渔翁密码卡应用
编程手册

版本：V2.0.0

山东渔翁信息技术股份有限公司

地　　址：山东威海市初河北路12号渔翁信息产业园
邮　　编：264209
网　　站：http://www.fisherman-it.com
电　　话：0631-5660861/2/5

声 明

版权声明：

警告和承诺：

我们做了大量的努力使本文档尽可能的完备和准确，但疏漏和缺陷之处在所难免。任何人或实体由于本文档提供的信息造成的任何损失或损害，山东渔翁信息技术股份有限公司不承担任何义务或责任。

山东渔翁信息技术股份有限公司保留未经通知用户对本文档内容进行修改的权利。

反馈信息：

如果您对本文档有任何疑问、意见或建议，请与我们联系。对您的帮助，我们十分感激。

目录

1 概述

本文档适用于渔翁密码卡跨平台应用层通用API编程接口。

此编程接口使用C语言编写，支持多线程和多进程调用，并同时兼容渔翁PCI V1.2、PCI V2.0、PCI-E V1.0、PCI-E V3.0、PCI-E V4.0、PCI-E V5.0、MINIPCIE系列密码卡。

2 接口使用

2.1.1 WINDOWS下接口使用

WINDOWS下使用接口需要以下文件：

头文件：fm_def.h、fm_cpc_pub.h。

动态库：fmapiv100.dll、fmapiv100.lib。

驱动：fm_cpc_drv.sys，fm_cpc_drv.inf。

编程时，应按顺序包含fm_def.h、fm_cpc_pub.h，并在编译链接选项中加入外部符号表fmapiv100.lib。

2.1.2 LINUX下接口使用

LINUX下使用接口需要以下文件：

头文件：fm_def.h、fm_cpc_pub.h。

动态库：libfmapiv100.so。

驱动：FM_CPC_DRV.ko、install.sh（PCI-E V 5.0密码卡还包括setup.sh等）。

编程时，应按顺序包含fm_def.h、fm_cpc_pub.h。

2.1.3 接口使用说明：

Ⅱ型MINI PCIE系列密码卡可使用接口部分：sm1，sm2，sm3, sm4,随机数，文件系统管理，设备管理。Ⅰ型MINI PCIE系统密码卡除个别接口不支持外（具体接口说明中有标注），其他接口均可以使用。

3 数据类型定义

```
#define FM_S8          char
#define FM_U8          unsigned char
#define FM_S16         short int
#define FM_U16         unsigned short int
#define FM_S32         int
```

```
#define FM_U32          unsigned int
#define FM_S64          long        /* only used in 64b os */
#define FM_U64          unsigned long  /* only used in 64b os */
#define FM_UP           unsigned long  /* sizeof(FM_UP)==sizeof(pointer) */
#define FM_F32          float
#define FM_F64          double
#define FM_VOID         void
#define FM_HANDLE       void *
#define FM_HKEYvoid *
#define FM_HUSER        void *
#define FM_BOOL         unsigned int
#define FM_NULL         ((void *) 0)
#define FM_TRUE         1
#define FM_FALSE        0
#define FM_U8_INVALID           0xff
#define FM_U16_INVALID          0xffff
#define FM_U32_INVALID          0xffffffff
#define FM_HANDLE_INVALID   (FM_HANDLE)(-1)
#define FM_I        /* input  parameter */
#define FM_O        /* output parameter */
#define FM_B        /* both input and output parameter */
```

其他类型请参照fm_def.h头文件。

4 接口函数定义

4.1 设备管理接口

4.1.1 FM_CPC_OpenDevice

函数定义

```
FM_RET FM_CPC_OpenDevice
(
   FM_I    FM_U8         *pu8Id,
   FM_I    FM_U32        u32Type,
   FM_I    FM_U32        u32Flag,
   FM_O    FM_HANDLE     *phDev
)
```

功能描述

打开密码卡设备。在使用其它API接口之前，必须首先调用本接口获取设备句柄。如果需要在多线程情形下调用密码卡接口，需在每个调用线程中执行一次打开设备操作。

参数描述

pu8Id[in]　　密码设备索引，合法范围：[0， 3]

u8Type[in]　　设备类型，有效值为：

FM_DEV_TYPE_PCI_1_2X：PCI 1.2系列密码卡

FM_DEV_TYPE_PCI_2_0X：PCI 2.0系列密码卡

FM_DEV_TYPE_PCIE_1_0X：PCIE 1.0系列密码卡

FM_DEV_TYPE_PCIE_3_0X：PCIE 3.0系列密码卡

FM_DEV_TYPE_PCIE_4_0X：PCIE 4.0系列密码卡

FM_DEV_TYPE_PCIE_5_0X：PCIE 5.0系列密码卡

FM_DEV_TYPE_MINPCIE_1_0X：MINIPCIE 1.0系列密码卡

（只能选择其中一个）

u32Flag[in]　　标识及选项，有效值为：

FM_OPEN_MULTITHREAD：使API接口支持多线程调用

FM_OPEN_MULTIPROCESS：使API接口支持多进程调用

（可采用位或进行组合）

phDev[out]　　返回的设备句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.1.2 FM_CPC_CloseDevice

函数定义

```
FM_RET FM_CPC_CloseDevice
(
   FM_I    FM_HANDLE          hDev
)
```

功能描述

关闭密码设备。在当前线程退出之前，需调用此接口关闭设备句柄以释放系统资源。

参数描述

hDev[in]　　已打开的设备句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.1.3 FM_CPC_GetDeviceInfo

函数定义

```
FM_RET FM_CPC_GetDeviceInfo
(
    FM_I    FM_HANDLE       hDev,
    FM_O    FM_DEV_INFO     *pDevInfo
)
```

功能描述

获取设备信息。包括设备的型号、序列号、存储空间大小以及所支持的算法等。

参数描述

hDev[in]	设备句柄
pDevInfo[out]	输出设备描述信息

返回值

FME_OK，成功。其他，返回相应的错误码。

4.1.4 FM_CPC_GenRandom

函数定义

```
FM_RET FM_CPC_GenRandom
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Len,
    FM_O    FM_U8           *pu8Random
)
```

功能描述

获取由物理噪声源产生的真随机数。

参数描述

hDev[in]	设备句柄
u32Len[in]	欲获取的随机数的字节长度
pu8Random[out]	缓冲区指针，用于存放获取的随机数

返回值

FME_OK，成功。其他，返回相应的错误码。

4.1.5 FM_CPC_GetErrInfo

函数定义

```
FM_RET FM_CPC_GetErrInfo
(
    FM_I    FM_U32      u32LanFlag,
```

```
    FM_I    FM_U32      u32ErrCode,
    FM_B    FM_U32      *pu32Len,
    FM_O    FM_S8       *ps8Info
)
```

功能描述

获取错误码的详细错误信息。

参数描述

u32LanFlag[in]	错误信息语言类型，有效值为： FM_LAN_CN：中文（推荐在WINDOWS下使用此选项） FM_LAN_EN：英文（推荐在LINUX下使用此选项）
u32ErrCode[in]	API函数返回的错误码
pu32Len[in out]	入参表示错误描述信息接收缓冲区的长度 出参表示错误描述信息的实际长度
ps8Info[out]	错误信息缓冲区

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2 非对称算法接口

4.2.1 FM_CPC_GenRSAKeypair

函数定义

```
FM_RET FM_CPC_GenRSAKeypair
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32KeyBits,
    FM_B    FM_HKEY             *phKey,
    FM_O    FM_RSA_PublicKey    *pPubkey,
    FM_O    FM_RSA_PrivateKey   *pPrikey
)
```

功能描述

产生指定模长的RSA密钥对，存储在卡内或通过参数导出。密钥参数除公钥指数e做特殊处理——只有前3个字节有效，且依次为01 00 01外，其余参数均按大字节序存储。当密钥句柄为FM_HKEY_TO_HOST时，通过参数导出生产的密钥对需要操作员权限；当密钥句柄不为FM_HKEY_TO_HOST时，通过参数导出生产的密钥对需要管理员权限。卡内默认可存储768对RSA密钥。

参数描述

hDev[in]　　设备句柄

u32KeyBits[in]　指定密钥的模长，有效值为1024或2048

phKey[inout]　　密钥句柄指针，有效取值如下：

FM_HKEY_TO_HOST：生成的密钥对由参数导出；

FM_HKEY_BYDEV_PERM：生成的密钥对永久地存储在卡内，密钥存储位置由密码卡自动查找；

0~63（99）：生成的密钥对永久性地存储在卡内，密钥存储位置由用户指定

pPubkey[out]　不为NULL时返回生成的RSA公钥部分

pPrikey[out]　　不为NULL时返回生成的RSA私钥部分

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.2 FM_CPC_DelRSAKeypair

函数定义

```
FM_RET FM_CPC_DelRSAKeypair
(
   FM_I     FM_HANDLE          hDev,
   FM_I     FM_HKEY            hKey
)
```

功能描述

删除密码卡内指定位置的RSA密钥对。需要管理员权限。

参数描述

hDev[in]　　设备句柄

hKey[in]　　密钥句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.3 FM_CPC_ImportRSAKeypair

函数定义

```
FM_RET FM_CPC_ImportRSAKeypair
(
   FM_I     FM_HANDLE          hDev,
   FM_B     FM_HKEY            *phKey,
   FM_I     FM_RSA_PublicKey   *pPubkey,
   FM_I     FM_RSA_PrivateKey  *pPrikey
```

)

功能描述

导入RSA密钥对到密码卡内指定的存储位置。需要管理员权限。

参数描述

hDev[in]	设备句柄
phKey[inout]	密钥句柄指针，有效取值如下： FM_HKEY_BYDEV_PERM：导入的密钥对永久地存储在卡内，密钥存储位置由密码卡自动查找； 0~63（767）：导入的密钥对永久性地存储在卡内，密钥存储位置由用户指定
pPubkey[in]	RSA公钥部分的数据
pPrikey[in]	RSA私钥部分的数据

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.4 FM_CPC_ExportRSAKeypair

函数定义

```
FM_RET FM_CPC_ExportRSAKeypair
(
  FM_I   FM_HANDLE          hDev,
  FM_I   FM_HKEY            hKey,
  FM_O   FM_RSA_PublicKey   *pPubkey,
  FM_O   FM_RSA_PrivateKey  *pPrikey
)
```

功能描述

导出密码卡内指定位置的RSA密钥对。如果导出私钥，需要管理员权限；如果只导出公钥，需要操作员权限。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄
pPubkey[out]	不为NULL时返回RSA公钥部分
pPrikey[out]	不为NULL时返回RSA私钥部分

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.5 FM_CPC_RSAEncrypt

函数定义

```
FM_RET FM_CPC_RSAEncrypt
(
   FM_I     FM_HANDLE          hDev,
   FM_I     FM_HKEY            hKey,
   FM_I     FM_U8              *pu8InBuf,
   FM_I     FM_U32             u32InLen,
   FM_O     FM_U8              *pu8OutBuf,
   FM_O     FM_U32             *pu32OutLen,
   FM_I     FM_RSA_PublicKey   *pPubkey
)
```

功能描述

使用指定的RSA密钥对的公钥部分对输入数据进行加密。要加密的数据存储格式应为大字节序。需要操作员权限。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pPubkey指定的外部公钥 0~63（767）：使用指定存储位置的卡内密钥
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度，有效取值如下： 密钥模长为1024时，应为128； 密钥模厂为2048时，应为256
pu8OutBuf[out]	输出数据
pu32OutLen[out]	输出数据的字节长度
pPubkey[in]	密钥句柄为FM_HKEY_FROM_HOST时，传入RSA公钥数据

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.6 FM_CPC_RSADecrypt

函数定义

```
FM_RET FM_CPC_RSADecrypt
(
   FM_I     FM_HANDLE          hDev,
```

```
    FM_I    FM_HKEY              hKey,
    FM_I    FM_U8                *pu8InBuf,
    FM_I    FM_U32               u32InLen,
    FM_O    FM_U8                *pu8OutBuf,
    FM_O    FM_U32               *pu32OutLen,
    FM_I    FM_RSA_PrivateKey *pPrikey
)
```

功能描述

使用指定的RSA密钥对的私钥部分对输入数据进行解密。要解密的数据存储格式应为大字节序。需要操作员权限。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pPubkey指定的外部公钥 0~63（767）：使用指定存储位置的卡内密钥
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度，有效取值如下： 密钥模长为1024时，应为128； 密钥模厂为2048时，应为256
pu8OutBuf[out]	输出数据
pu32OutLen[out]	输出数据的字节长度
pPrikey [in]	密钥句柄为FM_HKEY_FROM_HOST时，传入RSA私钥数据

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.7 FM_CPC_RSASign

函数定义

```
FM_RET FM_CPC_RSASign
(
    FM_I    FM_HANDLE            hDev,
    FM_I    FM_HKEY              hKey,
    FM_I    FM_U32               u32Alg,
    FM_I    FM_U8                *pu8DataBuf,
    FM_I    FM_U32               u32DataLen,
    FM_O    FM_U8                *pu8SignBuf,
    FM_O    FM_U32               *pu32SignLen,
```

```
    FM_I    FM_RSA_PrivateKey    *pPrikey
)
```

功能描述

使用RSA私钥对输入数据进行RSA签名运算。密钥格式，数据格式均为大字节序。需要操作员权限。

参数描述

hDev[in]	设备句柄
hKey[in]	指定的密钥句柄。hKey的有效值如下： 1)FM_HKEY_FROM_HOST: 使用pPrikey参数传入的私钥； 2)其他则使用密钥句柄指定的设备内部私钥；
u32Alg[in]	杂凑算法标示
pu8DataBuf[in]	缓冲区指针,用于存放输入数据
u32DataLen[in]	输入数据的字节长度，必须是密钥模长的整数倍
pu8SignBuf[out]	缓冲区指针,用于存放输出数据
pu32SignLen[out]	缓冲区指针,用于存放输出数据的字节长度
pPrikey[in]	密钥句柄为FM_HKEY_FROM_HOST时传入RSA私钥结构数据。

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.8 FM_CPC_RSAVerify

函数定义

```
FM_RET FM_CPC_RSAVerify
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_HKEY             hKey,
    FM_I    FM_U32              u32Alg,
    FM_I    FM_U8               *pu8DataBuf,
    FM_I    FM_U32               u32DataLen,
    FM_I    FM_U8                *pu8SignBuf,
    FM_I    FM_U32               u32SignLen,
    FM_I    FM_RSA_PublicKey     *pPubkey
)
```

功能描述

使用RSA公钥对输入数据进行RSA签名验证运算。 密钥格式，数据格式均为大字节序。需要操作员权限。

参数描述

hDev[in]　　设备句柄

hKey[in]　　指定的密钥句柄。hKey的有效值如下:

1)FM_HKEY_FROM_HOST: 使用pPubkey参数传入的公钥

2)其他则使用密钥句柄指定的设备内部公钥

u32Alg[in]　　杂凑算法标示

pu8DataBuf[in]　缓冲区指针,用于存放输入数据

u32DataLen[in]　输入数据的字节长度，必须是密钥模长的整数倍

pu8SignBuf[in]　缓冲区指针,用于存放签名数据

u32SignLen[in]　缓冲区指针,用于存放签名数据的字节长度

pPubkey[in]　　密钥句柄为FM_HKEY_FROM_HOST时传入RSA公钥结构数据。

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.9　FM_CPC_GenECCKeypair

函数定义

```
FM_RET FM_CPC_GenECCKeypair
(
   FM_I    FM_HANDLE          hDev,
   FM_I    FM_U32             u32Alg,
   FM_B    FM_HKEY            *phKey,
   FM_O    FM_ECC_PublicKey   *pPubkey,
   FM_O    FM_ECC_PrivateKey  *pPrikey
)
```

功能描述

产生指定类型的ECC密钥对，存储在卡内或通过参数导出。密钥结构中的各个参数均按大字节序存储。当密钥句柄为FM_HKEY_TO_HOST时，通过参数导出生产的密钥对需要操作员权限；当密钥句柄不为FM_HKEY_TO_HOST时，通过参数导出生产的密钥对需要管理员权限。卡内默认可存储256对ECC密钥。

参数描述

hDev[in]　　设备句柄

u32Alg [in]　　算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）

phKey[inout]　　密钥句柄指针，有效取值如下：

FM_HKEY_TO_HOST：生成的密钥对由参数导出；

FM_HKEY_BYDEV_PERM：生成的密钥对永久地存储在卡内，密钥存储位置由密码卡自动查找；

0~1023：生成的密钥对永久性地存储在卡内，密钥存储位置由用户指定

pPubkey[out]　不为NULL时返回生成的ECC公钥部分

pPrikey[out]　不为NULL时返回生成的ECC私钥部分

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.10 FM_CPC_DelECCKeypair

函数定义

```
FM_RET FM_CPC_DelECCKeypair
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_HKEY         hKey
)
```

功能描述

删除密码卡内指定位置的ECC密钥对。需要管理员权限。

参数描述

hDev[in]　设备句柄

hKey[in]　密钥句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.11 FM_CPC_ImportECCKeypair

函数定义

```
FM_RET FM_CPC_ImportRSAKeypair
(
    FM_I    FM_HANDLE           hDev,
    FM_B    FM_HKEY             *phKey,
    FM_I    FM_ECC_PublicKey    *pPubkey,
    FM_I    FM_ECC_PrivateKey   *pPrikey
)
```

功能描述

导入ECC密钥对到密码卡内指定的存储位置。需要管理员权限。

参数描述

hDev[in]　设备句柄

phKey[inout]　密钥句柄指针，有效取值如下：

FM_HKEY_BYDEV_PERM：导入的密钥对永久地存储在卡内，密钥存储位

置由密码卡自动查找；

0~1023：导入的密钥对永久性地存储在卡内，密钥存储位置由用户指定

pPubkey[in] ECC公钥部分的数据

pPrikey[in] ECC私钥部分的数据

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.12 FM_CPC_ExportECCKeypair

函数定义

```
FM_RET FM_CPC_ExportECCKeypair
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_HKEY             hKey,
    FM_O    FM_ECC_PublicKey    *pPubkey,
    FM_O    FM_ECC_PrivateKey   *pPrikey
)
```

功能描述

导出密码卡内指定位置的ECC密钥对。如果导出私钥，需要管理员权限；如果只导出公钥，需要操作员权限。

参数描述

hDev[in] 设备句柄

hKey[in] 密钥句柄

pPubkey[out] 不为NULL时返回ECC公钥部分

pPrikey[out] 不为NULL时返回ECC私钥部分

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.13 FM_CPC_ECCEncrypt

函数定义

```
FM_RET FM_CPC_ECCEncrypt
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_HKEY         hKey,
    FM_I    FM_U8           *pu8InBuf,
    FM_I    FM_U32          u32InLen,
```

```
    FM_I    FM_ECC_PublicKey  *pPubkey,
    FM_O    FM_ECC_Cipher     *pECCCipher
)
```

功能描述

使用指定的ECC密钥对的公钥部分对输入数据进行加密。要加密的数据存储格式应为大字节序。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pPubkey指定的外部公钥 0~1023：使用指定存储位置的卡内密钥
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度，有效取值如下： PCI 1.2系列密码卡目前只支持32字节 其他型号的密码卡最大支持136字节
pPubkey[in]	密钥句柄为FM_HKEY_FROM_HOST时，传入ECC公钥数据
pECCCipher[out]	输出密文结构

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.14 FM_CPC_ECCDecrypt

函数定义

```
FM_RET FM_CPC_ECCDecrypt
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32Alg,
    FM_I    FM_HKEY             hKey,
    FM_I    FM_ECC_Cipher       *pECCCipher,
    FM_I    FM_ECC_PrivateKey   *pPrikey
    FM_O    FM_U8               *pu8OutBuf,
    FM_O    FM_U32              *pu32OutLen
)
```

功能描述

使用指定的ECC密钥对的私钥部分对输入数据进行解密。要解密的数据存储格式应为大字节序。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pPrikey指定的外部私钥 0~1023：使用指定存储位置的卡内密钥
pECCCipher [in]	ECC密文结构
pPrikey[in]	密钥句柄为FM_HKEY_FROM_HOST时，传入ECC私钥数据
pu8OutBuf[out]	输出数据
pu32OutLen[out]	输出数据字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.15 FM_CPC_ECCSign

函数定义

```
FM_RET FM_CPC_ECCSign
(
   FM_I    FM_HANDLE          hDev,
   FM_I    FM_U32             u32Alg,
   FM_I    FM_HKEY            hKey,
   FM_I    FM_U8              *pu8InBuf,
   FM_I    FM_U32             u32InLen,
   FM_I    FM_ECC_PrivateKey  *pPrikey,
   FM_O    FM_ECC_Signature   *pSignature
)
```

功能描述

使用指定的ECC密钥对的私钥部分对输入数据进行签名。要签名的数据存储格式应为大字节序。签名之前需对数据进行摘要。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pPrikey指定的外部私钥 0~1023：使用指定存储位置的卡内密钥
pu8InBuf[in]	输入数据，应为摘要后的结果

u32InLen[in]　　输入数据的字节长度，最大支持32字节

pPrikey[in]　　密钥句柄为FM_HKEY_FROM_HOST时，传入ECC私钥数据

pSignature[out]　　输出ECC签名结果数据结构

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.16 FM_CPC_ECCVerify

函数定义

```
FM_RET FM_CPC_ECCVerify
(
    FM_I    FM_HANDLE          hDev,
    FM_I    FM_U32             u32Alg,
    FM_I    FM_HKEY            hKey,
    FM_I    FM_ECC_PublicKey   *pPubkey,
    FM_I    FM_U8              *pu8InBuf,
    FM_I    FM_U32             u32InLen,
    FM_I    FM_ECC_Signature   *pSignature
)
```

功能描述

使用指定的ECC密钥对的公钥部分对输入的签名值进行校验。所有输入的数据存储格式应为大字节序。需要操作员权限。

参数描述

hDev[in]　　设备句柄

u32Alg[in]　　算法标识，指定使用的ECC算法

hKey[in]　　密钥句柄，有效取值如下：

FM_HKEY_FROM_HOST： 使用由参数pPrikey指定的外部私钥

0~1023：使用指定存储位置的卡内密钥

pPubkey[in]　　密钥句柄为FM_HKEY_FROM_HOST时，传入ECC公钥数据

pu8InBuf[in]　　输入数据，应为摘要后的结果

u32InLen[in]　　输入数据的字节长度，最大支持32字节

pSignature[in]　　输入ECC签名结果数据结构

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.17 FM_CPC_GenerateAgreementDataWithECC

函数定义

```
FM_RET FM_CPC_GenerateAgreementDataWithECC
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32Alg,
    FM_I    FM_HKEY             hKey,
    FM_I    FM_U32              u32AgreementKeyLen,
    FM_I    FM_U8               *pu8SponsorID,
    FM_I    FM_U32              u32SponsorIDLen,
    FM_O    FM_ECC_PublicKey    *pSponsorPubKey,
    FM_O    FM_ECC_PublicKey    *pSponsorTmpPubKey,
    FM_O    FM_HANDLE           *phAgreementHandle
)
```

功能描述

密钥协商第一步，由发起方调用。发起方调用此函数来设置发起方ID及生成发起方临时公钥。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
hKey[in]	密钥句柄，指定之前已存储在卡内的一对ECC密钥（0~255）
u32AgreementKeyLen [in]	要协商密钥的字节长度
pu8SponsorID[in]	发起方ID
u32SponsorIDLen[in]	发起方ID字节长度
pSponsorPubKey[out]	返回发起方ECC公钥
pSponsorTmpPubKey[out]	返回发起方临时ECC公钥
phAgreementHandle[out]	暂未用到，设为NULL

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.18 FM_CPC_GenerateAgreementDataAndKeyWithECC

函数定义

```
FM_RET FM_CPC_GenerateAgreementDataAndKeyWithECC
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32Alg,
    FM_I    FM_HKEY             hKey,
```

```
    FM_I    FM_U32              u32AgreementKeyLen,
    FM_I    FM_U8               *pu8ResponseID,
    FM_I    FM_U32              u32ResponseIDLen,
    FM_I    FM_U8               *pu8SponsorID,
    FM_I    FM_U32              u32SponsorIDLen,
    FM_I    FM_ECC_PublicKey    *pSponsorPubKey,
    FM_I    FM_ECC_PublicKey    *pSponsorTmpPubKey,
    FM_O    FM_ECC_PublicKey    *pResponsePubKey,
    FM_O    FM_ECC_PublicKey    *pResponseTmpPubKey,
    FM_O    FM_HKEY             *phKeyHandle
)
```

功能描述

密钥协商第二步，由响应方调用。响应方调用此函数来设置响应方ID、生成响应方协商密钥及返回响应方临时公钥。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
hKey[in]	密钥句柄，指定之前已存储在卡内的一对ECC密钥（0~255）
u32AgreementKeyLen [in]	要协商密钥的字节长度
pu8ResponseID[in]	响应方ID
u32ResponseIDLen[in]	响应方ID字节长度
pu8SponsorID[in]	发起方ID
u32SponsorIDLen[in]	发起方ID字节长度
pSponsorPubKey[in]	发起方ECC公钥
pSponsorTmpPubKey[in]	发起方临时ECC公钥
pResponsePubKey[out]	返回响应方ECC公钥
pResponseTmpPubKey[out]	返回响应方临时ECC公钥
phKeyHandle[out]	生成的响应方协商密钥的句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.2.19 FM_CPC_GenerateKeyWithECC

函数定义

```
FM_RET FM_CPC_GenerateKeyWithECC
(
    FM_I    FM_HANDLE           hDev,
```

```
    FM_I    FM_U32              u32Alg,
    FM_I    FM_U8               *pu8ResponseID,
    FM_I    FM_U32              u32ResponseIDLen,
    FM_I    FM_ECC_PublicKey    * pResponsePubKey,
    FM_I    FM_ECC_PublicKey    *pResponseTmpPubKey,
    FM_I    FM_HANDLE           *phAgreementHandle,
    FM_O    FM_HKEY             *phKeyHandle
)
```

功能描述

密钥协商第三步，由发起方调用。发起方调用此函数来生成协商密钥。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，目前暂时只支持SM2算法（FM_ALG_SM2_1）
pu8ResponseID[in]	响应方ID
u32ResponseIDLen[in]	响应方ID长度
pResponsePubKey[in]	响应方ECC公钥
pResponseTmpPubKey[in]	响应方临时ECC公钥
phAgreementHandle	暂未用到，设为NULL
phKeyHandle[out]	生成的发起方协商密钥的句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3 对称算法接口

4.3.1 FM_CPC_GenKey

函数定义

```
FM_RET FM_CPC_GenKey
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_U32          u32InLen,
    FM_B    FM_HKEY         *phKey,
    FM_O    FM_U8           *pu8Key
)
```

功能描述

产生指定类型的对称密钥，存储在卡内或通过参数导出。需要操作员权限。卡内默认可存储

的对称密钥数量为：永久性存储做多支持1024个，临时性存储最多支持100个。

参数描述

hDev[in]	设备句柄
u32Alg[in]	算法标识，有效取值如下： FM_ALG_SM1：SM1算法； FM_ALG_SM6：SM6算法； FM_ALG_DES：DES算法； FM_ALG_3DES：3DES算法； FM_ALG_AES：AES128算法； FM_ALG_AES192：AES192算法； FM_ALG_AES256：AES256算法； FM_ALG_SM4：SM4算法
u32InLen[in]	密钥数据字节长度，最大支持32字节
phKey[inout]	密钥句柄指针，有效取值如下： FM_HKEY_TO_HOST：生成的密钥对由参数导出； FM_HKEY_BYDEV_PERM：生成的密钥永久地存储在卡内，密钥存储位置由密码卡自动查找； FM_HKEY_BYDEV_TEMP：生成的密钥对临时地存储在卡内，密钥存储位置由密码卡自动查找； 0~1023：生成的密钥对永久性地存储在卡内，位置由用户指定
pu8Key [out]	不为NULL时返回生成的对称密钥

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3.2 FM_CPC_DelKey

函数定义

```
FM_RET FM_CPC_DelKey
(
   FM_I     FM_HANDLE        hDev,
   FM_I     FM_HKEY          hKey
)
```

功能描述

删除密码卡内指定位置的对称密钥。需要操作员权限。

参数描述

hDev[in]	设备句柄

hKey[in]　密钥句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3.3 FM_CPC_ImportKey

函数定义

```
FM_RET FM_CPC_ImportKey
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_U8           *pu8Key,
    FM_I    FM_U32          u32KeyLen,
    FM_B    FM_HKEY         *phKey
)
```

功能描述

导入对称密钥到设备内部并存储。需要操作员权限。

参数描述

hDev[in]　设备句柄

u32Alg[in]　算法标识，有效取值如下：

FM_ALG_SM1：SM1算法；

FM_ALG_SM6：SM6算法；

FM_ALG_DES：DES算法；

FM_ALG_3DES：3DES算法；

FM_ALG_AES：AES算法；

FM_ALG_AES192：AES192算法；

FM_ALG_AES256：AES256算法；

FM_ALG_SM4：SM4算法

pu8Key[in]　密钥数据

u32KeyLen[in]　密钥数据字节长度，最大支持32字节

phKey[inout]　密钥句柄指针，有效取值如下：

FM_HKEY_BYDEV_PERM：生成的密钥永久地存储在卡内，密钥存储位置由密码卡自动查找；

FM_HKEY_BYDEV_TEMP：生成的密钥对临时地存储在卡内，密钥存储位置由密码卡自动查找；

0~1023：生成的密钥对永久性地存储在卡内，位置由用户指定

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3.4 FM_CPC_ExportKey

函数定义

```
FM_RET FM_CPC_ExportKey
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_HKEY         hKey,
    FM_O    FM_U8           *pu8Key,
    FM_B    FM_U32          *pu32Len
)
```

功能描述

导出密码卡内指定位置的对称密钥。需要操作员权限。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄
pu8Key[out]	密钥数据
pu32Len[inout]	入参表示密钥数据接收缓冲区的长度 出参表示密钥数据字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3.5 FM_CPC_Encrypt

函数定义

```
FM_RET FM_CPC_Encrypt
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_HKEY         hKey,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_U32          u32WorkMode,
    FM_I    FM_U8           *pu8InBuf,
    FM_I    FM_U32          u32InLen,
    FM_O    FM_U8           *pu8OutBuf,
    FM_O    FM_U32          *pu32OutLen,
    FM_I    FM_U8           *pu8Key,
```

```
    FM_I    FM_U32          u32KeyLen,
    FM_I    FM_U8           *pu8IV,
    FM_I    FM_U32          u32IVLen
)
```

功能描述

使用指定的密钥句柄和IV，以及指定的对称密钥分组加密算法和工作方式对输入数据进行对称加密运算。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pu8Key指定的外部密钥 0~1023：使用永久性存储在卡内指定位置的密钥 0~99，并置最高位为1：使用临时存储在卡内指定位置的密钥
u32Alg[in]	算法标识，有效取值如下： FM_ALG_SM1：SM1算法； FM_ALG_SM6：SM6算法； FM_ALG_DES：DES算法； FM_ALG_3DES：3DES算法； FM_ALG_AES：AES算法； FM_ALG_AES192：AES192算法； FM_ALG_AES256：AES256算法； FM_ALG_SM4：SM4算法
u32WorkMode[in]	运算模式，可取的值为：FM_ALGMODE_EBC或FM_ALGMODE_CBC
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度，必须是分组长度的整数倍
pu8OutBuf[out]	输出数据
pu32OutLen[out]	输出数据的字节长度
pu8Key[in]	密钥数据
u32KeyLen[in]	密钥数据的字节长度
pu8IV[in]	IV数据
u32IVLen[in]	IV数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.3.6 FM_CPC_Decrypt

函数定义

```
FM_RET FM_CPC_Decrypt
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_HKEY         hKey,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_U32          u32WorkMode,
    FM_I    FM_U8           *pu8InBuf,
    FM_I    FM_U32          u32InLen,
    FM_O    FM_U8           *pu8OutBuf,
    FM_O    FM_U32          *pu32OutLen,
    FM_I    FM_U8           *pu8Key,
    FM_I    FM_U32          u32KeyLen,
    FM_I    FM_U8           *pu8IV,
    FM_I    FM_U32          u32IVLen
)
```

功能描述

使用指定的密钥句柄和IV，以及指定的对称密钥分组解密算法和工作方式对输入数据进行对称解密运算。

参数描述

hDev[in]	设备句柄
hKey[in]	密钥句柄，有效取值如下： FM_HKEY_FROM_HOST： 使用由参数pu8Key指定的外部密钥 0~1023：使用永久性存储在卡内指定位置的密钥 0~99，并置最高位为1：使用临时存储在卡内指定位置的密钥
u32Alg[in]	算法标识，有效取值如下： FM_ALG_SM1：SM1算法； FM_ALG_SM6：SM6算法； FM_ALG_DES：DES算法； FM_ALG_3DES：3DES算法； FM_ALG_AES：AES算法； FM_ALG_AES192：AES192算法； FM_ALG_AES256：AES256算法； FM_ALG_SM4：SM4算法
u32WorkMode[in]	运算模式，可取的值为：FM_ALGMODE_EBC或FM_ALGMODE_CBC
pu8InBuf[in]	输入数据

u32InLen[in]　　输入数据的字节长度，必须是分组长度的整数倍

pu8OutBuf[out]　输出数据

pu32OutLen[out]　输出数据的字节长度

pu8Key[in]　　密钥数据

u32KeyLen[in]　密钥数据的字节长度

pu8IV[in]　　IV数据

u32IVLen[in]　IV数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4　杂凑算法接口

4.4.1　FM_CPC_HashInit

函数定义

```
FM_RET FM_CPC_HashInit
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Alg
)
```

功能描述

摘要运算第一步，运算参数初始化。

参数描述

hDev[in]　　设备句柄

u32Alg[in]　　目前暂时只支持SHA1算法（FM_ALG_SHA1）

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4.2　FM_CPC_HashUpdate

函数定义

```
FM_RET FM_CPC_HashUpdate
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Alg,
    FM_I    FM_U8           *pu8InBuf,
    FM_I    FM_U32          u32InLen
)
```

功能描述

摘要运算第二步，输入数据。

参数描述

hDev[in]	设备句柄
u32Alg[in]	目前暂时只支持SHA1算法（FM_ALG_SHA1）
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4.3 FM_CPC_HashFinal

函数定义

```
FM_RET FM_CPC_HashFinal
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32Alg,
    FM_O    FM_U8               *pu8HashBuf,
    FM_O    FM_U32              *pu32HashLen
)
```

功能描述

摘要运算第三步，获取运算结果。

参数描述

hDev[in]	设备句柄
u32Alg[in]	目前暂时只支持SHA1算法（FM_ALG_SHA1）
pu8HashBuf[out]	输出数据
pu32HashLen[out]	输出数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4.4 FM_CPC_SM3Init

函数定义

```
FM_RET FM_CPC_SM3Init
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_ECC_PublicKey    *pPubkey,
    FM_I    FM_U8               *pu8ID,
```

FM_I FM_U32 u32IDLen

)

功能描述

SM3摘要运算第一步，运算参数初始化。

参数描述

hDev[in]	设备句柄
pPubkey[in]	签名者的ECC公钥，在与ECC算法配合使用时，产生用于ECC签名的杂凑值时有效，其它情形下填NULL即可
pu8ID[in]	签名者的ID值，在与ECC算法配合使用时，产生用于ECC签名的杂凑值时有效，其它情形下填NULL即可
u32IDLen[in]	签名者ID的字节长度，最大支持64字节

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4.5 FM_CPC_SM3Update

函数定义

FM_RET FM_CPC_SM3Update

(

FM_I FM_HANDLE hDev,

FM_I FM_U8 *pu8InBuf,

FM_I FM_U32 u32InLen

)

功能描述

SM3摘要运算第二步，输入数据。

参数描述

hDev[in]	设备句柄
pu8InBuf[in]	输入数据
u32InLen[in]	输入数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.4.6 FM_CPC_SM3Final

函数定义

FM_RET FM_CPC_SM3Final

(

```
    FM_I    FM_HANDLE       hDev,
    FM_O    FM_U8           *pu8HashBuf,
    FM_O    FM_U32          *pu32HashLen
)
```

功能描述

摘要运算第三步，获取运算结果。

参数描述

hDev[in]	设备句柄
pu8HashBuf[out]	输出数据
pu32HashLen[out]	输出数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5 用户管理接口

4.5.1 FM_CPC_USER_Login

函数定义

```
FM_RET FM_CPC_USER_Login
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Type,
    FM_I    FM_U8           *pu8PinBuf,
    FM_I    FM_U32          u32PinLen,
    FM_O    FM_HUSER        *phUser,
    FM_O    FM_U32          *pu32RetryNum
)
```

功能描述

执行用户身份认证及登录。必须将用于身份认证的USB智能密码钥匙插在密码卡上，之后再调用此接口。注：MINI PCIE1.0密码卡不需要使用USB智能密码钥匙。

参数描述

hDev[in]	设备句柄
u32Type[in]	暂未用到，设为0
pu8PinBuf[in]	用户PIN码
u32PinLen[in]	用户PIN码的字节长度
phUser[out]	不为NULL时，返回已打开的用户句柄
pu32RetryNum[out]	当PIN码错误时，如果本参数不为NULL，将返回剩余的重试次数

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.2 FM_CPC_USER_Logout

函数定义

```
FM_RET FM_CPC_USER_Logout
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_HUSER        hUser
)
```

功能描述

注销指定的用户。

参数描述

hDev[in]	设备句柄
hUser[in]	用户句柄，有效取值如下： FM_HANDLE_INVALID：注销所有已登录的用户； 某个用户句柄：注销指定的用户

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.3 FM_CPC_USER_ChangePin

函数定义

```
FM_RET FM_CPC_USER_ChangePin
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_U32          u32Flag,
    FM_I    FM_U8           *pu8OldPinBuf,
    FM_I    FM_U32          u32OldPinLen,
    FM_I    FM_U8           *pu8NewPinBuf,
    FM_I    FM_U32          u32NewPinLen,
    FM_O    FM_U32          *pu32RetryNum
)
```

功能描述

修改用户PIN码。必须将用于身份认证的USB智能密码钥匙插在密码卡上，之后再调用此接口。注：MINI PCIE1.0密码卡不需要使用USB智能密码钥匙。

参数描述

hDev[in]	设备句柄
u32Flag[in]	操作标志，有效取值如下： FM_PIN_CHANGEOPER：修改用户PIN码 FM_PIN_CHANGEADMIN：修改USB智能密码钥匙超级用户PIN码 FM_PIN_UNBLOCKOPER：解锁用户PIN码
pu8OldPinBuf[in]	配合u32Flag一起使用，当u32Flag为FM_PIN_CHANGEOPER时，此参数为用户的旧PIN码；当u32Flag为FM_PIN_CHANGEADMIN时，此参数为USB智能密码钥匙超级用户的旧PIN码；当u32Flag为FM_PIN_UNBLOCKOPER时，此参数为USB智能密码钥匙的超级用户PIN码。
u32OldPinLen[in]	PIN码的字节长度，有效长度范围：6~16个字符
pu8NewPinBuf[in]	新PIN码
u32NewPinLen[in]	新PIN码的字节长度，有效长度范围：6~16个字符

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.4 FM_CPC_USER_GetInfo

函数定义

```
FM_RET FM_CPC_USER_GetInfo
(
  FM_I   FM_HANDLE          hDev,
  FM_O   CPC_USER_INFO      *pUserInfo
)
```

功能描述

获取密码卡内所有用户的详细信息，详细信息包括：对应的USB智能密码钥匙的序列号、用户角色以及登录状态等。注：MINI PCIE1.0密码卡不支持该接口。

参数描述

hDev[in]	设备句柄
aUserInfo[out]	用户信息结构体数组

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.5 FM_CPC_USER_UserMng

函数定义

```
FM_RET FM_CPC_USER_UserMng
```

(

FM_I FM_HANDLE hDev,

FM_I FM_U32 u32Flag,

FM_I FM_U8 *pu8Buf,

FM_I FM_U32 u32Len

)

功能描述

用户管理：添加或删除用户。必须将用于身份认证的USB智能密码钥匙插在密码卡上，之后再调用此接口。需要管理员权限。注：MINI PCIE1.0密码卡不支持该接口。

参数描述

hDev[in]	设备句柄
u32Flag[in]	操作标志，有效取值如下： CPC_USER_ADDADMIN：添加管理 CPC_USER_ADDOPER： 添加操作员 CPC_USER_DELADMIN：删除管理员 CPC_USER_DELOPER： 删除操作员
pu8Buf[in]	添加用户时传入用户PIN码 删除用户时传入相应USB智能密码钥匙的序列号
u32Len[in]	用户PIN码或序列号的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.6 FM_CPC_USER_BackupMng

函数定义

FM_RET FM_CPC_USER_BackupMng

(

FM_I FM_HANDLE hDev,

FM_I FM_U32 u32Flag,

FM_I CPC_BK_CONFIG *pstBkConfig,

FM_O FM_U32 *pu32UserAllNum,

FM_O FM_U32 *pu32UserDealNum

)

功能描述

密钥备份与恢复。需要管理员权限。注：MINI PCIE1.0密码卡不支持该接口。

参数描述

hDev[in]	设备句柄

u32Flag[in]	操作标志，有效取值如下：
	CPC_USER_BAK ：备份
	CPC_USER_RES：恢复
	CPC_USER_BAKINIT：备份初始化
	CPC_USER_RESINIT：恢复初始化
pstBkConfig[in]	备份配置信息（具体设置方法可咨询我公司技术人员）
pu32UserAllNum [out]	一共需要备份的次数
pu32UserDealNum[out]	当前已备份次数

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.7 FM_CPC_SetAuth

函数定义

```
FM_RET FM_CPC_SetAuth
(
   FM_I    FM_HANDLE   hDev,
   FM_I    FM_U32      u32Flag,
)
```

功能描述

保留操作员权限。当密码卡内存在操作员时，设置是否自动保留操作员权限，从而下次密码卡上电时可自动获取操作员权限。注：MINI PCIE1.0密码卡不支持该接口。

参数描述

hDev[in]	设备句柄
u32Flag[in]	操作标志，有效取值如下：

0：取消保留操作员权限。

1：保留操作员权限。

返回值

FME_OK，成功。其他，返回相应的错误码。

4.5.8 FM_CPC_GetAuth

函数定义

```
FM_RET FM_CPC_GetAuth
(
   FM_I    FM_HANDLE   hDev,
   FM_O    FM_U32      *pu32Flag,
```

)

功能描述

获取操作员权限状态。注：MINI PCIE1.0密码卡不支持该接口。

参数描述

hDev[in]	设备句柄
*pu32Flag[in]	操作标志，有效取值如下：

0：保留操作员权限功能未开启。

1：保留操作员权限功能已开启。

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6 文件系统接口

4.6.1 FM_CPC_FILE_Init

函数定义

```
FM_RET FM_CPC_FILE_Init
(
    FM_I    FM_HANDLE           hDev
)
```

功能描述

初始化密码卡文件系统。密码卡的文件系统大小为64K字节，其文件路径必须以"\"进行分割，目录和文件名都必须为字母、数字的组合。系统根目录为"\root"，所有创建的目录和文件必须在此路径下。注意：本函数会进行文件系统格式化，所有文件数据均会丢失，请谨慎使用。需要管理员权限。

参数描述

hDev[in]	设备句柄

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.2 FM_CPC_FILE_CreateDir

函数定义

```
FM_RET FM_CPC_FILE_CreateDir
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_S8               *ps8FullDir,
```

```
    FM_I    FM_U32          u32AccCond
)
```

功能描述

根据指定的路径创建目录。注意，本函数不支持递归创建，新目录之前的路径必须是已经存在的。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8FullDir[in]	路径名称，须包含要创建的目录。例如：当路径名为"\root\abc\123"时则表示在"\root\abc"目录下创建新目录"123"
u32AccCond[in]	暂未用到，设为0

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.3 FM_CPC_FILE_DeleteDir

函数定义

```
FM_RET FM_CPC_FILE_DeleteDir
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8FullDir
)
```

功能描述

删除指定的目录。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8FullDir[in]	路径名称，包含要删除的目录

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.4 FM_CPC_FILE_CreateFile

函数定义

```
FM_RET FM_CPC_FILE_CreateFile
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_I    FM_S8           *ps8FileName,
    FM_I    FM_U32          u32FileSize,
```

FM_I FM_U32 u32AccCond

)

功能描述

创建文件。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8DirName[in]	路径名称
ps8FileName[in]	文件名，长度不超过4字节
u32FileSize[in]	文件大小
u32AccCond[in]	暂未用到，设为0

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.5 FM_CPC_FILE_ReadFile

函数定义

```
FM_RET FM_CPC_FILE_ReadFile
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_I    FM_S8           *ps8FileName,
    FM_I    FM_U32          u32Offset,
    FM_I    FM_U32          u32Size,
    FM_O    FM_U8           *pu8Buf
)
```

功能描述

读文件。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8DirName[in]	路径名称
ps8FileName[in]	文件名，长度不超过4字节
u32Offset[in]	读文件的偏移量
u32Size[in]	读文件的大小
pu8Buf[out]	输出数据，必须大于u32Size

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.6 FM_CPC_FILE_WriteFile

函数定义

```
FM_RET FM_CPC_FILE_WriteFile
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_I    FM_S8           *ps8FileName,
    FM_I    FM_U32          u32Offset,
    FM_I    FM_U32          u32Size,
    FM_I    FM_U8           *pu8Buf
)
```

功能描述

写文件。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8DirName[in]	路径名称，长度不超过4字节
ps8FileName[in]	文件名，长度不超过4字节
u32Offset[in]	写文件的偏移量
u32Size[in]	写文件的大小
pu8Buf[in]	输入数据，必须大于u32Size

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.7 FM_CPC_FILE_DeleteFile

函数定义

```
FM_RET FM_CPC_FILE_DeleteFile
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_I    FM_S8           *ps8FileName
)
```

功能描述

删除文件。

需要操作员权限。

参数描述

hDev[in]	设备句柄

ps8DirName[in]　路径名称

ps8FileName[in]　文件名，长度不超过4字节

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.8 FM_CPC_FILE_EnmuDir

函数定义

```
FM_RET FM_CPC_FILE_EnmuDir
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_B    FM_U32          *pu32BufLen,
    FM_O    FM_U8           *pu8Buf,
    FM_O    FM_U32          *pu32DirNum
)
```

功能描述

枚举出指定目录的下的所有子目录。注意：枚举的仅是下一级目录。需要操作员权限。

参数描述

hDev[in]　设备句柄

ps8DirName[in]　路径名称

pu32BufLen[in out]　输入时用于指定结果缓冲区的长度；
输出时用于返回结果缓冲区中数据的实际字节长度或当结果缓冲区为NULL时，返回存储结果数据所需的字节长度

pu8Buf[out]　存放枚举结果的缓冲区，字符串以NULL分割

pu32DirNum[out]　不为NULL时返回枚举到的目录的数目

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.9 FM_CPC_FILE_EnmuFile

函数定义

```
FM_RET FM_CPC_FILE_EnmuFile
(
    FM_I    FM_HANDLE       hDev,
    FM_I    FM_S8           *ps8DirName,
    FM_B    FM_U32          *pu32BufLen,
    FM_O    FM_U8           *pu8Buf,
```

```
    FM_O    FM_U32              *pu32FileNum
)
```

功能描述

枚举出指定目录的下的所有文件。注意：枚举的仅是下一级文件。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8DirName[in]	路径名称
pu32BufLen[in out]	输入时用于指定结果缓冲区的长度； 输出时用于返回结果缓冲区中数据的实际字节长度或当结果缓冲区为NULL时，返回存储结果数据所需的字节长度
pu8Buf[out]	存放枚举结果的缓冲区，字符串以NULL分割
pu32FileNum[out]	不为NULL时返回枚举到的文件的数目

返回值

FME_OK，成功。其他，返回相应的错误码。

4.6.10 FM_CPC_GetInfo

函数定义

```
FM_RET FM_CPC_GetInfo
(
    FM_I    FM_HANDLE           hDev,
    FM_I    FM_U32              u32Flag,
    FM_I    FM_U32               u32InLen,
    FM_I    FM_U8               *pu8InBuf,
    FM_O    FM_U32              *pu32Len,
    FM_O    FM_U8               *pu8OutBuf
)
```

功能描述

获取设备内部指定信息。

参数描述

hDev[in]	设备句柄
u32Flag[in]	指定获取设备内部何种信息 1)FM_INFO_FILESIZE:获取文件信息 2)FM_INFO_SYMKEY_TEMP:获取临时对称密钥数目 3)FM_INFO_SYMKEY_PERM:获取永久对称密钥数目 4)FM_INFO_ASYMKEY_PERM:获取永久非对称密钥数目

u32InLen[in]	输入缓冲区的长度
pu8InBuf[in]	输入缓冲区指针
pu32Len[inout]	输出缓冲区的长度
pu8OutBuf[out]	输出缓冲区指针

返回值

FME_OK，成功。其他，返回相应的错误码。

4.7 证书管理接口

4.7.1 FM_CPC_ContainerWrite

函数定义

```
FM_RET FM_CPC_ContainerWrite
(
   FM_I FM_HANDLE  hDev,
   FM_I FM_U32   u32Flag,
   FM_I FM_S8    *ps8ContainerName,
   FM_I FM_U8    *pu8Data,
   FM_I FM_U32   u32DataLen
)
```

功能描述

创建密钥包容器，并写入相应的证书或密钥号。本密码卡支持创建4个密钥包容器，每个密钥包容器可存放一个交换证书及相应的交换密钥的密钥句柄以及一个签名证书及相应的签名密钥的密钥句柄。需要操作员权限。

参数描述

hDev[in]	设备句柄
u32Flag[in]	操作标识，有效值如下： FM_RSA_CERT_ENC：创建密钥包容器并写入RSA交换证书 FM_RSA_CERT_SIGN：创建密钥包容器并写入RSA签名证书 FM_RSA_KEYNUM_ENC：创建密钥包容器并写入RSA交换密钥句柄 FM_RSA_KEYNUM_SIGN：创建密钥包容器并写入RSA签名密钥句柄 FM_ECC_CERT_ENC：创建密钥包容器并写入ECC交换证书 FM_ECC_CERT_SIGN：创建密钥包容器并写入ECC签名证书 FM_ECC_KEYNUM_ENC：创建密钥包容器并写入ECC交换密钥句柄 FM_ECC_KEYNUM_SIGN：创建密钥包容器并写入ECC签名密钥句柄 FM_EMPTY_RSA_CONTAINER：创建空的RSA密钥包容器

FM_EMPTY_ECC_CONTAINER：创建空的ECC密钥包容器

ps8ContainerName[in]　密钥包容器名称

pu8Data[in]　输入数据

u32DataLen[in]　输入数据的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.7.2 FM_CPC_ContainerRead

函数定义

```
FM_RET FM_CPC_ContainerRead
(
    FM_I FM_HANDLE     hDev,
    FM_I FM_U32        u32Flag,
    FM_I FM_S8         *ps8ContainerName,
    FM_O FM_U8         *pu8Data,
    FM_B FM_U32        *pu32DataLen
)
```

功能描述

从密钥包容器内读取证书以及对应的密钥号信息。

需要操作员权限。

参数描述

hDev [in]　设备句柄

u32Flag [in]　操作标识，有效值如下：

FM_RSA_CERT_ENC：读RSA交换证书

FM_RSA_CERT_SIGN：读RSA签名证书

FM_RSA_KEYNUM_ENC：读RSA交换密钥句柄

FM_RSA_KEYNUM_SIGN：读RSA签名密钥句柄

FM_ECC_CERT_ENC：读ECC交换证书

FM_ECC_CERT_SIGN：读ECC签名证书

FM_ECC_KEYNUM_ENC：读ECC交换密钥句柄

FM_ECC_KEYNUM_SIGN：读ECC签名密钥句柄

ps8ContainerName [in]　密钥包容器名称

pu8Data [in]　输出数据

pu32DataLen [in out]　输入时为数据缓冲区的字节长度；

输出时为缓冲区中数据的实际字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.7.3 FM_CPC_ContainerDelete

函数定义

```
FM_RET FM_CPC_ContainerDelete
(
    FM_I FM_HANDLE      hDev,
    FM_I FM_S8          *ps8ContainerName
)
```

功能描述

删除指定的密钥包容器。需要操作员权限。

参数描述

hDev [in]	设备句柄
ps8ContainerName [in]	密钥包容器名称

返回值

FME_OK，成功。其他，返回相应的错误码。

4.7.4 FM_CPC_ContainerEnum

函数定义

```
FM_RET FM_CPC_ContainerEnum
(
    FM_I FM_HANDLE      hDev,
    FM_O FM_U8          *pu8ContainerNames,
    FM_B FM_U32         *pu32ContainerNamesLen
)
```

功能描述

枚举当前密码卡内的密钥包容器。需要操作员权限。

参数描述

hDev[in]	设备句柄
pu8ContainerNames [out]	返回的密钥包容器名称串，中间以NULL分割
pu32ContainerNamesLen [in out]	密钥包容器名称串的字节长度

返回值

FME_OK，成功。其他，返回相应的错误码。

4.7.5 FM_CPC_ContainerInfo

函数定义

FM_RET FM_CPC_ContainerInfo

(

FM_I FM_HANDLE hDev,

FM_I FM_S8 *ps8ContainerName,

FM_O FM_U32 *pu32ContainerType

)

功能描述

获取当前密钥包容器的类型（RSA or ECC）。需要操作员权限。

参数描述

hDev[in]	设备句柄
ps8ContainerName [in]	密钥包容器名称
pu32ContainerType [out]	反馈密钥包容器的类型，有效值如下： FM_CONTAINER_TYPE_RSA：RSA密钥包容器 FM_CONTAINER_TYPE_ECC：ECC密钥包容器

5 错误码定义

密码卡的错误码定义如下。

5.1 通用错误码

错误名称	错误码	错误码含义
FME_OK	0x000	成功，没有错误
FME_ERR	0x001	错误，通用错误码
FME_POK	0x002	部分正确
FME_UNKNOWN	0x003	未知错误
FME_NOTSUPPORT	0x004	不支持，功能或算法不支持
FME_PARA	0x005	参数错误
FME_NORIGHT	0x006	权限错误
FME_BUSY	0x007	设备忙
FME_TIMEOUT	0x008	操作超时
FME_NOMEM	0x009	内存不足
FME_NORES	0x00a	资源不足
FME_COMMERR	0X00b	通讯错误

FME_ACCESSREG	0x00c	寄存器存取错误
FME_STACKOVER	0x00d	堆栈溢出
FME_DEVINUSE	0x00e	设备正在被使用
FME_SESEXCEED	0x00f	打开会话数目超出限制
FME_DMAREADERR	0x010	DMA读错误
FME_DMAWRITEERR	0x011	DMA写错误
FME_CREATESYNCERR	0x012	创建同步对象错误
FME_GETSYNCERR	0x013	获取同步对象错误
FME_RELEASESYNCERR	0x014	释放同步对象错误
FME_DATALENERR	0x015	数据长度错误
FME_KEYLENERR	0x016	密钥长度错误或不支持

5.2 密码卡自检错误码

错误名称	错误码	错误码含义
FME_AT_OK	0x080	自检正常
FME_AT_USB	0X081	USB检测失败
FME_AT_RANDOM	0X082	随机数检测失败
FME_AT_SM1	0X083	sm1/scb2算法检测失败
FME_AT_PROGCHECK	0X084	程序完整性检测失败
FME_AT_STARTING	0X085	设备正在启动

5.3 算法通用错误码

错误名称	错误码	错误码含义
FME_KEYNOTEXIST	0x0a0	密钥不存在
FME_KEYNOFREE	0x0a1	没有空闲的密钥句柄
FME_KEYEXCEED	0x0a2	密钥句柄超出限制
FME_STEPERR	0x0a3	多步运算算法步骤出错

5.4 对称算法错误码

错误名称	错误码	错误码含义
FME_IVLENERR	0x100	CBC模式运算时IV长度错误

5.5 非对称算法错误码

错误名称	错误码	错误码含义
FME_ECC_NOTINIT	0x180	ECC算法曲线参数未初始化
FME_ECC_PUBKEYERR	0x181	ECC公钥数据错误
FME_ECC_PRIKEYERR	0x182	ECC私钥数据错误
FME_ECC_SIGNERR	0x183	ECC签名运算出错
FME_ECC_VERIFYERR	0x184	ECC验证运算出错
FME_ECC_ENCRYPTERR	0x185	ECC加密运算出错
FME_ECC_DECRYPTERR	0x186	ECC解密运算出错

5.6 杂凑算法错误码

错误名称	错误码	错误码含义
FME_SM3_IDLENERR	0x200	用户ID长度错误

5.7 文件系统错误码

错误名称	错误码	错误码含义
FME_FILE_NOTINIT	0x240	文件系统没有初始化
FME_FILE_DIRDEPTH	0x241	文件目录嵌套过深
FME_FILE_DIRNOTEXIST	0x242	目录不存在
FME_FILE_FILENOTEXIST	0x243	文件不存在
FME_FILE_DIREXIST	0x244	目录已存在
FME_FILE_FILEEXIST	0x245	文件已存在
FME_FILE_DIRNUMEXCEED	0x246	目录数超出限制
FME_FILE_FILENUMEXCEED	0x247	文件数超出限制
FME_FILE_NOSPACE	0x248	文件空间不足
FME_FILE_OPRANGE	0x249	文件操作超出限制
FME_FLASH_TIMEOUT	0x260	flash操作超时
FME_FLASH_WRITEERR	0x261	flash写错误
FME_FLASH_READERR	0x262	flash读错误
FME_FLASH_OPRANGE	0x263	flash读写超出限制
FME_EE_TIMEOUT	0x264	eeprom操作超时

FME_EE_WRITEERR	0x265	eeprom写错误
FME_EE_READERR	0x266	eeprom读错误
FME_EE_OPRANGE	0x267	eeprom读写超出限制

5.8 用户管理错误码

错误名称	错误码	错误码含义
FME_USER_NOTEXIST	0x280	用户不存在
FME_USER_EXIST	0x281	用户已存在
FME_USER_EXCEED	0x282	用户数超出限制
FME_USER_PINERR	0x283	用户PIN码错误
FME_USER_STEPERR	0x284	步骤错误
FME_USER_OPENDEVERR	0x285	打开用户设备错误
FME_USER_GETDEVINFOERR	0x286	获取用户设备信息错误
FME_USER_WRITEDEVERR	0x287	写用户设备存储空间错误
FME_USER_READDEVERR	0x288	读用户设备存储空间错误
FME_USER_NOLOG	0x289	用户没有登录