ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0127—2023

移动终端密码模块应用接口规范

Mobile terminal cryptographic module application interface specification

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院数据与通信保护研究教育中心、中国科学技术大学、中国科学院信息工程研究所、北京数字认证股份有限公司、北京理工大学、长春吉大正元信息技术股份有限公司、北京交通大学、中国信息通信研究院、北京信安世纪科技股份有限公司、中国人寿保险股份有限公司研发中心、国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国工业互联网研究院、中电科网络安全科技股份有限公司、格尔软件股份有限公司、北京中电华大电子设计有限责任公司、北京创原天地科技有限公司、北京小雷科技有限公司、北京国脉信安科技有限公司、财付通支付科技有限公司、北京炼石网络技术有限公司、深信服科技股份有限公司、北京路云天网络安全技术研究院有限公司。

本文件主要起草人：林璟锵、贾世杰、郑昉昱、徐博文、马原、夏鲁宁、夏冰冰、王安、高旭、黎琳、徐秀、汪宗斌、徐丽娟、张晓娜、黄晶晶、李琳、王平建、刘丽敏、王伟、牛莹姣、赵欣怡、吕娜、雷灵光、钱文飞、唐明环、于成丽、张立廷、尹一桦、赵丽丽、黄福飞、李涛、王睿、肖云松、柳增寿、袁峰、何畅、吴怡、白小勇、鲍旭华、孔勇。

引　言

在移动终端上调用各类密码模块实现密码服务的方式已逐渐普及，本文件目标是为各类移动终端密码模块的实现提供统一的应用接口规范，进一步推动密码算法在移动终端上的部署和应用。为移动终端密码模块的开发、使用及检测提供标准依据和指导，有利于提高移动终端密码模块的产品化、标准化和系列化水平。

移动终端密码模块应用接口规范

1 范围

本文件规定了移动终端密码模块的结构模型、数据类型定义、应用接口及安全要求。

本文件适用于移动终端密码模块产品的研制和使用，以及基于该类密码产品的应用开发与检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0017—2023 智能密码钥匙密码应用接口数据格式规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

密码模块 cryptographic module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

3.2

模块鉴别 module authentication

移动终端密码模块对应用程序的鉴别。

3.3

模块鉴别密钥 module authentication key

用于模块鉴别的密钥。

3.4

容器 container

密码模块中用于保存密钥所划分的唯一性存储空间。

3.5

应用 application

包括PIN、文件和容器的一种结构，具备独立的权限管理。

4 缩略语

下列缩略语适用于本文件。

MAC:消息鉴别码(Message Authentication Code)

PIN:个人身份识别码(Personal Identification Number)

5 结构模型

5.1 层次关系

在移动终端中,移动终端密码模块应用接口位于移动终端应用程序和移动终端密码模块之间,如图 1 所示。

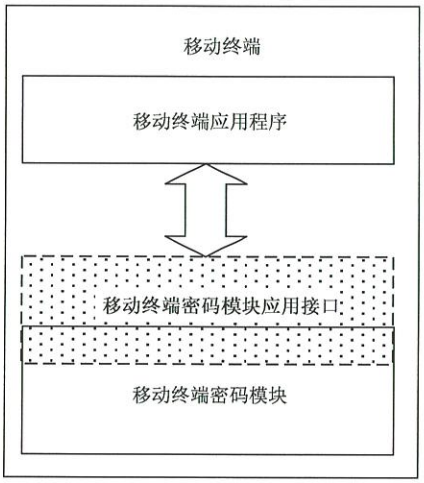

图 1 移动终端密码模块应用接口的位置

移动终端密码模块安装在移动终端中,支持密钥管理、密码计算和敏感信息存取等功能,移动终端中的应用程序通过调用移动终端密码模块应用接口执行相应的操作。

5.2 模块的应用结构

模块中存在模块鉴别密钥和多个应用,应用之间相互独立。

应用由管理员 PIN、用户 PIN、文件和容器等组成,一个应用中可以存在多个文件和多个容器。

一个应用中的文件、容器属于同一个用户。一个用户可使用一个应用或者多个应用进行文件管理与密钥管理等操作。每个应用维护各自的与管理员 PIN 和用户 PIN 相关的权限状态。

应用的逻辑结构见图 2。

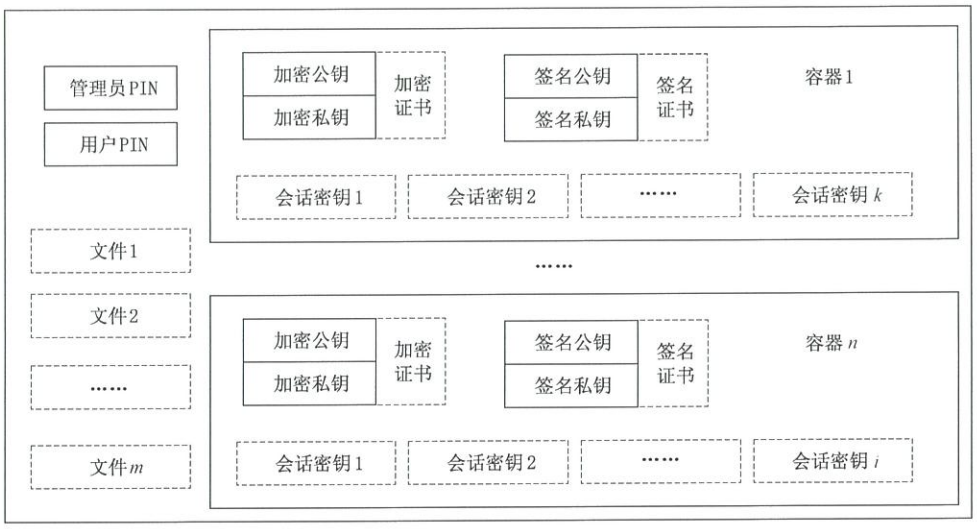

图 2　应用逻辑结构图

容器中存放加密密钥对、签名密钥对和会话密钥。其中，加密密钥对用于保护会话密钥，签名密钥对用于数字签名和验证，会话密钥用于数据加解密和 MAC 运算。容器中也可以存放与加密密钥对对应的加密数字证书和与签名密钥对对应的签名数字证书。其中签名密钥对由密码模块内部产生或协同产生，加密密钥对由外部产生并安全导入，会话密钥可由内部产生或者由外部产生并安全导入。

6　数据类型的定义

6.1　算法标识和数据类型定义说明

算法标识定义应遵循 GB/T 33560。

基本数据类型和复合数据类型均按照 Java 技术进行定义。

6.2　基本数据类型定义

字节数组均以高位字节在前(Big-Endian)的方式存储和交换。基本数据类型定义见表 1。

表 1　基本数据类型

类型名称	定义
short	有符号 16 位整数
int	有符号 32 位整数
long	有符号 64 位整数
byte	字节类型，有符号 8 位整数
char	字符类型
boolean	布尔类型，取值为 true 或 false
true	布尔值，判断逻辑条件为真
false	布尔值，判断逻辑条件为假
String	字符串类型
List	列表类型，java.util.List 类定义

6.3 复合数据类型定义

6.3.1 版本

6.3.1.1 类型定义

```
class Version{
        byte major;
        byte minor;
    }
```

6.3.1.2 数据项描述

数据项描述见表 2。

表 2 版本定义

数据项	类型	定义	备注
major	byte	主版本号	主版本号和次版本号以“.”分隔，例如，Version 2.3 表示主版本号为 0x02，次版本号为 0x03
minor	byte	次版本号	

6.3.2 模块信息

6.3.2.1 类型定义

```
    class ModInfos {
        Version version;
        String issuer;
        String label;
        String manufacturer;
        String serialNumber;
        Version hwVersion;
        Version firmwareVersion;
        long algSymCap;
        long algAsymCap;
        long algHashCap;
        long modAuthAlgId;
        long totalSpace;
        long freeSpace;
        long maxSM2BufferSize;
        long maxBufferSize;
}
```

6.3.2.2 数据项描述

数据项描述见表 3。

表 3　模块信息

数据项	类型	定义
version	Version	版本号
issuer	String	发行厂商信息
label	String	模块标签
manufacturer	String	模块厂商信息
serialNumber	String	序列号
hwVersion	Version	模块硬件版本
firmwareVersion	Version	模块本身固件版本
algSymCap	long	分组密码算法标识
algAsymCap	long	非对称密码算法标识
algHashCap	long	密码杂凑算法标识
modAuthAlgId	long	模块鉴别使用的分组密码算法标识
totalSpace	long	模块总空间大小
freeSpace	long	用户可用空间大小
maxSM2BufferSize	long	能够处理的 SM2 加密数据大小
maxBufferSize	long	能够处理的分组运算和杂凑运算的数据大小

6.3.3　文件属性

6.3.3.1　类型定义

```
class FileAttribute {
    String fileName;
    long fileSize;
    long readRights;
    long writeRights;
}
```

6.3.3.2　数据项描述

数据项描述见表 4。

表 4　文件属性

数据项	类型	定义	备注
fileName	String	文件名	—
fileSize	long	文件大小	创建文件时定义的文件大小
readRights	long	读取权限	读取文件所需要的权限
writeRights	long	写入权限	写文件所需要的权限

6.3.4 PIN 信息

6.3.4.1 类型定义

```
class PINInfo {
    long pinType;
    String pinValue;
    long retryCount;
    long maxRetryCount;
    boolean defaultPIN;
}
```

6.3.4.2 数据项描述

数据项描述见表 5。

表 5 PIN 信息

数据项	类型	定义	备注
pinType	long	PIN 码类型	0 为管理员 PIN； 1 为用户 PIN
pinValue	String	PIN 码的值	—
retryCount	long	PIN 码剩余重试次数	当值为 0 时，PIN 码被锁定
maxRetryCount	long	PIN 码最大重试次数	—
defaultPIN	boolean	PIN 码是否为出厂默认 PIN	true 表示是出厂默认 PIN； false 表示不是出厂默认 PIN

6.3.5 模块状态

模块状态的定义见表 6。

表 6 模块状态

模块状态	值	说明
MOD_ABSENT_STATE	0x00000000	模块不存在
MOD_PRESENT_STATE	0x00000001	模块存在
MOD_UNKNOW_STATE	0x00000002	模块状态未知

6.3.6 权限类型

权限类型的定义见表 7。

表 7　权限类型

权限类型	值	说明
SECURE_NEVER_ACCOUNT	0x00000000	不准许
SECURE_ADM_ACCOUNT	0x00000001	管理员权限
SECURE_USER_ACCOUNT	0x00000010	用户权限
SECURE_ANYONE_ACCOUNT	0x000000FF	任何人

6.3.7　分组密码参数

6.3.7.1　类型定义

```
class BlockCipherParam {
    byte[] iv;
    long paddingType;
    long feedBitLen;
}
```

6.3.7.2　数据项描述

数据项描述见表 8。

表 8　版本定义

数据项	类型	定义	备注
iv	byte[]	初始向量	—
paddingType	long	填充方式	0 表示不填充，1 表示填充
feedBitLen	long	反馈值的位长度	只针对 CFB、OFB 模式

6.3.8　SM2 算法相关数据格式

SM2 私钥数据、SM2 公钥数据、SM2 加密数据、SM2 签名数据以及 SM2 密钥对保护数据均以字节数组的方式进行传输，其数据格式均遵循 GB/T 35276。

7　移动终端密码模块应用接口

7.1　概述

本章以 Java 技术方案为例描述了移动终端密码模块中 SM2/3/4 系列算法的应用接口规范，使用 SM2/3/4 系列算法的应用可以调用这些应用接口以实现相应的密码功能。

7.2　密码算法实现要求

在移动终端密码模块中，SM2 椭圆曲线公钥密码算法实现应遵循 GB/T 32918(所有部分)，SM3 密码杂凑算法实现应遵循 GB/T 32905，SM4 分组密码算法实现应遵循 GB/T 32907，消息鉴别码算法实现应遵循 GB/T 15852.1。

7.3 密码应用包定义

密码应用包定义见表 9，密码应用包包含密码模块抽象类与密码应用接口。移动密码模块产品实现过程中可以根据厂商需求定义移动密码模块产品包。

表 9 包信息

项	定义
包名	com.mob.crypto
主版本号	1
次版本号	0

7.4 密码应用接口定义

7.4.1 类定义

定义密码模块抽象类(GMCryptoMod)，具体类定义如下。

class java.lang.object

—class com.mob.crypto.GMCryptoMod

7.4.2 接口定义

提供模块连接接口(IModuleConnection)、模块接口(IModule)、应用接口(IApplication)、容器接口(IContainer)、会话密钥接口(ISessionKey)、密码杂凑接口(IDigest)、消息鉴别码接口(IMac)、带密钥的杂凑运算接口(IHMAC)，具体接口定义如下。

interface com.mob.crypto.IModuleConnection

interface com.mob.crypto.IModule

interface com.mob.crypto.IApplication

interface com.mob.crypto.IContainer

interface com.mob.crypto.ISessionKey

interface com.mob.crypto.IDigest

interface com.mob.crypto.IMac

interface com.mob.crypto.IHMAC

接口方法异常码应按照附录 A 进行定义和说明。接口方法描述仅列出常见异常，在密码模块实现时可根据需要进一步扩展更多异常。

7.5 密码模块类

密码模块抽象类(GMCryptoMod)是移动终端密码模块的基类，所有密码模块的实现应扩展这个抽象类。

GMCryptoMod 类成员变量见表 10。

表 10　GMCryptoMod 类成员变量

类型	定义	说明
byte	modType	为 0 时表示该模块为硬件密码模块； 为 1 时表示该模块为软件密码模块
byte	modLevel	表示密码模块安全等级
byte	modAuth	为 0 时表示该模块不需要进行模块鉴别； 为 1 时表示该模块需要进行模块鉴别
byte	modPINMod	为 0 时表示该模块不准许修改 PIN； 为 1 时表示该模块允许修改 PIN
byte	modFileManage	为 0 时表示该模块不需要进行文件管理； 为 1 时表示该模块需要进行文件管理

7.6　模块连接接口

7.6.1　概述

模块连接接口主要完成对移动终端中的密码模块进行管理(包括连接模块、枚举模块、获取模块状态)。

IModuleConnection 接口系列方法见表 11。

表 11　IModuleConnection 接口系列方法

类型	定义	说明
IModule	SSF_ConnectMod	连接模块
List〈String〉	SSF_EnumMod	枚举模块
long	SSF_GetModState	获取模块状态

7.6.2　连接模块

方法声明　IModule SSF_ConnectMod(
　　String modName
　　) throws ResultCodeException

功能描述　连接一个模块。

参数　modName　模块名

返回值　IModule 接口实现类对象

抛出异常　ResultCodeException.SSF_UNKNOWNERR　异常错误
　　ResultCodeException.SSF_MODNOTEXIST　模块不存在

7.6.3　枚举模块

方法声明　List〈String〉 SSF_EnumMod(
　　) throws ResultCodeException

功能描述　枚举模块。
参数　　无
返回值　　模块名列表
抛出异常　ResultCodeException.SSF_UNKNOWNERR　异常错误

7.6.4　获取模块状态

方法声明　long SSF_GetModState(
　　String modName
　　) throws ResultCodeException
功能描述　获取模块是否存在的状态。
参数　　modName　　模块名
返回值　　模块状态(模块状态定义见 6.3.5)
抛出异常　ResultCodeException.SSF_UNKNOWNERR　异常错误
　　ResultCodeException.SSF_MODNOTEXIST　模块不存在

7.7　模块接口

7.7.1　概述

模块接口(IModule)主要完成对模块的管理(包括断开模块、设置模块标签等操作)和对应用的管理(包括创建应用、枚举应用、删除应用等操作)等。

IModule 接口系列方法见表 12。

表 12　IModule 接口系列方法

类型	定义	说明
void	SSF_DisconnectMod	断开模块
void	SSF_SetLabel	设置模块标签
ModInfos	SSF_GetModInfo	获取模块信息
void	SSF_LockMod	锁定模块
void	SSF_UnlockMod	解锁模块
String	SSF_Transmit	模块命令传输
void	SSF_ModAuth	模块鉴别
void	SSF_ChangeModAuthKey	修改模块鉴别密钥
IApplication	SSF_CreateApplication	创建应用
List〈String〉	SSF_EnumApplication	枚举应用
void	SSF_DeleteApplication	删除应用
IApplication	SSF_OpenApplication	打开应用
void	SSF_BackupApplication	备份应用
IApplication	SSF_RecoverApplication	恢复应用
byte[]	SSF_GenRandom	生成随机数

7.7.2 断开模块

方法声明	void SSF_DisConnectMod( ) throws ResultCodeException	
功能描述	断开一个已经连接的模块	
参数	无	
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_MODLOCKED	模块已锁定
备注	如果该模块已被锁定，应首先解锁该模块，断开连接操作并不影响模块的权限状态。	

7.7.3 设置模块标签

方法声明	void SSF_SetLabel(String label) throws ResultCodeException	
功能描述	设置模块标签。	
参数	label	模块标签字符串，该字符串长度应小于32字节
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.4 获取模块信息

方法声明	ModInfos SSF_GetModInfo( ) throws ResultCodeException	
功能描述	获取模块信息。	
参数	无	
返回值	ModInfos 模块信息类对象	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.5 锁定模块

方法声明	void SSF_LockMod(long timeOut) throws ResultCodeException	
功能描述	获得模块的独占使用权。	
参数	timeOut	超时时间，单位为毫秒；如果为0xFFFFFFFFF表示无限等待
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.6 解锁模块

方法声明	void SSF_UnlockMod( ) throws ResultCodeException
功能描述	释放对模块的独占使用权。

参数	无	
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.7 模块命令传输

方法声明	String SSF_Transmit(byte[] command) throws ResultCodeException	
功能描述	将命令直接发送给模块，并返回结果。	
参数	command	模块命令
返回值	结果数据	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	本方法仅用于模块检测。	

7.7.8 模块鉴别

方法声明	void SSF_ModAuth(byte[] authData) throws ResultCodeException	
功能描述	模块鉴别是模块对应用程序的鉴别，鉴别过程见 8.2.3。	
参数	authData	鉴别数据
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWERR	异常错误

7.7.9 修改模块鉴别密钥

方法声明	void SSF_ChangeModAuthKey(byte[] keyCipher byte[] keyMac) throws ResultCodeException	
功能描述	使用密文和 MAC 方式更改模块鉴别密钥。	
参数	keyCipher	新模块鉴别密钥的密文
	keyMac	报文鉴别码
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWERR	异常错误
备注	权限要求：模块鉴别成功后才能使用。新模块鉴别密钥的密文通过使用原模块鉴别密钥对新模块鉴别密钥进行 ECB 加密得到。报文鉴别码由原模块鉴别密钥对含有 keyCipher 的数据进行 CBC 加密得到。报文鉴别码的计算过程应符合 GM/T 0017—2023 中附录 B 的规定。	

7.7.10 创建应用

方法声明	IApplication SSF_CreateApplication(String appName, String adminPIN, long adminPINRetryCount,

	String userPIN, long userPINRetryCount, long createFileRights) throws ResultCodeException	
功能描述	创建一个应用。	
参数	appName	应用名称
	adminPIN	管理员 PIN 值
	adminPINRetryCount	管理员 PIN 值最大重试次数
	userPIN	用户 PIN 值
	userPINRetryCount	用户 PIN 最大重试次数
	createFileRights	在该应用下创建文件和容器的权限(见 6.3.6,可为各种权限的或值)
返回值	IApplication 接口实现类对象	
抛出异常	ResultCodeException.SSF_APPLICATIONNAMEINVALID	应用名称无效
	ResultCodeException.SSF_APPLICATIONEXISTS	应用已经存在
备注	权限要求:需要模块权限。	

7.7.11 枚举应用

方法声明	List〈String〉 SSF_EnumApplication( ) throws ResultCodeException	
功能描述	枚举模块中存在的所有应用。	
参数	无	
返回值	应用名称列表	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_OBJERR	对象错误

7.7.12 删除应用

方法声明	void SSF_DeleteApplication(String appName) throws ResultCodeException	
功能描述	删除指定的应用。	
参数	appName	应用名称
返回值	无	
抛出异常	ResultCodeException.SSF_APPLICATIONNOTEXISTS	应用不存在
	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_OBJERR	对象错误
	ResultCodeException.SSF_FILEERR	文件操作错误
	ResultCodeException.SSF_APPLICATIONALREADYOPENED	应用已经打开
备注	权限要求:需要模块权限。	

7.7.13 打开应用

方法声明	IApplication SSF_OpenApplication(

	String appName	
	) throws ResultCodeException	
功能描述	打开指定应用。	
参数	appName	应用名称
返回值	IApplication 接口实现类对象	
抛出异常	ResultCodeException.SSF_APPLICATIONNOTEXISTS	应用不存在
	ResultCodeException.SSF_APPLICATIONALREADYOPENED	应用已经打开
	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.14 备份应用

方法声明	void SSF_BackupApplication(	
	OutputStream backupFile,	
	IApplication application	
	) throws ResultCodeException	
功能描述	备份应用。	
参数	backupFile	要备份的文件流
	application	要备份的应用对象
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_APPLICATIONNOTEXISTS	应用不存在

7.7.15 恢复应用

方法声明	IApplication SSF_RecoverApplication(	
	InputStream backupFile	
	)throws ResultCodeException	
功能描述	恢复应用。	
参数	backupFile	已备份的文件
返回值	IApplication 接口实现类对象	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.7.16 生成随机数

方法声明	byte[] SSF_GenRandom(	
	long randomLen	
	) throws ResultCodeException	
功能描述	获取随机数。	
参数	randomLen	随机数字节长度
返回值	生成的随机数	
抛出异常	ResultCodeException.SSF_GENRANDERR	生成随机数错误

7.8 应用接口

7.8.1 概述

应用接口(IApplication)主要完成 PIN 码管理、容器管理和文件管理等操作。

IApplication 接口系列方法见表 13。

表 13　IApplication 接口系列方法

类型	定义	说明
void	SSF_CloseApplication	关闭应用
long	SSF_ChangePIN	修改 PIN
PINInfo	SSF_GetPINInfo	获取 PIN 相关信息
long	SSF_VerifyPIN	校验 PIN
long	SSF_UnlockPIN	解锁 PIN
void	SSF_ClearSecureState	清除应用安全状态
IContainer	SSF_CreateContainer	创建容器
void	SSF_DeleteContainer	删除容器
List〈String〉	SSF_EnumContainer	枚举容器
IContainer	SSF_OpenContainer	打开容器
void	SSF_CreateFile	创建文件
void	SSF_DeleteFile	删除文件
List〈String〉	SSF_EnumFile	枚举文件
FileAttribute	SSF_GetFileInfo	获取文件信息
byte[]	SSF_ReadFile	读文件
void	SSF_WriteFile	写文件

7.8.2　关闭应用

方法声明　void SSF_CloseApplication(
　　) throws ResultCodeException
功能描述　关闭应用。
参数　　无
返回值　　无
抛出异常　ResultCodeException.SSF_FAIL　　失败
　　ResultCodeException.SSF_UNKNOWNERR　　异常错误
备注　　此方法不影响应用的安全状态。

7.8.3　修改 PIN

方法声明　long SSF_ChangePIN(
　　long pinType,
　　String oldPIN,
　　String newPIN
　　) throws ResultCodeException
功能描述　调用该方法可以修改管理员 PIN 和用户 PIN 的值。如果原 PIN 码错误导致验证失

	败，该方法会返回相应 PIN 码的剩余重试次数，当剩余重试次数为 0 时，表示 PIN 已经被锁死。	
参数	pinType	PIN 类型
	oldPIN	原 PIN 值
	newPIN	新 PIN 值
返回值	出错后的相应 PIN 码的剩余重试次数	
抛出异常	ResultCodeException.SSF_PINLOCKED	PIN 被锁死
	ResultCodeException.SSF_PINLENRANCE	PIN 长度错误
	ResultCodeException.SSF_NOTSUPPORTYETERR	不支持的服务

7.8.4 获取 PIN 相关信息

方法声明	PINInfo SSF_GetPINInfo(long pinType) throws ResultCodeException	
功能描述	获取 PIN 码信息，包括最大重试次数，当前剩余重试次数，以及当前 PIN 码是否为出厂默认 PIN 码。	
参数	pinType	PIN 类型
返回值	PINInfo 类对象	
抛出异常	ResultCodeException.SSF_NOTSUPPORTYETERR	不支持的服务

7.8.5 校验 PIN

方法声明	long SSF_VerifyPIN(long pinType, String pin) throws ResultCodeException	
功能描述	校验 PIN 码。校验成功后，会获取相应的权限，如果 PIN 码错误，会返回 PIN 码的重试次数，当重试次数为 0 时，表示 PIN 码已经被锁死。	
参数	pinType	PIN 类型
	pin	PIN 值
返回值	出错后返回剩余重试次数	
抛出异常	ResultCodeException.SSF_PININCORRECT	PIN 不正确
	ResultCodeException.SSF_PINLOCKED	PIN 被锁死
	ResultCodeException.SSF_NOTSUPPORTYETERR	不支持的服务

7.8.6 解锁 PIN

方法声明	long SSF_UnlockPIN(String adminPIN, String newUserPIN) throw ResultCodeException	
功能描述	当用户的 PIN 码锁死后，通过调用该方法来解锁用户 PIN 码。解锁后，用户 PIN 码被设置成新值，用户 PIN 码的重试次数也恢复到原值。	
参数	adminPIN	管理员 PIN 值
	newUserPIN	新的用户 PIN 值

返回值	管理员 PIN 码错误时，返回剩余重试次数	
抛出异常	ResultCodeException.SSF_PININCORRECT	PIN 不正确
	ResultCodeException.SSF_PINLOCKED	PIN 被锁死
	ResultCodeException.SSF_PINLENRANGE	PIN 长度错误
	ResultCodeException.SSF_NOTSUPPORTYETERR	不支持的服务
备注	验证完管理员 PIN 才能够解锁用户 PIN 码，如果输入的管理员 PIN 不正确或者已经锁死，会调用失败，并返回管理员 PIN 的重试次数。	

7.8.7 清除应用安全状态

方法声明	void SSF_ClearSecureState( ) throws ResultCodeException	
功能描述	清除应用当前的安全状态。	
参数	无	
返回值	无	
抛出异常	ResultCodeException.SSF_NOTSUPPORTYETERR	不支持的服务

7.8.8 创建容器

方法声明	IContainer SSF_CreateContainer(String containerName) throws ResultCodeException	
功能描述	创建一个容器。	
参数	containerName	容器名称
返回值	IContainer 接口实现类对象	
抛出异常	ResultCodeException.SSF_CONTAINERALREADYEXIST	容器已经存在
备注	权限要求：需要用户权限。	

7.8.9 删除容器

方法声明	void SSF_DeleteContainer(String containerName) throws ResultCodeException	
功能描述	删除容器。	
参数	containerName	容器名称
返回值	无	
抛出异常	ResultCodeException.SSF_CONTAINERNOTEXIST	容器不存在
备注	权限要求：需要用户权限。	

7.8.10 枚举容器

方法声明	List〈String〉 SSF_EnumContainer( ) throws ResultCodeException	
功能描述	枚举所有已经创建的容器。	
参数	无	
返回值	容器名称列表	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.8.11 打开容器

方法声明	IContainer SSF_OpenContainer(String containerName) throws ResultCodeException	
功能描述	打开一个容器。	
参数	containerName	容器名称
返回值	IContainer 接口实现类对象	
抛出异常	ResultCodeException.SSF_CONTAINERALREADYOPENED	容器已经打开
	ResultCodeException.SSF_CONTAINERNOTEXIST	容器不存在

7.8.12 创建文件

方法声明	void SSF_CreateFile(String fileName, long fileSize, long readRights, long writeRights) throws ResultCodeException	
功能描述	创建文件。	
参数	fileName	文件名称
	fileSize	文件大小,参数大于 0
	readRights	文件读权限(见 6.3.6,可为各种权限的或值)
	writeRights	文件写权限(见 6.3.6,可为各种权限的或值)
返回值	无	
抛出异常	ResultCodeException.SSF_FILEALREADYEXISTS	文件已经存在
	ResultCodeException.SSF_FILEERR	文件操作错误
备注	创建文件需要应用指定的创建文件权限。	

7.8.13 删除文件

方法声明	void SSF_DeleteFile(String fileName) throws ResultCodeException	
功能描述	删除文件。	
参数	fileName	文件名称
返回值	无	
抛出异常	ResultCodeException.SSF_FILENOTEXISTS	文件不存在
	ResultCodeException.SSF_FILEERR	文件操作错误
备注	权限要求:删除一个文件应具有对该文件的创建权限。	

7.8.14 枚举文件

方法声明	List<String> SSF_EnumFiles(

	) throws ResultCodeException	
功能描述	枚举所有已经创建的文件。	
参数	无	
返回值	文件名称列表	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_FILEERR	文件操作错误

7.8.15 获取文件信息

方法声明	FileAttribute SSF_GetFileInfo(	
	String fileName	
	) throws ResultCodeException	
功能描述	获取文件信息。	
参数	fileName	文件名称
返回值	文件属性,FileAttribute 类对象	
抛出异常	ResultCodeException.SSF_FILENOTEXISTS	文件不存在
	ResultCodeException.SSF_FILEERR	文件操作错误

7.8.16 读文件

方法声明	byte[] SSF_ReadFile(	
	String fileName,	
	long offset,	
	long size	
	) throws ResultCodeException	
功能描述	读取文件。	
参数	fileName	文件名称
	offset	文件读取偏移位置
	size	要读取数据的长度
返回值	文件数据	
抛出异常	ResultCodeException.SSF_READFILEERR	读文件错误
	ResultCodeException.SSF_FILENOTEXISTS	文件不存在
备注	权限要求:须具备对该文件的读权限。	
	返回的文件数据的长度小于或等于要读取数据的长度。	

7.8.17 写文件

方法声明	void SSF_WriteFile(	
	String fileName,	
	long offset,	
	byte[] data,	
	long size	
	) throws ResultCodeException	
功能描述	写文件。	
参数	fileName	文件名称

	offset	偏移量，不可超过文件大小且大于或等于0
	data	待写入的数据
返回值	无	
抛出异常	ResultCodeException.SSF_WRITEFILEERR	写文件错误
	ResultCodeException.SSF_READFILEERR	读文件错误
备注	权限要求：须具备对该文件的写权限。	

7.9 容器接口

7.9.1 概述

容器接口(IContainer)主要完成数字证书的导入导出以及密码相关操作。移动终端与云服务协同数字签名是移动终端密码模块的重要实现方式，在容器接口中引入基于SM2的协同签名和解密系列方法(包括生成协同密钥对、SM2协同签名、SM2协同解密等功能)。各功能均可调用一次或多次请求生成与响应处理方法，通过协同密码机制标识参数以确定所使用的协同密码算法，并确定对相关参数的解析方法，从而实现对各类协同密码机制的兼容支持。

IContainer接口系列方法见表14。

表14 IContainer接口系列方法

类型	定义	说明
void	SSF_CloseContainer	关闭容器
long	SSF_GetContainerType	获得容器类型
void	SSF_ImportCertificate	导入数字证书
byte[]	SSF_ExportCertificate	导出数字证书
void	SSF_GenSM2KeyPair	生成SM2签名密钥对
void	SSF_ImportSM2KeyPair	导入SM2加密密钥对
byte[]	SSF_SM2SignData	SM2签名
boolean	SSF_SM2Verify	SM2验签
byte[]	SSF_SM2ExportSessionKey	SM2生成并导出会话密钥
byte[]	SSF_ExtSM2Encrypt	SM2外部公钥加密
byte[]	SSF_ExtSM2Decrypt	SM2外部私钥解密(仅测试)
byte[]	SSF_ExtSM2Sign	SM2外部私钥签名(仅测试)
boolean	SSF_ExtSM2Verify	SM2外部公钥验签
byte[]	SSF_GenerateAgreementDataWithSM2	SM2生成密钥协商参数并输出
ISessionKey	SSF_GenerateKeyWithSM2	SM2计算会话密钥
ISessionKey	SSF_GenerateAgreementDataAndKeyWithSM2	SM2产生协商数据并计算会话密钥
byte[]	SSF_genThresholdKeyPairRequest	SM2生成协同密钥对请求生成
void	SSF_genThresholdKeyPairResponseProcess	SM2生成协同密钥对响应处理

表 14　IContainer 接口系列方法（续）

类型	定义	说明
byte[]	SSF_thresholdSignDataResquest	SM2 协同签名请求生成
byte[]	SSF_thresholdSignDataResponseProcess	SM2 协同签名响应处理
byte[]	SSF_thresholdDecryptRequest	SM2 协同解密请求生成
byte[]	SSF_thresholdDecryptResponseProcess	SM2 协同解密响应处理
byte[]	SSF_ExportPublicKey	导出公钥
byte[]	SSF_ExtKeyEncrypt	外来对称密钥加密(仅测试)
byte[]	SSF_ExtKeyDecrypt	外来对称密钥解密(仅测试)
ISessionKey	SSF_ImportSessionKey	导入会话密钥

7.9.2　关闭容器

方法声明　void SSF_CloseContainer(
　　) throws ResultCodeException
功能描述　关闭容器。
参数　　无
返回值　　无
抛出异常　ResultCodeException.SSF_UNKNOWERR　　异常错误

7.9.3　获取容器类型

方法声明　long SSF_GetContainerType(
　　) throws ResultCodeException
功能描述　获取容器类型。
参数　　无
返回值　　容器类型(0 表示未定、尚未分配的类型或者为空容器,1 表示 SM2 容器)
抛出异常　ResultCodeException.SSF_UNKNOWERR　　异常错误

7.9.4　导入数字证书

方法声明　void SSF_ImportCertificate(
　　boolean signFlag,
　　byte[] cert
　　) throws ResultCodeException
功能描述　导入证书数据。
参数　　signFlag　　true 表示签名证书,false 表示加密证书
　　cert　　证书数据,不能为空
返回值　　无
抛出异常　ResultCodeException.SSF_UNKNOWERR　　异常错误

7.9.5 导出数字证书

方法声明 byte[] SSF_ExportCertificate(
boolean signFlag
) throws ResultCodeException
功能描述 导出证书数据。
参数 signFlag true 表示签名证书，false 表示加密证书
返回值 证书数据
抛出异常 ResultCodeException.SSF_CERTNOTFOUNDERR 证书未发现

7.9.6 生成 SM2 签名密钥对

方法声明 void SSF_GenSM2KeyPair(
long algId
) throws ResultCodeException
功能描述 生成 SM2 签名密钥对。
参数 algId 算法标识(只支持 SGD_SM2_1 算法)
返回值 无
抛出异常 ResultCodeException.SSF_UNKNOWNERR 异常错误
备注 权限要求：需要用户权限。

7.9.7 导入 SM2 加密密钥对

方法声明 void SSF_ImportSM2KeyPair(
byte[] sm2EnvelopedKey
) throws ResultCodeException
功能描述 导入 SM2 公私钥对。
参数 sm2EnvelopedKey 受保护的加密密钥对，不能为空
返回值 无
抛出异常 ResultCodeException.SSF_UNKNOWNERR 异常错误
备注 权限要求：需要用户权限。
sm2EnvelopedKey 数据格式为 SM2 密钥对的保护数据格式(见 6.3.8)。

7.9.8 SM2 签名

方法声明 byte[] SSF_SM2SignData(
byte[] hashData
) throws ResultCodeException
功能描述 SM2 签名(对原始数据的杂凑值进行签名)。
参数 hashData 原始数据的杂凑值，长度应为 32 字节
返回值 SM2 签名值
抛出异常 ResultCodeException.SSF_COMPUTEERR 计算错误
ResultCodeException.SSF_UNKNOWNERR 异常错误
备注 权限要求：需要用户权限。
输入数据为待签数据的杂凑值。当使用 SM2 算法时，该输入数据为待签数据经过

SM2 签名预处理的结果，预处理过程遵循 GB/T 35276。

7.9.9 SM2 验签

方法声明	boolean SSF_SM2Verify(byte[] sm2PublicKey, byte[] hashData, byte[] sm2Signature) throws ResultCodeException	
功能描述	SM2 验签(对原始数据的杂凑值验签)。	
参数	sm2PublicKey	SM2 公钥数据
	hashData	原始数据的杂凑值，长度为 32 字节
	sm2Signature	待验证的签名值
返回值	true 表示验证签名成功，false 表示验证签名失败	
抛出异常	ResultCodeException.SSF_KEYINFOTYPEERR	密钥类型错误
	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	输入数据为待签数据的杂凑值。当使用 SM2 算法时，该输入数据为待签数据经过 SM2 签名预处理的结果，预处理过程遵循 GM/T 35276。 sm2PublicKey 数据格式为 SM2 公钥数据格式(见 6.3.8)。	

7.9.10 SM2 生成并导出会话密钥

方法声明	byte[] SSF_SM2ExportSessionKey(long algId, byte[] sm2PublicKey) throws ResultCodeException	
功能描述	SM2 生成会话密钥并用外部公钥加密会话密钥。	
参数	algId	会话密钥算法标识
	sm2PublicKey	外部输入的公钥结构
返回值	加密后的会话密钥	
抛出异常	ResultCodeException.SSF_ENCRYPTERR	加密错误
	ResultCodeException.SSF_DATAKEYERR	加密密钥错误
备注	sm2PublicKey 数据格式为 SM2 公钥数据格式(见 6.3.8)。	

7.9.11 SM2 外部公钥加密

方法声明	byte[] SSF_ExtSM2Encrypt(byte[] sm2PublicKey, byte[] plainText) throws ResultCodeException	
功能描述	使用外部传入的 SM2 公钥对输入的数据进行加密并输出结果。	
参数	sm2PublicKey	加密数据使用的公钥
	plainText	待加密的明文数据
返回值	密文数据	
抛出异常	ResultCodeException.SSF_ENCRYPTERR	加密错误
	ResultCodeException.SSF_DATAKEYERR	加密密钥错误

备注　sm2PublicKey 数据格式为 SM2 公钥数据格式(见 6.3.8)。
返回的密文数据格式为 SM2 加密数据格式(见 6.3.8)。

7.9.12 SM2 外部私钥解密

方法声明　byte[] SSF_ExtSM2Decrypt(
byte[] sm2PrivateKey,
byte[] sm2Cipher
) throws ResultCodeException
功能描述　使用外部传入的 SM2 私钥对输入数据做解密运算并输出结果。
参数　sm2PrivateKey　SM2 私钥数据结构
sm2Cipher　待解密的密文数据
返回值　明文数据
抛出异常　ResultCodeException.SSF_DECRYPTERR　解密错误
备注　本方法仅用于测试和调试,不建议用于实际的密码服务。
sm2PrivateKey 数据格式为 SM2 私钥数据格式(见 6.3.8)。
sm2Cipher 数据格式为 SM2 加密数据格式(见 6.3.8)。

7.9.13 SM2 外部私钥签名

方法声明　byte[] SSF_ExtSM2Sign(
byte[] sm2PrivateKey,
byte[] data
) throws ResultCodeException
功能描述　使用外部传入的 SM2 私钥对输入数据做签名运算并输出结果。
参数　sm2PrivateKey　SM2 私钥数据结构
data　待签名数据
返回值　SM2 签名值
抛出异常　ResultCodeException.SSF_FAIL　失败
ResultCodeException.SSF_UNKNOWNER　异常错误
备注　本方法仅用于测试和调试,不建议用于实际的密码服务。
输入数据为待签数据的杂凑值。当使用 SM2 算法时,该输入数据为待签数据经过 SM2 签名预处理的结果,预处理过程遵循 GB/T 35276。
sm2PrivateKey 数据格式为 SM2 私钥数据格式(见 6.3.8)。
返回的 SM2 签名值数据格式为 SM2 签名数据格式(见 6.3.8)。

7.9.14 SM2 外部公钥验签

方法声明　boolean SSF_ExtSM2Verify(
byte[] sm2PublicKey,
byte[] data,
byte[] signature
) throws ResultCodeException
功能描述　使用外部传入的 SM2 公钥做签名验证。
参数　sm2PublicKey　SM2 公钥数据结构
data　待验证数据

	signature	签名值
返回值	true 表示验证签名成功，false 表示验证签名失败	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_KEYINFOTYPEERR	密钥错误
	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	输入数据为待签数据的杂凑值。当使用 SM2 算法时，该输入数据为待签数据经过 SM2 签名预处理的结果，预处理过程遵循 GB/T 35276。 sm2PublicKey 数据格式为 SM2 公钥数据格式(见 6.3.8)。 签名值数据格式为 SM2 签名数据格式(见 6.3.8)。	

7.9.15 SM2 生成密钥协商参数并输出

方法声明	byte[] SSF_GenerateAgreementDataWithSM2(long algId, byte[] ID) throws ResultCodeException	
功能描述	使用 SM2 密钥协商算法，为计算会话密钥而产生协商参数，返回临时 SM2 密钥对的公钥。	
参数	algId	会话密钥算法标识
	ID	发起方 ID，长度应不大于 32 字节
返回值	临时 SM2 密钥对的公钥	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	为协商会话密钥，协商的发起方应首先调用本方法。 返回值数据格式为 SM2 公钥数据格式(见 6.3.8)。	

7.9.16 SM2 计算会话密钥

方法声明	ISessionKey SSF_GenerateKeyWithSM2(byte[] tempSM2PublicKey, byte[] sm2PublicKey, byte[] ID) throws ResultCodeException	
功能描述	使用 SM2 密钥协商算法使用自身协商的参数和响应方的协商参数计算会话密钥，同时返回会话密钥(发起者调用)。	
参数	tempSM2PublicKey	响应方的临时 SM2 公钥
	sm2PublicKey	响应方的 SM2 公钥
	ID	响应方 ID，长度应不大于 32 字节
返回值	ISessionKey 接口实现类对象	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_OBJERR	对象错误
	ResultCodeException.SSF_INVALIDPARAMERR	无效的参数
备注	协商的发起方获得响应方的协商参数后调用本方法，计算会话密钥。计算过程遵循 GB/T 35276。	

响应方临时 SM2 公钥和 SM2 公钥数据格式为 SM2 公钥数据格式(见 6.3.8)。

7.9.17 SM2 产生协商数据并计算会话密钥

方法声明	ISessionKey SSF_GenerateAgreementDataAndKeyWithSM2(long algId, byte[] sponsorSM2PublicKey, byte[] sponsorTempSM2PublicKey, byte[] sponsorId, byte[] ID) throws ResultCodeException	
功能描述	使用 SM2 密钥协商算法,产生协商数据并计算会话密钥。	
参数	algId	会话密钥算法标识
	sponsorSM2PublicKey	发起方的 SM2 公钥
	sponsorTempSM2PublicKey	发起方的临时 SM2 公钥
	sponsorId	发起方 ID,长度应不大于 32 字节
	ID	响应方 ID,长度应不大于 32 字节
返回值	ISessionKey 接口实现类对象	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	本方法由响应者调用。 发起方临时 SM2 公钥和 SM2 公钥数据格式为 SM2 公钥数据格式(见 6.3.8)。	

7.9.18 SM2 生成协同密钥对请求生成

方法声明	byte[] SSF_genThresholdKeyPairRequest(long algId, byte[] param, boolean signFlag) throws ResultCodeException	
功能描述	生成 SM2 协同密钥对生成的请求数据。	
参数	algId	协同密钥对生成机制标识
	param	协同密钥对生成请求所需附加参数
	signFlag	密钥类型标识(true 表示生成签名密钥对,false 表示生成加密密钥对)
返回值	SM2 协同密钥对生成请求数据	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	权限要求:需要用户权限。 在实际应用中,加密密钥对一般由密钥管理中心进行生成和管理,因此 SM2 协同生成加密密钥对功能仅用于测试和调试,不建议用于实际的密码服务。	

7.9.19 SM2 生成协同密钥对响应处理

方法声明	void SSF_genThresholdKeyPairResponseProcess(long algId,

byte[] responseMsg,
boolean signFlag
) throws ResultCodeException

功能描述	处理服务端返回的协同签名密钥对生成响应消息,并生成客户端公钥。	
参数	algId	协同密钥对生成机制标识
	responseMsg	协同服务端的响应消息
	signFlag	密钥类型标识(true 表示生成签名密钥对,false 表示生成加密密钥对)
返回值	无	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	权限要求:需要用户权限。 SM2 协同生成加密密钥对功能仅用于测试和调试,不建议用于实际的密码服务。	

7.9.20 SM2 协同签名请求生成

方法声明 byte[] SSF_thresholdSignDataResquest(
long algId,
byte[] hashData,
byte[] param
) throws ResultCodeException

功能描述	生成 SM2 协同签名的请求数据(对原始数据的杂凑值进行签名)。	
参数	algId	协同签名机制标识
	hashData	原始数据的杂凑值,长度应为 32 字节
	param	协同签名机制相关参数
返回值	SM2 协同签名请求数据	
抛出异常	ResultCodeException.SSF_COMPUTEERR	计算错误
备注	权限要求:需要用户权限。 输入数据为待签数据的杂凑值。当使用 SM2 算法时,该输入数据为待签数据经过 SM2 签名预处理的结果,预处理过程遵循 GB/T 35276。	

7.9.21 SM2 协同签名响应处理

方法声明 byte[] SSF_thresholdSignDataResponseProcess(
long algId,
byte[] responseMsg
) throws ResultCodeException

功能描述	处理服务端返回的 SM2 协同签名响应信息并生成签名。	
参数	algId	协同签名机制标识
	responseMsg	协同服务端响应消息
返回值	SM2 协同签名值	
抛出异常	ResultCodeException.SSF_COMPUTEERR	计算错误
备注	权限要求:需要用户权限。	

7.9.22 SM2 协同解密请求生成

方法声明 byte[] SSF_thresholdDecryptRequest(

long algId,
byte[] sm2Cipher,
byte[] param
) throws ResultCodeException

功能描述　生成 SM2 协同解密的请求数据。

参数		
	algId	协同解密机制标识
	sm2Cipher	待解密的密文数据
	param	协同解密机制所需参数
返回值	SM2 协同解密请求数据	
抛出异常	ResultCodeException.SSF_DECRYPTERR	解密错误
备注	权限要求：需要用户权限。	

7.9.23　SM2 协同解密响应处理

方法声明　byte[] SSF_thresholdDecryptResponseProcess(
long algId,
byte[] responseMsg
) throws ResultCodeException

功能描述　处理服务端返回的 SM2 协同解密响应消息，并生成解密结果。

参数		
	algId	协同解密机制标识
	responseMsg	协同解密服务端响应消息
返回值	SM2 协同解密运算结果	
抛出异常	ResultCodeException.SSF_DECRYPTERR	解密错误
备注	权限要求：需要用户权限。	

7.9.24　导出公钥

方法声明　byte[] SSF_ExportPublicKey(
boolean signFlag
) throws ResultCodeException

功能描述　导出公钥。

参数		
	signFlag	true 表示导出签名公钥，false 表示导出加密公钥
返回值	SM2 公钥数据	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
备注	返回值 SM2 公钥数据格式为 SM2 公钥数据格式(见 6.3.8)。	

7.9.25　外来对称密钥加密

方法声明　byte[] SSF_ExtKeyEncrypt(
byte[] data,
byte[] key
) throws ResultCodeException

功能描述　使用外来加密密钥对指定数据进行加密，被加密的数据只包含单一分组，输出加密后的密文。

参数	data	待加密数据
	key	外来密钥
返回值	加密后的密文	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_ENCRYPTERR	加密错误
备注	本方法仅用于测试和调试，不建议用于实际的密码服务。	

7.9.26 外来对称密钥解密

方法声明
```
byte[] SSF_ExtKeyDecrypt(
byte[] data,
byte[] key
) throws ResultCodeException
```

功能描述	使用外来解密密钥对指定数据进行解密，被解密的数据只包含单一分组，输出解密后的明文。	
参数	data	待解密数据
	key	外来密钥
返回值	解密后的明文	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_DECRYPTERR	输入数据错误
备注	本方法仅用于测试和调试，不建议用于实际的密码服务。	

7.9.27 导入会话密钥

方法声明
```
ISessionKey SSF_ImportSessionKey(
long algId,
byte[] wrapedData
) throws ResultCodeException
```

功能描述	导入会话密钥密文，使用容器中的加密私钥解密得到会话密钥。	
参数	algId	会话密钥算法标识
	wrapedData	会话密钥密文(由加密密钥对加密)
返回值	ISessionKey 接口实现类对象	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_OBJERR	对象错误
	ResultCodeException.SSF_KEYNOTFOUNDERR	密钥未发现
备注	权限要求：需要用户权限。 wrapedData 数据格式为 SM2 加密数据格式(见 6.3.8)。	

7.10 会话密钥接口

7.10.1 概述

会话密钥接口(ISessionKey)主要完成对称码算法的初始化、加密、解密。

ISessionKey 接口系列方法见表 15。

表 15　ISessionKey 接口系列方法

类型	定义	说明
void	SSF_EncryptInit	加密初始化
byte[]	SSF_Encrypt	单包数据加密
byte[]	SSF_EncryptUpdate	多包数据加密
byte[]	SSF_EncryptFinal	结束加密
void	SSF_DecryptInit	解密初始化
byte[]	SSF_Decrypt	单包数据解密
byte[]	SSF_DecryptUpdate	多包数据解密
byte[]	SSF_DecryptFinal	结束解密

7.10.2　加密初始化

方法声明　void SSF_EncryptInit(
BlockCipherParam blockCipherParam
) throws ResultCodeException
功能描述　对称加密初始化，设置对称加密算法的相关参数。
参数　blockCipherParam　分组密码参数
返回值　无
抛出异常　ResultCodeException.SSF_FAIL　失败
ResultCodeException.SSF_UNKNOWNERR　异常错误
ResultCodeException.SSF_OBJERR　对象错误
ResultCodeException.SSF_INVALIDPARAMERR无效的参数

7.10.3　单包数据加密

方法声明　byte[] SSF_Encrypt(
byte[] data,
int dataLen
) throws ResultCodeException
功能描述　对单一分包的消息进行加密，并输出加密结果。
参数　data　待加密数据
dataLen　待加密数据长度
返回值　密文数据
抛出异常　ResultCodeException.SSF_ENCRYPTERR　加密错误
ResultCodeException.SSF_ENCRYPTPADERR　加密填充错误
ResultCodeException.SSF_OBJERR　对象错误
ResultCodeException.SSF_INVALIDPARAMERR无效的参数
ResultCodeException.SSF_NOTINITIALIZEERR 未初始化

7.10.4 多包数据加密

方法声明	byte[] SSF_EncryptUpdate(byte[] data, int dataOffset, int dataLen) throws ResultCodeException	
功能描述	对多个分包的消息进行加密计算,并输出加密结果。	
参数	data	加密数据
	dataOffset	加密数据偏移量
	dataLen	加密数据长度
返回值	密文数据	
抛出异常	ResultCodeException.SSF_NOTINITIALIZEERR	未初始化
	ResultCodeException.SSF_OBJERR	对象错误

7.10.5 结束加密

方法声明	byte[] SSF_EncryptFinal( ) throws ResultCodeException	
功能描述	结束多个分包数据的加密,并输出加密结果。	
参数	无	
返回值	剩余密文数据	
抛出异常	ResultCodeException.SSF_UNKNOWNERR	异常错误

7.10.6 解密初始化

方法声明	void SSF_DecryptInit(BlockCipherParam blockCipherParam) throws ResultCodeException	
功能描述	对称解密初始化,设置解密密钥的相关参数。	
参数	blockCipherParam	分组密码参数
返回值	无	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_OBJERR	对象错误
	ResultCodeException.SSF_INVALIDPARAMERR	无效的参数

7.10.7 单包数据解密

方法声明	byte[] SSF_Decrypt(byte[] data, int dataLen) throws ResultCodeException	
功能描述	对单一分包的消息进行解密,并输出解密结果。	
参数	data	待解密数据
	dataLen	待解密数据长度

返回值　明文数据

抛出异常　ResultCodeException.SSF_DECRYPTERR　解密错误

ResultCodeException.SSF_NOTINITIALIZEERR 未初始化

ResultCodeException.SSF_OBJERR　对象错误

7.10.8 多包数据解密

方法声明　byte[] SSF_DecryptUpdate(

byte[] data,

int dataOffset,

int dataLen

) throws ResultCodeException

功能描述　对多个分包的消息进行解密计算，并输出解密结果。

参数　data　待解密数据

dataOffset　待解密数据偏移量

dataLen　待解密数据

返回值　明文数据

抛出异常　ResultCodeException.SSF_DECRYPTERR　解密错误

ResultCodeException.SSF_NOTINITIALIZEERR 未初始化

ResultCodeException.SSF_OBJERR　对象错误

7.10.9 结束解密

方法声明　byte[] SSF_DecryptFinal(

) throws ResultCodeException

功能描述　结束多个分包数据的解密，并输出解密结果。

参数　无

返回值　明文数据

抛出异常　ResultCodeException.SSF_UNKNOWNERR　异常错误

7.11 密码杂凑接口

7.11.1 概述

密码杂凑接口(IDigest)主要完成密码杂凑算法的初始化、计算。

IDigest 接口系列方法见表 16。

表 16　IDigest 接口系列方法

类型	定义	说明
void	SSF_DigestInit	杂凑初始化
byte[]	SSF_Digest	单包数据密码杂凑
void	SSF_DigestUpdate	多包数据密码杂凑
byte[]	SSF_DigestFinal	结束密码杂凑

7.11.2 杂凑初始化

方法声明	void SSF_DigestInit(long algId, byte[] pubKey, byte[] pucID) throws ResultCodeException	
功能描述	杂凑初始化。	
参数	algId	密码杂凑算法标识
	pubKey	签名者公钥,当密码杂凑算法标识为 SGD_SM3 时有效
	pucID	签名者 ID 值,当密码杂凑算法标识为 SGD_SM3 时有效
返回值	无	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_INVALIDPARAMERR	无效的参数
	ResultCodeException.SSF_NOTSUPPORTALG	不支持的标识
备注	当密码杂凑算法标识为 SGD_SM3 且签名者 ID 值长度不为 0 的情况下,pubKey 和 pucID 有效,执行 SM2 算法签名预处理 1 操作,计算过程遵循 GB/T 35276。	

7.11.3 单包数据密码杂凑

方法声明	byte[] SSF_Digest(byte[] data, int dataLen) throws ResultCodeException	
功能描述	对单一分包的消息进行密码杂凑计算,并输出结果。	
参数	data	待计算数据,不能为空
	dataLen	待计算数据长度
返回值	杂凑值	
抛出异常	ResultCodeException.SSF_HASHERR	杂凑运算错误
	ResultCodeException.SSF_NOTINITIALIZEERR	未初始化

7.11.4 多包数据密码杂凑

方法声明	void SSF_DigestUpdate(byte[] data, int dataOffset, int dataLen) throws ResultCodeException	
功能描述	对多个分包的消息进行密码杂凑计算,不输出结果。	
参数	data	待计算数据,不能为空
	dataOffset	待计算数据偏移量
	dataLen	待计算数据长度

返回值　无

抛出异常　ResultCodeException.SSF_HASHERR　杂凑运算错误

ResultCodeException.SSF_NOTINITIALIZEERR　未初始化

7.11.5　结束密码杂凑

方法声明　byte[] SSF_DigestFinal(

) throws ResultCodeException

功能描述　结束多个分包消息的密码杂凑计算操作，输出结果。

参数　无

返回值　杂凑值

抛出异常　ResultCodeException.SSF_FAIL　失败

ResultCodeException.SSF_UNKNOWNERR　异常错误

备注　SSF_DigestFinal 应用于 SSF_DigestUpdate 之后。

7.12　消息鉴别码接口

7.12.1　概述

消息鉴别码接口(IMac)主要完成消息鉴别码运算的初始化、计算。

IMac 接口系列方法见表 17。

表 17　IMac 接口系列方法

类型	定义	说明
void	SSF_MacInit	消息鉴别码运算初始化
byte[]	SSF_Mac	单包数据消息鉴别码运算
void	SSF_MacUpdate	多包数据消息鉴别码运算
byte[]	SSF_MacFinal	结束消息鉴别码运算

7.12.2　消息鉴别码运算初始化

方法声明　void SSF_MacInit(

byte[] key

BlockCipherParam macParam

) throws ResultCodeException

功能描述　消息鉴别码初始化，设置计算消息鉴别码所需的参数。

参数　key　计算消息鉴别码的密钥

macParam　消息鉴别计算相关参数，包括初始向量、初始向量长度、填充方法等

返回值　无

抛出异常　ResultCodeException.SSF_FAIL　失败

ResultCodeException.SSF_UNKNOWNERR　异常错误

ResultCodeException.SSF_NOTINITIALIZEERR　未初始化

ResultCodeException.SSF_OBJERR　对象错误

备注　消息鉴别码采用分组加密算法 CBC 模式，将加密结果的最后一块作为计算结果。待计算数据的长度应是分组加密算法块长的倍数，接口内部不做数据填充。

7.12.3 单包数据消息鉴别码运算

方法声明　byte[] SSF_Mac(
byte[] data,
int dataLen
) throws ResultCodeException

功能描述　计算单一分包数据的消息鉴别码，并输出结果。

参数		
	data	待计算数据
	dataLen	待计算数据长度
返回值	消息鉴别码	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_NOTINITIALIZEERR	未初始化

备注　调用 SSF_Mac 之前，应调用 SSF_MacInit 消息鉴别码运算初始化操作。SSF_Mac 等价于多次调用 SSF_MacUpdate 之后再调用 SSF_MacFinal。

7.12.4 多包数据消息鉴别码运算

方法声明　void SSF_MacUpdate(
byte[] data,
int dataOffset,
int dataLen
) throws ResultCodeException

功能描述　计算多个分包数据的消息鉴别码，不输出结果。

参数		
	data	待计算数据
	dataOffset	待计算数据偏移量
	dataLen	待计算数据长度
返回值	无	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_NOTINITIALIZEERR	未初始化

备注　调用 SSF_MacUpdate 之前，应调用 SSF_MacInit 消息鉴别码运算初始化操作；调用 SSF_MacUpdate 之后，应调用 SSF_MacFinal 结束多个分组数据的消息鉴别码计算。

7.12.5 结束消息鉴别码运算

方法声明　byte[] SSF_MacFinal(
) throws ResultCodeException

功能描述　结束多个分包数据的消息鉴别码计算操作，输出消息鉴别码。

参数		
	无	
返回值	消息鉴别码	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误

备注　SSF_MacFinal 应在 SSF_MacUpdate 之后。

7.13 带密钥的杂凑运算接口

7.13.1 概述

带密钥的杂凑运算接口(IHMAC)主要完成带密钥的杂凑运算的初始化、计算。

IHMAC 接口系列方法见表 18。

表 18 IHMAC 接口系列方法

类型	定义	说明
void	SSF_HMACInit	带密钥的杂凑运算初始化
void	SSF_HMACUpdate	带密钥的多包杂凑运算
byte[]	SSF_HMACFinal	带密钥的杂凑运算结束

7.13.2 带密钥的杂凑运算初始化

方法声明 void SSF_HMACInit(
byte[] key
) throws ResultCodeException

功能描述 三步式带密钥的数据杂凑运算的第一步。

参数		
	key	密钥
返回值	无	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_OBJERR	对象错误

7.13.3 带密钥的多包杂凑运算

方法声明 void SSF_HMACUpdate(
byte[] data,
int dataLen
) throws ResultCodeException

功能描述 三步式带密钥的数据杂凑运算的第二步,对输入的明文进行杂凑运算。

参数		
	data	待计算数据
	dataLen	待计算数据长度
返回值	无	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误
	ResultCodeException.SSF_NOTINITIALIZEERR	未初始化

7.13.4 带密钥的杂凑运算结束

方法声明 byte[] SSF_HMACFinal(
) throws ResultCodeException

功能描述 三步式带密钥的数据杂凑运算的第三步,杂凑运算结束返回结果。

参数	无	
返回值	杂凑计算结果	
抛出异常	ResultCodeException.SSF_FAIL	失败
	ResultCodeException.SSF_UNKNOWNERR	异常错误

8 安全要求

8.1 模块使用阶段

模块的使用分成两个阶段。

a) 出厂阶段：模块出厂时，预置模块鉴别密钥，在此阶段除修改模块鉴别密钥以及创建应用操作外，禁止其他操作。

b) 应用阶段：已创建了应用的模块进入应用阶段。在此阶段，可进行所有操作。

8.2 权限管理

8.2.1 权限分类

权限分为模块权限、用户权限和管理员权限。

a) 模块权限：通过模块鉴别后获得模块权限。

b) 用户权限：用户 PIN 码验证通过后，获得用户权限，用户权限只作用于其所在的应用。

c) 管理员权限：管理员 PIN 码验证通过后，获得管理员权限，管理员权限只作用于其所在的应用。

8.2.2 权限使用

权限的使用遵循以下要求：

a) 模块权限仅用于创建应用、删除应用和修改模块鉴别密钥；

b) 创建和删除容器需要用户权限；

c) 创建文件的权限在创建应用时指定；

d) 文件的读写权限在创建文件时指定；

e) 容器内私钥的使用需要用户权限；

f) 用户 PIN 码和管理员 PIN 码均具有最大重试次数，在创建应用时设定，当验证 PIN 码错误次数达到最大重试次数后，PIN 码即锁死；

g) 用户 PIN 码的解锁需要管理员权限；

h) 用户 PIN 码的修改需要用户权限，管理员 PIN 码的修改需要管理员权限。

8.2.3 模块鉴别

应通过模块鉴别后才能在模块内创建和删除应用。

模块鉴别使用 SM4 分组密码算法和模块鉴别密钥进行，鉴别的流程如下：

a) 被鉴别方调用模块接口的 SSF_GenRandom 方法从模块获取 8 字节随机数 RND，并用 0x00 将其填充至密码算法的分块长度，组成数据块 D0；

b) 被鉴别方对 D0 加密，得到加密结果 D1，并调用模块接口的 SSF_ModAuth，将 D1 发送至模块；

c) 模块收到 D1 后，验证 D1 是否正确。正确则通过模块鉴别，否则模块鉴别失败。

8.2.4 PIN 码安全要求

PIN 码安全要求如下：

a) PIN 码长度不少于 6 个字节；

b) PIN 码在模块和本接口之间的传输过程中应采取保护措施，防止 PIN 码泄露；

c) PIN 码在模块中应安全存储，不可从模块中导出。

8.3 其他安全要求

移动终端密码模块的其他安全性设计应遵循 GB/T 37092 中的相关安全要求。

附 录 A
（规范性）
异常码预定义值和说明

密码模块接口方法中异常码预定义值和说明见表 A.1。

表 A.1 异常码预定义值和说明

异常码	预定义值	说明
SSF_FAIL	0x0D000001	失败
SSF_UNKNOWNERR	0x0D000002	异常错误
SSF_NOTSUPPORTYETERR	0x0D000003	不支持的服务
SSF_FILEERR	0x0D000004	文件操作错误
SSF_INVALIDPARAMERR	0x0D000005	无效的参数
SSF_READFILEERR	0x0D000006	读文件错误
SSF_WRITEFILEERR	0x0D000007	写文件错误
SSF_NAMELENERR	0x0D000008	名称长度错误
SSF_KEYUSAGEERR	0x0D000009	密钥使用错误
SSF_MODULUSLENERR	0x0D00000A	模的长度错误
SSF_NOTINITIALIZEERR	0x0D00000B	未初始化
SSF_OBJERR	0x0D00000C	对象错误
SSF_MEMORYERR	0x0D00000D	内存错误
SSF_TIMEOUTERR	0x0D00000E	超时
SSF_INDATALENERR	0x0D00000F	输入数据长度错误
SSF_INDATAERR	0x0D000010	输入数据错误
SSF_GENRANDERR	0x0D000011	生成随机数错误
SSF_HASHOBJERR	0x0D000012	杂凑对象错误
SSF_HASHERR	0x0D000013	杂凑运算错误
SSF_HASHNOTEQUALERR	0x0D000014	杂凑值不相等
SSF_KEYNOTFOUNDERR	0x0D000015	密钥未发现
SSF_CERTNOTFOUNDERR	0x0D000016	证书未发现
SSF_NOTEXPORTERR	0x0D000017	对象未导出
SSF_DECRYPTPADERR	0x0D000018	解密时做补丁操作
SSF_MACLENERR	0x0D000019	MAC 长度错误
SSF_BUFFERTOOSMALL	0x0D00001A	缓冲区不足
SSF_KEYINFOTYPEERR	0x0D00001B	密钥类型错误
SSF_NOTEVENTERR	0x0D00001C	无事件错误
SSF_MODREMOVEDERR	0x0D00001D	模块已移除

表 A.1　异常码预定义值和说明（续）

异常码	预定义值	说明
SSF_PININCORRECT	0x0D00001E	PIN 不正确
SSF_PINLOCKED	0x0D00001F	PIN 被锁死
SSF_PININVALID	0x0D000020	PIN 无效
SSF_PINLENRANGE	0x0D000021	PIN 长度错误
SSF_USERALREADYLOGGEDIN	0x0D000022	用户已经登录
SSF_USERPINNOTINITIALIZED	0x0D000023	没有初始化用户口令
SSF_MODLOCKED	0x0D000024	模块已锁定
SSF_USERTYPEINVALID	0x0D000025	PIN 类型错误
SSF_APPLICATIONNAMEINVALID	0x0D000026	应用名称无效
SSF_APPLICATIONEXISTS	0x0D000027	应用已经存在
SSF_USERNOTLOGGEDIN	0x0D000028	用户没有登录
SSF_APPLICATIONNOTEXISTS	0x0D000029	应用不存在
SSF_FILEALREADYEXISTS	0x0D00002A	文件已经存在
SSF_NOROOM	0x0D00002B	空间不足
SSF_FILENOTEXISTS	0x0D00002C	文件不存在
SSF_REACHMAXCONTAINERCOUNT	0x0D00002D	已达到最大可管理容器数
SSF_MODNOTEXIST	0x0D00002E	模块不存在
SSF_CONTAINERNOTEXIST	0x0D00002F	容器不存在
SSF_CONTAINERALREADYEXIST	0x0D000030	容器已经存在
SSF_PINERR	0x0D000031	PIN 错误
SSF_USERCANCELERR	0x0D000032	用户取消错误
SSF_APPLICATIONALREADYOPENED	0x0D000033	应用已经打开
SSF_CONTAINERALREADYOPENED	0x0D000034	容器已经打开
SSF_ENCRYPTERR	0x0D000035	加密错误
SSF_ENCRYPTPADERR	0x0D000036	加密填充错误
SSF_DECRYPTERR	0x0D000037	解密错误
SSF_PARSEERR	0x0D000038	解析错误
SSF_COMPUTEERR	0x0D000039	计算错误
SSF_HARDWAREERR	0x0D00003A	硬件错误
SSF_DATAKEYERR	0x0D00003B	加密密钥错误
SSF_NOTAUTHORIZED	0x0D00003C	未鉴别
SSF_NOTSUPPORTALG	0x0D00003D	不支持的标识