

H5 本机号码校验服务端接口文档

(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	本机号码校验接口	6
3.1	接口描述	6
3.2	消息定义	6
4	常见问题	11

1 产品介绍

1.1 产品说明

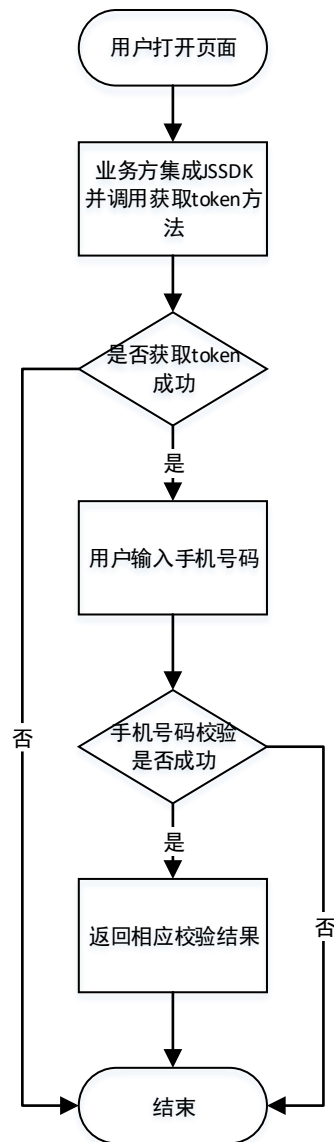
H5 本机校验微信小程序产品是中国移动推出的基于微信小程序提供的用户身份快捷校验产品。进入移动互联网时代，手机号码就是移动互联网的“身份证”，互联网用户通过手机号码将真实信息与互联网资产绑定在一起，互联网企业通过对手机号码的校验实现用户身份认证，进而对银行账号、会员资产、游戏资产等进行管理。

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：



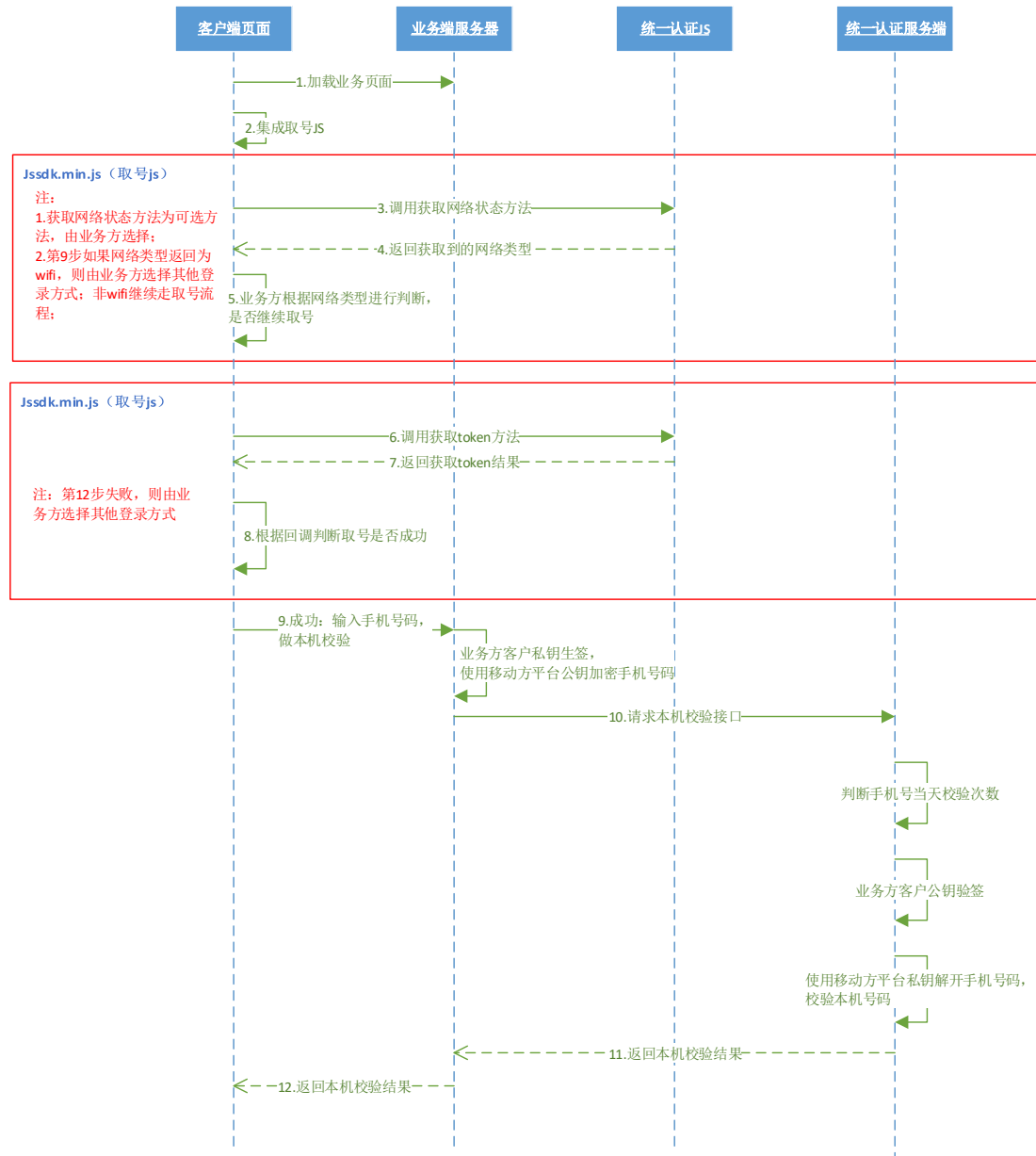
用户打开页面，业务方集成取号 JS 并调用 getToken 方法：如果取号成功，则返回 token 给业务方，如果取号失败则返回相应错误；

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 [jssdk 文档](#)）

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，填写公钥并妥善保管好私钥，使用方法见 2.3 加密包使用说明。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

生成公私钥秘钥对使用 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 本机号码校验接口

3.1接口描述

业务平台发起本机号码校验请求

接口名称：verifyVmMobileApi.htm

接口方向

接口调用方	接口提供方
业务方服务端	本机 token 校验

通信协议

协议: HTTPS+ application/json

方法: POST

环境说明：

现网联调地址：

<https://www.cmpassport.com/NumberAbility/h5/verifyVmMobileApi.htm>

3.2消息定义

3.2.1 请求消息

参数名称	约束	层级	参数类型	说明
header	必选	1		
version	必选	2	string	版本号,初始版本号 1.0,有升级后续

				调整
msgId	必选	2	string	使用 traceId 标识请求的唯一性 (32 位)
timestamp	必选	2	string	请求消息发送的系统时间，精确到毫秒，共 17 位，格式： 20121227180001165
appId	必选	2	string	应用 ID
body	必选	1		参见请求 body

3.2.2 请求 body

参数	说明	类型	是否必填
expandParams	扩展参数格式： param1=value1 param2=value2 方式传递，参数以竖线 间隔方式传递，此参数需 urlencode 编码。	String	否
phoneNum	待校验的手机号码，使用移动方提供的平台公钥加密（手机号码+appKey+timestamp） (注：“+”号为合并意思) 值。 例如： (13999994444AA03E6C60D	String	是

	0B0D14320B9A3F0B5AAD99 20121227180001165)		
token	身份标识，字符串形式的token	String	是
sign	签名，业务方RSA客户私钥生成签名 (appld+msgId+phoneNum+timestamp+token+version) (注：“+”号为合并意思，不包含在被加密的字符串中，参数名做自然排序（Java是用TreeMap进行的自然排序）)	String	是
userInformation	加密的浏览器指纹，由前端js采集	String	是

请求示例

```
{
  "header":{
    "version ":"1.0",
    "msgId ":"ee05d1635db847a2bf3c8317434539d6",
    "timestamp ":"20200628180001165",
    "appld ":"300012014310"
  },
  "body":{
    "expandParams":"","
    "phoneNum ":"I503NHqFiYHL2Y3xzH+PXBxyw2Rooqs5Gkyo3ZgdtTPtb1eIN7+dq3mTaavEUx64MyTJjEaQei0n4z6t+3Wa7zyGhGApN10BlpHWCwWphEIR2T8Vhi4+At5gyOlBqh03+wHg2GYOLDgsSnCp/B6IPL+dh/GI7KnI6oElzvbgsco=",
```

```

    "token":"VMHTTPS12c9519d861454f17c4f1439448c9295",
    "sign":"Vxb/fKx1CkTkErpXuYnUdouQCqV0UQ++N7JjPAVe/EDP3ZkBDpCK7CFg5nJrhJ
W7OKfS7inJ7rXmZ5IIVlfJTdVEIAOZuXc94p6DSAagskjY4mBgpw+7wJ8/bteP2FT5IRrCKo2J
80kK5aWOc8nmBeFOAojD//mWyMx4piRulo=",
    "userInfo":"V2luMzJAQE1vemlsbGEvNS4wIChXaW5kb3dzIE5UIDEwLjA7IFdPVz
Y0KSBBcHBsZVdlYktpdC81MzcuMzYgKETIVE1MLCBsaWtIIEdlY2tvKSBDaHJvbWUvODYuMC
40MjQwLjExMSBTYWZhcmlkNTM3LjM2QEBmMzFkOWU3MDc4OTIiN2U3YzE4Y2Y3ZWZiY
WUxOWVINA%3D%3D"
  }
}
```

3.2.2.1 响应消息

参数名称	约束	层级	参 数 类 型	说明
header	必选	1		
msgId	必选	2	string	对应的请求消息中的 msgid
timestamp	必选	2	string	响应消息发送的系统时间，精确到毫秒，共 17 位，格式：20121227180001165
appId	必选	2	string	应用 ID
resultCode	必选	2	string	规则参见 resultDesc 中的说明
body	必选	1		参见消息体 body

3.2.2.1.1 消息体 Body

参数名称	参数说明	是否 必填	数据类型	说明
taskId	流水号	是	String	服务端流水号

resultDesc	返回结果描述信息 000:是本机号码 001:非本机号码 130032:解析参数错误 130010:参数为空 121016:电信取号功能已关闭 121018:余量不可用 121017:联通取号功能已关闭 110027:能力不可用 103605:加密方式或密钥值为空 130016:解码失败 130018:验证签名失败 110022:应用ID不存在 110004:IP不在白名单 120020:token校验失败 121011:号码校验次数超限 121010:fromAppId校验失败 121002:无法验证 111075:使用次数为0 120009:token重复校验或已失效 170001:无效的请求 999999:系统异常	是	String	
------------	---	---	--------	--

	其中，000和001状态纳入计费次数			
expandParams	扩展参数格式： param1=value1 param2=value2 方式传递，参数以竖线 间隔方式传递，此参数需 urlencode 编码。	否	String	

响应示例

```
{
  "header":{
    "msgId ":"ee05d1635db847a2bf3c8317434539d6",
    "timestamp ":"20200828180001165",
    "appId ":"300012014310",
    "resultCode ":"000"
  },
  "body":{
    "taskId ":"64750145c2234bb5ac576418f2d16328",
    "resultDesc ":"是本机号码",
    "expandParams ":""
  }
}
```

4 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。

附录：常见返回码排查

返回码	排查方法
170001	小程序版本不校验集成页面和请求来源，请检查开放平台“接入场景类型”配置项是否正确选择。
111002	网关未插入手机号。常见原因是业务方使用了联通或电信的数据网络或者使用 wifi。
110027	能力不可用，常见原因是合同未绑定、合同余额不足和开放平台新申请的配置未生效。
130016	解码失败。常见原因是客户公私钥的生成未使用指定工具类方法，报备的客户公钥与客户私钥不配对、生签未使用指定工具类方法、phoneNum 加密出错等，请查看文档中关于加密包的说明。
130018	验证签名失败。常见原因是客户公私钥的生成未使用指定工具类方法，报备的客户公钥与客户私钥不配对、生签未使用指定工具类方法、phoneNum 加密出错等，请查看文档中关于加密包的说明。
130032	解析参数错误。原因一般是报文格式错误，不是标准的 json 格式。
103605	加密方式或密钥值为空。原因一般是现网联调的业务方错误访问了测试环境的地址或开放平台配置未生效。
110004	ip 不在白名单。常见原因是开放平台上报备的出口 ip 地址与实际的服务器 ip 地址不符。
110025	权益已失效。请检查能力配置页面中的下线时间是否过期。
111034	本机微信小程序信息错误。常见原因是 PC 端测试带入了 referer，建议在真机调试。
120020	token 校验失败。常见原因是超过 token 一分钟有效期、userinformation 缺失或编码出错以及 token 重复校验。
121011	号码校验次数超限。同一个手机号码一天校验的上限默认是 10 次，如有调整上限的需求，可报自行在开放平台配置项修改。
999999	系统异常。常见原因是网络波动或校验 token 时 phoneNum 加密出错。
130010	参数为空。原因可能是现网联调的业务方错误访问了测试线环境，导致调用获取 token 方法无法返回 token 和 userinformation。