盛世通宝内部通讯文档

（内部机密，严禁非授权传播）

定义

A方：交易系统

B方：商城系统

## 钱包转账协议

由B方请求A方将指定钱数从一个钱包转入另一个钱包

访问地址:

http://www.shengshitongbao.com/money/ts.json

访问方式：POST

参数：

|  |  |  |
| --- | --- | --- |
| 参数名 | 示例 | 说明 |
| pid | 1000 | B方在A方的合作伙伴ID |
| fromWallet | aa@aa.com | 转出钱包地址 |
| toWallet | bb@bb.com | 转入钱包地址 |
| money | 0.05 | 钱数，精确到小数2位 |
| timestamp | 1492995929 | 10位UNIX时间戳 |
| sign | auwiiaiidfiaidfiadf | 将returnUrl、pid、timestamp以字母顺序排序并以键值对形式排列后+key进行MD5校验 |

签名方法：

1、  把pid、fromWallet、toWallet、money、timestamp按照A-Z排序

2、  使用排序后的key=value&key=value做签名源，如：

fromWallet=aa@aa.com&money=100&toWallet=bb@bb.com&pid=1000&timestamp=11111111111111

3、  上述签名源+&key=md5Key

4、  进行md5，并放入sign参数

## 用户同步协议

### 2.1 请求用户信息

当B方未检测到用户信息时，将把用户重定向到A方登录地址，并指定返回地址returnUrl。

A方提供登录和注册界面给用户。

当用户在A成功登录后，A方将把用户名加密后传递给B方指定地址returnUrl。

B方将以A方提供的用户名作为用户登录凭证，忽略B系统的密码。

#### B方将未登录用户重定向到A方

访问地址:

http://www.shengshitongbao.com/user/login.shtml?returnUrl=http://www.shengshitongbao.cn/xxxxxx.shtml

访问方式：GET

参数：

|  |  |  |
| --- | --- | --- |
| 参数名 | 示例 | 说明 |
| returnUrl | http://xxxx.com | 登陆成功后的跳转地址 |
| pid | 1000 | B方在A方的合作伙伴ID |
| timestamp | 1492995929 | 10位UNIX时间戳 |
| sign | auwiiaiidfiaidfiadf | MD5签名，参考签名方法 |

#### A方将成功登录的用户重定向到B方

访问地址:

由B方提供

访问方式：GET

参数：

|  |  |  |
| --- | --- | --- |
| 参数名 | 示例 | 说明 |
| tbt |  | 加密后的参数 |

token包含如下参数

|  |  |  |
| --- | --- | --- |
| 参数名 | 示例 | 说明 |
| username | zhangsan | 甲方登录成功的用户名 |
| timestamp | 10位UNIX时间戳， | 1492995929 |
| sign | auwiiaiidfiaidfiadf | MD5签名，参考签名方法 |
| 以下为不参与签名的参数 | | |
| nickName |  | 用户昵称 |

将上述数据以URL请求方式排序后，使用AES密钥进行加密后作为token参数传递，即：

sign = md5(timestamp=1111111111&username=zhangsan&key=md5Key)

tbt=aes(timestamp=1111111111&username=zhangsan&sign=xxxxxxxxxxx)

或

tbt=aes(nickName=张三&timestamp=1111111111&username=zhangsan&sign=xxxxxxxxxxx)

请求URL为：

http://B方地址?tbt=token

注意：双方应以时间戳检验请求发起时间，超过1分钟则认为请求已失效。