

H5 本机号码校验快应用服务端接口文档

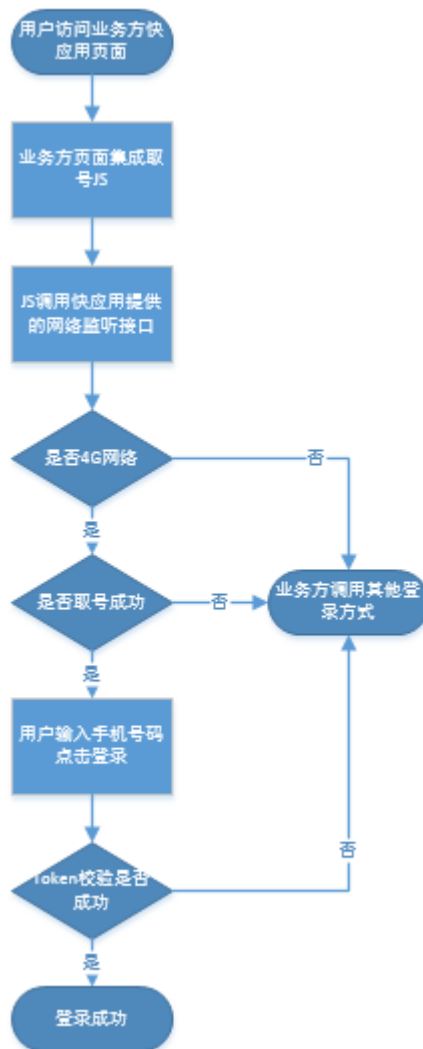
目 录

- 1 业务及交互流程2
 - 1.1 业务流程说明2
 - 1.2 认证交互说明3
- 2 重要参数说明.....4
 - 2.1 PACKAGE_NAME（包名）4
 - 2.2 公私钥说明4
 - 2.3 加密包使用说明5
- 3 本机号码校验接口5
 - 3.1 接口描述5
 - 3.2 消息定义6
 - 3.2.1 请求消息.....6
 - 3.2.2 响应消息.....9
- 4 常见问题.....11
- 附录：常见返回码排查.....13

1 业务及交互流程

1.1 业务流程说明

H5 本机号码校验快应用业务流程图

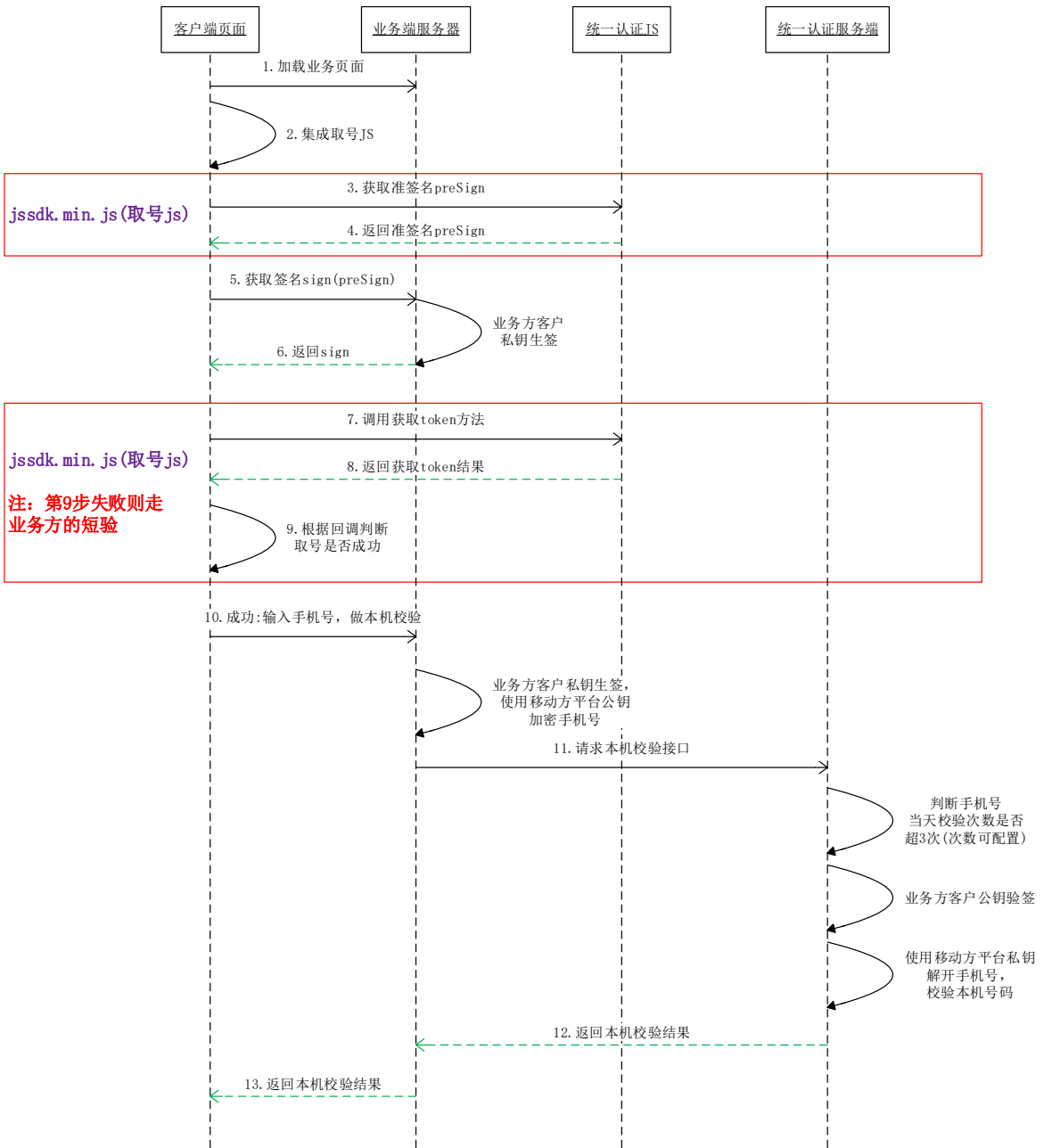


用户打开网页页面，业务侧调用取号 JS，JS 调用快应用提供的网络监听接口，如果是 4G 网络则进行取号，取号成功，JS 调用获取 token 接口，然后调用相关接口进行 token 和本机号码校验；取号失败，业务方可以调用其他登录方式。

1.2 认证交互说明

基于本机号码校验的能力，提供本机号码校验快应用产品。

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。

3-4 步通过 js 获取准签名，传入字段 appId 和 version，拼接字段：

appId+msgId+timestamp+uuid+version。

5-6 步将准签名发到业务服务端，做 RSA 客户私钥生签。

7-9 步通过 js 请求获取 token。

成功校验 token

10 步页面请求调用 token 校验接口。

11 步业务侧调用本机校验接口。

12 步返回本机校验结果到业务侧服务端。

13 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 packageName（包名）

指业务方在快应用平台报备的包名，示例如下：com.aaaa.bbbbbb

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[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:

测试联调地址:

<http://120.197.235.102/NumberAbility/h5/verifyVmMobileApi.htm>

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 UUID 标识请求的唯一性
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
appld	必选	2	string	应用 ID
body	必选	1		参见请求 body

3.2.1.1 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
phoneNumber	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： (13999994444AA03E6C60D0B0D14320B9A3F0B5AAD9920121227180001165) 生成后： 4526285940B6FA7FEF49E1DCB04EE944F41A8745444015DAF2771BFB7AD7C800	String	是
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+msgld+phonNum+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
userInfo	加密的浏览器指纹，由前端js采集	String	是

请求示例

```
{
  "header":{
    "version ":"1.0",
    "msgld ":"61237890345",
    "timestamp ":"20160628180001165",
    "appld ":"0008"
  },
  "body":{
    "expandParams": "",
    "phoneNum ":"4526285940B6FA7FEF49E1DC800",

```

```

"token": "VM_12c9519d861454f17c4f1439448c9295",

"sign": "490355e164168287bc5eb1f4840914c0",

"userInformation": "CB04EE944F41A8745444015DAF2771BFB7AD7"

}

}

```

3.2.2 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 消息体 Body

参数名称	参数说明	是否	数据类型	说明
		否		

		必填		
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 130010: 参数为空 130018: 验证签名失败 130032: 解析参数错误 120020: token校验失败 110022: 应用ID不存在 110023: 应用没有权益 110025: 权益已失效 110004: IP不在白名单111075: 使用次数为0 121011: 号码校验次数超限 999999: 系统异常 其中, 000和001状态纳入计费次数	是	String	

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 ":"61237890345",  
    "timestamp ":"20180828180001165",  
    "appld ":"0008",  
    "resultCode ":"000"  
  },  
  "body":{  
    "taskId ":"ffsfdfsfs3243dsfdf3432xxx",  
    "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短信验证码方式验证用户身份。

2、H5 本机号码校验快应用版本是否支持异网号码？

暂时不支持电信、联通。

3、是否支持 wifi 环境下取号？

取号走数据网络，因 jssdk 不支持 wifi 切 4G 的操作，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
500	取号环节失败统一封装的返回码。 生产环境（真实取号）中，业务方可以自己抓包获取具体的返回码，再根据下列对应的返回码排查。 测试环境（非真实取号）中，请对照集成说明文档检查 <code>expandparams</code> 扩展参数中是否传了 <code>phoneNum=手机号</code> 。
170001	快应用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、 <code>phoneNum</code> 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、 <code>phoneNum</code> 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 <code>referer</code> ，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、 <code>userinformation</code> 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 <code>phoneNum</code> 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 <code>userinformation</code> 。