长沙市轨道交通工程

清分中心系统设备采购及系统集成项目

长沙轨道交通AFC技术标准

（加密机使用及用户卡密钥计算）

v1.00

版本号	日期	编写者	审核者	描述
1.00	2015/08/07			文档编写。

1. 目的

描述长沙轨道交通加密机使用及户卡发行过程中的密钥计算。

2. 参考

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。

《KY-SJL06E型城市一卡通专用密码机用户手册》

3. 加密机使用

本章节描述用户卡发行过程中，卡密钥计算涉及的加密机的使用。

3.1. 加密机授权

在加密机进入工作状态后，向加密机插入A卡。

使用加密机“FC”指令进行加密机授权。

（注：“FC”指令使用说明详见《KY-SJL06E型城市一卡通专用密码机用户手册》内3.1.取得授权指令说明，指令涉及的HSM口令内容，请咨询加密机管理人员）

3.2. 加密机密钥计算准备

使用加密机“F0”指令进行CCK修订。

（注：“F0”指令使用说明详见《KY-SJL06E型城市一卡通专用密码机用户手册》内3.3.1.CCK初始化过程说明）

使用加密机“F4”指令进行IK导出。

（注：“F4”指令使用说明详见《KY-SJL06E型城市一卡通专用密码机用户手册》内3.3.4.输出制卡用TK或IK过程说明）

3.3. 用户卡密钥计算

使用“F6”指令进行用户卡密钥计算。

（注：“F6”指令使用说明详见《KY-SJL06E型城市一卡通专用密码机用户手册》内3.3.5. 输出制卡功能密钥过程说明）

4. 密钥关系

用户卡内所有功能密钥和加密机对应的应用密钥，其关系为加密机应用密钥对用户卡逻辑卡号进行一次分散计算，即可获得对应的卡功能密钥。

4.1. 分散算法

4.1.1. 算法标记

Y = DIV（ K ）[X]

其中，

Y 为16字节输出分散结果；

X 为 8字节分散内容；

K 为16字节计算用密钥。

4.1.2. 算法说明

分散算法简称 Diversify，是指将一个16字节的密钥 K，对分散数据 X进行处理，推导出一个16字节的密钥 Y。

推导过程分前后两部分：

- 前 8字节密钥推导方法是以分散数据作为输入数据，以密钥 K为密钥进行3DES加密所得的 8字节结果；
- 后 8字节密钥推导方法是以分散数据求反后作为输入数据，以密钥 K为密钥进行3DES加密所得的 8字节结果。

5. 密钥说明

用户卡发行涉及的加密机应用密钥，其在加密机内的安排如下表。

说明	组号	索引
充值主密钥	01	07
PIN解锁主密钥	01	09
PIN重装主密钥	01	10
应用文件更新密钥	02	01
钱包消费主密钥	02	02
应用锁定密钥	02	03
交易验证（TAC）主密钥	02	04
用户卡主控密钥（CPU）	03	01
用户卡维护密钥（CPU）	03	02
用户卡应用主控密钥(ADF1)	03	03
用户卡应用维护密钥(ADF1)	03	04
应用解锁密钥	03	05
应用文件更新密钥2	03	06

（注：系统正式和测试使用的密钥版本，请咨询加密机管理人员）