**斐讯云账户服务设计文档**

**产品型号：PhiCloudPlatform**

**模块名称：斐讯云账户服务**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 修 订 记 录 | | | | | |
| 修订日期 | 版本 | 修订内容摘要 | 修订 | 审核 | 批准 |
| 2016-11-07 | V1.0 | 初版 | 网管平台-公共业务中心 |  |  |
| 2017-03-23 | V1.1 | 增加云账户服务对智能硬件产品线的支持。  增加对多端登录的支持。  增加云服务对业务服务器的回调机制方案。 | 网管平台-公共业务中心 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目 录

[1. 关于文档 3](#_Toc466316720)

[1.1. 参考文档 3](#_Toc466316721)

[1.2. 缩略语解释 3](#_Toc466316722)

[1.3. 名词解释 3](#_Toc466316723)

[1.4. 背景与目的 3](#_Toc466316724)

[2. 架构综述 4](#_Toc466316725)

[2.1. 功能简介 4](#_Toc466316726)

[2.2. 功能框架 5](#_Toc466316727)

[2.3. 云账户用例 6](#_Toc466316728)

[3. 架构设计 8](#_Toc466316729)

[3.1. 云账户服务逻辑架构 8](#_Toc466316730)

[3.2. 云账户与其它服务的部署图 9](#_Toc466316731)

[3.3. 云账户工作流程图 10](#_Toc466316732)

[3.4. token机制 11](#_Toc466316733)

[3.5. 云账户角色设计 14](#_Toc466316734)

[3.6. 数据库设计 14](#_Toc466316735)

[3.7. 数据库加密 16](#_Toc466316736)

[3.8. 开源框架或工具包列表 17](#_Toc466316737)

[4. 附录 17](#_Toc466316738)

[4.1 约束与限制 17](#_Toc466316739)

# 关于文档

## 参考文档

《Subscriber Cloud HLD\_1.1.doc》

## 缩略语解释

JWT：JSON Web Token，一种token机制。

## 名词解释

账户绑定：新的Account账户系统中，会提供用户名、手机号和邮箱号三种登录方式，用户注册账号后，如果完善了这三个信息，可以使用其中任何一个作为账户进行登录，而且这三种登录方式的效果是完全一样的，即代表了同一个账户。

快捷登录：用户通过获取手机验证码的方式登录云账户系统，无需密码。

## 背景与目的

本次服务器升级的目的是，将“斐讯路由APP”账户、“斐讯商城”账户和“斐讯论坛”账户三个系统进行合并，实现统一账户管理的目的。但目前三个系统的账户体系各有特点，下面分别叙述各个账户系统的特点。V1.1版本以Android SDK和iOS SDK的方式增加了对智能硬件产品线的统一账户支持，目前包括：“斐讯健康APP Android/iOS版”，“斐讯运动APP Android/iOS 版”。同时增加对“环境猫”APP的账户支持。

“斐讯路由APP”账户有如下特点：

1. 分为邮箱账户和手机账户，这两个账户相互独立，不能互相绑定，但是可以互相关联共享设备列表。
2. 目前APP已经不支持邮箱账户的注册，但保留历史的邮箱账户的使用权限。
3. 老的路由器，如FIR系列可以通过路由器页面进行注册邮箱账户，而且同一个邮箱，在未激活之前可以重复注册。
4. 该系统对用户密码采用了自己的加密方式。
5. 目前改APP不允许用户多端登录。用户的最近一次登录会踢出其它设备上该APP的登录。

“斐讯商城”账户有如下特点：

1. 目前只有手机账户，没有邮箱账户。
2. 需要支持快捷登陆。V1.1版本取消对快捷登录的支持，页面提示用户通过“忘记密码”页面转化为正式注册用户。

“斐讯论坛”账户有如下特点：

1. 支持用户名登录。
2. 支持手机号登录。
3. 支持邮箱号登录。
4. 用户名、手机号和邮箱号三者可以实现绑定，即使用用户名、手机号、邮箱号登录的效果是一样的。
5. 该系统对用户密码采用了自己的加密方式，不同于“斐讯路由APP”账户系统。

本文就针对以上三个系统的特点，设计通用的云账户系统，并为今后的业务扩展建立基础。

“斐讯健康APP Android/iOS版”账户有如下特点：

1. 支持手机号登录。
2. 支持用户以QQ和微信账户三方登录。
3. 支持三方登录账户绑定新手机号。
4. 绑定手机号后，该手机号享受斐讯其他服务。

“斐讯运动APP Android/iOS版”账户有如下特点：

1. 支持手机号登录。

2 支持用户以QQ和微信账户三方登录。

1. 支持三方登录账户绑定新手机号。
2. 绑定手机号后，该手机号享受斐讯其他服务。

# 架构综述

## 功能简介

目前斐讯有众多业务都将用到云账户系统，如Smart Home、斐讯商城、斐讯论坛等，给用户提供统一、便捷、安全的账户系统是非常有必要的。

斐讯云账户服务提供统一的云账户管理接口，将服务于斐讯App产品、斐讯商城和斐讯论坛等。斐讯云账户管理系统严格遵循标准的软件工程规范进行设计，把原先附属于业务系统中的账户模块剥离出来，既提高了账户系统的性能，又防止因账户业务功能的修改给其它业务带来风险，从而保障了业务安全，最大程度降低了系统运行风险。同时，从系统架构上也更为先进，模块化的设计有利于系统的后续发展。

云账户模块中有打点需求，用于记录用户行为，在老的云服务中，打点功能和业务功能混淆在一起，造成代码结构相对混乱。新的云服务中，采用了API网关，所有的统计需求将会在API网关中实现，实现统计与业务的分离。

在安全性方面，新的云服务所有接口将会采用HTTPS协议，并且采用JWT的token机制保障接口的安全性。除此外，数据库安全也是很重要的方面，新的云服务将采用全新的数据库安全技术，即使数据失窃，也能保证数据不被轻易破解。

总而言之，新的云账户系统有如下特点：

1. 标准化。
2. 模块化。
3. 简洁化。
4. 性能提升。
5. 安全性提升。

## 功能框架



图 斐讯云账户服务架构框图

上图是斐讯云账户服务的架构框图，本服务的总体设计目标是，能覆盖斐讯的产品和业务，为用户提供方便快捷的账户管理平台，主要功能特性如下：

* 账户统一管理，各个平台业务使用统一的账户体系。
* 设备管理，用户登陆云服务后，可以接入设备管理服务，从而实现远程管理与监控设备。
* 增值服务，新增会员体系实现增值功能。
* 支付服务，用户将来在斐讯商城上可以直接下单，支付，并且查看物流信息等。
* 存储服务，每个用户会有一定的云存储空间用于存储用户照片，通讯录等隐私信息。
* 家庭服务，家庭成员之间可以一定程度上共享设备，增值服务等资源。
* 用户行为分析，针对用户使用习惯，偏好等进行大数据统计与分析，有助于进一步完善公司的产品质量。
* OAUTH支持，支持第三方通过标准OAUTH登陆。

技术上，参考业界主流技术，主要特性如下：

* 采用JWT Token实现跨服务器的安全认证，相对于传统的session机制，避免了session同步的问题，客户端应用只需要登陆账户服务器获取到JWT Token后，就可以凭JWT Token得到其他业务服务的认证，而业务服务器不需要与账户服务器同步任何数据，有利于云服务的分布式部署。
* HTTPS安全，云账户所有接口都将采用HTTPS安全加密，使得用户数据的传输更加安全可靠。
* 接口标准化，云账户接口参考业界的接口定义规范，将接口定义更加规范。

## 云账户用例



图 斐讯云账户服务针对用户用例图

上图是斐讯云账户针对用户的用例图，用户登陆云账户后，可以享受多元化的服务，实现账户-服务-设备之间的绑定，用户使用的将不是单一的个体，而是一整套完整的服务体系。



图 云账户服务与其它系统关系用例图

图是云账户系统用例图，云账户服务为斐讯APP、斐讯商城和斐讯论坛提供云账户操作相关的口，云账户主要包括自定义的云账户接口和标准的OAUTH接口。

斐讯APP从设备管理服务侧获取设备列表，然后通过路由器远程管控服务控制设备，路由器远程控制服务会检验App传来的token，是否是云账户服务颁发的。

云账户会用到短信和邮件服务，这两个部分在平台服务中提供。

# 架构设计

## 云账户服务逻辑架构



图 云账户服务逻辑架构图

上图是云账户服务的逻辑架构图，架构由上而下采用三层设计，即表现层，实体层和资源层。表现层提供给用户平台前端，用户可以通过平台前端注册、激活、登陆系统，并且可以在平台接入斐讯商城、斐讯论坛系统。还为运维或市场人员提供数据统计前端。

实体层提供业务服务和公共服务，为表现层提供API接口和后台服务。

资源层主要包括数据库、文件和其它平台资源。数据库利用读写分离，主备结合的方式实现分布式部署。文件主要包括：用户资料，用户头像和照片等。云账户还需要用到其它平台的资源，比如到设备服务获取设备资源，商城获取账单资源，物流公司获取物流资源等。

## 云账户与其它服务的部署图



图 新的云账户物理部署图

图是云账户与其它服务的部署图，新的云账户服务器和老的云账户服务器同时运作，作为中间过渡期形态。新的云账户服务增加了斐讯头像服务器集群，专门用于处理用户的头像、个人图片资料等信息。

【注】目前负载均衡采用Haproxy方案，后续将更换为API网管。

## 云账户工作流程图



图 新用户注册、登录流程图

上图是新用户注册、登录流程图，主要流程描述如下：

1. 应用(如斐讯商城、斐讯App、斐讯论坛等)请求授权码，应用需要传入clientID和secret，账户服务器根据应用返回授权码，授权码是被AES128加密的密文，根据授权码，服务器可以鉴别应用的身份。
2. 获取到授权码后，应用就可以调用云账户的接口，首先调用获取验证码接口，云账户服务会返回验证码。
3. 通过获取到的验证码进行账户注册。
4. 登陆云账户，获取token。该token采用JWT生成规则。
5. 接下来的操作都需要携带token值，并且定期刷新token。



图 跨应用自动登录流程

## token机制

**3.4.1 概述**

本方案中将采用JWT（JSON Web Token）作为登陆认证机制，基于token的身份验证是无状态的，我们不将用户信息存在服务器或session中，相比原始的Cookie+Session方式，更适合分布式系统的用户认证，绕开了传统的分布式session一致性等问题。

**3.4.1 JWT的组成**

一个JWT实际上就是一个字符串，它由三部分组成，头部，载荷与签名。

1. Header报头

Header部分主要包括两部分，一个是Token的类型，另一个是使用的算法。比如下面类型就是JWT，使用的算法是HS256.

{“typ”:”JWT”,”alg”:”HS256”}

Header内容要用 Base64 的形式编码，所以就变成这样：

ewogICJ0eXAiOiAiSldUIiwKICAiYWxnIjogIkhTMjU2Igp9

1. Payload载荷部分

Payload 里面是 Token 的具体内容，这部分内容可以自定义，JWT有标准字段，也可以添加其它需要的内容。

标准字段：

iss：Issuer，发行者

sub：Subject，主题

aud：Audience，观众

exp：Expiration time，过期时间

nbf：Not before

iat：Issued at，发行时间

jti：JWT ID

这是一个典型的payload信息，包含了发行者（网站）、过期时间和用户id：

{

"iss": "chblogs.com",

"exp": "1470730182",

"uid": "12345abcde",

}

这部分内容同样要用Base64 编码，生成编码类似如下格式：

ewogImlzcyI6ICJjaGJsb2dzLmNvbSIsCiAiZXhwIjogIjE0NzA3MzAxODIiLAogInVpZCI6ICIxMjM0NWFiY2RlIiwKfQ==

1. Signature签名部分

签名部分主要和token的安全性有关，Signature的生成依赖前面两部分。首先将Base64编码后的Header和Payload用.连接在一起，

ewogICJ0eXAiOiAiSldUIiwKICAiYWxnIjogIkhTMjU2Igp9.ewogImlzcyI6ICJjaGJsb2dzLmNvbSIsCiAiZXhwIjogIjE0NzA3MzAxODIiLAogInVpZCI6ICIxMjM0NWFiY2RlIiwKfQ

对这个字符串使用HmacSHA256算法进行加密，这个密钥secret存储在服务端，前端不可见

下面使用密钥 THISSHA 进行加密：

9q2eq8sa374ao2uq9607r6qu6

然后将Signature和前面两部分拼接起来，得到最后的token：

ewogICJ0eXAiOiAiSldUIiwKICAiYWxnIjogIkhTMjU2Igp9.ewogImlzcyI6ICJjaGJsb2dzLmNvbSIsCiAiZXhwIjogIjE0NzA3MzAxODIiLAogInVpZCI6ICIxMjM0NWFiY2RlIiwKfQ.9q2eq8sa374ao2uq9607r6qu6

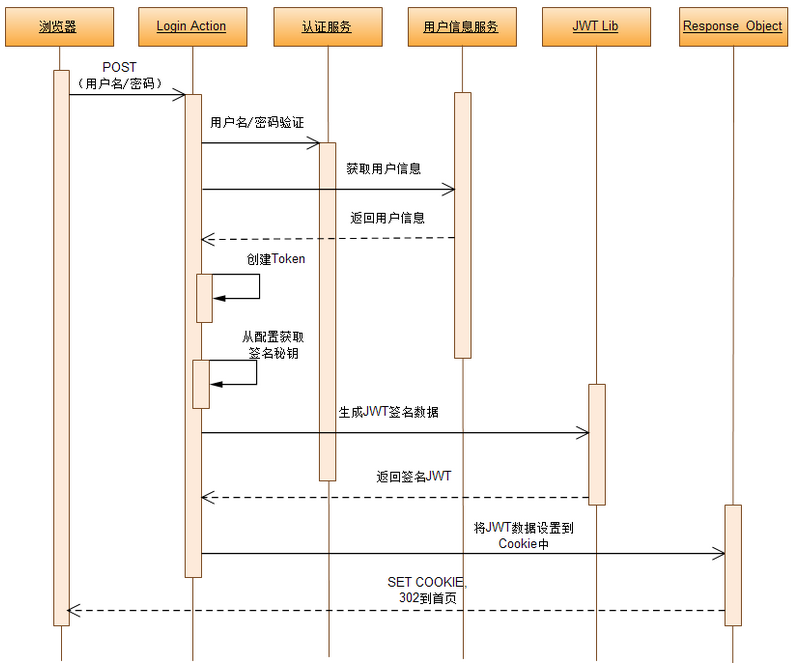


图 采用JWT登陆认证流程

图是通过JWT登陆认证的流程图，认证通过后，客户端会获取一个JWT字符串，客户端将该字符串保存到Cookie中，以后每次交互都需要将该字符串放到HTTP Request的Header中。

这样，服务器只需要维护秘钥secret即可，服务器与服务器之间不存在session的维护问题，服务器只需要维护同一个秘钥机制。为了进一步提升安全性，服务器侧应定期更换秘钥。由于本方案中的payload部分由BASE64编码，将BASE64解码后就可以轻松得到明文信息，因此，本方案更加适合于配合HTTPS协议。

## 云账户角色设计



图 云账户角色用例图

上图是云账户角色用例图，云账户主要包括客户账户和员工账户两个角色，客户账户又分为普通账户和会员账户。

为了便于管理，新增员工账户，以方便管理，角色可以分为运维人员、产品经理、研发人员和其它人员，每个角色都会有不同的职责和权限管理。

## 数据库设计

**3.6.1 ER模型**



图 云账户ER模型

上图是云账户的ER模型图，描述了账户属性以及与资源之间的关系。

**3.6.2 数据库Schema设计**



图 云账户Schema设计

上图是云账户的Schema相关设计，fx\_user表示用户表，fx\_user\_logininfo表示记录登录信息，fx\_user\_data记录用户的属性信息，fx\_role存储用户角色种类，fx\_resource存储资源信息以及对应资源的访问权限。

## 数据库加密

要完全防止信息泄露是非常困难的事情，除了防止黑客外，还要防止内部人员泄密。但如果采用合适的算法去加密用户密码，即使信息泄露出去，黑客也无法还原出原始的密码（或者还原的代价非常大）。也就是说我们可以将工作重点从防止泄露转换到防止黑客还原出数据。

**3.7.1 PBKDF2算法**

PBKDF2算法，该算法原理大致相当于在HASH算法基础上增加随机盐，并进行多次HASH运算，随机盐使得彩虹表的建表难度大幅增加，而多次HASH也使得建表和破解的难度都大幅增加。使用PBKDF2算法时，HASH算法一般选用sha1或者sha256，随机盐的长度一般不能少于8字节，HASH次数至少也要1000次，这样安全性才足够高。

一次密码验证过程进行1000次HASH运算，对服务器来说可能只需要1ms，但对于破解者来说计算成本增加了1000倍，而至少8字节随机盐，更是把建表难度提升了N个数量级，使得大批量的破解密码几乎不可行，该算法也是美国国家标准与技术研究院推荐使用的算法。

下表对比了常用的算法特点：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **算法** | **特点** | **有效破解方式** | **破解难度** | **其它** |
| 明文保存 | 实现简单 | 无需破解 | 简单 |  |
| 对称加密 | 可以解密出明文 | 获取秘钥 | 中 | 需要确保秘钥不泄露 |
| 单向Hash | 不可解密 | 碰撞、彩虹表 | 中 |  |
| 特殊Hash | 不可解密 | 碰撞、彩虹表 | 中 | 需要确保“盐”不泄露 |
| Pbkdf2 | 不可解密 | 无 | 难 | 需要设定合理的参数 |

## 开源框架或工具包列表

|  |  |
| --- | --- |
| 名称 | 版本 |
| Spring | 4.3.0 |
| Spring-Session | 1.2.0 |
| Spring-data-redis | 1.7.1 |
| Mysql-connector | 5.1.39 |
| MyBatis | 1.3.0 |
| Slf4j | 1.7.9 |
| Log4j | 1.7 |

# 附录

## 4.1 约束与限制

1. 由于第2章中“账户绑定”需求要实现用户名、手机号和邮箱号能代表同一个账户，而且所有账户要满足唯一性的特点，因此用户名的命名规则必须受到约束，即其格式不能与邮箱号或者手机号相同。

2. 用户名、邮箱号、手机号都可作为账号登录，一旦申请后，不得进行修改。

3. 如果用户已经注册并激活了邮箱账户A和手机账户B，这两个账户只能在“斐讯路由APP”中进行账户关联操作，不能进行账户绑定操作。只有在如下两种情况下才能进行用户绑定操作：

* 用户注册并激活了邮箱账户A，但未注册或未激活手机账户B，可以通过邮箱账户A绑定手机B，绑定账户B时，需要向账户B发送验证码。
* 用户注册并激活了收账户B，但未注册或未激活邮箱账户A，可以通过手机账户绑定邮箱账户A，绑定账户A时，需要向账户A发送验证码。

4. 用户注册账户时，必须依赖于手机账号或邮箱账号，通过手机或邮箱接受验证码，以便后续密码找回等操作。但用户注册时，手机号或邮箱号只能选择其一，因为注册时手机或邮箱必须接受验证码来验证操作的合法性，而手机或邮箱同时接受验证码并不合理。

5. 用户名、邮箱号、手机号三者绑定后，不得直接解绑，但应支持重新绑定操作。需求场景为：用户更改了手机号或邮箱号。如：用户名A---邮箱号B---手机号C三者已经绑定，此时要更改手机号为D，则需要发送验证码到手机D，认证通过后，绑定关系为：用户名A---邮箱号B---手机号D。手机号C直接被手机号D替代，手机号D将继承手机号C的原有属性。若要修改邮箱账号，同理。

6. 由于线上“斐讯路由APP”账户已经通过手机号或邮箱号注册了，并且没有绑定关系，也没有用户名，因此这些账号无法互相绑定，但可以设置用户名。

7. 若用户名被注册了，但未激活，在验证码失效时间内，该用户名不可以被其它手机号或邮箱号进行注册，在验证码失效后，该用户名可以通过其它手机号或邮箱号进行注册。

8. 对于论坛用户，由于原系统对密码有自己的加密方式，合并后也将采用原有的方式进行解密，但用户修改密码后，将采用统一的密码加密方式。

9. 由于新的账户体系中，有绑定账户的操作，与原有的“斐讯路由APP”关联用户操作，容易给用户带来混淆，建议后续APP去除关联账户操作，改为分享设备操作，目前的共存只是作为过渡形态。

10. 验证码存在失效时间，默认为15分钟（根据业务需求可灵活配置）。