36

[电子商务网站开发技术文档]

（信息安全设计与实践 I）

[项目名称: NFC 安全手机移动支付银行 APP]

[姓名：　　葛蒙蒙　　]

[学号：　　1130320215　　]

1.背景与意义

1.1 项目开发意义

随着移动通信技术的发展,智能手机在人们的生活中扮演着越来越重要的角色,手机应用已不再局限于电话、短信、上网等传统功能,也开始应用在移动支付等新领域我国经济社会发展和人民生活水平的提高,使得个人金融服务需求不断增长,尤其是对快捷性支付的需求更加突出。为满足人们日益增长的金融服务需求,中国人民银行下发了《关于改进个人支付结算服务的通知》。《通知》的第四部分强调:完善电子支付服务功能,推动自助、居家服务发展,银行要拓展网上支付、电话支付、移动支付等电子支付功能,提高电子支付的服务质量,提高业务离柜率,缓解网点柜面压力。

移动支付正是在这样的行业大发展背景下,得到了迅速发展。如今,全球互联网在快速发展,以安全、高效、便捷为优势的移动支付在电子支付领域备受推崇。日韩、欧美等国家,通过采用非接触式射频识别技术(RFID,RadioFrequency Identification)大力发展手机移动支付业务。经过近几年的发展,手机移动支付业务得到了广大用户的认可和接受,越来越多的用户借助手机实现电子支付,购买票据等业务,手机支付已成为日韩、欧美一些国家和地区主流的电子商业支付方式,据英国 Juniper Research 调研公司预测,到 2013 年全球手机支付额将达到 6000 亿美元[2]。我国的移动手机支付也发展了很多年,但在非接触式

刷卡方面大都还处于试点阶段,发展缓慢。实时、便捷、快速的移动支付方式不仅会给人们带来极大的便利,也会更加促进我国手机和银行金融业务的发展。

NFC(Near Field Communication)是一种标准的短距离无线连接技术,由 RFID 与互联技术的融合演变而来,利用磁场感应实现短距离电子设备之间的通信。NFC 把 RFID 读卡器与智能卡的功能整合在一起,可以直接利用现有的 RFID 基础设施,并从设计之初就考虑到了不同的 NFC 设备之间的交互(:P2P),非常适合手机[3]。与 RFID 相比,NFC 的优势在于:首先,NFC 提供了安全的无线连接,其传输范围比 RFID 小。RFID 的传输距离可达几米、甚至几十米,而 NFC 技术采取了信号衰减技术,尤其适用于小于 4cm 的短距离通信,与其他连接方式相比,NFC 是近距离的私密通信方式,使得 NFC 可以在门禁、手机支付等领域发挥巨大的作用;其次,NFC 提供了一种轻松、迅速的无线连接。NFC 是近距离连接协议,用户只需通过触摸,或者装置靠近,即可实现非接触式的交易、访问数字内容、连接电子装置,而无需像蓝牙进行繁琐的配对;最后,NFC 与现有非接触智能卡技术兼容,已成为越来越多主要厂商支持的正式标准[4]。NFC 的以上特性决定了其在移动支付方面的优势,要想更好的发展 NFC 移动支付,还需要强有力的平台支撑。Google 公司于 2011 年 2 月发布的 Android 2.3.3 SDK,实现了 NFC 通信技术与 Android 平台的结合 NFC 技术在该版本中得到了全面的支持,加入了完整的 NFC 读写/传输 API (应用程序接口)和 NFC 标准的支持。Android 系统的开放性和强大的通信功能,使 NFC 的各种应用能在

Android 上便捷的实现。Android 平台与 NFC 技术的结合,可以更加促进手机移动支付终端的发展,使其有广阔的前景。

1.2国内外现状及技术综述

一、国内外现状

（一）全球移动支付市场高速发展

最近几年，高速增长的全球移动支付市场发展迅猛，仅 2012 年全球移动支付总额将超过 1715 亿美元，较 2011 年的 1059 亿美元增长 61.9%；移动支付用户人数从 2011 年的 1.605 亿增加至 2.122 亿，增幅达 32%。2011-2016 年全球移动支付市场复合年均增长率为 42%，到 2016 年总额将达 6170 亿美元，届时移动支付用户人数将达 4.48 亿。移动支付市场将会随着消费者对便捷性日益增加的需求以及大量掌上商务应用的发展而推进。在新兴市场，移动设备受局限而短信却无处不在，因此短信仍是最主要的移动支付手段。而在北美和西欧，由于移动互联网已经在用户设备上普及，Web/WAP 是更受欢迎的支付方式。预计到 2016 年，北美市场的 WEB/WAP 支付比率将高达 88%，而西欧也将达到 80%。2015 年之前，NFC 支付的比例将维持相对低位，但 2016 年起，NFC 支付将蓬勃发展。NFC 支付涉及用户行为的变化，需要银行、移动运营商、支付卡网络运营商和商家等各利益相关者之间的合作。

（二）我国移动支付市场发展潜力巨大

作为全球最大的手机用户市场，中国具有其他国家无法比拟的先天优

势，有广大的用户群体，且使用手机尚处于初级阶段，其中使用移动支付业务的更是凤毛麟角。截至 2011 年底，我国手机用户就已达到 10 亿户，位居世界之首，手机 2 普及率也达到 80%以上。有如此庞大的手机用户群体，未来作为移动支付的推广和发展是其他任何一个国家都望尘莫及的。假如其中百分之十的用户使用移动支付业务，就能产生将近一亿的移动支付消费群体。无论是移动支付业务本身还是终端消费都是十分庞大的一个数字，带动的产业链可想而知。当然，不可否认中国虽然手机用户基数庞大，未来移动支付群体数众多，但就市场发展来说，整个行业仍然处于发展初级阶段，市场普及率很低，产业链结构尚不成熟。大部分移动支付平台或者方案仍处于理论阶段，或小规模试用阶段。可以说整个产业链的发展尚处于探索阶段，各地市政府也未有同意的标准和政策的扶持。就目前中国移动支付产业的发展状况来看，仅远程支付领域相对成熟，国内主要的金融服务平台，如手机支付宝等移动电子商务发展蒸蒸日上，不管是成交量还是交易金额都在攀升。在近场支付领域，发展始终落后，仅仅是运营商或者金融机构一枝独秀或行业企业的小众试点。

其中，中国联通与中国电信也曾在多个省市试点 NFC 移动支付，但效果不尽如人意，无法大规模商用。而作为中国通信业龙头老大的中国移动也迟迟未发展相关业务，仅仅在深圳短时间推广过手机通等业务，与真正的移动支付还相差甚远。 就目前对中国的移动支付市场上分析，主要有三大参与方，一是以银联为代表的金融机构，二是有广大用户群体的运营商以及有着丰富金融支付经验的支付宝等为代

表的三方支付机构。自然在商业模式上出现了各自主导的局面，他们都各具优势，如银联拥有完善、成熟的资金清算系统，而运营商和三方支付机构则拥有庞大的客户资源与销售渠道。多方的竞争关系依然存在，未来如果发展出符合各方利益的共赢机制和商业模式仍是亟待解决的问题。

就在去年七月，中国移动支付的标准之争终于尘埃落定，由中国人民银行科技司主办的中国金融移动支付技术规范专家评审会在北京举行，大会上主要讨论了中国移动支付未来的标准。参加大会的成员包括了国家金融方面的机构，各家银行、中国银联甚至包括工信部、密码管理局等权威部门。最终，大会上明确了中国金融体系移动支付进场通信的频率标准，即规定使用 13.56MHz 作为进场通信的标准频率。至此，争论了多年的中国移动支付标准有了结论。此次大会可谓为中国移动支付扫清障碍，相信从此中国移动支付将走向高速发展之路。 未来三至五年，相信中国移动支付比较受到全世界的关注，整个产业链也将会迅速形成。预计到 2015 年，移动支付将会发展成为主流的支付手段，特别是基于 NFC 技术的近场移动支付将会进一步普及。移动支付市场的竞争也将会更加激烈，而中国移动支付的主体：中国银联、移动营运商以及第三方支付公司的合作也将 成为关注的焦点。可谓竞争与合作并存，各方的博弈也会长期存在，而最终的局面也只有交给市场去验证。但不管各利益群体如何博弈，相信各方将会积极构建开放的商业模式，可信服的服务管理平台也将会陆续兴起，从而为共同构建的移动支付产业期待积极的促进作用，整合第

三方可信服的服务管理平台，构建开放式创新生态系统，为推进产业发展，促进各方合作共赢发挥重要的作用。

二、NFC 技术作优势

NFC 技术的优势十分明显，同样作为通过频谱中无线频率的电磁感应耦合方式传递的一种，NFC 技术与射频识别技术有着相同的本质和类似的传输方式，但在具体的实现时还是存在较大的差别。NFC 所提供的无线连接技术相对 RFID 来说更为安全迅速，但传输距离则相对要小很多，后者的传输距离可达几米远，在相当范围内仍然可以完成通讯。而 NFC 所运用的信号衰减技术使得其传输距离要近很多，也正因为如此，对 NFC 来说传输距离并非优势，其高带宽高和低能耗的特点才是最重要的。 其次，NFC 技术作为正式的标准技术，与现有非接触智能卡技术兼容，并得到了各厂商广泛的支持。同样作为一种近距离连接协议，它不仅提供了不同设备间的轻松连接，还具有私密的通信方式，所以在实际的使用中会更多用于需要安全性较高的方面。自然在移动支付上运用有着先天性的优势，而不像其他非接触技术被广泛用于产品跟踪、门禁交通等方面。

三、NFC 成本大大降低，适应大规模商用

如今的不少手机终端都已经潜入 NFC 芯片，相信在未来 NFC 芯片会像如今的 GPS 芯片一样，成为移动终端的标准配置。所以起低廉的成本优势将凸显，上游芯片生产将极具潜力。只需要终端设备嵌入芯片，通过智能手机软件的驱动和管理便可轻松实现在各种设备之间的通信和传输。

四、NFC 全球应用案例

1、三星联手 Visa 为伦敦奥运会提供 NFC 移动支付服务

三星和 VISA 达成了新的合作伙伴关系——两家公司已携手在 2012 年伦敦奥运会提供一个 NFC（近距离无线通信技术）移动支付解决方案，并在伦敦发布一款奥运会-残奥会特别版手机。这个手机添加了 NFC 移动支付技术和 Visa 支付应用程序，不仅如此，该手机还会使用一种特殊的 SIM 卡。

2、金雅拓演示 NFC 手机助力工作场所身份验证

在去年的西班牙巴塞罗那世界移动通信大会上，金雅拓公司上演示其创新型 NFC 应用。此次进行的企业应用概念验证演示能将手机转变为工作场所安全、便利的身份识别和验证设备。金雅拓的实验显示，利用该公司经实践检验的 UpTeq NFC SIM 卡可以安全、快速地进入建筑物，并能提供有关访问 PC、笔记本电脑、IT 网络和其他公司服务的强身验证，而所有这些仅需点一下手机即可完成。

2. 需求分析

2.1 总体需求

本移动应用基于 Android 手机平台，采用 C2C 和 C2O 的方式，其中 C2O 购物付款，C2C 转账付款。

本系统的用户可以划分成三类，分别是介入系统的购物网站的商家、系统普通用户和管理应用的管理员用户。

本系统的普通使用者定义为普通用户。用户可以通过系统实现在线充值、提现、付款和转账等业务。同时为了方便用户使用，我们采用了扫码支付和 NFC 安全支付的方式。用户只需扫描一下付款二维码，即能在手机端完成支付。在转账的时候，只需手机轻轻一触，即能通过 NFC 瞬时完成转账。同时为了丰富系统的功能，我们还加入了话费充值、实时汇率查询、快递查询、火车票预定等便民服务。

本系统的接入购物网站拥有者定义为商家。商家需要向系统后台提出接入申请，获得接入资格后方可通过本系统完成资金结算。当消费者在商家平台购物完成后，商家发出付款请求，生成付款二维码。用户通过应用扫描付款二维码，正确输入密码后，支付完成。同时系统将付款结果返回给商家。

本系统的维护人员角色定义为管理员。管理员使用本网站授权的管理员账号登录本系统网页管理端。管理员可以查看用户列表和联系方式。同时能审计日志，审计日志包括登陆日志审计和交易日志审计。

本系统使用全新的在线交易安全协议，保障了用户身份的认证及数据的加密传输，可以防止信息泄露、数据伪造、身份冒充、中间人等攻击，保证交易的安全性。同时加入 NFC、和扫码支付等新型支付方式，更具实用性和高效性。

2.2功能需求

2.2.1 用户功能需求

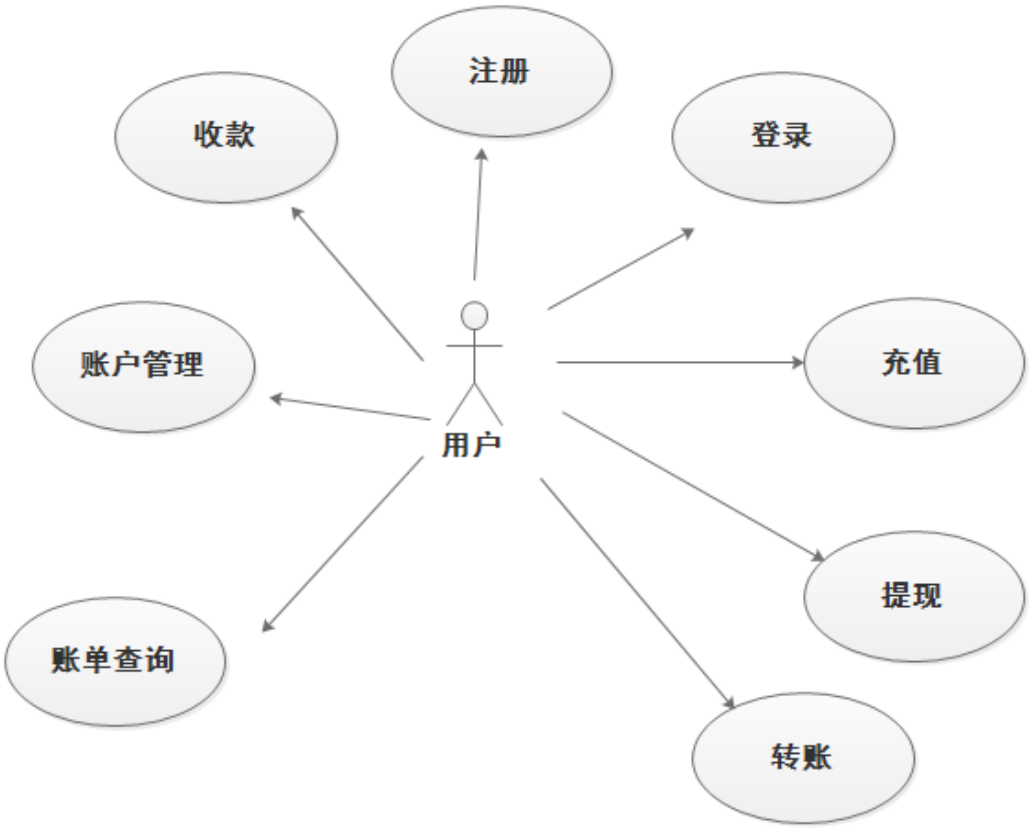


图 1

用户注册：用户通过注册成为系统用户并登录验证身份后，可以使用该系统提供的服务。注册时包括用户名、密码等基本信息。

用户登陆：用户通过系统的相关验证设计，登陆系统验证身份。在用户登录时为了保障用户账户的安全性，要求用户首次登陆时需要设定付款密码，付款密码不能和登陆密码相同。同时方面用户密码找回，要求用户绑定密保邮箱和密码问题。

充值：用户可以通过银行卡，给自己系统账户充值。

提现：用户可以把账户内余额，提取现金到指定银行卡。

转账：系统用户之间可以进行系统内转账，转账有三种实现方式。1、输入对方账号，转账金额和付款密码完成转账。2、扫描对方收款二维码完成转账。3、采用 NFC 支付，和收款方轻触完成支付。

付款：在商家平台购物完成后，扫描付款二维码即可完成付款操作。

账户管理：用户可以管理自己的账户，修改个人信息，修改登录密码和付款密码

账单管理：用户可以查看自己的消费记录，消费记录分为转账、付款、提现和充值四种

2.2.2 管理员功能需求

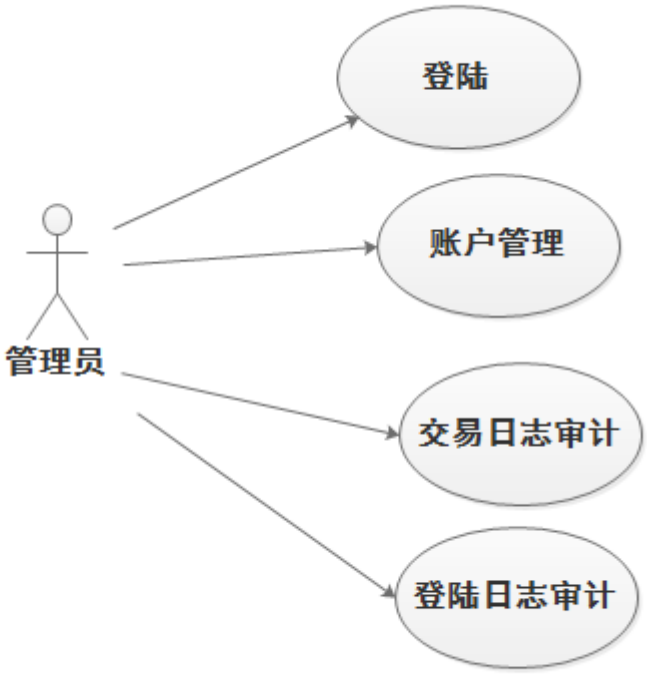


图 2

管理员登陆：管理员通过网页端通过验证后完成登陆，登陆系统后可以完成相应的管理操作

账户管理：管理员可以查看系统的所有注册用户账号，和对应的联系方式，方便系统管理。

交易日志审计：管理员可以查看系统内的交易日志，日志包括交易时间，交易对象，交易金额和双签名信息。

登陆日志审计：管理员可以查看系统的登陆日志，日志包括登陆对象、时间、地点。对于异常登录可以做出判断。

2.2.3 商家功能需求

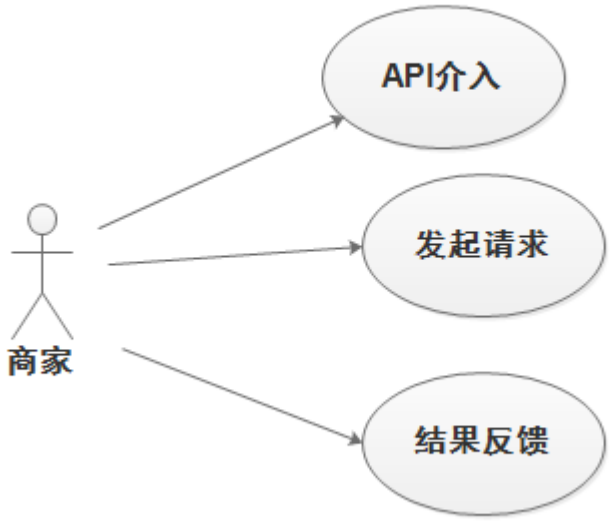


图 3

API 介入：商家通过向系统后台提出申请，申请接入平台。在管理员审核通过后，商家方可通过平台完成资金结算。

发起请求：当消费者在商家平台购物完成后，商家发出付款请求，生成付款二维码。用户通过应用扫描付款二维码，正确输入密码后，进行支付。

结果反馈：用户通过系统扫描二维码，正确输入付款口令后，系统完成资金结算，同时把将支付结果反馈给商家。

2.2.4 额外补充功能

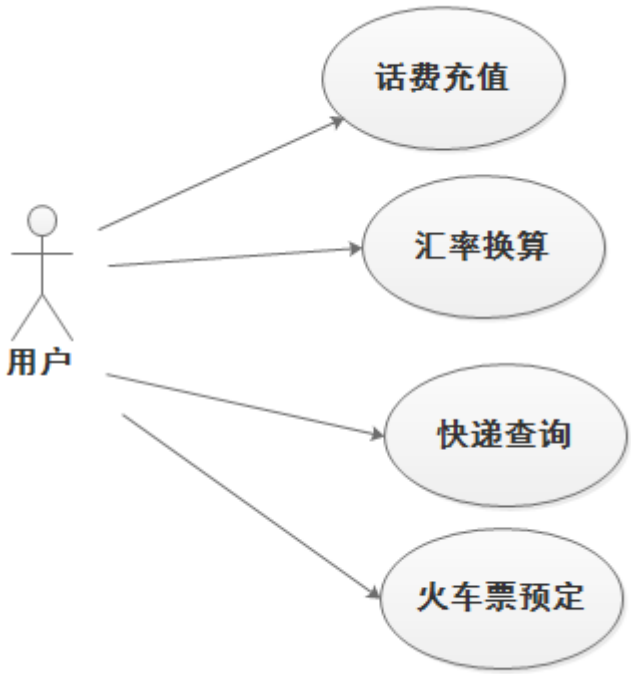


图 4

话费充值：用户可以通过系统内接入的第三方充值平台，完成手机话费充值。

汇率换算：我们在系统内还介入了实时汇率换算模块。用户可以通过系统计算实时的汇率信息。

快递查询：在付款完成后，用户需要等待收取商家邮寄的物品。我们提供了快递查询接口，方面用户实时了解所购物品的物流动态。

火车票预定：用户可以通过第三方购票平台，在系统内完成火车票的预定和支付。

2.3 性能需求

1)网站的页面载入速度较快，正常网速下每个页面载入时间小于 1s。

2）同时满足 1000 人交易操作。

3）用户的身份认证过程需要安全可靠，速度快，普通用户登录系统时间小于 2s，管理员登录系统时间小于 3s。

4）平台支持性要好。要求完全支持 Android2.3 及以上版本任一机型安卓手机。

5）系统可以 24 小时持续运行。

3.概要设计

3.1 硬件环境

一个真实的物理 IP 地址、一个真实域名

Android4.0 手机

网络带宽不低于 50Mbps

内存 4G，硬盘 500G，双核 CPU 处理器

3.2 软件工具

操作系统：Microsoft Windows 10 x64

开发工具：Eclips 4.4

Java 1.8

Android SDK 6.0

Pyrhon 2.7

Web 服务器: Apache 2.4

Django 1.8.5

数据库： MySQL 5.6

程序设计语言：Html,、Javascript、CSS、Xml

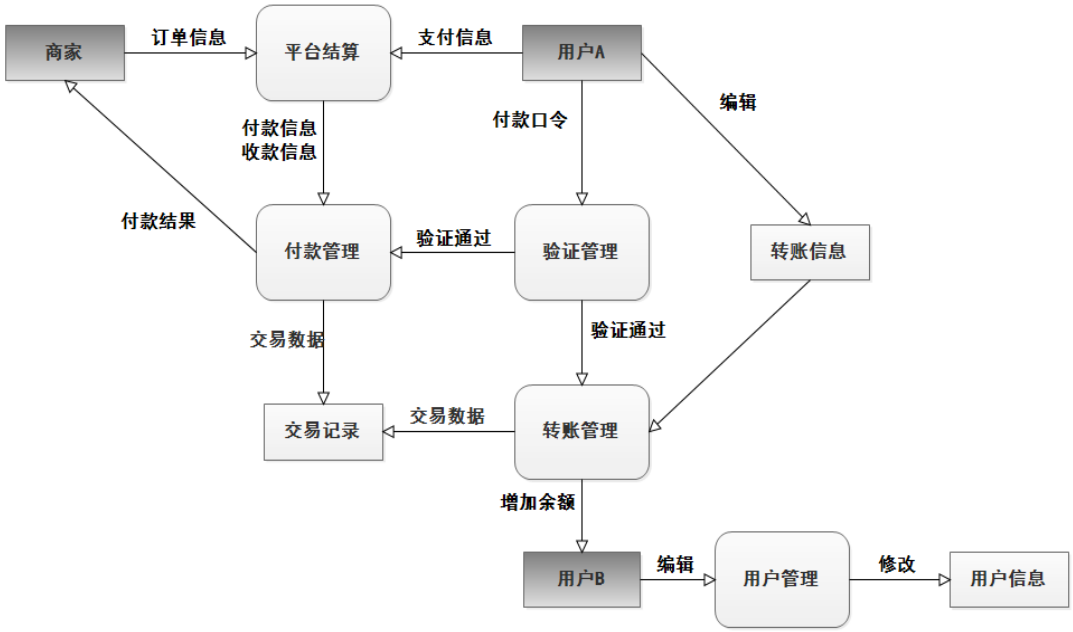
3.3 用户环境

Android 4.0 版本手机及以上

商家客户端：IE、 Chrome，其它 IE 内核浏览器

3.4 业务数据流

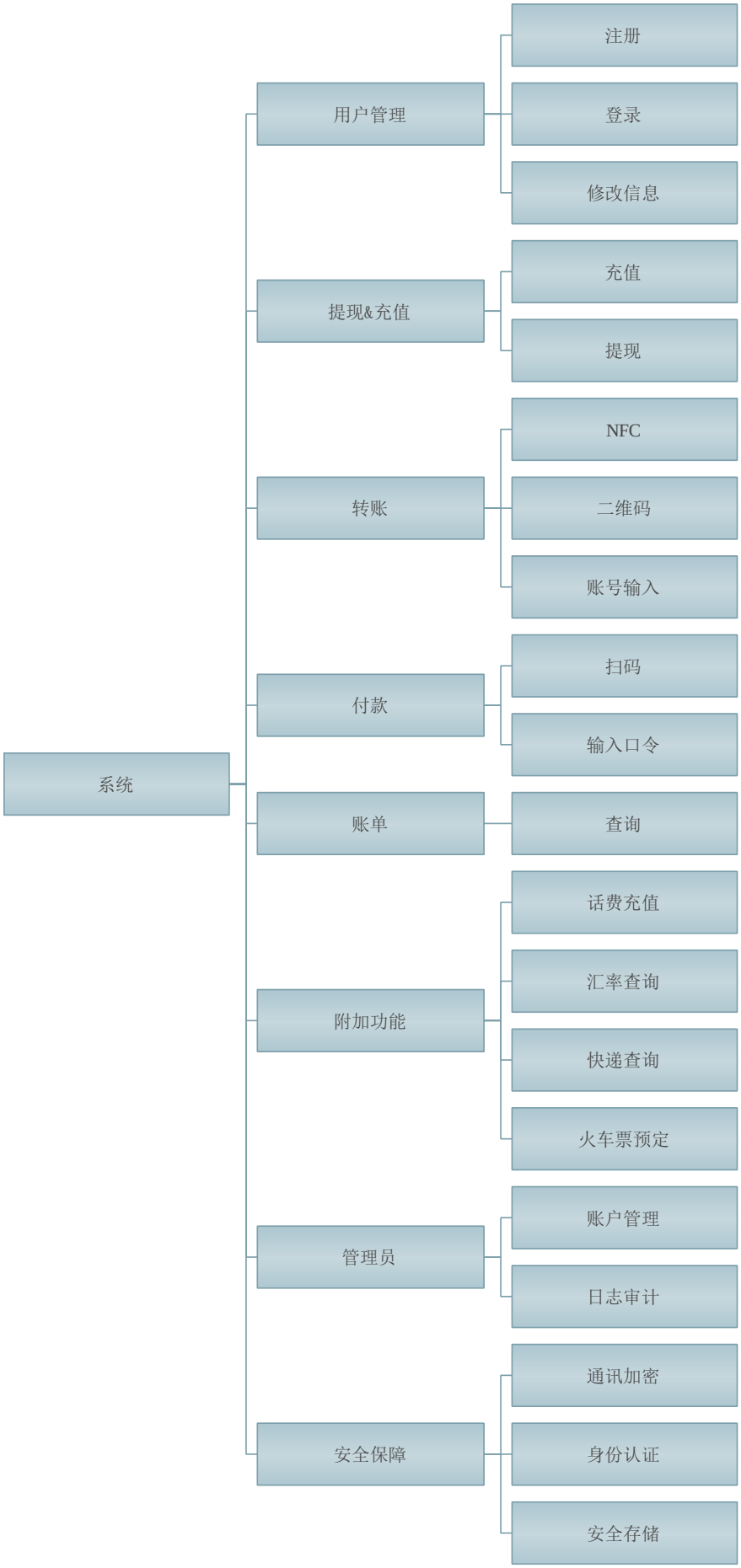
根据业务需求进行业务逻辑分析，得到下列业务数据流



数据流图

3.5 功能模块划分

根据业务处理逻辑进行功能模块划分


系统
用户管理
注册
登录
修改信息
提现&充值
充值
提现
转账
NFC
二维码
账号输入
付款
扫码
输入口令
账单
查询
附加功能
话费充值
汇率查询
快递查询
火车票预定
管理员
账户管理
日志审计
安全保障
通讯加密
身份认证
安全存储

3.6 功能模块定义

3.6.1 用户管理模块

主要功能：完成用户的注册、登陆和个人信息修改业务。

与其他模块关系：用户登陆通过验证后才能使用后续功能

3.6.2 提现&充值模块

主要功能：用户可以将钱从银行卡内转入到系统账户也可以把系统账户内的前提现到银行卡。

与其他模块关系：账户内有余额才能进行购物和转账

3.6.3 转账模块

主要功能：用户可以铜鼓该模块实现转账业务，转账方式有三种：输入对方账号转账、扫描对方收款二维码转账、NFC 支付。

与其他模块关系：需要运用到身份验证模块

3.6.4 付款模块

主要功能：通过扫描商家的付款二维码，完成购物付款

与其他模块关系：需要用到身份验证模块

3.6.5 账单

主要功能：查询账单详情

与其他模块关系：账单的生成来自付款、转账等模块产生的记录

3.6.6 附加功能

主要功能：用户可以完成话费充值、汇率查询、快递查询、火车票预定等业务

与其他模块关系：需要登录

3.6.7 管理员

主要功能：管理员实现用户管理、日志审计业务

与其他模块关系：管理员需登录

3.6.8 安全保障

主要功能：完成通讯加密、身份认证、安全存储三个方面。利用对称和非对称加密技术保证通讯安全、通过数字签名进行身份验证、通过哈希处理保证密钥安全存储。

与其他模块关系：保证其他模块通信安全和交互安全的基础。

3.7 数据库设计

user 表

字段	类型	说明
phone	char	用户 ID
name	char	用户名
Password1	char	登陆口令
Password2	char	付款口令

token	char	登陆凭证
email	char	邮箱
question	char	密保问题
answer	char	密保答案
flag	int	标志位
text	int	临时验证码

accounts 表

字段	类型	说明
user	char	用户名
num	char	余额
imei	char	设备号
pri	char	用户私钥
pub	char	用户公钥

jilu 表

字段	类型	说明
Id1	char	付款方
Id2	char	收款方
type	char	类型
pomd	char	商家哈希值
Pomd2	char	双签名
money	char	金额

admin 表

字段	类型	说明
Id	char	管理员账号
password	char	密码

loginlog 表

字段	类型	说明
Id	char	用户名
time	char	时间
city	char	地点

3.8 关键技术

3.8.1 认证技术

1、Hash 技术

使用哈希算法（MD5） 加密算法实现登录认证，注册时经 hash 后存入数据库中。当用户登录的时候，系统把用户输入的密码进行 MD5 Hash 运算，然后再去和保存在数据库中的 MD5 值进行比较，进而确定输入的密码是否正确。通过这样的步骤，系统在并不知道用户密码的明码的情况下就可以确定用户登录系统的合法性。这可以避免用户的密码被具有管理员权限的用户知道。 MD5 将任意长度的“ 字节串” 映射为一个 128bit 的大整数，并且是通过该 128bit 反推

原始字符串是困难的，换句话说就是，即使你看到源程序和算法描述，也无法将一个 MD5 的值变换回原始的字符串

2、设备绑定

在用户注册时，会记录用户的手机设备号（全球唯一），当用户登录时不仅要提交账号信息，系统还会自动读取手机的设备信息，当后台判断账号信息和设备信息不符时会拒绝用户登录。需要通过短信验证或者密保邮箱的方式完成设备解绑。

3.8.2 加密技术

机密性：在网站传输时采用 RSA+DES 的混合方式加密。用户用服务器的公钥 Pub 加密本次通信使用的对称密钥 Key,然后将需要传输的内容用对称密钥进行 DES 加密。服务器端利用私钥 Pri 解密得到 Key，利用 Key 对信息解密。

完整性：为了防止信息被他人篡改，将消息生成消息摘要 MAC。服务器接受到信息后将信息生成的摘要和 MAC 对比，如果一致则没有被篡改。

3.8.3 动态监测技术

每次用户登录时会记录用户的登陆地点，生成登陆日志。当用户异地登陆时系统会要求用户进行短信验证，防止账号信息被他人盗取。

3.8.4NFC 技术

（1）NFC 技术简介：

近距离无线通信技术(Near Field Communication，NFC)，是由飞利浦公司和索尼公司共同开发的一种非接触式识别和互联技术，可以在移动设备、消费类电子产品、PC 和智能设备间进行近距离无线通信。NFC 提供了一种简单的、非触控式的解决方案，可以让消费者简单直观地交换信息、访问内容与服务。NFC 整合了非接触式读卡器、非接触式智能卡和点对点(Peer-to—Peer)通信功能，为消费者开创了全新的便捷生活方式。

（2）NFC 终端工作方式有三种：

1）主动模式，NFC 终端作为一个读卡器，主动发出自己的射频场去识别和读，写别的 NFC 设备；

2)被动模式，NFC 终端可以模拟成一个智能卡被读，写，它只在其他设备发出的射频场中被动响应；

3)双向模式，双方都主动发出射频场来建立点对点的通信”。

（3）本次工程中的 NFC 技术：

本次工程中采用 NFC 的双向通讯模式，使用 Andriod SDK 4.0 中提供的 beam，来实现信息的传输。

详细内容阐述：

两个拥有 NFC 功能的客户端，首先要开启 NFC 功能和 beam，之后即可以进行快递信息的交换。

此 NFC 通讯模块的工作流程如下：

首先要实例化 NFC 适配器，检查是否有可用的 NFC 设备，然后采用 setNdefPushMessageCallback 方法 setOnNdefPushCompleteCallback

方法来分别注册发送 NDEF 的信息的回调以及接收 NDEF 信息的回调。建立连接之后，如果某一端选择发送信息，然后会使用 createNdefMessage 方法构造一个 NDEF 信息用于发送， 系统调用 onNdefPushComplete 时，NDEF 消息将被传递发出。此处采用的是 intent 发布系统，Intent 发布系统检查所有 Activities 的 intent filters，找出那些定义了可以处理此 tag 的 Activity，如果有多个 Activity 都配置了处理同一个 tag Intent，那么将使用 Activity 选择器来让用户选择使用哪个 Activity。用户选择之后，将使用选择的 Activity 来处理此 Intent.完成信息的传递,达到交换快递信息的目的

3.8.5 扫码支付技术

二维码是用某种特定的几何图形按一定规律在平面（二维方向上）分布的黑白相间的图形记录数据符号信息的。二维码是一种比一维码更高级的条码格式。一维码只能在一个方向（一般是水平方向）上表达信息，而二维码在水平和垂直方向都可以存储信息。一维码只能由数字和字母组成，而二维码能存储汉字、数字和图片等信息，因此二维码的应用领域要广得多。本次我们将二维码应用到快递物流领域。

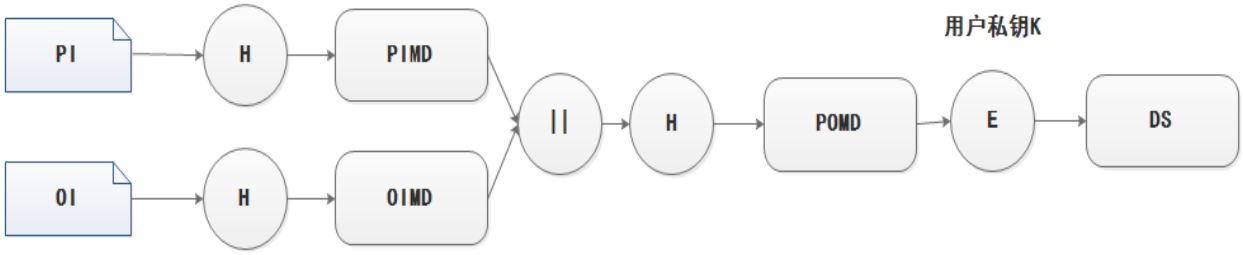
本次我们基于 ZXing 库实现二维码信息的编解码。ZXing 是一个开放源码的，用 Java 实现的多种格式的 1D/2D 条码图像处理库，它包含了联系到其他语言的端口。通过 Zxing 我们可以实现使用手机的内置的摄像头完成条形码的扫描及解码。同时也可以实现条形码编码和解码。目前支持以下格式：UPC-A，UPC-E、EAN-8，EAN-13、39 码、

93 码。

3.8.6 手机 U 盾技术

手机里离线存储着用户的私钥加密证书，当用户需要付款时必须用私钥证书中的私钥对信息签名后才能完成付款。如果没有手机里存储的私钥信息，即使知道账号和付款密码也不能完成支付。即每次支付必须要手机作为 U 盾才能完成支付，更加保障账户的安全。

3.8.7 双签名技术



生成过程：

1） 生成 OI（订单信息）、PI（支付信息）的消息摘要 OIMD、PIMD

2） 将 OIMD 和 PIMD 连接，形成 PO，再把 PO 经过散列计算得到 POMD

3） 用户使用其私钥 K 对 POMD 加密生成 DS

使用过程：

1） 银行获得 DS、OIMD 和支付信息

2） 商家获得 DS、PIMD 和订单信息

验证过程:

银行验证：银行首先计算支付信息的消息摘要 POMD，然后和商家的 OIMD 连接，得到 OI，对 OI 求信息摘要。将 DS 用用户的公钥解密，将得到的结果和 OI 的信息摘要对比，一致则说明正确。

商家验证：商家首先计算订单信息的消息摘要 IOMD，然后和银行的 PIMD 连接，得到 OI，对 OI 求信息摘要。将 DS 用用户的公钥解密，将得到的结果和 OI 的信息摘要对比，一致则说明正确。

双签名技术保证顾客传递给商家和银行的信息相互隔离，同时又确保信息的一致性，杜绝被顾客、商家和银行其中任一一方伪造。

4. 详细设计

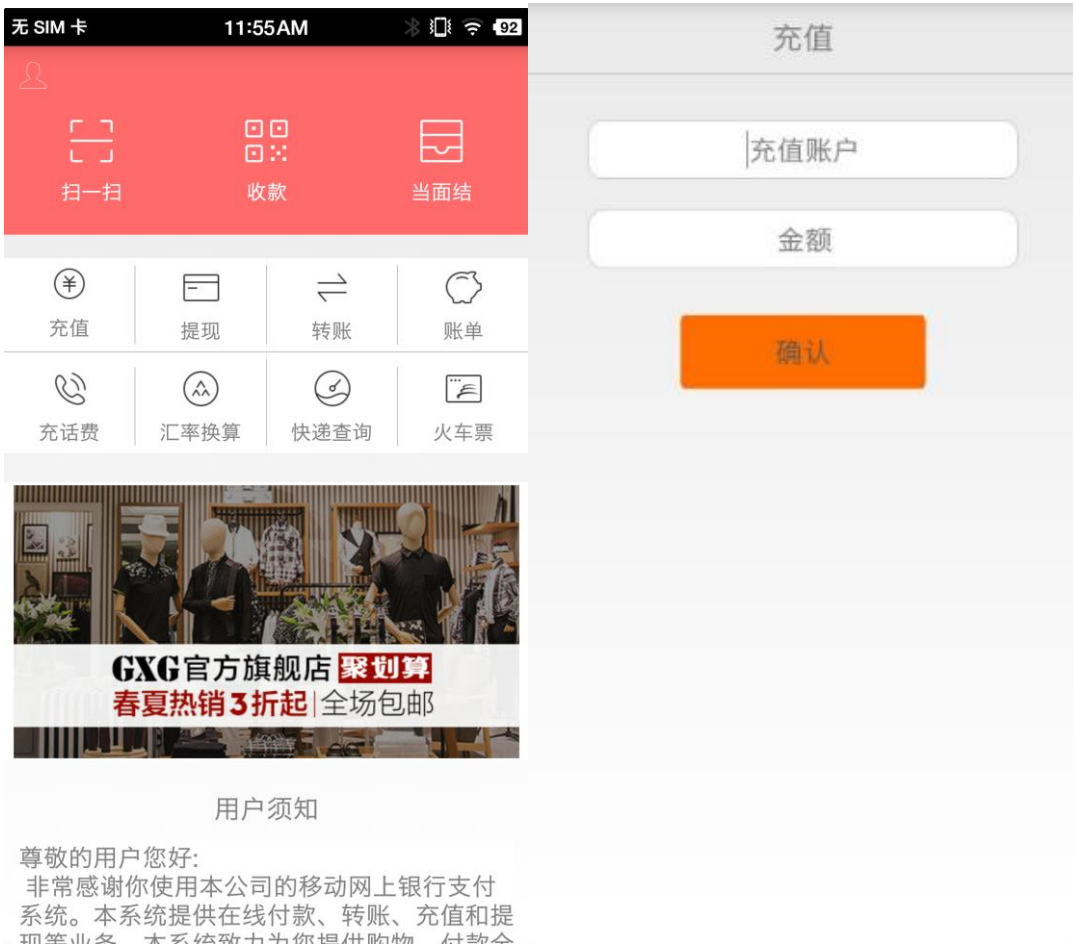
4.1 界面的详细设计

4.1.1 用户界面设计

1）如下图为用户主界面和充值界面

从左图中我们可以看到扫码支付、二维码收款、NFC 当面支付三种支付方式。同时子菜单中还有充值、提现、转账、账单等管理模块。在下面还可以看到花费充值、汇率换算、快递查询、火车票预定四个功能按键。

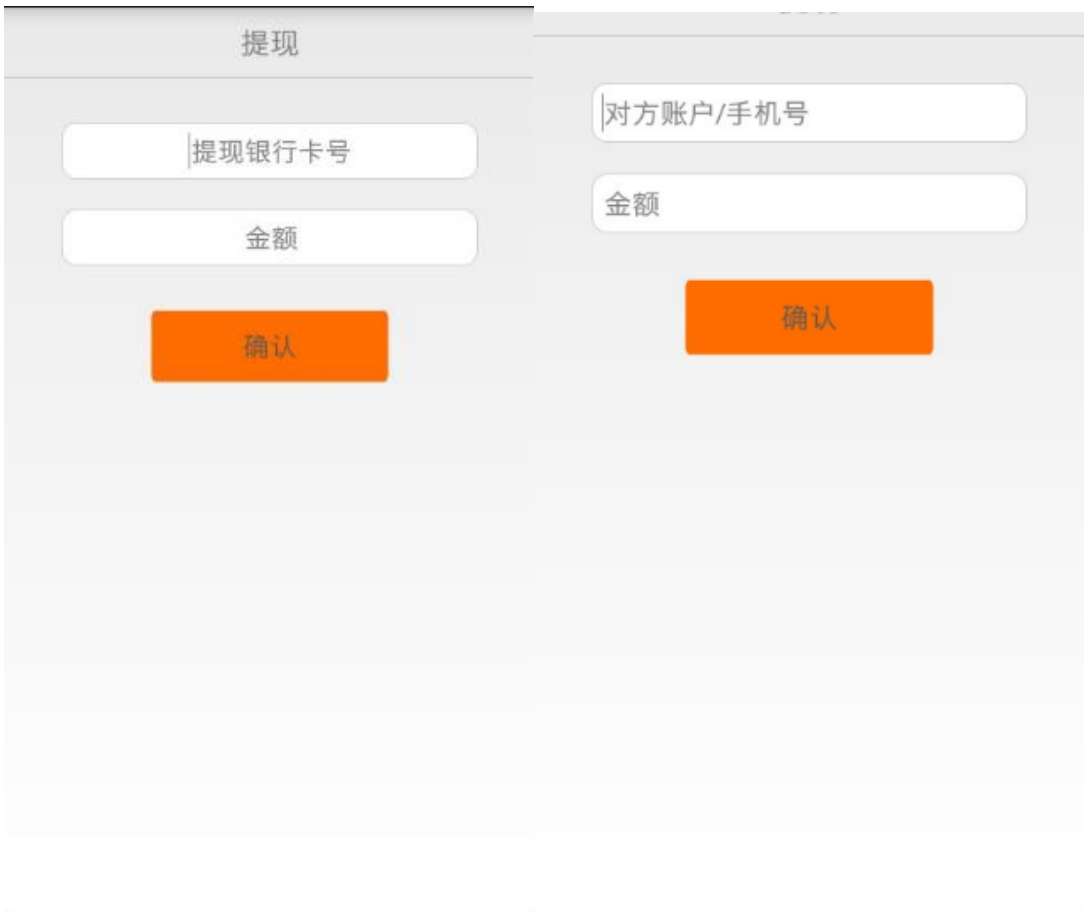
从右图充值界面中我们看到充值账户和充值金额。



2）下图为提现界面和转账界面。

左图为提现界面，用户输入提现卡号和金额后确认输入口令完成提现。

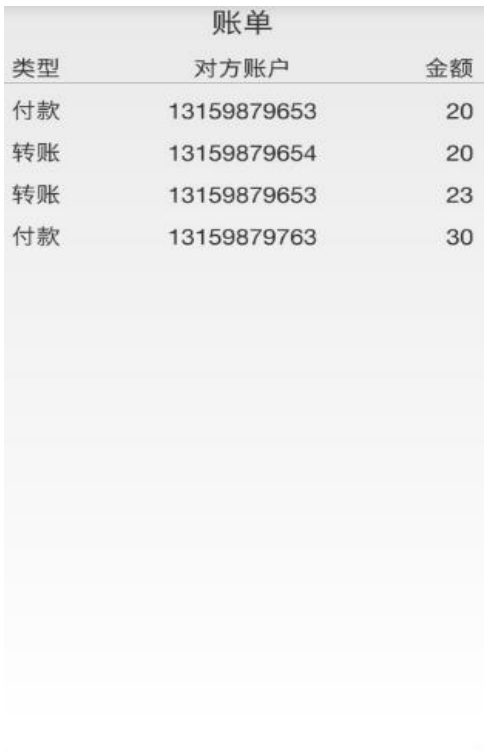
右图为转账界面：用户输入对方账号和转账金额，然后正确输入转账口令，完成转账。



3）下图为账单和话费充值界面。

左图为账单：从图中我们可以看到账单记录了每笔交易信息，包括类型、对方账户、金额三个属性。

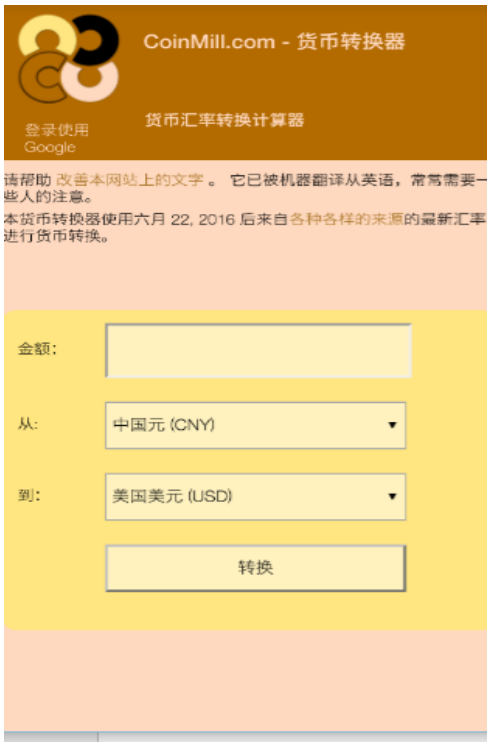
右图为话费充值界面：通过接入第三方平台，用户可以对移动、联通、电信三网手机进行花费充值。



4）下图为汇率换算和快递物流查询界面

左图为汇率换算界面，可以选择常用的国家货币进行换算

右图为快递物流查询，支持顺丰、中通、申通等近百个物流公司快递查询。

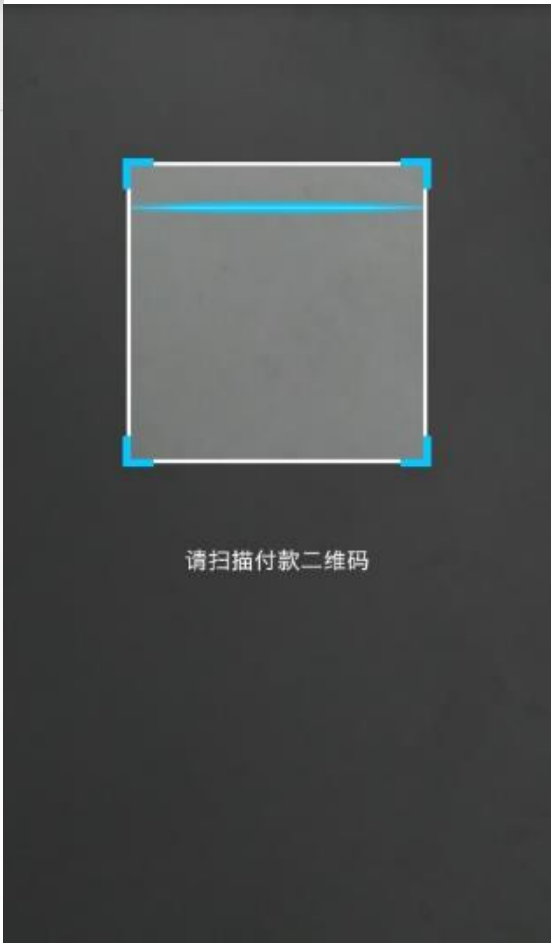


5）下图为火车票预定界面，用户可以在这完成国内所有列车的预定

6）下图为收款码和二维码付款界面

左图为收款码，只需扫描二维码，即可完成转账操作

右图为二维码扫描，用户扫描商家提供的付款码，即能完成付款操作



7)下图为 NFC 支付界面。同时具备 NFC 功能的手机只需轻触，即能完成转账支付。

8）如下图，左图为登陆界面，右图为登陆后界面。

9）如下图为注册界面

左图为基本信息填写，包括手机号、密码；右图为验证码输入界面，用户将手机接收到的验证码正确填写后才能完成注册。

10）如下图为首次登陆后的密码信息初始化界面。

左图为设置付款口令，且付款口令不能和登陆口令相同

右图为设置密保邮箱和密保问题界面，方便密码的找回。

4.1.2 管理员账户页面设计

1）下图为管理员的登陆界面，包括用户名和密码

2）下图为管理员登陆后查看到的用户信息，包括用户名和联系方式

用户列表

登陆日志 交易日志

用户名	联系方式
13159879652	gmm@outlook.cim
13159879653	d@hit.edu.cn
13159879655	g@outlook.cim
13159879666	g@outlook.com
13359879653	
5555	

3)下图为登陆日志审计，可以看到登陆用户的登陆时间和登陆地点

登陆日志

登陆日志 交易日志

用户	时间	地点
13159879652	2016-06-20 12:23:30	哈尔滨
13159879652	2016-06-20 12:23:46	哈尔滨
13159879652	2016-06-20 12:24:10	哈尔滨
13159879653	2016-06-20 12:24:34	哈尔滨
13159879652	2016-06-20 12:30:08	哈尔滨
13159879654	2016-06-20 12:35:09	哈尔滨
13159879652	2016-06-20 12:39:26	哈尔滨
13159879652	2016-06-20 12:40:34	哈尔滨
13159879652	2016-06-20 12:43:26	哈尔滨
13159879653	2016-06-20 12:45:28	哈尔滨
13159879652	2016-06-20 12:46:12	哈尔滨
13159879652	2016-06-20 13:42:18	哈尔滨
13159879655	2016-06-20 15:35:23	哈尔滨
13159879666	2016-06-22 11:59:03	哈尔滨

4）上图为交易日志审计，可以看到每笔交易的收款、付款方、类型、金额、商家签名信息和双签名信息。

交易日志

登陆日志 交易日志

用户	对方用户	类型	金额	商家签名	双签名
13159879652	13159879653	转账	13	转账	
13159879652	13159879653	付款	20	Z9yyLYWL6BOgKnD8	NO /ve /ve /vW/vv70zQRkx3bfvv73vv71
13159879652	13159879653	付款	12	7Ig69hj2tZ1mkHiE	Zzd 77 977 977 9Pu /ve /vRFdLxvvv70=
13159879652	13159879653	付款	12	FOwtyqIQj1KOg3IB	Du /ve /vSUb77 977 9eHE077 9A /vVU6HA==
13159879652	13159879653	付款	10	ymn7noIt1L9wWAV8	77 977 977 9Vg1rc /vULvv70sBSORCG8=
13159879652	13159879653	付款	20	aCnWbwjSvIoLcrsB	77 977 9He /vXwt77 977 9YDtb77 9GSo
13159879652	13159879653	付款	20	0bY8nLcE33SMFLiZ	HRfvv73vv70h77 977 926U e /vTbvv71077 9

4.2 功能的详细设计

4.2.1 用户功能

主要功能有：注册用户、登陆系统、充值、提现、付款、转账、便民服务等功能。

1）用户注册：用户通过注册成为系统用户并登录验证身份后，可以使用该系统提供的服务。注册时包括用户名、密码等基本信息。

2)用户登陆：用户通过系统的相关验证设计，登陆系统验证身份。在用户登录时为了保障用户账户的安全性，要求用户首次登陆时需要设定付款密码，付款密码不能和登陆密码相同。同时方面用户密码找回，要求用户绑定密保邮箱和密码问题。

3）充值：用户可以通过银行卡，给自己系统账户充值。

4）提现：用户可以把账户内余额，提取现金到指定银行卡。

5）转账：系统用户之间可以进行系统内转账，转账有三种实现方式。1、输入对方账号，转账金额和付款密码完成转账。2、扫描对方收款二维码完成转账。3、采用 NFC 支付，和收款方轻触完成支付。

6）付款：在商家平台购物完成后，扫描付款二维码即可完成付款操作。

7）账户管理：用户可以管理自己的账户，修改个人信息，修改登录密码和付款密码

8）账单管理：用户可以查看自己的消费记录，消费记录分为转账、付款、提现和充值四种

9）话费充值：用户可以通过系统内接入的第三方充值平台，完成手机话费充值。

10）汇率换算：我们在系统内还介入了实时汇率换算模块。用户可以通过系统计算实时的汇率信息。

11）快递查询：在付款完成后，用户需要等待收取商家邮寄的物品。我们提供了快递查询接口，方面用户实时了解所购物品的物流动态。

12）火车票预定：用户可以通过第三方购票平台，在系统内完成火车票的预定和支付。

4.2.2 管理员功能

主要功能有：登陆、账户管理、交易日志审计、登陆日志审计

1）管理员登陆：管理员通过网页端通过验证后完成登陆，登陆系统后可以完成相应的管理操作

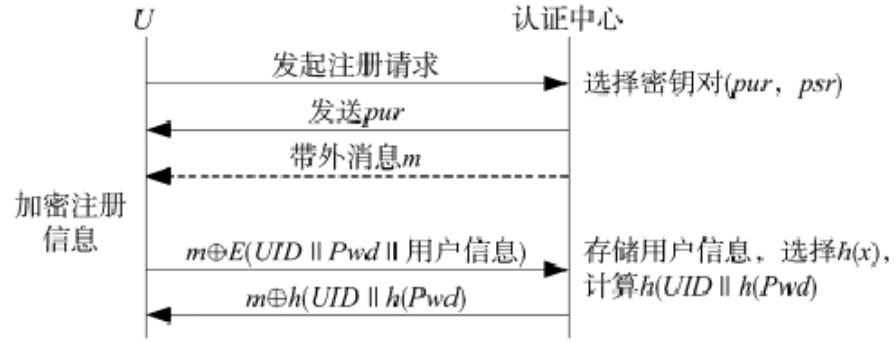
2）账户管理：管理员可以查看系统的所有注册用户账号，和对应的联系方式，方便系统管理。

3）交易日志审计：管理员可以查看系统内的交易日志，日志包括交易时间，交易对象，交易金额和双签名信息。

4）登陆日志审计：管理员可以查看系统的登陆日志，日志包括登陆对象、时间、地点。对于异常登录可以做出判断。

4.3 安全性保障详细设计

4.3.1 注册安全性



1) 首先，用户向服务器发起注册请求，服务器收到注册请求信息之后，选择一个 RSA 密钥对 (pur，psr)。

2) 认证中心将公钥 pur 发送给用户，并发送一条包含信息 m 的短消息给用户。

3) 用户 U 将 UID、密码和用户个人信息等用公钥 pur 加密后，将通过短消息收到的秘密信息 m 与加密信息进行异或，然后将结果向认证中心发送。

4) 认证中心收到消息后，通过异或去掉 m，使用私钥 psr 解密，然后选择一个散列函数 h(x) 对用户密码进行散列，得到 h(Pwd)，将 UID、h(Pwd)、用户信息存入安全数据库。

5) 认证中心将用户信息录入安全数据库之后，向用户发送注册成功的消息。

通过以上方式的同时进行了输入检查，防止非法字符输入；记录设备号，防止信息被他人盗取登陆。

4.3.2 登陆安全性

登陆界面会检查用户输入的用户名、密码是否包含非法字符，同时在用户提交身份信息时系统会自动获得用户的设备 IMEI，看身份信息和设备信息是否一致。如果不一致则拒绝用户登录，一致后将用户密码哈希后和数据库的哈希值进行比对，如果相同则登陆成功，服务器返回一个带生命值的 token 值。下次交互时凭借 token 进行身份验证。

4.3.3 数据传输安全性

机密性：在网站传输时采用 RSA+DES 的混合方式加密。用户用服务器的公钥 Pub 加密本次通信使用的对称密钥 Key,然后将需要传输的内容用对称密钥进行 DES 加密。服务器端利用私钥 Pri 解密得到 Key，利用 Key 对信息解密。

完整性：为了防止信息被他人篡改，将消息生成消息摘要 MAC。服务器接受到信息后将信息生成的摘要和 MAC 对比，如果一致则没有被篡改。

4.3.4 服务器安全性

数据加密：

为服务器提供了一种双向的数据加密的方式。设置秘钥为一个随机的 32 位长度的字符串，秘钥由 MD5 和 random()随机生成，并定期更换 json 数据的加密秘钥，采用 ECB 加密模式， 使得服务器和手机用用中所有的交互的数据都被加密，并且加密后的数据是原来数据函数长度的 2.6 倍，这些加密信息保护了整个网站的安全性。

防止 XSS 攻击：

XSS 攻击又称为跨站脚本攻击。 本网站采用特征匹配方式，在所有提交的信息中都进行匹配检查。 对字符串和数组进行过滤，去掉隐形字符串，并将 URL 解码，将字符串转为 ASCII 编码，再次去掉隐形字符串，将所有的分隔符转化为空格，再将所有不被允许的字符删除，并删除 HTML 标签中的恶意属性，净化 HTML 和超链接中的

js，从而起到了防止 XSS 攻击的作用。

防 SQL 注入攻击：

对输入数据库的合法性都进行了检测，对输入的可能会发生错误的字符串进行校验

5.实现与测试

5.1 实现

服务器基于 Django 框架实现，客户端基于 Android 实现

5.1.1 注册实现

注册模块主要有 sign.java 和 signcheck.java 实现。用户在注册界面填写用户手机号、密码。然后系统提交到服务器，服务器向用户手机号发送 6 为验证数字，用户正确输入 6 为验证数字后提交到服务器，服务器验证无误后完成注册。

5.1.2 登陆实现

登陆主要有 login.java 和 loginfirst.java 实现。当用户输入用户名、密码后系统将用户信息提交到服务器。如果是第一次登陆，系统要求用户设定付款密码初始值，同时初始化密保邮箱和密保问题。当用户的密码丢失时可以通过密保邮箱和短信验证找回。用户登陆成功后，服务器返回一个带生命值的 token。

5.1.3 转账实现

转账主要有 transmoney.java 实现，当用户登入系统后，用户输入对方账户和转账金额，提交给服务器，服务器验证无误后，要求用户输入付款口令。系统将用户输入的付款口令上传给服务器，服务器验证通过后完成转账。

5.1.4 付款实现

付款主要有 fukuan.java 实现。当用户登入系统后，用户通过扫描付款二维码，将获取的信息提交给服务器，服务器验证无误后，要求用户输入付款口令。系统将用户输入的付款口令上传给服务器，服务器验证通过后完成付款。同时将商家签名信息、双签名信息存入数据库。

5.1.5 扫码支付实现

本次我们基于 ZXing 库实现二维码信息的编解码。ZXing 是一个开放源码的，用 Java 实现的多种格式的 1D/2D 条码图像处理库，它包含了联系到其他语言的端口。通过 Zxing 我们可以实现使用手机的内置的摄像头完成条形码的扫描及解码。同时也可以实现条形码编码和解码。目前支持以下格式：UPC-A，UPC-E、EAN-8，EAN-13、39 码、93 码。

5.1.6NFC 实现

本次我们采用 NFC 的双向通讯模式，使用 Andriod SDK 4.0 中提供的

beam，来实现信息的传输。两个拥有 NFC 功能的客户端，首先要开启 NFC 功能和 beam，之后即可以进行快递信息的交换。此 NFC 通讯模块的工作流程如下：首先要实例化 NFC 适配器，检查是否有可用的 NFC 设备，然后采用 setNdefPushMessageCallback 方法和 setOnNdefPushCompleteCallback 方法来分别注册发送 NDEF 的信息的回调以及接收 NDEF 信息的回调。建立连接之后，如果某一端选择发送信息，然后会使用 createNdefMessage 方法构造一个 NDEF 信息用于发送， 系统调用 onNdefPushComplete 时，NDEF 消息将被传递发出。此处采用的是 intent 发布系统，Intent 发布系统检查所 Activities 的 intent filters，找出那些定义了可以处理此 tag 的 Activity，如果有多个 Activity 都配置了处理同一个 tag Intent，那么将使用 Activity 选择器来让用户选择使用哪个 Activity。用户选择之后，将使用选择的 Activity 来处理此 Intent.完成信息的传递,达到交换快递信息的目的

5.1.7 便民服务实现

便民服务通过 huafei.java, huilv.java, kuaidi.java, huochepiaojava 四个类实现。主要是在应用内开启一个 Web 服务，将第三方网站接口接入。从而用户可以在系统内完成话费充值、汇率查询、快递查询、火车票预定服务。

5.2 测试

5.2.1 注册测试

1） 用户点击注册，输入账号信息和密码

2） 服务器向用户手机发送验证码

3） 用户输入验证码

4） 完成注册

5.2.2 登陆测试

1）用户点击登陆

2）输入用户名和密码

3）服务器验证后登陆系统

4）初次登陆时要求设置初始付款口令和密保信息

5）登陆完成

5.2.3 付款测试

1）扫描商家给出的付款码

2）输入付款口令

3）服务器进行身份验证，验证无误后，资金结算。

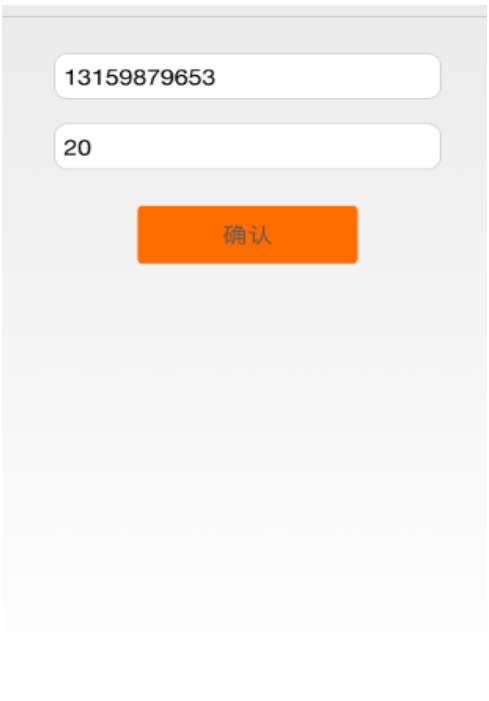
4）付款成功

5.2.4 转账测试

账号转账:

1） 点击转账按钮

2） 输入对方账户、转账金额



3） 输入付款口令

4） 完成转账

NFC 转账：

1） 打开 NFC 当面付

2） 输入付款密码、金额

3） 完成转账

5.2.5 管理员审计测试

1）管理员登陆系统

2）查看用户列表

用户列表

登陆日志 交易日志

用户名	联系方式
13159879652	gmm@outlook.cim
13159879653	d@hit.edu.cn
13159879655	g@outlook.cim
13159879666	g@outlook.com
13359879653	
5555	

3）查看登陆审计日志

登陆日志

登陆日志 交易日志

用户	时间	地点
13159879652	2016-06-20 12:23:30	哈尔滨
13159879652	2016-06-20 12:23:46	哈尔滨
13159879652	2016-06-20 12:24:10	哈尔滨
13159879653	2016-06-20 12:24:34	哈尔滨
13159879652	2016-06-20 12:30:08	哈尔滨
13159879654	2016-06-20 12:35:09	哈尔滨
13159879652	2016-06-20 12:39:26	哈尔滨
13159879652	2016-06-20 12:40:34	哈尔滨
13159879652	2016-06-20 12:43:26	哈尔滨
13159879653	2016-06-20 12:45:28	哈尔滨
13159879652	2016-06-20 12:46:12	哈尔滨
13159879652	2016-06-20 13:42:18	哈尔滨
13159879655	2016-06-20 15:35:23	哈尔滨
13159879666	2016-06-22 11:59:03	哈尔滨

4）查看交易审计日志

交易日志

登陆日志 交易日志

用户	对方用户	类型	金额	商家签名	双签名
13159879652	13159879653	转账	13	转账	
13159879652	13159879653	付款	20	Z9yyLYWL6BOgKnD8	NO /ve /ve /vW/vv7OzQRkx3bfvv73vv71
13159879652	13159879653	付款	12	7Ig69hj2tZ1mkHiE	Zzd 77 977 977 9Pu /ve /vRFdLxvvv7O=
13159879652	13159879653	付款	12	FOwtyqIQj1KOg3IB	Du /ve /vSUb77 977 9eHE077 9A /vVU6HA==
13159879652	13159879653	付款	10	ymn7noIt1L9wWAV8	77 977 977 9Vg1rc /vULvv7OsBSORCG8=
13159879652	13159879653	付款	20	aCnWbwjSvIoLcrsB	77 977 9He /vXwt77 977 9YDtb77 9GSo
13159879652	13159879653	付款	20	ObY8nLcE33SMFLiZ	HRfvv73vv70h77 977 926U e /vTbvv71077 9

经过测试，系统能正常运行

6. 结束语

经过本门课程的学习，自己得以将大二年级学的信息安全导论知识运用到实践，感到很兴奋，也很有成就感。在本次课程中，安全协议上自己对混合加密、公私钥签名认证、双签名技术有了更深刻的理解。在编程上，自己更加熟练的掌握了 Android 开发和 Web 开发。

同时自己能主动思考，考虑有可能产生的攻击，然后积极的和同学讨论，想出解决对策。

同时自己参加信息安全竞赛的经历，使得竞赛作品中有的技术得以在这门课中应用，我认为在本科期间应该多多动手，培养自己的实践能力。

同时非常感谢翟老师的指导和同学们的无私帮助，才使得自己的作品得以成型。

参考文献

【1】 翟建宏，信息安全导论，北京：科学出版社，2011.7

【2】 石亦欣，NFC 芯片与 SIM 卡连接的方案研究，复旦大学，2009

【3】 褚宝增，尹立杰，段岩，加密算法在 PKI 体系中的应用，计算机与网络，2012