与金融相关的业务问题

# 1 圈存与圈提

圈存

|  |
| --- |
| **圈存**，是将消费者平时从银行户头中提领现金放在口袋里进行消费付款的方式变成将消费者银行户头中的钱直接圈存（存入）IC晶片上，又称电子钱包，这样一来，消费者就免除携带现金找零、遗失、伪钞、被抢之风险。  圈存的资金大多是个人在特定的消费环境下进行刷卡消费的。  收款单位与银行签订协议后，可以通过银行卡向圈存消费卡上转帐，消费者再用消费卡刷卡消费。校园卡、公交IC卡也是这种模式。  我们常用的微信的零用钱就是全存的一种，微信零用钱是虚拟货币(微信零钱是没有利息的，可存可取)，或者可以称作虚拟圈存 |

圈提

|  |
| --- |
| **圈提**，同圈存并列存在，是银行为持卡人提供的主帐户同芯片帐户（电子存折、电子钱包）之间的转帐业务。  通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其在银行的相应帐户上。这种交易必须在金融终端上联机进行并要求提交个人密码（PIN）。只有电子存折应用支持圈提交易。 |

# 2密钥

|  |
| --- |
| 密钥是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥分为对称密钥与非对称密钥。  **对称密钥加密**  又称私钥加密或会话密钥加密算法，即信息的发送方和接收方使用同一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。  **非对称密钥加密系统**，  又称公钥密钥加密。它需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。  信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。  **注意：**我们电商系统的rsa的公钥和私钥采取的就是非对称密钥，我们是私钥加密公钥解密，目的是使用密钥生成的签名进行身份验证 |

# 3对账

什么是对账

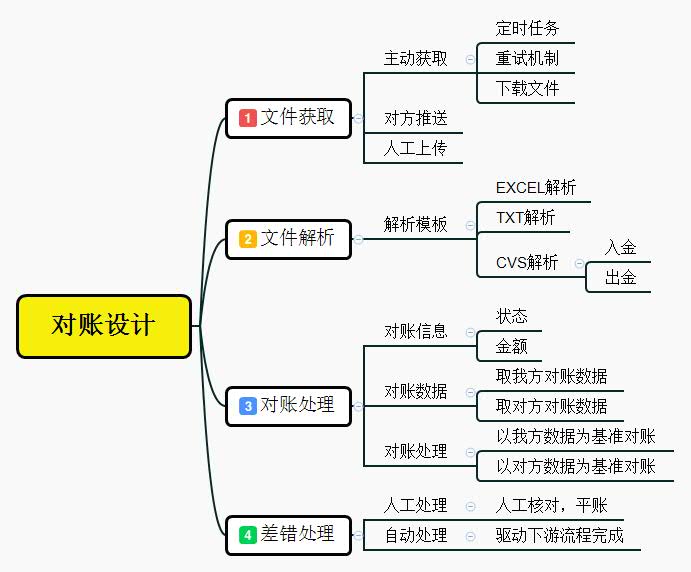
|  |
| --- |
| **银行对账：**在银行或者第三方支付中，对账其实是对一定周期内的交易进行双方确认的过程，一般都是在第二天银行或者第三方支付公司对前一日交易进行清分，生成对账单供平台商户下载，并将应结算款结算给平台商户。  **电商和互联网金融对账：**在往下一层，在互联网金融行业或者电商行业中，对账其实就是确认在固定周期内和支付提供方（银行和第反方支付）的交易、资金的正确性，保证双方的交易、资金一致正确。 |

对账方式

|  |
| --- |
| **单向对账：**一般拿第三方支付机构或银行流水，与自己系统进行对账，防止出现掉单问题；  **双向对账：**两个应用间的流水进行双向核对，如订单与财务系统，既要保证财务系统支付成功的记录，订单系统也是成功的；也要确保订单系统记录成功的记录，财务系统也成功。  **注意：**在gmall商城中，我们调用的是第三方支付系统支付宝，所以我们的支付服务需要与支付宝进行单项对帐，而订单系统可以与我们的支付服务进行双向对账(具体情况依项目而定)。 |

对账模块功能

|  |
| --- |
| 文件获取模块：下载或者读取各渠道对账文件  文件解析模块：创建不同的解析模板，根据渠道和文件类型获取对应的解析模板进行解析  对账处理模块：对账的业务逻辑处理  差错处理模块：处理差错池中的订单 |



对账流程

3、处理差异记录

2、以上游对账文件的表为基准，程序逐行读取并与我们系统的交易记录对比账务记录对比

1、从上游渠道（支付宝）获取对账文件，程序逐行解析入库

# 4 自动冲正

|  |
| --- |
| **冲正：**是银行术语，即对错误的转账、汇款业务纠正。自动冲正机制只有在某一方记账返回超时，银行方无法确定其记账结果，存在出现单边账的可能时。冲正就是“对错误的账务进行改正”。主要是在与银联POS刷卡交易的时候用到。  **注意：**gmall商城不涉及冲正问题，我们调用支付宝进行支付，不直接和银行进行交互 |

# 5 8583报文

简单来说：就是pos机所使用的传递给银行的一种依据8583协议生成通讯文件

|  |
| --- |
| **8583协议：**是基于ISO8583报文国际标准的包格式的通讯协议，8583包最多由128个字段域组成，每个域都有统一的规定，并有定长与变长之分。  8583包前面一段为位图，它是打包解包确定字段域的关键代替。8583协议多在POS机的开发上使用  **8583报文：**POS终端上送POS中心的消息报文结构包括TPDU、报文头和应用数据三部分  TPDU：长度为10个字节, 压缩时用BCD码表示为5个字节长度的数值。  报文头：总长度为12字节，压缩时用BCD码表示为6个字节长度的数值。  在POS上送的请求/通知报文中，该数值由POS终端应用程序在打包上送时根据POS终端参数和当前状态填入应用类别、软件总版本号、终端状态和软件分版本号（具体指各厂商的程序版本号），用于POS中心根据数值进行相应的处理。  在POS中心返回的应答报文中，由POS中心填入处理要求，其他域保持原值返回，POS将根据收到报文头中的处理要求进行相应处理。 |

# 6 银行协议

|  |
| --- |
| 银行协议跟我们没啥关系，我们没有金融系统。  金融系统(比如支付宝)需要跟银联，或者每个银行单独签署协议，每个银行的协议内容和服务费用不一样 |