移动安全认证系统
用户管理

接口规范 v1.0.0

目 录

1 文档说明 - 3 -
1.1 编制说明 - 3 -
1.2 参考资料 - 3 -
1.3 适用范围 - 3 -
2 接口列表 - 3 -
3 接口安全性 - 3 -
4 接口定义 - 4 -
4.1 用户管理接口 - 4 -
4.1.1 用户信息注册 - 4 -
4.1.2 用户信息更新 - 5 -
4.1.3 更新用户状态 - 7 -
5 示例代码 - 8 -
5.1 参数签名示例 - 8 -
6 错误码定义 - 9 -

1 文档说明

1.1 编制说明

移动安全认证系统以下简称为Mkey。

本文档描述MKey产品服务端用户信息管理同步的应用端接入规范。

1.2 参考资料

无。

1.3 适用范围

本规范适用于MKey产品服务端对外提供应用系统管理用户的接入规范，描述应用与MKey产品服务端的交互接口说明。

2 接口列表

提供者	接口说明	接口名称	备注
用户管理	用户信息注册	/user/register	注册用户
	用户信息更新	/user/update	用户信息更新
	更新用户状态	/user/status	更新用户状态

3 接口安全性

1、采用SSL来对传输通道进行加密保护，防止数据泄漏和恶意篡改；

2、采用接入应用私钥签名来对接入应用进行鉴权；

3、请求参数值在发送时均使用URLEncoder编码。

4 接口定义

4.1 用户管理接口

4.1.1 用户信息注册

4.1.1.1功能说明

应用调用此接口将用户信息注册到系统。

4.1.1.2接口说明

接口协议：HTTP协议

请求方式：POST

接口服务地址：https://ip:port/openapi/v1/user/register

4.1.1.3请求消息

消息流向：应用－>服务端

参数说明：

参数名称	字段类型	说明	必填
appId	String	分配的应用标识	是
id	String	用于标识用户在应用中的身份ID	是
userName	String	用户名称	是
idNoType	Integer	用户证件类型，取值{1|2|3|4|5} 1：身份证号码 2：港澳台身份证 3：国内/国外护照 4：军官证 5：回乡证	是
idNo	String	用户证件号	是
telephone	String	手机号码	是
email	String	电子邮箱	否
sign	String	使用应用私钥对参数“appId=xxx&id=xxx”进行签名，得到签名值Base64Encode后进行URLEncode(UTF-8)传输。应用私钥由平台分	是

		配，签名示例代码参考参数签名示例	

请求示例（键值对）：

appId=1&id=13800138000&userName=张三&idNoType=1&idNo=110101199003070791&telephone=13800138000&sign=Sxie7dRg/8VXLPvPJpNDDY9vpkdwe+V7F4SKqh1UhP/XiTCUtjJ4PZnXCB0RXil8JD94ncvUHO0VHwsxxDgvwNKwwyU8dWP1fyS887zvix91gEmnQgGJKVGLLGzzDbXmBjV58KrgVP0fGuv/t7YqU77TF1iFtlvkUnv9YR93hR4=

4.1.1.4响应消息

消息流向：服务端一>应用

返回JSON示例：

```
{
    "ret":"success",
    "msg":"success",
}
```

返回值说明：

字段	类型	说明
ret	String	结果码
msg	String	结果描述

4.1.2 用户信息更新

4.1.2.1功能说明

应用调用此接口变更用户信息。

4.1.2.2接口说明

接口协议：HTTP协议

请求方式：POST

接口服务地址：https://ip:port/openapi/v1/user/update

4.1.2.3请求消息

消息流向：应用一>服务端

参数说明：

参数名称	字段类型	说明	必填
appId	String	分配的应用标识	是
id	String	用于标识用户在应用中的身份ID	是
userName	String	用户名称	是
idNoType	Integer	用户证件类型，取值{1|2|3|4|5} 1：身份证号码 2：港澳台身份证 3：国内/国外护照 4：军官证 5：回乡证	是
idNo	String	用户证件号	是
telephone	String	手机号码	是
email	String	电子邮箱	否
sign	String	使用应用私钥对参数“appId=xxx&id=xxx”进行签名，得到签名值Base64Encode后进行URLEncode(UTF-8)传输。应用私钥由平台分配，签名示例代码参考参数签名示例	是

请求示例（键值对）：

appId=1&id=13800138000&userName=张三&idNoType=1&idNo=110101199003070791&telephone=13800138000&sign=Sxie7dRg/8VXLPvPJpNDDY9vpkdwe+V7F4SKqh1UhP/XiTCUtjJ4PZnXCB0RXil8JD94ncvUHO0VHwsxxDgvwNKwwyU8dWP1fyS887zvix91gEmnQgGJKVGLLGzzDbXmBjV58KrgVP0fGuv/t7YqU77TF1iFtlvkUnv9YR93hR4=

4.1.2.4响应消息

消息流向：服务端一>应用

返回JSON示例：

```
{
    "ret":"success",
```

```
    "msg":"success"
}
```

返回值说明：

字段	类型	说明
ret	String	结果码
msg	String	结果描述

4.1.3 更新用户状态

4.1.3.1功能说明

应用调用此接口变更用户状态。

4.1.3.2接口说明

接口协议：HTTP协议

请求方式：POST

接口服务地址：https://ip:port/openapi/v1/user/status

4.1.3.3请求消息

消息流向：应用一>服务端

参数说明：

参数名称	字段类型	说明	必填
appId	String	Mkey分配的应用标识	是
id	String	用于标识用户在应用中的身份ID	是
status	String	用户状态，1：启用，2：停用，3：注销	是
sign	String	使用应用私钥对参数“appId=xxx&id=xxx”进行签名，得到签名值Base64Encode后进行URLEncode(UTF-8)传输。应用私钥由平台分配，签名示例代码参考参数签名示例	否

请求示例（键值对）：

```
appId=1&id=13800138000&status=1&sign=Sxie7dRg/8VXLPvPJpNDDY9vpkdwe+V
```

7F4SKqh1UhP/XiTCUtjJ4PZnXCB0RXil8JD94ncvUHO0VHwsxxDgvwNKwwyU8dWP1fyS
887zvix91gEmnQgGJKVGLLGzzDbXmBjV58KrgVP0fGuv/t7YqU77TF1iFtlvkUnv9YR9
3hR4=

4.1.3.4响应消息

消息流向：服务端一>应用

返回JSON示例：

```
{
    "ret":"success",
    "msg":"success"
}
```

返回值说明：

字段	类型	说明
ret	String	结果码
msg	String	结果描述

5 示例代码

5.1 参数签名示例

- JAVA 版

```
/**
 * 使用私钥进行签名
 * @param privateKey 私钥
 * @param bData 参数数据
 * @return  BASE64 编码格式签名值
 */
private static String signature(String privateKey, byte[] bData) {
        String result = null;
        try {
            PKCS8EncodedKeySpec keySpec = new PKCS8EncodedKeySpec(
                    Base64.decode(privateKey));
            KeyFactory keyFactory = KeyFactory.getInstance("RSA");
            PrivateKey priKey = keyFactory.generatePrivate(keySpec);
```

```
            Signature oSig = Signature.getInstance("SHA256WithRSA");
            oSig.initSign(priKey);
            oSig.update(bData);
            byte[] signature = oSig.sign();
            if (signature != null && signature.length > 0) {
                result = new String (Base64.encode(signature));
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
        return result;
    }
```

- C# .NET 版

```
var rsa = new RSACryptoServiceProvider();
// privateKey 为应用私钥
rsa.FromXmlString(privateKey);
// data 为参数数据
byte[] signBytes =
    rsa.SignData(Encoding.UTF8.GetBytes(data), CryptoConfig.CreateFromName("SHA256"));
// BASE64 编码格式签名值
result = Convert.ToBase64String(signBytes);
```

6 错误码定义

接口错误码

名称	错误描述	解决方案
MKEY.authentication_fail	鉴权失败	请给接入应用授权
MKEY.invalid_transaction_id	业务流水号不正确	传入正确的业务流水号
MKEY.no_valid_arrangement	无有效合约	完成产品签约
MKEY.parameter_invalid	参数错误	修改接口参数
MKEY.system_error	系统错误	重试或反馈MKEY服务器技术支持
MKEY.transaction_id_expired	业务流水号已过期	请传入正确的业务流水号
MKEY.qrcode_error	二维码已失效	请重新生成二维码
MKEY.user_not_regist	用户未注册	请注册用户信息
MKEY.user_not_auth	用户未实名	请在后台配置用户实名信息

MKEY.invalid_user_status	用户状态被停用或注销	请在后台启用用户状态
MKEY.user_not_login	用户暂未登录	请用户登录MKey APP
MKEY.push_error	消息推送失败	请尝试再次推送
MKEY.push_sign_error	推送签名失败	请尝试再次推送
MKEY.user_cert_error	用户没有有效的证书	请用户申请数字证书
MKEY.batch_sign_config_error	用户未设置免密签名	请用户登陆MKey APP选择免密设置
MKEY.batch_sign_error	批量签名失败	密钥运算失败
MKEY.batch_sign_excess_size	批量签名条目超过限制	请减少每次请求的批量数据条目
MKEY.seal_error	处理签章业务失败	请确认签章服务器的运行状态

系统错误码

名称	错误描述	解决方案
MKEY.app_invoke_excess_limitation	应用调用服务次数超限	请降低应用调用的qps
MKEY.invoke_isp_error	调用服务接口错误	MKEY服务器内部服务出现错误，请稍后再试
MKEY.sign_system_param_error	平台私钥加签返回结果错误	MKEY服务器私钥配置错误
MKEY.verify_sign_app_public_key_error	应用公钥验签错误	请使用应用私钥加签
MKEY.encode_public_key_error	应用公钥加密错误	请使用应用公钥加密
MKEY.missing_param	缺少参数	缺少参数
MKEY.invalid_param	无效参数	无效参数
MKEY.invalid_app_status	应用生命周期状态错误	应用的状态必须是上线
MKEY.invalid_appruntime_state	应用运行状态错误	应用的运行状态必须是正常
MKEY.unknow_error	未知错误	重试
MKEY.user_seal_error	用户没有设置手写签名	用户设置手写签名
MKEY.user_have_error	用户ID已存在	设置其他的用户ID
Mkey.user_revoke_error	用户已注销	无法变更已注销用户状态