

（版本：v2.2）

Uyee（优易）智能密码钥匙产品

客户需求确认表

版权声明：本文档的版权属于中国金融认证中心，任何人或组织未经许可，

不得擅自修改、拷贝或以其它方式使用本文档中的内容。

中国金融认证中心

目录

[1 客户需求确认表 1](#_Toc74124534)

[2 产品外观 7](#_Toc74124535)

[3 产品规格 8](#_Toc74124536)

# 客户需求确认表

| **序号** | **类别** | **信息项** | **信息名称** |
| --- | --- | --- | --- |
|  | 重要信息 | 客户中文名称 | 中国金融认证中心 |
|  | 客户英文名称 | China Financial Certification Authority |
|  | 客户英文简称 | CFCA |
|  | 客户Logo |  |
|  | 管理工具主窗体名称 | 中国金融认证中心优易设备服务（人行集采版） |
|  | CSP Windows注册名称 | Uyee CSP v6.0 (PBOCGPC)  说明：客户定制版本，建议将Enterprise修改为客户英文简称。 |
|  | 设备序列号规则 | CFCA默认生产格式，长度固定10位。  **□**CFCA预植格式，长度固定16位，符合《CFCA预植证书DN规则》要求。  **□**客户自定义格式：  说明：序列号可由数字和大小写英文字母组成，最大长度16位。 |
|  | 光盘镜像 | 光盘镜像Logo | 工业设计团队定制 |
|  | 光盘镜像名称 | Uyee |
|  | 光盘镜像安装包内容 | Windows用户版设备服务软件  Windows PKCS#11  其它：  说明：请用户根据实际需要进行选择。如果用户同时勾选了用户版设备服务软件和PKCS#11，光盘镜像内将用户版设备服务软件和PKCS#11库合并成1个安装包。 |
|  | 光盘镜像安装包名称 | UyeeServiceInstall.PBOCGPC.exe  说明：客户定制版本，建议将Enterprise修改为客户英文简称。 |
|  | 设备服务 | 安装路径 | 默认安装路径（以32位系统为例）：C:\Program Files\PBOCGPC\UyeeService  说明：客户定制版本，建议将CFCA修改为客户英文简称。 |
|  | 重复安装提示方式 | 高版本直接覆盖低版本，安装版本低于已有版本时提示并放弃安装，安装版本与已有版本相同时提示是否安装。 |
|  | 快捷方式与系统托盘图标 | 工业设计团队定制 |
|  | 用户版管理工具按钮 | 修改PIN码 关于  **□**其它： |
|  | 插入设备后弹出指定网页 | **□**支持，网页地址：  不支持 |
|  | 证书到期提醒 | 证书90天到期或即将到期提醒的文字描述：您的数字证书即将到期/已经过期，请尽快联系管理员更换证书。 |
|  | 插入设备后，设备中证书注册到IE | 自动注册 **□**手动注册  说明：SM2证书不注册到IE中。 |
|  | 拔除设备后，设备中证书从IE注销 | **□**不注销 自动注销 |
|  | 支持的浏览器 | IE6 IE7 IE8 IE9 IE10 IE11  Firefox Chrome 360  其它： Chromium 内核信创浏览器(360 或奇安信) |
|  | 管理员版设备服务软件 | 默认功能：初始化优易设备。  定制功能： 支持使用专用管理key实现远程解锁用户PIN  说明：可支持使用专用管理key实现远程解锁用户PIN等。 |
|  | PKCS11 | PKCS11库 | 支持 **□**不支持  说明：客户有电子签章功能需求时提供，单个图章文件最大64KB，Uyee内部存储空间不足时，无法创建图章对象。 |
|  | PKCS11库名称 | UKEY\_CFCA\_CFCAKey.dll  说明：客户定制版本，建议将Enterprise修改为客户英文简称。 |
|  | 默认安装路径 | 默认安装路径（以32位系统为例）：C:\Windows\System32 |
|  | SKF | SKF库 | 支持 **□**不支持 |
|  | SKF库名称 | UkeySKF\_CFCA\_CFCAKey.dll  说明：客户定制版本，建议将Enterprise修改为客户英文简称。 |
|  | 密码算法 | 非国密算法 | 不支持非国密算法 |
|  |  |
|  | 国密算法 | SM1 SM2 SM3 SM4 |
|  | 数字证书 | 证书类型 | 个人普通 个人高级 企业普通 企业高级 |
|  | 证书预植 | **□**是 否 |
|  | 证书更新与换发策略 | 默认策略：相同算法，仅保存最新可用数字证书。  **□**自定义策略： |
|  | PIN码 | 初始默认用户PIN码 | 123456 |
|  | PIN码长度 | 最短6位，最长16位。 |
|  | PIN码最大连续错误次数 | 6 |
|  | PIN码组成要求 | **□**只含有数字  **□**必须是数字和字母的组合，字母区分大小写。  **□**必须含有数字、字母、符号中两种或两种以上组合，字母区分大小写。  其它： 为数字、字母或任意组合，字母区分大小写 |
|  | 默认用户PIN使用策略 | **□**提示，并强制修改  提示，但不强制修改。每次操作，都进行相关提示  **□**不提示，也不强制修改  其它提示方式：  建议：选择“提示，并强制修改” |
|  | 操作系统 | Windows系统 | win xp 32  win server 2008 32/64  win 7 32/64  win 8 32/64  win 10 32/64  其它版本： |
|  | 其它操作系统 | **□**Mac OS，需要提供的软件和主要功能：    其它操作系统需求：组合如下：   1. UOSV20 x86 Chromium 内核信创浏览器(360 或奇安信)注:针对涉及商密要求的系统，大众版尚不支持，统一采购购商用版 Chromium 内核商密浏览器。 2. UOSV20 ARM 浏览器同上 3. 银河麒麟V10/V10SP1 x86 浏览器同上 4. 银河麒麟V10/V10SP1 ARM 浏览器同上   说明：如需提供信创环境支持，需要明确列出操作系统、硬件平台，以及使用的浏览器。 |
|  | 其它 |  | 说明：以上4个平台，均需要提供对应的P11和SKF相关接口  SKF需要支持如下  /\*  \* 使用容器中指定的私钥解密数据  \* hContainer [IN] 容器句柄  \* bSignFlag [IN] TRUE表示使用签名私钥解密，FALSE表示使用加密私钥解密  \* pbWrappedData [IN] 待解密的数据 当容器为ECC类型时，此参数为ECCCIPHERBLOB密文数据  \* ulWrappedDataLen [IN] 待解密的数据长度  \* pbData [OUT] 指向解密后的数据缓冲区指针，当为NULL时可获得解密后的数据长度。  \* pulDataLen [IN OUT] 输入时表示结果数据缓冲区长度，输出时表示结果数据实际长度。  \*/  typedef ULONG SKFX\_PriKeyDecrypt(  IN HCONTAINER hContainer,  IN BOOL bSignFlag,  IN BYTE \*pbWrappedData,  IN ULONG ulWrappedDataLen,  OUT BYTE \*pbData,  IN OUT ULONG \*pulDataLen  ); |

# 产品外观





# 产品规格

|  |  |  |
| --- | --- | --- |
| **类别** | | **指标** |
| 密码算法 | | SM1、SM2、SM3、SM4、RSA2048、SHA256等。 |
| 随机数 | | 符合GB/T 32915-2016相关要求 |
| 安全芯片处理器 | | 国家商密认证32位安全处理器 |
| 电气特性 | USB接口协议 | Type A型 USB插头/USB 2.0 |
| 状态灯 | LED |
| 工作电压 | 3.5V-5.5V |
| 工作电流 | <100mA |
| 气候环境适应性 | 工作温度 | 0℃～60℃ |
| 贮存运输温度 | -20℃～55℃ |
| 工作相对湿度 | 20%～85%（40℃） |
| 贮存运输相对湿度 | 20%～93%（40℃） |
| 机械环境适应性 | 静电，接触放电 | ±4kV |
| 静电，空气放电 | ±8kV |
| 跌落 | >1m |
| 振动 | 频率范围：10Hz～150Hz  振动幅值：3.5mm  持续时间：30min |
| 防尘防水 | GB/T 4208-2008 ：IP44 |