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_正式版本）

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，正式上线系统中，卡的应用所需的根密钥所在加密机的密钥索引细节定义。

本文主要对象为业主单位密钥管理员，应用系统配置管理员。

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》

《乌鲁木齐轨道交通 AFC 技术标准（加密机密钥配置整体规划)》

3. 密钥版本定义

正式上线系统使用加密机的密钥应用版本 0定义的密钥索引。

4. 版本内功能密钥索引定义

4.1. CPU 卡应用密钥索引定义

CPU 卡维护密钥索引定义如下表。

密钥说明	索引	16进制
卡主控密钥	1	001
卡维护密钥	2	002
预留密钥	3	003
预留密钥	4	004
预留密钥	5	005
卡外部认证密钥	6	006
预留密钥	7	007
预留密钥	8	008

CPU 卡应用密钥索引定义如下表。

应用编号	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
密钥说明	索引								16进制							
	应用1	应用2	应用3	应用4	应用5	应用6	应用7	应用8	应用1	应用2	应用3	应用4	应用5	应用6	应用7	应用8
应用主控	9	33	57	81	105	129	153	177	009	021	039	051	069	081	099	0B1
应用维护	10	34	58	82	106	130	154	178	00A	022	03A	052	06A	082	09A	0B2
应用锁定	11	35	59	83	107	131	155	179	00B	023	03B	053	06B	083	09B	0B3
应用解锁	12	36	60	84	108	132	156	180	00C	024	03C	054	06C	084	09C	0B4
PIN 重装	13	37	61	85	109	133	157	181	00D	025	03D	055	06D	085	09D	0B5
PIN 解锁	14	38	62	86	110	134	158	182	00E	026	03E	056	06E	086	09E	0B6
预留密钥	15	39	63	87	111	135	159	183	00F	027	03F	057	06F	087	09F	0B7
文件维护密钥01	16	40	64	88	112	136	160	184	010	028	040	058	070	088	0A0	0B8
文件维护密钥02	17	41	65	89	113	137	161	185	011	029	041	059	071	089	0A1	0B9
文件维护密钥03	18	42	66	90	114	138	162	186	012	02A	042	05A	072	08A	0A2	0BA
文件维护密钥04	19	43	67	91	115	139	163	187	013	02B	043	05B	073	08B	0A3	0BB
预留密钥	20	44	68	92	116	140	164	188	014	02C	044	05C	074	08C	0A4	0BC
预留密钥	21	45	69	93	117	141	165	189	015	02D	045	05D	075	08D	0A5	0BD
预留密钥	22	46	70	94	118	142	166	190	016	02E	046	05E	076	08E	0A6	0BE
圈存密钥	23	47	71	95	119	143	167	191	017	02F	047	05F	077	08F	0A7	0BF
预留密钥	24	48	72	96	120	144	168	192	018	030	048	060	078	090	0A8	0C0
圈提密钥	25	49	73	97	121	145	169	193	019	031	049	061	079	091	0A9	0C1
预留密钥	26	50	74	98	122	146	170	194	01A	032	04A	062	07A	092	0AA	0C2
修改透支限额密钥	27	51	75	99	123	147	171	195	01B	033	04B	063	07B	093	0AB	0C3
预留密钥	28	52	76	100	124	148	172	196	01C	034	04C	064	07C	094	0AC	0C4
消费密钥	29	53	77	101	125	149	173	197	01D	035	04D	065	07D	095	0AD	0C5
预留密钥	30	54	78	102	126	150	174	198	01E	036	04E	066	07E	096	0AE	0C6
TAC 密钥	31	55	79	103	127	151	175	199	01F	037	04F	067	07F	097	0AF	0C7
外部认证密钥	32	56	80	104	128	152	176	200	020	038	050	068	080	098	0B0	0C8

4.2. 逻辑加密卡应用密钥

逻辑加密卡应用密钥索引定义如下表。

密钥说明	索引	16进制
卡认证密钥	201	0C9
预留密钥	202	0CA
预留密钥	203	0CB
卡消费密钥	204	0CC
预留密钥	205	0CD
预留密钥	206	0CE
TAC 密钥	207	0CF
预留密钥	208	0D0
预留密钥	209	0D1
预留密钥	210	0D2
预留密钥	211	0D3
预留密钥	212	0D4
预留密钥	213	0D5
预留密钥	214	0D6
预留密钥	215	0D7
预留密钥	216	0D8

4.3. PSAM应用密钥

PSAM应用密钥索引定义如下表。

密钥说明	索引	16进制
PSAM主控密钥	217	0D9
PSAM维护密钥	218	0DA
预留密钥	219	0DB
预留密钥	220	0DC
PSAM应用主控密钥	221	0DD
PSAM应用维护密钥	222	0DE
PSAM外部认证密钥	223	0DF
预留密钥	224	0E0
预留密钥	225	0E1
预留密钥	226	0E2
预留密钥	227	0E3
预留密钥	228	0E4
预留密钥	229	0E5
预留密钥	230	0E6
预留密钥	231	0E7
预留密钥	232	0E8

4.4. 系统应用密钥

密钥说明	索引	16进制
预留密钥	233	0E9
预留密钥	234	0EA
预留密钥	235	0EB
预留密钥	236	0EC
预留密钥	237	0ED
预留密钥	238	0EE
预留密钥	239	0EF
预留密钥	240	0F0
预留密钥	241	0F1
预留密钥	242	0F2
预留密钥	243	0F3
预留密钥	244	0F4
预留密钥	245	0F5
预留密钥	246	0F6
预留密钥	247	0F7
预留密钥	248	0F8
预留密钥	249	0F9
预留密钥	250	0FA
预留密钥	251	0FB
预留密钥	252	0FC
预留密钥	253	0FD
预留密钥	254	0FE
预留密钥	255	0FF