归档编号：

项目代号：

**金美康IM平台**

**协议设计**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号：V2.0 | | | |
| 编 制： |  | 日 期： | 2014/6/23 |
| 审 核： |  | 日 期： |  |
| 批 准： |  | 日 期： |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 发布日期： |  | 实施日期： |  |

**文件修订记录**

|  |  |  |
| --- | --- | --- |
| 日期 | 作者 | 主要修订内容 |
| 2014/6/23 |  | 拟定本过程文档初稿。 |
| 2014/7/7 |  | 3协议设计中规定数字字节序为小端 |
| 2014/7/8 |  | 3.1 鉴权请求回应增加 200 |
| 2014/7/9 |  | 3.1 注册请求增加密码字段 |
| 2014/7/10 |  | 3.1.3 增加密码规则  3.1 鉴权请求回应码改为统一码。 |
| 2014/7/10 |  | 3.1 鉴权请求回应码增加198，199 |
| 2014/7/15 |  | 3.1 返回码与3.2合并，3.2.2 返回码删除 |
| 2014/7/17 |  | 3.2 增加注销的消息类型  3.2 增加服务器推送消息终端的回应格式 |
| 2014/7/19 |  | 3.2 增加下线通知类型 |
| 2014/7/28 |  | 增加3.3， 3.4章节 |
| 2014/7/29 |  | 3.3 增加本地服务系统回应格式，并增加对应回应码120  3.3.1 组好友请求增加一个保留id字段 |
| 2014/7/31 |  | 增加3.3.2 告警消息及其它相关内容 |
| 2014/8/4 |  | 协议版本号V2.0，增加4章协议安全 |
| 2014/9/15 |  | 修改3.1鉴权请求部分注册流程及协议 |
| 2014/9/16 |  | 3.4 短信平台协议原有预留字段改为编码类型 |
| 2014/9/21 |  | 3.1.2 注册，注册信息中的验证码改为8B |
| 2014/9/29 |  | 3.1.1 登录，0x2添加数据体：ip和port  3.3.3 本地服务系统添加0x3获取token  3.3.4 转发短信告警信息给服务器 |
| 2014/9/30 |  | 3.3.4 转发短信告警信息给服务器，短信内容的编码格式为unicode |
| 2014/12/26 |  | 增加3.1.4 密码重置 |

# 1.引言

## 1.1目的

规定PTT多播平台中使用的传输协议。

## 1.2 阅读对象

本文档可供项目管理人员、系统分析人员、程序设计人员阅读和参考。

## 1.3 参考文档

## 1.4 术语与缩写解释

帐号：用户用于登录的帐户名称，唯一标识某个用户。本系统规定用于传输的帐号以ascii方式编码，需符合以下章节命名规范，最大长度15字节，需要以数值0作为结尾标记。即包含结尾0标记最长16字节。

昵称：用于在客户端软件呈现给用户的名称。

## 1.5 常量

预置KEY

｛0x37, 0x68, 0x99, 0x76, 0x13, 0x1b, 0x3c, 0xdd,0x19, 0x88, 0x7d, 0x1f,0xf3, 0xad, 0xde, 0x01｝

# 2.总体设计

## 2.1设计原则

# 3.协议设计

以下协议中出现的多字节表示数字的内容全部使用小端字节序，即传输数字0x12345678时，字节序如下：0x78, 0x56, 0x34, 0x12

返回码统一如下：

200：正常

100：token过期或错误

101：业务暂停

102：帐号错误，注册请求即用户已经注册，登录请求即该用户未注册

103：密码错误

104：昵称非法

105：参数错误，例如本地服务系统传来的组id错误等。

110：短信发送失败

120：邀请消息暂时不能接收

130：验证码错误

198：请求类型错误，例如在注册申请发出后未发注册请求而发了其它请求

199：未知错误

## 3.1鉴权请求

鉴权相关请求包含帐号注册，帐号登录两部分。统一使用以下命令格式：

鉴权请求：

MAGIC（4B）+ 0x86 + 操作类型（1B）+ SEQ（4B）+ 数据长度(4B) + 数据体

返回格式：

0x68 + 返回码(1B) + SEQ（4B） + 数据长度（4B） + 数据体

### 3.1.1登录

登录鉴权过程：

1. 客户端向服务器提交鉴权申请，申请中包含客户端帐号加扰1（流控点1）

2. 服务器向客户端返回Token

3. 客户端使用token对密码进行加扰2后发送鉴权请求

4. 服务端鉴权通过后返回200

操作类型：

0x1：鉴权申请，数据体为帐号（加扰类型1），最大16字节

返回：

200：正常，数据体为Token（8B） + Token过期时间，单位秒（2B）。

0x2：鉴权请求，数据体为token（8B） + 密码的扰文（加扰类型2）（16B）

数据采集时候的返回：

200：正常，数据体为ip（4B） + port（2B）。

### 3.1.2注册

注册过程参考《PTT平台帐号注册流程》。

0x3：注册申请，数据体为帐号（16B），用户名只允许使用字母、数字、下划线，需要使用加扰算法1进行加扰。

返回：

200：正常，数据体为Token(8B) + 图片验证码文件内容(VL，加扰算法2加密)。

0x5：手机号码验证请求，数据体为Token(8B)+手机号码（16B）+验证码（8B），除Token外的部分使用加扰算法2进行加密。验证码错误3次即过期，需要重新发起注册申请。

返回：

200：正常。数据体无。

0x4：注册请求，数据体格式如下

Token(8B) + 手机验证码（8B）+ 昵称UTF8（16B）+ 密码(16B) + 年龄及性别（1B，最高位1表示男，0表示女，后7位表示年龄）+身高（1B，单位cm）+ 体重（2B，单位1/10千克）（除Token外的部分使用加扰算法2进行加密）

手机验证码输入错误3次即过期，需要重新输入。

0x6：查询帐号是否可用

数据体为帐号（16B），用户名只允许使用字母、数字、下划线，需要使用加扰算法1进行加扰。

返回：

200：正常

### 3.1.3密码规则

密码原文可以由数字、字母、下划线和键盘可以输入的特殊符号组成，传输过程需要对原文做摘要及加扰处理。

顺序如下：

（1）通过原文计算16字节MD5摘要

（2）将摘要与1.5章预置KEY内容逐字节做XOR

### 3.1.4 密码重置

忘记密码时可发送密码重置请求进行密码重置。

0x7：密码重置申请，数据体为帐号（16B），需要使用加扰算法1进行加扰。

返回：

200：正常，数据体为Token(8B) + 图片验证码文件内容(VL，加扰算法2加密)。

0x8：手机号码验证请求，数据体为Token(8B)+手机号码（16B）+验证码（8B），除Token外的部分使用加扰算法2进行加密。验证码错误3次即过期，需要重新发起验证请求。

返回：

200：正常。数据体无。

0x9：密码重置请求，数据体格式如下

Token(8B) + 手机验证码（8B）+新密码（16B）

200：正常。数据体无。

## 3.2消息系统

登录鉴权后通信协议转为消息系统协议，消息系统请求格式如下：

MAGIC（4B）+ 0x87 + 操作类型（1B）+ SEQ（4B）+ Token(8B) + 数据长度(4B) + 数据体(VL)

返回格式：

0x78 + 返回码(1B) + SEQ（4B） + 数据长度（4B） + 数据体

服务器推送消息：

TCP长连接模式下，服务器可以向终端主动推送消息，格式如下：

MAGIC（4B）+ 0x88 +操作类型（1B）+ SEQ（4B）+ Token(8B) + 数据长度(4B) + 数据体(VL)

返回格式

MAGIC（4B）+ 0x98 + 返回码（1B） + SEQ（4B）+数据长度（4B）+数据体

### 3.2.1 操作类型列表

0x0：链路检查包，超过token有效期未收到此包，则token过期

0x1：语音多播类请求

0x2：数据采集类请求

0xfe：主动推送（0x88）的下线通知，数据体为通知文字，格式UTF-8

0xff：注销请求，数据体为空

## 3.3 本地服务系统

服务端提供一个供其它服务器程序与其通讯的接口，例如业务注册系统，告警系统等。

消息格式：

MAGIC（4B）+ 0x85 + 操作类型（1B）+ SEQ（4B）+ 数据长度(4B) + 数据体

操作类型如下，详细描述见下面章节：

0x1 组好友请求

0x2 告警消息

0x3 获取token

0x4 手机客户端向服务器发送告警信息，联网失败时，通过短信发送给服务器

回应格式

0x58 + 返回码(1B) + SEQ（4B） + 数据长度（4B） + 数据体

### 3.3.1 组好友请求

典型应用由组管理平台发起此项通知，告知本系统某组管理人员邀请某一用户加入该组。

操作类型：0x1

数据体：组id（4B）+ 管理人员id（4B）+ 目标用户id（4B）+ 保留id（4B）

（注：目前使用保留id字段存放由组管理平台创建的消息邮件id，将来可能做修改）

回应：正常返回码200， 数据体为空。失败码见本章头。

### 3.3.2 告警消息

由数据分析平台发起此项通知，告知某个群组关联的用户发起了某类告警事件。

操作类型：0x2

数据体：组id（4B）+ 告警类型(1B) + 附加数据（VL， MAX 32B）

附加数据目前定义为告警文字，最大32字节，现阶段实现可以留空。

回应：正常返回码200，数据体为空。失败码见本章头。

### 3.3.3 获取token

鉴权服务器去处理采集数据服务器获取token

操作类型：0x3

数据体：Account（16B）。

回应：正常返回码200，数据体为：token（8B）。

失败码见本章头。

### 3.3.4 转发手机客户端联网失败的发送的短信告警信息

手机客户端向服务器发送告警信息，联网失败时，通过短信发送给服务器

操作类型：0x4

数据体：PhoneNumberLen（1B）+ PhoneNumber + ContentLen（2B） + Content

Content的编码格式为：unicode

回应：正常返回码200

失败码见本章头。

## 3.4 短信平台

系统提供短信通知平台与本系统配合进行PTT离线状态下告警消息的SMS短信通知。在设计上，短信服务端为独立程序，通过socket与本系统连接，以TCP协议进行通信。

消息格式：

MAGIC（4B）+（编码类型）（1B）+(长度)（4B）+电话号码（16B）+内容（长度-16字节）

类型：0内容需要是UNICODE 2字节（UCS2）编码。

1 内容是ASCII编码

回应：

MAGIC（4B）+ 返回码（1B）

# 4. 协议安全

为保证用户数据的安全，需要在传输过程开启几个模块的信息加密

## 4.1 总述

数据的安全包含以下几项：

1. 传输过程中信息的安全

2. 用户数据在服务器存储的安全

3. 接入鉴权的安全

4. 协议算法及使用密钥的保密

总体要遵循以下原则：

1. 用户注册及登录时传递的密码信息不可明文方式传送，密码的原文不可使用可逆式加密，只能传递摘要信息。

2. 用户上传的文本和语音消息均可选用是否开启加密。

3. 服务器存储的语音数据商用前需要完成加密处理

4. 服务器存储的用户密码不允许是密码原文，只能是摘要信息。

5. 对外释放的客户端应用程序中，各种预置密钥不可以原序原文存储，需要做一定加花处理。

## 4.2 加密方法

### 4.2.1 AES算法

（1）AES算法：算法细节请参考相关资料。本系统使用128bits一个块（即16字节），对一组数据使用CBC式向量算法。

（2）密钥：AES使用128bit密钥，

（3）内容长度描述

使用AES加密时，若原文长度非16字节整倍数，需要对原文填充足16字节倍数后进行加密。前述协议中描述内容长度的参数均需要填写加密前的原文长度，但由于使用AES加密，密文信息实际需要发送16字节整数倍。例如对消息加密时，原文长度24字节，则数据包头中描述长度的部分应填写24，但实际发送时需要将原文补满32字节后进行AES加密然后传输32字节内容。接收端接收后解析到24字节长度后需要实际接收32字节内容解密，然后将解密内容中的前24字节作为数据内容，其余部分丢弃。

### 4.2.2 加扰算法1

加扰算法1用于对未获得Token时提交注册及登录请求时参数信息进行加密，此为静态加密，使用1.5章中预置KEY对16字节帐号进行AES加密，帐号不足16字节时，需要补齐，推荐在0结尾标记后面以PKCS5方式填充。

### 4.2.3 加扰算法2

加扰算法2用于获得了Token但无密码信息时，如鉴权时提交密码信息及注册时提交注册信息时对信息加密。方法如下：

使用服务器分发的Token后4字节对1.5章中预置KEY每32bits（即4字节）一组进行XOR，得到密钥后对内容进行AES加密。

### 4.2.4 消息系统内容加密

消息系统的承载内容加密使用用户密码及会话token同时生成密钥：

密钥为该用户登录密码摘要信息（见3.1章，摘要信息为密码原文MD5再与KEY做XOR操作）每32bit一组与token后4字节XOR异或运算得到。例如：

该用户密码摘要信息为：

0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77, 0x88, 0x99, 0xaa, 0xbb, 0xcc,0xdd,0xee,0xff

该用户当次登录token为0x00, 0x00, 0x00, 0x99, 0x12, 0x34, 0x56, 0x78

则密钥为

XOR((0x00, 0x11,0x22,0x33),(0x12,0x34,0x56,0x78)), XOR((0x44,0x55,0x66,0x77), (0x12,0x34,0x56,0x78)), XOR((0x88, 0x99, 0xaa, 0xbb),(0x12,0x34,0x56,0x78)), XOR((0xcc,0xdd,0xee,0xff),(0x12,0x34,0x56,0x78))

### 4.2.5 存储数据的加密

服务器存储的语音数据文件为加密存储，为提高效率，语音文件作为消息系统承载内容进行加密后放置于服务器。即：

1. 语音文件会包含传输层以下各层的数据头及语音文件数据体。

2. 解密用的密钥包含在语音消息中，随语音发送消息一同下发至终端。