中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

手 机 支 付 系 统
多 应 用 平 台 加 密 机 接 口 规 范

Title

版 本 号 ： 0.8.0

XXXX-XX-XX 发 布　　XXXX-XX-XX 实 施

中国移动通信有限公司　　发布

前　言

本规范规定了<*业务名称*>过程中涉及的网元设备间的通信接口，是<*业务名称*所涉及的网元设备需要遵从的技术文件。

本规范主要包括以下几方面内容<*对本规范中的主要章节和其中的内容进行列举和简要介绍*>。

附件 1 是*[提示性|标准性]*>附件

附件 2 是*[提示性|标准性]*>附件

附件 3 是*[提示性|标准性]*>附件

；明确附件的性质

本规范由中国移动通信集团公司技术部归口管理。

本规范解释权属于中国移动通信集团公司，具体技术细节由中国移动研发中心负责解释。

本规范起草单位：中国移动通信有限公司研究院

本标准主要起草人：*起草人 1 姓名*、*起草人 2 姓名*、……

目　录

1. 范围

本规范对~~手机支付系统 OTA 平台~~多应用开放平台与加密机之间的接口提出规定，中国移动通信集团内部和厂商共同使用，用于在工程建设方面为集团公司和省公司提供技术依据。

2. 引用标准

下列标准所包含的条文，通过在本标准中引用而成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

[1] 发布号 <引用标准的名称，版本号>
[2] 发布号 <引用标准的名称，版本号>
[3] 发布号 <引用标准的名称，版本号>

3. 相关术语与缩略语解释

<术语 1> <术语解释>
<术语 2> <术语解释>
<术语 3> <术语解释>

<缩略语 1> <缩略语英文解释> <缩略语中文解释>
<缩略语 2> <缩略语英文解释> <缩略语中文解释>
<缩略语 3> <缩略语英文解释> <缩略语中文解释>

4. 接口定义

本接口为JAVA接口，package OTAHSM，public class OTAAPI。

4.1. 产生随机数接口

4.1.1. 功能说明

产生指定长度的随机数

4.1.2. 函数原型

```
public native int HsmGenarateRandom(
                    int RandomLen,
                    byte[] Rand
                    )
```

4.1.3. 输入参数

参数名	类型和长度	说明
RandomLen	整型	需要产生的随机数长度(以字节为单位)

4.1.4. 输出参数

参数名	类型和长度	说明
Rand	字节数组	输出的指定长度的随机数

4.2. 分散导出多个密钥密文并计算校验值

4.2.1. 功能说明

根据指定参数要求分散得到一个或多个卡片子密钥采用保护密钥加密（没有填充） ，并计算密钥校验值输出。

4.2.2. 函数原型

```
public native int HsmGenerateMulKeyAndCheck(
            int AlgFlag,
            int SessionKeyFlag
            int EncKeyVer,
            int    EncKeyIndex,
            int    EncKeyDvsNum,
```

```
    int    EncKeyDvsData,
    byte[]    Seed,
    int KeyNum,
    byte[]    MulKeyVer,
    byte[]    MulKeyIndex,
    int    KeyDvsNum,
    byte[]    KeyDvsData,
    byte[]    MulKeys,
    byte[]    MulMAC
);
```

4.2.3. 输入参数

参数名	类型和长度	说明
AlgFlag	整型	分散算法标识，参见参数约定
SessionKeyFlag	整型	过程密钥标识
EncKeyID	整型	保护密钥标识
EncKeyVer	整型	保护密钥版本
EncKeyIndex	整型	保护密钥索引
EncKeyDvsNum	整型	保护密钥分散次数，1-3
EncKeyDvsData	字节数组 8/16/24	保护密钥分散因子
Seed	8	随机因子，计算保护密钥的会话密钥。如果过程密钥表示为 0，则该字段可以忽略。
KeyNum	整型	本指令请求的密钥个数 1-50
MulKeyID	字节数组	密钥标识，每一个字节对应一个密钥。 说明： 由于类型、版本、索引是多对多的关系，为了避免混乱，要求 MulKeyType、MulKeyVer、MulKeyIndex 三个属性，同时只能有一个是多字节。
MulKeyVer	字节数组	密钥版本 ，每一个字节对应一个密钥
MulKeyIndex	字节数组	密钥索引 ，每一个字节对应一个密钥
KeyDvsNum	整型	密钥分散次数（1-3） 。
KeyDvsData	字节数组 KeyNum *分散次数*8	密钥分散因子（多个密钥的分散因子连接在一起），每个密钥的分散因子可以不同。

说明：

1、 密钥的加密算法：参考《CMSAC 卡规范》B.1.1.2，3DES-ECB 算法

2、 校验值的算法：校验值算法见《CMSAC 卡规范》C.2 节的说明，包括对称密钥和公钥的校验值计算要求

4.2.4. 输出参数

参数名	类型和长度	说明
MulKeys	字节数组 N*16	依次连接所有密钥密文输出
MulCheckValue	字节数组 N*8	依次连接所有密钥校验值输出

4.3. 数据加密接口

4.3.1. 功能说明

用指定的密钥经过若干级分散（可选）和过程密钥计算（可选）后，使用指定的算法和填充方式对输入数据进行加密操作。

4.3.2. 函数原型

```
public native int HsmDataEncrypt (
    int KeyVer,
    int KeyIndex,
    int AlgFlag,
    int OperateFlag,
    int PadFlag,
    int DivNum,
    byte[] DivData,
    int SessionKeyFlag,
    byte[] SKeySeed,
    int DataLen,
    byte[] Data,
    int[] CipheredDataLen,
    byte[] CipheredData
)
```

4.3.3. 输入参数

参数名	类型和长度	说明

KeyID	整型	密钥标识
KeyVer	整型	密钥版本号
KeyIndex	整型	密钥索引号
AlgFlag	整型	算法标识： AES:0x88; 3DES-ECB：0x81 3DES-CBC:0x82 DES-CBC：0x84
EncDecFlag	整型	加解密标识： 加密：0（固定填写 0）
PadFlag	整型	填充标识： 外部填充：0； 内部填充：1；
DivNum	整型	密钥分散级数，应大于等于 0
DivData	字节数组	分散因子，多级分散则各级分散因子顺序连接，由于每级的分散因子都是 16 字节，固此参数必定是 16 字节的整数倍。
SessionKeyFlag	整型	是否需要过程密钥标识： 无过程密钥：0； 有过程密钥：1；

SKeySeed	字节数组	产生过程密钥的因子
DataLen	整型	输入数据长度
Data	字节数组	输入数据(要求由外部进行填充)

4.3.4. 输出参数

参数名	类型和长度	说明
OutputDataLen	整型	输出数据长度
OutputData	字节数组	输出数据

4.4. 数据解密接口

4.4.1. 功能说明

用指定的密钥经过若干级分散（可选）和过程密钥计算（可选）后，使用指定的算法和填充方式对输入数据进行解密操作。

4.4.2. 函数原型

```
public native int HsmDataDecrypt(
    byte[] Key,
    int AlgFlag,
    int OperateFlag,
    int PadFlag,
    int DivNum,
    byte[] DivData,
    int SessionKeyFlag,
    byte[] SKeySeed,
    int DataLen,
    byte[] Data,
    int[] OutputDataLen,
    byte[] OutputData
```

)

4.4.3. 输入参数

参数名	类型和长度	说明
Key	字节数组	密钥密文
AlgFlag	整型	算法标识： AES:0x88; 3DES-ECB：0x81 3DES-CBC:0x82 DES-CBC：0x84
EncDecFlag	整型	加解密标识： 解密：1
PadFlag	整型	填充标识： 外部填充：0； 内部填充：1；
DivNum	整型	密钥分散级数，应大于等于 0
DivData	字节数组	分散因子，多级分散则各级分散因子顺序连接，由于每级的分散因子都是 16 字节，固此参数必定是 16 字节的整数倍。
SessionKeyFlag	整型	是否需要过程密钥标识：

		无过程密钥：0； 有过程密钥：1；
SKeySeed	字节数组	产生过程密钥的因子
DataLen	整型	输入数据长度
Data	字节数组	输入数据(要求由外部进行填充)

4.4.4. 输出参数

参数名	类型和长度	说明
OutputDataLen	整型	输出数据长度
OutputData	字节数组	输出数据

~~4.4.~~4.5. 产生 MAC 接口

~~4.4.1.~~4.5.1. 功能说明

用指定的密钥经过若干级分散（可选）和过程密钥计算（可选）后，使用指定的算法和填充方式对输入数据求指定长度的消息认证码。

~~4.4.2.~~4.5.2. 函数原型

```
public native int HsmGenerateMAC(
        int KeyIndex,
        int KeyVer,
        int AlgFlag,
        int PadFlag,
        int DivNum,
        byte[] DivData,
        int SessionKeyFlag,
```

byte[] SkeySeed,
int DataLen,
byte[] Data,
int MACDataLen,
byte[] MACData
)

~~4.4.3.~~4.5.3. 输入参数

参数名	类型和长度	说明
KeyID	整型	密钥标识
KeyVer	整型	密钥版本号
KeyIndex	整型	密钥索引号
AlgFlag	整型	算法标识(具体定义同上一接口)
PadFlag	整型	填充标识(具体定义同上一接口)
DivNum	整型	密钥分散级数 ,应大于等于 0
DivData	字节数组	分散因子 ,多级分散则各级分散因子顺序连接 ,由于每级的分散因子都是 16 字节 , 固此参数必定是 16 字节的整数倍。
SessionKeyFlag	整型	是否需要过程密钥标识(具体定义同上一接口)

SkeySeed	字节数组	产生过程密钥的因子
DataLen	整型	输入数据长度
Data	字节数组	输入数据
MACDataLen	整型	需要的 MAC 数据长度

~~4.4.4.~~4.5.4. 输出参数

参数名	类型和长度	说明
MACData	字节数组	输出的指定长度的 MAC 数据

~~4.5.~~4.6. 验证 MAC 接口

~~4.5.1.~~4.6.1. 功能说明

用指定的密钥经过若干级分散（可选）和过程密钥计算（可选）后，使用指定的算法和填充方式对输入数据和指定长度的消息认证码进行验证。

~~4.5.2.~~4.6.2. 函数原型

```
public native int HsmVerifyMAC(
    int KeyVer,
    int KeyIndex,
    int AlgFlag,
    int PadFlag,
    int DivNum,
    byte[] DivData,
    int SessionKeyFlag,
    byte[] SkeySeed,
    int DataLen,
    byte[] Data,
    int MACDataLen,
    byte[] MACData
```

)

4.5.3.4.6.3. 输入参数

参数名	类型和长度	说明
KeyID	整型	密钥标识
KeyVer	整型	密钥版本号
KeyIndex	整型	密钥索引号
AlgFlag	整型	算法标识(具体定义同上一接口)
PadFlag	整型	填充标识(具体定义同上一接口)
DivNum	整型	密钥分散级数 ,应大于等于 0
DivData	字节数组	分散因子 ,多级分散则各级分散因子顺序连接 ,由于每级的分散因子都是 16 字节 , 固此参数必定是 16 字节的证书倍。
SessionKeyFlag	整型	是否需要过程密钥标识(具体定义同上一接口)
SkeySeed	字节数组	产生过程密钥的因子
DataLen	整型	输入数据长度
Data	字节数组	输入数据

MACDataLen	整型	需要的 MAC 数据长度
MACData	字节数组	输出的指定长度的 MAC 数据

~~4.5.4.~~4.6.4. 输出参数

参数名	类型和长度	说明
无	无	无

~~4.6.~~4.7. 产生 C-MAC 接口

~~4.6.1.~~4.7.1. 功能说明

用指定的密钥经过若干级分散（可选）和过程密钥计算（可选）后，使用指定的算法和填充方式对输入数据求指定长度的消息认证码。

~~4.6.2.~~4.7.2. 函数原型

```
public native int HsmGenerateCMAC(
    int KeyIndex,
    int KeyVer,
    int AlgFlag,
    int PadFlag,
    int DivNum,
    byte[] DivData,
    int SessionKeyFlag,
    byte[] SkeySeed,
    byte[] IcvData,
    int DataLen,
    byte[] Data,
    int MACDataLen,
    byte[] MACData,
    byte[] ICVResult
)
```

~~4.6.3.~~4.7.3. 输入参数

参数名	类型和长度	说明
KeyID	整型	密钥标识
KeyVer	整型	密钥版本号
KeyIndex	整型	密钥索引号
AlgFlag	整型	算法标识(具体定义同上一接口)
PadFlag	整型	填充标识(具体定义同上一接口)
DivNum	整型	密钥分散级数 ,应大于等于 0
DivData	字节数组	分散因子 ,多级分散则各级分散因子顺序连接 ,由于每级的分散因子都是 16 字节 , 固此参数必定是 16 字节的整数倍。
SessionKeyFlag	整型	是否需要过程密钥标识(具体定义同上一接口)
SkeySeed	字节数组	产生过程密钥的因子
IcvData	字节数组	ICV
DataLen	整型	输入数据长度

Data	字节数组	输入数据
MACDataLen	整型	需要的 MAC 数据长度

~~4.6.4.~~4.7.4. 输出参数

参数名	类型和长度	说明
MACData	字节数组	输出的指定长度的 MAC 数据
ICVResult	字节数组	8 字节 ,过程密钥的左半部对 MACData 结果做加密,输出

~~4.7.~~4.8. 产生 RSA 密钥

~~4.7.1.~~4.8.1. 功能说明

在指定位置随机产生指定长度 RSA 密钥。

~~4.7.2.~~4.8.2. 函数原型

```
public native int HsmGenerateRSAKey(
                int   KeyIndex,
                int   KeyLen,
                );
```

~~4.7.3.~~4.8.3. 输入参数

参数名	类型	说明
KeyIndex	整型	指定产生密钥存放位置索引
KeyLen	整型	指定密钥长度

~~4.7.4.~~4.8.4. 输出参数

无

~~4.8.~~4.9. 计算签名

~~4.8.1.~~4.9.1. 功能说明

对指定数据进行数字签名

~~4.8.2.~~4.9.2. 函数原型

```
public native int HsmGenSignature（
        int    KeyIndex,
        int Flag,
        int    DataLen,
        byte[]    data，
        int SignatureLen,
        byte[]    Signature
        );
```

~~4.8.3.~~4.9.3. 输入参数

参数名	类型	说明
KeyIndex	整型	指定产生密钥存放位置索引
Flag	整型	算法标识，默认值 0x90（SHA1）
DataLen,	整型	签名数据长度
Data	字节数组	签名计算数据

~~4.8.4.~~4.9.4. 输出参数

参数名	**类型和长度**	**说明**
SignatureLen	**整型**	**签名长度**
Signature	**字节数组**	**签名结果**

~~4.9.~~4.10.验证签名

~~4.9.1.~~4.10.1. 功能说明

验证一个 RSA 签名。

私钥计算签名和公钥验签的签名计算数据均为原始数据，加密机内部对原始数据做

SHA1，再对相应的 SHA1 结果做签名。

~~4.9.2.~~4.10.2. 函数原型

```
public native int HsmVerifySignature (
                int    KeyIndex,
                int    DataLen,,
                byte[]    data
                int    SignatureLen,
                byte[]    Signature
                );
```

~~4.9.3.~~4.10.3. 输入参数

参数名	类型	说明
KeyIndex	整型	指定产生密钥存放位置索引
Flag	整型	算法标识，默认值 0x90（SHA1）
DataLen,	整型	签名数据长度
Data	字节数组	签名计算数据
SignatureLen	整型	待验证签名长度
Signature	字节数组	待验证签名值

~~4.9.4.~~4.10.4. 输出参数

无

~~4.10.~~4.11. 导出 RSA 公钥

~~4.10.1.~~4.11.1. 功能说明

对指定的 RSA 密钥根据加密标志将公钥以明文方式导出。

~~4.10.2.~~4.11.2. 函数原型

```
public native int HsmExportPK(
    int PKIndex,
    int EncKeyID,
    int EncKeyVer,
    int EncKeyIndex,
    int PadDataLen,
    byte[] PadData,
```

int PKDataLen,
byte[] PKData，

int PKCheckLen，

byte[] PKCheckValue

)

~~4.10.3.~~4.11.3. 输入参数

参数名	类型和长度	说明
PKIndex	整型	指定需要输出公钥位置
PKType	整型	导出公钥的类型： 1：自定义 2：符合 DER 编码方式的公钥
EncKeyID	整型	密钥 ID： 1：计算公钥模数 2：计算公钥指数
EncKeyVer	整型	密钥版本号
EncKeyIndex	整型	密钥索引号
PadDataLen	整型	需要和公钥一起加密的填充数据长度
PadData	字节数组	需要和公钥一起加密的填充数据

~~4.10.4.~~4.11.4. 输出参数

参数名	类型和长度	说明
PKDataLen	整型	输出公钥模数/指数长度
PKData	字节数组	输出公钥模数/指数明文
PKCheckLen	整型	公钥模数/指数的校验值长度
PKCheckValue	字节数组	公钥模数/指数校验值

4.12. 转加密

4.12.1. 功能说明

将采用 Key1 加密的数据转换为 Key2 加密，该指令主要用于对密钥的转加密。

4.12.2. 函数原型

```
int HsmTranslateKey1ToKey2(
                                int Key1ID,
                                int Key1Ver,
                                int Key1Index,
                                int Key1AlgFlag
                                int Key1DivNum
                                byte[] Key1DivData
                                int Key1SessionKeyFlag
                                byte[] Key1SkeySeed
                                int Key2ID,
                                int Key2Ver,
                                int Key2Index,
                                int Key2AlgFlag
                                int Key2DivNum
                                byte[] Key2DivData
                                int Key2SessionKeyFlag
                                byte[] Key2SkeySeed
                                int inDatalen,
                                byte[] bInDataByKey1,
                                int[] outDatalen,
```

byte[] bOutDataByKey2
);

4.12.3. 输入参数

参数名	类型和长度	说明
Key1ID	整型	密钥 1 标识
Key1Ver	整型	密钥 1 版本号
Key1Index	整型	密钥 1 索引号
Key1AlgFlag	整型	算法标识： 0x81：3DES-ECB
Key1DivNum	整型	密钥分散级数，应大于等于 0
Key1DivData	字节数组	分散因子，多级分散则各级分散因子顺序连接，由于每级的分散因子都是 16 字节，固此参数必定是 16 字节的整数倍(如果采用标准的 PBOC 算法，则 16 字节分散因子为 8 字节因子+8 字节因子取反)。
Key1SessionKeyFlag	整型	是否需要过程密钥标识： 无过程密钥：0； 有过程密钥：1；
Key1SkeySeed	字节数组	产生过程密钥的因子
Key2ID	整型	密钥 2 标识
Key2Ver	整型	密钥 2 版本号
Key2Index	整型	密钥 2 索引号

AlgFlag	整型	算法标识： 0x81：3DES-ECB
DivNum	整型	密钥分散级数，应大于等于 0
DivData	字节数组	分散因子（分散算法采用 CMSAC 规范中规定的密钥分散算法），多级分散则各级分散因子顺序连接，由于每级的分散因子都是 16 字节，固此参数必定是 16 字节的整数倍。
SessionKeyFlag	整型	是否需要过程密钥标识： 无过程密钥：0； 有过程密钥：1；
SkeySeed	字节数组	产生过程密钥的因子
inDatalen	整型	Key1 加密的数据密文长度
bInDataByKey1	HEX	Key1 加密的数据密文

4.12.4. 输出参数

参数名	类型和长度	说明
outDatalen	整型	Key2 加密的数据密文长度
bOutDataByKey2	HEX	Key2 加密的数据密文

附录 A 参数约定

A.1.过程密钥标识

0：不使用过程密钥
1：使用过程密钥

A.2.加解密标识

1：加密
2：解密

A.3.函数返回值

0：表示返回正确
-1：加密机连接错误
-2：数据长度错
-3：离散次数错
-4：密钥版本错
-5：密钥索引错
-6：密钥类型参数错
-7：密钥长度参数错
-8：指定密钥不存在
-9：加密机主密钥不存在
-10：MAC长度错
>0：加密机厂商定义错误代码

A.4.算法标志

值	含义
‘00’-‘7F’	为私有定义预留
‘80’	DES
‘81’	预留（3DES）
‘82’	3DES-CBC
‘83’	DES-ECB
‘84’	DES-CBC
‘85’-‘87’	为其他对称算法预留
‘88’	AES
‘89’-‘8F’	为其他对称算法预留
‘90’	HMAC-SHA1

附录 B 编制历史

编制历史		
版本号	更新时间	主要内容或重大修改
~~1.2.0~~0.8.0	2011-12-1	根据电子现金应用个人化需求，增加转加密接口和加解密接口