# 账号体系说明

创建时间:2016-02-29

修改时间:\*\*\*

因为之前没有涉及到信息安全方面的知识,所以即使找了一些资料也没有关于这方面也没有什么好的解决办法.另外这方面问题不解决,也影响业务逻辑代码的编写.

幸好在田光前误打误撞下的指引下,也在修玉同学长的帮助下,我顺利地了解云账号(OpenAccount),并测试通过云账号的核心功能.

阿里百川云账号(OpenAccount)官方地址:

<http://baichuan.taobao.com/doc2/detail.htm?articleId=102958&docType=1&treeId=40>

由于云账号刚上线不久,文档还不详细.它提供的功能大概包括以下.

OpenAccount是阿里巴巴为开发者提供的独立账户注册、登录、管理的基础能力，能够帮助开发者降低开发成本，与阿里巴巴其他技术体系更好的集成。 OpenAccount提供的账号集成包括：新账号注册、开发者已有账号体系集成、第三方社交平台开放账号体系。并为以下服务提供账号支撑：IM、图片、社区、LBS、数据。

在我的理解下,OpenAccount提供了一个云服务,作为使用者,可以很简单地使用它的注册,登录,找回密码和登出功能.



Token的申请和校验

Token校验

在云账号移动端SDK（或PC端），用户进行**登录、注册和找密操作**成功之后，操作成功的状态需要使用Token（客户端android使用session.getAuthorizationCode()、IOS 上使用[[ALBBOpenAccountSession sharedInstance] getAuthToken]获得）可信的从ISV的客户端传递给ISV的服务端。ISV的服务端需要使用taobao.open.account.validate进行Token的校验，获得当前的用户的账号。

Token申请

使用token登录，建立SDK内登录态，进而使用其他依赖登录态的服务，如Open IM和Open Trade等。 通过taobao.open.account.token.apply申请TOKEN。

作为客户端开发人员,利用SDK可以非常方便地实现注册,登录,找回密码和登出功能(它的SDK提供图形化界面).和我的服务器端交互时,不再需要给出用户名和密码,只需持有token,服务器端就可以识别你的身份,从而完成身份验证工作.

不过修改密码的功能SDK并没有直接提供,需要向服务器端请求,再由服务端申请向OpenAccount服务器修改.

作为服务器端开发人员,我的最主要的工作之一就是验证客户端发来请求的token,这也由OpenAccount提供的验证方法.当验证成功并找到相应的账号,我才处理请求并返回响应内容.其余的工作包括同步用户账号,提供修改密码等功能.

具体的**使用方式**为:

1. 客户端登录同时,将token发送给我,我通过官方API来验证token的正确性,找到对应的用户信息,在服务器端记录token和对应的账号之间的绑定关系.(注意token从产生到失效只有一分钟的时间)
2. 客户端在请求其他业务操作时,需要在请求的同时将token传送给我,我在本地验证此token是否存在及对应的账号.

为了防止token被窃取,这里对token采取非对称加密RSA算法加密的办法,由于RSA加密对原文有长度限制,所以将token分为两部分,前一部分采用RSA加密(公钥加密),后一部分直接发送原文,在服务器(私钥解密)拼装成完整的token再进行验证.前一部分暂命名为tokenrsa,后一部分暂命名为tokenplain.

公钥如下:

private static String myPublicKey =

"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDiZnfrXIhQy3+J2glrMRqpX5XB"

+ "JuBT3+eRx4h7eaki3Jg6Pk8dV34iCK0AJyP2KdO2ZGWa7rlkTMbV+oIFW/d4nBEa"

+ "FzFI+ji90nQoJNLKEqwN5O/7Xu9ZVMgOYIZFUe1hAyGTzPJyBWz4o+Usr4WyCW4y"

+ "7gXqiI9Jf1W5L6xNbQIDAQAB";

但是这样仍然不能防止别人利用截取的请求进行重放攻击,或者通过保持tokenrsa和tokenplain不变同时修改其他参数来恶意篡改用户信息(中间人攻击).

我的解决办法是再设置一个参数signature,内容为token原文和请求时间距离1970年元旦零点的分钟数拼接后字符串的MD5值.

我的校验方法是,尝试三次核对,分别是:

1. 接收到请求时间距离1970年元旦零点的分钟数加上token的MD5值,
2. 前一分钟距离1970年元旦零点的分钟数加上token的MD5值,
3. 前两分钟距离1970年元旦零点的分钟数加上token的MD5值,

其中,在Java中, 距离1970年元旦零点的分钟数可以通过

System.currentMillsecond()/60000获得.

假如有任何一次核对正确,那么就认为请求合法,否则认为是非法请求.

1. 尝试用私钥解密tokenrsa,解密失败则返回验证失败
2. 将解密后的tokenrsa与tokenplain拼接得到token,向OpenAccount服务器验证token,验证失败则返回验证失败.
3. 根据token和距离1970年元旦零点的分钟数计算出数个备选signature,与请求参数中的signature相比较,若有一个相同则返回验证成功,否则返回验证错误.

登录时传送给我openaccountid,

/api/login?openaccountid=123&cellphone=123

OpenAccount的常见错误码如下



具体使用的附图如下:







另外一张附图由修玉同学长提供,这里放不下,为OpenAcount-xiuyutong.jpg.

俞霄翔,修玉同

2016/2/29