

# 证书应用环境(Windows)

## 用户手册

V3.8.2



## 目 录

欢迎使用	1
版权声明	1
<b>1 概述</b>	<b>2</b>
1.1 文档用途	2
1.2 名词解释	2
<b>2 产品介绍</b>	<b>3</b>
1.1 产品简介	3
1.2 产品架构	3
1.3 产品功能	4
<b>3 产品安装说明</b>	<b>6</b>
<b>4 使用操作说明</b>	<b>7</b>
4.1 使用前准备	7
4.2 使用说明	7
4.2.1 启动运行	8
4.2.2 首页	10
4.2.3 设置	20
4.2.4 关于	24
4.2.5 帮助	25
4.2.6 消息提醒	25
4.2.7 托盘菜单	26

## 欢迎使用

欢迎您使用证书应用环境产品，如果本手册能为您提供帮助，带来便利，我们将深感欣慰。如果您在使用过程中，遇到了问题，或对我们产品有好的建议，可以：

☎ 致电客户服务热线：4009197888

🌐 或访问公司网站：<https://www.bjca.cn>

与我们联系，对您提出的问题或建议，我们表示衷心的感谢。

## 版权声明

本手册著作权属北京数字认证股份有限公司所有，在未经本公司许可的情况下，任何单位或个人不得以任何方式对本手册的部分或全部内容擅自进行增删、改编、节录、翻印、改写，仅限和北京数字认证公司的项目合作方公司使用。

北京数字认证股份有限公司

©2020

# 1 概述

## 1.1 文档用途

文档主要介绍证书应用环境产品的架构、功能、特点，以及操作使用，文档主要给用户操作使用。

## 1.2 名词解释

术语	说明
证书应用环境	简称证书助手，基于 PKI 技术的应用安全基础套件，实现终端的证书签发、管理和应用等功能。
XTXAppCOM	简称 XTX，是证书应用环境的 COM 控件
数字证书	也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。
数字信封	一种数据结构，包含用对称密钥加密的密文和用公钥加密的该对称密钥。
时间戳	对时间和其它待签名数据进行签名得到的数据，用于表明数据的时间属性。
加密	对数据进行密码变换以产生密文的过程。
解密	加密过程对应的逆过程。
智能密码钥匙	实现密码运算、密钥管理功能，提供密码服务的终端密码设备。
PKI	公钥基础设施（Public Key InfrastructureI）

## 2 产品介绍

### 1.1 产品简介

证书应用环境由北京数字认证股份有限公司自主研发，是一款基于 PKI 技术的应用安全基础套件。提供证书助手和证书应用中间件，满足终端用户的证书颁发和证书应用需求。

本软件可以广泛应用于网上审批、网上办公、网上银行、网上证券和网上支付等电子政务和电子商务活动中，与安全服务端配合使用，保障各业务系统信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的合法性，从而为业务系统提供安全保护。

### 1.2 产品架构

证书应用环境主要包括四部分：应用组件、证书助手、在线升级工具、USB-Key 设备驱动程序。软件架构如下图所示：

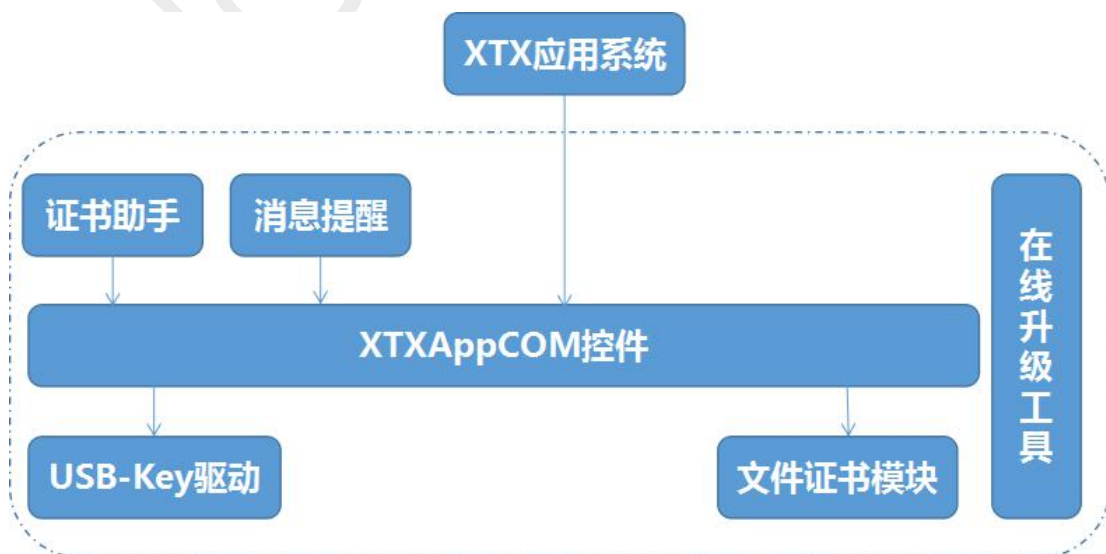


图 1.2 产品架构

**证书应用组件：**该部分是客户端环境的核心组成部分，包含 XTXAppCOM 控件、文件证书模块及 SecX 兼容控件。证书应用组件有以下三个主要特点：

1. 符合规范：证书应用组件的定义和实现遵照国密局颁发的 GMT0020-2012 《证书应用综合服务接口规范》；

2. 功能丰富：以接口动态库的形式发布，供部署在终端机上的应用客户端程序和证书助手集成调用，实现数据存取、证书管理、密码运算等功能，并与应用服务端配合，完成客户端用户身份认证、数字签名验证等功能；

3. 形式多样：新组件同时还兼容了 BJCA 原有 SecX ComV1、SecX ComV2 的常用接口，保证上层应用在客户端组件升级的过程中无需任何改动。

**证书助手：**通过调用应用组件完成对数字证书的管理和介质驱动的检测，通过调用在线升级工具完成 USB-Key 驱动在下载更新。

**在线升级工具：**通过自动连接在线升级服务，检测最新版本并下载安装。

**USB-Key 驱动：**被证书应用组件调用，实现证书应用组件与 USB-Key 的指令交互和数据传输。

## 1.3 产品功能

证书应用环境主要提供了三方面的功能：

### ■ 与上层应用集成

证书应用环境以客户端应用组件的方式为上层的证书应用系统提供简洁、易用的调用接口，提供的主要接口功能有：

- 1) 对称算法加解密数据和文件
- 2) RSA 加解密数据
- 3) 对数据和文件签名认证
- 4) 数字信封
- 5) 验证解析证书
- 6) 产生密钥对
- 7) 产生证书请求

## 8) 证书安装

应用系统可通过调用客户端组件实现数字证书身份认证、业务数据签名验证、敏感信息加解密等业务操作，从而保证业务系统的安全性，并为上层应用屏蔽了各 USB-Key 设备的差异性，屏蔽了各型号 USB-Key 设备的密码应用接口之间的差异性，实现应用与密码设备无关性，可简化应用开发的复杂性。

### ■ 供证书用户使用

证书应用环境提供证书助手，为用户提供证书环境、数字证书及 USB-Key 的检测修复、配置管理、消息提醒、证书在线服务功能。证书助手的主界面如下图所示：



客户端首页

### ■ 为终端软件升级

证书应用环境提供了在线升级工具，能够自动检测客户端软件的最新版本，并下载安装，还提供了在线升级工具自身的安装、更新和卸载、开机自启动、配置服务端地址、为低级别的操作用户提权等功能，以简化用户对在线升级工具的操作使用。

### 3 产品安装说明

本产品是软件方式安装部署，请参见：《证书应用环境软件安装部署手册》。

BJCA 证书助手



## 4 使用操作说明

### 4.1 使用前准备

- 1、检查环境满足：winxp、win7、win10、win11，支持 32 和 64；
- 2、准备并安装了“证书应用环境安装程序 V3. 8. 2. exe”程序。

### 4.2 使用说明

界面组成：快捷键、主界面信息、版本号和版本更新。



主界面

说明：本章节选择重点主要的功能操作进行说明，不常用的此处不再介绍。

## 4.2.1 启动运行

首先准备好 Usbkey 设备并插入到电脑的 USB 口上。

### 4.2.1.1 插入 UsbKEY

- 正常情况：

双击“开始菜单->BJCA 客户端->BJCA 证书助手”，正常弹出下图所示界面：



图 4.2.1.1-1 助手正常启动界面



图 4.2.1.1-3 不带提醒未插入 key 时的界面

说明：有的情况无法运行，这种情况需要给用户提升权限才能使用，请联系系统管理员，切换到管理员权限登录后，再运行证书助手。

#### 4.2.1.2 拔掉 UsbKEY

当插拔 UsbKey 时都会触发该功能，用户只需根据弹出的提示框来做相应的操作即可。



图 4.2.1.2 拔掉 Usbkey

## 4.2.2 首页

首页展示“证书信息”、“修改密码”、“找回密码”、“证书更新”、“设置”、“帮助”、“关于”等功能展示。

### 4.2.2.1 证书信息

提供对您的数字证书基本信息的查看功能，如果插入多个 Key 则会显示当前所选择 Key 的信息，您可自己选择要查看的证书，如下图所示；



图 4.2.2.1 证书信息

#### 4.2.2.2 更多证书信息

查看详细证书信息点击“更多证书信息”按钮，如下图所示；



图 4.2.2.2 更多证书信息

#### 4.2.2.2.1 导出证书

点击“导出证书”按钮，如下图所示，选择要导出证书的位置，输入导出的证书名称后，点击保存，即可导出用户证书。

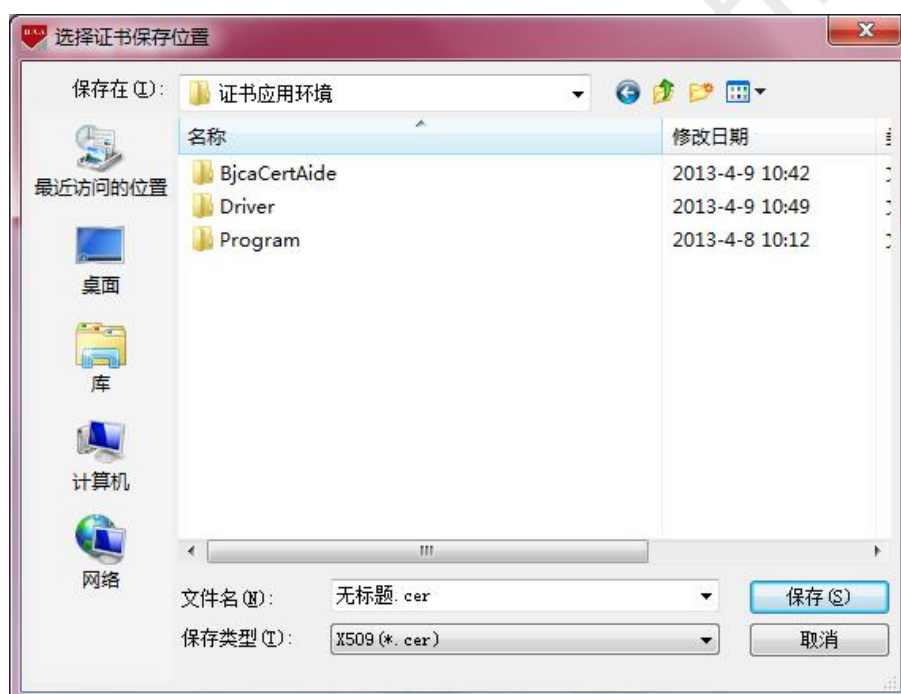


图 4.2.2.1 导出证书

#### 4.2.2.2.2 检查证书

点击“检查证书”按钮，如下图所示：



图 4.2.2.2 检查证书

### 4.2.2.3 修改密码


在首页点击“修改密码”按钮，修改密码时须按照新密码格式输入新密码：两次输入的新密码必须一致。具体操作如下图：



图 4.2.2.3 修改证书密码

#### 4.2.2.4 找回密码



点击 **找回密码** 按钮，执行两种情况，具体如下：

外网环境：打开 IE 浏览器，并跳转到找回密码对应的地址；

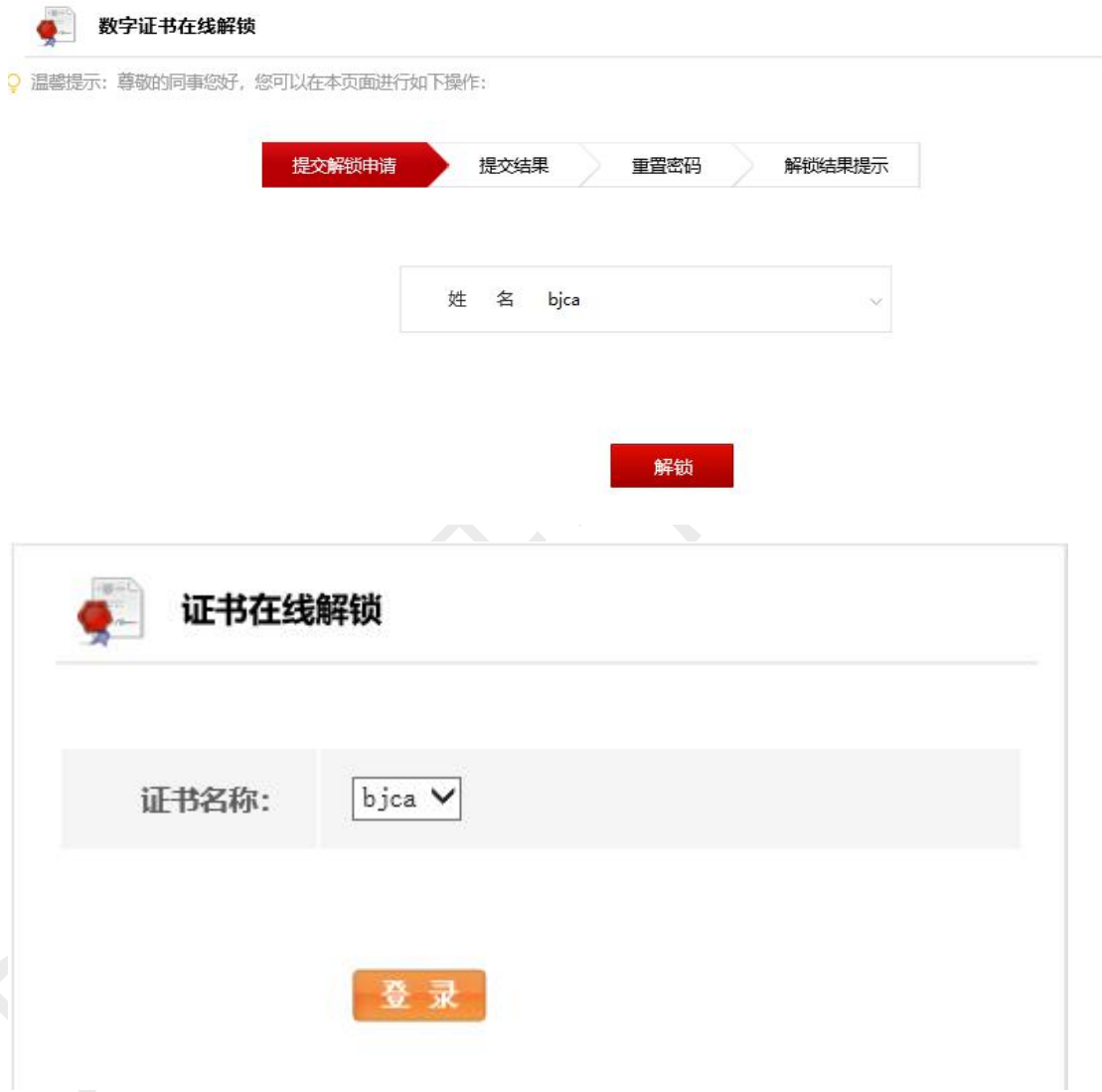


图 4.2.2.4-1 找回密码


内网环境：弹出提示框，提示用户联系系统管理员解锁，如下图：





图 4.2.2.4-2 找回密码

#### 4.2.2.5 证书更新

点击  按钮，执行两种情况，具体如下：

外网环境：打开 IE 浏览器，并跳转到证书更新对应的地址；





图 4.2.2.5-1 证书更新

内网环境：调用进程外控件，进行证书更新，如下图：



图 4.2.2.5-2 证书更新

#### 4.2.2.6 环境检测

本功能会详细的检测您的机器环境是否满足证书应用环境运行使用的要求，并将详细的检测项结果显示给您。


点击  环境检测 按钮即可，检测界面如图所示。



图 4.2.2.6-1 环境检测

您此时可点击“重新检测”再检测一遍，亦可点击“首页”返回首页；

当有检测项不通过时显示类似如图的界面；



图 4.2.2.6-2 检测未通过

此时，您需要点击“全部修复”进行修复，亦可点击“详情”查看未通过项的具体信息；

全部修复可以修复检测过程中不满足证书应用环境的设置（包括浏览器设置、控件安装、驱动安装等）。

只能修复 IE 设置、控件等问题，对于用户的操作系统版本、IE 版本、USB-Key 未插入等不可修复项给出提示和建议。

非管理员权限运行的证书助手，不能进行修复操作。

接口名字	检测状态
SOF_GetUserList	检测成功
SOF_Login	检测成功
SOF_Logout	检测成功
SOF_GetFinRetryCount	检测成功
SOF_GetCertInfo	检测成功
SOF_GetCertEntity	检测成功
SOF_SignData	检测成功
SOF_VerifySignedData	检测成功
SOF_EncryptData	检测成功
SOF_DecryptData	检测成功
SOF_SignMessage	检测成功
SOF_VerifySignedMessage	检测成功
SOF_GenRandom	检测成功
SOF_Base64Encode	检测成功
SOF_Base64Decode	检测成功

图 4.2.2.6-2 接口检测

点击“接口检测”按钮，对 XTXAppCOM 控件常用接口进行调用校验；

#### 4.2.2.7 检查更新

点击左下角 **检查更新**，弹出如图所示界面；



图 4.2.2.7 检测通过

点击弹出界面的“检查更新”按钮，检查当前是否有最新的证书助手更新版本，如已是最新版本，会显示当前版本已是最新版本；如果还有更高版本，显示更高版本的信息。

## 4.2.3 设置

点击“设置”进入如图所示页面



图 4.2.3 系统环境

主要包括五大项设置：系统设置、自动更新、日志管理、口令设置、拔出UKey；

### 4.2.3.1 系统设置

点击右上角的“恢复文件证书”，弹出选择证书备份文件窗口，默认路径为本机备份文件证书的路径，如图所示：

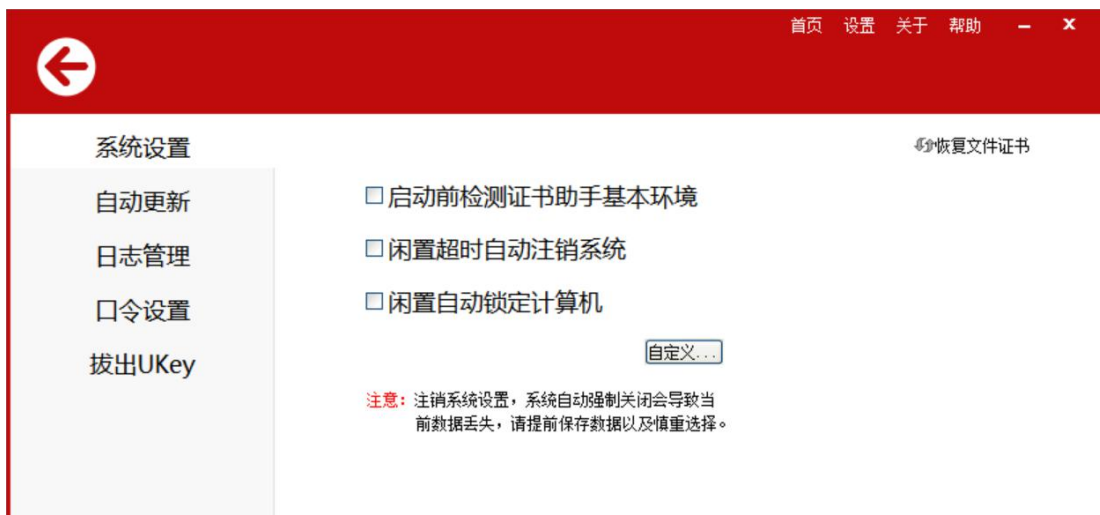


图 4.2.3.1 系统环境

#### 4.2.3.2 自动更新

如图所示，可以自己选择或输入证书助手自动更新的时间，可以选择 7 天，15 天，30 天，或者自定义，自己确定多少天更新。



图 4.2.3.2 自动更新

### 4.2.3.3 日志管理

如图所示，可以设置生成日志的级别以及大小；可以清空日志也可以导出日志到指定目录；



图 4.2.3.3-1 日志管理



图 4.2.3.3-2 日志管理



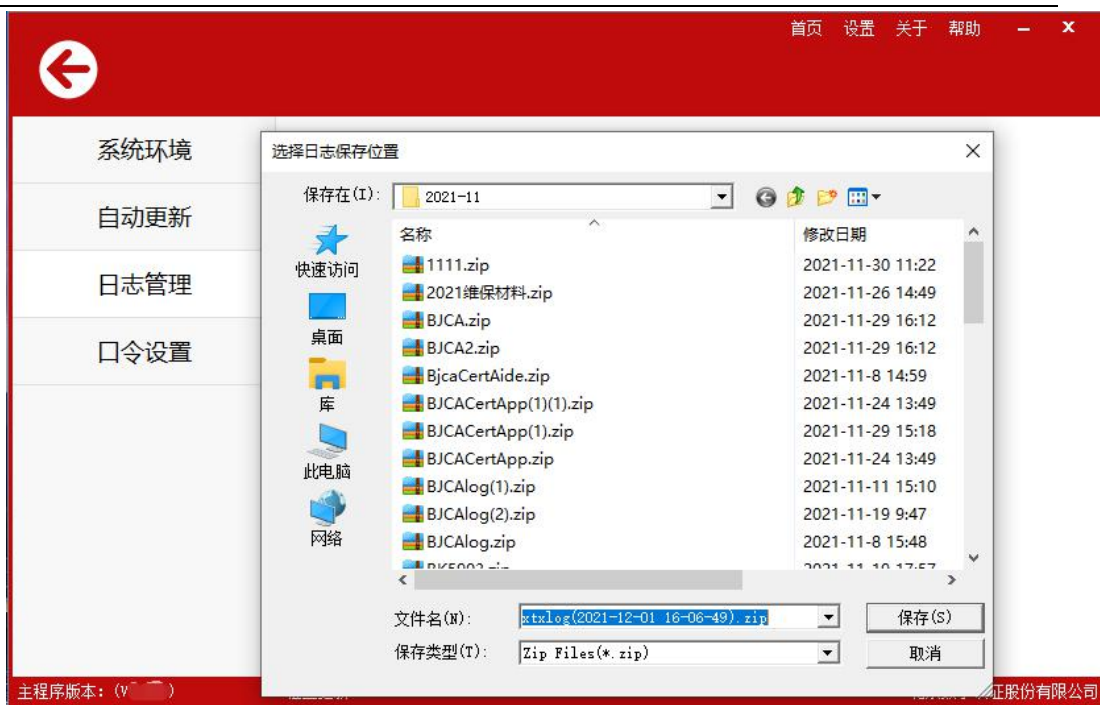


图 4.2.3.3-3 导出日志

#### 4.2.3.4 口令设置

如图所示，可以自己设置口令的有效期；



图 4.2.3.4 口令设置

### 4.2.3.5 拔出 UKey



图 4.2.3.5 拔出 UKey

### 4.2.4 关于

点击“关于”标签，打开关于页面，显示客户端常用的组件版本及安装信息，如图所示。

组件名称	组件版本	组件状态
32位客户端应用组件	3.8.22.923	已安装
64位客户端应用组件	3.8.22.923	已安装
32位XTXSecX兼容控件	2.14.1.2	已安装
64位XTXSecX兼容控件	2.14.1.2	已安装
32位XTXSecXV2兼容控件	2.14.1.2	已安装
64位XTXSecXV2兼容控件	2.14.1.2	已安装
BJCA证书助手	3.8.0.1	已安装

图 4.2.5 关于

## 4.2.5 帮助



图 4.2.4 帮助界面

**常用网站：**此处显示的是一些常用的网址的链接，您可点击某一项打开其链接，亦可点击“管理”，进行添加修改。

**常见问题：**对常用下载的说明，限数字认证内部使用。

**在线客服：**用于在线解答和人工解答问题（需要开通外网访问）

**意见反馈：**打开外网地址，填写 BJCA 服务质量调查。（需要开通外网访问）

## 4.2.6 消息提醒

当插入 UsbKey 时会检测当前证书的有效期，如果有过期证书则在桌面右下角弹出提示窗口，提示内容如下：

- 1、提示当前有效期；如果证书的有效期截止日期小于即将到期天数（默

认 60 天), 提示用户证书即将到期; 如果已经过期, 提示用户已经过期;

2、除了有效期提示外, 还提供证书即将到期时的更新链接, 证书如果即将到期, 可通过更新链接, 进入到更新页面;



3、提供证书助手的帮助平台页面链接, 如有其他需要了解的问题, 可通过“自助服务平台”链接进入到用户自助服务平台。




图 4.2.3.5-2 消息提醒设置

## 4.2.7 托盘菜单

### 4.2.7.1 打开助手

左键点击桌面上的托盘图标  打开证书助手; 或者右键点击托盘图标 , 然后在快捷菜单中点击“打开助手”菜单项也可以打开证书助手。

### 4.2.7.2 退出

右键点击托盘图标 , 然后在快捷菜单中点击“退出”菜单项可以退出证书助手。



BJCA 证书助手