专题讨论：

hi大家好！我叫姚刚，现在开始分享。之前看到群里分享了很多关于账务、会计、清算、对账的干货。我这次跟大家分享线下支付受理终端—POS的基本工作原理。近年来POS也不断更新换代，这里针对通用的能力做分享，有不准确的地方请大家指正。

POS（point of sale）算是一种终端，附属于计算机的一种设备。终端本身并不怎么处理程序和信息，而是将收集的信息发送给主机，由主机处理，然后将主机处理的结果反映出来。

1、POS交易。是一个过程性的概念，描述了如过程： （1）在POS上选择一种交易（消费，取现，改密等等），然后刷卡\插卡，再输入交易金额，持卡人密码等由POS提示要求输入的信息，POS将这些数据集中（打包）以某种方式发送给主机； （2）主机接收到此信息后，将它分解成原来各自独立的信息（解包），交给帐务处理程序处理，然后将处理结果（主要是一个返回码，有时可能有手续费，授权码等附加信息）再打包，发回给POS；（3）POS接收到返回信息后，解包进行相应处理（显示，打印，记POS流水等）

上面这三部分是紧密结合的，任何一部分未顺利完成，则不能算是一次完整的交易。可能是“通讯失败”、“POS出错”、“主机出错”或“数据库出错”。

图：2017-06-21 19:26:26

这是一个简单的交互图

2、交易成功。主机返回“成功”的返回码（一般是“00”），可能还有一些附加信息。例如：查询要返回余额；授权要返回授权码，有时还有“部分批准金额”（比如想取10000元，但卡上余额5000元，透支额度2000元，这7000元就是“部分批准金额”）；有时消费或取款也会返回授权码。

3、 交易失败。主机返回码不是“00”，返回码代表交易失败的原因。例如：“55”--持卡人密码不符，“03”--商户号错，“23”--余额不足等等。

4、 账务处理程序。银行主机内，对账户数据库操作的程序。这部分程序将POS送上来的数据进行实际的处理：检查信用卡是否过期，卡密码是否符合，将钱从持卡人账户中扣除，进入清算流程。

5、 前置机。在老的银行系统中，交易数据送到银行后，直接到主机，所有的处理（判断个人密码合法性，判断POS合法性，账务处理等）都在主机处理。新架构中，在银行主机之前搭建前置机，主要处理判断合法性等内容，以保证送到银行主机的数据是合法的，减轻主机负担，并担负管理终端设备（POS、ATM）的程序运行。

6、 自动冲正。当POS发送的数据被主机接收，主机已作相应的处理，但返回码因为各种原因（断电，线路故障）使POS没收到返回信息。这样POS无法知道主机的结果，于是会发冲正给主机，主机将相应交易置为无效，并返回信息告诉POS完成冲正。具体有两种实现：1. 一笔交易未收到返回信息，则一直发冲正，直到成功为止。2. 未收到返回信息，可按“取消”键退回主菜单，这时可作一些脱机交易（比如IC卡），因此后者有较多的优势。

7、POS流水 即“POS流水账”。POS完成一笔成功的交易（即引起银行帐户内金额改变，比如：消费，取款，存款，转帐），这种交易必须确保不出错。为此在POS内将这笔交易的内容（卡号，金额等等）记录下来，以备在结算时再与主机核对，或者供人工查询。

8、 POS结算 一般是在“日终”进行，主要目的是将POS在这一天所做过的转账类交易与主机上的记录核对一次，然后把POS流水中的记录删掉，供第二天使用。结算时一般核对该POS交易的总金额和总笔数，若POS总金额和总笔数中的某一个与主机不同，主机返回“核对不平”，POS就必须进行“批上送”，虽然这样不能检查出所有的错误，但是在自动冲正等安全措施保证下，结算时出错的概率已相当低，正好总金额和总笔数还相同，这种概率更低。 大家可能觉得每日POS结算时全部进行交易批上送比较安全，但这种方法实操性不强，POS一日的交易量会很大，一次批上送时间很长体验会较差。

9、 批上送 结算核对不平时，POS将流水逐条送到主机，主机逐条核对，作相应处理，然后POS才能删掉POS流水。在批上送结束之前不能作联机交易。一般来说，POS记录的金额就是实际的交易金额，人为修改也不可能，而主机上的数据虽有各种措施尽量保证数据的正确性，但不可能绝对正确，数据库也可能被人为修改，所以在核对数据和批上送时，大多以POS数据为准。但更保险的做法，是将POS与主机对不上的交易另外记录到一个数据库中，然后等待商户将打印票据送回，再由人工核对。

10、同步通讯协议 与 异步通讯协议 通常说的POS可以走同步、走异步就是指可以使用这两种通讯协议。 我们知道数据通讯就是两个通讯者之间发送、接收数字信号。假设发送以下一串数据： 12，23，34，45，56，67，78，89接收方要正确的接收这些数据，就必须知道数据什么时候开始，什么时候结束。否则会将信号收错。对于同步通讯协议，发送方在发送数据之前先发送一特殊的电信号，让接收方准备好接收数据，然后发送方就将以上数据连续发出，全发送完毕，再发送另一特殊的电信号表示结束。对于异步通讯协议，发送方每发送一个数值之前都发一“开始”标志，每个数值发送结束都发送一个“结束”标志。

11、8583数据格式 发送方发来的串数据，接收方如何能知道哪部分是卡号，哪部分是交易金额。因此通讯双方必须约定，比如：前16个数据是卡号，然后8个数值是密码······，当然8583数据格式没有这么简单，它是一种复杂的数据组合。8583数据格式是一种国际标准，它规定了金融交易的某些数据是必须在数据包中出现，但有些数据可出现也可不出现；数据包中某些部分被规定给某种数据使用，但还有很多部分的用途可以自己定义。

12、打包 和 解包 各种数据（卡号，密码等）原来是分散存放的，在发送之前，必须按数据格式的规定，将这些分散的数据联成一串连续的数据串，这就是打包。接收到连续的数据后，要使用某一数据，必须按照数据格式的规定从数据包中将这一数据分离出来，这就是解包。

13、网控器NAC 网控器主要有两个厂家：澳大利亚的Hypercom；香港的“瑞伯科技”。瑞伯科技的网控器类似Modem，每一块板都对应一个下行口（用电话线与POS相连）、一个上行口（用串口与主机相连），这种网控器市场上使用较少。 市场上主要使用Hypercom公司的NAC6/16，它的上行线路（与主机相连）一般只有一条（一块上行板），最多扩充到两块上行板足够用了，而可以管理十几个下行板（用电话线与POS相连）。这样能节省主机的端口，而又能同时允许十几台POS与下行板通讯，不致拨号老是占线，提高POS系统的使用效率。

14、持卡人密码 通常是6位数字（明文）。密码要送到银行主机内核对，在密码的传送过程中不能被其他人获得密码明文，因此在密码明文输入后就必须一直以密文的形式存在，就算是银行核对密码也是核对密码密文。 POS使用银行卡，持卡人在密码键盘上输入密码明文，从密码键盘出来的数据就是加密过的密码密文数据，这样在密码传输过程中就算被截取，也无法获知密码明文。

15、加密和密钥 密码明文转化为密文的方法就是秘钥。保护密钥不被他人获知，POS一般将密钥放在密码键盘里，密码键盘具有开机自毁功能，当企图获取密钥的人打开密码键盘机壳时，密钥将自动丢失。

Q1：POS里存的密钥是银行给的公钥吧

A1：不是。是终端主密钥。分为收单机构的和银行的，收单机构后面再发送银联。收单POS里存的一般叫子密钥，收单机构还有主密钥

A2：一般收单机构都自己有一套密钥系统，然后罐装到pos. 一个是为了防止pos程序被篡改，另一个为了对8583数据加密

Q2：麻烦问一下，关于POS这一块，银联是怎么给收单机构做资金的清结算的呢？资金流是怎么走的啊？是通过大小额做银行间清结算 然后再由备付金行结算给收单机构吗？

A1:都是银联清算的, 银联清算有3种模式.

第一种，收单行清算. 也就是资金给收单机构的开户行。然后再由收单机构清算给商户

第二种是结算行清算. 是统一结算给代理结算银行，再由代理结算银行清算

第三种就是银联小额入账，收单机构需要与银联签订代理清算协议，资金直接清算给商户.

Q3: 第一种模式的话，资金是通过收单机构的开户行实时入账给收单机构吗？银联需要在收单机构主备付金行做一个中间户吗？

A1: 不用啊，银联也是通过人行大小额系统啊

A2: 那也就是说： 1、结算给收单行，采用第一种模式 2、结算给收单机构，采用第二种模式 3、直接结算给商户，采用第三种模式

Q4: POS需要与多个银行或收单机构交互 实时下载别人的公钥就可以实现加密传输?

A1: 做不到实时的....必须罐装到pos.

Q5: pos里8583加密des貌似不是标准的des？

A1: 之前研究过8583算法，都是可以套用标准DES算法的

Q6: 现在建行的8583 64域就卡住了，不知道咋算的?

A1: 64域我记得是计算mac签名吧，要调用两次des算法。数据也要对才行

文档：中国银联银联卡受理终端应用规范 第1部分 销售点终端（POS）应用规范

A2: 按照文档加密算法做就好了，如果有硬件加密机估计简单点

A3：首先是两种加密吧，一种是终端到收单前置的加密，这个前置机一般有加密机解密，终端内部的加密是终端厂商根据终端主密钥和签到密钥加密上传前置机的

A4：Pos终端中的主密钥、工作密钥、pin密钥、mac密钥 - 百度文库 https://wapwenku.baidu.com/view/a10b8f6ecc1755270622085a.html?ssid=0&from=1012852r&uid=0&pu=usm@1,sz@320\_1004,ta@iphone\_2\_7.0\_11\_8.9&bd\_page\_type=1&baiduid=52B4074F2709EC36F13FCA23AA8725F7&tj=wenkuala\_2\_0\_10\_l1#1

一：聚合支付

Q1：聚合支付占有量大的是哪几家？

A1：线下的主要是哆啦宝和收钱吧

A2：ping++做的是聚合支付，品付也是

A3：最大的阴影聚合商是威富通，游戏虚拟类，交易量比较大的有爱贝

二：银联二维码

Q1：是否有学习资料？

A1：https://open.unionpay.com/ijweb/product/detail?id=181

https://open.unionpay.com/ajweb/index

https://static.95516.com/static/help/index.html

https://open.unionpay.com/ajweb/help/qrcodeFormPage

A2：文档（请群主帮忙）

中国银联二维码支付应用规范（QCUP 053-2016）.pdf

中国银联二维码支付应用规范（QCUP 053-2016）(1).pdf

二维码支付产品改造指南.doc

Q2：百度要接银联二维码吗？

A1：类似京东与银联对接的形式

三、银行存款余额调节:表

Q1：银行存款余额调节表 调节后的余额是该企业对账日银行实际可用的存款数额？

A1：余额调节法：是在银行对账单余额与企业账面存款余额的基础上，各自加上对方已收本单位未收账项数额，减去对方已付本单位未付账项数额，然后编制“银行存款余额调节表”验证经过调节后的存款是否相等的方法。如果相等，表明企业和银行的账目没有差错

A2：这个是资金系统是应付未付，都是在银行流水文件里面可以统计计算的

Q2：银行存款余额调节表 调节后的余额是该企业对账日银行实际可用的存款数额? 实存余额难道不是可支配的？

A1：就是统计一下未达款项，核对公司的账与银行账的差异，然后把差异注明原因，一般是财务部处理的。最终银行账面余额和公司会计账面余额需要一致，也可以在清结算系统出具银行余额调节日报。

Q3：我知道是统计未达项，但是为啥要拿 银行对账单余额与企业账面存款余额的基础上，各自加上对方已收本单位未收账项数额，减去对方已付本单位未付账项数额

A1：简单说就是存在在途资金，双方没有及时入账。就是入账时间不一致，还有就是你们没有及时入账。

图：2017-06-21 16:30:32

Q4：1.银行已收企业未收：银行已收到款项，回单未出，企业未入账 2.银行已付企业未付：银行已经扣款，回单未出，企业未入账 3.企业已收银行未收和4.企业已付银行未付呢？

A1：就是看一下你们账面的余额和你们实际的银行余额

Q5：银行对账单存款余额+企业已收而银行未收账项－企业已付而银行未付账项？

A1：公司在银行存款核对过程中可能经常会出现银行存款的日记账（账面的）和银行对账单（实际的）余额不一致，其原因除记账错误以外，还可能是由于未达账项引起的。

未达账项是指你们公司与银行之间，由于凭证（票据）传递上的时间差（对于清结算系统就是可能是你们系统和渠道反馈信息同步的时间差），导致一方已登记入账，而另一方尚未入账的账项。

A2：从你方系统和银行系统来看，有四种排列组合：

你们系统已经收款入账，而银行尚未收款入账；

你们系统已经记录付款入账，而渠道侧尚未付款入账；

银行侧已经收款入账，而你方尚未收到收款入账通知；

银行侧已经付款入账，而你方尚未收到付款通知；

那经过这样的调节后 理论上双方的余额就会平的。说个大白话，就是一笔交易就是你们会计要么早记账了 要么就是晚记账了 也就是你们会计在还么有收到银行的钱 就记账了 或者你们支付出去的钱 银行还没有支付出去 你们就已经记账了

A3：我们以前的做法是宁可记晚了，别记早了。记错了一堆麻烦，我们一般是后一天下班前把前一天的账记了就行。偶尔有退款，红冲还可以接受**。**不然一堆红冲的，哭死。不过这可能适合大额交易，小件因为晚记账会耽误效率。

Q6：对于一般企业来说，对接第三方支付(比如支付宝或者微信)，要做账面余额和商户的余额的核算，这个麻烦吗？

四：冲退

充退和退款的状态都属于退款，但充退的分类是在充值的下面。换句话说充值也有退款的状态就是充退。其实充退在我看来就是提现，都是出金业务。

五：支付路由

Q1：图2017-06-21 18:34:57

问题如图，就三个支付通道，假设只考虑支付费率与支付成功率，三方支付的B2B支付通道，如何实现路由？

A1：我计划做一个规则配置页面，把规则涉及要素的优先顺序进行配置好，然后规则与支付渠道进行关联。

A2：图2017-06-21 18:42:21

A3：老王开店和支付路由管理 - 知乎专栏 https://zhuanlan.zhihu.com/p/20060139

A4：就三个银行三个通道，手动是不是更好些，看谁家给的回扣多就用那家的

A5：我以前接触过不少P2P客户，他们用那家通道，都是看心情的，谁家这个月送卡了，就切点量过去

A6：我觉得如果规则仅取决于：业务，银行，通道，交易限额，交易成本这些相对静态的要素，路由是好设计的；如果要参考通道承载量、通道总限额、随规模而变的交易成本等这些动态要素，设计起来就比较复杂。

A7：你说的对，只有大量同类交易需要复杂通道属性判定的，需要动态路由，一般三条通道，其实手动更好，静态的也比较简单

Q2：B2B企业网银的支付过程有制单和复核，确实很难判断成功率问题，你这边有什么的方法吗？

A1：这种跳转银行页面的支付，除了在操作上提示客户操作步骤以外，没什么好办法，比如要求他先插U盾，还是限定什么浏览器之类的

A2：b2b业务涉及复核，支付成功率线上统计没有意义

六：OFO退款

Q1：请教个问题，退款的，如果我OFO的押金是通过支付宝绑定招行信用卡支付的，过了400天，我想退OFO的押金，这个时候是退到我招行的信用卡，还是OFO的现金账户，还是支付宝的余额账户。有其他的可能性么？

A1：信用卡，哪来的回哪去

A2：找不到原卡，应该退回失败。