H5 本机号码校验 JSSDK 集成文档（三网）- RSA

(V1.2)

注：**V1.2** 版本取号接口支持 https

1 产品介绍

1.1 产品说明

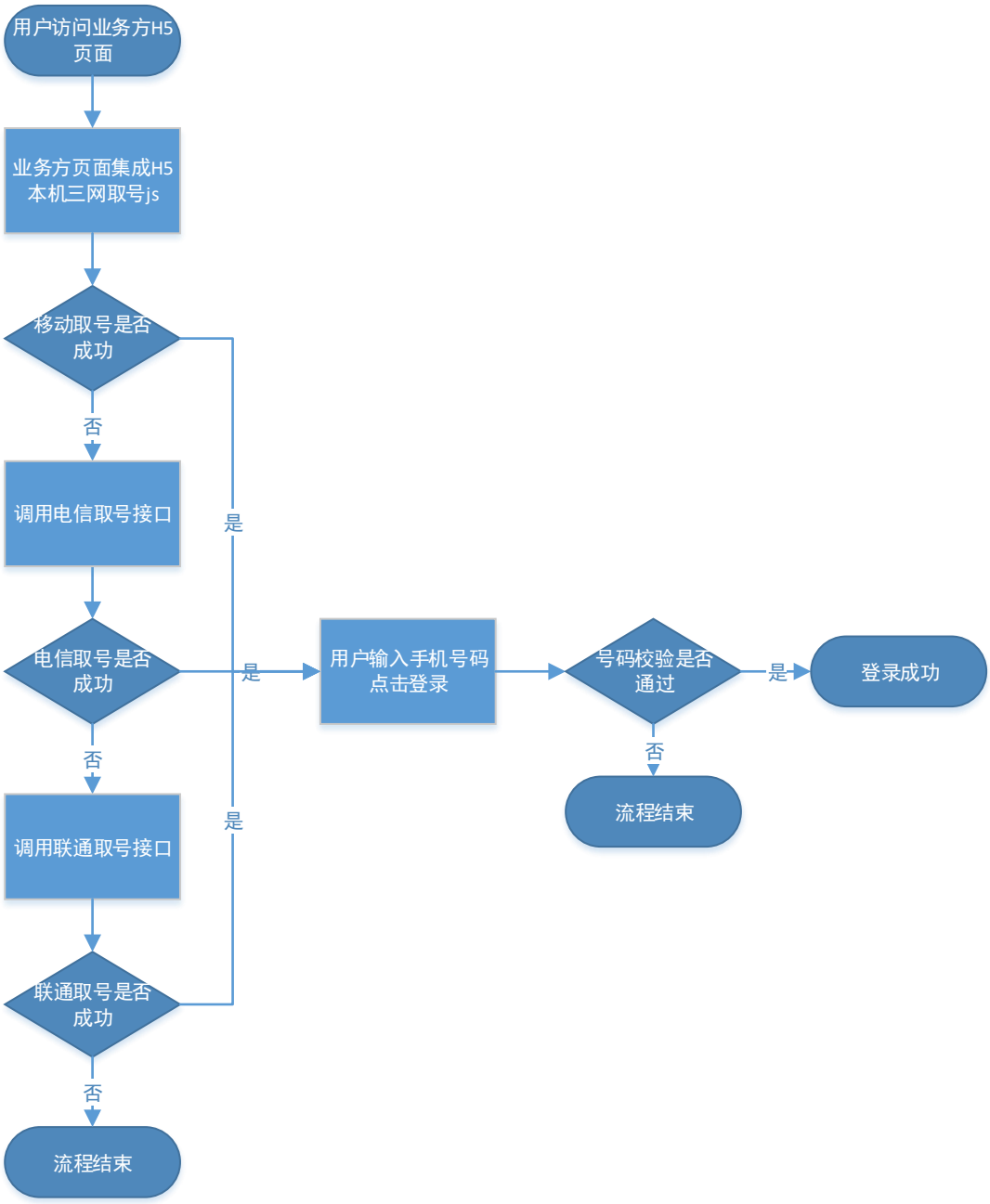
本机号码校验是中国移动推出的用户身份快捷校验产品。进入移动互联网时代，手机号码就是移动互联网的“身份证”，互联网用户通过手机号码将真实信息与互联网资产绑定在一起，互联网企业通过对手机号码的校验实现用户身份认证，进而对银行账号、会员资产、游戏资产等进行管理。

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的解决方案，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 本机号码校验版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：



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；

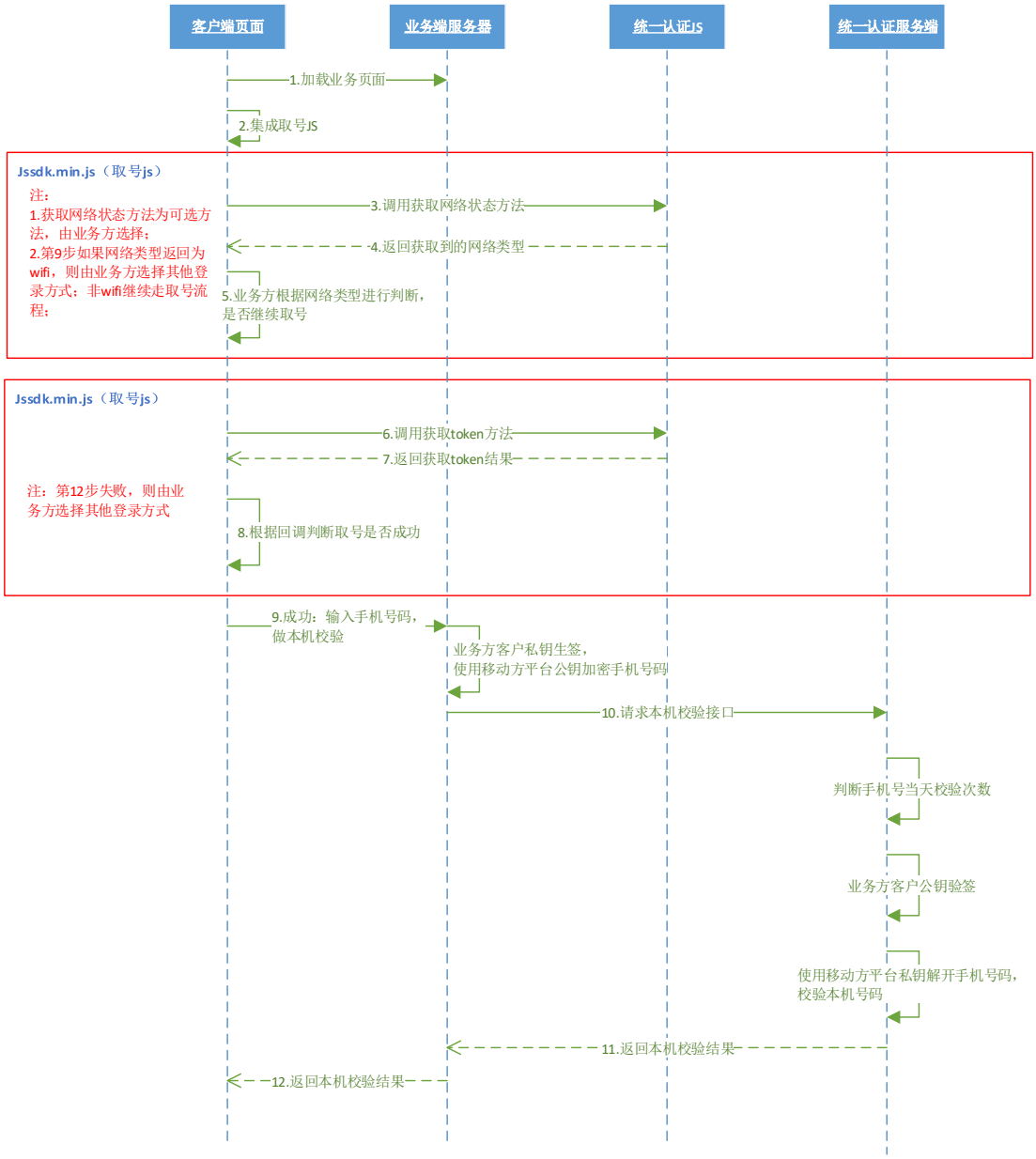
如电信取号失败，则 js 调用联通取号接口，联通取号成功，用户在前端页面输入手机号码，调用本机号码校验接口，校验通过则直接登录，校验失败则流程结束；联通取号失败，则流程结束。

3) 取号顺序：移动>电信>联通；

1.3 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（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。

3-5 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 3.1 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 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。平台公钥会在业务方于开放平台上填写配置信息时自动生成。

2.2 加密包使用说明

生成公私钥秘钥对可使用 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 JSSDK 集成说明

3.1获取网络类型（可选）

定义 connection 变量通过 YDRZ.getConnection 方法获取当前手机网络状态

示例：

var connection = YDRZ.getConnection(appid);

返回对象：

{

appid:“appid”，

msgid:“唯一标识”，

netType:（cellular 数据流量、unknown 未知、wifi）3 种状态

}

可根据 netType 状态自行选择后续流程。

注：此方法为可选，可以获取也可不获取。IOS 系统下由于兼容问题，netType 基本返回结果为 unknown 未知。

3.2引用 YDRZ.min.js

<script type="text/javascript" src="https://www.cmpassport.com/NumberAbility/jssdkVlm_yw/jssdk_v1.0.0.min.js"></script>

3.3使用方法：

//获取 token

YDRZ.getTokenInfo({

data: { //请求的参数

version: ‘1.0’, //接口版本号 （必填）

appId: appId, //应用 Id （必填）

sign: sign, //加密后的 sign（必填）。sign 生成规则： MD5(appId + businessType + msgId + timestamp + traceId + version+appkey） 注：msgID 要和 traceID 保持一致；“+”号为合并意思，不包含在被加密的字符串中。H5 本机 businessType 为 1

traceId: traceId, //业务方生成唯一标识

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

openType: openType, //值为 0 是移动本网，值为 1 按移动->电信->联通的顺序轮询

expandParams: expandParams, //扩展参数 格式：参数名=值 多个时使用 | 分割 （选填）

isTest: isTest //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，error 回调参数的状态码：

{

code："000000", message："token 获取成功",token:"",userInformation: '浏览器指纹'

code："500"，message："接口异常，获取 token 失败",

code："501"，message："接口异常，电信预取号接口失败",

code："502"，message："接口异常，电信取号接口失败",

code："503"，message："接口异常，获取异网 token 接口失败",

code："504"，message："联通 sdk 文件加载失败",

}

注意事项：所有参数请注意大小写。

3. 4具体错误返回码及描述：

移动取号：错误码及描述语

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

联通取号：错误码及描述语

错误码	**错误描述语**
100001	应用鉴权错误（clientID 或 clientSecret 错误）
200001	初始化失败
102	客户端类型错误
104	clientId 错误
106	请求时间超时
107	鉴权信息错误
108	应用签名错误
110	Referer 未报备
111	网络环境错误
113	客户端无权限
1002	网关错误
1003	预取号错误

1004	AccessCode 错误
1011	数据解析错误
1012	网络环境错误
1013	网络环境错误

电信取号：错误码及描述

错误码	**错误描述**
130032	解析参数错误
130010	参数为空
121016	电信取号功能已关闭
130018	验证签名失败
110022	应用 ID 不存在
110023	应用没有权益
110025	权益已失效
170001	无效的请求
999999	系统异常

4 本机号码校验接口说明

请开发者查看《H5 本机号码校验服务端接口文档（三网）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、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。