SIMKey安卓集成说明

# 概述

# 编写目的

给出安卓平台SIM卡SDK集成的使用说明。

# 项目结构

示例程序使用Android Studio开发，分为app和simkey\_nativelib两个模块。simkey\_nativelib为安卓native库，实现SIM卡具体功能并向外暴露接口。app为安卓应用程序，依赖simkey\_nativelib，演示了相关接口调用及使用方法。

simkey\_nativelib以cmake方式构建，依赖libsimkey.so、libtysimkeylib.so、libcurl.so 、libssl.so、libcrypto.so、libuv.so、libz.so，支持armeabi-v7a、arm64-v8a平台。

# 使用流程

# CTS协商、在线业务密钥协商



# 在线密钥协商

在线协商在cts协商的基础上增加了服务器与量子云控系统之间安全通道的建立与连接等特性，增强了密钥传输的安全性。客户端SDK使用流程与cts协商基本一致。



# 相关接口定义

# 设置文件路径

原型：public native boolean setRedirectFilePath(String filePath)

入参：filePath 文件路径

返回：是否成功

描述：设置设备及密钥相关文件的存储路径，应在动态库加载后第一时间执行。

# 枚举设备

原型：public native boolean enumDevice()

返回：是否成功

描述：枚举SIM卡物理设备，获取内部设备句柄，以供后续操作使用。

# 释放设备

原型：public native void freeDevices()

描述：释放枚举到的所有设备句柄。

# 登录设备

原型：public native boolean loginDevice()

返回：是否成功

# 登出设备

原型：public native boolean logoutDevice()

返回：是否成功

# 初始化资源

原型：public native boolean initResource()

返回：是否成功

# 更新资源

原型：public native boolean updateResource()

返回：是否成功

描述：使用密钥后需要更新内存的密钥状态到设备文件，否则会出现密钥状态与服务器不同步的问题。

# 销毁资源

原型：public native void destroyResource()

# 获取设备ID

原型：public native String getDeviceId()

返回：设备ID

# 获取系统ID

原型：public native String getSystemId(String appName, String conName)

入参：appName 应用名称

conName 容器名称

返回：系统ID

# 获取应用列表

原型：public native List<Application> getAppList()

返回：应用列表

# 删除应用

原型：public native boolean deleteApp(String appName)

入参：appName 应用名称

返回：是否成功

# 格式化设备

原型：public native boolean formatDevice()

返回：是否成功

# 查询密钥长度

原型：public native long[] queryKeyLength(String appName, String conName)

入参：appName 应用名称

conName 容器名称

返回：密钥长度数组

描述：密钥长度数组格式为[总长度, 已使用长度]，单位为字节。

# 在线充注密钥

原型：public native boolean chargeKey(String host, String appName, String conName, String userPIN)

入参：host 主机地址

appName 应用名称

conName 容器名称

userPIN 用户PIN

返回：是否成功

# 清理密钥

原型：public native boolean clearKey(String appName)

入参：appName 应用名称

返回：是否成功

# 协商在线业务密钥

原型：public native NegotiateInfo negoOLBizKey(String host, String deviceId, String systemId, String secretId, String serverId, String visitKeyBase64, String protectKey)

入参：host 主机地址

deviceId 设备ID

systemId 系统ID

secretId 密钥ID

serverId 密钥应用服务ID

visitKeyBase64 安全认证密钥

protectKey 保护密钥

返回：协商信息

描述：此为客户端协商，应配合服务端使用。

# 获取密钥句柄

原型：public native long getKeyHandle(String appName, String conName, String userPIN, String checkCode, String flag)

入参：appName 应用名称

conName 容器名称

userPIN 用户PIN

checkCode 协商校验码

flag 协商标志

返回：密钥句柄

# 获取在线协商密钥句柄

原型：public native long getOLKeyHandle(String qccsId, String sysId, String appName, String conName, byte[] flagChkV, String flag, int offerSoftKey, byte[] cipherQKey, int cipherQKeyLen, String pin);

入参： String qccsId 云控id

String sysId 密钥应用系统id

String appName 应用名称

String conName 容器名称

byte[] flagChkV 鉴别信息

String flag 密钥协商flag

int offerSoftKey 是否提供软密钥

byte[] cipherQKey 密文密钥

int cipherQKeyLen 密文密钥长度

String pin 用户pin码

返回：密钥句柄

# 释放密钥句柄

原型：public native void freeKeyHandle(long keyHandle)

入参：keyHandle 密钥句柄

描述：密钥句柄释放后不可再使用

# 加密

原型：public native byte[] encrypt(long keyHandle, byte[] plain)

入参：keyHandle 密钥句柄

plain 明文

返回：密文

# 解密

原型：public native byte[] decrypt(long keyHandle, byte[] cipher)

入参：keyHandle 密钥句柄

plain 密文

返回：明文

# 获取软密钥

原型：public native byte[] getSoftKey(long keyHandle, long keyLen)

入参：keyHandle 密钥句柄

keyLen 密钥长度

返回：密钥

描述：获取软密钥后可使用自定义软算法

# 获取在线协商软密钥

原型：public native long getOLSoftKey(String qccsId, String sysId, byte[] flagChkV, String flag, int offerSoftKey, byte[] cipherQKey, int cipherQKeyLen, String pin);

入参： String qccsId 云控id

String sysId 密钥应用系统id

byte[] flagChkV 鉴别信息

String flag 密钥协商flag

int offerSoftKey 是否提供软密钥

byte[] cipherQKey 密文密钥

int cipherQKeyLen 密文密钥长度

String pin 用户pin码

返回：软密钥

描述：获取软密钥后可使用自定义算法

# 导出证书

原型：public native byte[] exportCert(int type, String appName, String conName)

入参：type 证书类型 0-加密证书 1-签名证书 2-根证书

appName 应用名称

conName 容器名称

返回：证书

描述：返回的证书为PEM格式

# 导出公钥

原型：public native byte[] exportPubKey(int type, String appName, String conName)

入参：type 公钥类型 0-加密公钥 1-签名公钥

appName 应用名称

conName 容器名称

返回：公钥

描述：返回的公钥为PEM格式

# 验证应用PIN

原型：public native boolean verifyAppPIN(String appName, String PIN)

入参：appName 应用名称

PIN 应用PIN

返回：是否成功

描述：验证应用PIN有重试次数限制，超过重试次数会锁定PIN。