
支付宝会员信息展示规范

文档修订历史

版本号	作者	备注	修订日期
0.1	徐庶		2012 年 4 月 27 日
0.2	徐庶		2012 年 8 月 20 号
0.3	徐庶	增加淘宝昵称的隐藏展示规则	2012 年 9 月 13 日
0.4	徐庶	增加缺省隐藏规则, 军官证, 护照等证件的隐藏展示规则, 提供隐藏使用 JAR 包	2012 年 11 月 16 日

目 录

1	目标.....	3
2	适用范围.....	3
3	会员信息分级	3
3.1	会员信息分类.....	3
3.2	会员信息分级.....	4
4	会员信息保护策略	5
4.1	信息共享方式.....	5
4.2	信息共享策略.....	5
4.3	站内展示	6
4.3.1	前台业务系统.....	6
4.3.2	后台管理系统.....	7
5	信息展示实例	7
附录 1	：隐藏展示规则.....	11

1 目标

制定本规范为在支付宝各业务进行过程中,保护支付宝会员信息以及满足相关法律法规要求。

2 适用范围

所有涉及用户信息展示的支付宝系统,展示内容包含页面可见部分以及 html 源码中的注释和隐藏域。

3 会员信息分级

3.1 会员信息分类

根据支付宝会员信息的产生过程以及针对一些特殊信息,将会员信息分成以下 5 大类

信息分类		主要涵盖信息
专属安全信息		登录/支付密码 安保问题及答案 手机校验码 宝令动态密码 授权 token
会员属性信息	金融附加信息	借记卡号 信用卡号、有效期, CVV2/CVC2
	高敏感信息	手机号码 证件类型

		证件号码
	基本信息	姓名 地址（包括缴费户号等） 账号 IM（QQ,MSN,旺旺） 关联账号（淘宝）
支付活动信息		余额 交易明细 收支明细
站内附加信息		账户类型 是否认证 是否金账户
业务状态信息		业务处理结果（成功，失败） 时间戳

3.2 会员信息分级

根据上述的信息分类，将信息分成 4 级，具体如下表：

级别	概述
机密	专属安全信息。直接影响账户安全以及资金安全，设计密码

	以及用户身份验证类
敏感	金融附加信息。银行卡（包括信用卡）相关信息
	高敏感信息。手机号码、证件类型以及号码
隐私	其他个人信息
	支付活动信息，由用户在支付宝付款活动产生的信息，包括转账，交易涉及的信息
公开	站内附加信息，支付宝对于用户在支付宝的一些标注信息
	业务状态信息，交易，转账过程中的辅助信息

4 会员信息保护策略

4.1 信息共享方式

根据支付宝自身的业务以及系统架构，会员信息的共享主要可以分成两种

1. 站内展示：会员在支付宝网站上看到的与会员相关的信息；
2. 接口共享：与外部商户合作，通过接口调用和商户共享的信息；

4.2 信息共享策略

根据信息共享的方式以及信息的级别，制定支付宝会员信息的共享策略：

级别	共享方式	
	站内展示	接口共享
机密	否	否
敏感	隐藏展示（规则见附录 1）	否

隐私	其中会员的基本信息需要用户授权后共享 对于支付活动信息则是参与方可以直接获得 ,非参与方在用户授权后共享	
公开	是	是

具体的场景中处理如下

4.3 站内展示

4.3.1 前台业务系统

4.3.1.1 未登录

不应展示与具体用户相关的任何信息。展示业务活动时如果存在需要，则对信息进行部分隐藏后展示，确保无法直接或者间接的通过所展示信息和用户取得联系。例如：

特定产品，经用户授权后，可展示部分用户信息，例如：收款主页中，用户授权以后直接显示其完整姓名。

4.3.1.2 已登录

信息范围	展示规则
自己信息	查看所有自己的信息 <i>为防止用户被盗号以后危害的扩大化,对于身份证号,银行卡号等可利用来对用户进一步造成损失的信息进行隐藏展示</i>
他人信息	查看自己所参与的支付宝活动（交易、转账、抽奖活动）相关的信息。主要是防止单向的不需要对方确认的方式去获取对方信息,例如输入对方账号直接

	<p>回显对方姓名。</p> <p>涉及对方信息时，需要进行隐藏展示，当有以下情形时可不隐藏</p> <ol style="list-style-type: none">1. 信息为用户自己输入2. 对方主动发起的活动包含的信息，例如：对方发起交易、收付款3. 与对方通过某种途径建立了信任关系（潜在的授权），例如：比如向对方收款，对方已付款；向对方申请代付，对方同意付款；或者对方在自己的联系人中
--	---

4.3.2 后台管理系统

后台系统由于业务管理的需要，特别是客服查询为用户解决问题，交易相关信息不再隐藏，只根据相关法律法规以及认证要求，对部分特殊信息进行隐藏。例如：身份证号、银行卡号（包括信用卡），对于风控等特殊需求需要查看则可不隐藏。

5 信息展示实例

目前站内展示常见情况的说明：

1. 用户信息展示

未登录时能看到的所有用户信息必须是隐藏的，用户建议或者中奖名单，需要进行部分隐藏，如下图：

我有话说

VIP特权，希望有免邮的特权
hl06****@***.com 2011-11-02

我也要提意见

特殊产品用户授权后可进行展示部分用户信息，下图是收款主页用户同意后可展示其姓名



2. 账号与姓名对应关系

原则是：不让恶意攻击者无成本的通过遍历账号从而获取姓名


输入账号回显名字，或者在业务流程中，包括收银台以及最后的交易记录。名字需要进行首字隐藏，账号（邮箱或者手机号）为用户自行输入，因此不用隐藏，流程中涉及己方的信息也不用隐藏，如果对方是自己的联系人，则名字也可不用隐藏。

转账付款

原“我要付款”

[功能介绍](#)

 **转账到支付宝账户**

 **转账到银行卡**

收款人：

*静 (scuallan@163.com)



+向多人付款

付款金额：

| 元

 您是金账户用户，本月还可免费向支付宝账户转账19744.00元。查看收费标准

付款说明：

转账

添加备注

☐ 免费短信通知收款人

金额大于等于1元时可以使用该服务。

确认您的转账信息


收款人：



*静 (scuallan@163.com)

付款金额： 1.00元

付款说明： 转账

 转账后，资金将直接进入对方账户，无法退款，支付宝不介入双方纠纷处理。如果您在购物，推荐使用担保付款



确认信息并付款

[返回修改](#) | [找人代付](#)

 | 收银台

您好， 赵勇 (支付宝账户： zytiti@gmail.com)

[己方信息直接展示](#)

 您正在使用即时到账交易：付款后资金直接进入对方账户 

转账 [详单](#)

收款方： *静

[对方姓名隐藏展示](#)

您的支付宝账户： zytiti@gmail.com [己方信息直接展示](#)

可支付余额： 533.89 元

使用支付宝账户余额支付 1.00元。

支付宝支付密码： *****

[忘记密码？](#)

确认付款



3. 支付宝账号与淘宝账号对应关系

原则：禁止此类关系直接或者间接的获取

之前主要是发生在代付业务点，输入淘宝账号后后续业务流程中会显示自支付宝账号，可被利用来对淘宝交易进行欺诈。

4. 重要信息必须隐藏展示

身份证号、银行卡号必须进行隐藏展示



 招商银行 ***** 2174 信用卡 快捷	银行卡 快捷支付 已开通 关闭 申请时间 2011.12.07
 招商银行 ***** 0709 储蓄卡 快捷（含卡通）	付款 限额 付款限额
	安全 管理 手机：130****5358 修改

附录 1：隐藏展示规则

缺省信息隐藏规则：

显示前 1/3 和后 1/3，其他用*号代替（短信使用一个*）。内容长度不能被 3 整除时，

显示前 $\text{ceil}[\text{length}/3.0]$ 和后 $\text{floor}[\text{length}/3.0]$ 。

以下是针对特定类型的信息隐藏规则，如在下表中不存在，则使用缺省的信息隐藏规则：

敏感信息类型	信息范围	展示规范
密码/口令及相关	1) 登录密码、 2) 支付密码、 3) 手机校验码、 4) 密码保护问题答案、 5) 支付盾 PIN 码、 6) 宝令动态密码、 7) 汇票密码、 8) 3D 密码、 9) 银行卡 PIN、 10) sessionId 等	禁止展示
密钥	1) 数据加密密钥、 2) 签名私钥、 3) Md5/HMAC 消息认证密钥等	禁止展示
信用卡信息	1) 信用卡卡号	前 6 和后 4 位

	2) 信用卡 CVV2/CVC2 3) 信用卡有效期	禁止展示
借记卡信息	借记卡卡号	快捷：短信和收银台选择页面 显示后 4 位。如：“尾号 7750” 其他 显示前 6 位 + * (实际位数) + 后 4 位。如：622575*****1496, 交易完成后可全显
个人信息	1) 身份证号、军官证号、护照号	身份证号： 推荐 显示前 1 位 + * (实际位数) + 后 1 位，如：5*****9 最低要求 前 5 和后 2 位 军官证号，护照号： 使用缺省信息隐藏规则
	2) 姓名	如果要隐藏，隐藏第一个字
	3) 手机号	如需要部分隐藏，区号不算，隐藏中间四位 网站和手机客户端 大陆：显示前 3 位 + **** + 后 4 位。 如：137****9050 香港、澳门：显示前 2 位 + **** + 后 2 位。如：90****85 台湾：显示前 2 位 + **** + 后 3 位。如：90****856 其他海外地区：使用缺省隐藏规则 短信 大陆：显示前 3 位 + * + 后 4 位。 如：137*9050 香港、澳门：显示前 2 位 + * + 后 2 位。 如：90*85 台湾：显示前 2 位 + * + 后 3 位。如：90*856 其他海外地区：使用缺省隐藏规则
	4) 固定电话号码	如需要部分隐藏，推荐的规范：显示区号和后 4 位

	5) 邮箱	<p>如需要部分隐藏， 网站、手机客户端 @前面的字符显示 3 位，3 位后显示 3 个 *，@后面完整显示如： con***@163.com 如果少于三位，则全部显示，@前加***， 例如 tt@163.com 则显示为 tt***@163.com</p> <p>短信 短信必须控制在 60 字内，所以，需要隐藏更多字</p> <p>1) @前面的字符显示规则： 如果@前面的字符数小于等于 3 位，则全部显示字符，然后再加上* 如果@前面的字符数多于 3 位，则显示前三位字符，然后再加上*</p> <p>2) @后面的字符显示规则： 如果@后面第 1 个字符到第 1 个"."之前的字符数小于等于 7 位，则全部显示，并以.*结尾 如果@后面第 1 个字符到第 1 个"."之前的字符数大于 7 位，则显示前 7 位字符，并以.*结尾</p> <p>3) 示例： 如果账户为 tjyihui@126.com 则显示：tjy*.*@126.* 如果账户为 mm@hotmail.com 则显示：mm*.*@hotmail.* 如果账户为 iceziling@netvigator.com 则显示：ice*.*@netviga*.</p>
	6) 地址信息	暂无要求
	7) 企业工商注册号	显示后三位
	8) 淘宝昵称	显示首/尾各 1 位，中间加**

		例如：风**扬，m**d
--	--	--------------

附录 2：技术开发使用安全 JAR 包

POM 中引用最新版本的安全 JAR 包

```
<dependency>
```

```
    <groupId>com.alipay.service</groupId>
```

```
    <artifactId>alipay-service-security</artifactId>
```

```
    <version>查询使用最新版本号</version>
```

```
    <type>pom</type>
```

```
</dependency>
```

使用

com.alipay.service.security.utils. SensitiveDataUtil 类进行信息隐藏