

# 服务端接口文档

---

## 1.应用范围

## 2.接口概要

## 3.安全方式

## 4.手机号解密算法

## 4.一键登录V2（获取手机号码）接口

### 4.1接口地址和说明

### 4.2接口请求参数

### 4.3接口响应内容

### 4.4接口返回示例

## 5.本机认证V2（本机号码校验）接口

### 5.1接口地址和协议说明

### 5.2接口请求参数

### 5.3接口响应内容

### 5.4接口返回示例

## 6.附录

### 响应code码

## 1.应用范围

本文档包含创蓝闪验服务端API接口定义，供开发者参考使用。

本文档为V2版本服务端接口文档，对接2.3.0以后版本SDK（包含2.3.0）。V2版本接口与V1版本接口不兼容，2.3.0版本以前版本的SDK需对接V1版服务端接口。历史V1版本接口文档在资源下载的服务端Demo包中。

## 2.接口概要

接口使用https传输协议，POST方法，请求参数放到RequestBody中以application/x-www-form-urlencoded提交，非JSON格式，响应内容则为JSON格式。本文档包含获取手机号接口和本机号校验接口说明，如APP使用SDK一键登录功能则参考（4.获取手机号接口），APP使用SDK本机号校验功能则参考（5.本机号校验接口）。

## 3.安全方式

接口使用https传输协议，且闪验服务端使用HmacSHA256加密算法验证请求参数中的签名，确保传输过程内部不会被拦截篡改。返回参数中的手机号使用AES或RSA加密。另推荐本文档接口由APP服务端调用，不要在APP前端直接调用，这样可以在官网控制台配置IP白名单，只有在白名单的IP才是合法请求，提高安全性。

## 4.手机号解密算法

返回参数中的mobileName字段，需要使用解密算法解密，默认为AES算法，密文为16进制字符串，解密时需要做对应转换。如在控制台创建应用时如填写了RSA公钥，则只能使用RSA算法解密，推荐1024或2048位PKCS#8格式密钥对。**如未填写则只能使用AES CBC算法，以md5(appKey)前16位字符串为密钥，后16位字符为初始化向量解密。**解密方法详见demo代码中的解密工具类。

## 4.一键登录V2（获取手机号码）接口

### 4.1接口地址和说明

名称	说明
说明	本接口对接SDK一键登录功能，接收SDK一键登录返回的token将其置换为真实手机号码。 <b>本接口为V2版本服务端接口，对接2.3.0以后版本SDK（包含2.3.0）。V2版本接口与V1版本接口不兼容，2.3.0以前版本的SDK需对接V1版服务端接口。历史V1版本接口文档在资源下载的服务端Demo包中。</b>
协议	HTTPS
请求方式	POST
编码格式	UTF8
请求内容类型	application/x-www-form-urlencoded
响应内容类型	application/json
请求地址	<a href="https://api.253.com/open/flashsdk/mobile-query">https://api.253.com/open/flashsdk/mobile-query</a>

### 4.2接口请求参数

参数名	类型	参数描述	是否必填	说明
appld	String	应用的APPID	是	由控制台创建应用时生成。
token	String	运营商token	是	SDK返回的运营商TOKEN，有效期：移动2分钟、电信10分钟、联通30分钟，一次有效。
clientIp	String	客户端IP	否	由客户服务端获取的前端APP的IP，如需要使用反欺诈核验功能则传入，否则可以不传。
encryptType	String	手机号加密方式	否	返回的手机号码加密方式，值包含：0（AES加密）、1（RSA加密）缺省为0，如使用RSA方式则在创建应用时必须填写RSA公钥。
outId	String	客户方流水号	否	客户方流水号，可以为空。
sign	String	签名	是	<p>签名算法：hmacSHA256(所有传入参数按字段名正序排序后拼接的字符串，应用appKey)</p> <p>算法示例：</p> <p>1、只传入必填参数示例：</p> <pre>hmacSHA256("appldxxxxxxtokenxxxxxxxxxxxxxxx", "xxxxxxx")</pre> <p>2、传入了所有参数示例：</p> <pre>hmacSHA256("appldxxxxxclientIp1.1.1.encryptType0outId1111tokenxxxxxxxxxxxxxxxxxxxx", "xxxxxxx")</pre> <p>实际值示例：</p> <pre>9A92CD5A319D254B3DC6BEB7EAD4C2B4F4962B2F</pre>

## 4.3接口响应内容

响应body数据为JSON格式。

字段名	类型	参数描述	说明
code	String	响应代码	200000表示成功，其他代码都为失败，详情参考附录。
message	String	响应描述	响应代码描述

chargeStatus	Int	计费标识	是否收费，枚举值：1:收费/0:不收费
data	Object	数据内容	
data >mobileName	String	手机号密文	手机号密文，根据传入的encryptType值选择对应算法解密手机号。
data >tradeNo	String	交易流水号	闪验的交易流水号

## 4.4接口返回示例

```

1  {
2    "code": "200000",
3    "chargeStatus": 1,
4    "message": "成功",
5    "data": {
6      "tradeNo": "18112115031414011",
7      "mobileName": "1F881288CC68352FC410E8D4A36FC6E0",
8      "fanqizha": 1,
9      "tag": ""
10   }
11 }
12

```

## 5.本机认证V2（本机号码校验）接口

### 5.1接口地址和协议说明

名称	说明
----	----

说明	<p>本接口对接SDK本机认证功能，接收SDK返回的token和传入的手机号码，校验当前流量卡的手机号与传入的手机号码是否一致并返回校验结果。</p> <p>本接口为V2版本服务端接口，对接2.3.0以后版本SDK（包含2.3.0）。V2版本接口与V1版本接口不兼容，2.3.0以前版本的SDK需对接V1版服务端接口。历史V1版本接口文档在资源下载的服务端Demo包中。</p>
协议	HTTPS
请求方式	POST
编码格式	UTF8
请求内容类型	application/x-www-form-urlencoded
响应内容类型	application/json
请求地址	https://api.253.com/open/flashsdk/mobile-validate

## 5.2接口请求参数

参数名	类型	参数描述	是否必填	说明
appId	String	应用的APPID	是	由控制台创建应用时生成。
token	String	运营商token	是	SDK返回的运营商token，有效期：移动2分钟、电信10分钟、联通30分钟，一次有效。
mobile	String	手机号	是	待校验的手机号码
outId	String	客户方流水号	否	客户方流水号，可以为空。

sign	String	签名	是	<p>签名算法：hmacSHA256(所有传入参数按字段名正序排序后拼接的字符串，应用appKey)</p> <p>算法示例：</p> <p>1、只传入必填参数示例： hmacSHA256("appIdxxxxxxmobile1111111111tokenxxxxxxxxxxxxxxxxxx","xxxxxx")</p> <p>2、传入了所有参数示例： hmacSHA256("appIdxxxxxxmobile1111111111outId1111tokenxxxxxxxxxxxxxxxxxx","xxxxxx")</p> <p>实际值示例： 9A92CD5A319D254B3DC6BEB7EAD4C2B4F4962B2F</p>
------	--------	----	---	---

## 5.3接口响应内容

响应body数据为JSON格式。

字段名	类型	参数描述	说明
code	String	响应代码	200000表示成功，其他代码都为失败，详情参考附录。
message	String	响应描述	响应代码描述
chargeStatus	Int	计费标识	是否收费，枚举值：1:收费/0:不收费
data	Object	数据内容	
data >isVerify	String	校验结果	值：1 是本机号码 0 非本机号码
data >tradeNo	String	交易流水号	闪验的交易流水号

## 5.4接口返回示例

```

1  {
2    "code": "200000",
3    "chargeStatus": 1,
4    "message": "成功",
5    "data": {
6      "tradeNo": "18112115031414011",
7      "isVerify": "1"
8    }
9  }
10

```

## 6.附录

### 响应code码

状态码	描述
200000	请求成功
400001	参数校验异常
403000	用户校验失败 (一般为签名问题, 参考: 对接问题> <a href="#">服务端问题</a> )
415000	请求数据转换异常
500000	系统异常
500002	数据处理异常
500003	业务操作失败
500004	远程调用失败
500005	账户余额异常
500006	请求外部系统失败
504000	系统超时
400101	在下游系统中的商户信息不存在
403101	账户被下游系统禁用

403102	账户在下游系统中没有被激活
510101	在下游系统中的用户产品可用数量不足
400102	商户IP地址在下游系统中不合法
400200	黑名单列表
400201	手机号码不能为空
400901	账户信息不存在
400902	应用类型信息不存在
500901	邮箱未设置
500902	账户信息已存在
500903	账户相关能力已激活