

需求分析

项目名称： 基于二维码的虚拟城市一卡通平台开发

项目类别：
☐ 电子商务
☐ 移动终端应用
☐ 大数据分析
☒ 物联网应用
☐ 人机交互应用
☐ 其他()

命题企业： 浙江创建科技有限公司

咨询邮箱： wbl.cn@163.com

2017 年 12 月 1 日

项目需求分析

一、项目背景

进入互联网+时代，城市一卡通平台的实体卡线下业务已不能满足市民日益增长的移动互联网需求。为了紧跟信息技术发展的步伐，需要在城市一卡通平台（实体卡）的基础上，建设基于二维码的虚拟城市一卡通平台（虚拟卡），实现以移动终端为载体，二维码作为身份验证和支付交易的工具，围绕市民综合服务开展一卡通虚实结合应用，搭建基于城市一卡通的城市 O2O 生活服务平台。

二、项目概述

基于二维码的虚拟城市一卡通平台包括虚拟城市一卡通平台和二维码管理平台的建设。其中，虚拟城市一卡通平台主要实现虚拟一卡通账户的全生命周期管理（包含账户的注册、账户变更、账户注销等），以及客户管理、商户管理、清分结算、APP 接入管理、机构接入管理、终端管理、SDK 管理、API 管理、安全审计、系统管理等功能。二维码管理平台具有二维码类别管理、二维码发码管理、聚合支付路由管理、密钥管理、清分对账、运营支撑、安全管理、风控管理等功能。

三、项目需求

（一）功能需求

1. 虚拟城市一卡通平台

1.1 账户管理

虚拟城市一卡通的账户生命周期管理，包含账户的注册、账户变更、账户注销等。

1.2 客户管理

客户管理是建立并维护使用虚拟城市一卡通的客户（市民）数据库，记录客户的基本信息等参数。

1.3 商户管理

商户管理是建立并维护使用虚拟城市一卡通结算的商户数据库，登记商户的基本信息等参数。

1.4 交易清分处理

清算批处理包括：交易的日终处理，结息处理，月终、季末、年终处理，对账处理，报表生成，差错调账处理，清分数据查询，清分日志管理，交易数据管理等功能。

1.5 财务结算

1) 运营结算

将当日（或 T+1、T+n 日）资金结算信息提供给财务系统进行结算银行划账，完成结算中心与各营运公司、代理商账户的资金划拨；并通过系统将当日资金清算信息发送到银行划账系统以供结算银行划账。

2) 调账处理

事后发现有些账需要调整。此交易应由主管授权。注意：此功能在使用时一定要注意账务的平衡，即日报表借贷的平衡。不能只做单

边的调账处理。根据调账账号读取分户账文件，并判断是否未销户，并且余额是否足够；调整账户余额，同时调整对应总账金额。

1.6 APP 接入管理

接入到虚拟城市一卡通平台的 APP，需要在管理平台进行接入登记。包括提供 APP 相关信息，如名称，所属组织，APP 包名，应用签名等信息。系统管理员确认信息后，提交系统，生成虚拟化 SDK 调用的凭证。APP 开发商接入虚拟化 SDK 时，需要按照对接指南，利用分配的凭证接入系统。

1.7 机构接入管理

接入到虚拟城市一卡通平台的机构，需要在管理平台进行接入登记。包括提供机构信息，如名称，机构类型，接入 IP 地址，描述信息。系统管理员确认信息后，提交系统，分配机构编号和虚拟化 API 的接入凭证。机构业务系统接入时，需要按照对接指南，利用分配的凭证接入系统。

1.8 终端接入管理

接入到虚拟城市一卡通平台的终端，需要在管理平台进行接入登记。包括提供终端信息，如所属机构，终端类型，终端型号，硬件序列号，描述信息。系统管理员确认信息后，提交系统，分配唯一设备编号。识读终端通过机构业务系统接入虚拟城市一卡通平台，进行二维码验证时，需要提供设备相关信息，系统对设备合法性进行认证后，再进行二维码验证。

1.9 虚拟化 SDK

系统提供虚拟化 SDK，供第三方应用（如手机 APP、机顶盒应用、自助终端应用）集成，接入虚拟城市一卡通平台，完成虚拟城市一卡通的注册，二维码的申请。提供以下接口：账户注册、账户变更、账户注销、账户查询、账户交易、二维码申请、二维码验证。

1.10 API 开放平台

系统提供虚拟化 API，供第三方系统通过后台接口调用的方式集成，接入虚拟城市一卡通平台，完成虚拟城市一卡通的注册，二维码的申请。提供以下接口：账户注册、账户变更、账户注销、账户查询、账户交易、二维码申请、二维码验证、设备列表查询。

1.11 安全审计模块

1) 黑名单管理

交易清算结算系统在交易处理过程中，会出现一系列的异常情况，把这些情况中的卡号名单分类记录，归类灰名单和黑名单。

通过合理、有效的交易校验处理得到黑名单的预处理清单，加上其他有关的特别处理的结果构成初步的黑名单，通过适当条件的筛选，最终制定黑名单信息表，并通过一定的通信服务程序下载到系统所有营业网点终端设备中及商业网点 POS 机中。

系统在具体业务处理中及时核对和判别卡的有效性，阻止非法卡的交易完成。灰名单的处理与之相似。

2) 交易验证管理

在管理中心清算系统数据处理过程中，为了保证系统的安全性，在交易验证过程中，须对交易和卡号进行验证。

3) 交易审计日志

交易日志统一记录所有进入平台系统的交易。交易日志记录了交易处理过程中的状态，并可用于事后的审计和查询统计。

交易日志组件提供的组件包含但不限于：新增，查询，更新，删除交易日志及其他可由用户扩展的功能。

交易日志在业务范围层面分析属于跨业务共享的数据，适于统一管理。

4) 安全审计

在管理中心清算系统数据处理过程中，为了保证系统的安全性和可靠运行，在系统审计过程中，一般要对数据链路、设备运行、登录管理和通讯安全审计。

1.12 报表模块

支付清算系统的报表模块统计虚拟城市一卡通账户的资金交易情况，包括充值、消费、转账以及与商户机构之间的结算报表。

1.13 系统管理模块

1) 参数管理

营运单位、网点等基本信息设置。

支付系统科目、费率等参数设置。

对系统内操作员的权限管理。

系统运行参数、管理参数的维护。

2) 系统维护

包括数据库系统的备份，文件系统的备份等。

3) 信息查询

包括交易日志查询，卡账户查询，操作员查询，设备查询，网点账务查询，营运公司查询以及其他查询。

4) 业务监控

业务监控子系统监控网点、网站虚拟城市一卡通账户受理业务，虚拟城市一卡通账户在合作商户的消费业务以及在自助终端上的业务受理情况。主要作用在于监控虚拟城市一卡通账户的使用情况，防止账户被非法开通或非法使用。

5) 系统监控

包括系统进程监控，数据库监控，文件系统和数据库系统空间监控，网络设备监控，交易处理性能监控等。

监控各软硬件子系统、网络等的运行情况，如有异常情况，如网络终端、POS 机无法工作、服务器宕机等问题时应及时告警。并可以提供系统负载情况分析，检查系统瓶颈等功能，为今后系统的扩容提供依据。

2. 二维码管理平台

2.1 二维码结构设计

1) 动态二维码结构

动态二维码主要应用在用户联机或者伪联机的商户对接或自有应用的二维码的消费、用户认证等场景。

2) 静态二维码结构

静态二维码主要应用在用户对接无对接平台商户的接入，进行商

户支付的场景。

2.2 二维码类别管理

二维码类别包括身份识别二维码和支付业务二维码两种。

1) 身份识别二维码

用户通过统一认证平台多级的身份认证手段并完成“实名+实人”认证后，生成身份识别二维码，该二维码用于各个应用场景下的用户身份认证。

2) 支付业务二维码

实现不同的交易场景，包括：C 扫 B、B 扫 C 等。支付业务二维码设置有效时间及付款次数限制，如 1 分钟失效，付款 1 次后自动失效。

2.3 二维码系统设置

1) 失效设置

设置二维码失效的时间、付款次数等。

2) 阈值设置

可配置生成二维码余额下限阈值，如必须不低于 10 元，才能生成二维码。

3) 参数管理

对操作角色、权限等系统参数进行设置。

2.4 聚合支付路由管理

1) 路由控制

路由控制是交易网关系统以配置的方式对各接入方分配各自的

通讯端口、文件路径等。路由控制根据实际的交易情况，控制某一路由的最高并发量，从而对每一个接入方的资源使用率都是可控和可配置的。路由控制中包括路由切换功能，用户可以通过参数配置改变交易所使用的路由。

2) 格式转换

由于外部的参与方较多，且有着各自不同的报文格式。交易网关负责将各自不同的联机交易和批量文件转换成核心平台所能接受的统一格式。

在格式转换的过程中，还要对发起方的交易格式进行一定的校验。对于联机交易要取出格式有错误的交易并记录错误日志。而对于批量文件，要对错误格式的批量文件打上标记，以便后续的人工处理。

3) 身份校验

交易网关对接入的机构需要进行身份验证，机构在接入时为其分配密钥，在交易过程中通过加密机对报文进行加解密。

4) 权限校验

交易网关对外部机构发起的每一笔交易进行权限校验，校验机构是否有此类交易的权限，如果校验通过则触发后续功能，如果校验错误则返回错误应答并记录错误日志。

5) 数据校验

交易网关对交易报文的数据做基本的检查，检查内容包括：

(1) 非空域的检查

(2) 数据类型检查

(3) 最大最小值检查

(4) 数据格式校验

6) 交易分发

交易网关根据事先配置好的参数，对各种交易进行转发。

当交易发送给核心平台时，由于分压的需要核心平台可能有多台机器组成，交易网关根据每台机器的负载情况进行交易分发，从软件层面上实现负载均衡。

交易网关对分发交易的主机具有监控和管理的功能，对每台机器的负载情况进行监控和分析从而使每一笔交易都得到最高效的处理。同时分发的主机具有一个主机列表，有新的主机接入时只需要在主机列表中增加主机地址和端口，便可加入使用。

2.5 二维码验证管理

获取平台授权码，进行解密、验证发码机构、发码限制场景、授权时间是否合法根据相关验签算法验证二维码合法性。

2.6 密钥管理子系统

密钥管理子系统实现二维码密钥（包含安全密钥和保护密钥）的管理。

其中，安全密钥用于生成虚拟城市一卡通 ID。虚拟城市一卡通平台获得用户主索引 ID 后，虚拟化账户管理系统调用密码服务功能，以密钥管理子系统的安全密钥为根密钥，以用户的主索引 ID 作为分散因子，通过 SM4 算法计算产生用户身份认证密钥；通过用户身份认证密钥和 SM4 算法对用户证件类型和证件号码加密生成虚拟城市

一卡通 ID。

保护密钥用于动态二维码生成与验证。生成动态二维码时，二维码管理调用密码服务，通过 SM4 算法将有效时间的明文信息加密。验证动态二维码时，二维码管理调用密码服务，通过 SM4 算法将有效时间的密文解密，进行验证。

2.7 用户关系管理子系统

1) 用户管理管理

发码平台用户管理模块，包含用户的同步、用户的维护等功能。

2) 二维码应用平台用户关系维护

平台用户、账户唯一 ID、二维码应用平台唯一识别 ID 对应关系维护模块。

3) 用户行为日志分析模块

通过用户模型，建立用户行为信息分析报表。

2.8 发码平台前置子系统

1) 虚拟卡基础接口

（1）虚拟卡开卡接口

实现虚拟卡线上开卡，建立用户绑定关系。

（2）虚拟卡用户信息同步接口

实现二维码应用平台（如 APP）的用户信息同步。

（3）虚拟卡交易记录查询接口

实现二维码消费交易信息查询。

（4）虚拟卡退卡接口

实现二维码卡片注销和账户的注销退款业务接口。

（5）虚拟卡常见问题接口

实现虚拟卡常见问题的获取。

2) 静态二维码接口

（1）静态二维码申领接口

用户申请开通静态收款二维码应用功能接口。

（2）静态二维码消费接口

实现静态二维码用户消费功能。完成二维码识别 SDK 的封装。

（3）静态二维码消费推送接口

实现商户收款成功后推送信息信息到商户的 APP 下提醒收款成功。

3) 交易相关接口

（1）虚拟卡消费退货

实现虚拟卡账户的消费退货等功能。

（2）虚拟卡账户消费

实现虚拟卡账户的消费等功能。

4) 机具对接接口

（1）密钥和机具参数下发接口

实现二维码相关密钥的下发和二维码相关机具的动态库的下发。

（2）黑名单下发接口

实现用户黑名单的下发和管理。

2.9 清分对账子系统

实现相关系统的对账、业务日志进行清分，生成相关业务报表和财务报表。

2.10 运营支撑子系统

1) 静态二维码管理模块

实现静态二维码的申请、修改、注销等维护性功能。

2) 发码平台参数维护

实现发码平台相关参数的维护和调整。

3) 发码平台报表管理

实现发码平台运营报表和财务报表的展示。

4) 发码平台商户信息维护

实现二维码应用平台（如 APP 等）的信息签约、维护管理等。

5) 发码平台常见问题维护

实现发码平台常见问题的分类、增加、修改、删除等维护性功能。

2.11 二维码安全管理

1) 二维码防伪造

二维码标准统一容易伪造，用户主扫和被扫二维码都存在一定风险。为杜绝风险，对于不同应用场景进行不同等级的防止伪造处理。通过数据加密来保证静态码不被复制。通过加密体系+时间戳控制+动态密钥+在线离线来保证动态二维码防止伪造。

2) 二维码防止重放

二维码在离线或者非实时核销的时候会出现二维码重放的风险。重放的场景可分为两种，一种是离线场景，离线场景为不能实时验证

二维码是否已经核销的场景。该场景使用事后的风控模块进行处理，系统上通过手机的防止截屏处理。在业务风险高的时候，通过部署摄像设备进行把控，在事后在处理风险。在线场景通过二维码核销体系进行处理。

3) 二维码防抵赖

二维码使用过程中可能会出现业务抵赖情况。通过每个码都使用户证书签名来进行处理。每次扫描都使用用户的私有证书进行签名。二维码生成和扫描过程中记录用户硬件基本信息。通过用户行为数据监控和个人业务数据签名来防止抵赖。

4) 接口安全

(1) 内网应用对接接口安全

- 关键字段加密和报文签名保证通信系统的安全性。
- 网络使用专线和机具前置进行对接，保证网络上的安全。

(2) 互联网对接接口安全

- 接口使用关键字段加密和报文签名保证通信系统的安全性。
- 接口协议使用 HTTPS 协议进行对接。
- 接口实现 OAuth2.0 第三方认证机制。保证外网接口的使用安全和用户基本信息的安全。第三方可使用授权获取用户的基本信息。
- 硬件使用外网防火墙进行端口映射。对外进行访问控制，保证前置机的安全。

2.12 二维码风控管理

发码机构根据用户交易情况、信用等级等进行风险控制的系统，负责二维码发码安全管理；二维码发码平台负责结合账户的信用等级、风险等级等综合因素决定用户可进行预付费交易或信用支付交易。

1) 事先风险控制

用户和商户开户时，系统加强对其信用或资质的审核，并据此设定初始的风险控制参数。对于风险比较高的商户，系统可考虑在开户时收取风险保证金。

系统支持黑、白名单功能，并分别形成可配置的风险控制参数集，作为事中风险控制的基础。

对于被置入白名单的商户，风险控制策略相对放宽。用户不提供白名单的功能，其风险控制通过用户等级来实现。

对于被置入黑名单的用户和商户，业务功能受限，系统将采取进一步的措施。

2) 事中风险控制

（1）账户余额控制

根据用户等级，可设置不同的账户余额上限值。当用户进行退货、调账等操作时，账户余额不受上限的限制。根据不同等级用户提供不同的透支信用账户。

（2）转账风险控制

系统可以通过设置用户单笔转账额度（最大和最小额度）、每天转账次数、每天转账总额限度等方法进行风险控制。

（3）充值风险控制

根据用户等级的不同，设置以下向账户充值的限制：

- 每次充值的最大额度和最小额度；
- 每天充值总额；
- 每天允许充值的总次数。

（4）支付风险控制

系统可在以下方面对用户的支付操作进行控制：

- 限制每次交易的最大额度；
- 限制每天交易的总额度；
- 限制每月交易总额度。
- 离线支付透支额度。

用户可以设置自己每次消费的最大额度和每天消费的总额度，但此额度不得违背系统设置的额度。

3) 事后风险控制

系统进行统计分析后，调整用户的等级，并自动或手动更新黑、白名单。

系统支持审计功能，对业务日志进行数据处理和管理，并支持将数据交事后风险控制功能单元自动处理或提交管理员人工处理。

根据风控规则，系统发现可疑交易和可疑操作，可先进行受理，并提示用户此操作正在被后台审核。此类交易和操作相关信息由系统记录并转人工处理，待系统运营管理人员审批后方可完成。

系统运营管理人员定期抽查商户的网站、业务，防止商户从事非

法经营、违背协议中规定的内容等。

系统提供通过短信和消息推送的方式进行通知。透支后提醒用户充值。在用户出现抵赖情况下，通过人工客服方式进行催款等手段。

（二）运行环境需求

1. 软件环境

服务器操作系统及版本：

Windows Server 2008R2 及以上版本；

手机终端系统：

Android4.2 及以上版本；

iOS 7 及以上版本

2. 硬件环境要求

2.1 服务器部署

CPU：4 核 2.5GHz

内存：16G；

外存：硬盘 1T；

输入/输出设备列表：鼠标，键盘，显示器等。

2.2 手机客户端部署

支持 Android4.2 及以上版本，分辨率 720 及以上的手机；

支持 IOS 7 及以上版本，分辨率 640 及以上的手机。

3. 网络环境要求

服务端支持多运营商的同时接入，手机端支持 4G 网络下的流畅运行。