【门禁卡的两大类】

通常情况下分ID和IC两种类别。

ID卡：内部不存数据（金额次数等）卡相关的重要信息存在电脑数据库中。需要重要数据的时候只有连接系统才能获得。比如消费时POS机读取卡号，送到服务器上，服务器收到卡号后，在数据库中扣掉对应人员的消费金额，然后把结果送回POS机显示。

优点：灵活，不存在账务问题。

缺点：不能离线使用，存在透支现象，系统安全性差，很难组建大型一卡通系统。

IC卡：个人信息和金额存放在卡片上，消费时POS机直接扣除卡片上的金额，消费完成后再把记录上传到数据库中。

目前国内第一流的一卡通厂家都使用IC模式，公交系统使用IC模式。

优点：可离线使用，不存在透支，容易组建大型一卡通系统。

缺点：对帐复杂

【如何从表面区分ID卡和IC卡】

ID卡：钥匙扣上一般有00开头的10位或者8位数字，如001234567或0098764736

ID薄片卡和银行卡大小厚度差不多，卡上有00开头的18位数字，如0012345678 123 45678

ID厚卡1.8mm，一侧有一个长孔，有一面是斜坡面，卡下方有一串00开头的数字，如0065736487 989,123456

门禁卡，一般有00开头的10位或8位数字的为ID号，没有数字编号的为IC号，但不是绝对。通常是这样。

【ID卡和IC卡的深入技术区别】

ID卡：使用最多的频率为125KHZ，一般叫作低频卡。只有id号,正规id卡的卡号不能修改。如T5577卡 5200卡有密码,有类扇区结构，F8265卡
8268卡可以过防火墙，但只适用手持机操作，不适宜PM3操作。

IC卡：使用最多的频率为13.56MHZ，一般叫作高频卡。

M1卡,sok=08,0扇区不可写,天生可过防火墙

uid卡,sk=08,金扇区可读写,响应magic指令,遇防火墙失效。

cuid卡,sak=08,全扇区可读写,不响座magi指令，遇高級防火墙失效。

fuid卡,sak=08,0扇区只可写入一次,写入一次以后变为M1卡，可过防火墙。

ufuid,sak=08,锁卡前同uid,锁卡后变为M1.

cpu卡,sk=20,安全系最高,密码错误最大16次，超过后就锁死卡片,除非知道其cos系统指令,知道卡密码，否则将无解。

cpu模拟卡,sak=28,cpu卡加mn1卡的复合体。

【IC卡中M1卡的数据结构】

每张卡有16个扇区(0-15),每个扇区4块(0-3块)，

门禁卡数据表结构：

0扇区0块(或称绝对0块)的前4个字节为卡号(或称UID号),第5个字节为校验位,由卡号通过持定算法计算而来,填写镨误可能导致卡片锁死作废(一般写卡工具带有桉验功能,错误会提示),第6-8字节为卡片类型(基本上没啥用,改了也一样能识别到正确类型),最后8位为厂商代码(由卡片广家确定)。

每小扇区第3块的前6个字节为密码A,中间4个字节为存取控制(决定该扇区的读写权很),最后6个字节为密码B。

其会块为数据,用于存效数据。

M1卡常见存取控制位:

可通过M1控制位计算器进行计算,填写非法的按制位可能导致卡片锁死作废。

全加密卡:所有扇区密码A和密码B郝不是FFFFFFFFFFFF。

【ic卡系统中防火墙功能】

防火墙的主要作用是防止复制卡的使用。

ID普通防火墙:修改卡片id,判断是否为复制卡,复制卡则提示错误并阻止通过验证。

ID高級防火墙:(暂无相关参考资料,可能是通过读取卡片信息判断是否为T5577卡,由于F8268卡厂家没有公开相应指令，致使现阶殷很多门禁厂家无法 判断是否为8268卡,由于id门禁时代久远,今后即便公开操作指令冂禁升缀的几率也不大,茚竟成本很高。

IC普通防火墙:检测卡片是否响应magic指令,判断是否为uid卡,若是uid卡则禁止使用。

IC高級防火墙:使用密码修改0扇区0抉数据,成功则为cuid卡,针对检测原理可采用如下办法(需要尝試判断防火墙使用了何种检测技术)：

修改0扇区密码,cuid卡验证蜜码失败的情况,不可修改数据,但防火墙也可设计为先判断密码是否被修改,被修改了就直接提示锴误。

修改0扇区控制位,修改为不可写(具体参考m1控制位规范),但防火情同样可设置为检测控制位是舌被修改,如果被修改,则提示镨误。

由于FUID写入一次以后或UFUID锁卡后变为m1卡,和物业原卡一样,防火墙无法判断是否为复制卡，故FUID和UFUID都可以过防火墙。