

OPPO 广告主转化数据接入说明

方案设计

- 1、 背景..... 2
- 2、 接口说明..... 2
 - 2.1 转化数据同步接口..... 2
 - 2.2 签名算法..... 4
 - 2.3 加密算法..... 4

1、背景

OCPC 智能出价是 OPPO 广告系统通过优化转化率预估模型，帮助广告主提升推广精准度，降低转化成本的一种投放方式；而转化率的预估模型，需要广告主回传相关转化数据；该接口文档主要描述了接口的定义，对接方式以及相关注意事项。

2、接口说明

接口采用 https + post + json 的方式提交数据；

编码方式统一使用 UTF-8；

Salt: e0u6fnlag06lc3pl

Base64Key: XGAXicVG5GMBsx5bueOe4w==

2.1 转化数据同步接口

接口地址：

环境	地址	说明
测试	http://uapi.ads-test.wanyol.com/api/uploadActiveData	(仅内部测试可用)
线上	https://api.ads.heytaomobi.com/api/uploadActiveData	已成功部署

请求信息

请求头(header):

字段	类型	说明	是否必须
signature	string	根据签名算法计算得到的字符串，见签名算法 2.2	是
timestamp	string	时间戳转换为字符串（ long 毫秒 ）	是

数据字段(post body):

字段	类型	说明	是否必须
imei	string	客户端 imei 经过 AES 加密后的值,加密说明见 2.3	二选一
ouId	string	开发者 ID 经过 AES 加密后的值,加密说明见 2.3	
mac	string	客户端 mac 经过 AES 加密后的值,加密说明见 2.3	否
clientIp	string	事件发生时的客户端 ip, 如 210.210.210.210	是
timestamp	long	事件发生的时间戳(毫秒), 如 1522221766623	是
pkg	string	包名, 如 com.xxx	是
dataType	int	转化数据类型: 1、激活, 2、注册, 3、付费	是
channel	int	渠道: 1、OPPO, 2、一加, 0、其他	是
type	int	Imei 原始加密类型 1: md5 加密 0: 无加密 (默认为 0)	否
appType	int	应用类别: 1 应用 2 游戏 3 快应用 0 其他, 默认 1 应用	否
payAmount	long	付费金额 (单位: 分)	否
ascribeType	int	归因类型: 1:广告主归因, 0: OPPO 归因 (默认或者不填即为 0)	否
adId	long	广告主回传转化数据时, 附带已经归因好的广告 id	否

请求示例:

```

imei:123456789      ===AES 加密===>    mWxEB4Il3Q3MsW0/gVPqSw==
mac:12346789        ===AES 加密===>    13tTYshcNalBAxdvreL6A==
timestamp:1571995483916
clientIp:111.111.111.111
pkg:com.xxx.xxx
payAmount:0
appType:1
dataType:1
channel:1
type:0

```

请求报文:

```

(1)header:
signature: 67843bc0e7e7b09cc369beabf05e9d30
timestamp: 1571995483916

```

(2)body:

```

{"payAmount":0,"appType":1,"clientIp":"111.111.111.111","dataType":1,"channel":1,
"imei":"mWxEB4Il3Q3MsW0/gVPqSw==","type":0,"pkg":"com.xxx.xxx","mac":"13
tTYshcNalBAxdvreL6A==","timestamp":1571995483916}

```

返回参数:

字段	类型	说明	是否必须
ret	int	返回码, 0 正常, 1001 参数校验失败, 1002 未知错	是

		误 注意：如果是签名错误的话会返回 http status 403	
msg	string	如果有错误，则返回错误信息	否

返回示例：

```
{
  "ret":0
}
```

2.2 签名算法

使用 md5 对数据进行签名： md5(postData + timestamp + salt)。

timestamp: 时间戳

postData: post 的 JSON 格式数据

salt: OPPO 提供

如当前时间戳为 1522221766623, post 的 json 为

{"imei":"123456789"},OPPO 提供的 salt 字符为 oppo_salt_demo, 则

```
{ "imei": "123456789" }1522221766623oppo_salt_demo
=>
"e05ff81d7756c4b3dfd10cd5e0ccf16f"
```

2.3 加密算法

请求中的 imei 与 mac 字段均需通过 AES 算法进行加密，并且将加密后的二进制数据通过 base64 编码为字符串。为了方便配置，示例中的密钥是经过 base64 处理后的字符串(base64Key)。base64Key 在接入时由 OPPO 提供。

```
import java.security.GeneralSecurityException;
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import org.apache.commons.codec.binary.Base64;

public class Demo {
    public static String encode(byte[] data, String base64Key) throws
GeneralSecurityException {
        final Key dataKey = new SecretKeySpec(Base64.decodeBase64(base64Key),
"AES");

        Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, dataKey);
        byte[] encryptData = cipher.doFinal(data);

        return Base64.encodeBase64String(encryptData);
    }
}
```

3、其他说明

3.1 签名校验说明

若签名校验失败，直接返回 http status code : 403。