

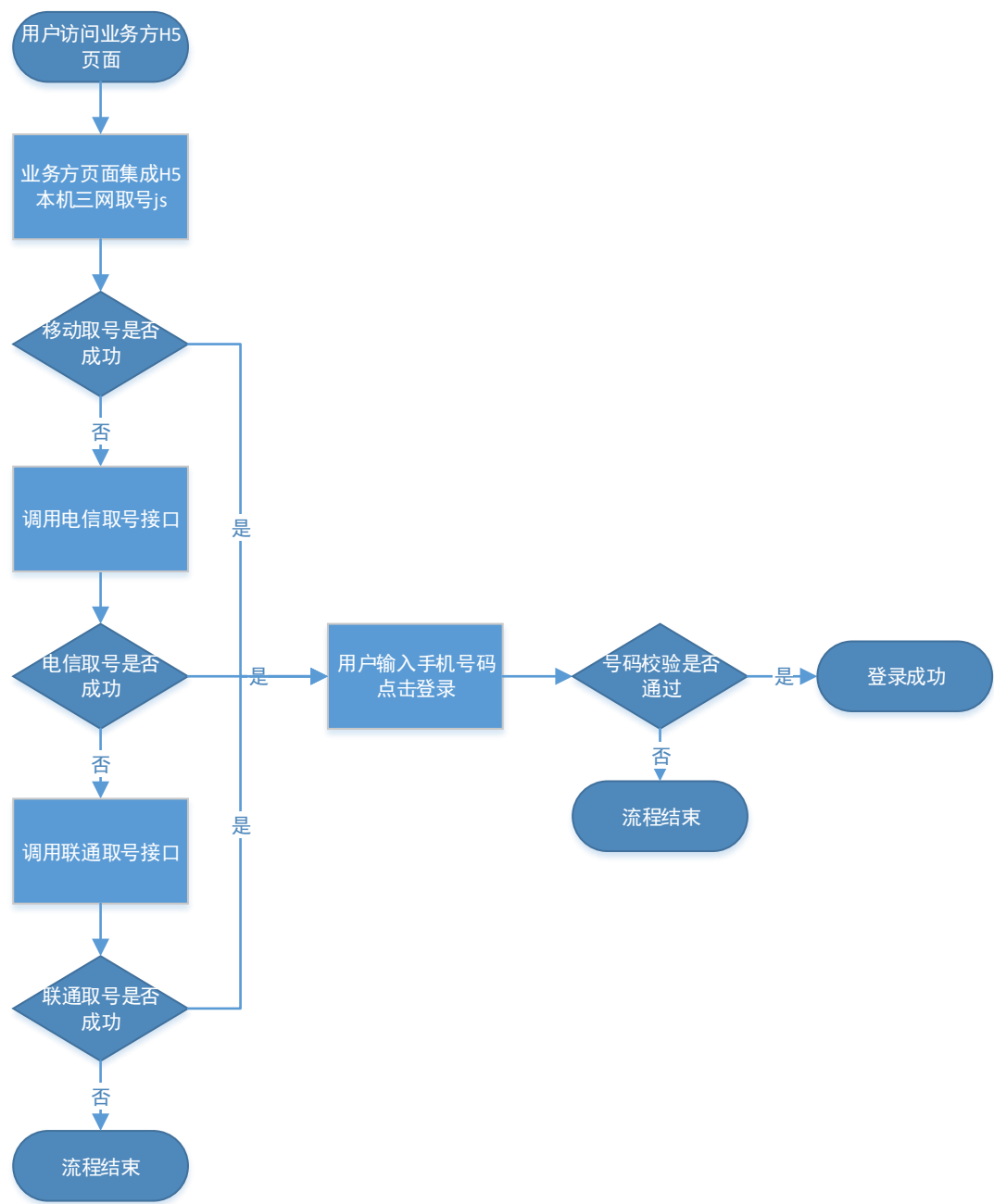
H5 本机号码校验 jssdk 集成文档 RSA（三网） - (V1.1)

1	业务及交互流程	2
1.1	业务流程说明	2
1.2	H5 认证交互说明	3
2	重要参数说明	5
2.1	公私钥说明	5
2.2	加密包使用说明	5
2.3	集成页面和请求来源说明	6
2.3.1	集成页面地址 (referer)	6
2.3.2	请求来源 (origin)	6
3	JSSDK 集成说明	7
3.1	引用 YDRZ.MIN.JS	7
3.2	使用方法:	7
3.3	获取网络类型 (可选)	8
3.4	获取 TOKEN	8
4	本机号码校验接口说明	10
5	常见问题	10
	附录: 常见返回码排查	11

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;

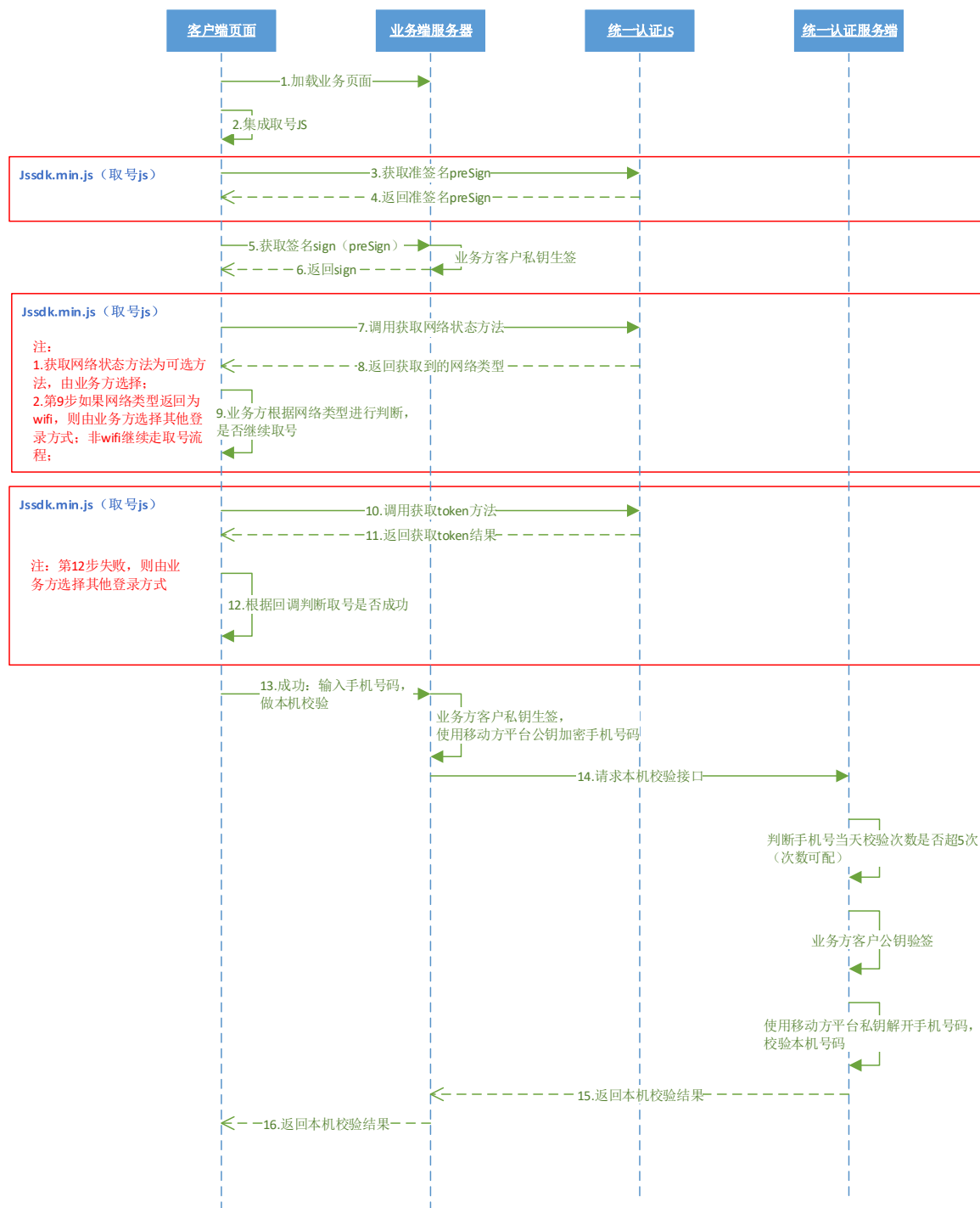
如电信取号失败, 则 js 调用联通取号接口, 联通取号成功, 用户在前端页面输入手机号码, 调用本机号码校验接口, 校验通过则直接登录, 校验失败则流程结束; 联通取号失败, 则流程结束。

- 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，填写公钥并妥善保管好私钥，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

生成公私钥密钥对必须使用 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 (referrer)

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

jssdk 建议在线引用

3.1 引用 YDRZ.min.js

```
<script type="text/javascript" src="https://hmrz.wo.cn/sdk-deliver/js/verify_mobile_sdk-1.2.0.js"></script>
```

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

3.2 使用方法:

定义 sign 变量通过 YDRZ.getSign 方法获取未加密前的 sign

示例:

```
var sign = YDRZ.getSign (appid,version) ; //请注意 2 个参数之间的顺
```

序, appid 为第一个, version 为第二个

重点: (获取 sign 后, 请调用业务方定义的 sign 加密接口, 进行 sign 加密, 后续均要使用到加密后的 sign)

3.3 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（此方法需在 getSign 之后调用）

3.4 获取 token

```
YDRZ.getTokenInfo({
```

```
  data://{请求的参数
```

```
    version:'1.0', //接口版本号 （必填）
```

```
    appId:"", //应用 Id （必填）
```

```
    sign: ' ' //RSA 加密后的 sign （必填）
```

```
    clientDomain:' ' , //接入方域名
```



```
openType:'1',

    expandParams: ' ' //扩展参数 格式：参数名=值 多个时使用 | 分割（选填，测试环境只能模拟取号，联调时需填写模拟取号的手机号码，如 phoneNum=18812345678，生产环境该扩展字段可不填）

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

},

success:function(res){//成功回调

    res.token,

    res.userInformation //如果没有编码的话。可根据实际情况进行二次编码。

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: "110027", message: "能力不可用",

code: "110028", message: "appId 不存在",

code: "130030", message: "参数无效",
```

```
code: "130018", message: "验证签名失败",  
  
code: "130032", message: "解析参数错误",  
  
code: "999999", message: "系统错误"  
  
code: "130010", message: "参数为空"  
  
code: "170001", message: "无效的请求"  
  
code: " 130101", message: "签名错误"  
  
code: "0", message: "请求异常",  
  
code: "500", message: "图片请求失败",  
  
code: "501", message: "接口异常, 获取电信取号接口失败",  
  
code: "502", message: "接口异常, 电信取号接口失败",  
  
code: "503", message: "接口异常, 获取 token 接口失败",  
  
code: " 200001", message: "接口异常, 联通取号初始化失败"  
  
code: " 1012", message: "联通取号失败"  
  
}
```

注意事项：常见返回码排查请见附录，所有参数请注意大小写。

4 本机号码校验接口说明

详细请开发者查看 H5 本机号码校验服务端接口文档说明。

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。

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。