|  |  |
| --- | --- |
| 项目标号 |  |
| 密级： | 绝密 机密 限制 一般 |
| 草稿文档： |  |
| 正式文档： |  |
| 正式文档修正： |  |

接入CAS

接口说明

盛大网络计费平台中心

文档修改记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 版本 | 修改者 | 主要修改内容 | 日 期 |
| 1 | V2010-06-02 | 王红霞 | 接入CAS的相关说明 | 2010-06-02 |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |

目录

[**1** 内容简介 4](#_Toc263239128)

[**2** OpenID接入CAS的认证流程 4](#_Toc263239129)

[**3** 接口明细 5](#_Toc263239130)

[**3.1** 获取token和timer接口 ………………………………………………………………………………….5](#_Toc263239131)

[**3.1.1** 参数列表 5](#_Toc263239132)

[**3.1.2** 返回值 5](#_Toc263239133)

[**3.2** 验证token和timer接口 ………………………………………………………………………………….6](#_Toc263239134)

[**3.2.1** 参数列表 6](#_Toc263239135)

[**3.2.2** 返回结果 6](#_Toc263239136)

[**3.3** 验证ticket接口 …………………………………………………………………………………………...6](#_Toc263239137)

[**3.3.1** 参数列表 6](#_Toc263239138)

[**3.3.2** 返回值 7](#_Toc263239139)

# 内容简介

此文档是针对OpenID接入CAS的详细说明，将重点阐述OpenID接入CAS后的认证流程，以及CAS提供的关键接口明细。旨在使读者能够对OpenID模式的应用接入CAS有一个整体的把握，并能根据接口明细成功的接入CAS。

# OpenID接入CAS的认证流程

接入CAS后的认证流程可用下图表示：

图1 OpenID接入CAS的认证流程图

其详细的认证流程如下所述：

（1）用户在OpenID 登录后，访问OpenID URL是<http://xxxx2.do>

（2）OpenID服务器在服务器端将pt账号ptid、数字账号sdid、原始输入账号originid提交给CAS，调用的接口为

[http://dev.cas.sdo.com:8171/cas/Cas.SSO.Key.aspx?ptid=&sdid=&originid](http://61.172.252.14:8171/cas/Cas.SSO.Key.aspx?ptid=&sdid=&originid)= ，CAS接口将动态密钥token和时间戳timer返回给OpenID服务器

（3）OpenID服务器获取到token和timer后，将其编码加密后形成的字符串vkey，在客户端提交给CAS进行验证，重定向的URL地址为

[http://dev.cas.sdo.com:8171/cas/Cas.Sso.aspx?vkey=&service=xxxx2.do](http://61.172.252.14:8171/cas/Cas.Sso.aspx?vkey=&service=xxxx2.do)

（4）CAS对vkey进行验证，成功后将浏览器重定向至OpenID，并将ticket以参数形式传递给OpenID务器，URL表现为<http://xxxx2.do?ticket>=

注：token和timer是CAS与OpenID服务器之间的信任机制，OpenID服务器在服务器端获取到CAS生成的token和timer，并将其编码加密后传递给CAS，CAS验证此token和timer的确是自己发给该url的，才会将ticket传递给OpenID服务器

（5）OpenID服务器在服务器端把ticket传递给CAS做校验，其验证接口为 [http://dev.cas.sdo.com:8171/cas/Validate?ticket=&extend](http://61.172.252.14:8171/cas/Validate?ticket=&extend)=，接口会将用户的PT账号返回给OpenID服务器

# 接口明细

## 获取token和timer接口

测试环境地址： [http://dev.cas.sdo.com:8171/cas/Cas.SSO.Key.aspx?ptid=&sdid=&originid](http://61.172.252.14:8171/cas/Cas.SSO.Key.aspx?ptid=&sdid=&originid)=

正式环境地址：<https://cas.sdo.com/cas/cas.sso.key.aspx?ptid=&sdid=&originid>=

调用方式：OpenID服务器在服务器端调用该URL接口

### 参数列表

|  |  |  |
| --- | --- | --- |
| 参数名 | 参数说明 | 备注 |
| ptid | Pt账号 | 该参数可以不传入，如果有的话尽量传过来，可以加快服务速度 |
| sdid | 数字账号 | 该参数必须传入 |
| originid | 用户输入的原始账号 | 该参数可以不传入，如果不传，在后面调用CAS的验证接口时不会获得用户原始输入的账号，可能是邮箱账号、手机账号 |

### 返回值

|  |  |
| --- | --- |
| 返回值格式 | 返回值说明 |
| yes char(10) token char(10) timer char(10) | * Char(10)表示换行符\n * Token是CAS生成的动态密钥 * Timer是CAS生成的时间戳 * OpenID服务器获取到该返回值后，需要对token和timer编码提交给CAS |

## 验证token和timer接口

测试环境地址： [http://dev.cas.sdo.com:8171/cas/Cas.Sso.aspx?vkey=&service=](http://61.172.252.14:8171/cas/Cas.Sso.aspx?vkey=&service=xxxx2.do)

正式环境地址： <https://cas.sdo.com/cas/Cas.sso.aspx?vkey=&service>=

调用方式：在客户端将浏览器重定向至该URL

### 参数列表

|  |  |  |
| --- | --- | --- |
| 参数名 | 参数说明 | 备注 |
| vkey | 将token和timer编码后形成的字符串 | 编码格式：  string vkey  =     string.Format("{0}{1}{2}{3}", ptid, sdid, timer, token); //如果第一步里ptid, sdid任何一个没传,就填写""  vkey         =     FormsAuthentication.HashPasswordForStoringInConfigFile(vkey, "md5");  注：返回的timer、token只能用一次，提交给CAS后便失效不能再用 |
| service | 验证成功后CAS返回给OpenID服务器ticket的url | 该URL需要进行url编码 |

### 返回结果

有两种情况：

|  |  |
| --- | --- |
| 返回结果 | 结果说明 |
| 1．如果该用户绑定了密宝、安全卡，客户端浏览器会跳转到输入相关动态认证信息的页面 |  |
| 2 如果用户没有绑定密宝、安全卡，CAS对token和timer验证成功后，会将客户端浏览器重定向至service表示的url，并传入参数ticket  如：<http://xxxx2.do?ticket>= | 该ticket是以时间戳及随机值生成的字符串，service对应的URL服务获取ticket后需要提交给CAS进行验证  注：ticket也是只能使用一次的 |

## 验证ticket接口

测试环境地址：<http://dev.cas.sdo.com:8171/cas/Validate?ticket=&extend>=

正式环境地址：<https://cas.sdo.com/cas/validate?service=&ticket=&extend=>

调用方式：OpenID服务器在服务器端调用该URL接口

### 参数列表

|  |  |  |
| --- | --- | --- |
| 参数名 | 参数说明 | 备注 |
| ticket | Ticket是CAS返回给OpenID服务器的随机值 | Ticket只能使用一次，提交给CAS后便失效不能再次使用 |
| extend |  | 此参数可带可不带   * 传入该参数表示该接口需要返回数字账号和用户原始输入的账号 * 不传入表示只返回PT账号 |

### 返回值

有三种情况：

|  |  |
| --- | --- |
| 返回值格式 | 返回值说明 |
| 如果ticket验证成功且不带extend参数，返回  yes char(10) PT char(10) | * Char(10)表示换行符\n |
| 如果ticket验证成功且带extend参数，返回  yes char(10) PT char(10) sdid char(10) originid char(10) | * PT——pt账号 * Sdid——数字账号 * Originid——用户输入的原始账号，如pt账号、邮箱账号、手机账号等 |
| 如果ticket验证失败或service为无效的URL，返回  no char(10) char(10) |  |

以上就是OpenID接入CAS时用到的接口，为了更明确这些接口的参数及返回值情况，我们提供各种类型的账号的测试接口，接入方可以参考理解：

（1）普通账号（未绑定密宝、安全卡）传入ptid、sdid、originid

<http://dev.cas.sdo.com:8171/cas/Test.Cas.SSO.Ex?ptid=mobfan&sdid=28400156&originid=testmobfan&service=http%3A%2F%2Fdev%2Ecas%2Esdo%2Ecom%3A8171%2Fcas%2FTest%2ECas%2ESSO%2EEx>

（2）普通账号只传入sdid、originid

<http://dev.cas.sdo.com:8171/cas/Test.Cas.SSO.Ex?sdid=28400156&originid=testmobfan&service=http%3A%2F%2Fdev%2Ecas%2Esdo%2Ecom%3A8171%2Fcas%2FTest%2ECas%2ESSO%2EEx>

（3）X6密宝用户

<http://dev.cas.sdo.com:8171/cas/Test.Cas.SSO.Ex?ptid=lidex6&sdid=37818218&originid=testekeyX6&service=http%3A%2F%2Fdev%2Ecas%2Esdo%2Ecom%3A8171%2Fcas%2FTest%2ECas%2ESSO%2EEx>