人行集采Uyee设备

中国金融认证中心

PKCS#11使用说明

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 | 初稿 | 2023/03/20 | 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、模块简介 1](#_Toc77089132)

[二、算法支持 2](#_Toc77089133)

[1. 操作系统支持 2](#_Toc77089134)

[2. 非对称加密算法 2](#_Toc77089135)

[3. 对称加密算法 2](#_Toc77089136)

[4. 哈希算法 2](#_Toc77089137)

[5. 电子签章 2](#_Toc77089138)

[三、安装使用 3](#_Toc77089139)

[1.安装 3](#_Toc77089140)

[2.卸载 3](#_Toc77089141)

[3.使用 3](#_Toc77089142)

[四、其他事项 4](#_Toc77089143)

# 一、模块简介

PKCS#11是公钥加密标准（PKCS, Public-Key Cryptography Standards）中的一份子 ，由RSA实验室(RSA Laboratories)发布，它为加密令牌定义了一组平台无关的API。人行集采Uyee设备PKCS#11模块按照此标准的v2.20版本，配合人行集采Uyee设备完成各种密码运算，以及支持制章签章功能。

# 二、算法支持

## 操作系统支持

Windows：Win XP SP3及以上版本操作系统（32位和64位）；

## 非对称加密算法

RSA： 1024/2048位

SM2：国密标准，256位

## 对称加密算法

DES、3DES、SM1、SM4

## 哈希算法

MD5、SHA-1、SHA256、SHA512、SM3

## 电子签章

最多支持4个图章对象，单个图章大小无限制，但图章总大小不超过设备的剩余可用空间（建议不超过64k）。

。

# 三、安装使用

## 1.安装

人行集采项目PKCS#11无独立安装包，需要与设备服务程序安装包集成或单独复制到系统库目录。

## 2.卸载

与设备服务程序一并卸载或直接删除动态库。

## 3.使用

Windows平台PKCS#11动态库名称“UKEY\_CFCA\_CFCAKey.dll”，Linux系统PKCS#11动态库名称为“libUKEY\_CFCA\_CFCAKey.so”。动态库位于系统库目录，在Windows系统的路径为”C:\Windows\System32”及”C:\Windows\SysWow64”，在Linux下路径一般为”/lib”、”/lib64”、”/lib/x86\_64-gnu-linux”等目录。按照一般的动态链接库加载方式进行调用即可。

# 四、其他事项

参考《pkcs-11v2-20.pdf》