乌鲁木齐市轨道交通

清分中心系统设备采购项目

乌鲁木齐轨道交通 AFC 技术标准

（加密机密钥配置整体规划）

20180424v01.00

文档历史

版本号	日期	编写者	审核者	描述
20180424v01.00	20180424	铭鸿数据		定稿版

1. 目的

定义了乌鲁木齐轨道交通系统中，卡的应用所需的根密钥所在加密机的密钥配置规划。

本文主要对象为业主单位系统管理员和密钥管理员。

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。

《CJ/T 0025.1 中国金融集成电路（IC）卡规范 第 1 部分：电子钱包 / 电子存折应用卡片规范》

《CJ/T 0025.2 中国金融集成电路（IC）卡规范 第 2 部分：电子钱包 / 电子存折应用规范》

《CJ/T 0025.9 中国金融集成电路（IC）卡规范 第 9部分：电子钱包 / 电子存折扩展应用指南》

《CJ/T 166-2006 建设事业集成电路（IC）卡应用技术》

《CJ/T 330-2010 电子标签通用技术要求》

《CJ/T 331-2010 城市公用事业互联互通卡通用技术要求》

《CJ/T 333-2010 城市公用事业互联互通卡密钥及安全技术要求》

3. 密钥版本定义

加密机的密钥版本定义如下表。

版本号	占用空间	起始	结束
密钥应用版本 0	255	1	255
密钥应用版本 1	255	257	511
密钥应用版本 2	255	513	767
密钥应用版本 3	255	769	1023

每个密钥版本占用 255条密钥索引，共定义 4个版本。

4. 版本内密钥功能划分

每个密钥版本内密钥的功能划分如下表所示。

功能划分	占用空间	起始	结束
CPU卡应用密钥	192	1	192
逻辑加密卡应用密钥	16	193	208
PSAM应用密钥	16	209	224
系统应用密钥	31	225	255

功能密钥的具体索引，可按版本内密钥索引加上版本号乘以 256获得。