

Copyright© 1999-2016 ctrip.com. All rights reserved.

# API 使用规范

*V1.0*

用车事业部 李龙康

2016-7-12

目录

- 总述.....3
  - 1) Http 请求方式 .....3
  - 2) 加密方式 .....3
  - 3) 密钥 .....3
  - 4) 字符集.....3
  - 5) 报文消息格式.....3
- 1. 供应商提供 API 规范.....4
  - 1.1 url 列表： .....4
  - 1.2 参数介绍.....4
    - 系统级参数： .....4
    - 应用级参数： .....4
  - 1.3 消息体加密.....5
    - 示例 .....5
  - 1.4 签名方法.....6
    - 示例 .....6
- 2. 携程提供 API 规范 .....6
  - 2.1 通信方式 .....6
  - 2.2 消息体加密.....6
  - 2.3 签名 .....7

# 总述

该部分内容同时适用于供应商提供 API 规范和携程提供 API 规范

## 1) Http 请求方式

POST

## 2) 加密方式

- MD5 签名
- DES 加密消息体

## 3) 密钥

测试 **SecretKey** : 12345678

生产 **SecretKey** : 上线时确认

## 4) 字符集

所有字符集均采用 UTF-8

## 5) 报文消息格式

Json 消息格式。

请在 Http 请求头中指定 *Content-Type*

Json: *application/json, text/json*

*Json:*

*{*

*}*

# 1. 供应商提供 API 规范

## 1.1 url 列表：

**{domain}/{channel}/productquery/{version}/{timestamp}/{sign}**

**{domain}/{channel}/ordercreate/{version}/{timestamp}/{sign}**

**{domain}/{channel}/ordercancel/{version}/{timestamp}/{sign}**

**{domain}/{channel}/orderupdate/{version}/{timestamp}/{sign}**

**{domain}/{channel}/orderquery/{version}/{timestamp}/{sign}**

## 1.2 参数介绍

API 的输入参数包含系统级参数和应用级参数。

### 系统级参数：

对于每个 API 均一致，用于加密、标识用户身份、API 协议版本等用途。

系统级参数明细：

名称	是否必选	含义	类型	取值示例及说明	附加信息
domain	是	供应商 URL	String		url 中定义
channel	是	渠道	String	OCH 海外接送机 JNT 国内接送机 DAY 日租	url 中定义
version	是	API 版本号	String	1.0	url 中定义
timestamp	是	时间戳	String	yyyyMMddHHmmss	url 中定义
sign	是	API 输入参数签名结果	String	XXXXXXXX	url 中定义

### 应用级参数：

针对 API 的不同用途，应用级参数各不相同，详细参见供应商对接文档。

## 1.3 消息体加密

使用 DES 加密，密钥为携程提供的 SecretKey。加密体是{应用级参数及参数值}，加密。

密文= DESEncrypt({应用级参数及参数值}, SecretKey)

**\*DES加密规格：**

CipherMode. ECB;

PaddingMode. PKCS7;

字节编码方式：16进制大写

## 示例

明文：

```
{"UseType":1,"PatternType":1,"VehicleTypeList":[51],"DuseLocation":{"Address":"樟宜机场","DetailAddress":"樟宜机场","Longitude":103.991531,"Latitude":1.36442},"AuseLocation":{"Address":"新加坡洲际酒店(Intercontinental Singapore)","DetailAddress":"80MiddleRd","Longitude":103.85626,"Latitude":1.297311},"UseTime":"2016-04-05 23:05","FixedCode":"SIN"}
```

密文：(密钥：12345678)

C556A38F5790A1D1EE462A6B1A35681234D2D645124A07D16EE044123B2C9C836FC92  
904D699CC657B15035721C8BBB6F8C77F8BE6D9ADAF65FB174ADDB381C12BB4B014  
1D30623038AEC90FB815364B0BFBE6500C148FCDF095042BD3EA60BBF61DC3C1871C  
EEC7385197AECAAC6C002F23965F9F2F078C9A1E1DB4561567DB420B5BC59149997B3  
42632206E2EC7F8505B9D5F90A17AD2E338230D04D975127C86873ACB9CB9ACBD6E7  
FD40B09401D721C9E5934896CCEEEDBF400606DCCEF27A68531C9848A8E67E443C6C  
DB4B79BDBC0151AE6639A55CBC89A4A7E6075CCBD0175AC09A151394FAAD8BF8BD  
9D4EF24E8FE00DEA8E30AF61DC3C1871CEEC7349D51BD72769633915E0B3E0071F28E  
F0D75EF7D4FC0E842DDB7ED79D1A246EDD33AFDED0EC3047DD8A03CF4AFB817D1  
1CDA6312E589C5380E33387444A9DC5538FAEF3409087EA1BD640A0374962208BDB107  
0A5B1C0110695CF9787FFB8C7BE8D1804C7627C646FD5500F7681DAF6

## 1.4 签名方法

MD5 签名将供应商 ID、版本号、渠道、时间戳、加密密钥、消息体长度字符串拼接之后 MD5 加密

Auth = MD5(VendorID + Version + Channel + TimeStamp + SecretKey + {消息体加密后内容}.Lenth) 转换为小写字符

- + 代表字符串拼接
- {消息体加密后内容}.Lenth 代表加密后消息体长度，注意消息体中请清除所有/r/n 空格之类的格式化符号

## 示例

VendorID : 13593

Version : 1.0

Channel: OCH

TimeStamp : 20160712212208

SecretKey: 12345678

消息体加密后长度 : 784 (消息体加密中的示例)

明文 :

135931.0OCH2016071221220812345678784

密文 :

2bf16185baf294d843af4b9725144a77

# 2. 携程提供 API 规范

## 2.1 通信方式

- 携程采用 API 的方式为供应商提供业务数据推送等服务。
- API 地址 :
  - 测试环境 : <http://service-car.fat.ctripqa.com/chvendormessagebus>
  - 生产环境 : <http://openapi.car.ctrip.com/chvendormessagebus>

## 2.2 消息体加密

使用 DES 加密，密钥为携程提供的 SecretKey。加密体是 {body 内容}，加密。

密文 = DESEncrypt({body 内容}, SecretKey)

- {Envelope 加密后内容}.Lenth 代表加密后 Envelope 长度，注意 Envelope 中请清除所

有/r/n 空格之类的格式化符号

**\*DES加密规格：**

CipherMode. ECB;

PaddingMode. PKCS7;

字节编码方式：16进制大写

## 2.3 签名

MD5 签名将供应商 Id、请求时间戳、加密密钥、消息体长度字符串拼接之后 MD5 加密  
Auth =MD5(VendorID+TimeStamp+SecretKey+{ **Envelope**加密后内容}.Lenth) 转换为小写  
字符

- +代表字符串拼接
- { **Envelope**加密后内容}.Lenth 代表加密后**Envelope**长度，注意**Envelope**中请清除所有/r/n 空格之类的格式化符号