

密级：内部公开

# 乐家易付支付清算服务系统

## 总体设计方案

V4.0

### 知识产权说明

本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属浙江航天电子所有，受到有关知识产权及版权法保护。任何个人机构未经浙江航天电子的书面授权许可，不得复制或引用本文件，包括任何介质的载体。



## 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	范光涛
2	2.1	设计原则	2016-06-03	V1.0	V2.0	郭彦江
3	2.2	系统功能结构	2016-07-10	V2.0	V3.0	韩凯
4	2.6	应用系统扩展功能	2016-08-01	V3.0	V4.0	韩凯

## 目录

1、	前言.....	1
2、	总体设计.....	1
2.1	设计原则.....	1
2.2	系统功能结构.....	6
2.3	系统软件架构.....	7
2.4	与其它系统的接口.....	13
2.5	在线支付系统数据存储设计.....	15
2.6	应用系统扩展功能.....	15
3、	系统功能说明.....	16
3.1	在线支付子系统.....	16
3.2	商户平台子系统.....	19
3.3	系统管理子系统.....	22
4、	系统集成方案设计.....	28
4.1	网络拓扑图.....	28
4.2	主机平台方案.....	29
4.3	数据存储方案.....	29
4.4	数据备份方案.....	30
4.5	网络设备方案.....	32
4.6	系统安全方案.....	34
5、	系统备份与恢复.....	34
5.1	应用程序备份.....	35
5.2	主机系统备份.....	35
5.3	恢复策略.....	36

## 1、前言

- 确立支付清结算系统（简称本系统）的业务目标和性能目标；
- 界定支付清结算系统的功能范围；
- 明确支付清结算系统所涉及的实际业务流程和使用场景；
- 和后期的需求变更单文档一起作为支付清结算系统项目验收的标准（如果两者有冲突，以变更文档为准）。

本文档的内容将作为项目设计及实现阶段的基础，具有重要的指导意义。

## 2、总体设计

### 2.1 设计原则

#### 2.1.1 先进性

系统的设计中要体现技术的先进性，以确保系统在未来一定时期内，具有技术领先性。

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、遵循 JavaEE 开放标准，整体采用 B/S 结构完成系统的搭建。

#### 2.1.2 实用性

系统的先进性与实用性之间存在一定得矛盾，太先进的东西不一定实用。系统设计必须找好两者之间的结合点，使设计出来的软件一方面满足先进性的要求，体现行业最新技术水平和技术发展趋势，保证系统在很长一段时间内不落伍；

另一方面，要充分考虑系统相关人员的利益，以人为本，从提升系统性能、搭建更便利的操作界面、减少用户操作步骤、提高输入速度、易于管理、部署、升级等多个方面入手，提高系统的实用性。使设计出来的软件要简洁而不简陋、美观而不花哨、庄重而不失灵性。

### 2.1.3 可扩展性

在设计上必须具有适应业务变化的能力，如随着业务的发展，需要增加新的支付清结算场景、增加新的风控规则、增加新的管理权限等，应尽可能地保证业务变化造成的影响局部化。

利用平台提供的开放接口，在交互层上进行扩充，引进标准界面组件、web 交互框架、公共功能库等内容，大大提升系统的可维护性和可扩展性。

### 2.1.4 易用性

系统设计中，将充分考虑系统的易用性。具体包括：

1. 所有的业务功能界面操作简单；
2. 突出用户的中心地位，在满足系统交互要求的同时考虑降低用户劳动强度，保证用户使用习惯；
3. 按个人或组织进行信息组合，以提供快速准确的信息服务；
4. 业务表单尽量做到所见即所得；
5. 操作错误的提示信息是用业务用语描述；
6. 详细完整的用户使用指南。

### 2.1.5 可靠性

1) 基础平台软件应具有稳定性、可靠性、容错性、健壮性。

基础软件平台采用业界先进的、久经考验的 oracle/mysql、linux、tomcat 等作为系统软件，可信度非常高。在稳定性、可靠性、容错性、健壮性等多个因素的考量上，要以提升系统质量为根本要义，以提升软件质量来保证这些要素的根本实现。

2) 提高应用系统的开发质量，优化软件，减少软件缺陷。

系统的质量是通过系统设计、实现、过程质量保障等一系列手段来实现的，在软件开发过程中要综合运用这些手段来帮助提升系统质量。在软件优化上，从性能优化和易用性优化等多个方面进行，提高系统性能并保证完成的软件易用、好用、适用。加强系统测试，采用功能测试、回归测试等多种手段进行代码实现缺陷排查，加强白盒测试、系统代码审查、同行评审等，强化软件质量意识，提升软件质量水平。

3) 整个系统要有一套完善的错误处理机制，应保证在正常情况下和极端情况下业务逻辑的正确性。

系统通过设置一整套的异常处理机制，区分系统异常和应用异常两种情况。其中的系统异常是由于发生难以恢复的系统错误，如网络、硬件等等问题而产生的，对这些异常的处理要做到早发现，早预防，在系统发生后要尽快查找原因并予以解决，并且系统要设置捕捉机制，保证系统出现难以恢复的系统异常后能够释放系统资源，并对相关的系统管理

人员提出警示等。而对于应用异常，则是可以恢复的，系统必须要能够提供应用异常的捕获机制，根据异常的情况，编排合适的提示信息提示给引发该异常行为的具体操作人员，帮助其发现系统使用过程中的问题，如录入超出边界，录入数字非法、越权使用系统等等。

### 2.1.6 可用性

1) 系统自动失效转移，避免单点故障而影响整个系统的正常运行。系统部署采用负载均衡方式部署，利用负载均衡技术的失效转移特性，消除单点故障的可能性。负载均衡在各个节点上合理分配负载，在系统运行过程中，如果一个节点出现故障，控制系统将会自动把该业务转移到其他节点上，而这一切对于用户来说都是透明的，前端用户根本感觉不到这种失效情况的存在。在服务器节点修复之后，可以动态的加入到集群中，恢复其服务能力。

2) 制定应急预演计划和灾难恢复计划。基于过去的系统运营经验，将提供完整的应急预演计划和灾难恢复计划。确保在极端情况下，保证系统的可恢复性。

3) 高效的备份 / 恢复流程和技术，缩短由于数据库、硬件和应用升级等所带来的停止服务时间。

### 2.1.7 可维护性

1) 采用面向服务架构（SOA）、模块化、组件化和松耦合系统设计。软件能够被简单方便地修改和升级，包含可读性、可修改性、可测试性等。

2) 基于标准的 HTTP 协议通讯，减少对防火墙以及服务

递送机制的维护工作。

3) 基于工作流和规则库。系统应采用参数化设计, 可以根据实际情况对功能进行灵活调整而无需修改程序。

系统整体框架的设计和实现按照 SOA 思想进行搭建, 模块化和组件化是本系统搭建的基本要求。各个组件通过软件平台进行通讯, 相互之间不直接联系, 是一个松散耦合的系统。

平台所提供的规则库、权限、报表等可参数化配置模块, 也给系统带来了前所未有的灵活性, 能够在不修改软件代码的情况下通过配置系统参数就能够进行软件功能的调整, 满足业务系统扩充的需要。

#### 2.1.8 可管理性

1) 每个层次、每个构件都提供标准的管理接口。实现统一的、一致的监控和日志功能。

2) 提供实时系统健康检查手段, 准确易用的监控、错误定位功能。

#### 2.1.9 安全性

1) 统一用户身份认证和权限管理, 实现单点登录机制。

2) 必须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、VPN 技术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。

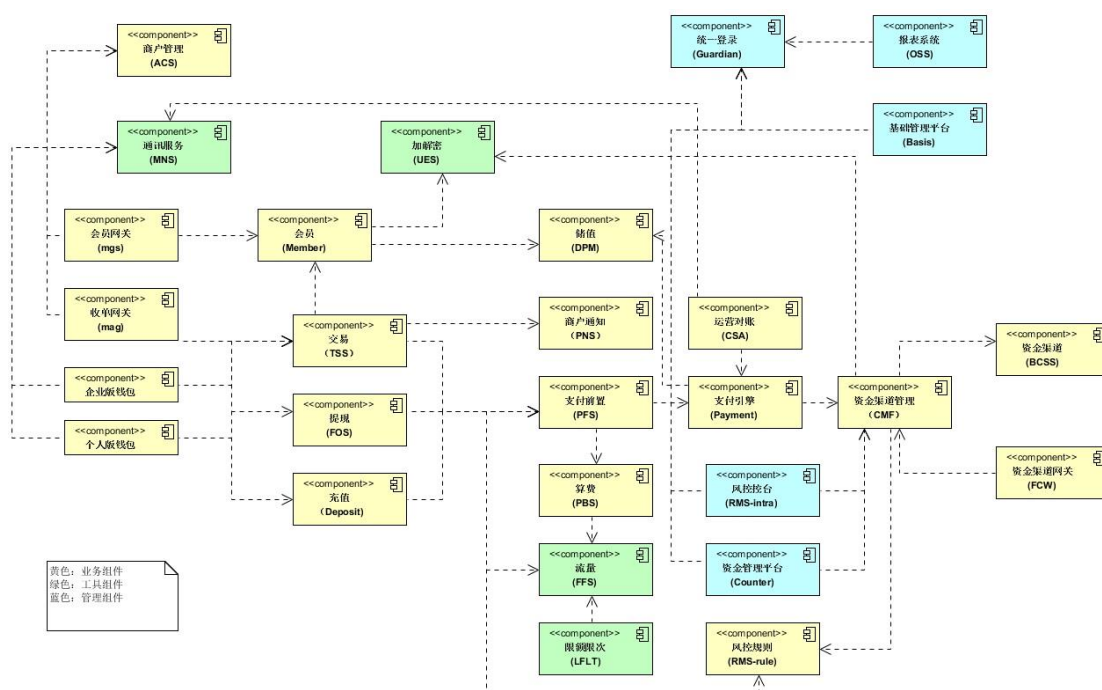
4) 提供数据完整性保证及行为的不可抵赖性保障。非对称密码密钥技术就是对数据的加解密密钥是成对出现的，有使用人持有并秘而不宣的密钥称为私钥，对其他人员、机构共享的密钥则成为公钥。利用在这种密码技术上发展起来的数字签名技术，就可以实现数据完整性保证及行为的不可抵赖性保障。

## 2.2 系统功能结构

系统中，按职责划分各个功能模块

统一消息服务	统一缓存服务	数据处理服务	统一文件存储	统一文件存储控台	资金渠道回调站点	模拟银行渠道	缓存监听	会员网关
静态资源	统一缓存管理	测试应用	内部系统静态资源	会员网关测试应用	验证码处理	储值	储值批量任务	储值管理
会员账户	商户通知服务	收银台	收银台接口	出款服务	风控规则	规则cep引擎	风控规则监控系统	风控后台
统一凭证系统	短信发送系统	短信发送系统的mq监听器	短信发送系统定时任务	短信发送管理系统	统一加密	资金渠道管理	资金渠道管理任务启动	限额限次
应用配置服务	新支付引擎	短信网关服务	算费支撑系统	充值服务	交易服务	计费系统	支付前置-支付服务	支付前置-对外基础服务
支付前置-后台管理服务	充值服务定时任务	权限API接口	权限管理后台	统一审计API接口	统一鉴权API接口	统一登录系统	收单网关	流量系统
运营对账系统	管理后台	统一加密控制台	资金管理平台	资金管理后台-接口	运营支撑平台	征信库	支付业务运行服务	统一认证系统
手机钱包	手机收银台	支付引擎-定时任务	支付引擎-结转	测试银行出款	会员权限管理（内部配置使用）	会员权限管理（会员/操作员使用）	个人钱包	企业钱包
认证服务	短信网关	mns-mock渠道（外部WEB服务）	资金托管渠道	安全中心	账户管理	帮助中心	支付运营后台	信贷管理后台

各主要模块间的逻辑视图如下



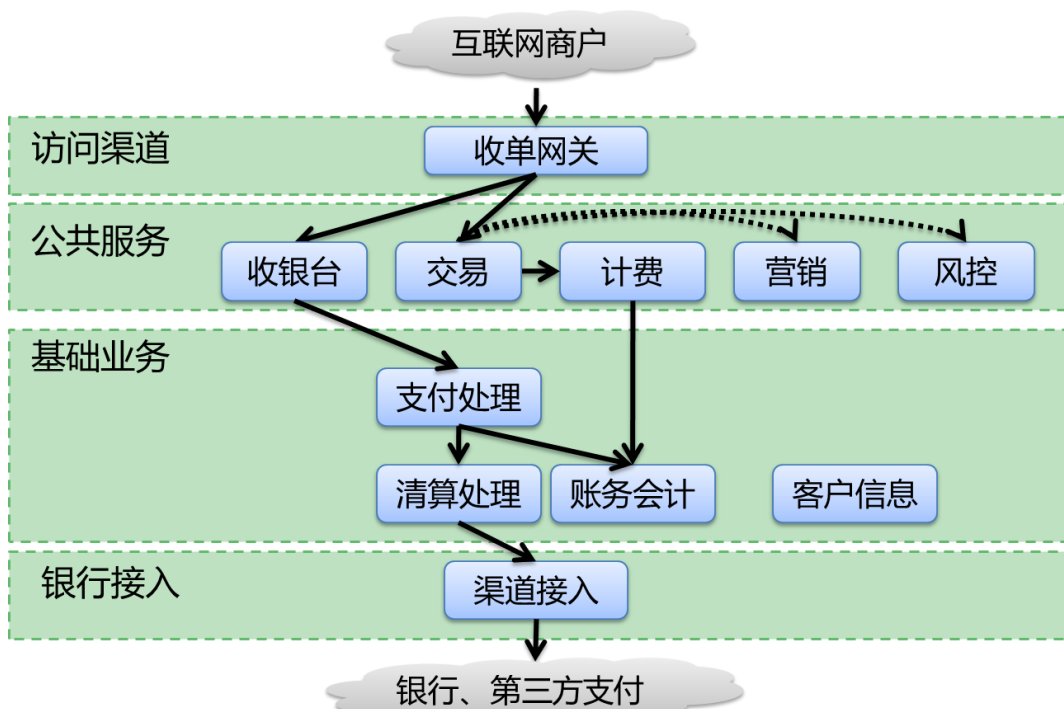
## 2.3 系统软件架构

### 2.3.1 应用架构

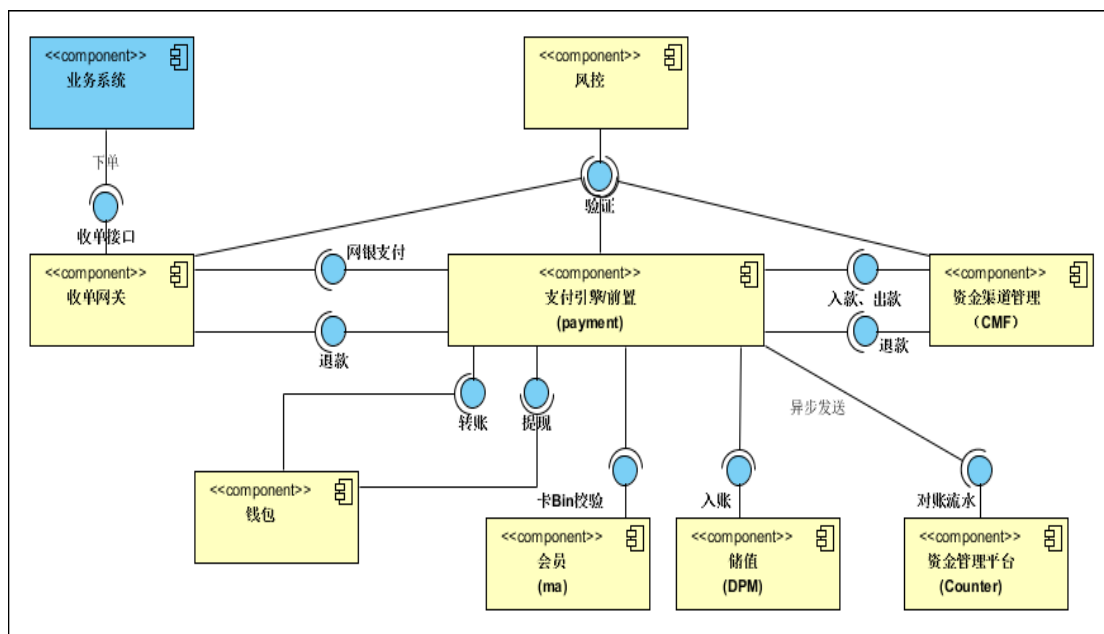
## 1、总体架构



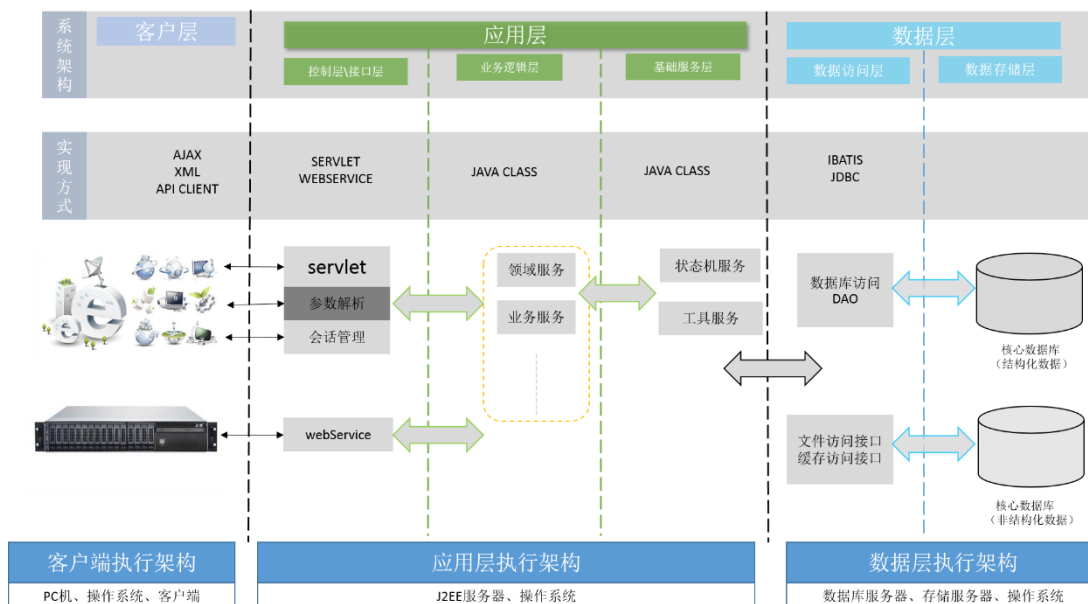
## 2、支付业务系统处理模式



### 3、支付调用的模块和概略



### 2.3.2 技术架构



架构说明：

1、高配置性：

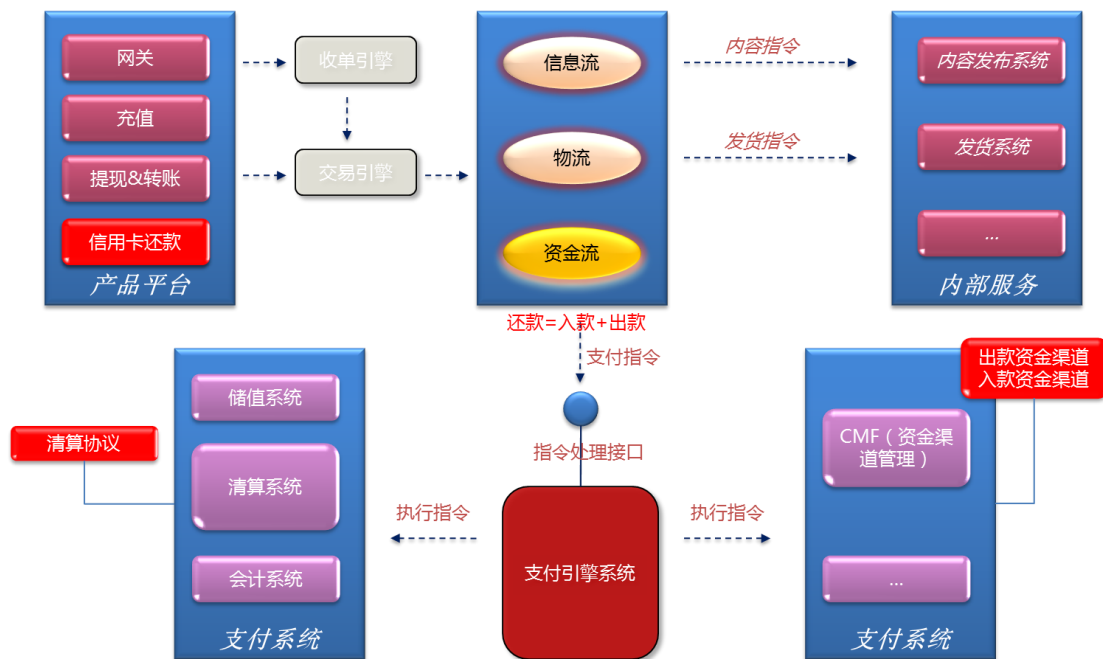
- ✓ 费率，结算周期等设置可以针对单个用户
- ✓ 费率支持多种模式，如：固定费率，单笔，阶梯等，可适应互联网证券的经纪业务和其它业务的灵活要求
- ✓ 收银台银行排列顺序可配置
- ✓ 对账任务，对账计划可配置
- ✓ 清结算协议可配置
- ✓ 支付服务可配置
- ✓ 银行往来文件解析可配置
- ✓ 系统通知信息可配置
- ✓ 资金渠道路由可配置
- ✓ 会计科目可配置

## 2. 灰度能力：

灰度能力是指能够测试、部署新系统时的控制性，并且能够有针对性地发布新产品，如针对特定人群的测试性发布或者按类型控制，如地域，年龄，或其他信息等。这样可以根据最真实的用户反馈决定下一步策略。

### 2.3.3 核心模块架构

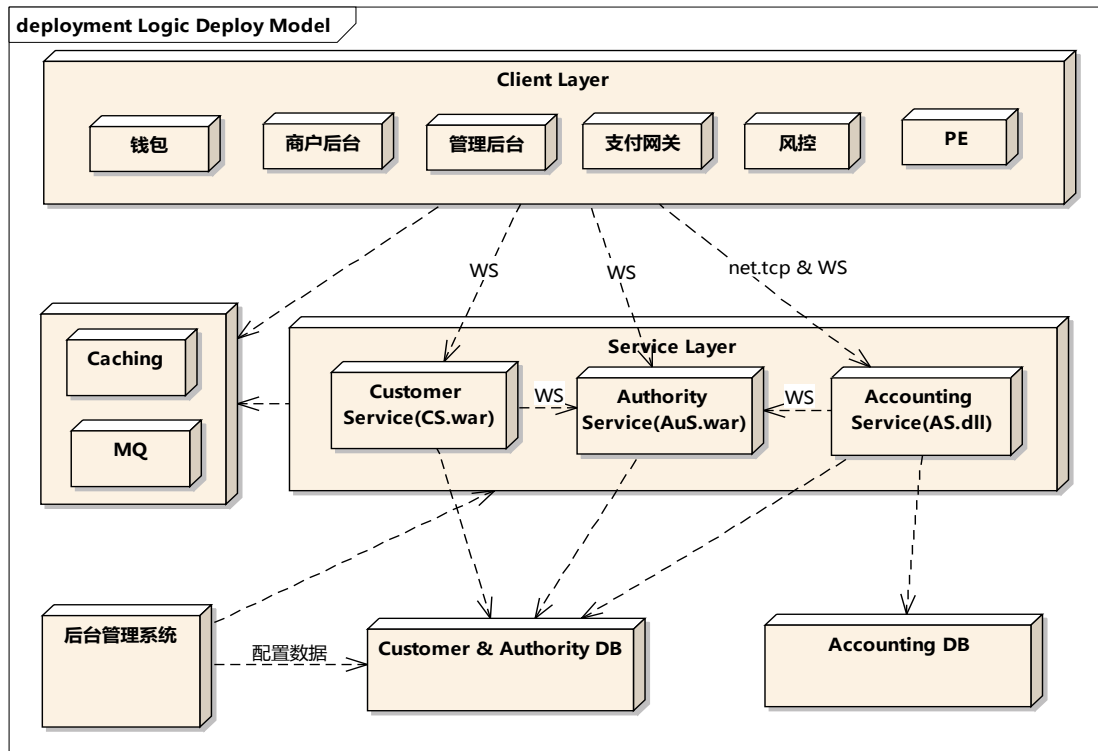
#### 1、支付引擎整体机构



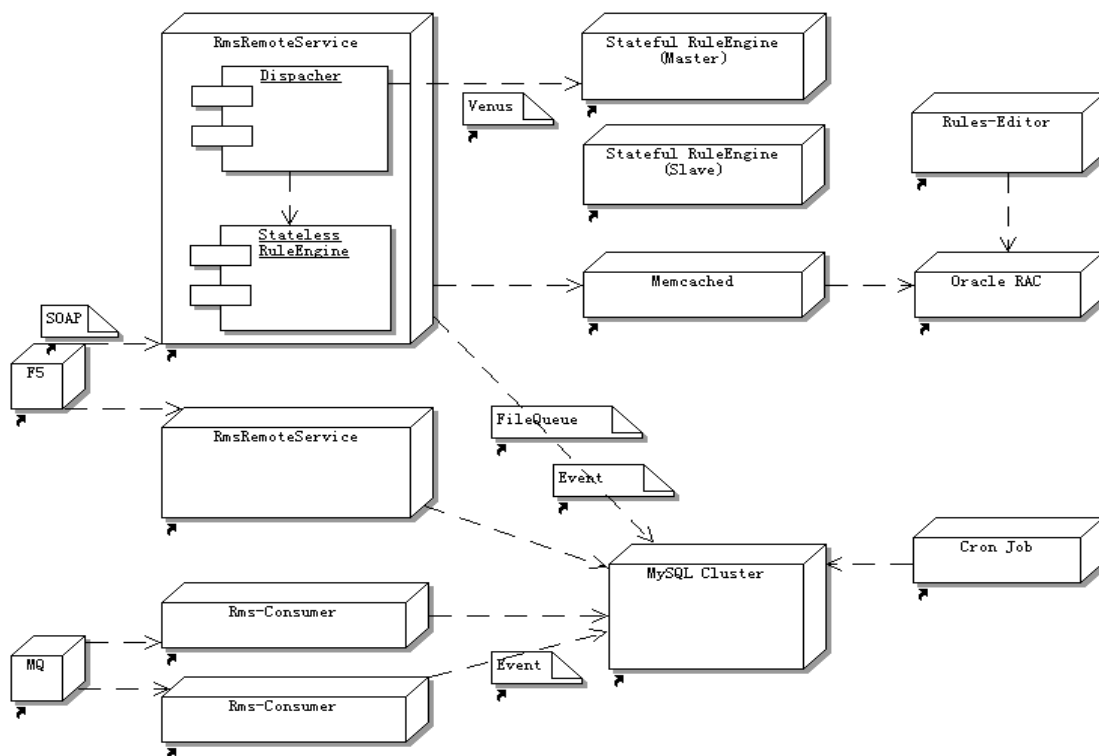
## 2、资金渠道路由整体架构



## 3、会员体系整体架构



#### 4、风控模型



## 2.4 与其它系统的接口

### 2.4.1 短信网关接口

#### 2.4.1.1 请求基本参数

请求基本参数是下面所有请求接口都要加上的。

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
version	接口版本	Number(5)	接口版本, 目前只有固定值 1.0	不可空	1.0
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	e8qdwI9caset5zugji2r7q0k8ikopxor
sign_type	签名方式	String(10)	签名方式只支持 DSA、RSA、MD5。	不可空	MD5
memo	备注	String(1000)	说明信息	可空	

#### 2.4.1.2 短信交易网关接口

支持多件商品提交, 支持选择多种支付方式。

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
业务参数					
request_id	请求编号	String(32)	钱包合作商户网站唯一请求号(确保在合作伙伴系统中唯一)。	不可空	请求编号: 20131105154925
external_pk	外部系统业务主键	String(32)	来自调用接口的外部短信接收系统中, 接收到用户短信回复记录的主键。	不可空	2013110500000123
dialing	主叫号码	String(32)	用户回复短信的主叫号码	不可空	1065822100021



biz_type	业务类型	String(16)	标识业务操作的类型	不可空	余额代扣: BALANCEWITH HOLD
sms_content	短信内容	String(512)	用户回复短信的内容	不可空	用户回复验证码: Xrj387
mobile_ticket	手机加密串	String(64)	使用 RSA 加密手机号后的加密串	与手机加密串 2 者不能都为空	123456788...
mobile	手机号原文	String(32)	用户回复短信的手机号	与手机加密串 2 者不能都为空	13923120345
extension	扩展信息	String(512)		可空	

### 2.4.1.3 同步返回基本参数

部分接口调用接口成功时，有会同步返回。注意：这里的成功只是调用接口成功，不代表业务的成功，业务是否成功，依赖异步通知消息。

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	e8qdwI9caset5zugii2r7q0k8ikopxor
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	

## 2.5 在线支付系统数据存储设计

在实际的数据存储设计中，我们把表分为三类：基本表、冗余表和关联表。

- 基本表：就是那些最普通的存储基本数据的表。
- 冗余表：冗余表的作用通常是缓存一些要经常使用的而且需要通过较长时间计算才能得到的数据。如某数据列的合计，最大值等数据。它的存在破坏了规范化的数据库设计，一般使得数据库的更新，删除，插入操作更为复杂，但大大提高了检索的速度，某些情况下可有效地提高程序性能。
- 关联表：通常用于存储两个数据列的二元多对多关系（关联表也可表示多元关系，但一般这种情况较少见）。一般就是两列数据：关联项一，关联项二，每行代表一条关系。

## 2.6 应用系统扩展功能

在应用系统扩展方面，主要考虑：

- 1) 支持资金渠道扩展，能够在平台方对渠道管理进行统一管理；通过配置的方式，支持各资金渠道的对账处理。
- 2) 支持对接外部服务，如公共事业（如对电煤缴费）缴费，手机充值接入

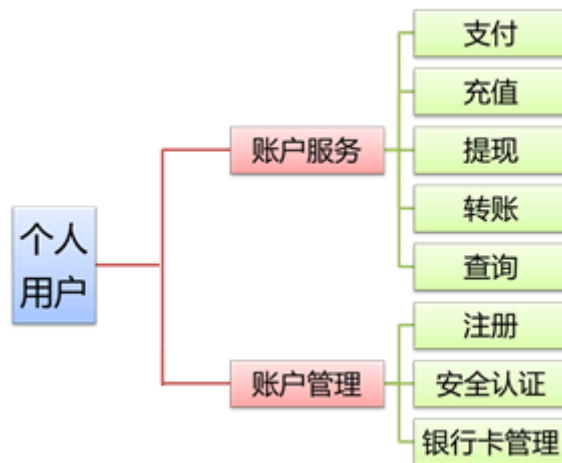
作为基础设施，本系统支持上层业务系统（包括但不限于信贷、保理、理财等）的业务实现，完成如放款、还款、收益

发放等场景中涉及的资金操作

### 3、系统功能说明


#### 3.1 在线支付子系统

个人用户支付



对于个人用户，主要用户场景有：

➤ 支付：支付宝、银联、快钱



您正在使用 钱包交易

类型	名称	交易号	对方	金额
担保交易	H-19	101140772728471808352	yangzi2012	2880.00 元

合计: **2880.00** 元


余额: 1.00 元, 可支付余额 **1.00** 元。


☒ 使用余额支付 **1.00** 元


储蓄卡


信用卡


支付 **2879** 元


 中国光大银行  
Citic Bank


 广东发展银行  
GUANGDONG DEVELOPMENT BANK


 浦发银行  
SPD BANK


 交通银行  
BANK OF COMMUNICATIONS


 招商银行  
CITIC BANK


 中国建设银行  
China Construction Bank


 中国银行  
BANK OF CHINA


 中国农业银行  
AGRICULTURAL BANK OF CHINA


 中国工商银行  
INDUSTRIAL BANK OF CHINA

 兴业银行  
XINGYE BANK CO., LTD.


 中国邮政储蓄银行  
POSTAL SAVINGS BANK OF CHINA


 上海银行  
Bank of Shanghai


 平安银行  
PINGAN BANK


 中信银行  
CITIC BANK

 华夏银行  
HUAXIA BANK

 北京银行  
BANK OF BEIJING

 上海农商银行  
SRCB

 北京农村商业银行  
BEIJING RURAL COOPERATIVE BANK

 民生银行  
MIN SHENG BANK

## ➤ 充值

充值账户:  账户余额: **1.00** 元

充值金额:  元

储蓄卡

\*根据中国人民银行相关规定, 禁止信用卡套现, 钱包禁止使用信用卡充值和提现, 否则引起的法律后果由用户自行承担

支付 **0** 元

 中国光大银行  
Citic Bank

 广东发展银行  
GUANGDONG DEVELOPMENT BANK

 浦发银行  
SPD BANK

 交通银行  
BANK OF COMMUNICATIONS

 招商银行  
CITIC BANK

 中国建设银行  
China Construction Bank

 中国银行  
BANK OF CHINA

 中国农业银行  
AGRICULTURAL BANK OF CHINA

 中国工商银行  
INDUSTRIAL BANK OF CHINA

 兴业银行  
XINGYE BANK CO., LTD.

 中国邮政储蓄银行  
POSTAL SAVINGS BANK OF CHINA

 上海银行  
Bank of Shanghai

 平安银行  
PINGAN BANK

 中信银行  
CITIC BANK

 华夏银行  
HUAXIA BANK

 北京银行  
BANK OF BEIJING

 上海农商银行  
SRCB

 北京农村商业银行  
BEIJING RURAL COOPERATIVE BANK

 民生银行  
MIN SHENG BANK

## ➤ 提现: 提现到用户在钱包绑定银行卡, 只能是储蓄卡

提现账户：██████ 账户可提现余额：18064.00 元 [查询提现记录](#)

选择银行卡： [+添加银行卡](#)

提现金额：

\*支付密码：  [忘记密码？](#)

[提交](#) [返回钱包首页](#)

## ➤ 转账到户：账户间转账

转账账户：██████ 账户可用余额：18064.00 元 [查询转账记录](#)

\*收款人手机/邮箱：

\*转账金额(元)：

转账说明：

☐ 免费给收款人发送短信通知

[去付款](#)

## ➤ 信息查询管理

综合信息显示：余额（包括冻结余额和可用余额）、收支总览

欢迎您，测试

手机号：15\*\*\*\*\*54 | 上次登录时间：2016-06-23 12:41:54 | 会员等级： [新增防伪信息](#)

**账户设置**

- ✉ 邮箱设置
- 📱 手机修改
- 👤 实名认证

**安全设置**

- 🔑 银行卡管理
- 🔒 修改登录密码
- 🔒 修改支付密码

**常见问题**

**账户余额**

0.00 元      0.00 元 (冻结余额)

[充值](#) [提现](#) [转账](#)

**账户资产**

📄 银行卡：0 张 [管理](#)

**交易记录**

[最近交易记录](#) | [充值记录](#) | [提现记录](#) | [转账到户记录](#) | [转账到银行卡记录](#) | [退款记录](#)

创建时间	名称/交易号	对方	金额	状态	操作
2016-06-23 16:33	东风雪铁龙 101146667080038031063	上海大众4S店	-0.20	交易结束	

[查看所有交易记录](#)

交易记录显示和查询（交易、充值、提现、退款）



我的钱包 **交易记录** 账户管理

创建日期

2016-05-18 到 2016-06-17

搜索

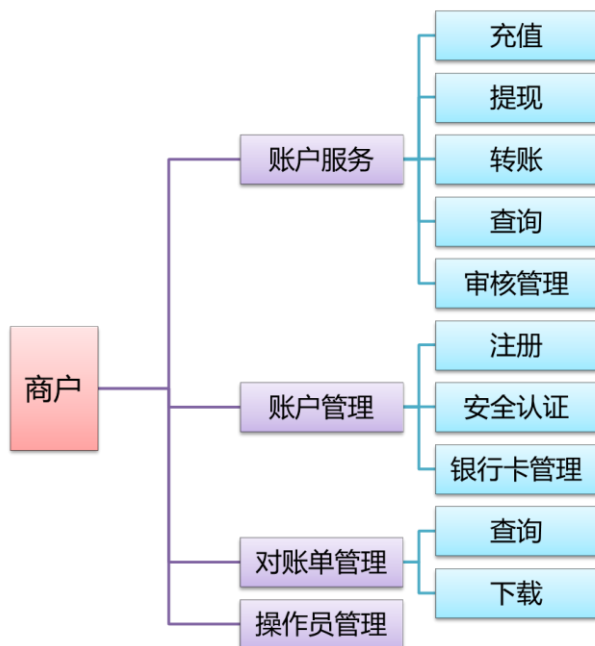
交易类型 **交易** 充值 提现 转账到户 转账到银行卡 退款

创建时间	名称 交易号	对方	金额	状态	操作
2016-06-17 14:50	测试 102146614622543322020	佳佳	-50.00	转账成功	

收支明细

➤ 账户管理

### 3.2 商户平台子系统



对于商户用户，主要用户场景有：

- ✓ 充值功能
- 银行卡充值
- ✓ 转账功能
- 账户间转账

转账用户：面包 可转账余额: 2000.00 元 [转账记录](#)

---

转账到户

转账到卡

收款人：

邮箱地址/手机号码

转账金额：

请输入转账金额

元

转账说明：

备注

发送短信：

☐ 免费给收款人发送短信通知

支付密码：

[忘记密码？](#)

确认

图- 1

- ✓ 提现功能
- 绑定账号的银行卡提现
- ✓ 信息显示查询
- 综合信息显示：账户余额、可结算余额、当期收支汇总
- 交易记录显示和查询：交易、充值、提现等（按时间段，资金流向、类型等查询，并可以导出。）

我的钱包

交易记录

对账单

账户管理

操作员管理

创建日期

2016-05-21 到 2016-06-21

搜索

交易类型

交易

充值

提现

转账到户

转账到卡

退款

审核

创建时间	名称   交易号	对方	金额	状态
2016-06-21 10:43	测试 102146647700953223541	测试	-20.00	转账成功

1

图- 2

- 收支明细（可以导出到 excel）

## ■ 对账单显示和下载



日期	摘要	收款	扣款	余额
	接上月余额	-	-	0.00
2016-06-20 18:27	入账结算 - 申请	2000.00	-	2000.00
2016-06-21 10:43	转账 - 申请	-	- 20.00	1980.00
	本月合计	2000.00	-20.00	1980.00

图- 3

- ✓ 账户管理
  - 用户注册
  - 用户登录
  - 登录退出
  - 找回密码
  - 实名认证
  - 账户激活
  - 基本信息管理
  - 账户安全设置
  - 操作员管理





图- 4

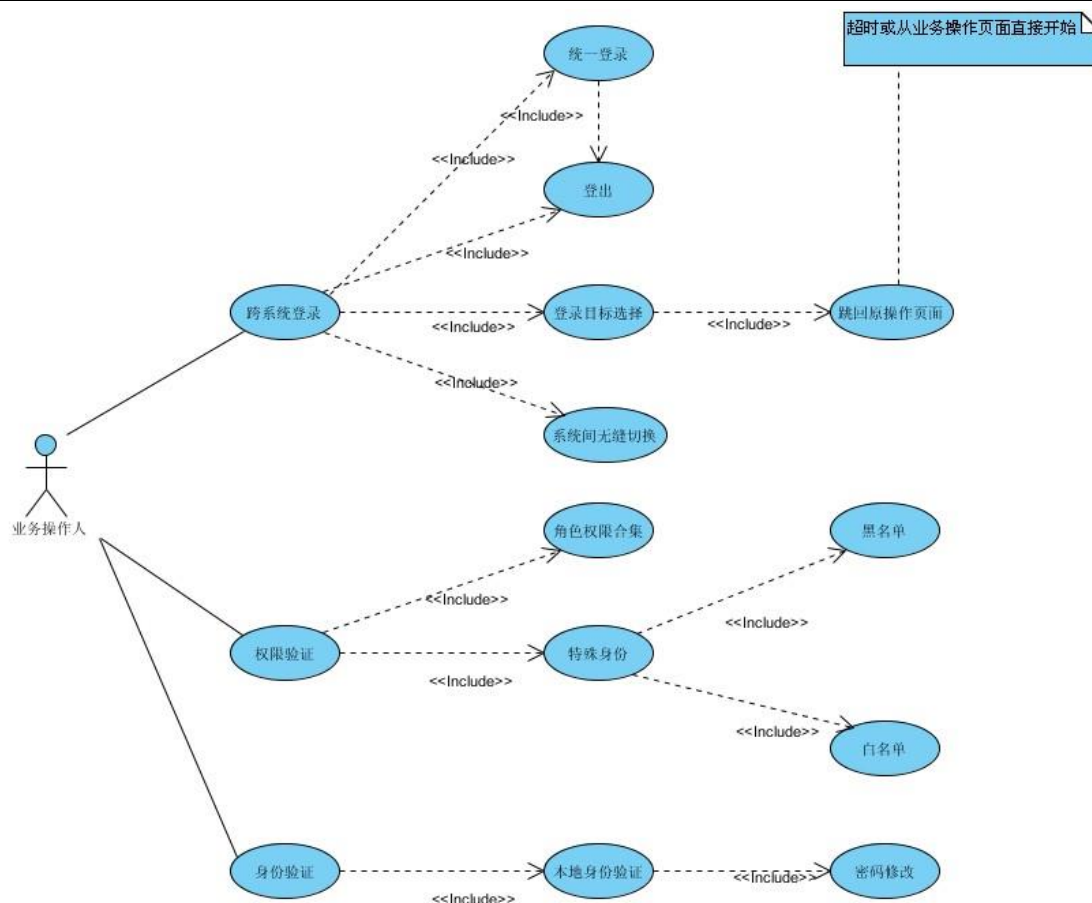
## ■ 复核员管理

### 3.3 系统管理子系统

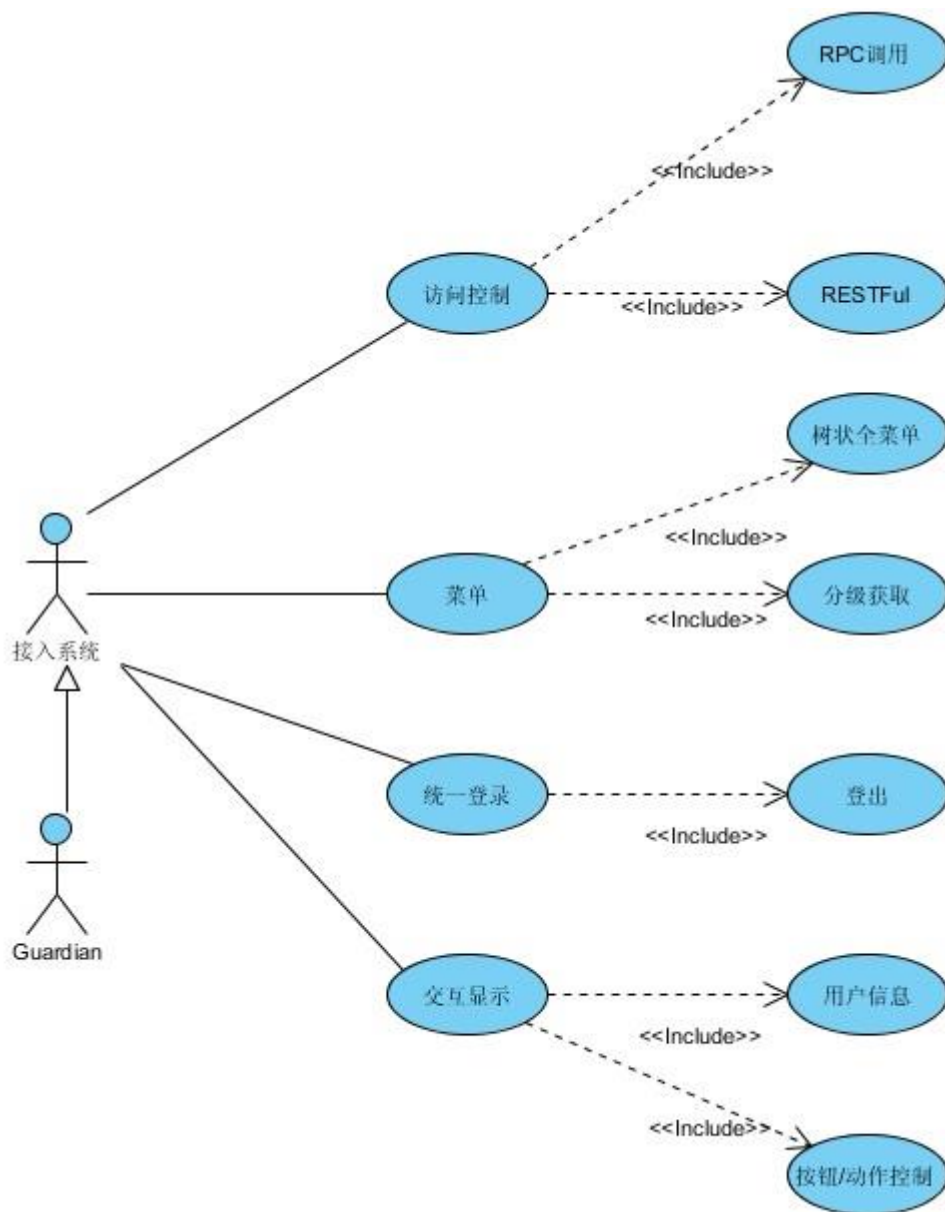
#### 3.3.1 系统管理

##### 3.3.1.1 用例图

#### ➤ 业务操作员



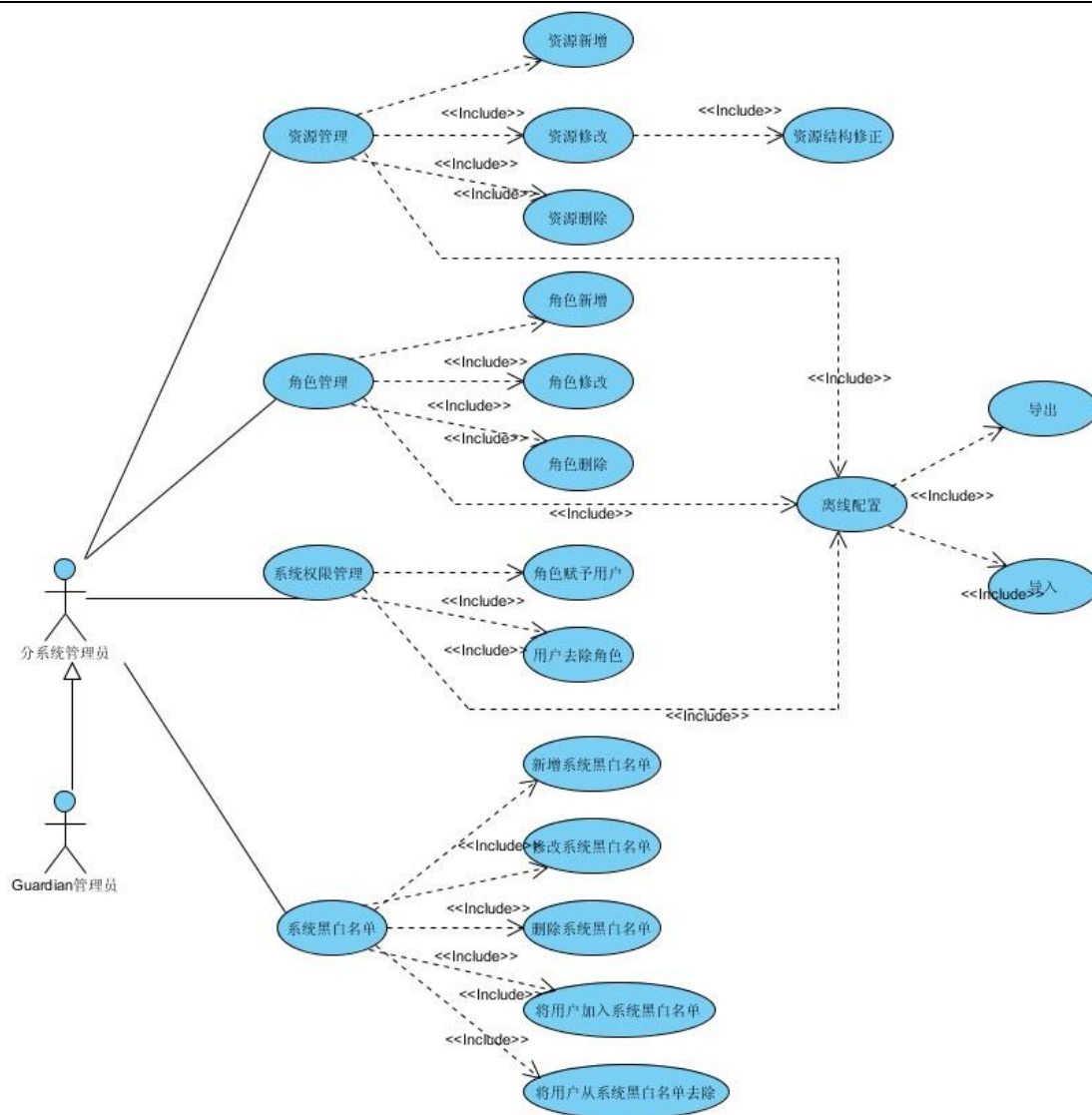
➤ 接入系统



➤ 接入系统管理员

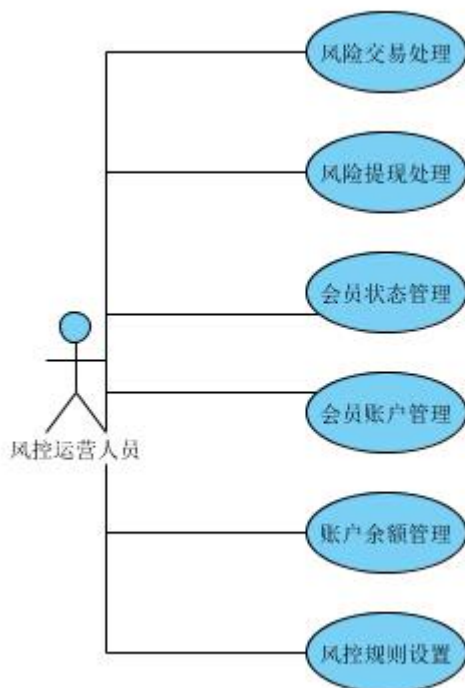


## ➤ 基础设置管理员



### 3.3.2 风控

#### 3.3.2.1 用例图



### 3.3.2.2 功能描述

#### ➤ 风险交易处理

对于判断为有风险（依规则而定）的充值，交易等，系统会进行拦截（资金进入入款中间账户），经风控人员审核后，继续或退回原交易

#### ➤ 风险提现处理

对于判定为有风险（依规则认定）的提现，系统会进行拦截，经过风控人员审核后，继续或终止提现

#### ➤ 会员状态管理

风控人员按需对会员进行锁定，锁定的会员无法再登录钱包

#### ➤ 会员账户管理

风控人员按需对会员账户进行止入止出，限制该会员的资金操作

➤ 账户余额管理

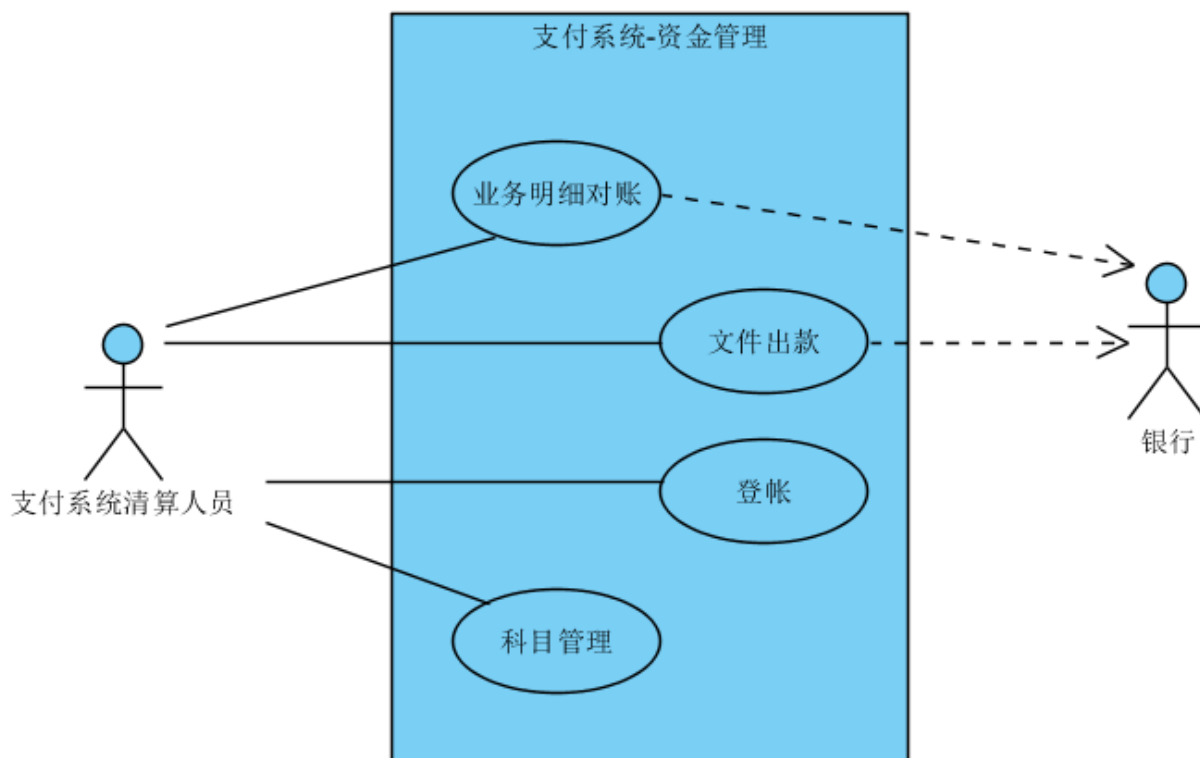
风控人员按需对会员账户中的部分余额进行冻结

➤ 风控规则设置

风控人员设置风控规则（一般需要研发人员配合），及相关规则参数（如规则中使用的黑白名单等）

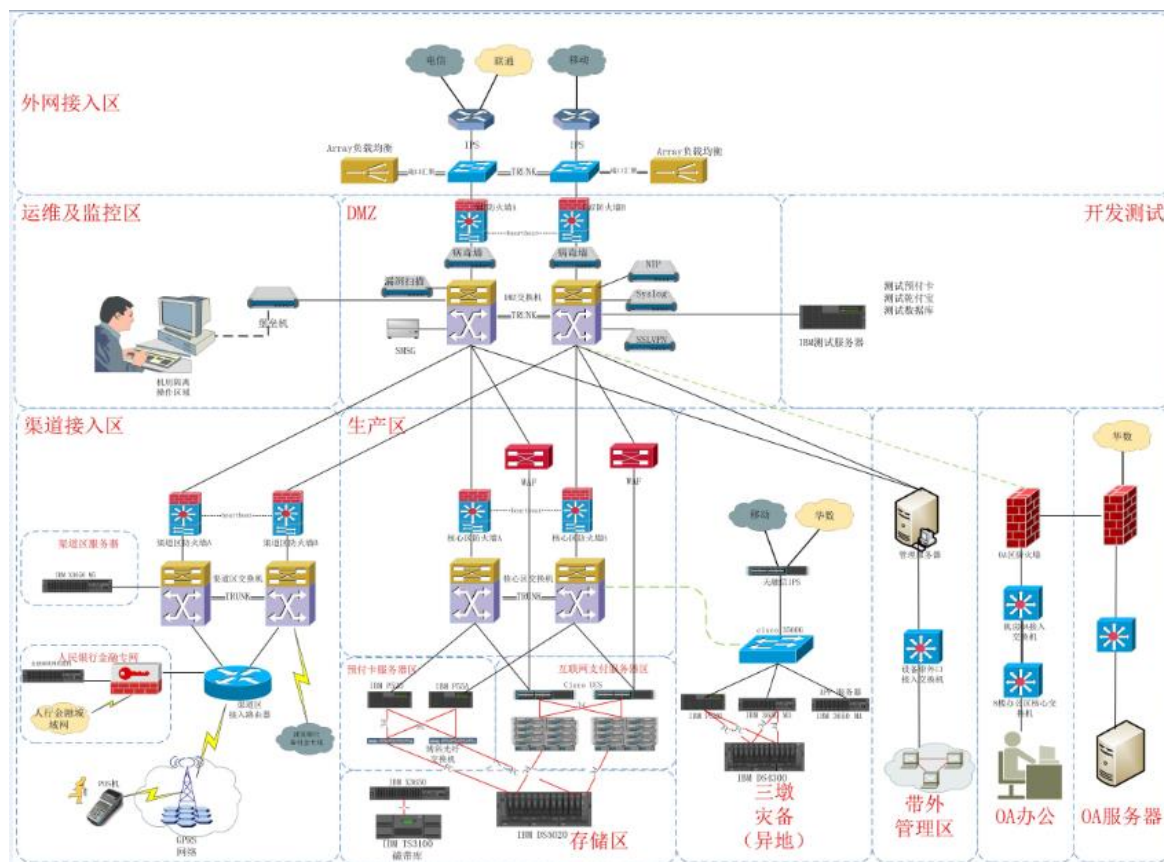
### 3.3.3 资金管理

#### 3.3.3.1 用例图



## 4、系统集成方案设计

### 4.1 网络拓扑图



## 4.2 主机平台方案

航天电子业务系统采用了思科 UCS 统一数据中心架构，将数据中心与智能云网络集成于一体。简化了 IT 操作、加强安全性、提高业务灵活性。统一数据中心提供了一个高效完整的数据中心架构。它将计算、网络、安全及管理集成到一个阵列架构中，一方面简化了 IT 操作，降低 IT 成本，一方面又实现了出色的业务性能和灵活性。

## 4.3 数据存储方案

航天电子采用了 IBM DS5020 用于数据存储，DS5020 提供了支持 8Gbps 的高性能光纤通道连接、可选的 1Gbps iSCSI 接口用于要求稍低的应用程序和较低成本的实施、高达



50. 40TB 的光纤通道物理存储容量、112TB 的 SATA 物理存储容量以及强大的系统管理、数据管理和数据保护功能。使用 EXP520 扩展单元后，DS5020 可连接多达 6 个光纤通道扩展单元，从而将容量扩展到企业级。高效的存储利用可降低原始容量要求，并且支持混用高性能和高容量驱动器以便实现基于机柜的分层存储。这些独特的功能可以减少满足性能和/或容量需求所需的驱动器数量，从而减少购置和运营费用支出。

#### 4.4 数据备份方案

##### 4.4.1 数据备份的目的

随着互联网技术的发展，数据的安全性日益引起每个 IT 行业部门的高度关注，一旦出现数据丢失或者数据损害，对企业的最终结果就是直接的经济损失。可见数据安全对一个企业来说是非常重要的。为此，本公司指定了以下备份制度，以保证数据的安全和业务的可靠和连续性。

##### 4.4.2 数据的备份对象及方式

备份对象为乐家易付所有数据库 schema，Mysql 数据库的备份方式主要为使用 mysqldump 工具实施数据文件转储。

命名：epay\_备份日志.sql.gz

##### 4.4.3 备份策略

为了保证数据备份的有效进行，本公司特此指定了以下备份策略：

Mysql 备份策略名	备份频度	备份保留时间	确认备份审查频度
Mysql 备份	每天 00: 30	30 天	90 天

##### 4.4.4 恢复策略

为了验证备份数据的有效性，确保在数据出现损坏时，保证数据能够正常和快速的恢复，提高业务的可用性和连续性。为此，本公司指定了以下恢复策略：

#### 4.4.4.1 主机系统的恢复：

恢复频度为每年一次

主机系统的恢复采用测试机器，通过恢复光盘的方式将系统恢复至测试机器上。

#### 4.4.4.2 Mysql 数据的恢复：

恢复频度为每年一次

主机系统恢复完成后，将 Mysql 的备份数据恢复到该测试主机上，然后测试数据的一致性和有效性。

#### 4.4.5 恢复方案

##### ➤ 部分数据库对象损坏

当数据库中特定的数据对象损坏时，可以通过 mysqldump 备份进行恢复，具体的命令模板如下：

```
mysql -u 用户名 -p 密码 --one-database 数据库名 < dbbackups.sql
```

#### 4.4.6 全部数据文件丢失

当出现全部数据文件丢失时，可以通过 mysqldump 的备份进行全库恢复，具体的命令模板如下：

```
mysql -u 用户名 -p 密码 < dbbackups.sql
```

#### 4.4.7 数据灾备

##### 4.4.7.1 灾备环境方案

当全库数据出现损坏，如出现水灾、火灾、爆炸等一些不可抗拒的因素，为了保证业务可以在最短的时间之内恢复正常。因此，本公司特此建立的 Mysql

数据库灾备，采用的是 Mysql Replication 机制，通过传输主库的二进制日志到从库上来实现主库与从库的数据同步。

#### 4.4.7.2 灾备数据库故障切换

从库：

停止 IO\_THREAD 线程

```
root@localhost:francs>stop slave IO_THREAD;
```

激活从库(从库上操作)

```
root@localhost:francs>stop slave;
```

```
root@localhost:francs>reset master;
```

```
root@localhost:francs>reset slave all;
```

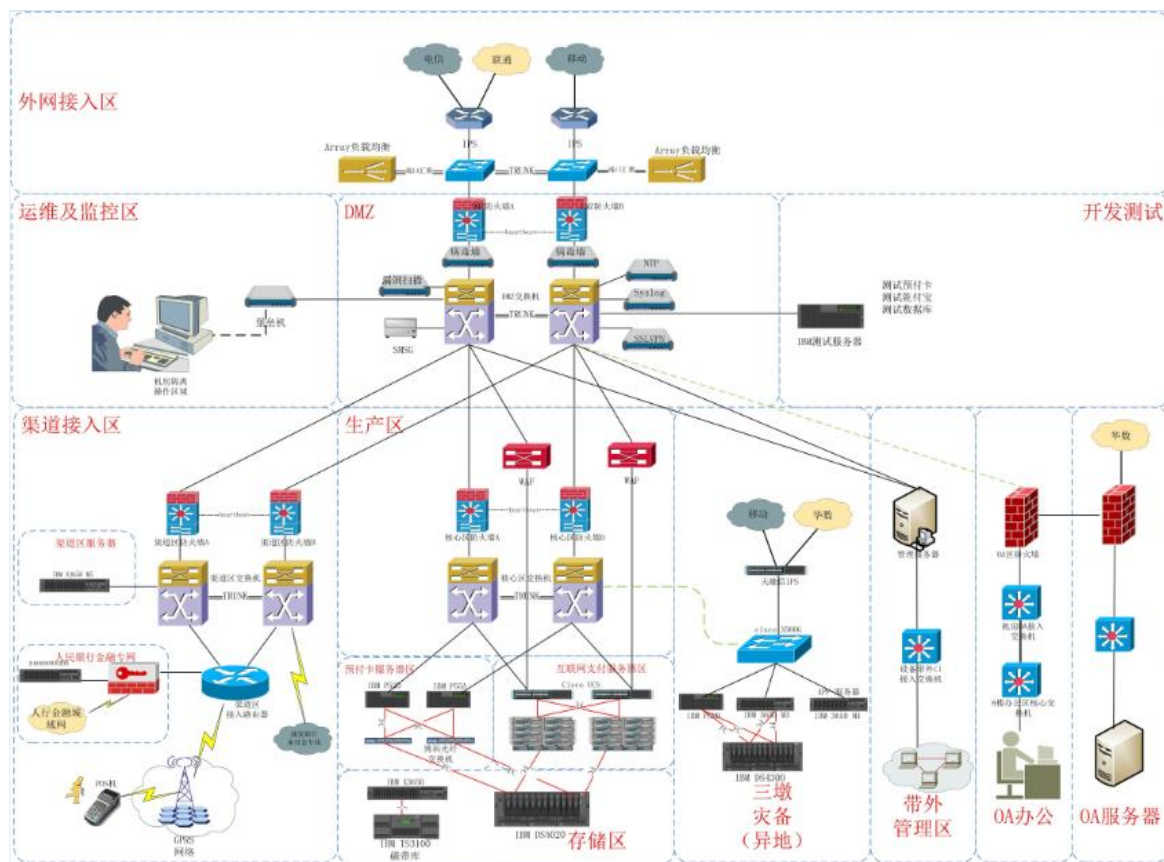
```
root@localhost:francs>show binary logs;
```

```
+-----+-----+
| Log_name          | File_size |
+-----+-----+
| bin-log.000001    | 120       |
+-----+-----+
```

```
1 row in set (0.00 sec)
```

### 4.5 网络设备方案

#### 4.5.1 网络拓扑



高可用性：航天电子互联网支付系统中所有的设备都是冗余部署的，即使设备出现故障，也能实现设备自动切换实现故障的恢复。

#### 4.5.2 多链路接入

航天电子网络支付系统网络接入了三大运营商的网络，将运营商故障对业务的影响降到最低。

安全性：航天电子支付系统网络建设支持就考虑到了网络安全性，根据功能的不同进行了区域划分分为外网接入区、DMZ区、生产区、互联网支付服务器区、存储区、渠道接入区、灾

备区、带外管理区、OA 办公区、OA 服务器区等。主要的区域与区域之间都部署了防火墙以提高安全性、DMZ 区域部署了病毒墙、漏洞扫描、WAF 等安全设备以防止通过互联网方向可能存在的木马病毒、漏洞扫描、网页篡改等安全攻击形式。

#### 4.5.3 高可扩展性

在设计园区网时，通过层次化的设计可保证网络的扩展性。层次化结构包括三个功能部分：即接入层、汇聚层和核心层，层次化的设计除了能带来便于扩展的优势以外，还可节约成本和加强故障隔离能力。

#### 4.6 系统安全方案

航天电子系统在建设之初从多个方面进行了安全建设的考虑与规划

- 1、 使用防火墙、病毒墙、WAF、漏洞扫描、IPS 等设备对内部与外部之间的流量进行隔离与管控
- 2、 外部互联网管理操作需要通过双因子认证拨通 VPN 才能够进行访问
- 3、 内部管理操作对于终端计算机的端口、MAC 进行了限定
- 4、 主机的访问均需要通过堡垒机进行访问、并对所有的操作进行记录

### 5、系统备份与恢复

备份的时间、性能应符合各系统服务级别的规定，各系统服务级别有系统所在部门和使用部门商议。

备份介质需包含操作人信息，备份时间，应用程序版本号信息。

要使用脚本来进行备份和恢复，避免手工操作，尽量安排在非工作时间进行备份。

所有的备份介质需贴上标签，标签内容包括介质编号、备份内容、备份日期时间、备份人员名字等内容；数据备份在制作、传递、转移过程中，必须填写<<数据备份登记表>>，详细记录备份数据制作、传递、转移过程与责任人；数据备份的存放处必须符合防火、防水、防磁的安全要求；保存期在一年以上的备份磁带应半年进行重写处理；长期保存的介质应记录使用次数，保证介质在规定内的次数内使用；归档数据备份介质应该实施异地档案室存放。

### **5.1 应用程序备份**

1、当系统配置数据发生变动时，应马上备份应用程序，备份介质保留至下一次应用程序全备份。

2、当生产环境中的应用程序变更时，应对变动前的应用程序版本进行全备份，备份后应用程序恢复后运行正常并可成功追溯到变更前版本。

3、文件全备份。将主机系统和其他服务器的数据作全备份。选择在周日自动进行。

4、文件增量备份。在周一到周四(或周五)之间备份文件的增量。

### **5.2 主机系统备份**

1、每月初的周日进行系统完全备份。

2、每周非工作时段进行系统增量备份。

3、主机系统(操作系统、工具软件、数据库系统软件、应



用等)变化的频率,全备份的频率应与业务系统变化频率成正比。

4、当主机系统发生重大变更时,应马上对主机系统进行一次全备份。

5、考虑全备份的容量,全备份的频率应与其备份容量成反比。

6、系统全备份方式使用于使用小型机设备的系统,使用 PC 服务器的系统采用克隆系统应急盘方式。

7、在备份和恢复操作流程发生变动时,对操作人员进行培训;进行恢复演练的频率与流程变化的频率成正比;进行实际恢复演练的频率与恢复失败的频率成反比。

### 5.3 恢复策略

所有生产系统和数据的恢复都要预先得到数据库管理员的批准;对存档备份介质的调阅需要登记,并且只能拷贝不能外借。为了防备数据丢失,公司定期进行灾难演练,以熟练灾难恢复的操作过程。检验所生成的灾难备份介质是否可靠。

公司灾难恢复操作通常分为三种情况。

#### 1、全盘恢复

在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等时系统管理员进行全盘恢复。

#### 2、个别文件恢复

利用网络备份系统的恢复功能。恢复受损的个别文件。浏览备份数据库或目录。找到该文件。触动恢复功能,软件将自动驱动存储设备。加载相应的存储媒体,然后恢复指定文件。

#### 3、重定向恢复

将备份的文件恢复到另一个不同的位置或系统上去，而不是进行备份操作时它们当时所在的位置。重定向恢复可以是整个系统恢复也可以是个别文件恢复。重定向恢复时需要慎重考虑。需确保系统或文件恢复后的可用性。