**手机盾参数介绍**

|  |  |  |
| --- | --- | --- |
| **功能** | **说明** | **功能类型** |
| **证书应用** | | |
| 数字签名 | 支持对指定数据进行签名，格式满足PKCS#1、PKCS#7标准 | 基本功能 |
| 数字签名验证 | 支持使用对指定签名进行验证，签名标准为PKCS#1、PKCS#7 | 基本功能 |
| 数字信封加密 | 支持使用数字证书制作数字信封，格式满足PKCS#7标准 | 基本功能 |
| 数字信封解密 | 支持使用数字证书解密PKCS#7数字信封 | 基本功能 |
| 对称加密 | 支持对称算法加密，算法包括SM4 | 基本功能 |
| 证书信息获取 | 支持获取证书信息 | 基本功能 |
| 密钥管理 | 密钥管理支持密钥冻结和解冻 | 基本功能 |
| **安全性** | | |
| 密钥安全 | 个人客户端和服务端密钥都被加密保护，并且服务端使用硬件密码机保护 | 高级功能 |
| 数据安全 | 随机数安全性符合《随机数检测规范》 | 高级功能 |
| 协议安全 | 符合国密SSLVPN协议进行安全保护 | 高级功能 |
| 管理安全 | 符合三权分立要求 | 高级功能 |
| 认证安全 | 通过和设备硬件绑定，保障密钥的可使用范围 | 高级功能 |
| 软件安全 | 对软件代码和服务提供安全保障 | 高级功能 |
| **易用性** | | |
| 用户界面友好 | 用户界面进行过整体设计，风格统一，易于操作、辨识 | 基本功能 |
| **扩展性** | | |
| 证书介质接口符合国密规范 | 证书介质接口满足《0016-2012智能密码钥匙密码应用接口规范》 | 扩展特性、基本功能 |
| SDK接口使用标准AIDL | 支持第三方APP单独通过自定义AIDL接口操控移动证书助手 | 基本功能、扩展特性 |
| 安全通道身份鉴别和密钥满足国密规范 | 安全通道身份鉴别和密钥交互满足规范《0024-2014\_SSLVPN技术规范》 | 基本功能、扩展特性 |
| **兼容性** | | |
| Android4.4+ | 移动端应用支持 | 兼容特性 |
| iOS 9.0 + | 移动端应用支持 | 兼容特性 |
| Windows XP SP3+ | 支持桌面操作系统 | 兼容特性 |
| Linux2.6 + | 支持国产化系统 | 兼容特性 |
| **性能** | | |
| 对称算法加解密 | ECB算法 | 2000次/S |
| CBC算法 | 2000次/S |
| SM2运算 | SM2验签运算 | 2000次/S |
| SM2签名运算 | 4000次/S |
| SM2加密 | 2000次/S |
| SM2解密 | 2000次/S |
| ECC密钥生成速度 | ECC密钥生成速度 | 8000次/S |