

理财平台银行通道接入

需求说明书

部门：产品部

日期：2014年07月20日

版本历史记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日 期 | 版本号 | 版本内容 | 作者 | 审核人 | 审核日期 |
| 20140720 |  | 理财平台银行通道使用需求 | 方爽 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 引言

## 背景

理财平台项目在开展业务基金支付业务中，因业务流程与支付产品的特殊性，需要用到专用的银行通道以满足用户在鉴权、绑卡、付款等业务流程。

## 编写目的

此需求说明书描述了本次需要接入的工行快捷支付接口提供的主要功能，后续的接口调试、编码、测试以此为基准进行。

本文档预期读者为业务需求人员、设计人员、编码人员、测试人员。

# 系统业务处理流程

无

# 系统功能需求

## 接口主要实现功能

本次工行快捷支付通道接入，需要包含以下功能：

* 身份认证（鉴权、绑卡）接口

用户通过输入姓名、身份证、银行卡、开户手机号等信息，由顺银发送至银行，并通过短信验证，确认用户身份；

* 扣款接口

用户通过输入姓名、身份证、银行卡、开户手机号等信息，或者由支付系统带入基金销售系统传过来的绑卡文件（含银行支付信息），完成付款确认；

* 撤销接口

在用户支付操作的T日，用户可使用此接口完成撤销，通过输入或由系统带入银行卡支付信息，确认完成撤销申请；

* 退款接口

在用户支付操作的T+1日之后，用户可使用此接口完成退款，通过输入或由系统带入银行卡支付信息，确认完成退款申请；

撤消和退款走的一样的通道？

* 结果查询接口

在理财平台没有正常收到通道处理结果返回时，理财平台可通过此接口实时查询请求订单的支付状态；

# 顺银需求影响全景图

|  |  |  |
| --- | --- | --- |
| 序号 | 项目 | 项目影响 |
| 1 | 需求编号 |  |
| 2 | 需求名称 | 理财平台银行通道接入需求说明书 |
| 3 | 收派员巴枪 | 无影响 |
| 4 | 顺银系统响应巴枪 | 无影响 |
| 5 | 分点部操作环节(收款员) | 无影响 |
| 6 | 速运财务流(区部，总部财务) | 无影响 |
| 7 | 速运营运(区部，总部) | 无影响 |
| 8 | 顺银运营处 | 无影响 |
| 9 | 结算环节(顺银结算处) | 无影响 |
| 10 | 运单对账清分 | 无影响 |
| 11 | 日切逻辑 | 无影响 |
| 12 | 顺银风控数据获取，规则变更 | 无影响 |
| 13 | 顺银客服，集团客服 | 无影响 |
| 14 | 持卡人门户 | 无影响 |
| 15 | 短信交互 | 无影响 |
| 16 | 动态培训 | 无影响 |
| 17 | 权限变更 | 无影响 |
| 18 | 上线验证 | 理财平台联调测试时才能验证 |
| 19 | 备注 | 无 |

# 系统非功能性需求

## 可靠性需求

|  |  |
| --- | --- |
| **主要质量属性** | **详细要求** |
| **正确性** | * 系统必须保证所有业务操作能够被正确处理 |
| **健壮性** | * 系统良好运行时间，满足7×24小时可用 |
| **可靠性** | * 应用系统应能够1小时内从停机中恢复 * 程序和数据可进行逻辑备份 |

## 安全性需求

|  |  |
| --- | --- |
| **3.1 需求级别：高** | |
| **分类** | **要求** |
| **密码保护** | 图形验证码：应满足， 1、由数字和字母组成(长度≥4位)； 2、随机产生； 3、包含足够的噪音干扰信息； 4、具有使用时间限制(≤10分钟)并仅能一次。 |
| 密码策略： 1.长度≥6位。 2.复杂度≥两种字符，支持字母、数字、特殊字符。 3.密码中不能包含有连续四位及以上顺序(或逆序)数字或字母；（如：1234、abcd等）。 4.密码中不能包含有连续四位及以上重复字符，字母不区分大小写；（如：8888、AAAA、$$$$等）。 5.不能将帐号名作为密码的一部分存在于密码，帐号密码也不能一样；（如：帐号为1355，密码不允许设置为\*\*\*1355\*\*\*\*）。 6.常用禁忌词不区分大小写不能作为密码的一部分存在于密码中；（如：admin, pass）。 |
| 产品必须提供密码修改功能，修改密码时须验证原密码。 |
| 登录密码和支付密码须分开设置且不能一样。 |
| 如有系统默认初始密码，首次登录时应强制用户修改初始密码。 |
| 密码需要使用安全的加密方法，不易破解（如：md5+salt)。 |
| **密码重置** | 须具备密码重置功能。 1.问题+短信重置：先回答问题，再发送短信。短信验证码要求：长度为≥6位，纯数字，有效性≤5分钟。 2.问题+邮箱重置：先回答问题，再发送邮件。邮箱要求：邮箱必须经过验证，重置密码链接有效性≤24小时，且只使用1次。禁止直接发送明文密码。 3.其他重置：必须经过身份认证，确定为授权人员，方可进行密码重置。（如：电话重置等） 参考问题如下，可在以下多项任选，但必须包含自定义问题： 1）你配偶的生日是；2）你母亲的生日是；3）你父亲的生日是；4）你的小学校名是；5）你的小学班主任的名字是；6）你的初中班主任的名字是；7）你的高中班主任的名字是；8）你的出生地是；9）你的配偶的姓名是；10）你的父亲的姓名是；11）你的母亲的姓名是；12）你的闺蜜的姓名是；13）你的学号是；14）你的工号是；15）你最喜欢的老师是；16）你最要好的室友是；17）自定义问题。 |
| **登录控制** | 终止会话要求：1.退出登录，立即终止会话；2.关闭客户端程序，立即终止会话；3.关闭浏览器页面，立即终止会话。 说明：保证无法通过后退、直接输入访问地址等方式重新进登录后的页面。 |
| 失败登录次数限制≤6次，应在剩余3次时给予提示，超过限制次数应在一定时间内锁定登录权限。 第一次锁定时限：≥20分钟； 第二次锁定时限：≥60分钟； 第三次锁定时限：≥24小时。 如重置密码成功应自动解锁。 说明：手动锁定与手动解锁请咨询风险管理部相关要求。 |
| **手机短信动态密码** | 短信动态密码长度为≥6位纯数，有效性≤5分钟。 |
| **邮箱识别** | 需要通过邮箱识别的须经过双向验证。 |
| **安全审计** | 须具备基本的用户登录、操作等日志功能，包括但不限于：用户登录日志、业务（支付交易等）日志、修改信息（包括密码）日志、用户授权日志、用户导出（下载）数据统计日志、用户业务数据查询日志（余额查询等）。 |
| **用户授权** | 内部和外部用户须按最小化原则合理授权。授予用户为完成各自承担业务所需的最小权限。如：按模块操作类授权、读写执行授权（增、删、改、查等）、用户分类授权、功能详细授权等等。 |
| **安全认证** | 空闲会话要求：空闲时间≤30分钟，自动关闭当前会话，用户再次操作时必须重新登录。 |
| **通讯协议** | 应使用强壮的加密算法和安全协议保护客户端与服务器之间所有连接，例如：使用SSL/TLS和IPSEC协议。 |
| 如果使用SSL协议，应使用3.0及以上相对高版本的协议，取消对低版本协议的支持。 |