智能卡与NFC

党凡

i@dangfan.me

智能卡示例

银行卡、交通卡

身份证、护照

SIM卡

门禁卡

数字电视

基础知识

什么是智能卡

Tamper-resistant computer, on a single chip, embedded in piece of plastic, with very limited resources.

capable of securely:

- storing data
- processing data

* Smartcards and RFID （http://www.cs.ru.nl/~kursawe/SiO2011/Slides/sio_smartcards.pdf）

智能卡分类

Memory Card vs Processor Card

接触式 vs 非接触式

主动式 vs 被动式

智能卡标准

- 接触式智能卡
  - ISO/IEC 7816

- 非接触式智能卡
  - ISO/IEC 14443
    - Part 1：物理特性
    - Part 2：射频能量和信号接口
    - Part 3：初始化和防冲突——Type A/B
    - Part 4：传输协议

智能卡硬件

- CPU
  - 例如 8051
- 可能还有随机数发生器、协处理器
- 存储器：RAM、ROM 和 EEPROM
- 通常无源

- MIFARE Classic / Ultralight / DESFire
- FM1208
- NXP SmartMX

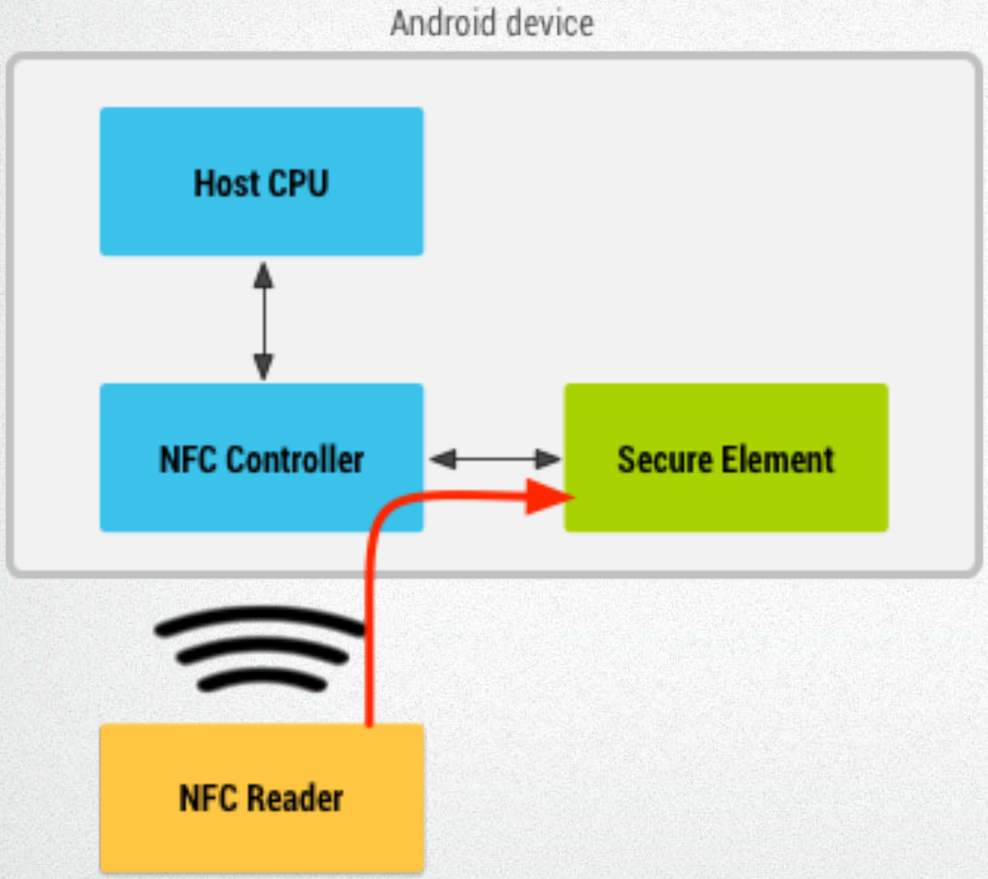
智能卡软件

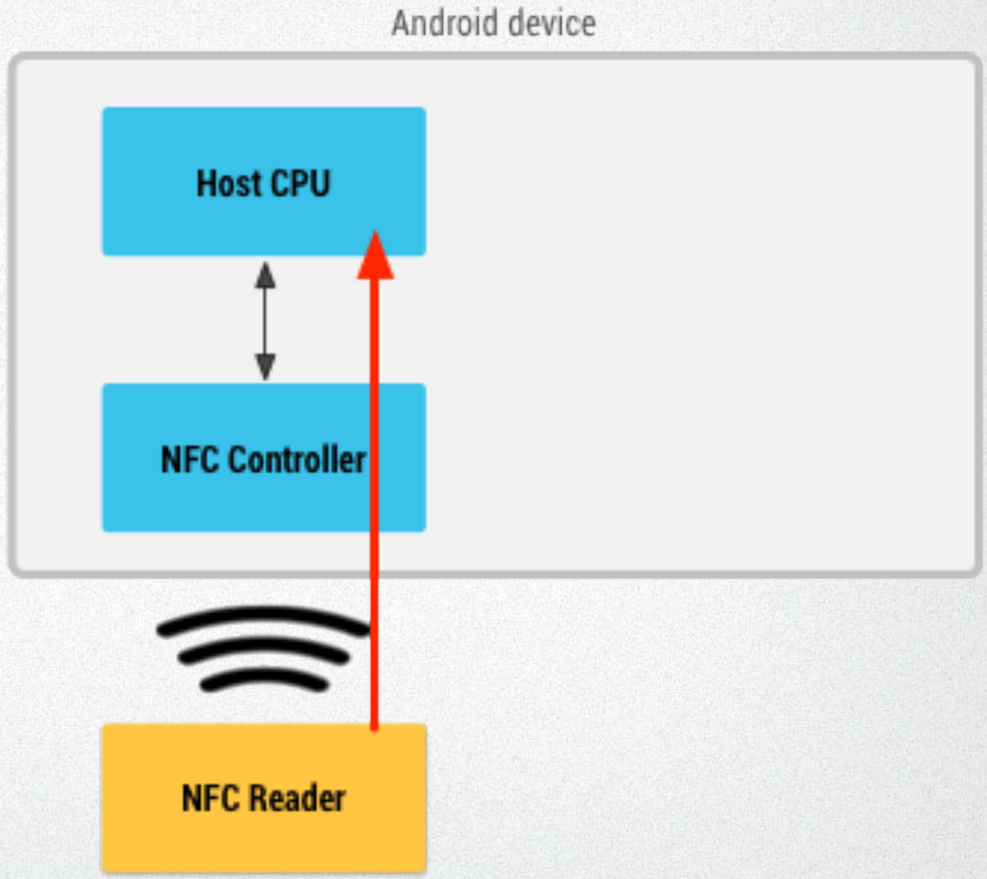
- COS
  - FMCOS / MIFARE DESFire
- 平台
  - JavaCard

什么是NFC

- 索尼、飞利浦于2002年提出
- 2013年成为ISO/IEC 18092标准
- 与14443 Type A/B、FeliCa兼容
- 三种工作模式
  - 卡模拟
  - 读写器
  - P2P

卡模拟





SD SIM eSE

一些话题

有趣的话题

01 门禁是怎么回事?

02 如何破解?

03 各种支付各种Pay

04 校园卡如何工作?

05 开始入门

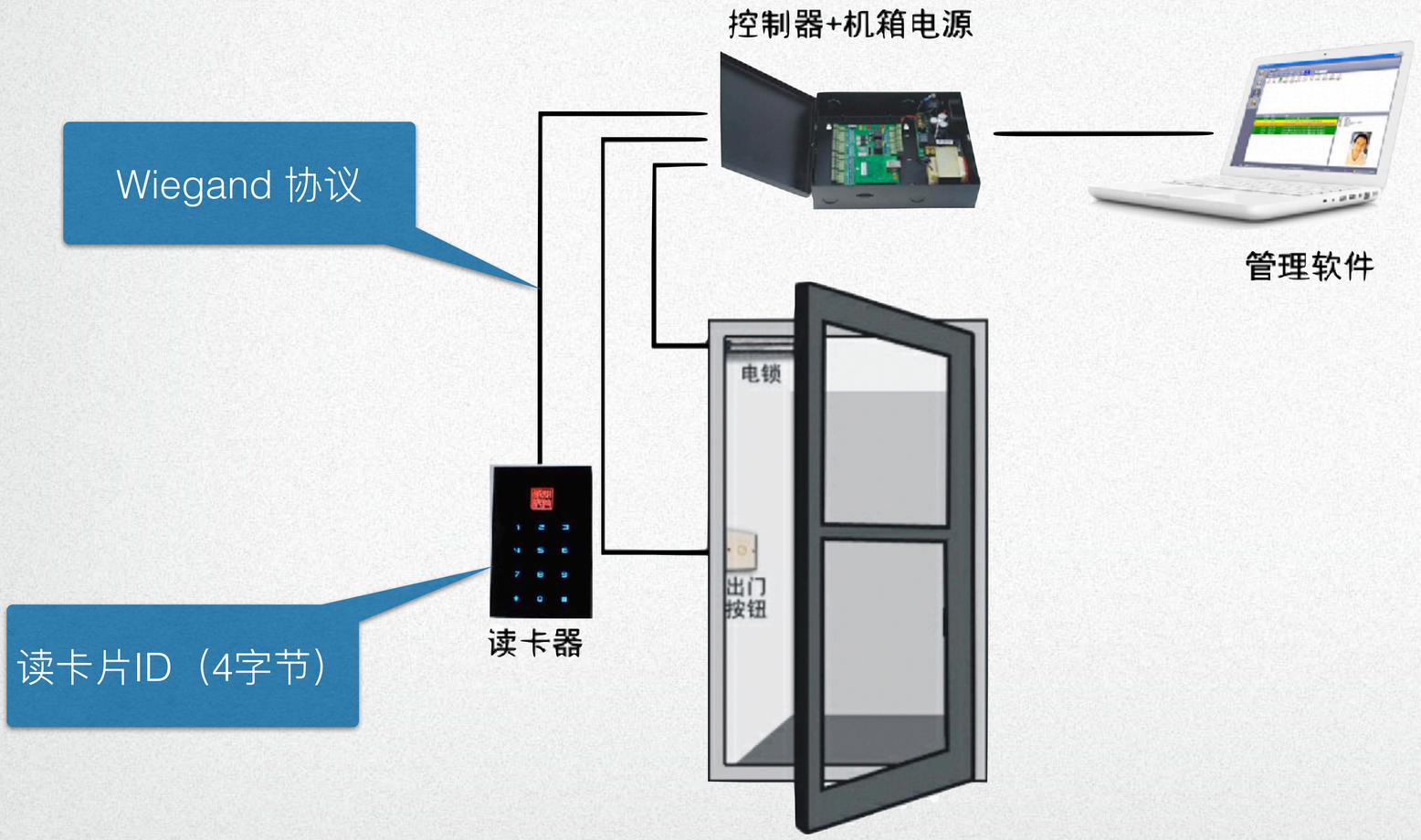
（普通的）门禁


满300个送id机器一部
复制门禁卡/停车卡/电梯卡/考勤卡/
买复制器送软件
可反复擦写
PREFERENTIAL
RECEIVE
2号id卡扣
QUALITY ASSURANCE
中 阳 门 禁


地表上最強拷貝機
熱銷
NO.1


可重复复制
双频卡
一卡两用
ID+IC
专业品质 品质保证

（普通的）门禁



卡类型：

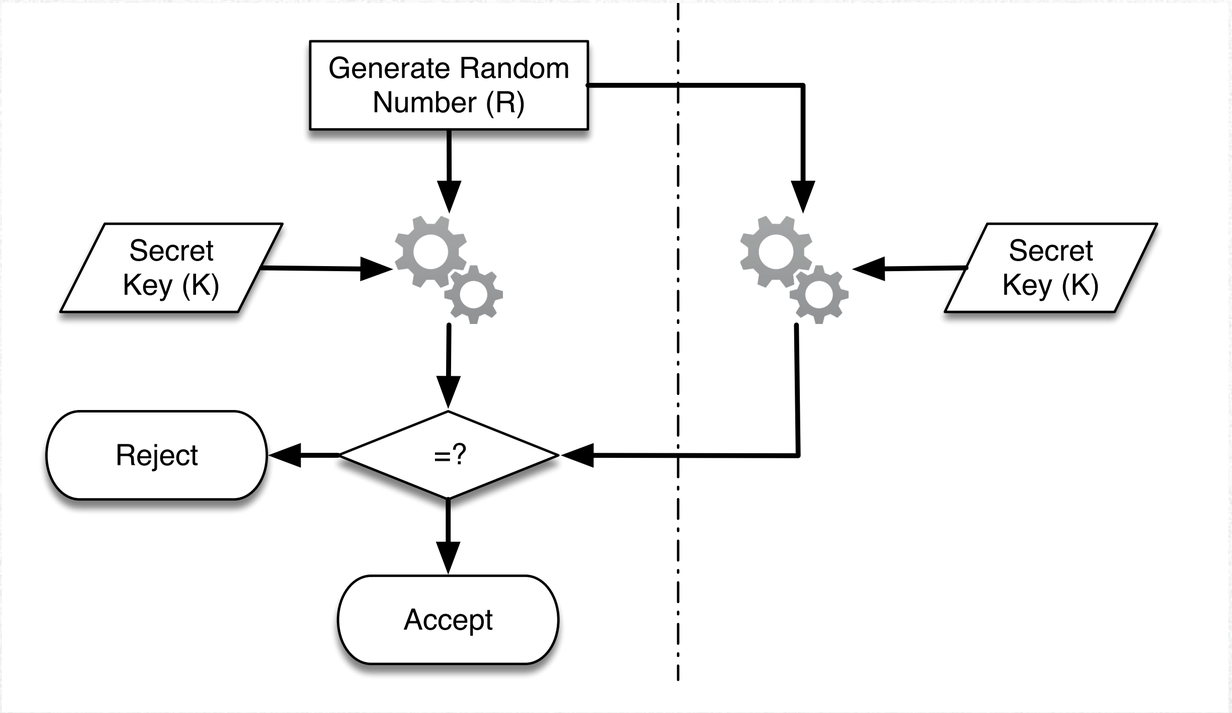
13.56MHz - Type A

125KHz - ID

（普通的）门禁

如果你的手机使用Broadcom的控制器，参考：
http://stackoverflow.com/questions/28409934/editing-functionality-of-host-card-emulation-in-android
修改UID

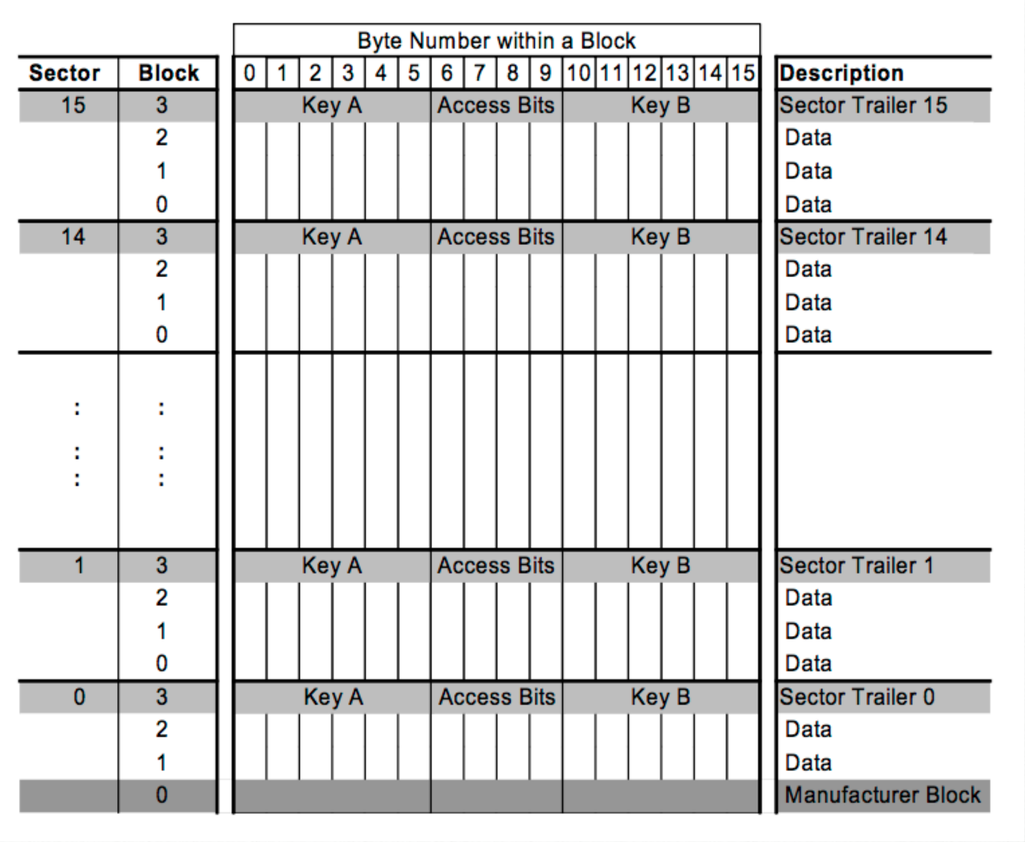
安全的门禁


Generate Random Number (R)
Secret Key (K)
Secret Key (K)
Reject
=?
Accept

如何破解?

2008年，MIFARE Classic卡被破解。破解方式为在显微镜下逐层分析电路，得到了MIFARE卡的随机数发生器的算法。

- 知道一组密钥
- 暴力破解



Sector	Block	Byte Number within a Block 0 1 2 3 4 5	6 7 8 9	10 11 12 13 14 15	Description
15	3	Key A	Access Bits	Key B	Sector Trailer 15
	2				Data
	1				Data
	0				Data
14	3	Key A	Access Bits	Key B	Sector Trailer 14
	2				Data
	1				Data
	0				Data
:	:				
:	:				
:	:				
1	3	Key A	Access Bits	Key B	Sector Trailer 1
	2				Data
	1				Data
	0				Data
0	3	Key A	Access Bits	Key B	Sector Trailer 0
	2				Data
	1				Data
	0				Manufacturer Block

如何破解?

入门工具:

mfoc

闪付

银联金融 IC 卡闪付

NFC 手机闪付

请认准银联“闪付”标识：

UnionPay 银联 Quick 闪付Pass

闪付

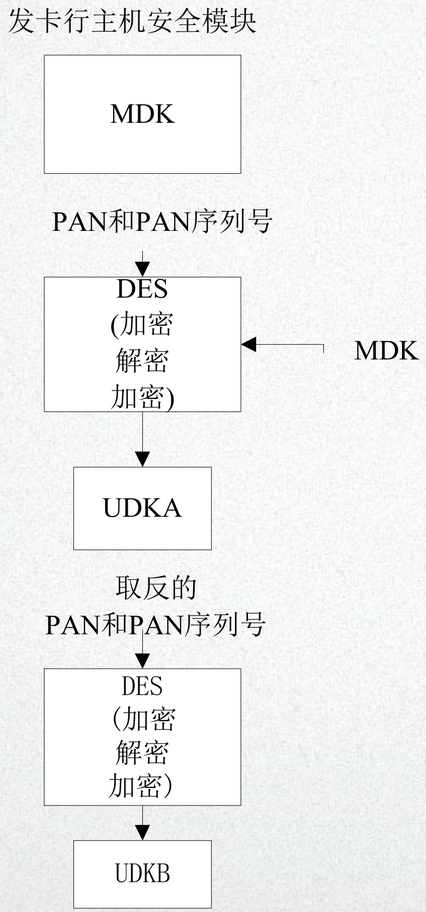
“闪付”是指符合国家金融标准的非接触式支付规范，其使用非接触式（感应式）的方式，支持借贷记功能、电子现金功能和其他应用功能。

联机

脱机

闪付（联机）

A. 密钥



B. 校验码

SK = f(ATC, UDKA, UDKB)

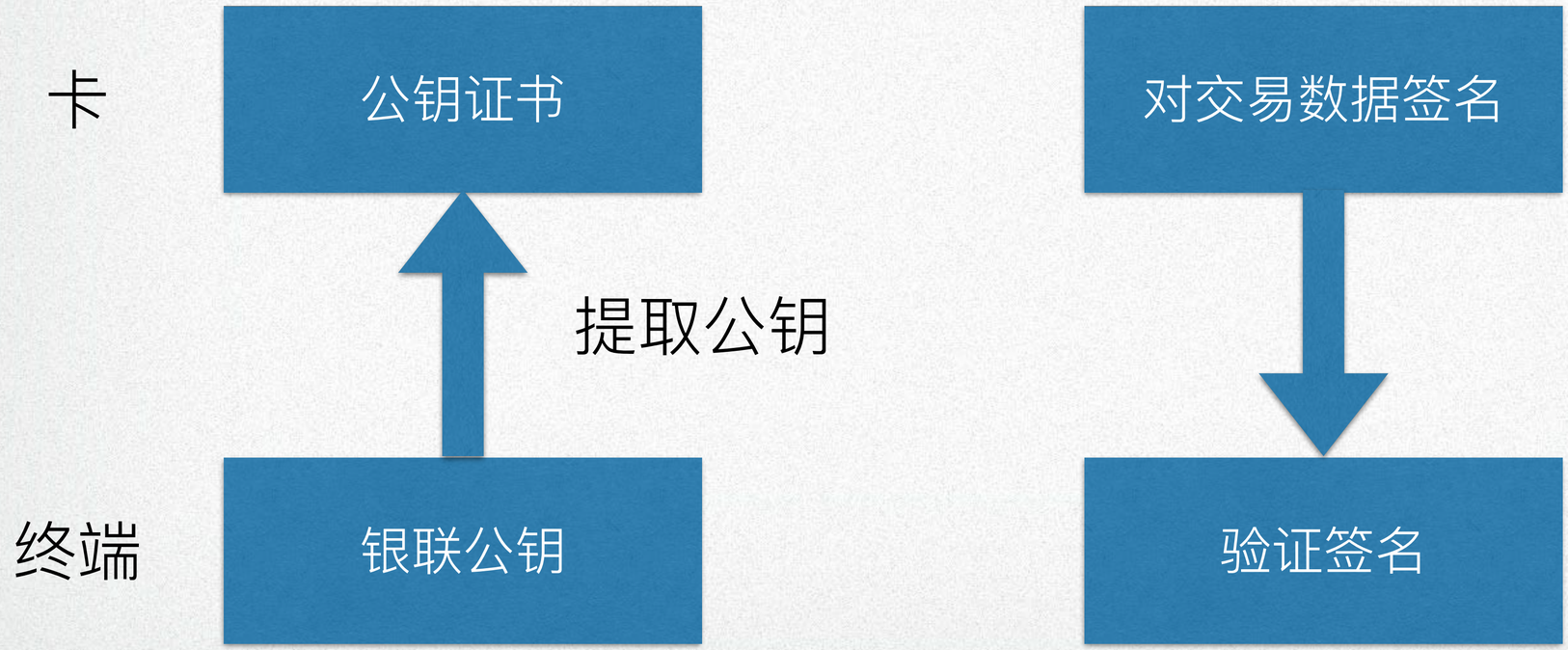
ARQC = g(交易金额, 随机数, ATC, …)

中国工商银行特约商户POS签购单
持卡人存根　　请妥善保管

商户名称:北京麦当劳华清餐厅
商 户 号:102100058140197
终 端 号:10202675　操作员号:　　22
日期时间:2016-10-09 12:02:30
收 单 行:中国工商银行　发 卡 行:63020000
卡　　号:622916******2992
有 效 期:2102　交易类型:消费
批次号:001368　凭证号:004386
系统参考号:120230034303
金额 RMB:6.00
ARQC:40E3E8996D9566A3 TSI:0000 ATC:003B
AIP:7C00 CSN:001 CVMR:020000
AID:A0000000333010102 UNPR_NO:61ED24D3
APPLAB:PBOC CREDIT TERM_CAPA:E0A9C8
TVR:0000000000
IAD:07011703A00000010D0701000000000080B0AA
E3171F
备注:电子现金余额: 0.00
IC联机批准

本人确认以上交易,同意将其记入本卡帐户
持卡人签名(SIGNATURE):
此单金额不足300.00元，可以免签

闪付（脱机）



/Samsung/MI Pay

就是一张基于eSE的闪付卡（目前仅联机）

校园卡如何工作

电子钱包（PBOC 2.0）

公交卡（Type A）

清华大学校园卡（Type B）

见同方智能卡COS手册

IC 卡		POS 机		PSAM 卡
		POS 上电、PSAM 卡上电 PSAM 卡初始化	→	初始化
		…	←	PSAM 标识符
卡片插入		…		…
交易预处理	←	交易预处理		
发卡商标识（8） 卡片应用序列号（10）	→	设置 PSAM 卡交易密钥命令 发卡商标识（8） 卡片应用序列号（10）	→	由应用序列号生成消费子密钥
命令处理	←	消费初始化命令 （DATA:密钥索引 交易金额 终端机编号）	←	返回密钥索引号
返回：卡片余额、脱机交易序号、透支限额、密钥版本号、算法标识、伪随机数	→	申请 PSAM 卡产生交易 MAC1 卡片余额、脱机交易序号、 随机数、…	→	命令处理
命令处理 验证 MAC1 的有效性	←	消费命令 （DATA:终端交易序号 终端交易日期 终端交易时间 MAC1）	←	返回终端交易序号、MAC1
MAC1 有效，返回 TAC 、MAC2，并进行以下交易处理： 从余额中扣减消费金额；卡内脱机交易序号加 1；更新交易记录	→	申请 PSAM 卡验证 交易认证码 MAC2 （TAC、MAC2）	→	验证 MAC2
卡片拔出		写交易明细 完成交易	←	终端交易序号加一，返回签名 MAC_0

开始入门

使用NFC手机：

NXP TagInfo
Banking Card Reader
NFC Tools Pro

使用PC（Windows）：

ACR 122u
mfoc
SpringCard/CardWerk API

开始入门

Smart Card Handbook
MIFARE Classic/Ultralight/DESFire Datasheet
FMCOS 2.0 Manual
PBOC 3.0
GB/T 31778

FAQ