中金国信Uyee设备

中国金融认证中心

PKCS#11接口说明

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

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。

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 内容 | 日期 | 编写 | 审核 |
| 1.0.0.1 | 完成初稿 | 2023/03/09 | 简志栋 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目录

[一、简介 1](#_Toc129271287)

[二、遵循标准 2](#_Toc129271288)

[三、调用方法 3](#_Toc129271289)

[四、接口函数列表 4](#_Toc129271290)

# 一、简介

本文档主要描述中金国信Uyee设备PKCS#11接口，为上层应用集成开发提供参考。

# 二、遵循标准

（1）RSA Laboratories. PKCS #11 v2.20: Cryptographic Token Interface Standard. 28 June 2004.本文简称：Cryptoki.

（2）RSA Laboratories. PKCS #1 v2.2: RSA Cryptography Standard. 27 October 2012.

# 三、调用方法

按照一般的动态链接库加载方式进行调用即可。调用前请对文件的代码签名进行验证，确保库文件内容不被恶意篡改。

# 四、接口函数列表

表4-1 PKCS#11接口函数列表

| 分类 | 接口函数名称 | 功能描述 | 备注 |
| --- | --- | --- | --- |
| 通用接口 | C\_Initialize | 初始化动态库 | 详见Cryptoki第11.4节 |
| C\_Finalize | 完成动态库调用 | 详见Cryptoki第11.4节 |
| C\_GetInfo | 获取通用信息 | 详见Cryptoki第11.4节 |
| C\_GetFunctionList | 获取动态库函数的指针 | 详见Cryptoki第11.4节 |
| 槽和设备管理 | C\_GetSlotList | 获取槽列表 | 详见Cryptoki第11.5节 |
| C\_GetSlotInfo | 获取槽信息 | 详见Cryptoki第11.5节 |
| C\_GetTokenInfo | 获取设备信息 | 详见Cryptoki第11.5节 |
| C\_WaitForSlotEvent | 等待槽设备插拔事件 | 不支持 |
| C\_GetMechanismList | 获取支持的功能列表 | 详见Cryptoki第11.5节 |
| C\_GetMechanismInfo | 获取某项功能的信息 | 详见Cryptoki第11.5节 |
| C\_InitToken | 初始化设备 | 不支持 |
| C\_InitPIN | 初始化PIN | 不支持 |
| C\_SetPIN | 修改PIN | 详见Cryptoki第11.5节 |
| 会话管理 | C\_OpenSession | 打开一个会话 | 详见Cryptoki第11.6节 |
| C\_CloseSession | 关闭一个会话 | 详见Cryptoki第11.6节 |
| C\_CloseAllSessions | 关闭设备全部会话 | 详见Cryptoki第11.6节 |
| C\_GetSessionInfo | 获取会话信息 | 详见Cryptoki第11.6节 |
| C\_GetOperationState | 获得会话的操作状态 | 不支持 |
| C\_SetOperationState | 设置会话的操作状态 | 不支持 |
| C\_Login | 登录设备 | 详见Cryptoki第11.6节 |
| C\_Logout | 登出设备 | 详见Cryptoki第11.6节 |
| 对象管理 | C\_CreateObject | 创建一个对象 | 详见Cryptoki第11.7节 |
| C\_CopyObject | 创建一个对象的拷贝 | 不支持 |
| C\_DestroyObject | 销毁一个对象 | 详见Cryptoki第11.7节 |
| C\_GetObjectSize | 获取对象的大小 | 不支持 |
| C\_GetAttributeValue | 获取对象的属性 | 详见Cryptoki第11.7节 |
| C\_SetAttributeValue | 修改对象的属性 | 详见Cryptoki第11.7节 |
| C\_FindObjectsInit | 查找对象初始化 | 详见Cryptoki第11.7节 |
| C\_FindObjects | 查找对象 | 详见Cryptoki第11.7节 |
| C\_FindObjectsFinal | 结束查找对象 | 详见Cryptoki第11.7节 |
| 加密 | C\_EncryptInit | 加密初始化 | 详见Cryptoki第11.8节 |
| C\_Encrypt | 单组数据加密 | 详见Cryptoki第11.8节 |
| C\_EncryptUpdate | 多组数据加密 | 不支持 |
| C\_EncryptFinal | 结束多组数据加密 | 不支持 |
| 解密 | C\_DecryptInit | 解密初始化 | 详见Cryptoki第11.9节 |
| C\_Decrypt | 单组数据解密 | 详见Cryptoki第11.9节 |
| C\_DecryptUpdate | 多组数据解密 | 不支持 |
| C\_DecryptFinal | 结束多组数据解密 | 不支持 |
| 杂凑 | C\_DigestInit | 杂凑初始化 | 详见Cryptoki第11.10节 |
| C\_Digest | 单组数据杂凑 | 详见Cryptoki第11.10节 |
| C\_DigestUpdate | 多组数据杂凑 | 不支持 |
| C\_DigestKey | 密钥杂凑 | 不支持 |
| C\_DigestFinal | 完成多组数据杂凑 | 不支持 |
| 签名 | C\_SignInit | 签名初始化 | 详见Cryptoki第11.11节 |
| C\_Sign | 单组数据签名 | 详见Cryptoki第11.11节 |
| C\_SignUpdate | 多组数据签名 | 不支持 |
| C\_SignFinal | 完成多组数据签名 | 不支持 |
| C\_SignRecoverInit | 初始化数据可从签名结果中恢复的签名操作 | 不支持 |
| C\_SignRecover | 数据签名，数据可从签名结果中恢复 | 不支持 |
| 验签 | C\_VerifyInit | 验签初始化 | 详见Cryptoki第11.12节 |
| C\_Verify | 单组数据验签 | 详见Cryptoki第11.12节 |
| C\_VerifyUpdate | 多组数据验签 | 不支持 |
| C\_VerifyFinal | 完成多组数据验签 | 不支持 |
| C\_VerifyRecoverInit | 初始化数据可从签名结果中恢复的验签操作 | 不支持 |
| C\_VerifyRecover | 数据验签，数据可从签名结果中恢复 | 不支持 |
| 双功能密码运算 | C\_DigestEncryptUpdate | 多组数据杂凑和加密 | 不支持 |
| C\_DecryptDigestUpdate | 多组数据解密和杂凑 | 不支持 |
| C\_SignEncryptUpdate | 多组数据签名和加密 | 不支持 |
| C\_DecryptVerifyUpdate | 多组数据解密和验签 | 不支持 |
| 密钥管理 | C\_GenerateKey | 生成一个对称密钥或一组密钥参数 | 不支持 |
| C\_GenerateKeyPair | 生成密钥对 |  |
| C\_WrapKey | 封装密钥 | 不支持 |
| C\_UnwrapKey | 解封装密钥 | 不支持 |
| C\_DeriveKey | 派生密钥 | 不支持 |
| 随机数 | C\_SeedRandom | 设置随机数种子 | 详见Cryptoki第11.15节 |
| C\_GenerateRandom | 生成随机数 | 详见Cryptoki第11.15节 |
| 并行功能管理 | C\_GetFunctionStatus | 已废弃函数 | 不支持 |
| C\_CancelFunction | 已废弃函数 | 不支持 |
|  |  |  |  |