# OSPN跨界群通信协议

## 群ID

地址是作为网络上身份的唯一标识。

本协议中的地址是ECDSA公钥的散列组合，ECDSA采用Prime256V1曲线。

他的定义如下

|  |  |  |  |
| --- | --- | --- | --- |
| 字段尺寸 | 描述 | 数据类型 | 说明 |
| 2byte | Version | uchar | 地址使用版本号，初始版本为0x1000。群ID的版本号为0x1010 |
| 1byte | PUBLIC flag | uchar | ECDSA公钥采用压缩模式和非压缩模式两种  04表示非压缩模式，公钥长度为64byte  03 02 表示压缩模式，公钥长度为32byte |
| 64/32byte | Publickey | uchar[] | 非压缩公钥长度为64byte，压缩公钥只保留X，长度为32byte。 |
| 32byte | Shadow hash | uchar[] | 一个地址的生成需要2对椭圆加密密钥对，后一对在地址中仅保留公钥的hash |

该地址进行base58以后加上标志头。

地址标志头：OSN

Base58编码与bitcoin的base58编码一致。

明私钥：public key对应的私钥。

暗私钥：shadow hash对应的私钥。

## 群的创建

群主创建群需要向运营商提供群ID和私钥,命令如下：

{

command:creategroup

version:初始版本为1000

owner:群主ID

groupid:群id（由群主生成）

privatekey:明私钥

groupname:可为空

timestamp:

sign:使用groupid签名

}

创建群成功的回复：

{

command:recreategroup

result:success

groupid:

version:

total:总人数

}

失败的回复：

{

command:recreategroup

groupid:

result:failed

description:

}

## 添加初始成员名单

{

command:addmembers

version:

groupid:

members:{id1,id2,id3...}

timestamp:

publickey:

sign:

}

## 邀请新成员

{

command:invite

version: 1000

from:

to:

groupid:

groupname:

timestamp:

signbyfrom：

}

现有群成员邀请新成员以后，由群ID给新成员发送一条邀请消息。

{

command:invite

version: 1000

from:

to:

groupid:

groupname:

timestamp:

signbyfrom:

signbygroup:

}

邀请成员需要知道是谁发出的邀请。

## 申请加入群

{

command:join

version:

groupid:

memberid:

timestamp:

description:

sign:

}

群主确认或者拒绝

{

command:rejoin

version:

groupid:

memberid:

timestamp:

result:拒绝或者同意

redescription:拒绝时才可能会有内容

sign:

}

## 删除群用户

该指令由群主发出

{

command:deletemembers

version:

groupid:

members:

timestamp:

publickey:

sign:

}

群收到消息以后会给成员发送一条指令

{

command:deletemembers

version:

groupid:

members:

timestamp:

signbygroup:

}

## 更新群头像

该指令由群主发出

{

command:upgroupface

version:

groupface:

timestamp:

publickey:

sign:

}

## 更新群公告

该指令由群主发出

{

command:upaffiche

version:

affiche:

timestamp:

publickey:

sign:

}

## 更新群名称

该指令由群主发出

{

command:upgroupname

version:

groupname:

timestamp:

publickey:

sign:

}

## 更新群ID

{

command:changeacc

version:

groupid:

newgroupid:

timestamp:

publickey:老id的暗公钥

privatekey:新id的明私钥

sign1:对command、groupid、newgroupid、timestamp签名，sign1需要发送给其他成员。

sign2:对command、groupid、newgroupid、timestamp、privatekey签名，sign2给群服务器验证使用

}

群收到群ID的更新信息以后，需要给所有人发送指令

{

command:changeacc

version:

groupid:

newgroupid:

timestamp:

publickey:

sign:见changeacc 中的sign1。

}

群成员收到消息以后会更新群id，使用新id更新群的所有信息。

## 获取群信息

{

command:getgroupinfo

version:

groupid:

memberid:

timestamp:

sign:

}

回复：

{

command:groupinfo

version:

groupid:

groupname:

total:群最高人数

count:当前人数

affiche:公告信息

link:连接

protocol:osn/tcp/websocket支持的协议

sign:

}

## 获取成员列表

{

command:getgroupmembers

version:

groupid:

memberid:

timestamp:

sign:

}

回复：

{

command:groupmembers

version:

count:

members:

}

member:

{

memberid:

nickname:

face:

}

## 获取成员列表（仅账号）

{

command:getgroupmemacclist

version:

count:

memberid:

timestamp:

sign:

}

## 获取成员详情

{

command:getmeminfo

version:

memberid:

desmemberid:

timestamp:

sign:

}

{

command:meminfo

memberid:

nickname:

face:

}

## 更换群运营商

更换运营商是一个很复杂的过程。

1. 在新的运营商处创建群
2. 添加群初始成员列表
3. 更新群ID

## 发送群消息

发送群消息流程：

1. 成员发送消息给群ID

{

command:message,

version:

from:

groupid:

crpyto:

content:

description:

timestamp:

hash: Hash由from、groupid、content、description、timestamp组合成的字符串进行sha256运算后得到。

sign:

}

1. 群ID解密以后，重新加密，分发给其他群成员。

{

command:message,

version:

from

groupid:

to:

crpyto:

content:

description:

timestamp:

hash: Hash由from、groupid、to、content、description、timestamp组合成的字符串进行sha256运算后得到。

sign:对hash进行签名

}

1. 成员收到以后发送回执给群id。

{

command:complete

version:

from:

to:

sign:

msghash:[“hash1”,”hash2”,”hash3”]

}

## 用户退出群

{

command:escape

version:

groupid:

memberid:

timestamp:

sign:

}

群收到退群消息以后，会转发给群主。

## 更新头像

{

command:upface

version:

groupid:

memberid:

face:

timestamp:

sign:

}

## 更新昵称

{

command:upgroupnickname

version:

groupid:

memberid:

nickname:

timestamp:

sign:

}