企业网银蓝牙KEY技术参数

参数一

|  |
| --- |
| **物理特性** |
| 简称 | 蓝牙Key |
| 尺寸 | 59.5\*35.9\*4.6mm |
| 重量 | 10.6g |
| 颜色 | 白色 |
| 外壳材料 | ABS |
| 表面处理 | 哑面 |
| 面板 | PMMA（颜色、LOGO可定制） |
| 序列号 | 后壳LOGO丝印，序列号镭雕，可定制 |
| 抗性 | 从1.5米高处跌落硬质地面不影响正常工作，防水，防静电。 |
| **交互式组件参数** |
| 按键支持 | 四个按键，确定、取消/开关机、上翻、下翻。 |
| 按键耐用性 | ≥100,000次 |
| 屏幕类型 | LCD |
| 屏幕尺寸 | LCD：非点阵屏,26.58mm×14.86mm,16\*4(EN),8\*4(CH), |
| 显示 | 4行，每行可显示16个字符（8个汉字）。 |
| 可视角度 | 左右 ≥ 50°，上下 ≥ 50° |
| 字体大小 | LCD:10磅 |
| 编码格式 | UTF-8、GBK，默认采用UTF-8格式。 |
| 字符集 | GB18030，兼容GBK，约27000个字符。 |
| 显示语言 | 简体、繁体中文、英文/其他国语言 |
| **硬件参数** |
| USB接口 | Micro母头 |
| 蓝牙特性 | 单模：蓝牙BLE。 |
| 蓝牙传输性能 | 单模：＞16Kb/s |
| 蓝牙通讯距离 | 3米内。 |
| 电池 | 可充电电池。空电满充：2小时。满电续航：2.5小时以上（双模）/5小时以上（单模）。满电待机：6个月以上。 |
| 蓝牙搜索时间 | 单模：<1s。 |
| 自动休眠 | 可支持待机超过 10 秒进入休眠状态（极低功耗）。 |
| 自动关机 | 待机超过 3 分钟自动关机。 |
| 工作电压 | 5V±10%。 |
| 工作电流 | 40mA、2.5mA，最大工作电流≤40mA，休眠电流≤2.5mA。 |
| 储存温度 | -40℃~85℃ |
| 工作温度 | -25℃~75℃ |
| 工作湿度 | 0~90% |
| 资质认证 | BQB、FCC、CE、RoHS、国密 |
| **软件参数** |
| PC平台系统支持 | WINDOWS、MACOS、Linux，通过USB方式接入。 |
| 移动平台 | Android、iOS，通过蓝牙方式接入。 |
| 浏览器 | 支持微软（基于IE 内核的如IE6及以上、360、TT、Maxthon等）、苹果（safari）、火狐（Firefox）、谷歌（Chrome）等主流浏览器。 |
| 驱动类型 | HID、CCID可选，默认采用HID驱动，支持智能卡登录需要采用CCID驱动。 |
| COS规范 | 支持ISO7816标准规范。 |
| 自动运行 | 可支持，默认无自动安装支持，安装包大小最大不超过1.2M。 |
| PC平台二次开发 | CSP、PKCS11、SKFAPI，动态库方式提供。 |
| 移动平台二次开发 | 自定义接口。 |
| 内置算法 | 哈希算法：MD5、SHA1、SHA256、SHA384、SHA512、SM3（可选）对称算法：DES、3DES、SM1、SM4（可选）、AES（可选）非对称算法：RSA1024、RSA2048、RSA4096（可选）、SM2（可选）、ECDSA（可选）、ECDH（可选） |
| 证书支持 | X509、CFCA预植、双证，CFCA预植支持需要特殊说明；支持签名证书和交换证书功能；同时支持RSA证书和SM2证书。 |
| 证书规范 | 支持ITU-T X.509 V3标准证书存储。 |
| 证书机制 | 具备证书自动注册到IE和从IE中注销功能。 |
| 随机数 | 支持硬件真随机数发生器。 |
| 内存 | 64K/128K |
| 可擦写次数 | ≥100,000次 |
| 数据保持时间 | ≥10年 |

参数二

|  |
| --- |
| **软件参数** |
| 微软标准 | Microsoft Crypto APICryptographic Service Provider （CSP）CNG API  |
| 接口标准 | 支持微软标准CSP接口、PKCS#11接口以及银行自定义接口 |
| 证书规范 | 符合ITU-T X.509 V3 |
| 软件安装包 | 包含CSP、PKCS#11库、证书监控程序、驱动程序和用户USBKEY管理工具等。USBKEY管理工具除安装需要系统管理员权限以外，在已经安装好USBKEY软件的的计算机上使用普通用户身份可以正常操作USBKEY。 |
| 证书系统（CA） | CFCA、农信银中心证书及银行自建证书系统。 |
| 证书存储 | 支持RSA2048和SM2两种算法证书同时存储 |
| 密码算法 | 支持SHA1、SHA-256、SHA-384、SHA-512哈希算法支持1024位和2048位RSA算法支持SM2、SM3、SM4国密算法 |
| 软件认证资质 | 通过中国金融认证中心的认证 |
| 通过国际标准FIPS140-2 认证 |
| 通过中国信息安全测评中心的认证 |
| 兼容性 | Windows平台：支持Windows32位及64位系统，包括Windows 2000、XP、2003、2008、Vista、Win7、Win8、Win10、Linux 2.6 及以上版本Fedora/Debian/Opensuse/Ubuntu、及以上版本及以后更新版本。Linux平台：基于Kernel 内核2.6以上的32位和64位发行版本,支持麒麟系列，UOS等国产操作系统。MacOSX平台：Mac OS 9.X、10.X及以上版本 |
| **硬件参数** |
| 防止跌落 | 外壳材料注重加固及减震设计，符合1.2米跌落硬质地面的标准 |
| 防水 | 整机具备防泼溅功能，达到IPX1防水等级要求 |
| 防尘 | 整机具备一定防尘功能，灰尘侵入不影响设备正常运行 |
| 防刮花 | 液晶显示屏配置专用镜片，起保护屏幕作用 |
| 防潮 | 整机具备防潮设计，10-99%湿度环境可用 |
| 防静电干扰 | 具备防静电干扰能力，能够在经受接触放电6KV、空气放电8KV的静电放电干扰后正常工作。 |
| 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。 |
| 防冲击 | 整机具备防冲击设计，冲击加速度150m/s2，在X、Y、Z三轴向各测试，产品保证正常工作 |
| 电磁兼容 | 通过FCC认证，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。 |
| 序列号 | 采用激光刻蚀工艺；序列号规则严格按照客户编码规则生产 |
| USB接口类型 | 具有标准USB接口 |
| USB接口规范 | 符合USB 2.0规范，在USB1.1或USB2.0接口上都能正常工作 |
| 蓝牙规范 | 支持蓝牙4.0及以上 |
| USB HUB级联 | 支持5级USB HUB级联正常工作 |
| USB口插拔次数 | 2万次以上 |
| 工作温度 | -10℃ ~70℃ |
| 工作高度 | 海拔5000米以下  |
| 贮存温度 | -25℃ ~75℃  |
| 工作湿度 | 10% ~ 99% |
| 存储湿度 | 10% ~ 99% |
| 工作电源 | 5V ±5% 范围可长时间工作 |
| 工作电流 | 小于32mA |
| 数据存储 | 室温下数据保持时间可以达到100 年室温下最少擦写次数30万次 |
| 液晶屏幕寿命 | >70000 小时 |
| 整机寿命 | >7年 |
| 环保要求 | 通过RoHS认证 |
| 存储容量 | 4MB 空间 |
| 设备类型 | UDK设备 |
| 扩展设备要求 | USB Key具有确认键，用于交易数据签名的用户确认 |
| 显示要求 | 显示屏可显示银行系统指定的交易信息格式 |
| 外壳丝印设计 | 可依据银行需求提供定制化服务 |
| 按键功能 | 采用机械物理按键，能完成确认、取消、上翻页、下翻页的功能，按键大小适中，方便客户操作用户进行网上交易时可通过上\下翻页键查看交易信息；通过确定、取消键控制本次交易，口令PIN码修改、口令PIN码交易验证需通过确定按键进行确认；需要用户按确定和取消键时，设备液晶屏幕会有相应的提示。USBKey内置物理“确认”按键，用于交易数据签名的用户确认；对于SSL登录和证书下载、更新过程的签名操作不需要用户进行按键确认操作，也不需要用户输入PIN码。 |
| 按键布局 | 在保证客户操作便捷的前提下，USBKey的上下翻键须与“确定”键、“取消”键在布局上分离，原则上应不在同一操作区域，减少客户翻页浏览屏显信息时误按“确定”或“取消”键的概率，降低操作风险，提升客户体验。 |
| 按键尺寸 | “确定”键大于“取消”键 |
| 按键寿命 | 按键操作寿命10万次以上（每个按键） |
| 显示屏材质 | LCD |
| 面板点阵 | 128×64  |
| 显示字符数 | 4行×16英文字母， 4行×8个汉字 |
| 字体颜色 | 白底黑字 |
| 可视角度 | 左右≥50° 上下≥50° |
| 字体大小 | 10 磅 |

参数三

|  |  |  |
| --- | --- | --- |
| 物 理 参 数 | 芯片 | 32位国密安全芯片 |
| 工作电压 | 3.5V-5.5V |
| 工作电流 | <100mA |
| 工作温度 | -10℃～60℃ |
| 存储温度 | -10℃～40℃，过低或过高的温度长期存储会影响电池寿命。 |
| USB协议 | USB 2.0 |
| 蓝牙规格 | 支持协议 | BLE 4.0 |
| 协议栈 | 采用蓝牙芯片自带协议栈 |
| 蓝牙标签 | 支持 |
| 独立MAC地址 | 支持 |
| 通讯稳定性 | 由蓝牙芯片和蓝牙通讯协议保证。 |
| 通讯连续性 | 由蓝牙芯片和蓝牙通讯协议保证。 |
| 通讯范围 | 20m |
| 省电模式 | 30 秒不通信进入低功耗睡眠模式，通信断开2分钟后自动关机。 |
| 电池 | 使用寿命 | >5年 |
| 容量 | 100mah锂离子电池 |
| 充电工作温度 | 0℃～50℃ |
| 放电工作温度 | -10℃～40℃，过低或过高的温度长期存储会影响电池寿命。 |
| USB充电 | USB接口通信状态下可同时充电 |
| 蓝牙通信状态下可同时通过USB链接充电 |
|  | 电量显示 | 能够在主界面显示蓝牙通信状态和电池电量信息 |
| 液晶屏 | 工作寿命 | >10000 hrs |
| 分辨率 | 128×64，支持4行×16个英文字符，4行×8个中文汉字，字体约9磅。 |
| 续航能力 | 5小时，连续签名支持150分钟。 |
| 存储空间 | 安全芯片存储容量 | 64KB |
| 普通存储容量 | 4MB |
| 读写寿命 | >=10万次 |
| 存储寿命 | >=10年 |
| 外壳 | 尺寸 | 73.5mm（长）×38.2mm（宽）×8.5mm（厚） |
| 材质 | PC |
| 抗冲击 | 表面硬度大于2H，基材透光率92%以上可以达到，现使用面板抗冲击力是0.02J左右 |
| 性能 | 密钥对生成 | 密码算法 | 生成速率 |
| RSA2048bit | 5s/对 |
| SM2 | 10次/s |
| USB报文签名（非xml） | 密码算法 | 签名速率 |
| RSA1024bit | 13次/s |
| RSA2048bit | 5次/s |
| SM2 | 13次/s |
| USB报文签名（xml） | 密码算法 | 签名速率 |
| RSA1024bit | 1.2次/s |
| RSA2048bit | 1次/s |
| SM2 | 1.5次/s |
| 蓝牙方式签名（非xml） | 密码算法 | 签名速率 |
| RSA1024bit | 770ms/次 |
| RSA2048bit | 1300ms/次 |
| SM2 | 740ms/次 |
| 蓝牙方式签名（xml） | 密码算法 | 签名速率 |
| RSA1024bit | 3.07s/次 |
| RSA2048bit | 3.53s/次 |
| SM2 | 2.6s/次 |
| 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  |
| 蓝牙USBKey产品安全性检测项目技术报告 |
| 兼容性 | 支持平台与终端 | Windows 2000 Server；Windows 2003 Server；Windows 2008 Server；Windows XP；Windows Vista 32位和64位版本；Windows 7 32位和64位版本；Windows 8 32位和64位版本；Windows 10 32位和64位版本；支持Mac OS X 10.5 及以上版本；支持IOS 6、Android 4.4、windows phone8.1 及以上手机操作系统。 |
| 支持浏览器 | IE浏览器为6.0以上版本；遨游浏览器、360浏览器等基于IE内核的浏览器。FireFox/Mozilla浏览器为17.x以上版本；Chrome浏览器25.x以上版本；Safari浏览器，支持苹果电脑的MacOS X 10.x自带Safari浏览器及后续版本； |
| 功能 | 支持算法 | 支持3DES、MD5、SHA1、SHA-256等算法；支持1024位和2048位RSA算法；支持SM2、SM3、SM4等国密算法 |
| COS标准 | 自主知识版权COS系统，符合《中国金融集成电路（IC）卡规范》、《中国金融集成电路（IC）卡应用规范》 |
| COS支持的所有指令及所有参数，运行在安全芯片中，不留有后门指令，不泄露安全敏感信息 |
| 私钥由COS内部管理，使用COS文件访问指令不访问到私钥文件 |
| 密钥对生成由COS内部实时生成，COS内部不固化密钥对和保留用于生成密钥对的静态因子。 |
| 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，通过第三方权威机构测试 |
| 安全性 | 支持有效防范暴力破解、隐私窃取、远程控制、数据篡改、交易抵赖等各种安全威胁 |
| 支持在手机蓝牙设备列表中不可见，防止产品被恶意连接攻击。 |
| 支持与移动设备端的通讯中所有数据均以密文方式传输，保证数据在蓝牙通信信道传输不被截获。 |
| 采用国家密码管理局批准的安全芯片。安全芯片内置真随机数发生器，符合国家密码管理局《随机性检测规范》安全标准 |
| 具有LCD屏幕显示及按键确认等功能。可自动解析指定的报文格式，并在屏幕上显示签名数据等待按键确认。 |
| 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  |
| 蓝牙USBKey产品安全性检测项目技术报告 |