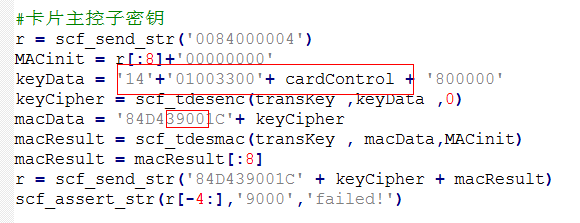
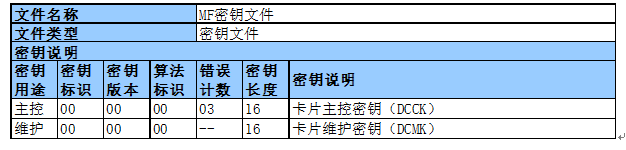
长沙卡开发过程中的疑问

# 存在的问题

* 个人化过程中密钥设置和文档完全不同



截图来自于华大脚本



截图来自于文档

脚本中密钥类型是39，文档中是00.

脚本中密钥版本是01，文档中是00

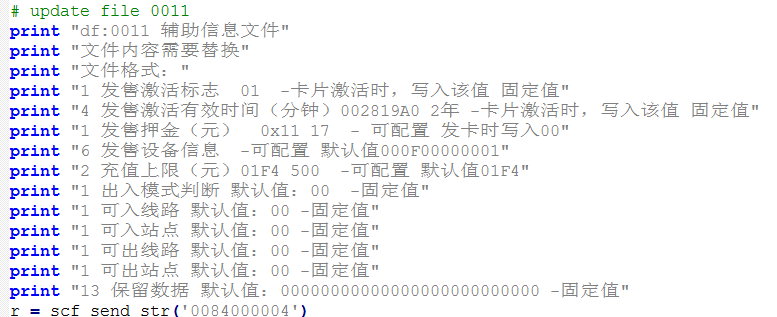
脚本中算法标识是00， 文档中是00.

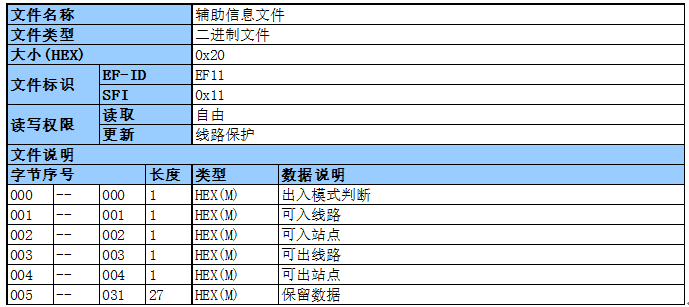
脚本中错误计数器是33， 文档中是03

脚本中后续安全状态是00， 文档中无。

注：所有密钥设置都有同样的问题，此处不一一列出。

* 发卡脚本中没有给出PIN密钥设置的脚本。但是在充值过程却需要用到这个密钥。
* 请提供个人化过程中，初始化持卡人基本数据文件的指令。我想看一下会不会和文档有出入。
* 辅助信息文件个人化过程文档和脚本有出入

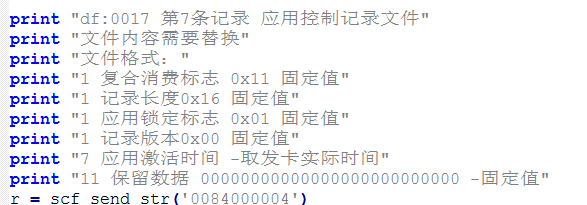




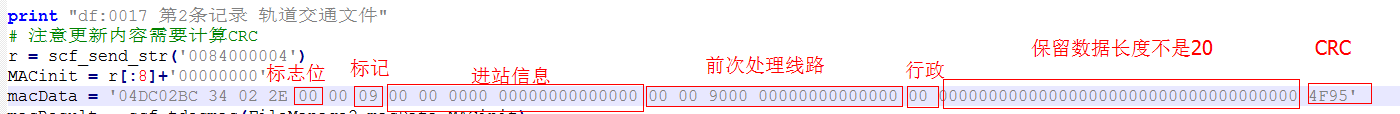
* 保留数据文件需要个人化吗？
* 复合交易记录文件的问题

1. 目前脚本只会添加两条记录，分别是应用控制记录和轨道交通记录，其它5条记录不用初始化吗？特别是公交应用，如果不初始化这条记录，这张卡难道可以用在公交车上？
2. 应用控制记录，脚本和文档不符合



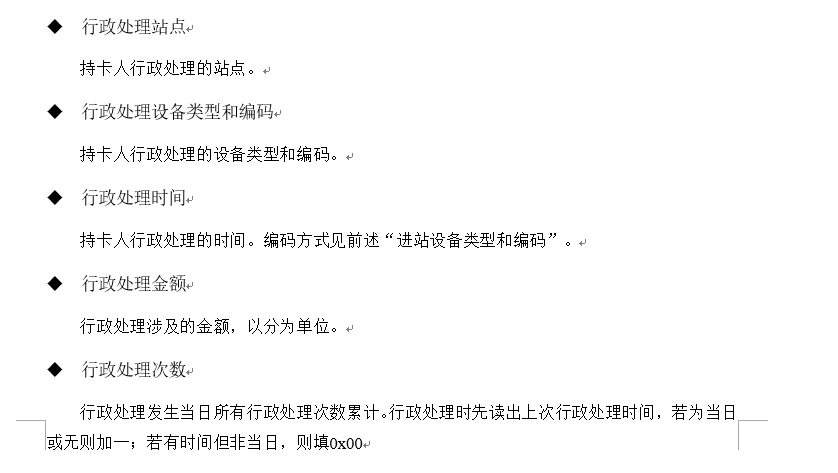


3.轨道交通记录



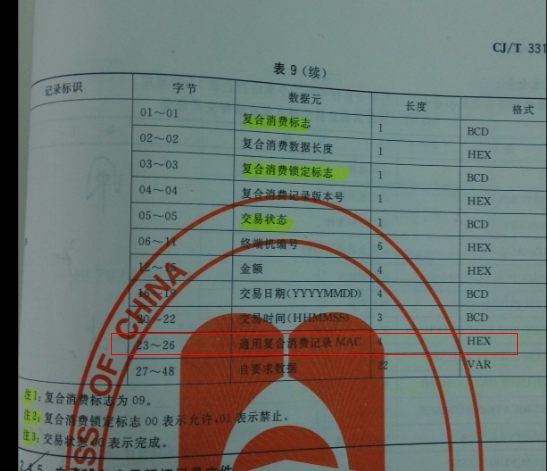
需要CRC编码没有在文档中说明。



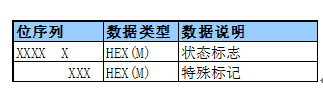


这些行政信息反映在哪几个字节？

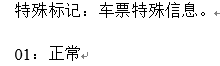
按住建部标准，记录文件中应包括mac值，可以用来做冲突处理(CLA80 INS5A)。现在applet也可以返回mac或tac，不过就有什么说明吗？



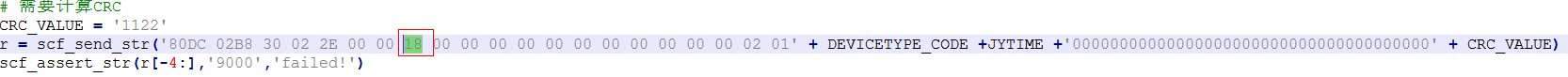
复合交易需要判断进站和出站，按住建部标准应该是判断第第3个字节即状态标志。







是不是00100001代表进站？

测试脚本

0x18=00011000和文档根本没法对应。要么文档是错的，要么脚本是错的。

* 请提供一下普通消费的测试脚本
* BOM/TVM是否会使用到以下pin reload, change, unblock指令？
* 提供两张实际实用的长沙交通卡，用以比对返回的FCI。FCI需要写在applet中。

Select指令需要返回FCI.

分析卡结构，比如读取复合消费记录文件的轨道交通记录。

# 测试系统

李春德开发的测试系统是否可以提供充值，普通消费，复合消费，查询日志的操作说明。

# 开发发卡系统和密钥系统的必要条件

由于我们没有自己的发卡系统，不得不把我们的applet兼容华大的发卡系统。又由于文档不是很完善，反而给开发带来了很多困扰。没有发卡系统，我们自己想要个人化一张卡做测试都非常困难，需要指令一条一条输入，效率非常低。如果发现有bug，这个过程又要重新再来一遍。

* 提供长沙现有华大发卡系统的文档，越完整越好。
* 加密机
* 制卡设备
* GP标准

# 开发测试系统

测试指令需要加密。加密过程中有随机数参与，交易序号又会自增，所以每次指令都会不同。

开发一套类似华大脚本的测试系统。可以提高测试效率。

# 最紧迫的事

周四或周五，我会实际向各位演示一下目前没有发卡系统和测试系统的痛苦。光有卡应用，没有与之配套的系统，技术上受制于人，无法形成闭环，是多么的痛苦。

* 完善文档
* 开发发卡系统
* 开发测试系统