人行集采电子招投标

国密SKF接口

软件需求说明书（7.1.0.0）

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 |
| 7.1.0.0 | 新建 | 2023/03/15 | 庄瑞 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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

[第一章 项目范围 3](#_Toc130372771)

[1. 项目描述 3](#_Toc130372772)

[2. 项目背景 3](#_Toc130372773)

[3. 项目目标 3](#_Toc130372774)

[第二章 操作系统 3](#_Toc130372775)

[第三章 功能需求 3](#_Toc130372776)

[1. 函数接口 3](#_Toc130372777)

[1.1 SKF\_WaitForDevEvent 3](#_Toc130372778)

[1.2 SKF\_CancelWaitForDevEvent 4](#_Toc130372779)

[1.3 SKF\_EnumDev 4](#_Toc130372780)

[1.4 SKF\_ConnectDev 4](#_Toc130372781)

[1.5 SKF\_DisConnectDev 4](#_Toc130372782)

[1.6 SKF\_GetDevState 4](#_Toc130372783)

[1.7 SKF\_GetDevInfo 4](#_Toc130372784)

[1.8 SKF\_VerifyPIN 4](#_Toc130372785)

[1.9 SKF\_ChangePIN 4](#_Toc130372786)

[1.10 SKF\_ClearSecureState 4](#_Toc130372787)

[1.11 SKF\_EnumApplication 4](#_Toc130372788)

[1.12 SKF\_OpenApplication 4](#_Toc130372789)

[1.13 SKF\_CloseApplication 4](#_Toc130372790)

[1.14 SKF\_EnumFiles 4](#_Toc130372791)

[1.15 SKF\_GetFileInfo 4](#_Toc130372792)

[1.16 SKF\_CreateFile 4](#_Toc130372793)

[1.17 SKF\_WriteFile 5](#_Toc130372794)

[1.18 SKF\_ReadFile 5](#_Toc130372795)

[1.19 SKF\_DeleteFile 5](#_Toc130372796)

[1.20 SKF\_EnumContainer 5](#_Toc130372797)

[1.21 SKF\_OpenContainer 5](#_Toc130372798)

[1.22 SKF\_CloseContainer 5](#_Toc130372799)

[1.23 SKF\_DeleteContainer 5](#_Toc130372800)

[1.24 SKF\_CreateContainer 5](#_Toc130372801)

[1.25 SKF\_ImportCertificate 5](#_Toc130372802)

[1.26 SKF\_ExportCertificate 5](#_Toc130372803)

[1.27 SKF\_GenRandom 5](#_Toc130372804)

[1.28 SKF\_GenRSAKeyPair 5](#_Toc130372805)

[1.29 SKF\_ImportRSAKeyPair 5](#_Toc130372806)

[1.30 SKF\_RSASignData 5](#_Toc130372807)

[1.31 SKF\_RSAVerify 5](#_Toc130372808)

[1.32 SKF\_ExtRSAPubKeyOperation 6](#_Toc130372809)

[1.33 SKF\_GenECCKeyPair 6](#_Toc130372810)

[1.34 SKF\_ImportECCKeyPair 6](#_Toc130372811)

[1.35 SKF\_ECCSignData 6](#_Toc130372812)

[1.36 SKF\_ECCVerify 6](#_Toc130372813)

[1.37 SKF\_ExtECCEncrypt 6](#_Toc130372814)

[1.38 SKF\_GenerateAgreementDataWithECC 6](#_Toc130372815)

[1.39 SKF\_GenerateAgreementDataAndKeyWithECC 6](#_Toc130372816)

[1.40 SKF\_GenerateKeyWithECC 6](#_Toc130372817)

[1.41 SKF\_ExportPublicKey 6](#_Toc130372818)

[1.42 SKF\_ImportSessionKey 6](#_Toc130372819)

[1.43 SKF\_SetSymmKey 6](#_Toc130372820)

[1.44 SKF\_EncryptInit 6](#_Toc130372821)

[1.45 SKF\_Encrypt 6](#_Toc130372822)

[1.46 SKF\_EncryptUpdate 6](#_Toc130372823)

[1.47 SKF\_EncryptFinal 7](#_Toc130372824)

[1.48 SKF\_DecryptInit 7](#_Toc130372825)

[1.49 SKF\_Decrypt 7](#_Toc130372826)

[1.50 SKF\_DecryptUpdate 7](#_Toc130372827)

[1.51 SKF\_DecryptFinal 7](#_Toc130372828)

[1.52 SKF\_MacInit 7](#_Toc130372829)

[1.53 SKF\_Mac 7](#_Toc130372830)

[1.54 SKF\_MacUpdate 7](#_Toc130372831)

[1.55 SKF\_MacFinal 7](#_Toc130372832)

[1.56 SKF\_DigestInit 7](#_Toc130372833)

[1.57 SKF\_Digest 7](#_Toc130372834)

[1.58 SKF\_DigestUpdate 7](#_Toc130372835)

[1.59 SKF\_DigestFinal 7](#_Toc130372836)

[1.60 SKF\_CloseHandle 7](#_Toc130372837)

[1.61 SKFX\_PriKeyDecrypt 7](#_Toc130372838)

[2. 支持的算法 8](#_Toc130372839)

# 项目范围

## 项目描述

该文档描述优易国密SKF接口的需求，按照操作系统分为Linux版和Windows版。

## 项目背景

为满足CFCA签章、智能网关等产品使用优点设备，提供相应的Linux系统和Windows系统的SKF接口动态库，支持标准企业版优易设备，支持多个优易设备同时使用。

## 项目目标

中国金融认证中心开发部进行优易国密SKF接口开发，并最终提供优易国密SKF接口动态库，上层应用可以通过国密SKF接口实现签名验签、加密解密、PIN码验证等功能。

# 操作系统

1、麒麟、统信等国产操作系统

2、Windows版支持Windows 7及以上版本

# 功能需求

## 函数接口

接口参数请参考《GM-0016-2012-智能密码钥匙密码应用接口规范.pdf》。

### SKF\_WaitForDevEvent

### SKF\_CancelWaitForDevEvent

### SKF\_EnumDev

### SKF\_ConnectDev

### SKF\_DisConnectDev

### SKF\_GetDevState

### SKF\_GetDevInfo

### SKF\_VerifyPIN

### SKF\_ChangePIN

### SKF\_ClearSecureState

### SKF\_EnumApplication

### SKF\_OpenApplication

### SKF\_CloseApplication

### SKF\_EnumFiles

### SKF\_GetFileInfo

### SKF\_CreateFile

### SKF\_WriteFile

### SKF\_ReadFile

### SKF\_DeleteFile

### SKF\_EnumContainer

### SKF\_OpenContainer

### SKF\_CloseContainer

### SKF\_DeleteContainer

### SKF\_CreateContainer

### SKF\_ImportCertificate

### SKF\_ExportCertificate

### SKF\_GenRandom

### SKF\_GenRSAKeyPair

### SKF\_ImportRSAKeyPair

### SKF\_RSASignData

### SKF\_RSAVerify

### SKF\_ExtRSAPubKeyOperation

### SKF\_GenECCKeyPair

### SKF\_ImportECCKeyPair

### SKF\_ECCSignData

### SKF\_ECCVerify

### SKF\_ExtECCEncrypt

### SKF\_GenerateAgreementDataWithECC

### SKF\_GenerateAgreementDataAndKeyWithECC

### SKF\_GenerateKeyWithECC

### SKF\_ExportPublicKey

### SKF\_ImportSessionKey

### SKF\_SetSymmKey

### SKF\_EncryptInit

### SKF\_Encrypt

### SKF\_EncryptUpdate

### SKF\_EncryptFinal

### SKF\_DecryptInit

### SKF\_Decrypt

### SKF\_DecryptUpdate

### SKF\_DecryptFinal

### SKF\_MacInit

### SKF\_Mac

### SKF\_MacUpdate

### SKF\_MacFinal

### SKF\_DigestInit

### SKF\_Digest

### SKF\_DigestUpdate

### SKF\_DigestFinal

### SKF\_CloseHandle

### SKFX\_PriKeyDecrypt

## 支持的算法



非对称算法：RSA-2048、国密SM2；

对称算法： 3DES（ECB）、SM1（ECB、CBC、MAC）、SM4（ECB、CBC、MAC）；