H5 本机号码校验服务端接口文档（三网）

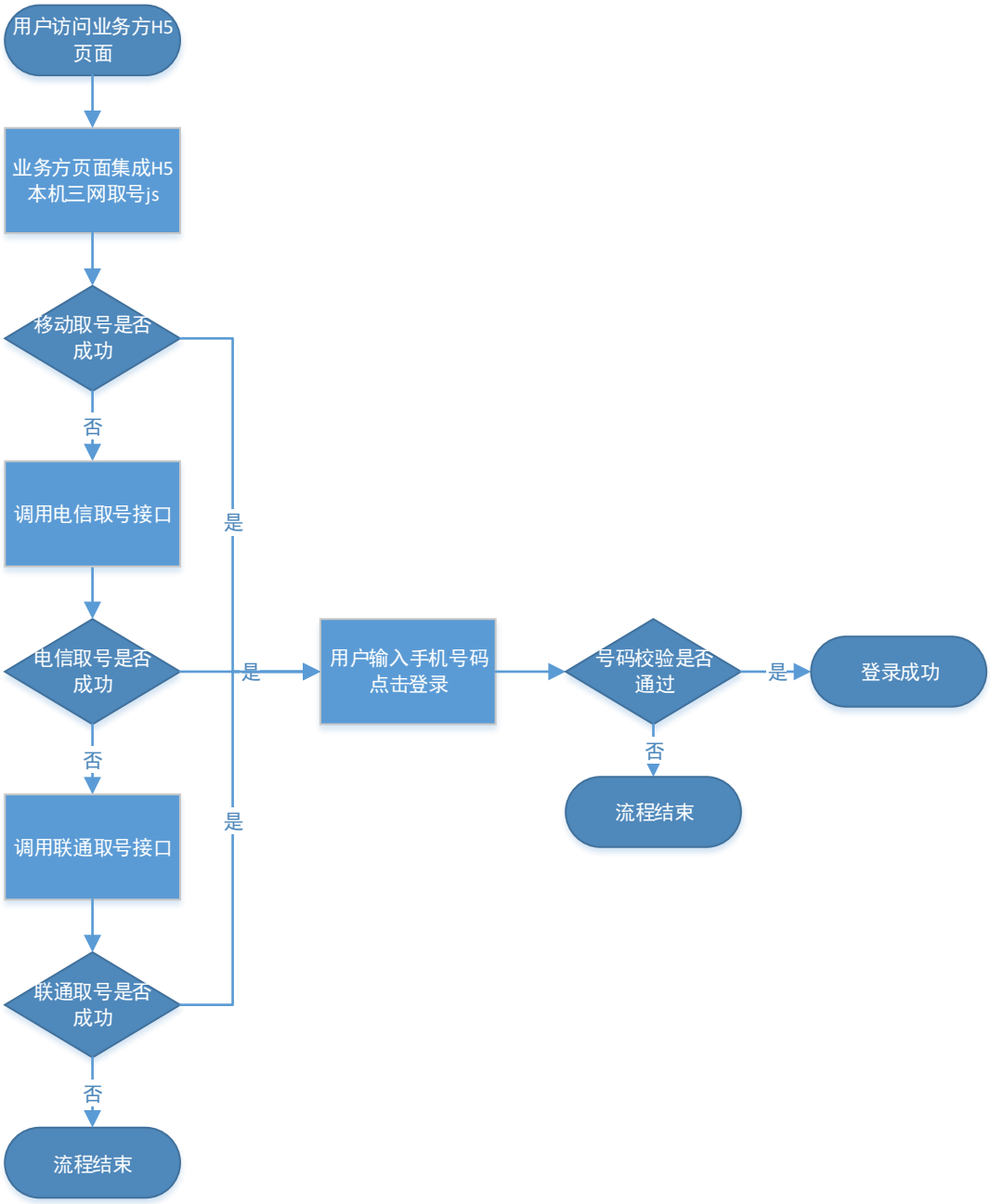
- RSA

(V1.1)

1　业务及交互流程

1. 1业务流程说明

业务流程图：



流程说明：

1)　业务方页面集成 H5 本机三网取号 js；

2)　js 优先进行移动取号，取号成功，用户在前端页面输入手机号码，调用本机号码校验接口，校验通过则直接登录，校验失败则流程结束；

如移动取号失败，则 js 调用电信取号接口，电信取号成功，用户在前端页面输入手机号码，调用本机号码校验接口，校验通过则直接登录，校验失败则流程结束；

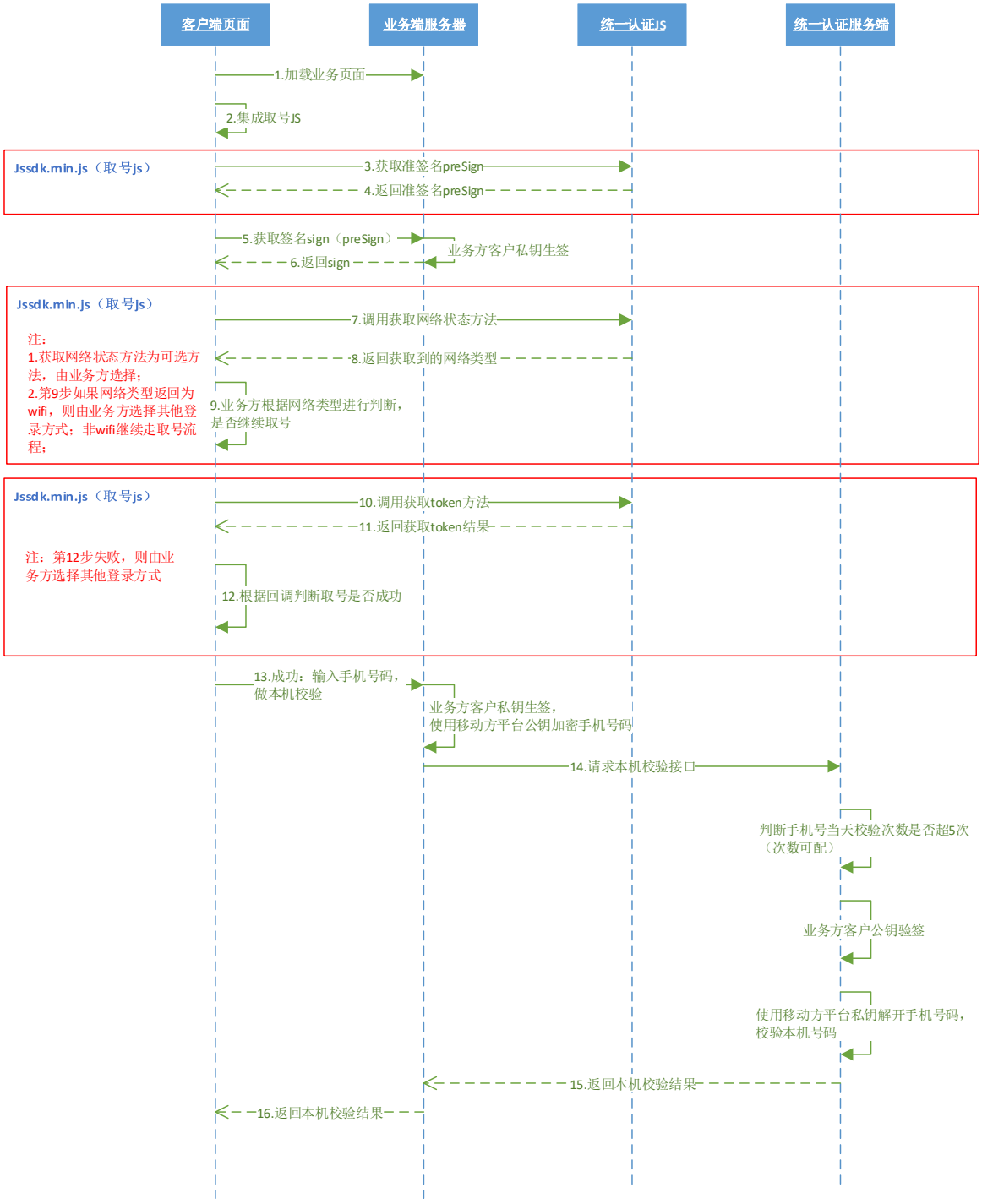
如电信取号失败，则 js 调用联通取号接口，联通取号成功，用户在前端页面输入手机号码，调用本机号码校验接口，校验通过则直接登录，校验失败则流程结束；联通取号失败，则流程结束。

3)　取号顺序：移动>电信>联通；

1.2 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（三网）的产品。

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。

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 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)

10-12 步通过 js 请求获取 token。

成功校验 token

13 步页面请求调用 token 校验接口。

14 步业务侧调用本机校验接口。

15 步返回本机校验结果到业务侧服务端。

16 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 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。

2.2 加密包使用说明

生成公私钥秘钥对必须使用 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));

利用私钥生成签名可使用 RsaUtils 中的 sign 方法。

利用公钥验证签名可使用 RsaUtils 中的 verify 方法。

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

2.3 集成页面和请求来源说明

2.3.1 集成页面地址（referer)

指集成了智能取号的页面访问地址，若多个页面集成用英文逗号分隔上报。必须报备可访问的完整页面地址，不允许使用通配符！

注：

① 假如业务方集成取号的页面访问地址为< http://www.abc.com/a/mobile.html/#/abc>，则报备地址为< http://www.abc.com/a/mobile.html/，

② 假如业务方集成取号的页面访问地址为< http://www.abc.com/a/mobile.html/?abc>，则报备地址为< http://www.abc.com/a/mobile.html/)。

③ 生产上有 https 访问的，https 请求跨域，会导致上报的 referer 为空，请在 head 中

添加代码：<meta content="always" name="referrer">解决此问题。

2.3.2 请求来源（origin）

指发起请求的业务来源。一般为 protocol+host，不包含路径等信息。

几种示例如下：

①假如业务方集成取号的页面访问地址为<http://www.abc.com/a/mobile.html>，则 origin 为<http://www.abc.com>

②假如业务方集成取号的页面访问地址为<https://www.abc.com/a/mobile.html>，则 origin 为<https://www.abc.com>

③假如业务方集成取号的页面访问地址为<http://127.0.0.1:8080/a/mobile.html>，则origin 为<http://127.0.0.1:8080>

④假如业务方集成取号的页面访问地址为<https://127.0.0.1:8080/a/mobile.html>，则origin 为<https://127.0.0.1:8080>

3 本机号码校验接口说明

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
appId	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
phoneNum	待校验的手机号码，使用开放平台提供的平台公钥加密（手机号码	String	是

	+appKey+timestamp） （注：“+”号为合并意思） 值。 例如： （13999994444AA03E6C60D0B0D14320B9A3F0B5AAD99201212271800011 65） 生成后： 4526285940B6FA7FEF49E1DCB04EE944F41A8745444015DAF2771BFB7AD7C800		
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 (appId+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	String	是

	是用TreeMap进行的自然排序))		
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 ":"61237890345",
      "timestamp ":"20160628180001165",
      "appId ":"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 103605 加密方式或密钥值为空 130010: 参数为空 130018: 验证签名失败	是	String	

	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 110027: 能力不可用 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**			
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",
    "appId ":"0008",
```

```
    "resultCode ":"000"
  },
  "body":{
    "taskId ":"ffsfsfsfs3243dsfdf3432xxx",
        "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、H5 认证是否支持异网号码?

支持。除移动外，支持电信和联通取号。

3、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
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 expandparams 扩展参数中是否传了 phoneNum=手机号。

170001	① referer 校验失败。常见原因是 https 请求跨域导致 referer 为空，生产上有 https 访问的，请在 head 中添加代码：<meta content="always" name="referrer">解决此问题； 或实际使用的 referer 集成页面地址和在开放平台上面报备的不一致。请正确报备集成地址。 ② origin 校验失败。常见原因是在开放平台上面报备的请求来源与实际不符是 origin 结尾处多了“/”。请查看文档中关于 origin 的说明。
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。
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。