智能卡金融行业应用电子钱包的消费交易流程，开发人员可参考

　　首先终端和卡片有一个共同的密钥叫做消费密钥：PurchKey

　　假设PurchKey = 11223344556677888877665544332211

　　在满足安全条件的情况下：

　　第一步：终端向卡片发送消费初始化命令：

　　Apdu: 80 50 01 02 0B 01 00001000 001122334455

　　CLA INS P1 P2 LC KeyIndex 交易金额 终端机编号

　　卡片返回15个字节的数据如下(不包括9000)：

　　00000000 0000 000000 01 00 11223344

　　卡片余额 交易序号 透支限额 密钥版本号 算法标识 随机数

　　MAC1的计算过程如下(终端):

　　1.计算过程密钥:SessionKey

　　InputData = 11223344 0000 0001 (8bytes)

　　随机数 卡片脱机交易序号 终端交易序号后四位

　　PurchKey = 11223344556677888877665544332211

　　SessionKey = 3DESEnypt(InputData, PurchKey) = 003238ABC57659DD

　　用LoadKey对InputData 做3DES加密

　　2.计算MAC1

　　InputData1 = 00001000 06 001122334455 20120229135100

　　交易金额 交易类型 终端机编号 日期时间

　　SessionKey = 003238ABC57659DD

　　MAC1 = MAC(InputData1 SessionKey ) = F15CAB75

　　用SessionKey对InputData1做MAC运算

　　第二步：终端向卡片发送消费命令：

　　Apdu: 80 54 01 00 0F 00000001 20111221214822 3A845BF0

CLA INS P1 P2 LC 终端交易序号 交易日期时间 MAC1

　　卡片用同样的方法计算MAC1并验证终端发来的MAC1是否正确，从而确认终端是否合法。如果MAC1验证没有通过，卡片会返回MAC错误终止交易。如果MAC1验证通过，进行第三步。

　　第三步：卡片修改余额,脱机交易序号加1并计算MAC2 和TAC,并返回给终端

　　计算MAC

　　InputData2= 00001000

　　交易金额

　　SessionKey = 003238ABC57659DD

　　MAC2 = MAC(InputData2 SessionKey ) = 56988A13

　　用SessionKey对InputData2做MAC运算

　　计算TAC

　　卡片和终端还有一个共同的密钥TAC密钥：TACKey

　　假设TACKey = 00112233445566778899AABBCCDDEEFF

　　TACSessionKey=XOR( Left(8),Right(8)) =8888888888888888

　　TACKey左右8个字节做异或运算

　　InputData3=00001000 01 001122334455 00000001 20111221 214822

　　交易金额 交易类型 终端机编号 终端交易序号 交易日期 交易时间

　　TAC = MAC(InputData3, TACSessionKey) = 3FF7A28A

　　MAC2和TAC作为消费命令的返回数据返回给终端，消费交易到此就结束了，

　　TAC作为清算的时候验证交易数据真伪和完整性的重要依据，连同交易记录一同保存在终端。