Server API

**1. 获取public key**

* API： http://{HOST}/{VERSION}/api/auth/getSecretKey
* Method： GET
* Desc： 获取Server RSA Public\_Key(公钥)
* 请求参数：NULL
* 返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| status | int | 状态 | Yes |
| data | Object | 数据 | Yes |
| message | String | 描述 | Yes |

* data参数解析

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| secretKey | String | 服务端公钥 | Yes |

* 返回示例

Success：

{

status: 200,

data: {

secretKey: "-----BEGIN PUBLIC KEY-----\r\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXfH0eMqhpOxaDNyWZ1yjjv15f\r\n7qm0hnllBDLwI7O1ANYSStEQaqC3JS3dbx76OI2rhukFu2+f38jY4uJWc1FA3PuB\r\n1Ko1rtDIpmz2e0Gb2Qlx/h4qUkLuNdZGn8oa+xAvP4r7LrLQXgBj6KOwRfSvRYfU\r\ny4o9otafl9Dg6WmwRwIDAQAB\r\n-----END PUBLIC KEY-----"

},

message: “Get secret key success”

}

Fail：

{

status: 400,

data: {},

message: “Get public key fail”

}

**2. 获取手机验证码**

* API： http://{HOST}/{VERSION}/api/auth/obtainSMSCode
* Method： POST
* Desc： 获取手机验证码
* 请求参数：e.g. { codeType: “register”, telephone: “13621004542”, clientPublicKey: “public key” }

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| codeType | String | 请求类别（register/others） | Yes |
| telephone | String | 电话号码 | Yes |
| clientPublicKey | String | 客户端公钥 | Yes |
| data | Object | 参数内容 | Yes |

* **备注： 限流：60s / 条， 60min / 5条， 24h / 10条**
* 返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| status | int | 状态 | Yes |
| data | Object | 数据 | Yes |
| message | String | 描述 | Yes |

* data参数解析

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| skipVerify | Boolean | 是否跳过验证 | Yes |
| verifyCode | String | 验证码 | Yes |
| expiresAt | String | 过期时间 | Yes |

* 返回示例

Success：

{

status: 200,

data: {

skipVerify: false, (value: true / false),

verifyCode: “12345”,

expiresAt: “xxxxxxxxxx”

},

message: “Send SMS verify code success, expires time is 15min”

}

Fail：

{

status: 400,

data: {},

message: “Get telephone validate code fail”

}

**3. 验证手机验证码**

* API： http://{HOST}/{VERSION}/api/auth/verifySMSCode
* Method： POST
* Desc：验证手机验证码
* 请求参数：e.g. { codeType: “login”, telephone: “13621004542”, ’code’: ‘12345’, clientPublicKey: “public key” }

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| codeType | String | 请求类别（login/others） | Yes |
| telephone | String | 电话号码 | Yes |
| code | String | 验证码 | Yes |
| clientPublicKey | String | 客户端公钥 | Yes |

* 返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| status | int | 状态 | Yes |
| data | Object | 数据 | Yes |
| message | String | 描述 | Yes |

* data参数解析

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| user | Object | 用户信息 | Yes |
| secretKey | String | AES秘钥 | Yes |

* 返回示例

Success：

{

status: 200,

data: {

user: {

"\_id": "59e07ba748104a2d60a6c0bd",

"telephone": “13631210000”,

"password": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.IjEyMzQ1NiI.ZV8PqvhDmhbB1S8pSF-PEXXJxoyoJWc\_Zs6QSH5wFKc",

"nickname": "Jamestest3",

"\_\_v": 0,

"meta": {

"updateAt": "2017-10-13T08:39:03.826Z",

"createAt": "2017-10-13T08:39:03.826Z"

},

"status": true,

"role": 0,

"deviceID": "",

"expires": "2017-10-14T09:29:32.722Z",

"token": "7y6GxZZ7Kj34b33ZABcyG4AHmMmJ4WJJ",

"signature": "This guy is lazy. He doesn't fill in anything...",

"male": false

},

secretKey: "DE\_MA\_XI\_YA!!!"

},

message: “Telephone verify success”

}

Fail：

{

status: 400,

data: {},

message: “Get telephone validate code fail”

}

**4. 用户注册(Register)**

* API： http://{HOST}/{VERSION}/api/auth/signup
* Method： POST
* Desc： 用户注册
* 请求参数：e.g. { user: { userData }, verifyCode:”12345”, clientPublicKey: “public key” }

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| telephone/email | String/String | 电话号码/邮件 | Yes |
| password | String | 密码 | Yes |
| nickname | String | 用户昵称 | Yes |
| deviceID | String | 设备ID | YES |
| countryCode | String | 国际码 | No |
| male | Boolean | 是否女生 | No |
| signature | String | 签名 | No |
| verifyCode | String | 验证码 | YES |
| clientPublicKey | String | 客户端公钥 | Yes |

* 返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| status | int | 状态 | Yes |
| data | Object | 数据 | Yes |
| message | String | 描述 | Yes |

* data参数解析

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| user | Object | 用户信息 | Yes |
| secretKey | String | AES秘钥 | Yes |

* 返回示例

Success：

{

status: 200,

data: {

user: {

"\_id": "59e07ba748104a2d60a6c0bd",

"telephone": “13631210000”,

"password": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.IjEyMzQ1NiI.ZV8PqvhDmhbB1S8pSF-PEXXJxoyoJWc\_Zs6QSH5wFKc",

"nickname": "Jamestest3",

"\_\_v": 0,

"meta": {

"updateAt": "2017-10-13T08:39:03.826Z",

"createAt": "2017-10-13T08:39:03.826Z"

},

"status": true,

"role": 0,

"deviceID": "",

"expires": "2017-10-14T09:29:32.722Z",

"token": "7y6GxZZ7Kj34b33ZABcyG4AHmMmJ4WJJ",

"signature": "This guy is lazy. He doesn't fill in anything...",

"male": false

},

secretKey: "DE\_MA\_XI\_YA!!!"

},

message: “User regist success”

}

Fail：

{

status: 400,

data: {},

message: “Sorry, Please fill in telephone”

}

**5. 用户登录(Login)**

* API： http://{HOST}/{VERSION}/api/auth/signin
* Method： POST
* Desc： 用户登录
* 请求参数：e.g. { user: { userData }, clientPublicKey: “public key” }

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| telephone | String | 用户名 | Yes |
| password | String | 密码 | Yes |
| deviceID | String | 设备ID | Yes |
| clientPublicKey | String | 客户端公钥 | Yes |
| verifyCode | String | 验证码 | No |

* 返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| status | int | 状态 | Yes |
| data | Object | 数据 | Yes |
| message | String | 描述 | Yes |

* data参数解析

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 说明 | 必含 |
| user | Object | 用户信息 | Yes |
| verifyTelephone | Boolean | 异常登录？ | Yes |
| secretKey | String | AES秘钥 | Yes |

* 返回示例

Success：

{

status: 200,

data: {

user: {

"\_id": "59e07ba748104a2d60a6c0bd",

"telephone": "13631210000",

"password": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.IjEyMzQ1NiI.ZV8PqvhDmhbB1S8pSF-PEXXJxoyoJWc\_Zs6QSH5wFKc",

"nickname": "Jamestest3",

"\_\_v": 0,

"meta": {

"updateAt": "2017-10-13T08:39:03.826Z",

"createAt": "2017-10-13T08:39:03.826Z"

},

"status": true,

"role": 0,

"deviceID": "",

"expires": "2017-10-14T09:29:32.722Z",

"token": "7y6GxZZ7Kj34b33ZABcyG4AHmMmJ4WJJ",

"signature": "This guy is lazy. He doesn't fill in anything...",

"male": false

},

verifyTelephone: false, (value: true / false)

secretKey: "DE\_MA\_XI\_YA!!!"

},

message: “Login success, welcome”

}

Fail：

{

status: 400,

data: {},

message: "Sorry, Your password is invalid"

}

Constants

1. HOST：”127.0.0.1”
2. VERSION：”v1”
3. Aes secret:
4. Aes secret: 'DE\_MA\_XI\_YA!!!'