支付系统设计：绑卡、签约和身份验证（四）

在上一篇 支付系统之银行卡支付中，挖了个坑，就是关于绑卡的坑。 在用户使用银行卡做支付之前，首先需要完成绑卡的操作。怎么实现绑卡，怎么验证用户绑的是自己的而不是隔壁老王的卡，这就是本期的重点。

为什么要求用户绑卡？这和快捷支付有关。参见上一篇文章的分析，绑卡是将用户卡信息提供给电商，以后电商就用这个信息去银行完成支付。绑卡实际上是一个授权，让用户允许商家自动从他的账户上扣除资金。所以绑卡也叫签约，用户和银行，商家的三方签订的支付合约。 但我们知道，绑卡对用户和商户来说都存在巨大风险。

如果说用户绑卡是图省事，那商户为什么要做这个事？首先当然是提升用户体验了，让用户花钱更容易。其次，提升支付成功率。使用网银支付成功率在 20%左右，银联直联成功率一般在 50%左右，银行卡直联可以提升到 70%左右。这是相当可观的数据。所以，当你看到绑卡送洗衣粉之类做法时，不需要担心商家会不会赔本。

怎么绑卡？我们知道对接银行有两种途径，直接对接银行接口和通过银联来间接对接。这两种情况下绑卡处理也不同。

绑卡场景

直观的，电商网站会在用户后台提供一个绑卡的入口，让用户直接绑卡。以支付宝绑卡流程为例，我们可以体验下：

这里有如下要点：

只能绑自己的卡，这主要从安全角度考虑。
需要用户在银行侧预留的手机号进行短信验证。但不是所有银行都需要。这个时候，为了统一处理，可以考虑自己发验证短信。

对这个入口不要指望太多，更多的用户是在支付中绑卡。也就是提交订单后，发现没有银行卡了，就开始绑卡。 和纯绑卡流程不同的是，最后一步，绑卡成功后，一般都同时完成支付。有些渠道会提供绑卡并支付的接口，减少交互次数。

绑卡流程

先介绍比较简单的银联直联绑卡。为了保证卡的安全，绑卡有这些前置需求：

用户必须已经绑定了手机号。该手机号用于修改支付密码；
用户需设置了支付密码。支付密码不同于登录密码。

针对用户不同状态，绑卡流程上有区别。当然，绑卡是安全操作，要求用户必须登录到系统中。为了避免和服务器端的交互被劫持，所有操作必须在安全链接中进行，即使用 https。当用户开始绑卡时，执行如下流程：

检查用户是否有手机号。没有则进入设置手机号流程。
检查用户是否设置支付密码。如果已经设置，则需要用户输入密码。确认后开始绑卡。否则，也是先进去绑卡后设置密码。
用户输入卡号，系统根据卡号判断卡的发卡行，并显示给用户。有些实现，如微信支付，会提供扫卡识码功能。
用户输入银行预留手机。对于没有绑过卡的用户，需要用户提供真实姓名和身份证号。对于信用卡，还需要输入 cv 码和有效期。这一步，卡的信息都收集全了。
调用银行绑卡验证接口进行绑卡。这里有一个四要素验证的概念。由于国内要求实名制，所有银行卡都是实名办理的，所以银行可以验证姓名，身份证号，银行卡号和手机号是不是一致的，如果没问题，则会发短信到手机上。
用户输入短信验证码并确认绑卡，服务器端将用户实名信息以及短信验证码组合形成报文，发送给银行，执行签约操作。银行侧签约成功后，返回签约号给商户。

卡 bin

这里有个问题，如何根据卡号判断发卡行？这就需要卡 bin。 BIN 号即银行标识代码的英文缩写。BIN 由 6 位数字表示，出现在卡号的前 6 位，由国际标准化组织（ISO）分配给各从事跨行转接交换的银行卡组织。银行卡的卡号是标识发卡机构和持卡人信息的号码，由以下三部分组成：发卡行标识代码（BIN 号）、发卡行自定义位、校验码。

目前，国内的 银行卡 按照数字打头的不同分别归属于不同的银行卡组织，其中以 BIN 号“4”字打头的银行卡属于 VISA 卡组织，以“5”字打头的属于 MASTERCARD 卡组织，以“9”字和“62”、“60”打头的属于中国银联，而“62”、“60”打头的银联卡是符合国际标准的银联 标准卡 ，可以在国外使用，这也是中国银联近几年来主要发行的银行卡片。 大部分银行卡号前 6 位即可确定发卡行和卡类型，但也有非标卡需要 6-10 位才可以判断出来。需要维护一个卡 bin 库。附件是一个比较完整的卡 bin 库， csv 格式的。

短信和身份验证

一般绑卡操作第五步需要银行下发短信验证码。 短信验证的接口，不同银行还不一样。有些银行是短信和身份验证一起做了；有些银行是可以配置身份验证是否同时发短信。还有些比较奇葩的机构，比如某联，接口中让你传身份信息，但实际上没传也是可以的，也不验证身份信息到底对不对。这在对接渠道时需要特别注意。

此类接口一般包含如下内容：

版本号：当前接口的版本号；
编码方式： 默认都是 UTF-8，指传输的内容的编码方式；
签名和签名方法： 生成报文的签名。 不是所有的字段都需要放到签名中，文档中会说明哪些字段需要签名；
签名算法：生成签名的算法，RSA， RSA128， MD5 等。
商户代码：在渠道侧注册的商户号。
商户订单号：即发送给渠道的订单号；
发送时间：该请求送出的时间。
账号和账号类型： 银行卡、存折、IC 卡等支持的账号类型以及对应的账号；
卡的加密信息：如信用卡的 CVN2，有效期等。
开户行信息：开户行所在地以及名称；大部分是不需要的。
身份证件类型和身份证号： 可以用于实名验证的证件，指 身份证、军官证、护照、回乡证、台胞证、警官证、士兵证等。不同银行可以支持的证件类型不一样，这也不是问题。大部分就是身份证了。
姓名：真实姓名，必须和身份证一致；

手机号：在所在银行注册的手机号。

系统会返回上述数据的验证结果。如果验证通过，则会发短信。但这不是所有的渠道都是这样。哪些字段会参与验证、需不需要发短信，需要注意看接口文档。

绑卡接口

绑卡接口和发短信接口类似，还需要将用户的卡号，身份证等信息传递过去。在绑卡成功后，会返回一个签约号。这个签约号是后续调用支付，解约等接口所必须的。 这里有个问题，已经绑卡的用户，调用绑卡签约接口再绑一次，会出现什么情况？这个和银行实现有关。 大部分银行，如农业、浦发、建行等，对绑卡签约接口调用，会首先验证身份信息，如果验证不通过，则不执行后续操作。验证通过后，再检查这个卡在该商户下是否已经绑过了， 如果没有绑过，则执行绑卡，否则会提示卡已经绑定过了，不能重复签约。但工行的实现不一样，他是首先验证这个卡是不是已经绑过了，如果已经绑卡，则不继续验证身份信息。 总之，银行都不支持重复绑卡。

银联绑卡

银联直联绑卡和银行绑卡类似，但是得注意验证接口，仅验证卡号和姓名，不验证身份证号和手机号。这导致第 5 步无法正常进行。银联只有到第六步执行绑卡时才做身份验证。所以在处理上，还需要做一些调整，来确保和银行的流程的一致。 一种处理方法是，对银联，在第五步就开始调用银联接口执行绑卡操作，但是在本地标记为预绑卡状态；商户侧发送短信验证码，验证通过后，才将状态设置为绑卡成功。

银联网银绑卡处理起来比较麻烦。用户在电商页面上输入卡号，然后被导航到银联页面上去完成绑卡操作，成功后，银联返回一个 token 作为签约号，用于支持后续操作。这问题就来了，用户可以在银联页面上绑定一个别人的卡，而电商侧是无法知道这个卡的情况的。所以这种方式尽量不要用。

实名认证

绑卡操作有个不错的副产品，就是实名认证。常说的二要素，三要素，四要素认证，可以通过这个操作完成。 二要素指姓名和身份证号，三要素加上银行卡号，四要素则加上手机号。看起来，似乎银行都应该支持四要素验证，但大部分银行接口仅支持三要素，毕竟手机号还是非常容易变。 当然，实名认证，也就是二要素认证，是应用最多的认证了。国内唯一的库是在公安部这，由 NCIIC 负责对外提供接口。可以提供如下功能：

简项核查：返回“一致”“不一致”“库中无此号”
返照核查：返回“一致+网纹照片”“不一致”“库中无此号”
人像核查：返回“同一人”“不同人”“库中无此号”

官方接口收费是 5 元/条。 市面上主要的第三方服务提供商有国政通（简项、返照）、诺证通（简项）、IDface（三接口）等，收费简项核查：0.5~2.0 元、返照核查为 0.8~2.1 元、 人像核查 2.0~8.0 元不等。一般都和访问量有关，量大从优。

当然，这里也要注意，涉密人员是没法查到相关信息的。 性能上， XX 通一般在 200ms 内即可返回结果，普通商用应该是没问题的。 有些公司还会额外提供四要素接口，以 XX 通为例，它号称支持大部分银行卡的四要素认证。但是实现上有点儿懵，居然是实时请求银行的接口，这就导致接口延迟非常高，1 秒以上的占大部分，甚至 10 秒以上的都不少见，基本无法商用。这种情况下，还不如直接上银联。

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）

支付系统设计：银行卡支付（三）

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。