或升级安装：



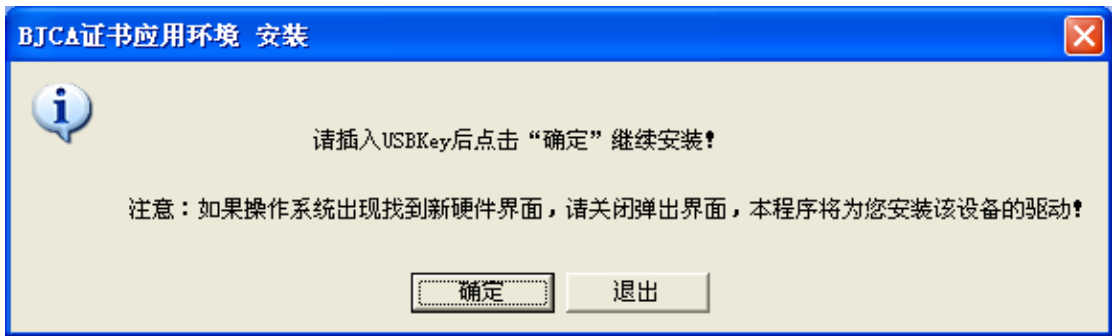
点击“是”进行升级安装，点击“否”则不进行升级。

若您安装过同版本的证书应用环境则会有以下提示：

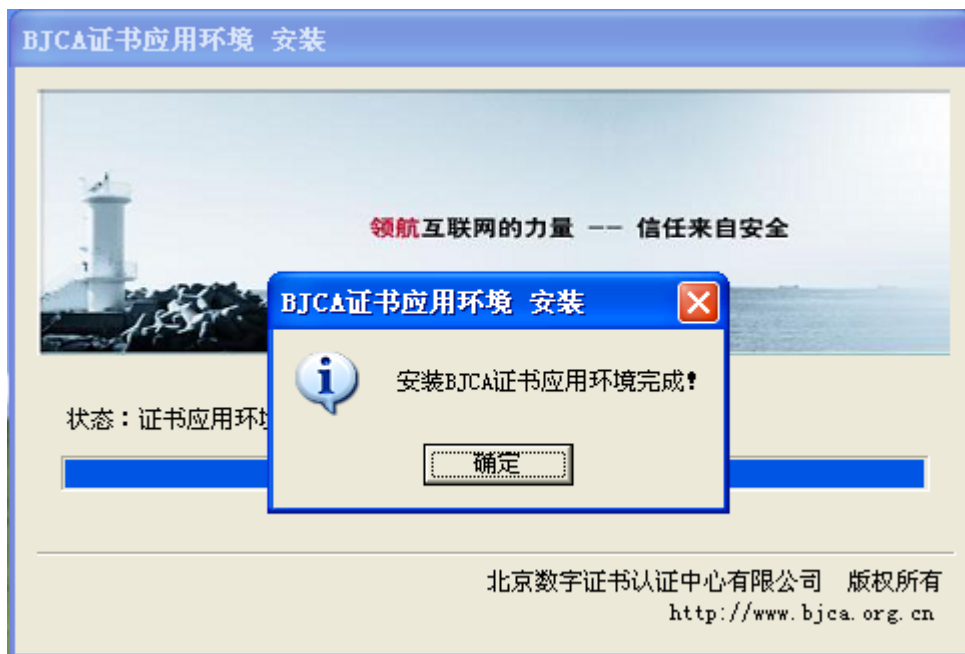


点击“是”进行重新安装，点击“否”则不会重复安装。

点击“是”开始程序安装后，您可能会遇到以下界面：



此时您需要检查您的 USBKey 是否已经插入电脑的 USB 接口中，若还没有插入，请您插入 USBKey，然后点击“确定”，系统将自动完成安装程序，在安装程序运行完毕时，会弹出如下安装界面：



## 卸载

若您希望卸载 BJCA 证书应用环境，有以下 2 种方法可供您选择：

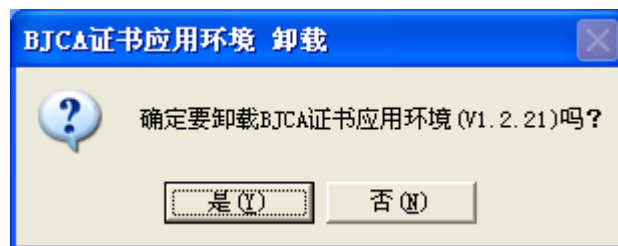
1. 点击“开始”按钮→选择“所有程序”→再选择“BJCA 证书应用环境”，点击“卸载 BJCA 证书应用环境”。



2. 在 Windows 中选择“控制面板”→“添加/删除程序”→选择“BJCA 证书应用环境 卸载程序”→点击“更改/删除”。



无论您采用以上哪种卸载方式，您都将遇到以下提示：



点击“是 (Y)”卸载程序将自动完成全部卸载工作，点击“否 (N)”将不会进行卸载操作，证书应用环境仍可继续使用。

卸载程序完成后会弹出以下提示：

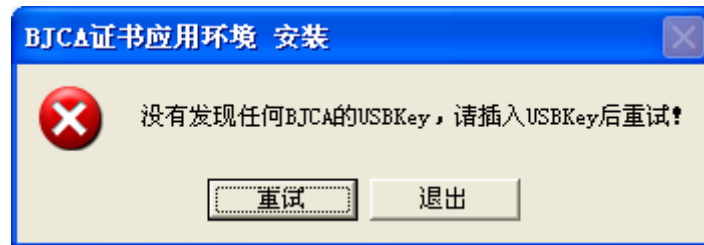


## 相关问题

在安装或卸载过程中您可能遇到某些问题，请严格依照我们的提示信息操作以确保证书应用环境的顺利安装。

## 提示插入 USBKey

若在安装程序提示插入 USBKey 时没有插入 USBKey，直接点击了“确定”，则会弹出如下界面：

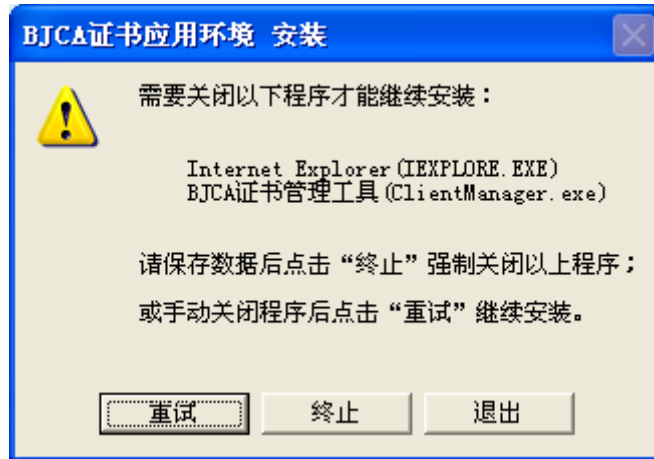


这时您可以插入 USBKey，点击“重试”，进行正常的安装。

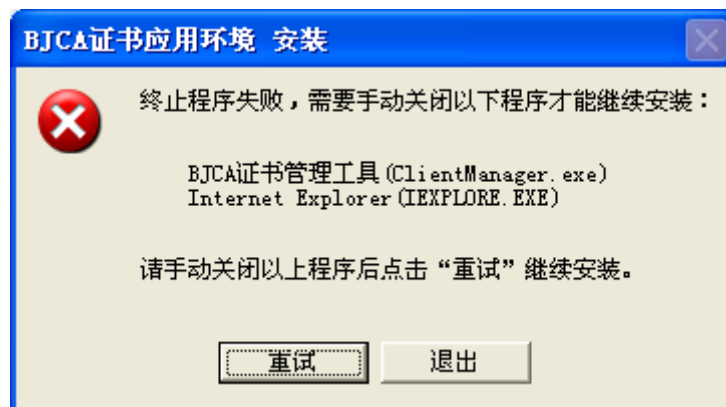
## 提示程序占用

在安装或卸载过程中可能会提示文件被程序被占用，解决办法如下：

以安装过程为例，当安装过程中出现以下提示时：

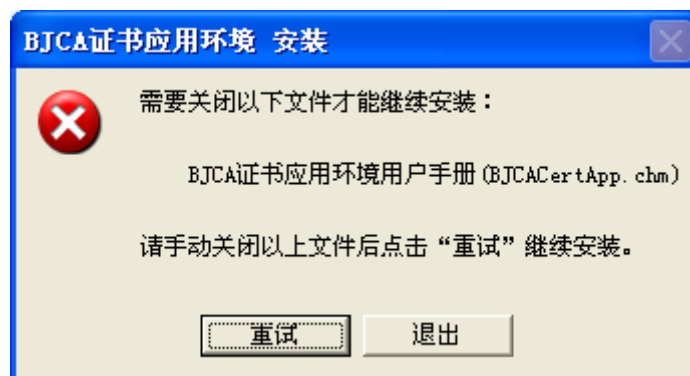


点击“终止”安装程序会自动关闭占用程序并继续安装，或手动关闭程序后点击重试继续安装，若点击“终止”后安装程序未能成功关闭，则会提示您必须手动关闭该程序：



手动关闭占用程序后点击“重试”即可继续安装。

当您遇到以下错误提示：

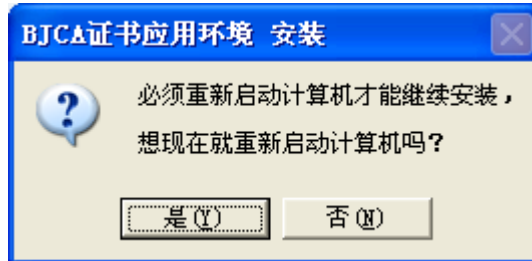


请检查您是否打开了程序自带的用户使用手册，关闭手册后点击“重试”即可继续安装。



## 提示重启计算机

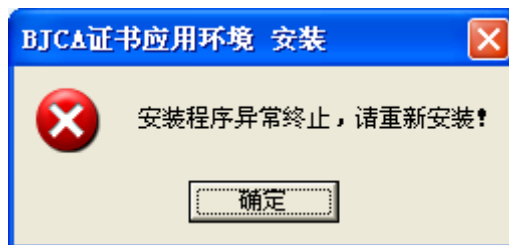
若您以前有安装过旧版本的 USBKey 驱动程序，系统会自动检测卸载，并为您安装新的驱动。此时可能会弹出如下界面，要求您重启计算机。



当出现此提示时，请按照要求重启计算机。重启后系统会自动继续为您安装完证书应用环境。

## 关于严重错误

当您在安装过程中遇到类似以下提示时：



此时证书应用环境未能被完全安装，无法正常使用。请务必重新执行安装程序，以保证您的证书可以正常使用。

**以上问题在卸载程序过程中也可能出现，请采取相同的处理办法。**

## 证书管理工具使用指南

BJCA 证书管理工具具有简单的友好的用户界面。界面左边是功能操作区,右边是解释和信息区。

### 证书管理主页面

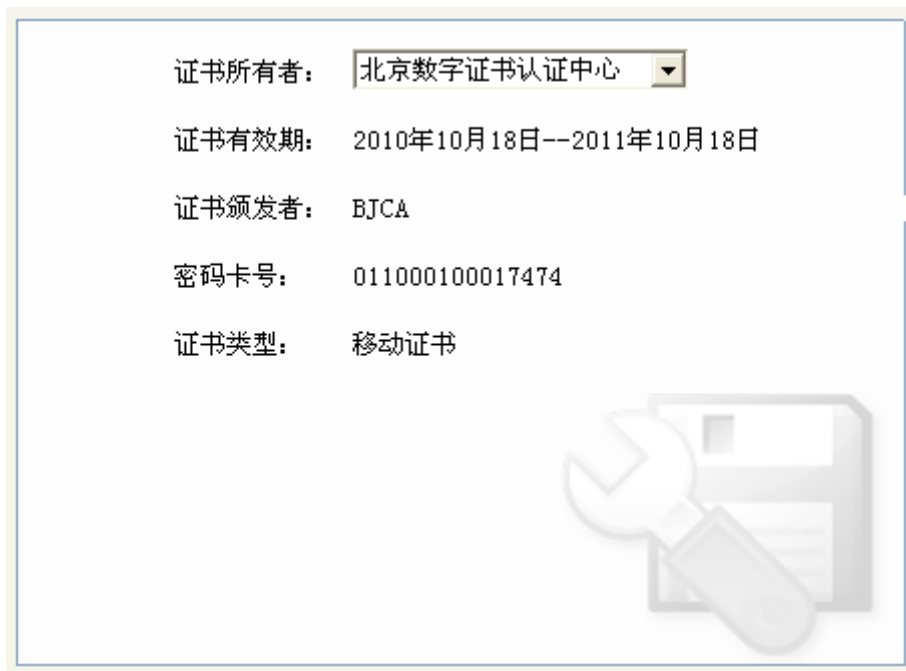
使用**证书管理**标签(如下),您可以查看和管理您的证书信息:



您可以点击左边操作功能键进行具体功能操作,分别为“修改密码”、“查看证书”和“帮助”。



在右边则能看到当前证书的基本信息。



## 修改证书密码

您可以点击**证书管理**标签页左边的





修改密码


修改证书密码:

**证书密码修改**



所有者: 业务管理员001  
有效期: 2010年09月15日--2011年09月15日  
证书类型: 移动证书


当前密码:  

新设密码:  

二次确认:  

修改说明:  
密码只能使用数字、字母以及-和\_, 如果使用字母  
务必区分大小写。

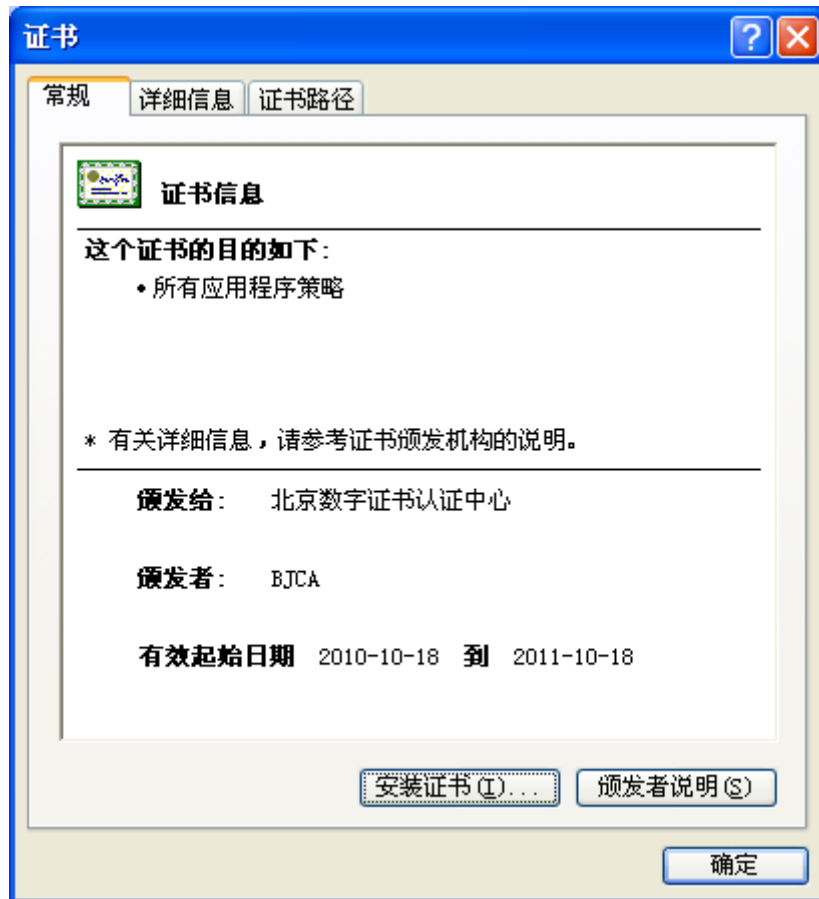
 确定  取消



输入证书的当前使用密码和新设置的密码，确认后点击**确定**，新的密码即生效。（密码长度为 4-16 位）。若想放弃修改密码，请点击**取消**。


## 查看证书

点击**证书管理**标签页的  [查看证书](#) 可以查看您的证书信息：



点击上方的**详细信息**和**证书路径**面板，可以查看更多证书内容。

## 帮助

点击  **帮助** 可以打开本帮助文档。



## 服务与保障

BJCA 为所有证书用户提供全套的软件工具包,帮助用户高效的使用 BJCA 所颁发的数字证书。

一旦您在任何 BJCA 注册机构或受理点办理了数字证书,您就成为我们的证书用户,在证书有效期期内您将获得如下服务:

- 证书管理软件更新。
- 证书管理软件的安装、配置及使用支持,用户可以通过电话或者电子邮件获得此服务。
- 获取 BJCA 产品更新信息,获取世界上新近流行的网络安全信息。

**BJCA 并不提供有关操作系统的使用及性能方面的服务支持或其他技术支持。**



## 常见问题解答（FAQ）

### 证书管理工具问题

针对于用户在使用 BJCA 证书管理工具过程的遇到的问题，本节提供了常见问题的详细解答。

**问题：为什么在打开管理工具时会提示“没有可以使用有效证书，请先插入 USBKey”？**

有如下几种可能：

- 首先请您确认是否有 BJCA 发放的 USBKey 插入电脑，如有插入，或 USB 接口已损坏，请检测 USB 接口，确认 USBKey 能够正常连接电脑。
- USBKey 驱动程序被误删除，请重新安装 BJCA 证书应用环境。
- USBKey 内证书损坏，请拨打我们的热线电话寻求技术支持。**热线电话：(010)58515511**
- USBKey 硬件损坏，请到原证书办理点进行更换，更换原则请参照《质保说明》。

**问题：为什么修改密码时无法粘贴？**

为了安全起见，我们在密码框内禁用了粘贴功能，请手动输入密码，确保您的密码不被别人修改。

**问题：证书到期了怎么办？**

如果您希望继续使用数字证书，请您在证书到期前的到您的证书办理点办理证书更新业务，请您在办理更新业务时携带好您的 USBKey，这样您将不需要支付证书介质费用。

### 关于 360 安全卫士

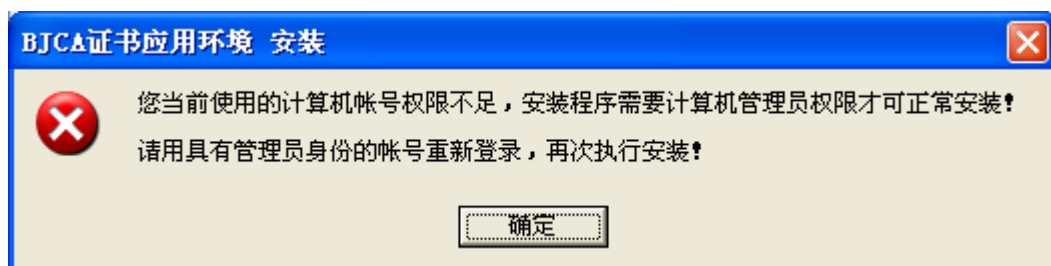
若您安装了 360 安全卫士，在安装过程中可能会出现如下拦截界面：



为了保证证书应用环境的正确安装，请您选择“允许程序的所有操作”。

## 关于管理员权限

当您在安装过程中遇到以下提示项：



请您以计算机管理员用户登录操作系统再运行安装程序。

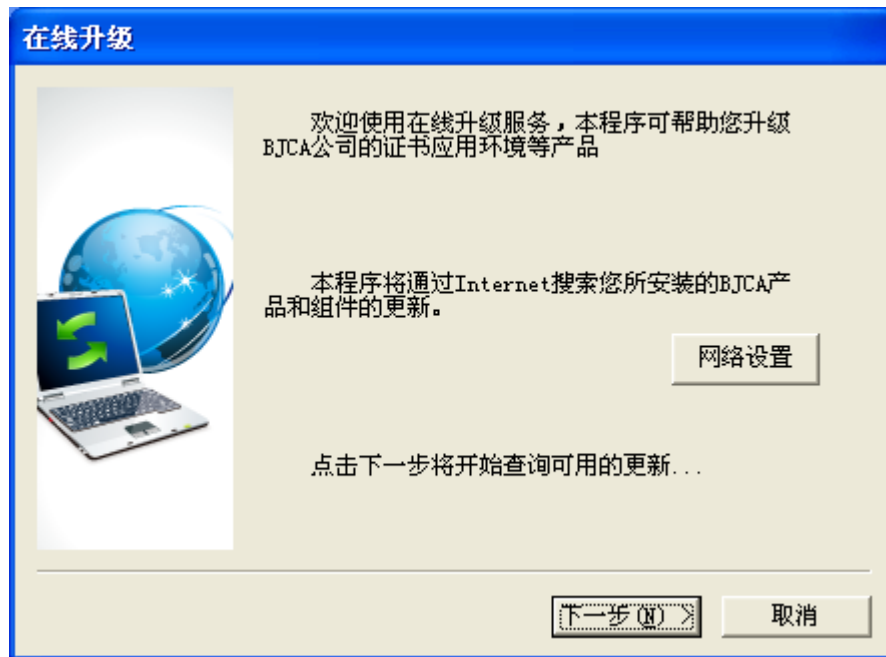


## 在线升级

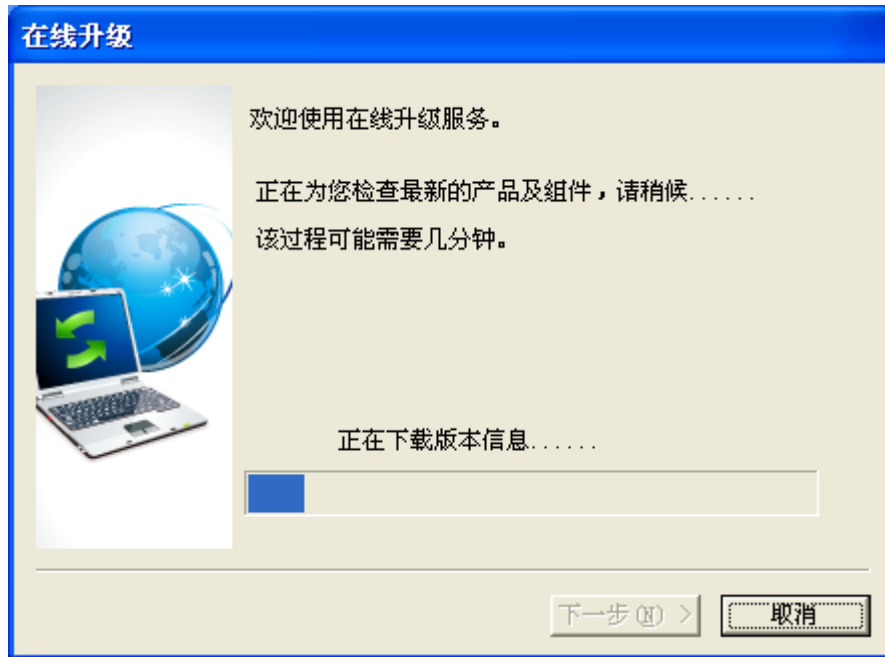
BJCA 证书应用环境自带在线升级功能，每次启动计算机后在线升级程序都会自动检测证书应用环境版本，若当前安装版本低于官方版本，则会自动升级。开机扫描在每次成功升级后的 15 天内不会再次进行升级，如果有需要可以采取手动方式启动在线升级程序。

手动升级操作如下：点击“开始”按钮→选择“所有程序”→再选择“BJCA 证书应用环境”，点击“在线升级”。

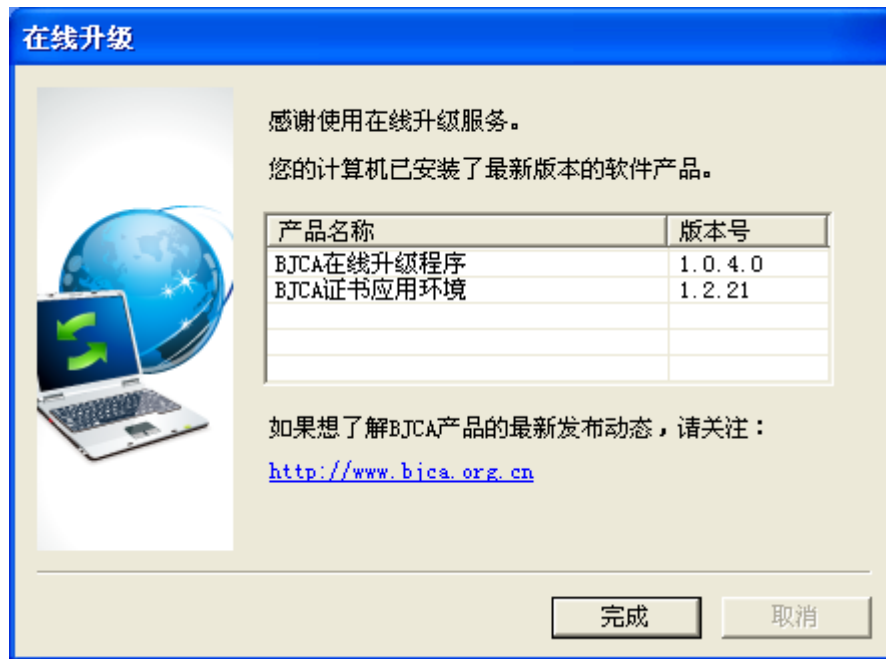
界面如下：



点击“下一步 (N) >” 自动升级程序会自行检测当前证书应用环境版本并升级，检测及升级界面如下：



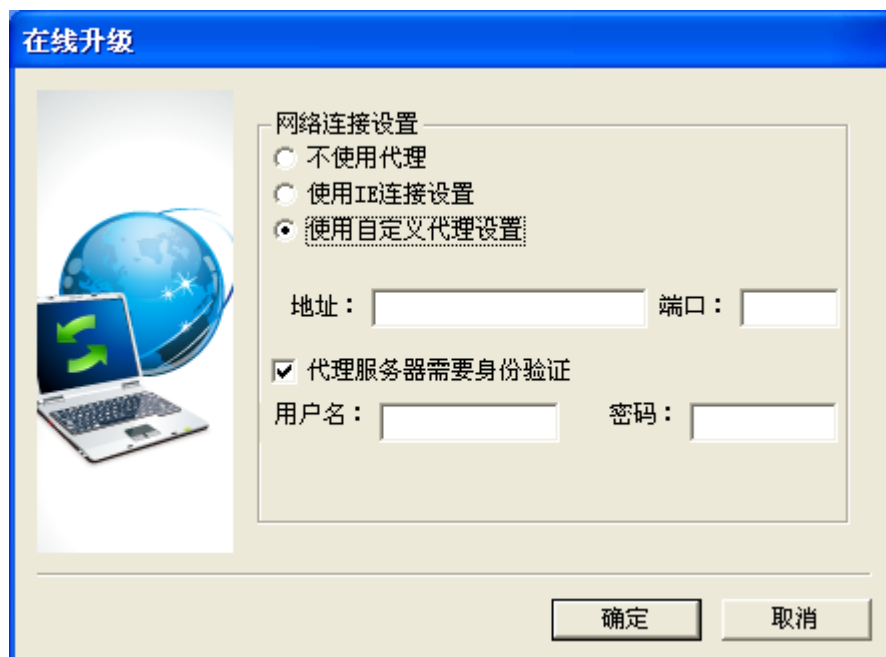
升级完成后会显示以下界面：



此界面会告知您当前最新的证书应用环境版本和在线升级程序版本，点击“完成”即可退出在线升级程序。

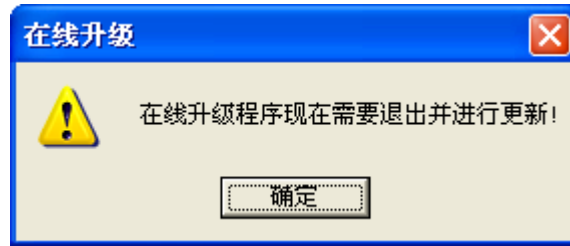
*注：如您的计算机内安装版本已是最新版，则会直接跳转至以上界面。*

如您需要使用代理才可以正常登录外网，请点击“网络设置”



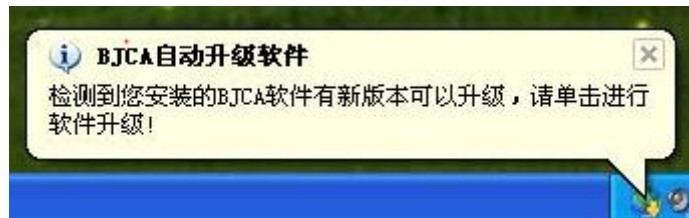
设置好代理地址后点击“确定”将会保存网络设置。

如您在升级过程中碰到以下界面：



此界面表示在线升级程序需要升级自身版本，点击“确定”后在线升级程序将会自行升级。

当程序检测到有新版本可供升级时，会在桌面右下角标处弹出以下提示：



此时点击角标将自动启动在线升级程序并进行升级。

## 关于我们

北京数字证书认证中心（简称 BJCA）成立于 2001 年 2 月，是获得国家信息产业部电子认证服务许可资质的电子认证服务商，是具有国家涉密集成资质国家信息安全服务安全工程类资质和北京市信息安全服务能力壹级资质的信息安全服务商。

作为权威的电子认证服务商，BJCA 遵照《中华人民共和国电子签名法》的要求和相关管理规定，为用户提供全面的数字证书申请、审核等服务，并通过一系列应用安全产品和信息安全解决方案，为电子政务、电子商务、企业信息化的发展构建安全、可靠的信任环境。在业务的开展中，BJCA 率先开始以客户为中心的新型电子认证服务体系建设，引领着电子认证服务行业的发展方向。

作为专业的安全服务商，BJCA 拥有国内一流的信息安全专家和专业的安全服务队伍，紧跟信息安全领域发展动态，熟悉各种信息安全政策、标准、指南和要求，遵循“分域防护、深层防御、分级保护、动态防范”的原则，为客户提供全方位、专业性、持续性和个性化的安全技术支持与服务。

经过几年的高速发展，通过营造良好的企业文化，建立有效的激励机制，提供广阔的发展空间，BJCA 已经成为人才荟萃、朝气蓬勃的创新型高科技企业，建立了一支拥有 300 多名员工，集产品设计、技术研发、工程实施、市场营销、经营管理和运行服务于一体的专业队伍，并将继续贯彻“以人为本，追求卓越，求实创新，和谐共生”的企业理念，实现员工进步、企业发展、客户满意，不断向社会提供高品质的信息安全服务，帮助用户创建安全可信的网络空间。

## 我们的其它产品

BJCA 是国内发行量最大的数字证书产品供应机构之一，每天都有来自全国各地各个领域的新用户加入 BJCA 信任体系的温暖怀抱，享用 BJCA 提供的安全保障。

### 首都政务通数字证书

“首都政务通”是通行首都电子政务的安全钥匙。通过“首都政务通”的数字证书服务，用户可安全访问北京市政府对公共各种业务，进行税务、工商、社保、公积金、政府招投标等业务的在线办理。

北京数字证书认证中心为广大用户提供的“首都政务通”数字证书服务，符合《中华人民共和国电子签名法》的要求，使电子政务业务能够安全可靠开展，同时业务中使用数字证书进行的数字签名与手写签名具有相同法律效力。

### 信天行数字证书

#### 产品简介

信天行是北京数字证书认证中心 (BJCA) 为电子商务和电子政务领域提供的权威、合法、安全、便捷的第三方电子认证服务产品，是 BJCA 旗下应用最广泛、服务最完善的电子认证服务品牌。使用它，可以解决电子商务应用中的安全问题，保障用户在电子交易活动中的合法权益，符合《电子签名法》对可信数据电文的要求。

#### 产品功能

- 身份认证——对证书用户严格的身份鉴证，可以证明用户真实身份。
- 数字签名——在进行业务交易时，对业务数据用数字证书进行数字签名和加密，保证数据不被非法篡改或泄漏。
- 抗抵赖——交易数据进行数字签名后，可作为合法的交易举证证据，用于纠纷处理。

#### 产品种类

- 个人数字证书——用于标识个人在网络通讯中的身份。
- 单位数字证书——用于标识单位在网络通讯中的身份。
- 服务器证书——用于标识服务器在网络通讯中的身份。



## 产品特点

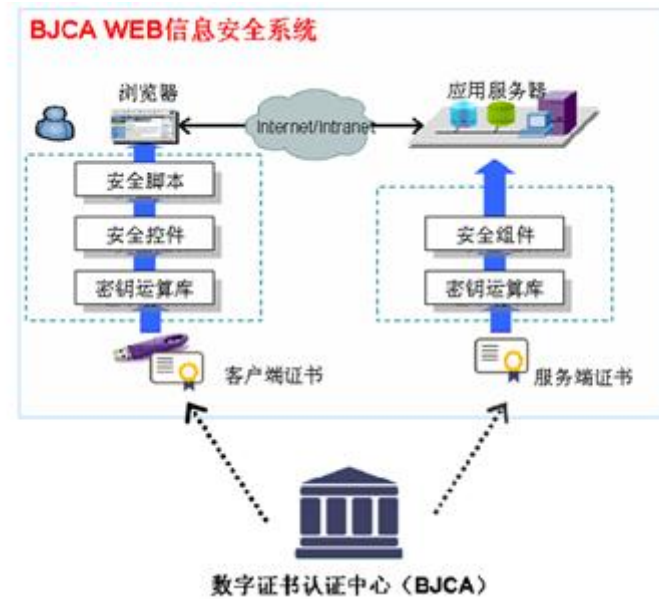
- 通用性——可以在 BJCA 开展的所有电子商务应用系统中通用，最大限度地减轻的负担。
- 即插即用——USBKey 为无驱型，且数字证书无需安装，真正实现了“即插即用”。
- 丢失后自我保护——USBKey 丢失后有自我保护功能，只要密码连续输入错误 10 次，自动锁死，有效保护真正拥有者的利益。
- 简易的申请流程——用户可进行在线申请，流程简便。
- 易于实施——采用标准的证书集成接口，可与各种 Web 应用系统无缝集成，实施成本低。

## BJCA WEB 信息安全系统

网络技术的发展给人们带来便利的同时，安全问题也日益凸现，冒充合法用户登录系统、窃取敏感信息、篡改资料、否认重要操作行为等等案例层出不穷。因此，用户急需一种灵活、便捷、高效的方法可以有效解决这些问题。利用 BJCA Web 信息安全系统与网上业务系统的结合可有效的解决电子商务或电子政务活动当中交互双方网上身份的真实性和可靠性认证的问题，化解业务风险。

BJCA Web 信息安全系统产品是一款利用 X.509 数字证书、数字信封、数字签名等先进的安全技术，通过和应用系统集成，实现用户登录应用系统的身份真实性认证、对敏感信息进行加密、签名保护的数字证书应用产品。

## 系统架构



### 系统功能：

- 实现有效身份验证：BJCA Web 信息安全系统 利用 PKI 技术体系解决 Internet 上信任问题，通过数字证书标识网上各方的真实身份，保证了身份验证的有效性。
- 实现可靠的电子签名：BJCA Web 信息安全系统 利用可信第三方签发的数字证书、结合数字签名等安全技术实现业务信息操作的责任认定，并且符合《电子签名法》对可靠电子签名的技术要求。
- 实现信息加密防护：BJCA Web 信息安全系统 利用可信第三方签发的数字证书、结合数字信封等安全技术实现对敏感业务信息加密操作，防止敏感信息被非法窃取。

### 系统特点：

- 有效的身份认证机制：PKI 是解决 Internet 上信任问题的最佳方案。BJCA Web 信息安全系统完全采用业界这一先进方案，通过数字证书标识网上各方的真实身份，保证了身份验证的有效性。
- 效能突出：在安全运算处理上，将对称、非对称加密、Hash 运算有机结合，实现安全与效率之间的平衡，保障安全处理的高效性；在通讯上，不建立额外的信道，实现运行的高效率。
- 遵循安全技术标准：BJCA Web 信息安全系统在加密算法和数字证书方面均遵循相应的安全技术标准，如 X.509v3 、CSP、PKCS 系列标准。在信息传输方面，遵循了 http 标准通讯协议。
- 集成简便：采用通用的组、控件技术，适用于多种应用环境，集成开发便利。



- 安全稳定：采用独立的安全设计思想，使用安全系统架构，通过严格的应用测试，具有较好的稳定性和安全性。

- 扩展性好：同时支持 B/S 和 C/S 应用，支持第三方硬件加密卡、机，具有很好的可扩展性。

#### 应用领域：

- 电子政务系统，如政府机关的网上申报系统、政府采购、内部办公系统等。
- 电子商务系统，如支付平台、网上交费、网上商店、网上炒股、网上博彩等。
- 办公自动化系统，如企事业单位内部、远程办公等。
- 电子金融，如网上银行、网上保险等。
- 电子医疗系统，如电子处方、电子病历等。
- 招投标系统，如政府采购等。

## BJCA 电子签章软件

BJCA 电子签章结合成熟的组件技术、PKI 技术、图像处理技术以及智能卡技术，按照一系列的标准体系，以电子形式对电子文档签名并加盖签章。

软件采用 COM 组件技术，将传统印章与电子签名技术完美结合，通过签章可以确认文档来源、确保文档的完整性、防止对文档未经授权的篡改以及确保签名行为的不可否认。

#### 系统特点：

- 电子签章具有高度权威及法律效力：支持权威机构—北京数字证书认证中心颁发的数字证书，使用双证书体系，采用国密办批准的 USBKey，签名私钥不出 Key，保证签名私钥不可复制，充分符合《电子签名法》各项要求，使电子签章具有足够的法律效力及高度权威性。

- 对电子印章进行整个生命周期的管理：包括印章制作、印章信息管理、印章发放、印章挂失、印章停用、印章重新制作的全过程的记录和管理。

- 支持签章过程的统一监管，实现签章流程可控：在线签章时系统需要验证数字证书和智能 USBkey 的合法性；系统自动监控和记录在线签章的全过程。



- 支持离线签章的临时授权，满足不同用户需求：客户端不能联网时，用户为了能正常进行签章，可向管理员申请临时授权签章功能。

- 基于组织机构对个人和单位用户进行管理：对于个人用户和单位用户按组织结构进行分类，并能以目录树形态友好展现，能够对机构和用户进行统一管理、统一监督；以机构和用户的信息作为出发点对电子印章进行查询和统计管理。

- 支持多种不同安全特性的用户身份凭证：电子签章管理系统支持操作员使用用户名/口令或者智能 USBKey 等硬件介质的身份凭证，能够根据业务的不同安全等级合理使用凭证。

- 同时支持在线签章与离线签章授权：可以根据需要授权用户在线签章或离线签章；在线签章需要验证数字证书和智能 USBkey 的合法性。同时系统自动监控和记录在线签章全过程；在客户端不能联网时，用户为了能正常进行签章，可向管理员申请临时授权签章功能。

- 完善的安全机制：电子签章管理系统可根据不同的安全需求配置相对应的凭证安全策略、日志安全策略、访问控制策略。同时，系统自身也采取了周密的安全措施，包括管理员的高强度认证登录、分级授权管理，以及完备的审计日志机制。

#### 系统功能：

- 电子印章整个生命周期的管理：包括电子印章制作、印章启用、印章挂失、印章停用、印章重新制作、印章在线使用控制的全过程的管理。

- 组织机构用户管理：对组织机构、用户和管理员的维护和管理。

- 日志审计：实现对电子签章管理系统的管理和维护、电子印章的管理、电子印章的使用等进行详细的日志记录和审计。

- 加盖签章：文档加盖签章，证明签名人的身份。

- 验证签章：验证文档签章，证实文档有效性。

- 抗抵赖：签名者认可所签文档内容，不能对签名行为抵赖。

- 抗伪造：签章不能通过复制或其他方式进行伪造或冒充。

- 防篡改：文档一旦被篡改，签章即失效。



## BJCA 统一认证管理系统

BJCA 以 PKI 技术为基础，以整合信息资源为目的，面向所有业务系统提供支持数字证书的安全认证、单点登录及访问控制服务，并对全网系统访问情况进行安全审计。建立统一的身​​份认证和授权管理平台，实现基于用户数字身份管理、授权管理、认证管理和安全审计的 4A 解决方案，满足电子政务资源整合和复杂业务管理的需要，全面提升政府信息化综合安全管理能力，有效推动网络信任体系建设。

### 统一用户管理：

构建完整可信的用户资源信息库，集中实现用户信息、凭证、组织机构等信息的统一管理。实现用户的流程化管理，控制帐号的整个生命周期，为人员岗位变更和离职等应用场景提供安全可靠的帐号管理解决方案。

### 系统授权管理：

实现多业务系统的统一访问控制授权，降低多个业务系统管理维护的复杂度，有效减少人为原因造成的安全性缺失，为业务系统维护的安全性和便利性找到合适的平衡点。支持基于 RBAC 授权管理模型的角色授权，支持多安全域内的多级交叉授权管理模式。

### 统一身份认证：

统一用户身份标识，有效区分内部人员、普通市民和外部合作人员。提供不同安全等级的身份认证服务包括用户名/口令、数字证书、智能卡、动态口令、指纹识别等多种认证方式。

### 安全单点登录：

为用户提供基于可靠访问控制的“一点登录、多点漫游”功能，用户只需一次登录就可以访问授权范围内的应用系统。

### 全网访问审计：

对用户访问所有应用系统的情况进行记录及审计，提升信息化应用资源的全局安全管控能力。



## 联系我们

如果您有任何问题、意见或者建议，请提交给我们的注册机构，或者直接提交给北京数字证书认证中心。我们很乐意通过电话或者电子邮件为您提供和我们产品相关的服务。您所有的建议和意见都将得到我们认真的考虑。

地址：北京市海淀区北四环西路 68 号双桥大厦 15 层（左岸工社）100080

客服热线：(010)58515511

电话：(010)58045600

传真：(010)58045678

网址：<http://www.bjca.org.cn>

销售联系：[market@bjca.org.cn](mailto:market@bjca.org.cn)

客户服务：[service@bjca.org.cn](mailto:service@bjca.org.cn)

人力资源：[hr@bjca.org.cn](mailto:hr@bjca.org.cn)

法律事务：[cps@bjca.org.cn](mailto:cps@bjca.org.cn)

