支付系统设计：应用内支付（五）

应用内支付指使用手机操作系统自带的支付功能来支持支付。目前国内主要的应用内支付有 Google Pay、Apple Pay、小米支付、华为支付等。 其中 Apple Pay 是典型的一个应用内支付，Android 平台的各种支付也一般是沿用 Apple Pay 的设计。

为什么要 IAP

相对来说，应用内支付的用户体验，和微信支付、支付宝相比，还是有一定差距的，但是为什么要开发应用内支付呢？ 这个和苹果的 AppStore 的审核政策有关。 在官方的（App Store Review Guidelines）中， 有如下几条意见：

1.2 Apps utilizing a system other than the In-App Purchase API (IAP) to purchase content, functionality, or services in an App will be rejected.

在 App 内使用非 IAP 的系统来购买内容、功能或服务将被拒绝。

11.3 Apps using IAP to purchase physical goods or goods and services used outside of the App will be rejected.

IAP 购买实物或者应用外的商品或服务将会被拒绝；

11.4 Apps that use IAP to purchase credits or other currencies must consume those credits within the App

通过 IAP 购买的积分或者其他货币必须只在 App 内使用。

这问题就来了，如果要购买的服务，即在 IOS 内使用，也在 Android 等 IOS 系统外使用，那应该是使用规则 11.2 或者规则 11.3 来执行？ 比如说视频网站，视频既可以在 IOS 上看，也可以在 Android 上看，那是否是需要通过 IAP 来购买？ 苹果公司在这一点上采取模糊的策略。 爱奇艺、腾讯视频，在 IOS 上购买会员，只能用 IAP 支付。这就和苹果公司的审核有关。

IAP 支付流程

一般 IAP 支付的开发流程，首先需要一些准备工作，包括：

在 developer.apple.com 上配置一个 App ID，使用该 ID 生成和安装相应的 Provisioning Profile 文件。
登录到 iTunes Connect，使用 App ID 创建一个新的应用，在该应用中，创建应用内付费项目，设置好价格和 Product ID 以及购买介绍和截图。
添加一个用于在 sandbox 付费的测试用户，填写相关的税务，银行，联系人信息。

完成这些准备工作后，既可以进入正式的开发，开发代码我们这里就不说了，流程如下：

用户选择要购买的内容并点击购买按钮；
用户通过 App Store 账户验证
苹果服务器验证用户请求
苹果服务器从用户帐号扣款
苹果向用户返回购买成功信息
软件接收并显示用户购买信息

老司机都能看出来，这里有好多好多的坑。

用户访问 AppStore 时使用的是 Apple 的账号，不是应用系统的账号。 也就是说，我们并不知道到底是谁在购买这个内容。 比如在应用中有两个账号 A 和 B，用 A 账号登录后，上 IAP 买了东西，然后用 B 账号来登录，也上 IAP 买东西， 这两次购买，用的是同一个 Apple 账号。苹果也不会告诉你，到底是哪个账号付了钱。 账号坑在单次购买中还没什么问题，但碰到订阅的情况，得好好处理下。在订阅章节中会详细说明。从上述流程可以看出，苹果服务器都是和客户端打交道的，这里面似乎没有应用服务器什么事情。 只有在客户端接收到苹果返回信息后，才可以把这个信息转发给应用服务器。 如果用户一直不打开手机上的应用，那应用服务器就一直收不到通知了。 好在后来苹果提供了一个验证功能，应用服务器可以把接收到的返回信息（加密后的字符串）发送给苹果服务器来验证和解密。

IAP 订阅

IAP Subscription 又是一个大坑。 官方的文档在这里。内容不多，没有说明的东西却很多。

续费周期的计算

IAP 主要提供给周期性订阅的音乐、电子书等内容使用。 一般就按月来计算周期。苹果是以自然月来算权益周期。比如在 1 月 3 号买了权益，到 2 月 3 号，这个权益就过期啦，需要在此之前完成续费。 那问题来了，1 月 31 号买的权益，到几号过期？以自然月算，这个权益会在 3 月 1 日前到期，如果 2 月份，3 月份都续费了，到 4 月份，也是享受到 4 月 30 日了。

自动续费

应用开发应该不需要关心续费的细节。苹果会做自动处理。在权益到期前 10 天，苹果检查用户账户是否可以扣款，商品价格是否有变动。在权益到期前 24 小时，苹果开始扣款，如果失败，会多次重试，直到成功。问题来了，这个重试，会延续到用户权益过期后一小段时间，苹果没有说这段时间该算是有权益还是没有，但开发人员需要注意应该如何处理。

免费试用

免费试用不是强制需求，但这有利于用户判断是否值得购买这个物品。免费试用期是在 itunes connect 中设置。 当用户第一次购买这个东西的时候， 客户端接收到的 Receipt 中包含免费试用信息。在免费期快到的时候，苹果发起第一次扣款。整个过程和自动续费类似，唯一区别是第一个月是免费的。

Receipt 验证

客户端接收到 Receipt 之后，需要提交到服务器端进行处理，开通权益。 这就来了个问题：Receipt 应该在客户端还是服务器端解析？当然需要在服务器端处理，这样可以防止越狱后的一些插件，如 IAP Cracker、IAP Free 等伪造交易凭证，欺骗苹果服务器，开通权益。 此外，还需注意，客户端和服务器端之间需通过 HTTPS 以及参数签名等方式来确保通讯安全。 服务器端接收到 Receipt 之后，首先验证请求的有效性， 然后将 Receipt 发送到苹果服务器上进行验证和解析。 接收到苹果处理结果后， 将 Receipt 中的 user_id, product_id、purchase_date、transaction_id 等做验证和处理。

IAP 破解和防御

既然 Iap 的验证主要是在苹果服务器端和手机客户端进行，并且是使用域名。这简直是为攻击打开了一扇大门，而不仅仅是漏洞。 早期的 IAP 内购解锁工具 IAP cracker 对 IAP 的破解比较简单粗暴。写过 IAP 程序的人都知道， 程序中基本都是用 transactionState 来判断交易是否成功。

transactionState 有四个状态：

SKPaymentTransactionStatePurchasing
SKPaymentTransactionStatePurchased
SKPaymentTransactionStateFailed
SKPaymentTransactionStateRestored

SKPaymentTransactionStatePurchased 表示购买成功了。 只要修改这个变量值，如果客户端应用直接根据交易状态来处理业务流程，那就会收到这个假的交易成功信息，接下来用户就能不花钱得到所买的物品。这个过程，甚至都不需要接入网络。

另一个工具 IAPfree 功能更强大，安装使用也复杂很多。它是通过修改 DNS，让客户端访问黑客提供的服务器来取代访问苹果服务器，实现所谓的 MITM 中间人攻击。当用户在客户端触发购买流程时，会被引导到伪装的苹果服务器上，不扣款而直接返回扣款成功收据。用户不需要支付任何资金，客户端能够拿到完整的收据。如果是在客户端处理收据验证也没有任何问题。为了避免用户所使用的设备被封，这些软件甚至可以提供伪造 UDID 的功能。 为此，苹果特别说明，一定要在服务器端验证用户购买信息，验证内容包括收据签名，证书，产家信息等，确保收据无误后，才能授予权益。如果发现有诈，则将用户拉黑。

两套账户体系

苹果支付的账户体系,当然是以 apple id 为基础的，它允许用户在多台设备上共用一个账户。一台设备上，一般只有一个激活账户。但对应用系统来说，大部分是允许多个账号登陆的。这对续费来说就是个大问题。 用户以账户 a 登录后，发起续费，获得权益。然后以账号 B 登录了，显然，A 的权益不会衍生给 B。过几天 A 开始续费了，续费之后，切换到 B 账号登录，客户端在 B 账号登录时得到续费的收据并发送给应用服务器。那这算是谁的续费请求？当然是 A 的。在这个 apple id 发起的续费请求，所有的收据都会有一个相同的原始交易号 original transaction Id。在用户发起订阅时，需要记录这个 id 和账号的关系，每次续费，需要在解析收据后，根据原始交易号从这里获取真正的充值账户，不能从客户端提交的用户 id 作为凭据。

还是这个坑，如果在账户 b 登录后也发起订阅请求，会怎么样？这个调用将会失败，所以需要阻止用户发起这样的请求。或者设置多个产品副本来让用户购买。

分成，定价和国际化

在 iTunes 中的给的产品定价必须是税前的，苹果和商家的分成，也是按税前算。商家给出在一个主要销售国家和地区（比如国内的基本就是中国了）的价格，即基准价格。在其

他地区的销售价格，苹果会自动根据当前的汇率来换算成当地的货币。当然，也可以自己修改设定在这些国家或者地区的当地价格。目前是支持到 155 个国家。还要特别注意版权问题。

基准价格调整，如果是往高了调整， 则在用户下一次续费时，需要用户确认。如果往低了调，那就不需要用户确认，直接扣款了。

苹果对商家的产品价格体系有分组（Group）的概念，同国内说的价格体系，比如白金会员、黄金会员、贵宾等，在同一个 Group 里面，用户只能选择一个档，比如用户要么是白金要么是黄金会员，不会同时是。

在同一个分组中，如果用户订阅时间超过一年（365 天），则商家可以得到来自这个用户收益的更多的分成，目前是 85%。这个订阅时间不包括免费试用期。 同时可以有 60 天的宽限。也就是说，这一年中，如果用户曾经停止续费，然后又开始继续续费，只要中间不续费的时间不超过 60 天就行。

更多的坑

目前用的是 IOS 10.0 版本， 这个版本和 IAP 有关的坑，先记录下：

沙盒环境，没法做取消订阅操作。 只能在线上模拟。 所以产品设计和开发时，尽量不要依赖取消订阅操作，也应该不依赖于这个操作。
沙盒环境下，有些 receipt 可能会收不到 transaction id，线上的暂未发现这个问题。
苹果提供单个收据和列表收据两种格式。推荐使用列表数据，但问题是，这个列表收据的长度，苹果也不知道最多会有多少。

Android IAP

好吧，用这个话题作总结，不是太好。IOS 上用苹果支付是被逼的，android 上用 IAP 是图什么？支付宝和微信支付有这么多用户基数，接入也很方便，费用比 IAP 便宜多了。如果你有接入 android IAP 经验，期待分享。

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）

支付系统设计：绑卡、签约和身份验证（四）

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。