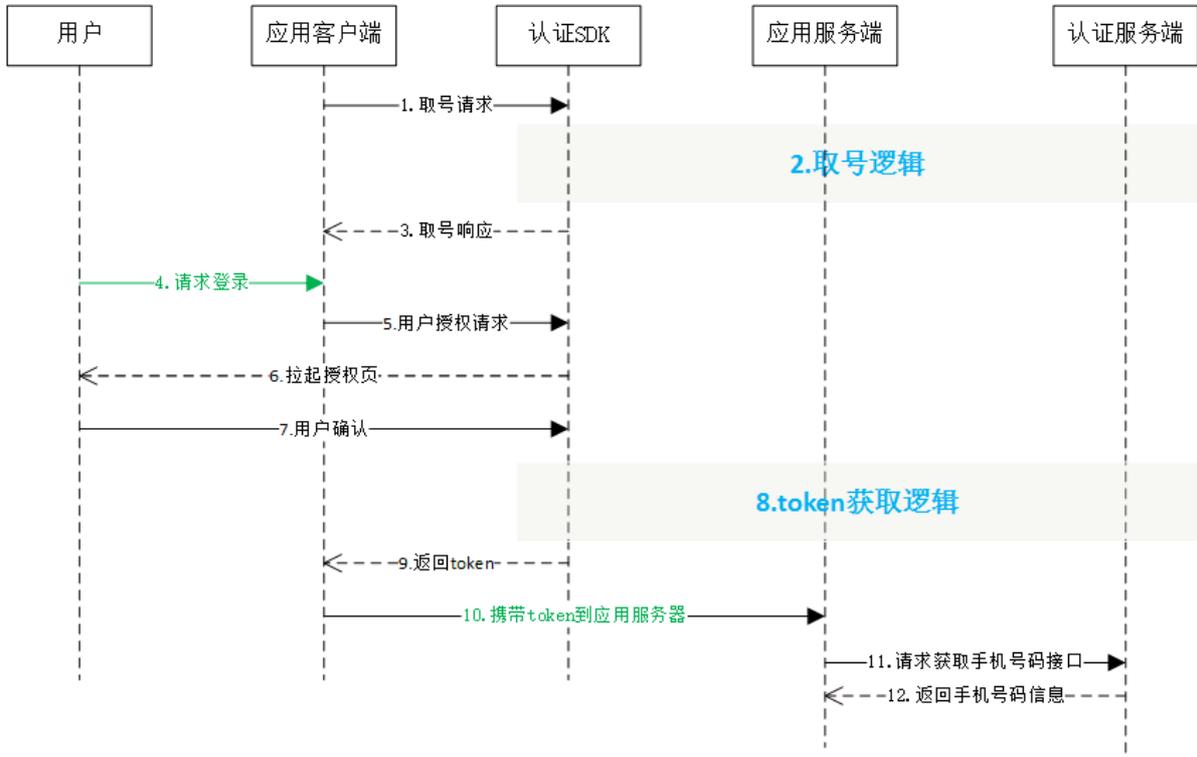


# 1. 获取手机号码接口

## 1.1. 业务流程



## 1.2. 接口说明

请求地址: <https://www.cmpassport.com/unisdsk/rsapi/loginTokenValidate>

协议: HTTPS

请求方法: POST+json,Content-type设置为application/json

注意: 开发者需到开发者社区填写服务端出口IP地址后才能正常使用

## 1.3. 参数说明

- 1、json形式的报文交互必须是标准的json格式
- 2、发送时请设置content type为 application/json
- 3、参数类型都是String

请求参数

参数	是否必填	说明
version	是	填2.0
msgid	是	标识请求的随机数即可(1-36位)
systemtime	是	请求消息发送的系统时间，精确到毫秒，共17位，格式：20121227180001165
strictcheck	是	暂时填写"0"，填写"1"时，将对服务器IP白名单进行强校验（后续将强制要求IP强校验）
appid	是	业务在统一认证申请的应用id
expandparams	否	扩展参数
token	是	需要解析的凭证值。
sign	是	当 <code>encryptionalgorithm≠"RSA"</code> 时， <code>sign = MD5(appid + version + msgid + systemtime + strictcheck + token + APPSecret)</code> （注：“+”号为合并意思，不包含在被加密的字符串中），输出32位大写字母； 当 <code>encryptionalgorithm="RSA"</code> ，开发者使用在社区配置的验签公钥（应用公钥1）对应的私钥进行签名(appid+token)，签名算法为SHA256withRSA，签名后使用hex编码。
encryptionalgorithm	否	推荐使用。开发者如果需要使用非对称加密算法时，填写“RSA”。（当该值不设置为“RSA”时，执行MD5签名校验）

**注1：**对于2018年12月26日前申请、验签方式为appkey的appid，可选择升级为使用APPSecret验签。但由于升级一经提交立即生效，因此在提交前请确保已与您的服务端研发进行了充分沟通，以免服务端生成sign的参数未替换导致验签失败。使用RSA验签加密的开发者不受影响。

**注2：**对于使用RSA验签加密的开发者，生成RSA公私钥对请使用PKCS#8算法，在公钥报备时，请使用Base64格式

#### 响应参数

参数	说明
inresponseto	对应的请求消息中的msgid
systemtime	响应消息发送的系统时间，精确到毫秒，共17位，格式：20121227180001165
resultCode	返回码
msisdn	表示手机号码，如果加密方式为RSA，开发者使用在社区配置的加密公钥（应用公钥2）对应的私钥进行解密
taskId	话单流水号

## 1.4. 示例

## 请求示例

```
{
  "encryptionAlgorithm": "",
  "expandParams": "",
  "appid": "10000001",
  "sign": "0C17F305AB3E8B4694829319167310D1",
  "strictCheck": "0",
  "msgid": "bed1dc7f6cd645b9be9006ae08040c93",
  "systemTime": "20190226111842617",
  "version": "2.0",
  "token": "STsid0000001551151128045KPXuevVDFwyMSy00gbDjxTnn3BVKqXJJ"
}
```

## 响应示例

```
{
  "inResponseTo": "bed1dc7f6cd645b9be9006ae08040c93",
  "resultCode": "103000",
  "msisdn": "159xxxxxxxx",
  "systemTime": "20190226111849953",
  "taskId": "188b0744159f413e9bfe7ecc5d5bcc71"
}
```

## 1.5. 返回码列表

返回码	返回码描述
103000	返回成功
103101	签名错误
103113	token格式错误
103119	appid不存在
103133	sourceid不合法（服务端需要使用调用SDK时使用的appid去换取号码）
103211	其他错误
103412	无效的请求
103414	参数校验异常
103511	请求ip不在社区配置的服务器白名单内
103811	token为空
104201	token失效或不存在
105018	用户权限不足（使用了本机号码校验的token去调用本接口）
105019	应用未授权（开发者社区未勾选能力）
105312	套餐已用完
105313	非法请求

## 2. 本机号码校验接口

开发者获取token后，需要将token传递到应用服务器，由应用服务器发起本机号码校验接口的调用。

校验结果有两种：1.是本机号码；2.非本机号码。对于校验结果为**2.非本机号码**的请求，开发者可以选择使用短验辅助校验功能，通过短信验证码验证用户身份（**短验辅助校验无法保证校验的号码和本机号码一致**）

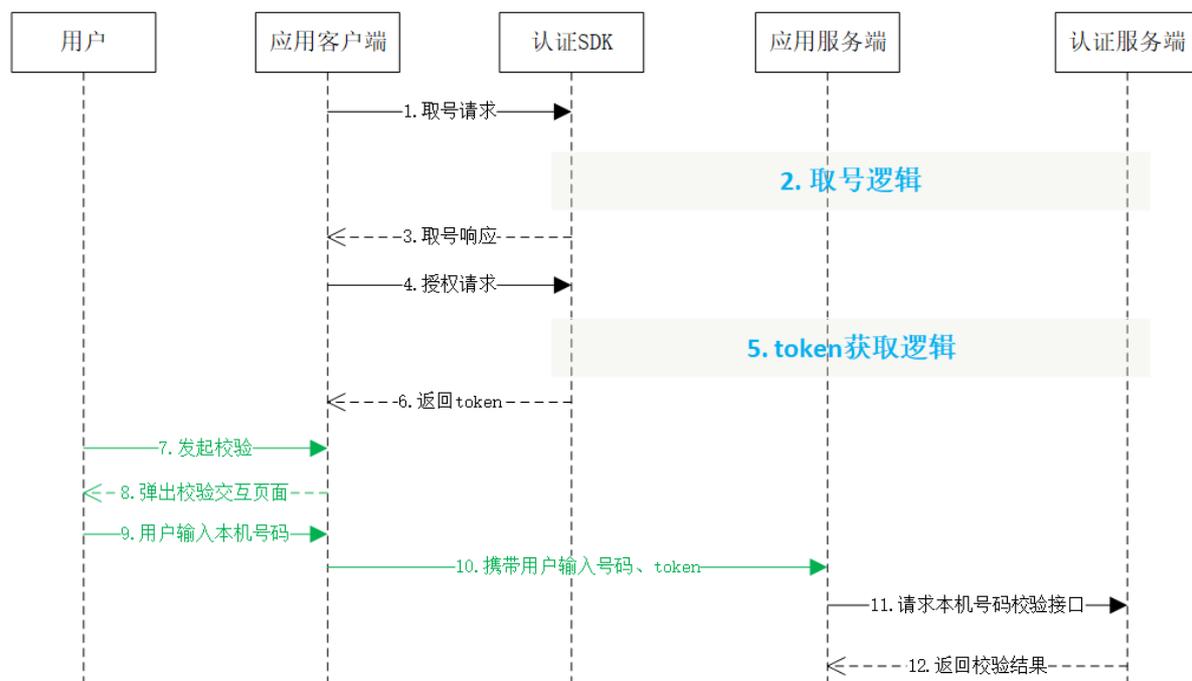
调用本接口，必须保证：

1. token在有效期内（2分钟）。
2. token还未使用过。
3. 应用服务器出口IP地址在开发者社区中配置正确。

对于本机号码校验，需要注意：

1. 本产品属于收费业务，开发者未签订服务合同前，每天总调用次数有限，详情可咨询商务。
2. 签订合同后，将不再提供每天免费的测试次数。

### 2.1. 业务流程



### 2.2. 接口说明

**调用次数说明：** 本产品属于收费业务，开发者未签订服务合同前，每天总调用次数有限，详情可咨询商务。

**请求地址：** <https://www.cmpassport.com/openapi/rs/tokenValidate>

**协议：** HTTPS

**请求方法：** POST+json

### 2.3. 参数说明

- 1、json形式的报文交互必须是标准的json格式
- 2、发送时请设置content type为 application/json

3、参数类型都是String

**请求参数**

参数	层级	是否必填	说明
<b>header</b>	<b>1</b>	是	
version	2	是	版本号,初始版本号1.0,有升级后续调整
msgId	2	是	使用UUID标识请求的唯一性
timestamp	2	是	请求消息发送的系统时间,精确到毫秒,共17位,格式:20121227180001165
appId	2	是	应用ID
<b>body</b>	<b>1</b>	是	
openType	2	否, requestertype 字段为0时是	运营商类型: 1:移动; 2:联通; 3:电信; 0:未知
requesterType	2	是	请求方类型: 0:APP; 1:WAP
message	2	否	接入方预留参数,该参数会透传给通知接口,此参数需urlencode编码
expandParams	2	否	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。
keyType	2	否	手机号码加密方式: 0:默认phonenum采用sha256加密,sign采用HMACSHA256算法 1:RSA加密 (注: keyType=1时, phonenum和sign均使用RSA, keyType不填或非1、0时按keyType=0处理)
phoneNum	2	是	keyType为0时,表示(待校验的手机号码 + appKey + timestamp, "+"号为合并意思)的64位sha256值,字母大写。 keyType为1时,表示使用开发者社区提供的RSA公钥(即“平台公钥”)加密手机号码后的密文串,加密内容为手机号码 + appKey + timestamp, "+"号为合并意思 (注: 建议开发者对用户输入的手机号码的格式进行校验,增加校验通过的概率)
token	2	是	身份标识,字符串形式的token

参数	层级	是否必填	说明
sign	2	是	keyType为0时, 表示签名, HMACSHA256(appId + msgId + phoneNum + timestamp + token + version), 输出64位大写字母 (注: "+"号为合并意思, 不包含在被加密的字符串中, appkey为密钥, 参数名做自然排序 (Java是用TreeMap进行的自然排序) ) keyType为1时, 表示签名, 使用在开发者社区中填入的RSA公钥对应的私钥进行加密, 加密内容为appId + msgId + phoneNum + timestamp + token + version。签名算法MD5withRSA

**注:** 对于使用RSA验签的开发者, 生成RSA公私钥对请使用PKCS#8算法, 位数1024, 在公钥报备时, 请使用Base64格式。使用时, 注意phoneNum使用平台公钥加密, sign使用客户公钥所对应的私钥加签。

### 响应参数

参数	层级	说明
<b>header</b>	<b>1</b>	
msgId	2	对应的请求消息中的msgId
timestamp	2	响应消息发送的系统时间, 精确到毫秒, 共17位, 格式: 20121227180001165
appId	2	应用ID
resultCode	2	平台返回码
<b>body</b>	<b>1</b>	
resultDesc	2	平台返回码
message	2	接入方预留参数, 该参数会透传给通知接口, 此参数需urlencode编码
accessToken	2	使用短验辅助服务的凭证, 当resultCode返回为001时, 并且该appId在开发者社区配置了短验辅助功能时返回该参数。accessToken有效时间为5min, 一次有效。
expandParams	2	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。
taskId	2	话单流水号话单流水号

## 2.4. 示例

### 请求示例

```
{
  "header": {
```

```
    "appId":"300066666666",
    "timestamp":"20180104090953788",
    "version":"1.0",
    "msgId":"8ADFF305C7FCB3E1B1AECC130792FBD0"
  },
  "body":{
    "openType":"1",
    "token":"STsid0000001515028196605yc1oYNTuP1T1LT10AR3ywr2WApEq14JH",
    "sign":"227716D80112F953632E4AFBB71C987E9ABF4831ACDA5A7464E2D8F61F0A9477",
    "phoneNum":"38D19FF8CE10416A6F3048467CB6F7D57A44407CB198C6E8793FFB87FEDFA9B8",
    "requesterType":"0"
  }
}
```

## 响应示例

```
{
  "body":{
    "message":"",
    "resultDesc":"是本机号码"
    "taskId": "b62585d15ee34869bd3c7e6ad62688e2"
  },
  "header":{
    "appId":"3000*****40",
    "msgId":"8ADFF305C7FCB3E1B1AECC130792FBD0",
    "resultCode":"000",
    "timestamp":"20180104090957277"
  }
}
```

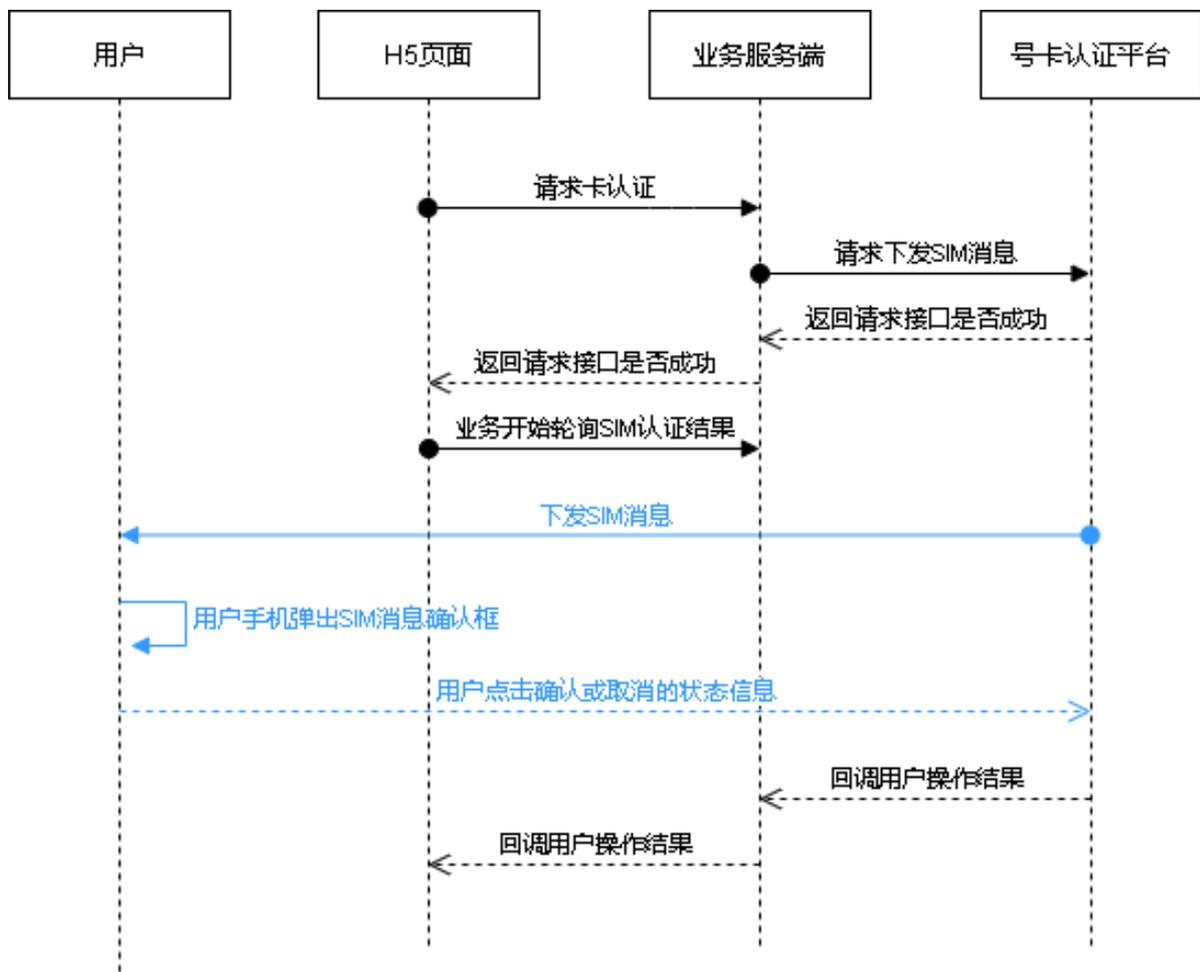
## 2.5. 返回码列表

返回码	返回码描述
000	是本机号码（纳入计费次数）
001	非本机号码（纳入计费次数，允许使用短验辅助）
002	取号失败
003	调用内部token校验接口失败
004	加密手机号码错误
102	参数无效
124	白名单校验失败
302	sign校验失败
303	参数解析错误
606	验证Token失败
999	系统异常
103420	本机号码校验能力使用权限不足

## 3、SIM认证请求接口

**SIM认证：**即SIM快捷认证，用户手动输入待认证号码，触发SIM卡的快捷认证流程实现用户身份确认。对于不支持SIM快捷登录的终端和SIM卡，可选择回落到短信验证码登录。

### 3.1. 业务流程



### 3.2.接口说明

**功能说明:** 在使用SIM认证业务时，由业务服务端向认证平台发起请求，如果用户终端和SIM卡支持SIM认证功能，后台将给用户终端下发一条SIM消息

**调用方向:** 业务平台 => 认证平台

接口名称	bisSimAuthReq
接口描述	在使用SIM认证业务时，由业务服务端向认证平台发起请求，如果用户终端和SIM卡支持SIM认证功能，后台将给用户终端下发一条SIM消息
承载协议	HTTP
承载网络	公网
请求方式	POST
请求限制	
数据格式	Json
接口URL	<a href="https://www.cmpassport.com/h5/localSimCert/bisSimAuthReq">https://www.cmpassport.com/h5/localSimCert/bisSimAuthReq</a>
使用说明	

### 3.3.参数说明

#### 请求参数

#### Request Header

参数名称	说明	类型	是否必填
interfaceVersion	版本号2.0	string	是
traceld	使用UUID标识请求的唯一性	string	是
clientEnv	使用SIM快捷服务的业务平台, clientEnv=1, APP端 clientEnv=2, H5端 clientEnv=3, PC端	string	是
apld	业务方在能开平台上注册通过后获得的业务方标识 apld	string	是
appld	应用ID	string	是
timestamp	请求时间戳, 如: 202010201200030	string	是

### Request Body

参数名称	说明	类型	参数类型
reqData	AES加密的数据, 包含手机号码和消息模板id, 使用业务方的appKey的前16位作为加密key	string	必选
sign	签名, MD5生成签名, MD5(timestamp + traceld + interfaceVersion + appld + reqData + appKey) (注: "+"号为合并意思, 不包含在被加密的字符串中)	string	必选

reqData解密后数据 (json) 格式

参数	说明	类型	是否必填
phoneNumber	手机号码	String	是
templateId	消息模板id	String	是
callbackUrl	用户确认信息回调接口的url	String	是
msgType	认证登录消息类型。1: 认证登录消息, 2: 短验消息, 3: 认证+自动转短验	String	是
templateParam (只有半固定模板才有自定义项目)	若模板ID关联的是半固定模板时, 则该项必填。多个自定义项目之间以英文字符“,”隔开。SIM认证消息模板中, 有自定义项目的, 按模板设定的自定义项目位置顺序——校验, SIM认证消息自定义项目数量及位置由模板决定。	String	否
encVcode	加密验证码 (使用SIM认证平台公钥加密验证码, base64编码, 格式要求4-8位数字); 业务方使用自己生成的验证码时, 该值必传。	String	否

## 响应参数

### 响应\*\*http header\*\*

参数名称	说明	类型	是否必填
traceId	对应的请求消息中的traceId	String	必选
timestamp	响应消息发送的系统时间, 精确到毫秒, 共17位, 格式: 20121227180001165	String	必选
appId	应用ID	String	必选

### 响应\*\*body\*\*

参数名称	父层	说明	类型	是否必填
resultCode		规则参见具体接口返回码说明 103000: SIM下发请求成功 其他, 失败, 透传SIM侧响应描述, 响应码新增	String	是
desc		响应描述, 处理状态编码 请求SIM平台响应错误时, 透传SIM平台响应描述, 新增响应码	String	是
data		数据对象, 层级不为1的参数在此参数中, 无返回数据时, 不需要响应此字段	object	否
taskId	data	返回与任务唯一对应的ID。通过任务ID可与回调信息匹配。	String	是
templateId	data	认证登录模板ID	String	是
templateName	data	返回任务关联的认证登录模板所对应的名称。	String	是
msgText	data	返回拼接后的SIM认证消息文本。	String	是
vcode	data	短信验证码,base64编码 (消息类型为短验消息时返回)	String	否

### 3.4.返回码列表

---

接口	Code	说明
通用接口返回		
1	成功!	
524	号码格式错误	
529	请求时间错误	
534	必要参数缺失	
535	快显系统内部错误	
536	Ip校验不通过	
1001	appld错误	
1004	taskld错误	
1006	系统内部错误	
1009	appld不存在	
1019	业务方已停用	
1015	CapUser不存在	
1020	业务方已被删除	
1021	业务方不存在	
3012	aplId错误	
3013	aplId不存在	
3014	appld不属于该aplId	
3015	signature为空	
3016	signagure校验不通过	
认证登录接口		
1005	模板不存在	
1011	能力不可用	
1012	余量不足	
1016	模板不属于该用户	
1023	pc手机登录发送失败	
1022	模板已停用	
1025	非PC手机登录用户	
2001	内容含有敏感词	
3000	卡无返回	

接口	Code	说明
3002	用户非快捷用户	
3003	用户SIM能力处于关闭状态	
3004	用户手机状态为非正常状态	
3005	其他错误	
3006	用户终端机型不适配	
3027	短验模板未配置	
3028	msgType错误	
3021	短信下发失败	
3022	发送次数超过限制	
3025	短信发送太频繁	
3026	一天内短信发送超过最大值	
3029	signagure签名异常	
3032	短验模板不存在	
3033	短验模板不可用	
短信验证码校验接口		
3023	验证码失效或不存在	
3024	短信验证码为空	
3034	短验校验不通过	
3036	短验有效时间过长	
3037	短验有效时间格式错误	
3038	短信验证码不合法	
3039	短信验证码解密失败	

## 4、业务方回调接口

业务方实现此接口，并在SIM认证请求接口参数callbackUrl中带入接口地址。

业务方接收到数据后，可异步处理具体的逻辑。此接口返回http状态码200就当接收成功

### 4.1.接口说明

**调用方向：**认证平台 => 业务平台

**请求方法：**POST+ json。http 请求头必须设置 Content-Type:application/json;charset=UTF-8

**数据格式：** json

## 4.2.参数说明

http body

返回值字段	父层	参数类型	必填	说明
resultCode		String		103000成功，看simData的数据。
desc		String		描述
data		Object		sim平台相关数据
result	data	String	是	PC手机登录请求任务的结果码
resultDes	data	String	是	结果码描述
callBackType	data	String	是	回调类型：01为SIM认证消息，02为追尾短信，03为短验消息
taskId	data	String	是	返回与任务唯一对应的ID。
taskStartTime	data	String	是	返回任务开始时间，yyyy-MM-dd HH:mm:ss
paid	data	Boolean	是	该条pc手机登录是否计费，true计费，false不计费
vcode	data	String	否	短信验证码,base64编码
phoneSendStat	data	Object	是	返回该用户的操作行为
phone	phoneSendStat	String	是	手机号
state	phoneSendStat	Long	是	用户操作状态：0代表 验证成功or确认 1代表 取消 2代表 用户响应超时 -1代表 sim消息因空号、异、非sim快捷等原因下发失败
signature	simData	String	是	对data除了signature使用sim公钥验证签名 data转为json或map. 然后使用TreeMap自然排序后，使用验证签名方法进行验证。公钥为sim平台公钥

**响应参数**

**http status 200**

**响应body**

