支付系统设计：银行卡支付（三）

这一期，回到支付系统的核心业务，即支付。每个电商公司的支付系统都已经或多或少的实现了交易核心功能，可也都是一直在改进，总是不断的有新的需求冒出来。所以这一期开始，我们梳理一下：到底有哪些支付方式？每种支付方式都是怎么运作的？

支付和交易

说到支付就不得不提交易。这两个概念在不同公司中是不一样的。我们的定义是，交易是生成订单；支付是对订单进行付款。 订单生成过程我们以后另开话题来说。这一次重点介绍支付。而就支付行为来说，我们碰到的大部分都是单次支付，其次还有转账和退款。在苹果推出订阅支付后，国内支付宝等也在陆续跟进。 单次支付是我们用的最多的支付方式了，即一次结清所有款项。把单次支付走通了，其他支付方式也容易处理。 本期重点介绍单次支付。

银行卡支付

先说大家比较熟悉的银行卡支付，它分为线上支付和线下支付两种形式。线下支付就是通常说的 POS 收单，这里不介绍这个内容。对线上支付，按照卡的类别，分为贷记卡支付，也叫 motopay、ePOS，即信用卡支付；和借记卡支付。按照支付形态，又分为认证支付、网银支付、快捷支付几种形态。银行卡网银支付要求银行卡必须开通在线支付功能，而快捷支付并不需要开通在线支付功能。主要利用支付验证要素（卡号、密码、手机号、CVN2、CVV2 等），结合安全认证（例如短信验证码），让持卡人完成互联网支付。

认证支付

指用户在绑卡时，将卡信息提供给电商。这样在支付时，用户无需再输入这些信息，由电商在服务器侧保留用户的账户信息，比如身份证号，卡号，手机号。在用户支付时，无需再输入这些内容，最多就提供个密码或者校验码，就可以完成支付。这基本不会打断用户的使用体验，所以也是电商喜欢的支付方式。但认证支付最让人诟病的就是安全性。一方面需要向电商暴露个人信息，一旦被窃取，资金就容易被盗走。还有在手机上执行支付，一旦手机丢失，窃取者就可以轻而易举的使用或者转移资金。

快捷支付

快捷支付和认证支付类似，不同点在于绑卡之后，有些银行接口会返回 token，后续使用 token 来作为支付凭证，无需提供卡号信息，这样电商也不需要本地保留卡号了。目前主要是银联有提供 token 接口。

网银支付

相对来说，网银支付要安全很多。网银支付是由银联或者银行提供支付界面，用户必须在页面上输入卡号，密码等验证信息才可以执行支付。大部分银行还要求用户使用 U 盾或者其它安全硬件。但安全和易用永远是个矛盾。网银使用会打断用户体验，增加用户使用难度。对使用硬件加密的支付，不可能天天带着 U 盘跑。另外网银主要用在 web 端，在手机端，嵌入网银页面，还是比较难看的

支付流程

走一个具体的例子看看吧。比如用户在电商系统中买了 200 块钱的东西，然后通过浦发银行卡做结算，用的是快捷支付。这个过程是：

用户在交易界面上，提交订单到交易系统中； 交易系统确认订单无误后，请求支付系统进行结算。这是在交易系统做的，后面工作就进入支付系统。

用户被引导到收银台页面， 让用户确认交易金额，选择支付方式，调用支付系统接口。

支付系统接收到支付请求，验证请求的各个字段是否有问题，确认无误后，调用支付网关执行支付。

支付网关请求浦发银行的快捷支付接口执行支付。

支付网关接收到支付结果报文后，对结果报文做解析，获取结果，并将结果告知交易系统。这可以通过 URL 或者 RPC 调用来实现。

商城系统收到支付结果后，开始执行后续操作。如果是支付成功，则开始准备出库。这一步在交易系统中处理，这里不做介绍。

网银支付，和快捷相比，就在第 4 步，插入一个步骤，将用户导航到网银页面输入支付信息，后续步骤是一样的。在资金流上也是相同的。 而在第五步获取返回结果上，一般银行就直接同步返回，银联是分为同步和异步返回。同步告知操作成功或者失败，异步告知扣款成功或者失败。同步操作和异步操作都需要调用方提供一个回调的 URL 地址，银联会将参数附加在这个地址上。通过解析这些参数可以得到执行结果。异步操作一般有 2-3 秒的延迟，取决于网络，以及该交易处理的复杂度。

资金流

上一节说的是支付的信息流，那资金流应该是怎么走的？ 在第三步，会触发资金流。资金从用户个人账户上转移到电商公司的账户。当然，银行也不是活雷锋，这一笔交易是要收手续费的。资金是实时到账的，手续费一般是按月结算。有按交易笔数计费的，但大部分还是按照交易金额来收费。

同行快捷支付是比较简单的场景，让我们来逐步增加难度。如果支付系统没有对接浦发银行，那对浦发卡，就得走其它支付方式：银联或者第三方支付。

先说银联快捷。银联提供的多种接入方式，常说的快捷支付，在银联文档中叫商户侧开通 token 接口。通过这个接口，可以实现同行和跨行资金结算。不管收款行是浦发还是其它行，都可以完成结算。对本地和用户来说，体验是一样的。而在银联侧，后台资金流处理却不一样。了解这个资金流，有助于在异常情况下，了解资金到底跑到哪里了。

如果收款行也是浦发银行，银联发报文给浦发，浦发使用内部系统完成两个账户间的转帐，即时完成。

如果收款行是他行，比如工行。银联发指令给浦发和工行，分别完成各自账户上资金余额的增减，对个人和电商来说，这笔资金算是落地了。但实际资金流并不是立即发生。银联会在半夜做清结算后处理这笔资金。这个过程就是金融机构之间的清结算了，一般不需要关注。

如果使用的是第三方支付，对用户来说，处理的流程和银联一样。但资金流会不一样。第三方支付在浦发和工行一般都会有落地的托管资金。 发生交易后，一般来说不会产生跨行资金流动。用户在浦发行的钱会被结算到第三方支付在浦发行的托管账户，而在工行的钱，会由第三方支付在工行的账户打到客户账户上。 这就降低了跨行资金流动成本。

目前国内主要银行都提供快捷和直联的接口。对电商来说，要对接哪些银行是个需要考虑的问题。怎么对接银行，渠道和第三方支付。

银联 Token 支付

一般来说，大部分银行都提供直联和网银接口，但不需要直接对接所有银行。银联和第三方支付也提供直联接口，可以直接对接国内主要银行。也不是所有银行都被银联支持，这和银联签约的接口有关，需要在对接时咨询银联。从我们使用情况看， 浦发借记卡、邮储银行卡是不支持的。 另外 交行、平安（含原深发）、上海银行、浦发、北京银行，上述银行卡需通过 这个地址 开通银联在线支付业务。

对接银行

大部分银行提供的银行卡支付接口，借记卡支付和贷记卡支付是不一样的。但也有几个好心的银行，可以用一套接口同时开通借记卡和贷记卡。点名赞一下这些银行： 宇宙第一大行工商银行和建设银行。其他同学对接中如果也发现借记卡和贷记卡用一个接口的，也请及时告知。 作为国内最保守的软件团队，和银行对接时务必做好足够的准备。在商务谈判完成、拿到银行的接口文档后，需要考虑两个问题：专线问题、加密问题。

专线问题

首先是专线问题。 大部分银行对接是需要专线的。 与银行沟通的时候，注意收集如下信息：

专线类型： MSTP 类型或者 SDH 类型。
专线接入点：目前国内主要是联通、电信。
封装类型： HDLC 或者 PPP
专线代宽：默认是 2M

前置机 IP，这个需要在银行侧和电商侧进行配置。 专线其实是在银行和电商之间建立一个局域网，需要双方分配通讯 IP。 其实这两组 IP 都是 NAT 后的 IP，银行分配给我们的是电商真实的前置机 IP 经过最外端的网络防火墙转换后的 IP 段，后者也是对方的真实前置机 IP 经过转换后的 IP 段。 出于安全考虑，双方都不会将真实 IP 暴露出去，所以要 NAT。

接入地址：即电商这边机房的地址。

这些专业名词，可以自己检索，太专业了，其实我也不懂。从可靠性角度考虑，一般建议从联通、电信各拉一条线路出来。一旦有一个线路出问题了，也不会导致所有交易被终止了。不需要专线的银行接口有：浦发、工行、交行信用卡等。 需要专线的有中行、农行、建行等。一般专线需要 1 个月左右的时间，包括银行侧的申请、施工时间。

加密问题

其次是加密问题。部分银行，如中行，前置要求使用加密机。此处加密机的常用功能有三方面：

MAC 加密（完整性）；
支付会话\密码加密（安全性）；
密钥交换加密（防截取）。

对开发来说，加密机的主要作用，是让黑客都无法从内存中看到密码。 不是做广告，国内对接银行一般就用江南天安的加密机了

对接银联

对接银联比对接银行简单， 不需要专线，不需要加密机。 不过需要获取 ADSS 认证。 银联最近在推 Token 接口，有两套接口，一套是银联侧开通，一套是商户侧开通。前者类似网银支付，后者类似快捷支付。 务必要求接入后者接口啊。基本上读完接口文档就知道怎么写代码了。

接下来，这里将分别介绍如何对接第三方支付、应用内支付等内容。敬请关注。

相关阅读

支付系统设计：支付系统的账户模型（一）

支付系统设计：对账处理（二）

作者：凤凰牌老熊，程序员 & 架构师，来自中科大的本科，研究生在软件所学习。先后在中科辅龙、三星（中国）研究院和国内一些大型的互联网公司呆过。在中科辅龙公司负责电子政务内容管理系统建设，负责研发龙驭系列产品的研发，这款产品最终实施到 2000 多个电子政务网站上，期间也参与了一些支付反洗钱以及支付系统的建设。之后在三星中国研究院，负责自然语言处理（NLP）以及智能家居相关项目。智能家居项目在 2014CES 消费电子展上作为三星重点项目推介。2014 年开始加入爱奇艺公司，负责数据仓库和支付系统的建设。

本文由@凤凰牌老熊（微信公众号：shamphone） 原创发布于人人都是产品经理 。未经许可，禁止转载。