**银企直联操作手册**

[**上线流程**](http://wiki.paas.sogou-op.org/pages/viewpage.action?pageId=114591612)

一配置前置机

1招行技术人员配置前置机环境，插上ukey

二配置业务机

    1配置mysql环境

    2依次执行remit工程Sql文件夹下的建表语句

    3执行data.sql，初始化数据

    4发布remit

    5测试通信

6将业务机ip加入短信发送ip白名单（联系姚峥，需志勇确认）

7去除ssh登录功能（

#vi /etc/ssh/sshd\_config

PermitRootLogin yes->no

#service sshd restart

）

8iptables（

# cp /etc/sysconfig/iptables /var/tmp #备份

vi /etc/sysconfig/iptables

-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT（允许80端口通过防火墙）

/etc/init.d/iptables restart

#systemctl restart iptables.service

）

9将console登录密码交付给财务

三业务机与前置机

1测试通信

2去除前置机的远程登录功能（右击计算机->属性->远程设置）

4前置机访问ip设为只有业务机能够访问（网络设置联系张硕，防火墙设置:控制面板->防火墙->高级->入站规则）

5锁机

# [审核流程](http://wiki.paas.sogou-op.org/pages/viewpage.action?pageId=114591614)

一配置审核员

    1系统发布时sql脚本初始化一个管理员

    2用该管理员账号登录，加入各级审批员

二各级审批员审批

    1各级审批员登录系统（oa账号密码和短信验证码确认登录）

2各级审批（初级30w，中级50w）

# [数据报表](http://wiki.paas.sogou-op.org/pages/viewpage.action?pageId=114591616)

每天会发邮件到制定邮件组，内容为昨日付款单明细

聚合内容为总金额，总笔数，成功金额，成功笔数

# [风险控制](http://wiki.paas.sogou-op.org/pages/viewpage.action?pageId=114591618)

风险点

如欲盗取公司资产，有两种方式

    方法一需要同时满足以下两点

        1能够获取pandora系统与银企直联通信证书和秘钥，熟悉pandora系统与银企直联通信规则

           此时可以发送伪造付款信息

        2能够掌握财务审核人员的oa密码和手机

           此时可以审核通过伪造付款单

    分析:同时满足两点的成本极高，可以认为安全

    方法二：直接进入机房打开保险柜，登录业务机，发送伪造报文

    分析:该人员需要有自由进出机房的权限，同时了解通信报文规则，成本极高，可以认为安全