密级：内部公开

乐家易付支付清算服务系统

概要设计说明书

V4.0

修订历史记录

编号	章节	修订说明	修订日期	修订前版本号	修订后版本号	修改人
1		文档创建	2016-05-04		V1.0	孙少军
2	6.3.2	修改会员网关	2016-05-10	V1.0	V2.0	孙少军
3	7.2.3	修改费率、结算周期配置	2016-06-09	V2.0	V3.0	孙少军
4	2	设计约束与限制	2016-07-11	V3.0	V4.0	孙少军
5	4	软件平台体系设计	2016-07-13	V4.0	V4.0	孙少军

目录

1、引言

1.1 编写目的和范围

在支付清结算系统的前一阶段，也就是需求分析阶段中，已经将系统用户对本系统的子模块功能做了详细的阐述，这些模块功能具体设计将在本报告中详尽得以叙述及阐明。

本阶段已在系统的需求分析的基础上，对支付清结算系统做概要设计。

主要解决了实现该系统在功能模块的划分、模块的层次结构以及相关调用关系的情况进行详细的说明。

在下一阶段的编码过程中，相关架构师和设计人员可参考此概要设计说明书，在逻辑层面上对支付清结算系统有一个充分的认识和了解，在此基础上，完成支付清结算系统的详细系统设计工作。

1.2 名称解释

名词	说明
电子支付	以电子化方式发起、处理、接收的支付。电子支付过程中，货币债券以数字信息的方式被持有、处理、接收，由电子支付工具发起实现货币债券转换。
支付产品	提供给用户直接使用的支付使用形态的包装，开通产品后用户才能使用相关功能。
接入渠道	支付订单的入口来源，如官网、WAP、商家接口等
支付渠道	包装给用户使用的支付通道。呈现在收银台上，如网银、钱包、快捷等
资金渠道	外部金融机构售卖的支付通道，而作为接入方而言则表现为外部资金通路。
支付模式	资金渠道不同方式的归类，不同模式意味着交互流程、传递信息存在比较明显的差异。如余额、网银、外部签约快捷、直连签约快捷、无磁无密等，同时可以把外部签约快捷、直连签约快捷、无磁无密统一包装为快捷支付渠道给用户使用
借/贷	会计记账的标识符号，没有实际含义 一般用于两种情况： 描述科目的余额方向，借方余额或者贷方余额，在会计平衡体系中，借方余额总和=贷方余额总和 描述记账方向，相对于余额方向，同向的记账使余额增加，反向的记账使余额减少

会计科目	对各项会计要素按其反映的经济内容和管理要求不同所进行科学分类的项目
会计核算	也称会计反映，以货币为主要计量尺度，对会计主体的资金运动进行的反映。它主要是指对会计主体已经发生或已经完成的经济活动进行的事后核算，也就是会计工作中记账、算账、报账的总称。

2、设计约束与限制

此处说明架构方面的约束和限制

2.1.1运行环境

序号	项目	详细信息
1	运行平台	JavaEE 平台，需支持 JDK 1.6 及以上
2	应用服务器	需支持 Tomcat 6.0.30 及以上版本
3	操作系统	需支持 CentOS 6.8 和 Redhat 6（64 位）
4	数据库环境	需支持 MySql（5.6.26）及 Oracle（11g）数据库
5	客户端软件环境	需支持 MS IE 8 及以上版本、Chrome 及 Firefox 等主流浏览器

2.1.2接口标准

系统内部各子系统的接口以 WebService 形式提供。各子系统需负责提供接口描述、依赖说明等，并提交相应的资源文件。

系统对外部系统提供的接口（如收单、支付等）以 http/https 形式提供。外部接口调用时，需要使用非对称加/解密，数字签名等技术保证调用的安全性和不可抵赖性。

2.1.3关键数据存储

出于系统安全性及用户保护等因素考虑，对于用户相关敏感信息,(包含并不限于)比如用户绑定的银行卡信息(含卡号，有效期，CVV2 等)，实名认证等信息在进行数据库存储时，不得直接存储明文（需要进行加密或 token 化等方式处理)；应用日志中，不得出现上述关键（不限于）信息的明文内容。

2.1.4软件开发工作的限制

经费限制，开发期限，硬件限制，编程语言，通信协议，安全和保密要求，开发过程中须遵守的某些标准或规则。

本节是为具体需求以及设计约束的描述提供依据。

经费限制：41.07 万；

开发期限：2002 年 8 月 31 日完成；

硬件限制：硬设备有部分配置比较低，完成本需求说明中的功能和性能要求没有问题；

编程语言：Noter Script HTML，C++ BUILDER Visual C++

通信协议：TCP/IP，X.509

安全和保密要求：Noter 提供的七级权限控制；CA 加密认证；

开发过程中须遵守的某些标准或规则;编码规范采用 Noter Script，C++ BUILDER Visual C++的编码规范进行。

3、系统物理结构设计

根据系统分析阶段所确定的新系统的逻辑模型、功能要求，在用户提供的环境条件下，设计出一个能在计算机网络环境上实施的方案，即建立新系统的物理模型。这个阶段的任务是设计软件系统的模块层次结构，设计数据库的结构以及设计模块的控制流程，其目的是明确软件系统"如何做"。这个阶段又分两个步骤：概要设计和详细设计。概要设计解决软件系统的模块划分和模块的层次机构以及数据库设计；详细设计解决每个模块的控制流程，内部算法和数据结构的设计。

4、软件平台体系设计

在整个系统的设计上，在保证系统效率的前提下，突出系统的开放性、标准化、模块化、易用实用、性能优化、可靠稳定等特点。

为充分保证系统在安全性、跨平台性、易扩展性、易维护性等方面的要求，各子系统采用分层应用体系结构。

4.1 平台设计原则

系统设计中，使用面向对象思想指导领域模型的搭建，并选用 UML 作为模型表示的手段。在软件实现上，采用 Java 语言（或 Java 生态中支持的其他语言）、遵循 JavaEE 开放标准，整体采用 B/S 结构完成系统的搭建。

4.2 性能设计原则

最大支持前台在线用户：注册用户千万级，活跃用户百万级，在线用户十万级的系统承载要求

最大支持前台并发用户：最大支持 1 万并发

最大后台管理系统操作用户：满足未来 100 管理用户的需求

最大后台管理系统并发用户：管理系统最大并发数 10 个

单笔交易响应时效：单笔峰值响应时间 1~3 秒/笔

系统交易最大处理能力：系统交易能力为 500-1000tps（受硬件配置影响）

4.3 用户体验设计原则

我们在本系统的开发过程中将遵循以下几个原则：

适用性　根据现有软硬件平台的实际情况和未来发展方向，使系统的设计方案具有良好的适用性。

易用性　为了确保多种层次计算机应用水平的员工均能够快速地掌握并进行方便地使用，要求开发出的系统管理容易、操作简便、易用上手。

可靠性　系统要能够提供每天 24 小时，每周 7 天的不间断运作能力，并保证系统在访问高峰期能作到正常工作且快速响应。

安全性　由于网络的开放性，传输数据不可避免的要受到来自各方的恶意侵害。在系统安全性方面，为系统提供保护，保证系统的正常运作；在用户安全性方面，通过技术手段和合规运营保障用户信息和资金的安全。

4.4 数据库设计原则

建立完善的数据库结构管理设备的基本参数、运行状态和各种工作计划。数据库的框架和结构必须根据设备和运行状态而设计，方便提供强大的录入、查询、统计、分析和报表等各种功能，较好的反映业务的基本情况和运行状况，满足信息化的要求。

根据本系统数据的特点，需支持 MySQL 和 Oracle 数据库（集群）作为系统的数据库平台，并且数据库开发方面采用标准 SQL 语句，以便将来的扩展和维护。系统采用数据库建模工具（如 PowerDesign），根据系统职责划分，构建出整个数据库。在构建数据库时，需定义好数据库表的约束、关联以及索引。

根据本系统的结构和应用场景，同时考虑到整个系统的一体化方案、功能扩展和灵活性，数据库采用主备的方式，数据备份支持实时备份，并支持使用数据库集群进行扩展。

5、接口设计

接口文档设计分为两部分：

5.1 对外接口设计

提供完整的接口文档，示例如下：

请求的基本参数

参数	参数名称	类型（长度范围）	参数说明	是否可为空	样例
基本参数					
service	接口名称	String(64)	接口名称。	不可空	send_goods_confirm_by_platform
partner_id	合作者身份 ID	String(16)	签约合作方的钱包唯一用户号。	可空	2088001159940003
input_charset	参数编码字符集	String(10)	商户网站使用的编码格式，如 utf-8、gbk、gb2312 等。	不可空	GBK
sign	签名	String(64)	参见“签名机制”。	不可空	e8qdwl9caset5zugii2r7q0k8ikopxor
sign_type	签名方式	String(10)	签名方式只支持 DSA、RSA、MD5。	不可空	MD5
return_url	页面跳转同步返回页面路径	String(1000)	钱包处理完请求后，当前页面自动跳转到商户网站里指定页面的 http 路径。批量，多商品的接口，无此字段		
memo	备注	String(1000)	说明信息	可空	

同步返回时，需要的基本参数

参数	参数名称	类型 （长度范围）	参数说明	是否可为空	样例
基本参数					
is_success	成功标识	String(1)	表示接口调用是否成功，并不表明业务处理结果。	不可空	T
partner_id	合作者身份 ID	String(16)	签约合作方的钱包唯一用户号。	可空	2088001159940003
input_charset	参数编码字符集	String(10)	商户网站使用的编码格式，如 utf-8、gbk、gb2312 等。	不可空	GBK
sign	签名	String(64)	参见“签名机制”。	不可空	e8qdwl9caset5zugii2r7q0k8ikopxor
sign_type	签名方式	String(10)	签名方式只支持 DSA、RSA、MD5。	不可空	MD5
error_code	返回错误码	String(30)	参见附录	可空	PARTNER_ID_NOT_EXIST
error_message	返回错误原因	String(200)	参见附录	可空	合作方 Id 不存在
memo	备注	String(1000)	说明信息	可空	

5.2 内部接口设计

1. 发布 façade 接口 jar 包,包含了 API、request、response
2. 提供接口对应的 response 返回码说明，及接口所需属性枚举常量定义

示例如下：

接口名称:	出款-fundout			
请求参数	属性	描述	是否必填	字段类型
FundoutRequest	fundoutOrderNo	交易凭证号	Y	String(32)

	paymentOrderNo	支付凭证号	Y	String(32)
	memberId	会员 Id	Y	String(32)
	productCode	产品编码	Y	String(32)
	accountNo	储值账户号	Y	String(32)
	amount	金额	Y	Money
	cardId	卡号 Id	N	String(32)
	cardNo	卡号	N	String(32)
	cardType	卡类型(DC/CC)	N	String(2)
	name	户名	N	String(32)
	bankCode	银行编码	N	String(32)
	bankName	银行名称	N	String(64)
	branchName	分支行信息	N	String(256)
	branchNo	联行号	N	String(12)
	prov	省市信息	N	String(64)
	city	城市	N	String(64)
	companyOrPersonal	对公/对私	N	String(1)
	fundoutGrade	到账等级		String(1)
	purpose	目的	N	String(256)
	extension	扩展信息	N	String(2000)
返回参数	属性	描述	是否必填	字段类型
	returnCode	返回码	Y	String
FundoutResponse	returnMessage	返回信息	N	String
	extension	扩展信息	N	String

6、模块功能介绍

6.1 钱包

6.1.1个人钱包

功能模块	功能点	描述

基本产品	充值	通过收银台将外部资金转入钱包账户
	提现	需实名认证
	转账到账户	钱包账户间转账
	转账到卡	钱包账户转出到任意银行卡
银行卡管理	添加银行卡	管理用于提现的银行卡
订单管理	交易查询	交易、充值、提现、转账、转账到卡、退款记录查询
	合并付款	多笔交易合并后一次付款
登陆	单点登陆	
	登陆验证码	
账户管理	登陆密码	修改密码，手机、邮箱找回
	支付密码	修改密码，手机、邮箱找回
	密码安全控件	
	实名认证	上传身份证
	绑定手机管理	绑定、修改、解绑
	绑定邮箱管理	绑定、修改、解绑
帮助中心	帮助中心	钱包介绍、账户设置、付款方式、安全服务、规则协议介绍

6.1.2企业钱包

功能模块	功能点	描述
基本产品	充值	通过收银台将外部资金转入钱包账户
	提现申请	需实名认证
	转账到账户申请	钱包账户间转账
银行卡管理	添加银行卡	管理用于提现的银行卡
订单管理	交易查询	交易、充值、提现、转账查询
	钱包对账单	钱包账户收支明细
	结算对账单	收单交易、退款及汇总信息
	对账单下载	收单交易具体付款、结算、退款明细查询和下载，CSV 和 Excel
登陆	单点登陆	
	登陆验证码	
账户安全	登陆密码	修改密码，手机、邮箱找回

	支付密码	修改密码，手机、邮箱找回
	密码安全控件	
	实名认证	上传营业执照、组织机构代码证、法人身份证、开户许可证、ICP 证等
	绑定手机管理	绑定、修改、解绑
	绑定邮箱管理	绑定、修改、解绑
操作员管理	添加操作员	添加一个可以独立登陆的操作员
	权限设置	授予操作员提现、转账、账号管理及操作员管理的权限
	重置登陆密码	重新设置操作员的登陆密码
审核记录	提现审核	审核提现申请
	转账审核	审核转账申请
帮助中心	帮助中心	钱包介绍、账户设置、操作员管理、审核管理、安全服务、规则协议介绍

6.2 收银台

功能模块	功能点	描述
支付渠道	网银支付	跳转银行网银完成支付
	快捷支付	
	余额支付	直接用钱包账户余额支付
	组合支付	网银+余额，快捷+余额
支付安全	支付密码验证	
	密码安全控件	
运营功能	定制支付渠道	根据产品等要素定制可用支付渠道

6.3 网关

6.3.1收单网关

功能模块	功能点	描述
交易类接口	即时到账交易接口	买家付款后，卖家立即收到货款；支持有脸、无脸支付；支持分润
	担保交易接口	买家付款后，货款暂由平台保管，买家发起确认收货后，卖家才收到货款；支持有脸、无脸支付
	确认收货接口	支持分润

	退款接口	支持退分润
	交易取消接口	取消交易
转账类接口	转账接口	账户间转账交易
出款类接口	付款到卡接口	将会员账户的资金提现到指定银行卡
控制类接口	冻结资金接口	冻结指定会员账户的资金
	解冻资金接口	根据原冻结资金订单解冻部分或全部资金
查询类接口	交易查询接口	交易、退款、提现订单查询
合作方通知	合作方通知	交易、退款、出款、转账状态变更通知

6.3.2会员网关

功能模块	功能点	描述
个人会员类	开个人户接口	
	激活接口	激活会员
	修改手机号	修改个人会员手机号
	修改个人信息接口	修改个人会员的会员名称
企业会员类	开企业户接口	
	修改企业信息接口	修改企业会员的信息
	新增银行卡接口	为企业会员绑定一张银行卡
公共	查询余额接口	查询会员所有账户余额和可用余额

6.4 后台

6.4.1运营管理系统

功能模块	功能点	描述
订单管理中心	联合查询	订单全景视图查询
	订单查询	按时间段，业务类型（交易、充值、出款），会员标识，交易金额范围来查询订单
	支付前置	业务订单、支付订单查询
	统一通知	系统间通知情况查询，及通知补发
	机构订单管理	机构订单、结果查询
	统一缓存刷新	刷新特定系统使用的分布式缓存

银行渠道管理	基础信息管理	与支付相关的基础信息（如：分支行、卡 bin 等）查询
	信息导入	与支付相关的基础信息（如：分支行、卡 bin 等）导入
	资金源配置管理	资金机构、目标机构、资金源、渠道接口、维护期配置管理
	路由规则管理	渠道路由规则管理
	结果代码管理	API 结果代码，统一结果代码管理
	机构归档模板管理	批量文件出款打批配置
	系统配置管理	备付金余额查询后通知邮件地址，手机号码的配置
	渠道缓存管理	新增或修改渠道的配置后刷缓存、让别的系统取到最新的信息。
支付清结算	清结算配置管理	支付服务、清结算协议、清结算规则、资金源信息配置
	缓存管理	修改支付服务、清结算协议、清结算规则后需要刷新缓存
	定时任务触发器	手工控制清算出场等任务执行
	控制指令执行	手工控制清算场次出场、支付重试等
会员管理	会员导入	老系统会员数据迁移
	会员信息核对	用户提交的信息核对，甄别会员身份的合法性
	会员综合管理	查询会员详细信息
	会员缓存管理	修改商户信息后，刷新会员缓存
	商户配置	新增商户并给商户配置对应的即时到账、担保交易等接口权限。
	实名认证	个人、企业实名认证审核
运维工具	运营对账	对账定义、计划和任务管理
	联合查询配置	配置订单关联及显示
	储值后台	账务系统缓冲入账规则及明细管理
运营工具	费率配置管理	支付算费策略配置
	限额限次配置管理	限额限次策略配置

6.4.2资金管理系统

功能模块	功能点	描述
入款管理	退款管理	手工退款后置状态
	线下充值	凭证文件上传、线下充值登帐
	入款补单	文件补单、补单查询

出款管理	出款记录查询	查询、退票
	文件出款	出款文件生成、下载，复核文件回导、核对，结果文件回导、核对
	重路由	切换出款渠道
	退票记录查询	退票记录查询
资金对账	银行交易对账	清算文件上传、对账、汇总确认
	对账管理	渠道对账、文件解析配置
	流水管理	入账流水、清算流水、历史流水管理，入账流水汇总查询
会计管理	科目管理	三级科目管理、科目树查询
	账户管理	内外部账户查询，创建内部户，账户变动明细查询
	挂销账	清算流水挂、销账，长短款挂、销账
	凭证管理	凭证查询
	登帐管理	内外部账户登帐、批量登帐
综合管理	审核管理	操作审核、审核日志查询
	财务报表	试算平衡表查询、下载
	会员管理	会员账户查询
	文件解析管理	批量登帐等文件解析脚本管理

6.4.2.1 相关功能细节说明：

- 账务和会计对账

凭证系统可以记录原始凭证、交易凭证、支付凭证等等以及中间处理过程的一系列凭证，真正保证帐帐相符、帐证相符、帐表相符、帐实相符。

- 账账相符：核对不同会计账簿记录是否相符。包括：总账有关账户的余额核对；总账与明细账核对；总账与日记账核对等。在现金账户体系里，由报表之间的核对来完成这个任务。
- 账证相符：主要体现在会计凭证与原始凭证的核对上。

- 账表相符：是将报表与有关的账簿记录相核对。核对总分类账、明细分类账与各报表的相关项目数据是否一致，查明账表是否相符。现金账户的帐表核对主要是用账户余额和科目明细表余额的勾稽关系来完成的。
- 账实相符：主要体现在财务日记账面余额与银行实存余额的核对上。

而且对账系统采用多频度，多层次的对账方式，每 10 分钟就会对不同模块间的凭证进行对账，能在第一时间发现问题，及时处理，尽可能地降低损失。

6.4.3风控管理系统

子系统	功能模块	功能点	描述
风控管理后台	业务查询	出款风险订单查询	出款业务风险订单查询处理
		入款风险订单管理	入款业务风险订单查询处理
		风险资金落地管理	资金源风险订单
		异常充值退款	异常充值资金，手工退回
	账户管理	账户冻结解冻	账户冻结解冻申请、审核、复核
		余额冻结解冻	余额冻结解冻申请、审核、复核
	业务审核复核	审核	风险订单、异常订单、账户操作审核
		复核	风险订单、异常订单、账户操作复核
	基础信息管理	黑名单管理	黑名单库管理
风控监控后台	风控规则管理	检查点管理	风控埋点
		规则管理	风控规则
	风控策略管理	策略上下线	检查点关联规则
	综合管理	操作日志	

6.4.3.1 风控子系统说明

- 风控系统支持多流程多控制点；
- 灵活的风险控制框架
- 不同风险采用不同应对措施，且可以根据业务自行定义风控的埋点和流程；
- 脚本化风控规则配置，快速上线新的风控规则
- 采用 Wilson-Clark 安全模型定义正常交易类型，对异常交易的严格监控
- 支持旁路设置,可以在不影响运营的情况下完成一些规则上线效果的观察,以便正式上线运营前做适当调整
- 支持黑白名单配置
- 规则和参数分离,运营人员要求相对较低,只需要配置参数即可

6.4.4其他管理后台

子系统	功能模块	功能点	描述
加密设置系统	加解密	查询原文	显示加密前的原始数据
		加密	显示加密后的密文
	更新证书	创建、下载、更新证书	更新加密证书
消息管理系统	消息发送	消息发送	测试短信、邮件通道
	消息管理	查询消息详情	
		重发、转发消息	
文件系统管理	资源管理	文件目录浏览	
		下载文件	
	权限管理	接入系统管理	
		下载权限管理	
报表综合管理系统	报表管理	报表查询	自定义报表查询
		报表配置	自定义报表配置
		统计计划配置	自定义统计任务
	综合管理	配置备份	报表、统计计划配置导入导出
		操作日志查询	

6.4.5基础设置系统

功能模块	功能点	描述
基础信息管理	系统管理	后台系统信息录入，设置管理员
	系统角色管理	系统角色管理
	系统资源管理	系统菜单、按钮信息管理，资源角色导出导入
	审计日志查询	资源访问情况记录
权限管理	角色资源配置	给角色分配资源
	角色用户配置	给用户分配角色
	系统黑白名单配置	给用户设置资源访问的黑白名单
	全局黑白名单配置	设置全局资源访问权限的用户黑白名单
	用户管理	LDAP 同步，重置本地登陆密码，设置登陆方式

7、商户管理

7.1 开通商户申请

商户填写申请资料包括开通产品、费率、结算周期、有效期等信息。

上传认证文件。

7.2 审核通过

7.2.1产品权限配置

交易接口：即时到账交易、担保交易、交易取消、退款、结算（分账）、付款到卡、交易查询。

7.2.2支付方式权限配置

支付方式：余额、网银、POS 刷卡、现金、快捷

7.2.3费率、结算周期配置

费率，结算周期等设置可以针对单个商户

费率支持多种模式。如：固定费率，单笔，阶梯等。

7.3 审核拒绝

商户填写的资料及上传认证文件不符合要求，审核拒绝，商户修改后，重新申请。

8、运营管理

8.1 资金对账

资金对账分为入款资金对账、退款资金对账、出款资金对账。

资金对账是系统流水与银行对账流水进行金额、订单号的比对，来判断系统与银行之间是否存在差异问题。

清结算人员对对账结果进行查询，处理账务不平的问题。

8.1.1系统自动获取对账单

有些银行提供接口，支付系统自动获取对账单。

8.1.2人工获取对账单

有些银行不提供接口，清结算人员手动下载对账单。

1）去银行网银端下载对账文件。

2）导入到系统中。

经办人员下载对账文件并导入系统；

复核人员下载对账文件并导入系统，

系统自动核对经办人员和复核人员导入系统的对账文件。

3）对导入的文件进行资金对账。

4）将对账确认过的资金流水进行汇总确认操作。

5）完成账户变动，完成对账操作。

8.1.3对账处理结果查询

由于对账的数据量往往比较大，对账操作需要耗时比较长。通过处理结果查询模块可以了解到对账状态等信息。

8.1.4对账流水查询

8.1.4.1 入账流水查询

入账流水是指内部系统发生的交易流水。

该功能用来查询未汇总确认之前的入账流水。

8.1.4.2 清算流水查询

清算流水是指银行端的流水，一般是通过银行对账文件导入获取。

注：清算人员只能对自己上传的清算流水进行修改、删除、对账等操作。

8.1.4.3 历史流水查询

当入账和清算流水汇总确认完毕后，系统会把这部分流水迁移至历史流水中。

8.1.4.4 入账流水汇总

通过汇总可以了解每个渠道的发生金额和发生笔数。

8.1.5掉单问题

8.1.5.1 系统自动补单

8.1.5.2 人工补单

当系统出现入款掉单的情况，而超过了系统能自动处理的补单范围，这个时候就需要通过资金管理后台介入，进行人工补单。上传的文件可以是当天的银行交易文件也可以是隔日的银行对账文件，具体视不同的渠道处理。

8.1.6对账渠道管理

该功能是用来控制是否对某个渠道的流水进行对账，是否

自动汇总确认。

8.1.7文件解析维护

该功能是用来配置对账脚本，一般由技术人员操作

8.2 线下充值

当会员从系统外打款至公司银行账户后，需要通过线下充值功能从银存登帐至会员账户。充值金额与线下打款发生的金额保持一致。

8.3 退款管理

退款管理是提供给清算人员查询人工退款记录、修改退款状态、生成退款文件，批量退款。

8.4 出款管理

8.4.1直连出款

银行提供直连出款接口，系统自动把出款请求发送到银行请求出款，清结算人员每日操作出款对账进行账务核对。

8.4.2文件出款

银行没有提供直连出款接口，需要清结算人员把出款文件上传到银行网银进行出款请求。

操作流程如下：

1) 清算人员首先根据出款文件生成时间去系统下载出款文件。
2) 将提现文件提交到银行控台后，再下载到本地通过此处回导，来确定银行接受到的文件没有错误。比对从银行下载到的提现请求文件和上传的原件。这里可以发起批

次核对和批次废除的操作。

3) 将核对通过的出款文件上传至银行系统，并将出款结果文件下载导入到资金管理后台。

通过比对出款文件和回导的结果文件，来判断出款是否正确。核对首次导入和二次导入的提现结果文件是否一致。查询结果文件统计信息，可以发起对账请求，显示对账结果。通过组合查询条件，查询匹配的出款记录。并可以查询出款记录详细信息、修改出款记录、设置出款打批时间，对已经显示出款成功的记录进行退票操作。

8.5 会计管理

该模块主要处理登帐、挂销账、内部户开户、科目管理等操作。

8.5.1科目管理

通过可以管理可以查看科目树，创建新科目，修改，删除已有科目。

8.5.2账户信息查询

根据组合查询条件查询内外部户账户信息，并可以查看到账户的账户变动明细。

8.5.3凭证查询

清算人员对于资金、账务的操作很多都会生成凭证，通过凭证查询可以查看到原始交易信息。

8.5.4登帐

当需要做登帐业务时，可以使用资金管理平台的登帐功能。登帐分为：内部户登帐、外部户登帐、内转外登帐、外传

内登帐。

登帐操作是账务处理的一种，非必须情况下不建议使用。

如资金对账出现多账时应使用挂销账操作，而非登帐处理。

登帐完成后，需要复核人员审核通过才能生效。

- 批量登帐

当存在大量登帐需求时，以上传文件的方式实现批量登帐操作。

8.5.5挂销账

挂账是指业务操作中存在待查问题，比如对账多账等，当前无法解决，这个时候可以采用挂账的形式，将这笔待查操作挂账到挂账账户，如待查长款、待查短款。

销账是对挂账的冲销操作，将挂账账户的金额销账到指定账户。

挂销账操作，需要复核人员审核通过后才能生效。

待查长款挂账类型包括“待查长款-其他-挂账”、“待查长款-退票-挂账”和“待查长款-线下充值-挂账”三种，区分各类待查长款，是因为线下充值业务，退票业务，是待查长款中，比较常见的，业务量较大的，为了规避资金风险，人员操作风险，所以将这 2 大类待查业务单独挂账，单独销账，规定销账方向，同时也将内外部户的销账分离。

清算人员在资金对账后，会发生多帐或者金额不符的情况，而操作人员不明确资金的来源，需要根据规则将暂不明确的资金做挂账处理。此时使用的挂账类型使用“待查长款-其他-挂账”或者“待查短款-其他-挂账”。

当涉及跨行提现失败时，清算人员通过“待查长款-退票-挂账”，来处理资金流动。

挂账类型只有“待查短款-其他-挂账”，主要用于资金对账多帐，银行多扣钱情况，目前基本不会发生。

挂销账映射关系介绍：

挂账类型	对应可销账类型
待查长款-其他-挂账	待查长款-其他-转线下充值，待查长款-其他-销重复入款，待查长款-其他-转退票，待查长款-其他-销内部账户，待查长款-其他-销补单
待查长款-线下充值-挂账	待查长款-线下充值-销会员户，待查长款-线下充值-转其他
待查长款-退票-挂账	待查长款-退票-销账，待查长款-退票-转其他，待查长款-退票-销内部账户
待查短款-其他-挂账	待查短款-其他-销内部账户

8.6 资金变动审核

审核是复核人员用来审核经办申请的业务。

审核人员通过查询条件定位到待审核的订单，查看审核订单详情后，判断是否审核通过。

所有人工发起的账务变动都需要审核。

8.7 联合查询

可自定义的订单查询服务，可逐级关联，遍历查询出所有相关凭证，提醒订单的整个生命周期。运营人员可以根据该查询定位异常订单的原因。

通过不同账户、订单、流水等不同类型的信息查询出对应的信息，但仅能查看不能做任何操作。

8.8 运营对账

包括对账任务管理、对账计划管理、对账定义管理等。

通过运营对账能及时发现支付清结算系统在业务运营过程中，由于网络延迟、消息通知堵塞、程序 BUG 等原因引起的

问题。对账发现的异常结果将以邮件或短信的方式发送到指定的负责人，负责人能够根据对账结果快速定位问题；发现问题的及时性、可定位性大大提高，问题造成的影响面大大降低。

对账定义：定义“哪个子系统的数据”和“哪个子系统的数据”进行对账

对账计划：对账定义执行的时间和频率

对账任务：对账计划执行的结果

对账标签：对账结果送达的通知地址（如 Email,手机号）

8.9 资金渠道配置

接入银行渠道，开发人员完成编码工作，配置银行接口的信息，如访问 url 、属性值等信息。

8.10 实名认证审核

个人会员、企业会员、商户提交的认证资料，运营人员核对信息后进行审核。

9、风险管理

9.1 风控规则

9.1.1规则配置

风控规则分类	具体规则说明	建议措施	说明	备注
防钓鱼相关	浏览器 Referer 信息为空	预警	非法来源或其他途径导致的系统无法获取 Referer 信息，需要关注	

	网银支付钓鱼拦截	进入风控人工管理后台，1.审核：业务审核-》风险资金落地审核（审核人员决定订单是继续完成，还是拒绝该订单。） 2. 复核：业务复核-》风险资金落地复核（复核人员是否同意 审核人员的审核结果。）	被判定为有风险的订单，资金被滞留在入款中间账户，由人工审核	审核交易订单金额和上送银行扣款金额是否一致
	收单请求的域名防钓鱼规则 （域名白名单，限制请求的来源）	驳回	解析正常来源交易中的 Referer 信息，获取域名；按商户分别配置的域名白名单进行匹配	
防用户账户入侵	个人会员单笔提现限额	进入风控人工管理后台，1.审核：业务审核-》出款风险订单审核（审核人员决定订单是继续完成，还是拒绝该订单。）	个人会员每笔提现金额超过指定额度时需要工作人员介入，进行审核。	在参数里配置额度，可按需调整
	个人会员每日提现限额		个人会员每日提现累计不能超过 20000（参数按需调整）	在参数里配置额度，可按需

		2. 复核：业务复核-》出款风险订单复核（复核人员是否同意 审核人员的审核结果。）		调整
	个人会员每月提现累计限额		个人会员每月提现累计额度限制。	在参数里配置额度，可按需调整
防商户账户入侵	商户单日提现次数限制	进入风控人工管理后台，1.审核：业务审核-》出款风险订单审核（审核人员决定订单是继续完成，还是拒绝该订单。） 2. 复核：业务复核-》出款风险订单复核（复核人员是否同意 审核人员的审核结果。）	商户单日提现次数限制。	在参数里配置次数，可按需调整
	商户单日提现累计限制		商户单日提现累计额度限制，超过指定的额度，需要工作人员介入审核。	在参数里配置额度，可按需调整
防平台方账户入侵	平台方单日出款限额	进入风控人工管理后台，1.审核：业务审核-》出款风险订单审核（审核	平台方单日出款累计额度限制，超过指定的额度，需要工作人员介入审核。	在参数里配置次数，可按需调整

		人员决定订单是继续完成，还是拒绝该订单。） 2. 复核：业务复核-》出款风险订单复核（复核人员是否同意 审核人员的审核结果。）		
黑名单相关	支付时，支付 IP 段在黑名单中	进入风控人工管理后台，1.审核：业务审核-》风险资金落地审核（审核人员决定订单是继续完成，还是拒绝该订单。） 2. 复核：业务复核-》风险资金落地复核（复核人员是否同意 审核人员的审核结果。）	被判定为有风险的订单，资金被滞留在入款中间账户，由人工审核	对交易时间，交易金额，及时间段内交易记录进行审核，是否异常
	会员提现黑名单	进入人工审核	如提现会员在黑名单中，该会员的提现申请需要审核	

其他	提现最小额度限制(不区分个人或商户)	驳回	如提现额度较小的申请。	
	CMF 风险资金落地	进入风控人工管理后台，1.审核：业务审核-》风险资金落地审核（审核人员决定订单是继续完成，还是拒绝该订单。） 2. 复核：业务复核-》风险资金落地复核（复核人员是否同意 审核人员的审核结果。）	入款(充值)成功后渠道放回交易是否有风险，如渠道返回该交易有风险，但是渠道还是会让这笔订单继续走下去，至于是否有风险，由支付平台来判断，如支付平台认为有风险，发起退款；如 支付平台认为属于正常情况，可以忽略。	

规则信息包括：规则所属的检查点，规则编号，类型（本地、远程或 Global，远程规则依赖服务器的资源，全局规则定义风险数据是否需要同步调用远程规则进行风险判定），引擎类型（无状态或有状态），引擎实例（有状态规则时选择），描述，Agenda（和规则中的 package 一致），是否支持短路（是的话如果本规则通过，则不再执行其他规则），规则内容（Drools 的规则脚本），状态（是否上线）等。

规则定义完成后，需要配置到策略中才会生效。

9.1.2策略配置

策略是风控系统中对于同一检查点内的规则的分组。

策略配置的信息包括：策略组（枚举字段中定义），编号，状态，过滤条件（检查点中设置过过滤字段的话），以及本策略组中选定的规则。

9.1.3风险事件查询

本功能用以查询按照风险事件存储配置存储的数据

9.2 风控后台操作

- 风险订单实时查询
- 账户冻结解冻（账户状态变更）
- 充值订单查询
- 风险资金落地审核查询
- 风险资金落地复核查询
- 风险关注订单查询

9.3 反洗钱

1. 大额可疑机制

无论是对公（就是两家企业间）还是对私（也就是个人）发生的任何交易，只要有交易发生了，涉及到动户（也就是你的帐户有资金出入）了，那么在一段时间后，反洗钱系统会根据交易情况生成各种各样的报表。很容易可以从某个帐户的交易中看出某一段时间内资金进出及额度情况。根据《人民银行反洗钱工作手册》中的规则，反洗钱系统中设置了与其相对应的预警机制，一旦触发，就会将情况报送给中台反洗钱工作人员，由他们进行判断是否真正是大额可疑。一旦确认，则报送

人行；反之，取消预警。也就是说，反洗钱系统根据规则筛选出交易，然后由人工进行二次判断。

2.黑名单机制

所谓黑名单，是指在交易过程中，首先会向反洗钱系统发一个查询，检查这个帐户的持有人是否存在在黑名单中，如果存在在黑名单中，反洗钱系统即时给正在交易的系统进行反馈，并提醒冻结帐户。

10、 运行设计

10.1 运行模块的组合

描述系统运行时，模块之间的调用，组合关系。给出在不同运行控制下，各个模块的组合方式，以及每种

运行所经历的内部模块的控制流和数据流。

10.2 运行控制

描述系统运行时，模块之间的调用控制关系，包括控制范围和作用范围等。说明各种运行方式及其具体操作步骤。

10.3 运行时间

描述系统对整体及单个模块运行时间的要求，以及所要达到的运行时间标准。

11、 数据库设计

11.1 物理结构设计

11.1.1 表空间 SQL 规程

Mysql 存储类型设置为：InnoDB

创建数据库（一个库就是一个 Schema）:create database

deposit

11.1.2 数据库用户创建

create user 'deposituser'@'%' identified by 'xxxxx';

11.1.3 角色授权

grant select,insert,update,delete,execute on `deposit`.* to 'deposituser'@'%';

11.2 运用设计

在进行数据库相关要素设计时，需要遵循如下规范

序号	项目	说明
1	表名	数据表名称以 T 开头，后跟模块名，模块名之后是业务名；三者之间用“_”分割开；业务名需要有特征含义的单词或缩写组成，如有必要，中间用“_”分割，例如：T_模块名_业务名。
2	字段名	字段名称必须用字母开头，采用有特征含义的单词或缩写，特殊情况可以使用拼音命名。不能使用特殊字符。
3	主键名	前缀为 PK_。主键名称应是 前缀+表名+构成的字段名。如果复合主键的构成字段较多，则只包含第一个字段。主键名长度最长 30。
4	外键名	前缀为 FK_。 外键名称应是 前缀+ 外键表名 + 主键表名 + 外键表构成的字段名。外键名长度最长 30(如果超过长度，表名可使用缩写)。 建议只给配置表建立外键，对数据量比较大的业务数据不要

		建立外键，否则操作地不会会对性能有比较大的影响，而且增加 dba 对数据操作的成本。
5	普通索引	前缀为 I_。索引名称应是 前缀+表名+构成的字段名。如果复合索引的构成字段较多，则只包含第一个字段，并添加序号。
6	唯一索引	前缀为 UK_。索引名称应是 前缀+表名+构成的字段名。
7	外键索引	前缀为 I_FK_。索引名称应是 前缀+表名+构成的外键字段名。
8	其他	

11.3 安全保密设计

不同应用程序根据 Schema 不同，创建不同用户；不同用户访问 Schema 权限不同，如：cmfuser 只有 cmf-Schema 的管理权限（增、删、改），对于其它 Schema 没有任何权限；reader 用户对所有 Schema 仅有查询权限。

12、 安全设计

12.1 敏感数据加密

用户敏感信息不可以直接落地数据库,或者明文展示在 log 信息中。需要加密处理,

12.2 密码锁定

为了防止用户暴力破解用户密码信息，密码在错误验证一定次数后可自行锁定，通过短信验证，或者邮件认证找回。

13、 系统安全设计

13.1 系统安全设计

13.1.1 完善的登录验证，密码找回流程设计

细化到产品，商户，账户的授权模型

所有资金操作的多人复核设计

对于不同层次的敏感数据，采用不同加密方式，兼顾安全和效率。且支持密钥统一定期更新。

13.1.2 防 SQL 注入

系统使用 MyBatis 框架作为一款半自动化的持久层框架，MyBatis 启用了预编译功能，在 SQL 执行前，会先将 SQL 发送给数据库进行编译；执行时，直接使用编译好的 SQL，从而来避免了 SQL 注入的问题。

13.1.3 防跨站攻击

系统内部做了 XSS 过滤，对用户输入的地方和变量都需要仔细检查长度和对”<”,”>”,”;”,”’”等字符做过滤；阻止攻击者利用在被攻击网站上发布跨站攻击语句不可以信任用户提交的任何内容。

13.2 软件安全设计

1）统一用户身份认证和权限管理，实现单点登录机制。

2）在设计上保护用户身份的安全，实现功能权限和数据权限控制，保证客户端与服务器以及服务器之间的数据传输安全、关键数据的存储安全。客户端与服务器端数据传输采用加密方式进行，可以利用 https 协议、对称加密技术和数字签名技术等来保证传输的安全性和不可抵赖性。对于系统的关键数据存储，可以采用加密存储方式，在对数据库的访问上，合理划分用户身份权限，按照要求把权限划分成可读、可写、读写、拒绝访问等多个类型，避免服务器端泄密的情况发生。

3）对于关键业务操作必须提供安全审计功能。将关键功能的使用权限严格限制在所要求的合法用户范围之内，并对这些用户的身份信息进行定期或不定期审查。要求系统记录完成的业务功能操作日志，包含操作人、时间、功能名称、所变更的业务内容、功能的等级等，通过事后对这些日志的审计，可以审查系统使用的违规情况。

4）提供数据完整性保证及行为的不可抵赖性保障。

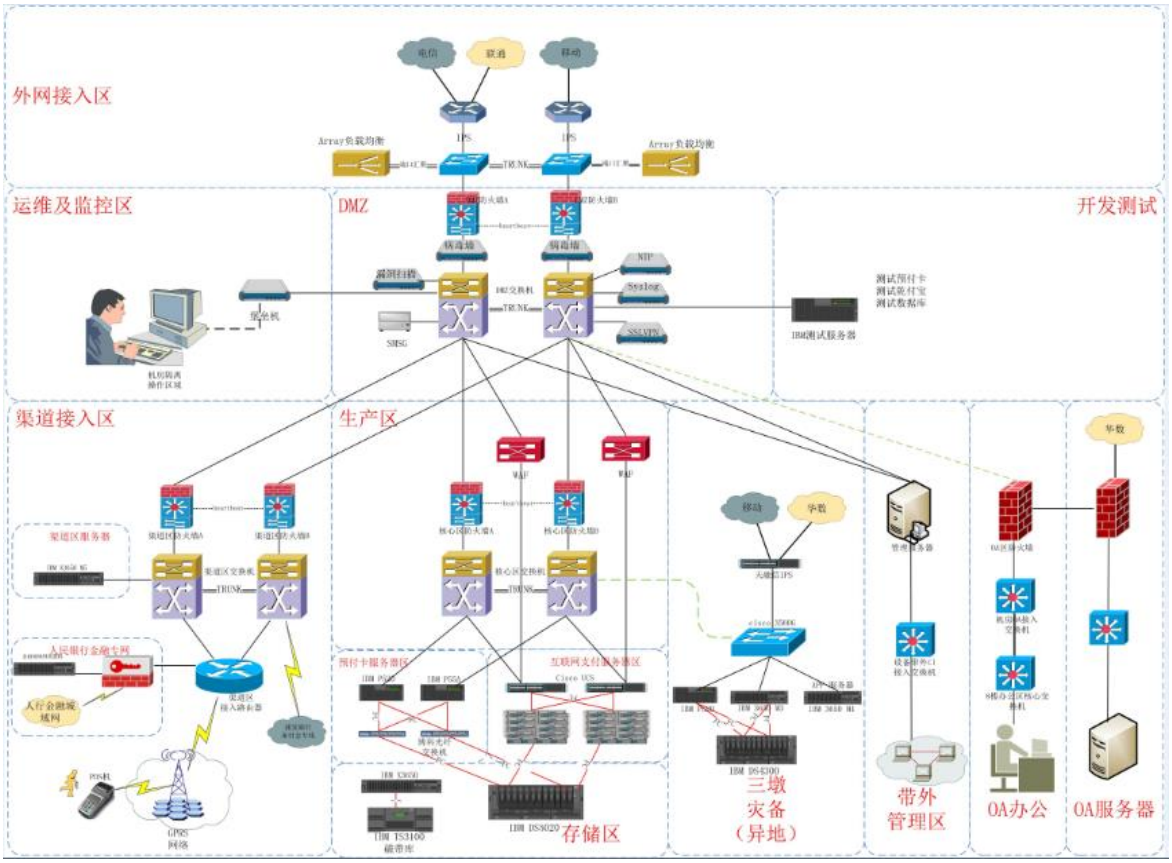
非对称密码密钥技术就是对数据的加解密密钥是成对出现的，有使用人持有并秘而不宣的密钥称为私钥，对其他人员、机构共享的密钥则成为公钥。利用在这种密码技术上发展起来的数字签名技术，就可以实现数据完整性保证及行为的不可抵赖性保障。

13.3 网络安全设计

13.3.1 网络架构设计

合理的网络拓扑设计

完善的理灾备解决方案



13.3.2 安全的网络设计

参考 cisco 的 SAFE 模型构建的划区域服务提供和全冗余的网络架构

完善的边界安全管理标准，依据不同的安全要求定制设备，避免安全事故的泛洪效应

13.3.3 完善的安全机制

对所有维护人员统一采用堡垒机的方式进行统一权限管理，对于服务器的用户进行最小化控制

建立了符合 ISO27000 的安全管理体系，来保障 IT 系统的

长期稳定运行

13.3.4 有效的权限管理

“最小化”权限控制

操作审计

异常操作报警

13.3.5 机制化的日常监控，维护

定期漏洞，病毒，木马扫描

及时更新系统补丁

安全设置定期 review

14、 系统维护设计

系统功能日常维护

定期对系统巡检。具体包括补丁升级的运行状况、运行日志检查、系统错误的归纳分析及解决。

对系统日常运行涉及的主机、数据库、中间件、应用情况、硬件设备进行及时监控，定期生成运行状态报告。对发现的问题，及时通知运维人员排除故障；对潜在可能存在的问题进行分析预警。

定期查看数据库里面的告警日志和慢查询日志，根据日志信息分析数据库的性能瓶颈，对数据库进行性能优化。