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_测试版本）

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 4
2. 参考 4
3. 密钥版本定义 4
4. 版本内功能密钥索引定义 4
4.1. CPU卡应用密钥索引定义 4
4.2. 逻辑加密卡应用密钥 6
4.3. PSAM 应用密钥 6
4.4. 系统应用密钥 7

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。

本文主要对象为系统开发单位开发人员。

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 2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	513	201
卡维护密钥	514	202
预留密钥	515	203
预留密钥	516	204
预留密钥	517	205
卡外部认证密钥	518	206
预留密钥	519	207
预留密钥	520	208

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	521	545	569	593	617	641	665	689	209	221	239	251	269	281	299	2B1
应用维护	522	546	570	594	618	642	666	690	20A	222	23A	252	26A	282	29A	2B2
应用锁定	523	547	571	595	619	643	667	691	20B	223	23B	253	26B	283	29B	2B3
应用解锁	524	548	572	596	620	644	668	692	20C	224	23C	254	26C	284	29C	2B4
PIN 重装	525	549	573	597	621	645	669	693	20D	225	23D	255	26D	285	29D	2B5
PIN 解锁	526	550	574	598	622	646	670	694	20E	226	23E	256	26E	286	29E	2B6
预留密钥	527	551	575	599	623	647	671	695	20F	227	23F	257	26F	287	29F	2B7
文件维护密钥01	528	552	576	600	624	648	672	696	210	228	240	258	270	288	2A0	2B8
文件维护密钥02	529	553	577	601	625	649	673	697	211	229	241	259	271	289	2A1	2B9
文件维护密钥03	530	554	578	602	626	650	674	698	212	22A	242	25A	272	28A	2A2	2BA
文件维护密钥04	531	555	579	603	627	651	675	699	213	22B	243	25B	273	28B	2A3	2BB
预留密钥	532	556	580	604	628	652	676	700	214	22C	244	25C	274	28C	2A4	2BC
预留密钥	533	557	581	605	629	653	677	701	215	22D	245	25D	275	28D	2A5	2BD
预留密钥	534	558	582	606	630	654	678	702	216	22E	246	25E	276	28E	2A6	2BE
圈存密钥	535	559	583	607	631	655	679	703	217	22F	247	25F	277	28F	2A7	2BF
预留密钥	536	560	584	608	632	656	680	704	218	230	248	260	278	290	2A8	2C0
圈提密钥	537	561	585	609	633	657	681	705	219	231	249	261	279	291	2A9	2C1
预留密钥	538	562	586	610	634	658	682	706	21A	232	24A	262	27A	292	2AA	2C2
修改透支限额密钥	539	563	587	611	635	659	683	707	21B	233	24B	263	27B	293	2AB	2C3
预留密钥	540	564	588	612	636	660	684	708	21C	234	24C	264	27C	294	2AC	2C4
消费密钥	541	565	589	613	637	661	685	709	21D	235	24D	265	27D	295	2AD	2C5
预留密钥	542	566	590	614	638	662	686	710	21E	236	24E	266	27E	296	2AE	2C6
TAC 密钥	543	567	591	615	639	663	687	711	21F	237	24F	267	27F	297	2AF	2C7
外部认证密钥	544	568	592	616	640	664	688	712	220	238	250	268	280	298	2B0	2C8

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	713	2C9
预留密钥	714	2CA
预留密钥	715	2CB
卡消费密钥	716	2CC
预留密钥	717	2CD
预留密钥	718	2CE
TAC 密钥	719	2CF
预留密钥	720	2D0
预留密钥	721	2D1
预留密钥	722	2D2
预留密钥	723	2D3
预留密钥	724	2D4
预留密钥	725	2D5
预留密钥	726	2D6
预留密钥	727	2D7
预留密钥	728	2D8

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	729	2D9
PSAM维护密钥	730	2DA
预留密钥	731	2DB
预留密钥	732	2DC
PSAM应用主控密钥	733	2DD
PSAM应用维护密钥	734	2DE
PSAM外部认证密钥	735	2DF
预留密钥	736	2E0
预留密钥	737	2E1
预留密钥	738	2E2
预留密钥	739	2E3
预留密钥	740	2E4
预留密钥	741	2E5
预留密钥	742	2E6
预留密钥	743	2E7
预留密钥	744	2E8

4.4. 系统应用密钥

密钥说明	索引	16进制
预留密钥	745	2E9
预留密钥	746	2EA
预留密钥	747	2EB
预留密钥	748	2EC
预留密钥	749	2ED
预留密钥	750	2EE
预留密钥	751	2EF
预留密钥	752	2F0
预留密钥	753	2F1
预留密钥	754	2F2
预留密钥	755	2F3
预留密钥	756	2F4
预留密钥	757	2F5
预留密钥	758	2F6
预留密钥	759	2F7
预留密钥	760	2F8
预留密钥	761	2F9
预留密钥	762	2FA
预留密钥	763	2FB
预留密钥	764	2FC
预留密钥	765	2FD
预留密钥	766	2FE
预留密钥	767	2FF