接入与使用规则

快捷登录接口(alipay.auth.authorize)

附录文档

版本号：1.0

目录

1 文档说明

1.1 文档说明

本文档是《快捷登录接口(alipay.auth.authorize)》附录文档，它详细解释了在技术接入与使用过程中需要注意的地方，以帮助商户避免风险产生。

阅读后如有疑问，请联系支付宝相关技术支持。

1.2 业务术语

表1-1 业务术语

术语	解释
返回	支付宝根据得到的数据处理完成后，支付宝将处理完成的结果信息反馈给商户网站。
防钓鱼	“网络钓鱼”攻击利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、口令和社保编号等内容，造成损失。防钓鱼用来防止以上情况的发生。
敏感词	带有敏感政治倾向、暴力倾向、不健康色彩或不文明的词。
请求	通过 HTTP 协议把需要传输的数据发送给接收方的过程。
授权令牌	经过用户授权，支付宝提供给商户在一定时间内对支付宝某些服务的访问权限，此权限通过授权令牌标记。
通知	服务器异步通知。支付宝根据得到的数据处理完成后，支付宝的服务器主动发起通知给商户的网站，同时携带处理完成的结果信息反馈给商户网站。

2 责任归属

文档中所涉及到的规则都是根据在接入与使用支付宝接口的过程中出现的一些主要风险而做的防范措施，请商户予以关注。请在接入及使用支付宝接口的过程中，严格依照支付宝提供的接口技术文档（快捷登录接口(alipay.auth.authorize).docx）、代码示例、本文档（快捷登录接口(alipay.auth.authorize)接入与使用规则）等接口资料，否则由此导致的风险以及资金损失或者扩大情形需商户自行承担。

3 技术接入规则

表3-1 技术接入规则

类型	细则	原因
账号	配置的合作者身份 ID 与安全校验码 key 必须保证与签约信息匹配	防止接口无法正常使用或出现资金损失
	必须保护合作者身份 ID 与安全校验码 key 的隐私性	防止签约的账号信息被盗用，导致资金受损、被他人恶意利用等。
	测试完毕后，要把测试账号立刻更换成签约账号。	避免出现返回的用户信息不是签约时的用户信息。
安全	支付宝的通知 IP 是 121.0.26.1 与 121.0.26.2。该 IP 地址不是商户访问支付宝的地址，而是支付宝发送通知给商户的出口地址。	如果商户网站设置了 IP 白名单（即 IP 过滤），需要把支付宝的通知 IP 地址加入白名单中。
	商户必须以 DNS 解析的方式访问支付宝接口，不要设置 DNS cache，不要绑定支付宝 IP。如果为了商户自身安全必须绑定支付宝 IP 时，必须向支付宝的技术支持人员备案。	支付宝 IP 地址一旦变更，会导致商户无法请求或访问支付宝，致使商户业务直接不可用。
签名	请求的所有参数，需要根据参数名=参数值的格式，由字母 a 到 z 的顺序进行排序，待签名字符串需要以“参数名 1=参数值 1&参数名 2=参数值 2&….&参数名 N=参数值 N”的规则进行拼接。	避免接口无法正常使用
	在对请求的参数做签名时，这些参数必须来源于请求参数列表，并且除去列表中的参数 sign、sign_type。	避免接口无法正常使用
	在对请求的参数做签名时，对于请求参数列表中那些可空的参数，如果选择使用它们，那么这些参数的参数值必须不能为空或空值。	避免接口无法正常使用
参数配置	在请求参数列表中，不可空的参数必须配置。	避免接口无法正常使用
	在请求参数列表中，可空的但需要多选一的多个参数中，必须配置至少一个。	避免接口无法正常使用
	必须按照请求参数列表中各参数的格式要求配置	避免接口无法正常使用
	必须设置请求参数_input_charset（编码格式），即该参数不能为空，并让该参数加入签名运算。	避免接口无法正常使用
接口构造	必须使用支付宝的网关发送请求信息给支付宝，请求网关：https://mapi.alipay.com/gateway.do。	避免被钓鱼网站利用

类型	细则	原因
	发送给支付宝的请求，请求参数不仅包含参与签名的参数，还包含参数 sign、sign_type。	避免接口无法正常使用
	发送给支付宝的请求，如果使用 form 表单传输，需要按照以下要求编写： ● action的值必须为“https://mapi.alipay.com/gateway.do?_input_charset=该值”， 如：https://mapi.alipay.com/gateway.do?_input_charset=utf-8。 不允许写成完整的请求链接地址，即禁止https://mapi.alipay.com/gateway.do?后带有所有要请求给支付宝的请求参数数据； ● <form>与</form>之间需包含所有要请求给支付宝的参数，且每个参数的格式为<input type="hidden" name="参数名" value="参数值" />； ● 在众多请求参数中，请求参数_input_charset（编码格式）必须存在于 form 表单中，即 form 表单中必须含有<input type="hidden" name="_input_charset" value="参数值">； ● <form>与</form>之间包含的数据只允许是要请求给支付宝的参数，禁止出现商户自行命名，不在接口技术文档请求参数列表中的其他数据； ● form 表单的 method 属性，可自行选择 get、post 两种。	● 避免请求支付宝时报错，错误码为 ILLEGAL_SIGN； ● 在 win7 系统下，如果浏览器是 IE8 以上，有可能出现发送请求链接时会无法跳转到支付宝，当前页面为空白页的情况。
数据传输	必须使用 https 协议，支持 get 或 post 方式提交。	避免接口无法正常使用
通知返回验证	如果有设置通知路径及触发条件，则必须使用获取到的参数 notify_id 再次请求支付宝，获取是否是支付宝发送的验证结果。该请求链接是： https://mapi.alipay.com/gateway.do?partner=合作者身份 ID&notify_id=通知 ID 的值	验证是否是支付宝发来的请求
	在对通知的参数做签名时，这些参数必须来源于支付宝通知回来的参数，并且除去列表中的参数 sign、sign_type，依照“参数名 1=参数值 1&参数名 2=参数值 2&…&参数名 N=参数值 N”的规则进行拼接，得到的签名结果与获取到的参数 sign 值做比较。	验证返回的签名
返回数据处理	必须对返回的数据进行处理	以便商户能够了解接口的使用情况，以及进行商户的后续业务操作。

类型	细则	原因
	必须判断登录操作以后的业务逻辑处理程序是否有重复执行	防止出现商户的业务操作被重复执行，导致出现资金损失，如重复充值、重复付款等。
	建议每一次登录操作需以日志形式记录到商户网站的日志操作数据库中	用来在必要时检查或跟踪业务处理情况
	必须保存返回信息授权令牌 token，且不能篡改该信息。	用于操作其他接口（如即时到账、担保交易等)时，用户免登录功能。
	保存下来的返回参数授权令牌 token，必须与快捷登录使用的登录支付宝账号对应，不能与其他支付宝账号混淆。	避免用户免登录时，校验不通过。
	确保返回的用户相关信息与签约时开通的信息一致，无遗漏或多余。	根据不同的签约商户，返回的用户相关信息完整程度不同。返回用户具体信息的完整程度由商户签约时双方约定。
接入环境	不能把接口嵌入 iframe 框架中	避免接口无法正常使用
错误码处理	非法参数（ILLEGAL_ARGUMENT）	若其他参数全部符合接口参数格式要求，请检查 return_url 是否为空。
	无权访问（HAS_NO_PRIVILEGE）	若该商户已经申请并且开启了快捷登录接口，由于网络或者缓存原因，用户登录后获取用户信息失败导致无权访问。解决办法：清除浏览器缓存，重新打开浏览器做登录操作。
自主编写接口代码规则	如果不使用支付宝提供的代码示例来集成接口，那么必须根据技术文档中签名机制和通知返回数据处理章节及本文档的技术接入规则、接口使用规则、测试流程规则，来编写符合商户网站项目的接口代码。	避免接口无法正常使用

4 接口使用规则

表4-1 接口使用规则

类型	规范点	原因
业务操作	申请快捷登录接口开通	快捷登录需申请且签约才能开通，未签约的商户或未开通的商户不能使用。
	通过快捷登录后，商户网站此时须让买家直接进入下单流程即当前界面为填写订单的页面，或者让当前界面跳回买家登录前的那一个页面。禁止出现让用户设置商户网站的会员密码的操作界面等把支付宝会员转换为商户网站自己的会员的操作。	在商务协定上，商户不能有把支付宝会员转换为商户网站会员的行为。
	在商户网站中必须使用支付宝用户号（返回参数 user_id）作为唯一标识，禁止使用其他信息作为唯一标识。	参数 user_id 对于支付宝系统是唯一且不会变更的，而支付宝账号的登录账号支持支付宝用户手动更改，这样会导致商户得到的支付宝会员信息错乱。
	• 如果用户是通过快捷登录接口访问商户网站，且商户能获取到返回参数 real_name 的信息，那么商户网站上须显示此时获取到的参数 real_name 的信息，即支付宝用户真实姓名； • 如果用户是通过一淘且该用户已登录支付宝或淘宝并访问商户网站，商户网站上需显示此时获取到的参数 real_name 的信息，即支付宝用户真实姓名或淘宝昵称。	在商务上保证名称显示的规范与统一
	获取到的参数 real_name 需匹配一致性	通过快捷登录接口获取到的真实姓名（参数 real_name，即支付宝会员名），与通过一淘调用获取到的支付宝会员名或淘宝昵称（参数 real_name）有可能造成 real_name 不一致，因为同一个用户的支付宝会员名（一般为真实姓名）与淘宝昵称是不一样的。商户可以依照自己的业务逻辑把这两个信息都储存下来，也可以只选取其中的一个储存。
保密性	禁止滥用获取到的会员信息做非法用途或传播	避免信息泄露，支付宝会员的信息具有保密性。
一淘	如果返回的信息中存在参数 target_url，那么执行完 return_url 文件后，程序须自动跳转到 target_url 指定页面路径中。	用于在一淘上点击某商户的商品后，当前界面自动跳转到 target_url 的页面地址中，且此时根据用户是否已登录一淘，来判定在商户网站中是否也需处于已登录状态。

类型	规范点	原因
网络	确保网络顺畅，防止系统间通信异常。	防止用户登录不成功或登录成功后跳转对应的商户返回页面异常

5 测试流程规则

表5-1 测试流程规则

步骤	调试内容	备注
第一步：在本机单独对这个接口进行调试。	• 申请快捷登录接口开通； • 请求授权平台授权，跳转到快捷登录页面； • 用户做支付宝账户登录操作； • 成功登录后，跳转对应的商户返回地址页面，并将用户的基本信息传递给对应的商户。	仅仅把接口配置好，不要放在商户的网站项目中。
第二步：在服务器上单独对这个而接口进行调试	• 申请快捷登录接口开通； • 请求授权平台授权，跳转到快捷登录页面； • 用户做支付宝账户登录操作； • 成功登录后，跳转对应的商户返回地址页面，并将用户的基本信息传递给对应的商户。	本机调试没有问题后，再放入服务器中调试。
第三步：接口融合到网站项目中	• 申请快捷登录接口开通； • 请求授权平台授权，跳转到快捷登录页面； • 用户做支付宝账户登录操作； • 成功登录后，跳转对应的商户返回地址页面，并将用户的基本信息传递给对应的商户。	把调试好的接口与商户网站项目的业务流程进行衔接和融合。

步骤	调试内容	备注
第四步：在本机对融合后的网站项目进行调试	• 申请快捷登录接口开通； • 请求授权平台授权，跳转到快捷登录页面； • 用户做支付宝账户登录操作； • 成功登录后，跳转对应的商户返回地址页面，并将用户的基本信息传递给对应的商户。	在本机调试衔接到网站项目后的接口。
第五步：在服务器对融合后的网站项目进行调试	• 申请快捷登录接口开通； • 请求授权平台授权，跳转到快捷登录页面； • 用户做支付宝账户登录操作； • 成功登录后，跳转对应的商户返回地址页面，并将用户的基本信息传递给对应的商户。	本机调试没有问题后，再放入服务器中调试。