

	文档编号	版本号	页数	密级
	CSC-6106	V2.0		

产品说明书

一卡通 CPU 卡

（仅供内部使用）

文档作者	GJM	日 期	2017-05-08
审 核		日 期	
批 准		日 期	

赤松城（北京）科技有限公司

二〇一七年



赤松城(北京)科技有限公司

文档修改履历

序号	日期	修改范围	新版本号	修改人
1	2017-05-08	修改自“产品说明书_国密认证消费一卡通_V3.2.pdf”	V1.0	GJM
2	2017-5-10	1、将门禁认证的相关信息改为门禁消费一卡通 2、增加了卡片基本指令，填充了互联互通应用指令和门禁消费一卡通应用指令	V1.1	DZH
1	2017-05-12	修改指令名称	V2.0	GJM



目 录

1	产品简介	1
1.1	产品特性	1
1.2	产品型号	1
2	功能说明	2
2.1	预置文件结构	2
2.1.1	根目录	2
2.1.2	门禁消费一卡通应用	3
2.1.3	住建部互联互通应用(金融应用)	3
2.2	标准 CPU 卡指令	4
2.2.1	卡片基本指令	4
2.2.2	门禁消费一卡通应用指令	5
2.2.3	住建部互联互通应用指令	6
3	常用产品型号	7

表目录

表 1	卡片基本指令	4
表 2	门禁消费一卡通应用指令	5
表 3	住建部互联互通应用指令	6
表 4	常用 CPU 卡产品型号	7

图目录

图 1	一卡通应用预览图	1
图 2	CPU 卡产品型号	1
图 3	根目录文件系统图	2
图 4	门禁消费一卡通应用文件系统图	3
图 5	互联互通应用文件系统图	3



1 产品简介

本文档介绍了 T6 一卡通系统中 CPU 卡产品的功能及使用范围，该产品包含小额支付、身份识别、自助消费、快速通过等多种应用，内置国密/3DES 等多种加密算法，可用于军工、校园、企业、城市、智慧园区、充电桩等。



图 1 一卡通应用预览图

1.1 产品特性

- 高安全 CPU 卡，可选 SM1/2/3/4, SM7, DES/3DES, RSA 等多种加密算法；
- 支持住建部 IC 卡应用规范，3GPP 标准，PBOC 标准；
- 卡内预置住建部互联互通应用，可用于公交卡，城市一卡通，市民卡等；
- 卡内预置门禁消费一卡通应用，可用于校园、医院、智慧园区、企业、军工等一卡通应用；
- 标准卡片指令，兼容华大、同方、复旦、大唐、NXP 等多种卡片，方便无缝升级和替换；
- 符合 7816/ISO14443 标准，兼容 M1 卡；
- 可选 8KB~1MB 数据空间，支持图片存储；
- 满足 10 万次擦写指标；
- 数据有效期 10 年；
- 交易时间<350ms
- 卡工作温度 -25C~70C
- 应用范围：门禁、食堂、超市、水电、公交、手机、充电桩、部队、城市、校园、企业等

1.2 产品型号

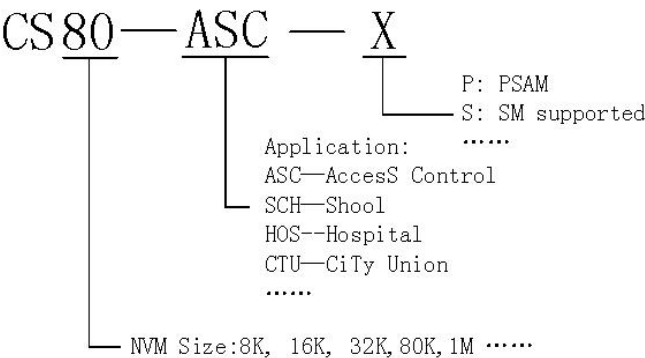


图 2 CPU 卡产品型号



2 功能说明

该系列产品在常用 CPU 卡芯片基础上预置了多种应用,可以根据客户需求选用华大、同方、复旦、大唐、NXP 等通用 CPU 卡芯片。

使用统一的卡片指令,免除了升级和兼容性问题。

2.1 预置文件结构

CPU 卡内可根据客户需求定制应用,常用型号主要预置了以下两种应用:

1> 住建部互联互通标准应用: 可用于公交卡,城市一卡通,市民卡等;

2> 门禁消费一卡通应用: 可用于校园、医院、智慧园区、企业、军工等一卡通应用;

以上两种应用均支持电子钱包消费,符合 PBOC 标准。

2.1.1 根目录

根目录文件下存储着卡片基本信息以及持卡人数据信息

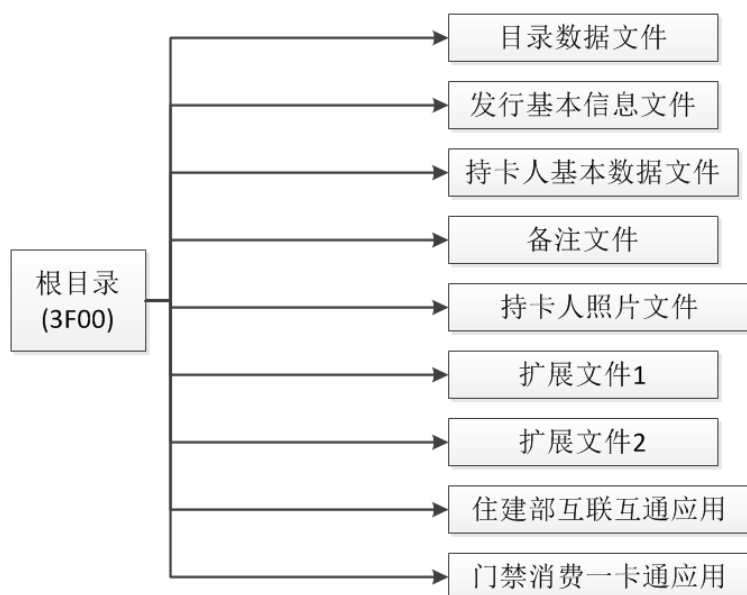


图 3 根目录文件系统图



2.1.2 门禁消费一卡通应用

主要应用于各种通用场景，比如校园、医院、智慧园区、企业、军工等一卡通系统，主要包括以下文件。

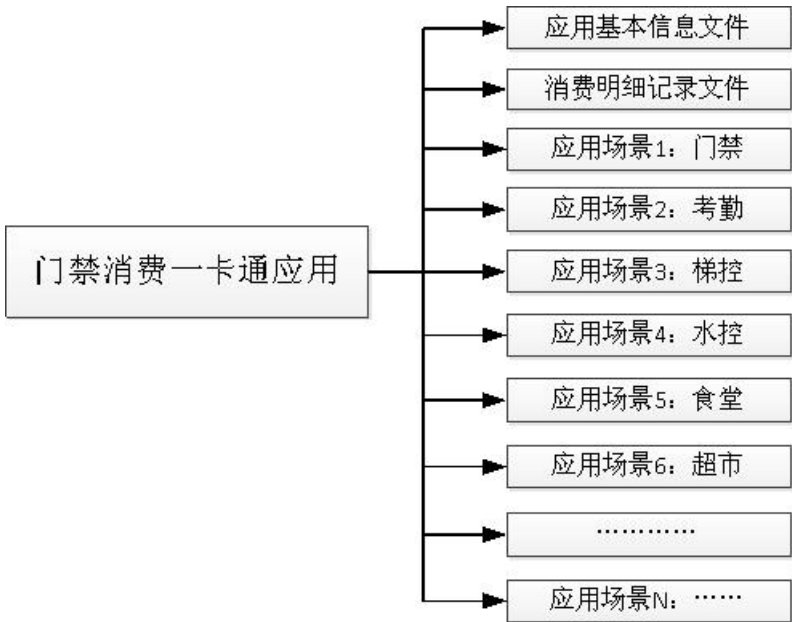


图 4 门禁消费一卡通应用文件系统图

2.1.3 住建部互联互通应用(金融应用)

本应用根据建设部 IC 卡标准建立文件结构，支持 PBOC 规定的电子钱包应用和电子扩展钱包应用，主要包括电子钱包及以下文件。

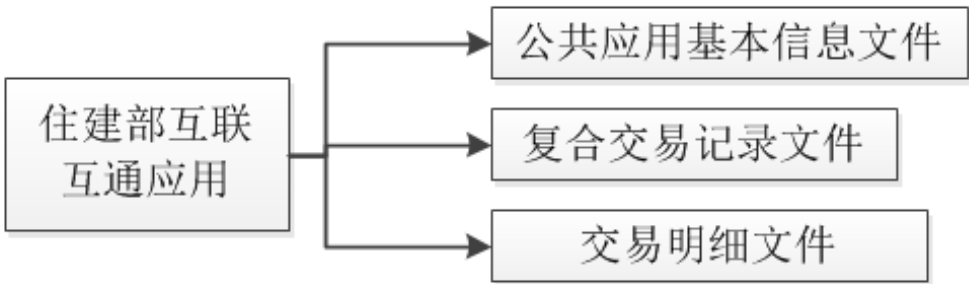


图 5 互联互通应用文件系统图



2.2 标准 CPU 卡指令

用户通过通用读写器发送以下指令，即可对卡进行激活、加密、挂失、销毁、录入持卡人信息、读取持卡人信息、充值、消费、查询余额等操作。

2.2.1 卡片基本指令

下表只列出了常用的指令，更详细的说明请联络我司技术支持。

序号	指令名称	指令代码	说明
1	设置卡片 管理员权限密钥		该密钥为卡片根密钥，由卡片发行单位掌握，如公交公司，学校等 管理员权限可以激活，锁死、解锁、销毁卡片 密钥无法读取，只能用带 PSAM 母卡的读写器重置
2	激活卡		用户来激活卡片
3	锁死卡		用户锁死卡片，此后卡片无法使用
4	解锁卡		用户解锁已锁死的卡片，卡恢复使用
5	重置卡		清空卡内所有信息，回到初始发卡状态
6	销毁卡		销毁不再使用的卡，卡数据永远不再恢复
7	设置卡片 读写权限密钥		读写权限密钥可以设置文件读写权限，用来对文件进行加密和解密 密钥无法读取，但可以用带 PSAM 子卡的读写器重置
8	读卡号		
9	写发卡信息		对应住建部规范：发行基本信息文件，包含发卡方、城市代码、行业代码、 组织机构代码、应用场景列表、发卡时间、读写权限等
10	读发卡信息		
11	写持卡人身份信息		包含姓名、年龄、性别、证件类型、证件号码、电话、手机号、地址、照片 读写权限等
12	读持卡人身份信息		
13	写扩展文件		更新用于客户自行扩展的文件，每个扩展文件包含 0x32 个字节，可支持 6 个扩展文件
14	读扩展文件		

表 1 卡片基本指令



2.2.2 门禁消费一卡通应用指令

下表只列出了常用的指令，更详细的说明请联络我司技术支持。

序号	指令名称	指令代码	说明
1	设置当前应用 管理员权限密钥		该密钥为本应用的根密钥，由卡片使用单位掌握，如某个地铁售票窗口，学校超市等 管理员权限可以激活，锁死、解锁、销毁当前应用 密钥无法读取，可以用带 PSAM 子卡的读写器重置
2	激活应用		用户来激活当前应用
3	锁死应用		用户锁死当前应用，此后卡片此应用无法使用，但不影响使用其他应用
4	解锁应用		用户解锁已锁死的当前应用，应用恢复使用
5	重置		清空当前应用内所有信息，回到初始发卡状态
6	设置当前应用下		可以设置当前应用下文件读写权限，用来对文件进行加密和解密 密钥无法读取，但可以用带 PSAM 子卡的读写器重置
7	写应用信息		当前应用描述，包含发卡方、城市代码、行业代码、组织机构代码、应用场景列表、发卡时间、读写权限等
8	读应用信息		
9	写第 N 个应用场景 文件		一个应用中可以包含多个应用场景，如：门禁、食堂、考勤、超市等，每个应用场景对应一个描述文件 包含发卡方、城市代码、行业代码、场景激活标识、场景版本、互通标识、场景序列号、场景启动和有效日期，场景认证权限、场景消费权限等
10	读第 N 个应用场景 文件		
11	设置消费权限密钥		消费权限可以设置各个应用场景是否有使用电子钱包消费的权限 密钥无法读取，但可以用带 PSAM 子卡的读写器重置
12	写消费记录信息		包括消费交易的记录信息，包括充值、消费等记录
13	读消费记录信息		
14	充值		对当前应用电子钱包进行充值
15	消费		对当前应用电子钱包进行消费
16	查询余额		查询当前电子钱包余额
17	重置钱包		重置当前电子钱包，余额归零

表 2 门禁消费一卡通应用指令



2.2.3 住建部互联互通应用指令

下表只列出了常用的指令，更详细的说明请联络我司技术支持。

序号	指令名称	指令代码	说明
1	设置当前应用 管理员权限密钥		该密钥为本应用的根密钥，由卡片使用单位掌握，如某个地铁售票窗口，学校超市等 管理员权限可以激活，锁死、解锁、销毁当前应用 密钥无法读取，可以用带 PSAM 子卡的读写器重置
2	激活应用		用户来激活当前应用
3	锁死应用		用户锁死当前应用，此后卡片此应用无法使用，但不影响使用其他应用
4	解锁应用		用户解锁已锁死的当前应用，应用恢复使用
5	重置应用		清空当前应用内所有信息，回到初始发卡状态
6	设置当前应用下 文件读写权限密钥		可以设置当前应用下文件读写权限，用来对文件进行加密和解密 密钥无法读取，但可以用带 PSAM 子卡的读写器重置
7	写应用信息		当前应用描述，包含发卡方、城市代码、行业代码、组织机构代码、应用场景列表、发卡时间等
8	读应用信息		
9	设置消费权限密钥		消费权限可以设置各个应用场景是否有使用电子钱包消费的权限 密钥无法读取，但可以用带 PSAM 子卡的读写器重置
10	写消费记录信息		包括消费交易的记录信息，包括充值、消费等记录
11	读消费记录信息		
12	充值		对当前应用电子钱包进行充值
13	消费		对当前应用电子钱包进行消费
14	查询余额		查询当前电子钱包余额
15	重置		重置当前电子钱包，余额归零

表 3 住建部互联互通应用指令



3 常用产品型号

下表列出了常用产品型号，客户可根据需求进行选择：

CPU 卡型号	可选芯片	内置应用	说明
CS08-ASC/-S	FM1208 CIU5108A	门禁消费一卡通	8K 数据空间，兼容 M1 卡，可用于校园、医院、智慧园区、企业、军工等一卡通。带 S 后缀的支持国密算法，不带-S 的只支持 DES 算法
CS16-ASC/-S	FM1216	门禁消费一卡通	16K 数据空间
CS80-ASC/-S	FM1280 CIU51L80	门禁消费一卡通	80K 数据空间
CS08-CTU/-S	FM1208, CIU5108A	住建部互联互通应用	8K 数据空间，兼容 M1 卡，可用于公交卡，城市一卡通，市民卡等。带 S 后缀的支持国密算法，不带-S 的只支持 DES 算法
CS16-CTU/-S	FM1216	住建部互联互通应用	16K 数据空间
CS80-CTU/-S	FM1280 CIU51L80	住建部互联互通应用	80K 数据空间

表 4 常用 CPU 卡产品型号

注意：上表仅列出了非接触卡型号，接触卡和双界面卡型号请咨询我司技术支持。