密钥获取应用接口

（版本 0.1.2）

长沙轨道交通

广东铭鸿数据有限公司

二零一三年八月一日

文档历史

序号	版本	日期	修改人	注释
1	0.1.0	2013.8.1		定义密钥获取应用接口
2	0.1.1	2013.9.13		增加单程票数据获取应用接口
3	0.1.2	2014.2.26		初始化增加密钥版本接口

文档目录

表格目录

1. 范围

本文档定义了用户卡制作的密钥获取应用接口。

2. 引用文档

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的相关引用文件，其随后所有的修改单（不包括堪误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

3. 术语和定义

4. 符号及缩略语

下列符号和缩略语适用于本文档。

IC	集成电路（Integrated Circuit）
MF	主文件（Master File）
ADF	应用定义文件（Application Definition File）
EF	基本文件（Elementary File）
PIN	个人识别码（Personal Identification Number）

5. 接口说明

5.1. 概述

用户卡制卡的密钥获取应用接口采用windows API动态库的模式封装。

制卡应用接口动态库的名称为“GET_CARD_KEY.dll”。

制卡应用接口动态库提供一个应用 API接口，其 C语言声明如下：

```
DWORD WINAPI get_card_key_op(char* In, char* Ot);
```

其中In为应用接口输入，Ot为应用接口输出。

制卡接口应用实现采用阻塞式接口调用，即应用过程为“一问一答”的模式。接口在应用过程中，不允许多进程或多线程调用。

输入输出数据格式均采用 ASCII编码的“0”～“9”和“A”～“F”。

输入数据格式如下表所示。

表格 5- 1 数据交换_输入数据格式

数据元	长度	说明
协议版本	2	接口协议版本
辅助参数	2	接口辅助参数
应用标识	2	应用类型标识
命令标识	2	应用命令标识
命令数据	不定	应用命令执行相关数据

输出数据格式如下表所示。

表格 5- 2 数据交换_输出数据格式

数据元	长度	说明
协议版本	2	接口协议版本
执行响应	2	命令执行结果
应用标识	2	应用类型标识
命令标识	2	应用命令标识
响应数据	不定	应用执行响应相关数据

5.2. 应用接口列表

接口库支持应用接口列表如下表所示。

表格 5- 3 接口库支持应用接口

应用标识	命令标识	命令说明
"00"		通用指令
	"01"	获得加密机授权
	"02"	获取密钥
	"03"	获取单程票数据

5.3. 接口通用错误代码

表格 5- 4 接口通用错误代码

错误代码	说明
"F1"	输入(长度、内容)错误
"F2"	版本错误
"F3"	卡类别错误
"F4"	命令标识不支持

5.4. 接口详细说明

5.4.1. 通用指令

5.4.1.1. 获得加密机授权

输入数据格式如下表所示。

表格 5- 5 通用指令_获得加密机授权_输入数据格式

数据元	长度	说明
协议版本	2	"01"
辅助参数	2	辅助参数
卡类标识	2	"00"
命令标识	2	"01"
命令数据	8	加密机IP地址
	4	加密机端口
	8	加密机授权PIN
	2	使用的版本信息

执行成功数据格式如下表所示。

表格 5- 6 通用指令_获得加密机授权_执行成功数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	"00"
卡类标识	2	"00"
命令标识	2	"01"
响应数据	0	无

执行失败数据格式如下表所示。

表格 5- 7 通用指令_获得加密机授权_执行失败数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	错误代码
卡类标识	2	"00"
命令标识	2	"01"
响应数据	0	无

错误代码说明如下表所示。

表格 5- 8 通用指令_获得加密机授权_错误代码说明

错误代码	说明
"01"	获得授权失败
"02"	CCK 初始化失败
"03"	产生制卡用IK失败
"04"	IK获取失败
"05"	IK的 MAC校验失败

5.4.1.2. 密钥获取

输入数据格式如下表所示。

表格 5- 9 通用指令_密钥获取_输入数据格式

数据元	长度	说明
协议版本	2	"01"
辅助参数	2	辅助参数
卡类标识	2	"00"
命令标识	2	"02"
命令数据	16	用户卡逻辑卡号

执行成功数据格式如下表所示。

表格 5- 10 通用指令_密钥获取_执行成功数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	"00"
卡类标识	2	"00"
命令标识	2	"02"
响应数据	544	密钥信息

密钥信息结构如下表所示。

表格 5- 11 通用指令_密钥获取_执行成功密钥信息结构

字节序号			长度	类型	密钥说明
000	--	031	32	HEX(M)	卡片主控密钥
032	--	063	32	HEX(M)	卡片维护密钥
064	--	095	32	HEX(M)	外部认证密钥
096	--	127	32	HEX(M)	应用主控密钥（DACK）
128	--	159	32	HEX(M)	应用维护密钥（DAMK）
160	--	191	32	HEX(M)	消费密钥（DPK）
192	--	223	32	HEX(M)	圈存密钥（DLK）
224	--	255	32	HEX(M)	交易认证TAC 密钥（DTK）
256	--	287	32	HEX(M)	应用维护密钥01（DAMK01）
288	--	319	32	HEX(M)	应用维护密钥02（DAMK02）
320	--	351	32	HEX(M)	应用锁定密钥（DABK）
352	--	383	32	HEX(M)	应用解锁密钥（DAUK）
384	--	415	32	HEX(M)	PIN 解锁密钥（DPUK）
416	--	447	32	HEX(M)	PIN 重装密钥（DPRK）
448	--	479	32	HEX(M)	修改透支限额密钥（DUK）
480	--	511	32	HEX(M)	圈提密钥密钥（DULK）
512	--	543	32	HEX(M)	外部认证密钥（DAEAK）

执行失败数据格式如下表所示。

表格 5- 12 通用指令_密钥获取_执行失败数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	错误代码
卡类标识	2	"00"
命令标识	2	"02"
响应数据	0	无

表格 5- 13 通用指令_密钥获取_错误代码说明

错误代码	说明
"11"	获取失败（DCCK）
"12"	获取失败（DCMK）
"13"	获取失败（DCEAK）
"21"	获取失败（DACK）
"22"	获取失败（DAMK）
"23"	获取失败（DPK）
"24"	获取失败（DLK）
"25"	获取失败（DTK）
"26"	获取失败（DAMK01）
"27"	获取失败（DAMK02）
"28"	获取失败（DABK）
"29"	获取失败（DAUK）
"2A"	获取失败（DPUK）
"2B"	获取失败（DPRK）
"2C"	获取失败（DUK）
"2D"	获取失败（DULK）
"2E"	获取失败（DAEAK）

5.4.1.3. 获取单程票数据

输入数据格式如下表所示。

表格 5- 14 通用指令_获取单程票数据_输入数据格式

数据元	长度	说明
协议版本	2	"01"
辅助参数	2	辅助参数
卡类标识	2	"00"
命令标识	2	"03"
命令数据	8	物理卡号
	8	用户卡逻辑卡号

执行成功数据格式如下表所示。

表格 5- 15 通用指令_获取单程票数据_执行成功数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	"00"
卡类标识	2	"00"
命令标识	2	"03"
响应数据	8	认证mac
	12	认证密钥

执行失败数据格式如下表所示。

表格 5- 16 通用指令_获取单程票数据_执行失败数据格式

数据元	长度	说明
协议版本	2	"01"
执行响应	2	错误代码
卡类标识	2	"00"
命令标识	2	"03"
响应数据	0	无

表格 5- 17 通用指令_获取单程票数据_错误代码说明

错误代码	说明
"41"	单程票 mac获取失败
"42"	单程票 key获取失败