密码设备国标接口配置说明

一、依赖库及配置文件说明

1、依赖库

需要将API和国标库（libfmapiv100.so、libsgd.so）放到相应位置。

Windows环境：放到系统目录C:\WINDOWS\system32或者syswow64目录下；

Linux环境：放到/lib或者/lib64目录下；

2、配置文件

需要将配置文件（SDFDevice.conf）放到相应位置。

Windows环境：放到系统目录C:\WINDOWS\system32或者syswow64目录下；

Linux环境：放到/etc目录下；

3、SDFDevice.conf说明

```
[LOG]
level=3;                          //国标API输出日志级别
[CARDTYPE]
type=FM_DEV_TYPE_PCIE_1_0X //加密卡设备类型，可从fm_cpc_pub.h获取
[LOGPATH]
log=C:\\SDFsgd.log          //国标API日志输入位置
[KEYINDEX]
flag=1                            //私钥权限码标记
```

二、使用TestSGD之前的准备

1、pintool为设置私钥权限码工具，依赖libfmapiv100.so；

2、使用TestSGD测试国标接口之前，需要先生成2号和3号膜长为1024的RSA密钥对，生成2号和3号SM2密钥对，1号对称密钥；并使用pintool设置国标接口1号RSA密钥和1号SM2密钥的私钥权限码为12345678。

三、非对称密钥对国标密钥号与API密钥号之间的对应关系

国标接口遵循《GMT 0018-2012 密码设备应用接口规范》开发，国标的每一个密钥号对应两个非对称密钥对，其中单号用于签名验签，双号用于加密解密。

目前使用TestCard生成的密钥为API密钥号，与国标实际密钥号对应关系为，1号国标密钥，对应API接口的2号和3号；2号国标接口，对应API接口的4号和5号....以此类推，要想使用n号国标密钥，需要先调用API接口生成2n和2n+1号密钥。

使用pintool时输入的密钥号为国标密钥号。

四、关于设备密钥

根据规范，国标的0号密钥为设备密钥。

用户无法使用或修改设备密钥，并且国标的0号与API接口的0号和1号并没有实际的对应关系。即使API接口的0号和1号密钥不存在，设备密钥依然存在。

五、获取私钥权限注意事项

在调用获取私钥权限码（GetPrivateKeyAccessRight）和释放私钥权限码（ReleasePrivateKeyAccessRigh）接口时，传入的第二个参数需注意：如果是获取SM2密钥对的私钥权限，那么密钥索引值需要加上偏移量383。即如果需要获取1号SM2私钥权限，需要传入384；获取RSA私钥权限传入的索引值不变，获取1号RSA私钥，索引值传入1即可。

六、其他

目前全系列加密卡中，MINI PCI-E 2.0卡和PCI-E 5.0卡本身不支持RSA算法，

在使用TestSGD时，涉及到RSA算法的部分会报错。但并不影响您进行开发。