付费P2P文件分享软件

开发项目解决方案说明书(SO)

|  |  |  |
| --- | --- | --- |
| 文件状态  [V]草稿  [ ]正式发布  [ ]正在修改 | 文件标识 | 米唻哆-iSeek 1.0.0.1-SO |
| 当前版本 | 1.0 |
| 作 者 |  |
| 完成日期 | 2016-09- |

版 本 历 史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 提交日期 | 版本号 | 作 者 | 修 改 内 容 | 备注 |
| 2016-09- | 1.0 |  | 初始版本 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

术语缩写与解释

|  |  |  |  |
| --- | --- | --- | --- |
| 缩 写 | 解 释 | 缩 写 | 解 释 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目 录

1. 解决方案概述 5

2. 交互设计与使用说明 5

3. 技术选型与研发环境 5

4. 总体设计 5

4.1 网络结构 5

4.2 子系统 5

4.3 接口 5

5. 售后服务 5

## 1. 解决方案概述

## 2. 交互设计与使用说明

## 3. 技术选型与研发环境

## 4. 总体设计

### 4.1 网络结构

### 4.2 子系统

### 4.3 身份认证安全设计

身份认证体系借鉴和简化自Kerberos V4。

1）总体约定：

界面输入的任何密码，在系统内一律使用：

**HEX(MD5("5X#6423D79C74b6b+实际输入的密码+AB8471%VAED8A76E"))**

以下简称“变换后的密码”。

（其中“+”表示拼接字串，在实际拼接出的字串中不包括这个加号，下同。）

2）注册及修改密码：凡需传输密码，前端须对“变换后的密码”做AES加密再传输，即：

**Base64(AES("变换后的密码", KEY("CEEF0B3D241F4f3798FF89384BE7ACA1"), "AES/CFB/NoPadding")**

服务端存入数据库时，先解密出“变换后的密码”，再换KEY做AES加密保存，即：

**Base64(AES("变换后的密码", KEY("6A38719F22424b2d94227923E966F9AC"), "AES/CFB/NoPadding")**

3）登录（包括PC端及Web端登录）：前端登录请求中包含登录名，以及：

**Base64(AES("****32Byte随机密钥+登录名+前端系统UTC时间yyyyMMddhhmmss", KEY("变换后的密码"), "AES/CFB/NoPadding")**

其中：

随机密钥由前端在每次登录时随机生成，服务端用它来加密登录响应。

服务端收到请求后，从数据库中读取并解密出“变换后的密码”，作为密钥解密上述密文，核对登录名及前端系统时间，如果登录成功，服务端响应中包含：

**Base64(AES("32Byte传输密钥+登录名+服务器系统UTC时间yyyyMMddhhmmss", KEY("32Byte随机密钥"), "AES/CFB/NoPadding")**

其中：

传输密钥由服务端在每次登录时重新分配，前端登出或断开时销毁，可用来加密后续的关键私密消息。

4）单点登录：通过PC客户端点击链接免输密码进入充值等Web页。在每次点击链接时，先从服务端获取单点登录字串，请求消息中包含登录名，以及：

**Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")**

如果获取成功，服务端响应包含如下单点登录字串：

**URLCode（Base64(AES("8Byte令牌+登录名+服务器系统UTC时间yyyyMMddhhmmss", KEY("32Byte服务端密钥"), "AES/CFB/NoPadding"))**

其中：

令牌按一定跳进算法（或随机算法）生成，每个令牌只能用来登录一次，且有效期只有3分钟。

服务端密钥只在服务端保存，不下发到客户端。

获取单点登录字串成功后，调用系统浏览器打开URL，在URL中携带单点登录字串进行登录。

如果登录成功，服务端响应中包含：

**Base64(AES("登录名+服务器系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")**

### 4.4 iSeek.exe与业务服务器的接口

iSeek.exe与业务服务端的接口基于HTTP协议，字符编码为UTF-8，数据封装格式为JSON。

所有数字值，0都表示无效值。

返回字串为json字串（包含flag ，msg ,totalSize,rc对象）

其中flag msg为必备返回字段；totalSize在需要分页的地方需要返回

flag标示请求成功与否的状态（flag=0代表请求成功 flag为非0代表请求失败）

flag=0状态下 如果需要则返回rc数据对象

1：rc对象为数组 返回示例 rc:[{},{}]

2：rc对象为对象 返回示例rc:{}

## 检测软件版本

#### 接口地址

/ iseek/api/pcclient/update

#### 请求参数

|  |  |  |
| --- | --- | --- |
| **类型** | **说明** | |
| String | client\_ver | 客户端版本号 |
| 示例 | / iseek/api/pcclient/update?client\_ver =1 | |

#### 返回结果

|  |  |  |
| --- | --- | --- |
| **字段** | **类型** | **说明** |
| flag | int | 状态标志  0:成功  非0:失败 |
| msg | string | 提示信息 |
| rc | int | update\_flag: 登录令牌 //软件更新标志，u16，1：无需更新，2：非强制更新，3：强制更新 |
|  | List | update\_file：可选，如果软件有更新，这里是要更新的版本文件列表 |
| 示例 | {  “flag”: 0,  “msg”:"成功",  “rc”: {  " update\_flag ":1,  "update\_file":  [{  url:"xx" //URL  type:0 //文件类型，u16，1：安装包  }]  }  } | |
|  |  | |

## 获取资讯页内容

#### 接口地址

/ iseek/api/pcclient/getinfopage

#### 请求参数

|  |  |  |
| --- | --- | --- |
| **类型** | **说明** | |
| 无 |  |  |
| 示例 | / iseek/api/pcclient/getinfopage | |

#### 返回结果

|  |  |  |
| --- | --- | --- |
| **字段** | **类型** | **说明** |
| flag | int | 状态标志  0:成功  非0:失败 |
| msg | string | 提示信息 |
| rc | String | big\_picture\_url //大图URL |
|  | String | small\_picture\_url //小图URL |
|  | List | links: //资讯链接列表 |
| 示例 | {  “flag”: 0,  “msg”:"成功",  “rc”: {  " big\_picture\_url:"xx", //大图URL  "small\_picture\_url:"xx" ,//小图URL  links: //资讯链接列表  [{  update\_time:0L //更新时间，u64，UTC时间戳  text:"xx" //显示文字  url:"xx" //URL  }]  }  } | |
|  |  | |

## 用户登录接口

#### 接口地址

/ iseek/api/pcclient/login

#### 请求参数

|  |  |  |
| --- | --- | --- |
| **类型** | **说明** | |
| String | login\_name | 客户端版本号 |
| String | login\_str | //登录请求的密文串，生成规则为Base64(AES("32Byte随机密钥+登录名+前端系统UTC时间yyyyMMddhhmmss", KEY("变换后的密码"), "AES/CFB/NoPadding") |
| 示例 | / iseek/api/pcclient/ login? login\_name=root&login\_str=xxx.... | |

#### 返回结果

|  |  |  |
| --- | --- | --- |
| **字段** | **类型** | **说明** |
| flag | int | 状态标志  0:成功  非0:失败 |
| msg | string | 提示信息 |
| rc | String | tokenId：/登录成功响应的令牌， 该令牌在其后所有接口中都要带上 |
| 示例 | {  “flag”: 0,  “msg”:"成功",  “rc”: {  "tokenId":"xx" //登录成功响应的密文串,在后面的接口中该参数都要有  }  } | |
|  |  | |

## 获取系统消息

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/getnotice | GET |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  } | 此消息需要每10秒向服务端轮询一次 |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  type:0 //消息类型，u8，1：会员续费或充值成功提醒，2：会员到期提醒，3：公告信息  notice:"xx" //消息内容  url:"xx" //可选，链接URL  } |  |

#### 4.4.6 获取用户信息接口

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/getuserinfo | POST |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  } |  |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  login\_name:"xx" //登录名  nickname:"xx" //昵称  sex:0 //性别，u8，1：男，2：女  mobile:"xx" //手机号码  email:"xx" //邮箱  member\_expiry\_day:0L //会员到期日，u64，UTC时间戳，精确到天  } |  |

#### 4.4.7 获取关注的用户信息

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/getfriends | POST |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  } |  |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  friends: //关注的好友列表  [{  user\_id:0L //用户ID，u64  login\_name:"xx" //登录名  nickname:"xx" //昵称  }]  } |  |

#### 4.4.8 关注或取消关注用户

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/setfriend | POST |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  user\_id:0L //用户ID，u64  is\_friend:0 //是否关注，u8，1：关注，2：取消关注  } | 关注是单向的，即A关注B，B并不一定关注A |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  } |  |

#### 4.4.9 搜索文件

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/seekfile | POST |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  key\_word:"xx" //搜索的关键字  file\_type:0 //要搜索的文件类型，u8，1：音频文件，2：压缩文件，3：文件专辑  style\_type:"xx" //要搜索的文件风格类型  } |  |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  files: //搜索到的文件列表  [{  id:0L //文件ID，u64  hash:"xx" //文件MD5  type:0 //文件类型，1：MP3，2：Wav，3：压缩文件  name:"xx" //文件名  size:0L //文件大小，u64，字节数  time\_span:0 //可选，音乐时间长度，u32，秒数  Kbps:0 //可选，音乐比特率，u32  src\_count:0 //源数量，u32  }]  } |  |

#### 4.4.10 获取文件所有者

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/getfileowners | POST |
| 请求 | {  user\_id:0L //用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  file\_id:0L //文件ID，u64  } |  |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  owners: //拥有文件的用户列表  [{  user\_id:0L //用户ID，u64  login\_name:"xx" //登录名  nickname:"xx" //昵称  share\_file\_count:0 //共享的文件数量，u32  is\_friend:0 //是否已关注，u8，1：已关注，2：未关注  }]  } |  |

#### 4.4.11 获取单个用户共享的文件

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/seekfilebyuser | POST |
| 请求 | {  user\_id:0L //申请者用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  files\_owner\_user\_id: 0L //文件拥有者用户ID，u64  } |  |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  files: //搜索到的文件列表  [{  id:0L //文件ID，u64  hash:"xx" //文件MD5  type:0 //文件类型，1：MP3，2：Wav，3：压缩文件  name:"xx" //文件名  size:0L //文件大小，u64，字节数  time\_span:0 //可选，音乐时间长度，u32，秒数  Kbps:0 //可选，音乐比特率，u32  src\_count:0 //源数量，u32  sub\_dir:"xx" //文件所在目录，软件设置的共享目录之下的相对路径，两级目录间用“\”隔开，路径最后要带上“\”  }]  } |  |

#### 4.4.12 上传共享的文件列表

|  |  |  |
| --- | --- | --- |
| URL | iseek/api/pcclient/putfilesinfo | POST |
| 请求 | {  user\_id:0L //申请者用户ID，u64  auth\_str:"xx" //身份认证密文串，生成规则为Base64(AES("登录名+客户端系统UTC时间yyyyMMddhhmmss", KEY("32Byte传输密钥"), "AES/CFB/NoPadding")  files: //搜索到的文件列表  [{  hash:"xx" //文件MD5  type:0 //文件类型，1：MP3，2：Wav，3：压缩文件  name:"xx" //文件名  size:0L //文件大小，u64，字节数  time\_span:0 //可选，音乐时间长度，u32，秒数  Kbps:0 //可选，音乐比特率，u32  share\_dir:"xx" //文件所在的，软件设置的共享目录，两级目录间用“\”隔开，路径最后要带上“\”  sub\_dir:"xx" //软件设置的共享目录之下的相对路径，两级目录间用“\”隔开，路径最后要带上“\”  }]  } | hash、type、size、time\_span、Kbps都相同的文件（如果是压缩文件只需hash、type、size都相同），在服务端作为同一个文件处理。  文件要一对多关联到每个所有者用户。  hash、type、size、time\_span、Kbps、创建新文件记录时的name，作为文件数据。  name、share\_dir、sub\_dir作为文件与用户关联的数据。 |
| 响应 | {  ret\_code:0 //返回码，u16  ret\_msg:"xx" //可选，返回错误时的错误描述  } |  |

#### 4.4.13 返回码定义

1：正常

10001：内部错误

10002：参数错误

10003：网络错误

20001：验证错误

...

### 4.5. UDPClient.dll提供的调用接口

UDPClient.dll提供的调用接口，也是整个P2P体系对外提供的接口，为C格式的API。

详细定义见IUDPClient.h。

### 4.6. 数据库

## 5. 质量保证及维护说明