

H5 本机号码校验 jssdk 集成使用文档

(微信小程序) V1.2-RSA

注：V1.2 取号接口支持 HTTPS

1	产品介绍	2
1.1	产品说明	2
1.2	业务流程说明	2
1.3	H5 认证交互说明	3
2	重要参数说明	5
2.1	WXAPPID (微信小程序 APPID)	5
2.2	公私钥说明	5
2.3	加密包使用说明	5
3	JSSDK 集成说明	6
3.1	引入 JS 文件	6
3.2	使用方法：	6
4	本机号码校验接口	9
5	常见问题	9

1 产品介绍

1.1 产品说明

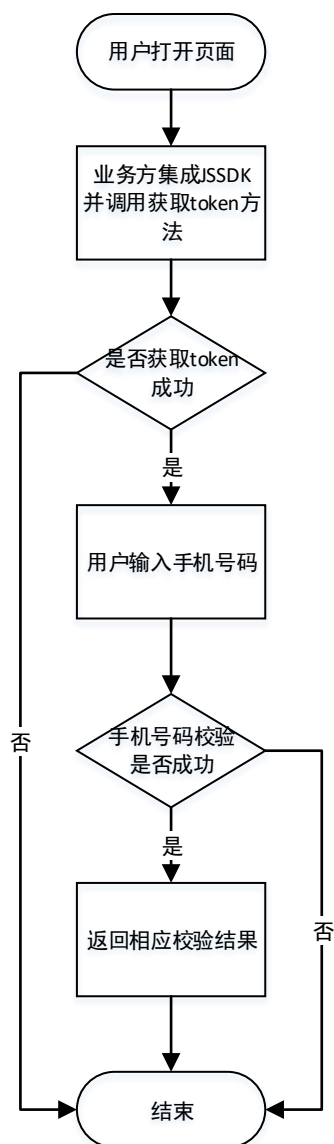
H5 本机校验微信小程序产品是中国移动推出的基于微信小程序提供的用户身份快捷校验产品。进入移动互联网时代，手机号码就是移动互联网的“身份证”，互联网用户通过手机号码将真实信息与互联网资产绑定在一起，互联网企业通过对手机号码的校验实现用户身份认证，进而对银行账号、会员资产、游戏资产等进行管理。

传统的互联网企业通过短信验证码的方式完成用户身份校验，但是短信验证流程存在等待时间长、超时失效、木马劫持、陌生端口号骗取验证码等问题，安全性与便捷程度都已经无法满足当今移动互联网要求。对此，移动认证本机号码校验产品提出了更佳解决方案，利用应用层无法截取的网络层号码认证能力来验证号码的真实性，免去了传统短信验证环节，后台操作，用户无感知，高效省心，有效促活。

H5 本机号码校验微信小程序产品是通过移动认证平台提供的网页自动取号能力，在用户数据网络下打开手机网页时，直接获取用户手机号码，并与用户输入的手机号码进行对比校验，快捷高效，降低用户流失率。

1.2 业务流程说明

业务流程图：



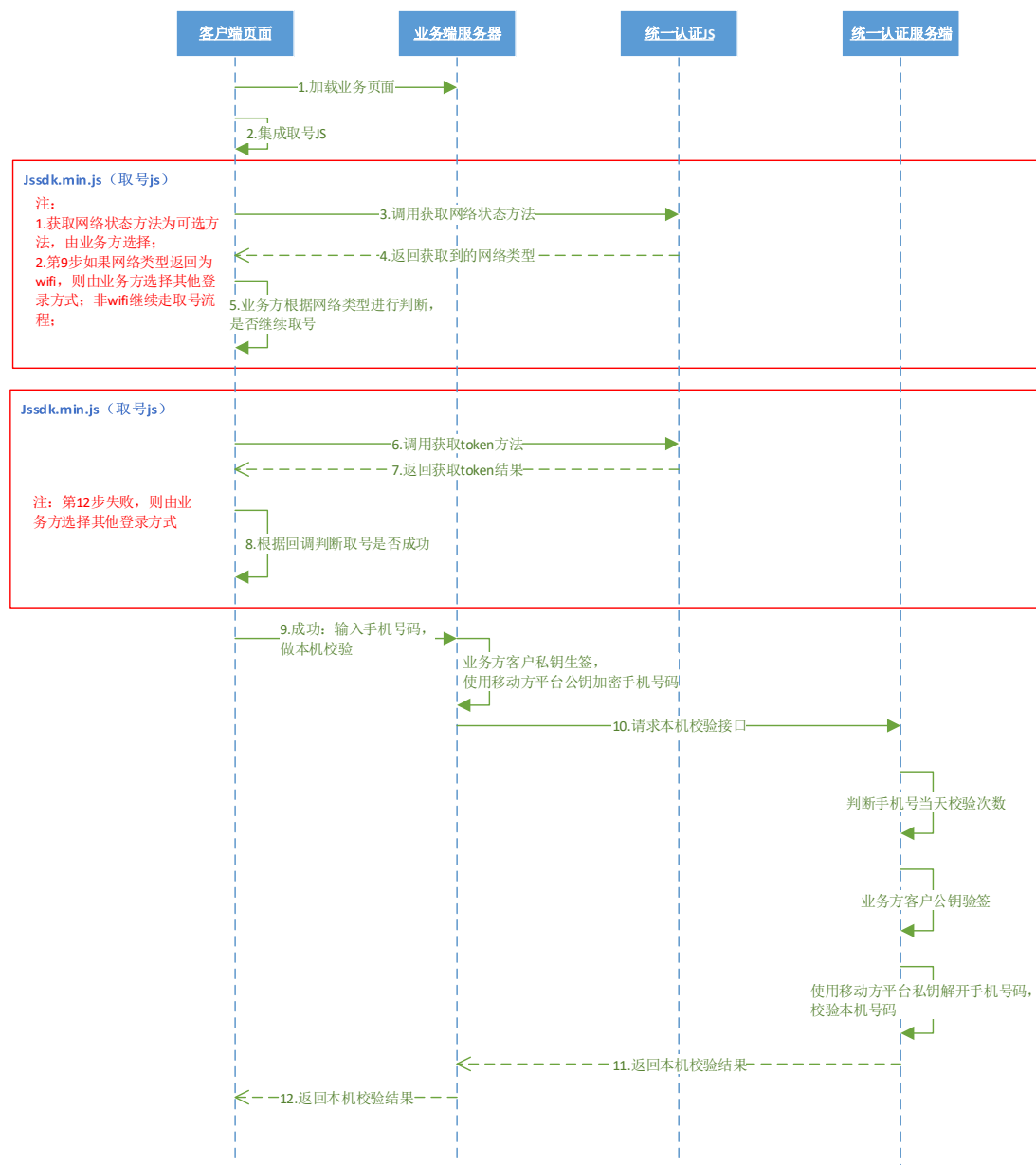
用户打开页面，业务方集成取号 JS 并调用 getToken 方法：如果取号成功，则返回 token 给业务方，如果取号失败则返回相应错误；

如果取号成功，业务方携带用户输入的手机号码及 token 进行本机号码校验，校验成功则返回本机号码校验结果，校验失败则流程结束。

1.3 H5 认证交互说明

基于 H5 本机号码校验的能力，提供 H5 本机号码校验微信小程序产品。。

业务方只需要集成相关 js，调用本机号码校验接口，即可完成接入



流程说明：

1 步用户打开客户端页面。

2 步页面集成取号 js。

3-5 步通过 js 获取网络状态方法，判断用户使用网络情况。（此步骤为可选方法，详见

3.2.1 获取网络类型（可选）

6-8 步通过 js 请求获取 token。

成功校验 token

- 9 步页面请求调用 token 校验接口。
- 10 步业务侧调用本机校验接口。
- 11 步返回本机校验结果到业务侧服务端。
- 12 步业务服务端返回本机校验结果到页面。

2 重要参数说明

2.1 wxappid (微信小程序 appid)

指业务方申请微信小程序时生成的 appid，示例：wx10a00cf000000000

2.2 公私钥说明

开发过程中涉及两对公私钥：一对为客户生成的公私钥，用于生签验签；一对为认证平台生成的公私钥，用于在调用校验 token 接口时 phoneNum 字段的加解密。

注意：请开发人员务必使用接入指南中的「RSA」工具类生成客户密钥对，填写公钥并妥善保存好私钥，使用方法见[错误!未找到引用源。](#)。平台公钥在开放平台上，业务方填写配置信息时会自动生成。

2.3 加密包使用说明

生成公私钥密钥对使用 RsaUtils 中的 genKeyPair 方法。代码示例如下：

```
Map<String,Object> keyMap = genKeyPair();

System.out.println("publicKey:"+getPublicKey(keyMap));

System.out.println("privateKey:"+getPrivateKey(keyMap));
```

利用私钥生成签名使用 RsaUtils 中的 sign 方法。

利用公钥验证签名使用 RsaUtils 中的 verify 方法。

利用公钥使用 RsaUtils 中的 encryptedDataOnJava 方法进行字符串加密。

3 JSSDK 集成说明

接入方向

调用方	提供方
客户端 H5 页面	移动认证平台

jssdk 建议在线引用

3.1 引入 js 文件

[https://www.cmpassport.com/NumberAbility/jssdkVIm_MiniProg/jssdk_v1.](https://www.cmpassport.com/NumberAbility/jssdkVIm_MiniProg/jssdk_v1.0.0.min.js)

[0.0.min.js](#)

3.2 使用方法：

3.2.1 获取网络类型（可选）

创建变量接收获取网络信息回调方法

```
var connection = YDRZ.getConnection({
  appId:that.data.appId, //应用 Id
  success:function(res){
    that.setData({ connectionType: res });
    // that.connectionType = res;
    // console.log(that.connectionType.netType)
  }
});
```

```

},
error:function(res){
    that.setData({ connectionType: res });
}
});

```

注：此方法为异步请求，获取网络类型之后的逻辑请卸载 success 回调和 error 回调中

3.2.2 引入 js 文件

示例：

```
import YDRZ from '../utils/jssdk.js' //引入 js 文件
```

3.2.3 获取 token

```
YDRZ.getTokenInfo({
    data: //请求的参数
    version: '1.0' , //接口版本号 （必填）
    sign: '' , //加密后的 sign （必填）。sign 生成规则： MD5(appld + businessType + msgld +
timestamp + traceld + version+appkey) 注： msgld 要和 traceld 保持一致； businessType 在微信
小程序中取值为 5，“+” 号为合并意思，不包含在被加密的字符串中。
```

```
    traceld: '' , //业务方生成唯一标识
```

```
    timestamp: '' , //请求消息发送的系统时间，精确到毫秒，共 17 位，格式：20121227180001165
```

```
    appld: '' , //应用 Id （必填）
```

```
    openType: '1', //取号类型
```

```
    expandParams: '' , //扩展参数 格式：参数名=值 （选填）
```

```
    isTest: '1' //是否启用测试线地址（传 0 时为启用不为 0 或者不传时为不启用）
```

```
},
```

```
success: function (res) { //成功回调},
```

```
error: function (res) { //错误回调}
```

});

Success 回调参数的状态码：

```
{ code: "103000", message: "token 获取成功",token:"",userInformation: '浏览器指  
纹' }
```

error 回调参数的状态码：

返回码	描述语
130010	参数为空
105112	时间戳非法
103101	错误的请求签名
110024	businessType 配置错误
110025	businessType 错误
110023	应用没有权益
110025	权益已失效
103111	WAP 网关 IP 错误
111002	黑名单号码用户
103609	物联网 IP 不允许取号
105002	移动网关取号失败
103211	其他错误

4 本机号码校验接口

请开发者查看《H5 本机号码校验微信小程序服务端接口文档 V1.2-RSA》。

5 常见问题

1、取号不成功时，怎么办？

取号不成功，会返回空 token，业务侧可根据业务实际需要自行使用其他登录方式。

2、是否支持 wifi 环境下取号？

取号走数据网络，不支持 wifi 环境下取号，所以只要用户开启了 wifi 就无法取号。