## 附件1

## 江西•农商银行网上银行二代USBKEY

## 技术规格标准

一、产品外观参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **功能** | **技术参数** | **备注** |
| 1 | 外观设计 | * 外观美观、大方、携带方便、易用。 | 提供良好的用户体验 |
| * 壳体尺寸一般不超过75mm\*45mm\*8mm | 尺寸标准（长\*宽\*厚度） |
| * 外壳为高强度高韧性高耐磨的PC材质或金属材质或含玻璃纤维材质 * 抗扭曲、耐磨，耐高、低温，手感顺滑、质感良好 | 外壳标准 |
| * 支持4个按键；用户可实现确认、取消交易，上下翻页显示信息的功能；使用次数不低于10万次； * 确认：用于用户确认信息 * 取消：用于用户取消操作 * 上翻：用于用户查看上页显示信息 * 下翻：用于用户查看下页显示信息 * 开关机：用于蓝牙USBKEY开机和关机，可与取消按键复用，短按为取消，长按为开关机 | 按键设计应美观、大方，符合大众操作习惯，按键按下后可正常弹回，按键不回弹时不应导致使用异常，支持根据银行要求定制 |
| * 附带不短于30cm的标准USB延长线 | 自带线KEY不做要求 |
| * 背光LCD显示屏或OLED自发光显示屏，采用128\*64以上点阵 * 不少于4行×16字符，可显示交易、翻页提示信息 * 每行8个汉字或16个英文字符，字体大小不小于8磅 | 支持0x00到0x7F内所有可见ascii字符，所有字库应进行加密，避免被篡改 |
| * 提供满足银行业务需求的接口设计，可实现设备连接、通信和传输数据等功能，能够满足与市场中常用的不同品牌、类型的移动终端设备稳定连接。 | Micro 或Mini USB或Tape C接口、蓝牙USBKEY配备蓝牙协议支持 |
| 2 | 定制设计 | * 支持按照银行的要求进行定制化印刷，例如：行方Logo、名称、序列号、客服电话、网银登录地址、手机登录地址、风险提示标语等信息 | 可根据银行需求随时修改，并制定多个不同的版本 |
| 3 | 配件 | * 提供满足银行需求的配件 |  |

二、产品硬件参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **功能** | **技术参数** | **备注** |
| 1 | 密钥管理 | * 要求私钥由COS内部管理，使用COS文件访问指令不得访问到私钥文件 * 密钥对生成必须由COS内部实时生成，COS内部不得固化密钥对和保留用于生成密钥对的静态因子。 |  |
| 2 | COS指令 | * COS支持的所有指令及所有参数，运行在安全芯片中，不得留有后门指令，不得泄露安全敏感信息 |  |
| 3 | 抗SP攻击 | * USBKEY在执行不同指令操作时，其功耗电流变化波型不得泄露COS内部安全敏感信息 |  |
| 4 | 抗物理攻击特性 | * 要求USBKEY在高低温、强光、强紫外线、强电磁辐射和强静电环境下保存和工作，不得泄露COS内部安全敏感信息 |  |
| 5 | 电流 | * USB模式：最大工作电流≤100mA * 蓝牙模式：最大工作电流≤70mA |  |
| 6 | 电压稳定性 | * 要求USBKEY在高、低电压或者电压波动状态下工作时，不得泄露COS内部安全敏感信息 * USB模式：4.5V～5.5V范围内正常工作 |  |
| 7 | 电池 | * 内置可充电电池，符合国家锂离子蓄电池规范，通过中国质量认证中心产品认证 * 电池寿命不少于5年，在产品使用与存放过程中应当有保护措施，防止电池过放与泄露 * 充满电后，静置6个月电量下降不超过50% * 电量从零至充满电不多于4小时 * 满电状态下，进行300次/小时速率的普通签名操作，至少可使用3小时。 | 液晶USBKEY不做此要求 |
| 8 | 连接设计 | * 蓝牙KEY产品蓝牙连接能够满足与不同品牌、类型的移动终端设备相连接。 |  |
| 9 | 防尘特性 | * 整机具备防尘功能。液晶屏幕配置专用防尘垫，防止灰尘进入影响使用效果。 |  |
| 10 | 防水特性 | * 整机应具备防泼溅功能。 |  |
| 11 | 防潮特性 | * 整机应具备防泼溅功能具备防潮设计，在1～99%湿度环境可用 |  |
| 12 | 工作温度 | * -10℃～60℃ |  |
| 13 | 存储温度 | * -10℃～60℃ |  |
| 14 | 防电磁干扰 | * 具备防电磁干扰能力，能够在场强3V/m、调制频率1KHz、调制度80%的条件下从80～1000MHz进行扫频干扰后正常工作。 |  |
| 15 | 防紫外线干扰 | * 具备防紫外线干扰能力，能够在经受15Ws/cm2紫外线干扰后正常工作。 |  |
| 16 | 防静电干扰 | * 具备防静电干扰能力，能够在经受接触放电4KV、空气放电8KV的静电放电干扰后正常工作。 |  |
| 17 | 防静电 | * 具备防静电设计，能够在干燥环境中正常使用。 |  |
| 18 | 防跌落 | * 符合1.5米跌落硬质地面标准 |  |
| 19 | 防拉 | * USB延长线能承受5kg拉力测试 |  |
| 20 | 按键异常处理要求 | * 当按键损坏无法抬起，处于长按状态时，交易签名核对页面应无法弹出，不应展示KEY显信息或认作连续完成按键行为。 |  |
| 21 | 蓝牙特性 | * 支持BLE4.0低功耗协议 * 蓝牙设备具有独立的MAC地址 * 准确测量当前电池实际电量，并实时显示。 * 连接状态显示 |  |

三、产品软件参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **功能** | **技术参数** | **备注** |
| 1 | 适用操作系统 | * 以下所列操作系统必须全部支持，并能支持简体中文、繁体中文和英文三种语言的版本 * 支持WinXP、Win2003、Win2008、Win2016、Vista、Win7、Win8、Win10、Win11等各种版本系统，兼容32位和64位系统 * 支持linux2.6及以上版本 * 支持Mac O SX 10.10及以上版本 * 支持信创操作系统（统信、麒麟） * 蓝牙USBKEY需支持iOS 6、Android 4.3平台以上等手机操作系统，支持鸿蒙NEXT系统、平板电脑，能够兼容市场上的所有主流手机 |  |
| 2 | 移动平台蓝牙通讯兼容性要求 | * 应支持与iOS、Android及鸿蒙手机主流机型通讯，包括华为、小米、三星、魅族、锤子、OPPO、VIVO、HTC、LG、夏普、联想、摩托罗拉、一加及Apple等品牌2010年以后发布的机型 * 应对蓝牙通讯涉及的相关设置及权限进行对应配置，保证可在手机各种异常环境下正常通讯并成功执行全部功能。 * 移动端软件应对软件完成全部功能所需的权限进行处理，在使用相关权限前进行申请，保证可正常执行所有功能，同时不影响其他软件的正常执行（包括但不限于检测并提示用户位置权限） |  |
| 3 | 适用浏览器 | * 支持Internet Explorer 6.0及以上版本 * 支持Edge浏览器1703及以上版本 * 支持FireFox 10.0及以上版本 * 支持Safari 7及以上版本 * 支持Chrome 38.0及以上版本 |  |
| 4 | 设备类型 | * CCID、HID或USBMassStorage设备，在Windows2000以上平台，第一次插入计算机可自动安装USBKEY软件，如用户系统屏蔽了自动安装功能，要求可以手动运行USBKEY内的安装包进行安装 |  |
| 5 | 芯片类型 | * 32位安全芯片 |  |
| 6 | 芯片安全存储容量 | * 安全芯片存储容量不小于 64KB（存储 COS、密钥、证书、蓝牙协议栈等关键数据） |  |
| 7 | 普通存储容量 | * 1MB以上 （存储驱动安装引导程序、字库等） |  |
| 8 | COS 标准 | * 符合ISO7816-4标准 * 具有自主知识产权 |  |
| 9 | 显示要求 | * 显示屏可显示银行系统指定的交易信息格式 * 支持一次批量审核50笔以上交易 |  |
| 10 | 签名流程 | * 进行签名操作时，由客户端软件将交易关键信息的原文传入USBKEY中，USBKEY解析显示关键交易信息，并等待用户物理按钮确认后，COS进行签名 * USBKEY要具有将签名原文和签名值同时回传的功能，并且可以通过指令指定是否回传原文 * 所有涉及私钥操作的COS指令，只要传入的数据符合银行签名数据的编码格式，COS自动显示交易信息并等待用户确认。是否需要用户确认由COS进行判断，不得由USBKEY外部控制 * USBKEY等待用户确认期间，用户可以通过软件操作取消签名指令，如用户没有取消也没有确认，USBKEY需要在一定超时时间后自动取消交易并返回错误码 |  |
| 11 | 用户确认方法 | * 用户通过显示屏核对交易信息无误后，按动USBKEY上的确认按钮，USBKEY进行交易数据签名，并返回签名值 |  |
| 12 | 硬件接口 | * 具有一个Micro 或MINI USB或Tape C接口，符合USB2.0规范，在USB1.1及以上接口能正常工作。 |  |
| 13 | 蓝牙特性要求 | * 蓝牙USBKEY需要具有绑定至少4台已配对手机设备功能 * 蓝牙USBKEY连接要求：要求产品的使用模式不能冲突，蓝牙接口的使用与USB接口的使用有逻辑限制。设计模式为谁先通信谁先占有模式：当USB已连接并已有数据通信时，当前不能再使用蓝牙连接；当蓝牙已连接并已有数据通信时，当前不能再使用USB连接（但此时仍可以插入PC端充电） * 蓝牙通信要求：应采取有效措施保证蓝牙通讯稳定，应采取有效措施保证蓝牙通讯连续性，蓝牙通讯时的交易数据采用加密方式传输，防止其他人截获交易信息造成信息泄露，蓝牙通信信号范围控制在10米以内 * 蓝牙通讯模式下，交易签名时间小于3 秒(签名时间包括三部分:从手机端提交签名请求到 PIN密码框出现，从Verify PIN 到 USBKEY上显示签名信息的时间和从按OK键确认到签名数据回传到手机的时间)。设备应支持设定蓝牙通讯超时时间，在超时时间内被中断的通讯可以自动恢复 * 支持蓝牙4.0BLE 及以上版本连接，具备省电模式，30秒不通信进入低功耗睡眠模式，通信断开5 分钟后自动关机 * 必须以安全方式与手机建立蓝牙连接 * 可采用蓝牙芯片自带协议栈， * 蓝牙芯片必须确保与手机设备极优的稳定性、 兼容性 |  |
| 14 | 证书需求 | * 可以存放多张数字证书 * 支持预置CFCA证书 |  |
| 15 | 证书安全 | * USBKEY应采取有效措施保护客户证书下载安全，防止篡改与证书盗用，保证交易安全； |  |
| 16 | 支持算法 | * 支持3DES（128位及以上密钥）对称算法 * 支持MD5、SHA1、SHA-256、SHA-512哈希算法 * 支持1024位和2048位RSA算法 * 支持SM2（256位密钥）、SM3、SM4（128位密钥）算法 |  |
| 17 | 密钥对生成 | * USBKEY内部硬件支持密钥对生成算法，密钥对必须安全芯片内部生成，私钥在任何时刻都不得以任何形式出现在芯片外部。 |  |
| 18 | 数字签名算法 | * RSA2048-SHA1算法，RSA2048-SHA256算法，RSA2048-SHA384算法，RSA2048-SHA512算法，SM2-SM3算法，签名运算必须在USBKEY内进行 |  |
| 19 | 密钥长度 | * RSA支持1024位、2048位密钥对生成及签名算法 * SM2支持256位密钥对生成及签名算法 |  |
| 20 | RSA密钥对生成时间 | * 生成1024位RSA密钥对平均时间≤2秒 * 生成2048位RSA密钥对平均时间≤8秒 |  |
| 21 | RSA签名时间 | * 生成1024位RSA签名平均时间≤100毫秒 * 生成2048位RSA签名平均时间≤200毫秒 |  |
| 22 | SM2密钥生成时间 | * SM2密钥对平均时间≤74.75 ms/对 |  |
| 23 | SM2签名时间 | * SM2签名平均时间≤32.35 ms/次 |  |
| 24 | PIN码传输要求 | * PIN码必须经过加密才能在物理通道上传输，修改和验证PIN码时USB端口、蓝牙接口传输的数据不得出现PIN码明文 |  |
| 25 | 证书下载 | * 支持PC端下载/更新证书 |  |
| 26 | 支持语言 | * 支持简体中文、繁体中文、英文显示 * 支持GBK、UTF-8编码 * 内置GB18030编码格式字库 |  |
| 27 | 随机数发生器 | * 内置硬件随机数发生器，能产生真随机数，并符合国际FIP140-2标准，通过商用密码管理局测试 |  |
| 28 | 芯片读写次数 | * ≥10万次 |  |
| 29 | USB头稳定性 | * 插拔次数≥5000次 |  |
| 30 | 存储有效期 | * ≥10年 |  |
| 31 | 多厂商支持 | * 可同时使用两个以上商业银行不同厂商的网上银行二代USBKEY，相互之间互不干扰。 |  |
| 32 | 蓝牙通讯休眠处理 | * 一段时间无数据通信和无按键操作进入休眠状态；一段时间无数据通信和无按键操作自动关机；在休眠状态下可通过数据交互或按键唤醒 |  |
| 33 | 无缝集成能力 | USBKEY驱动程序需全面适配网上银行客户端及网银助手产品，实现以下集成特性：   * 支持静默安装模式，通过后台进程自动完成驱动部署，无需用户手动干预。 * 兼容主流操作系统环境（Windows 7/10/11、macOS 10.15+、Linux 主流发行版）、信创环境（统信/麒麟操作系统）。 * 与现有安全防护机制（如数字证书校验、密码控件、签名控件）深度协同。 |  |
| 34 | 更新管理 | * 提供标准化驱动更新检查接口，深度适配网银助手与网上银行客户端运行场景，实现网银助手与网上银行客户端启动时的自动化驱动检测与更新功能。 |  |
| 35 | 产品资质 | * 国家密码管理局商用密码产品认证证书 * 公安部计算机信息系统安全产品销售许可 * 国家版权局计算机软件著作权登记证书 * 中国金融认证中心的数字证书设备认证证书 |  |