目錄

[一、 界面功能需求 2](#_Toc555)

[1. 核心功能是支付 下单 查单 回调 2](#_Toc4082)

[二、 对接sdk 2](#_Toc8843)

[三、 对接文档 openapi 3](#_Toc1639)

[四、 kms密钥管理 3](#_Toc22921)

[五、 会话管理 3](#_Toc12016)

[六、 IM模块 3](#_Toc8577)

[七、 审计日志 3](#_Toc5100)

[八、 WORM合规留存 4](#_Toc14081)

[九、 siem模块部分接入，安全信息事件管理 4](#_Toc5301)

[十、 预警模块 4](#_Toc17651)

[2. 自动化响应 封禁IP/冻结账号 等措施 4](#_Toc15768)

[十一、 数据一致性 4](#_Toc18234)

[十二、 安全需求 5](#_Toc24724)

[3. 权限rbac模式 5](#_Toc32499)

[4. Pam特权账号管理 动态授权，会话审计 5](#_Toc32004)

[5. Mfa多元素认证 5](#_Toc28149)

[6. 黑白名单 5](#_Toc13728)

[7. 强密码策略密码强度校验 5](#_Toc15193)

[8. 防泄露，需要尽可能加密存储aes rsa等 5](#_Toc20340)

[9. 分离存储 5](#_Toc12539)

[10. 防xss 强检测模式 6](#_Toc18891)

[11. 防数据遍历拖库 6](#_Toc16989)

[12. Crsf防护，使用jwt token等模式，不使用session cookie模式 6](#_Toc24085)

[13. 防注入使用安全参数化api 6](#_Toc20308)

[14. 防重放 6](#_Toc28751)

[15. 防爆破攻击 适当限流频控 6](#_Toc10597)

[16. 数据脱敏令牌环 6](#_Toc31619)

[17. Soar安全编排自动化响应 安全告警自动化处理 6](#_Toc22714)

[18. Ueba用户实体行为分析，，检测异常用户行为 6](#_Toc9037)

[十三、 防篡改 7](#_Toc17947)

[19. 权限细化 7](#_Toc6798)

[20. 三方篡改，使用签名模式 7](#_Toc22862)

[21. 运维等内部渗透存储篡改防止 7](#_Toc20660)

[22. 防止替换回滚攻击 7](#_Toc22467)

[十四、 其他金融合规需求 7](#_Toc8766)

[十五、 稳定性 性能 维护性需求 略 7](#_Toc28041)

# 界面功能需求

## 核心功能是支付 下单 查单 回调

，左侧菜单菜单项是用户管理，代理管理，管理员管理，资金账变，资金操作，订单管理，渠道管理，产品管理，上游管理。系统配置

列表字段是 支付渠道，拉单笔数，成功笔数，成功率，下单金额，成功金额，手续费。

商户管理的页面列表。字段是商户编号，用户名，通道名称及编号，总代收金额，总提现金额，总代付金额，总代收usdtt，总提取usdt，是否禁用，最后登录时间，历史登录IP，操作。

代收资金订单列表页面。字段是时间日期，系统订单号，商户订单号，商户编号，商户名称，收款类型，收款通道，金额，实际金额，手续费，订单状态，是否回调。操作

通道列表，页面字段是编号，类型，名称，接入编号，接入手续费率，是否开启，创建时间，更新时间，操作。

管理员管理列表，，字段是编号，用户名，职位，是否开启谷歌验证码，创建时间，更新时间，操作。

通道总表（列表页面），字段是编号，类型，通道名称，接入编号，总入金额，手续费，实际金额，总提款，我要提款，提款记录，通道余额，是否开启，创建时间。

# 对接sdk

|  |  |  |
| --- | --- | --- |
|  | java php c# go | 20 |

# 对接文档 openapi

# kms密钥管理

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| kms密钥管理 | 密钥生成，加密，解密等 |  |  |  |

# 会话管理

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 会话管理 + | token签发，拉黑，洗白，注销，强制登出 |  |  |  |
| 会话管理 + | 多因子认证 |  |  |  |
|  | 展示在线管理员，强制退出、限制多设备登录等功能 |  |  |  |

# IM模块

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| im模块 | mfa验证接收，安全通知等 |  |  |  |
|  | 收发消息 |  |  |  |

# 审计日志

|  |  |  |
| --- | --- | --- |
| 审计日志 | 安全日志与审计 |  |
|  | 操作日志 |  |
|  | api接口审计日志 |  |
|  | 登录日志 |  |
|  | 重要参数变更记录 |  |
|  | WORM防篡改日志 |  |
|  | 签名区块链日志 |  |

# WORM合规留存

# siem模块部分接入，安全信息事件管理

核心重要业务事件接入siem

# 预警模块

|  |  |  |
| --- | --- | --- |
| 预警机制 | 定义若干异常点，预警通知 |  |
|  | 预警机器人 |  |
|  | 监控埋点 |  |

## 自动化响应 封禁IP/冻结账号 等措施

# 数据一致性

|  |  |  |
| --- | --- | --- |
| 数据一致性 |  | 防止错乱 |
|  |  | 聚合统计 |
|  |  | 异步补偿 |
|  |  | 幂等处理 |
|  |  | 强一致机制锁 |
|  |  | 数据回写补偿 |
|  |  | 数据版本控制 |

# 安全需求

## 权限rbac模式

## Pam特权账号管理 动态授权，会话审计

## Mfa多元素认证

|  |  |
| --- | --- |
| 防刷库防止遍历 |  |
| 反爬 |  |
| 黑白名单 |  |
| 强密码策略密码强度校验 |  |
| 账号锁定机制 |  |
| 冻结期设计 |  |
| 设备指纹识别 |  |

## 防泄露，需要尽可能加密存储aes rsa等

## 分离存储

## 防xss 强检测模式

金融级别防护，遇到不合理输入检测不通过不入库。。从原头禁止存储不合理数据。。

不使用过滤机制，使用前置检测机制

## 防数据遍历拖库

数据id等不能以自动id模式，要是有uuid模式，防止遍历整个数据

## Crsf防护，使用jwt token等模式，不使用session cookie模式

## 防注入使用安全参数化api

Jpa mybatis参数化api等

## 防重放

## 防爆破攻击 适当限流频控

## 数据脱敏令牌环

## Soar安全编排自动化响应 安全告警自动化处理

## Ueba用户实体行为分析，，检测异常用户行为

# 防篡改

## 权限细化

## 三方篡改，使用签名模式

## 运维等内部渗透存储篡改防止

要使用不可篡改的日志记录

## 防止替换回滚攻击

# 其他金融合规需求

# 稳定性 性能 维护性需求 略