



互联网医院处方平台 对外标准接口文档

文件状态： [] 草稿 [√] 正式发布 [] 正在修改	报告编号：			
	当前版本：			
	编写人：		编写日期	
	审批人：		审批日期	
	保密级别：	保密		

厦门市易联众易惠科技有限公司
2023 年 02 月

版本控制信息

版本	日期	修改人	审核人	说明
V1.0	2020-09-29	林逸祥	林逸祥	初始版本
V2.0	2023-02-15	xuwy	xuwy	

目录

版本控制信息	1
1 引言	3
1.1 目的	3
1.2 文档阅读对象	3
1.3 参考文档	3
1.4 术语说明	3
2 业务流程	3
2.1 业务流程	3
3 接口规则	4
3.1 协议规则	4
3.2 格式规定	4
3.2.1 日期时间格式	4
3.2.2 交易金额格式约定	4
3.2.3 商户订单号约定	4
3.2.4 报文格式约定	4
3.3 数据字典	6
3.3.1 处方状态类型字典	6
4 接口定义	6
4.1 处方状态变更接口	6
4.1.1 接口概述	6
4.1.2 交易类型代码	6
4.1.3 请求地址	6
4.1.4 请求方式	6
4.1.5 出入参说明	7
4.1.6 报文示例	8
4.1.7 常见返回码说明及解决办法	9
附录 1 安全规范	9
1.1 签名算法说明	9
1.1.1 请求参数签名	9
1.1.2 返回参数验签（与请求签名类似）	12
1.2 加密算法说明	12
1.2.1 请求报文加密	13
1.2.2 返回报文解密	14

1 引言

1.1 目的

本文档主要表述了互联网医院产品-处方平台涉及的业务流程以及接口出入参调用示例等，内容包含了 HIS 推送处方审核状态，处方信息同步等业务接口。编写该文档的目的在于对处方平台产品的接口方案进行详细的说明，使接口开发人员能够深刻理解接口方案。

1.2 文档阅读对象

本文档的读者为软件开发人员、软件设计人员、软件实施人员、测试人员以及与该项目相关的其他人员等。

1.3 参考文档

1.4 术语说明

术语	说明

2 业务流程

2.1 业务流程

3 接口规则

3.1 协议规则

规则	规则描述
调用方式	HTTP/HTTPS
提交方式	POST
数据格式	提交和返回数据均为 JSON 格式
字符编码	统一采用 UTF-8 字符编码
判断逻辑	先判断协议字段返回，再判断业务返回，最后判断交易状态
签名算法	请求和响应可选择签名，采用 MD5 算法（或其他）

3.2 格式规定

3.2.1 日期时间格式

统一：yyyyMMddHHmmss。

3.2.2 交易金额格式约定

交易金额默认为人民币交易，接口中参数支付金额单位为【元】。对账单中的交易金额单位为【元】。

3.2.3 商户订单号约定

商户支付、退款的外部订单号由商户自定义生成，并要求商户订单号保持唯一性（建议根据当前系统时间加随机序列加各自系统标识符 APP/WX/ALI/CK/SST 等来生成订单号）。

重新发起一笔支付要使用原订单号，避免重复支付，如该笔订单已支付过或已调用退款的订单号不能将支付失败。

3.2.4 报文格式约定

请求报文和响应报文都由报文头和报文体(param)组成;以下是通用报文头的说明；具体报文体参

数(param)详见各个业务接口说明。注:若业务接口无特殊说明,请求报文均需要组装报文头参数,若字段的可空属性出现 N/Y 的情况,则表明需要根据具体医院来定是否必传。

3.2.4.1 通用请求报文头参数说明

字段名	变量名称	类型	可空	描述
alg	签名方式	String (200)	N	PLAIN, PLAIN
appId	应用编号	String (32)	N	处方平台分配给开发者的应用 ID
timestamp	请求时间戳	String (14)	N	时间格式: YYYYMMDDHHmms s
id	请求 ID	String (12)	N	请使用时间戳
sign	签名值	String (12)	N	通过算法得出的签名值: 9292DD1A8F9B985CE3933C74592BC05D
serviceId	接口服务 ID	String	N	例如 hos.recipe.main.updateRecipeState
termId	终端号	String	N	处方平台分配给开发者的终端号
params	业务入参	JSON	N	详见下表定义
version	版本号	String	N	固定值: V.SDK

3.2.4.2 通用响应报文头参数说明

字段名	变量名称	类型	可空	描述
code	返回码	String (200)	N	接口响应状态码, 000000 表示成功
msg	返回码说明	String (200)	N	接口返回说明: 处理成功
timestamp	返回时间戳	String (200)	N	无
alg	签名算法	String (12)	N	MD5:MD5 算法
sign	签名值	String (12)	N	通过算法得出的签名值: 9292DD1A8F9B985CE3933C74592BC05D
result	业务出参	JSON	N	返回结果

3.3 数据字典

3.3.1 处方状态类型字典

处方状态类型字典	处方状态类型名称
exam_pass	处方审核通过
exam_fail	处方审核不通过
dispensed	已配药（线下取药场景：患者可取药 线上配送场景：可物流下单）
taken	已取药（线下取药场景：患者已取走药 线上配送场景：快递员已经取走药品，线上场景如果 HIS 没有维护该状态则需提前告知）
return	已退药（患者退药退款场景）
invalidated	作废处方（线下直接作废删除该处方场景，可选）

4 接口定义

4.1 处方状态变更接口

4.1.1 接口概述

院内同步处方状态。选用场景：药师审核处方，患者取药完成，患者线下退费退药等。推送给互联网医院处方平台，处方平台记录更新处方状态

4.1.2 交易类型代码

hos.recipe.main.updateRecipeState

4.1.3 请求地址

- 测试地址：待定

4.1.4 请求方式

POST

4.1.5 出入参说明

4.1.5.1 请求入参

请求报文头参数，详见接口规则 3.2.4.1 通用请求报文头参数说明；

请求报文体 param 入参：

字段名	变量名称	类型	可空	描述
data	请求内容体	JSON	N	

请求 data 说明

字段名	变量名称	类型	可空	描述
orgCode	机构编码	String	Y	机构标识
registerNo	挂号流水号	String	N	
drugstoreId	药房编号	String	Y	his 系统中的药房编号
drugstoreName	药房名称	String	Y	his 系统中的药房名称
operatorId	操作员编号	String	N	his 系统中药师或者其他具体操作员编号
operatorName	操作员姓名	String	N	his 系统中药师或者其他具体操作员名称
name	患者姓名	String	N	患者姓名
cardNo	患者卡号	String	N	患者卡号
extra	拓展参数	String	Y	拓展参数
recipeList	处方状态列表	JSONArray	N	处方号集合

recipeList 实体入参：

字段名	变量名称	类型	可空	描述
hisRecipeNo	处方号	String	N	处方号
recipeState	处方状态	String	N	参考字典 处方状态类型字典
remark	备注	String	Y	异常情况下需填入异常情况

4.1.5.2 响应出参

通用报文头参数，详见接口规则 3.2.5.2 通用响应报文头参数说明；

返回报文体 result 出参：

字段名	变量名称	类型	可空	描述

4.1.6 报文示例

说明：此示例属于非 SDK

4.1.6.1 请求参数示例

```
{
  "alg": "PLAIN.PLAIN",
  "appId": "8a8a87106b72a440016b72bf44a10004",
  "id": "1589280374315",
  "params": {
    "data": {
      "registerNo": "0123451",
      "name": "张三",
      "recipeList": [{
        "hisRecipeNo": "21354687",
        "recipeState": "exam_fail"
      }]
    },
    ...
  },
  "serviceId": "hos.recipe.main.updateRecipeState",
  "sign": "rasfs2334214fasf",
  "termId": "1234",
  "timestamp": "1589280374315",
  "version": "V.SDK"
}
```

4.1.6.2 响应参数示例

```
{
  "id": "1589280374315",
  "alg": "PLAIN.PLAIN",
  "version": "V.SDK",
  "code": "000000",
  "timestamp": "20200521180737",
  "appId": "8a8a87106b72a440016b72bf44a10004",
```

```
"termId": "1234",
"sign": null,
"msg": "处理成功"
}
```

4.1.7 常见返回码说明及解决办法

返回码	描述	原因	解决方案

附录 1 安全规范

1.1 签名算法说明

1.1.1 请求参数签名

1. 筛选 获取所有请求参数，不包括字节类型参数，如文件、字节流，剔除 sign 字段。
2. 排序 将筛选的参数按照第一个字符的键值 ASCII 码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值 ASCII 码递增排序，以此类推。
3. 拼接 将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，最后拼接上应用密钥在“…参数=参数值&key=你的密钥”，此时生成的字符串为待签名字符串，将待签名字符串 MD5 运算，即是签名（sign）的值。

```
{
  "alg": "AES.MD5",
  "appId": "8a8a87106b72a440016b72bf44a10000",
  "id": "47485F619033464DBB58586735710BC5",
  "params": {
    "data": {
      "age": "23",
      "bcghcs": 1,
      "bcsfcs": 1,
      "bqmc00": "高血脂",
      "cardNo": "DD3558167",
      "cfxms0": "1",
      "detailList": [{
```

```

        "cfhao0": "sfsdfs",
        "dcyydw": "个",
        "fpxmbh": "02",
        "jx0000": "药品",
        "qyzl00": "25",
        "qyzldw": "25",
        "sfybxm": "Y",
        "sptxbm": "2555555",
        "xmdw00": "包",
        "xmgg00": "g/g",
        "xmmc00": "大力丸",
        "xmsl00": 2,
        "ylts00": "3",
        "yppl00": "3 次/日",
        "ypts00": 3,
        "ypyf00": "口服",
        "ysxm00": "dsfdf"
    }],
    "idNo": "35052619900316453X",
    "ksbm00": "255222",
    "ksmc00": "内一科",
    "operId": "crd",
    "operName": "陈仁地",
    "sfrq00": "20190731",
    "sfygwd": "Y",
    "userName": "陈仁地",
    "xtgzh0": "HIS20190801091631",
    "ysbh00": "326562",
    "ysxm00": "张麟经",
    "yszjdj": "111",
    "yszjhm": "212484154654",
    "zdxxList": [{
        "bqzdbm": "MLIL.OLKL",
        "bqzdms": "头痛"
    }]
}

},
"serviceId": "hos.recipe.main.createRecipeFromHIS",
"termId": "1234",
"timestamp": "20190801091631",
"version": "V.SDK"
}

```

按规则拼接报文成

alg=AES.MD5&appId=8a8a87106b72a440016b72bf44a10000&id=47485F619033464DBB58586735710B

C5¶ms={"data":{"age":"23","bcghcs":"1","bcsfcs":"1","bqmc00":"高血脂","cardNo":"DD3558167","cfxms0":"1","detailList":[{"cfhao0":"sfsdfsfs","dcyydw":"个","fpxmbh":"02","jx0000":"药品","qyzl00":"25","qyzldw":"25","sfybxm":"Y","sptxbm":"2555555","xmdw00":"包","xmgg00":"g/g","xmmc00":"大力丸","xmsl00":"2","ylts00":"3","yppl00":"3次/日","ypts00":"3","ypyf00":"口服","ysxm00":"dsfdf"}],"idNo":"35052619900316453X","ksbm00":"255222","ksmc00":"内一科","operId":"crd","operName":"陈仁地","sfrq00":"20190731","sfygd":"Y","userName":"陈仁地","xtgzh0":"HIS20190801091631","ysbh00":"326562","ysxm00":"张麟经","yszjdj":"111","yszjhm":"212484154654","zdxxList":[{"bqzdbm":"MLIL.OLKL","bqzdms":"头痛"}]}}&serviceId=hos.recipe.main.createRecipeFromHIS&termId=1234&tamp=20190801091631&version=V.SDK&key=8a8a87106b72a440016b72bf44a10000

MD5 加签成

F2F279E2058688F6B18C03C40CA3AD2F

得到新的报文

```
{
  "alg": "AES. MD5",
  "appId": "8a8a87106b72a440016b72bf44a10000",
  "id": "47485F619033464DBB58586735710BC5",
  "params": {
    "data": {
      "age": "23",
      "bcghcs": 1,
      "bcsfcs": 1,
      "bqmc00": "高血脂",
      "cardNo": "DD3558167",
      "cfxms0": "1",
      "detailList": [{
        "cfhao0": "sfsdfsfs",
        "dcyydw": "个",
        "fpxmbh": "02",
        "jx0000": "药品",
        "qyzl00": "25",
        "qyzldw": "25",
        "sfybxm": "Y",
        "sptxbm": "2555555",
        "xmdw00": "包",
        "xmgg00": "g/g",
        "xmmc00": "大力丸",
        "xmsl00": 2,
        "ylts00": "3",
        "yppl00": "3次/日",
        "ypts00": 3,
      }],
    }
  }
}
```

```

        "ypyf00": "口服",
        "ysxm00": "dsfdf"
    }],
    "idNo": "35052619900316453X",
    "ksbm00": "255222",
    "ksmc00": "内一科",
    "operId": "crd",
    "operName": "陈仁地",
    "sfrq00": "20190731",
    "sfygd": "Y",
    "userName": "陈仁地",
    "xtgzh0": "HIS20190801091631",
    "ysbh00": "326562",
    "ysxm00": "张麟经",
    "yszjdj": "111",
    "yszjhm": "212484154654",
    "zdxxList": [{
        "bqzdbm": "MLIL.OLKL",
        "bqzdms": "头痛"
    }]
    },
    "serviceId": "hos.recipe.main.createRecipeFromHIS",
    "sign": "F2F279E2058688F6B18C03C40CA3AD2F",
    "termId": "1234",
    "timestamp": "20190801091631",
    "version": "V.SDK"
}

```

1.1.2 返回参数验签（与请求签名类似）

1.2 加密算法说明

加密模式 1 初始向量（密钥偏移量） 0102030405060708 字符编码 UTF-8 在线加解密工具地址：
<http://www.seacha.com/tools/aes.html>

处方平台提供 JAVA 版本 Server SDK 已将加解密方法封装，开发者只需要调用 sdk 配置业务入参即可，用 sdk 封装的方法发送请求到开放平台时，sdk 会自动加解密。如开发者不用 sdk，可根据 AES 或 DES 加密算法，自己加解密 encryptData 参数。以下是结合开放平台业务对自主加解密进行简单说明：

1.2.1 请求报文加密

1. 组装请求报文 根据 API 列表定义参数,整理请求报文,将 params 字段值,转换为 JSON 字符串 jStr:

```
{"data":{"age":"23","bcghcs":1,"bcsfcs":1,"bqmc00":"高血脂",  
"cardNo":"DD3558167","cfxms0":"1","detailList":[{"cfhao0":"sfsdfsfsf","dcyydw":"个",  
"fpxmbh":"02","jx0000":"药品",  
"qyzl00":"25","qyzldw":"25","sfybxm":"Y","sptxbm":"2555555","xmdw00":"包",  
"xmgg00":"g/g","xmmc00":"大力丸","xmsl00":2,"ylts00":"3","yppl00":"3 次/日",  
"ypts00":3,"ypyf00":"口服",  
"ysxm00":"dsfdf"}],"idNo":"35052619900316453X","ksbm00":"255222","ksmc00":"内一科",  
"operId":"crd","operName":"陈仁地","sfrq00":"20190731","sfygdw":"Y","userName":"陈仁地",  
"xtgzh0":"HIS20190801095852","ysbh00":"326562","ysxm00":"张麟经",  
"yszjdj":"111","yszjhm":"212484154654","zdxxList":[{"bqzdbm":"MLIL.OLKL","bqzdms":"头痛"}]}}
```

根据 ALG 声明加密算法 AES(AES 算法加密参数见开头备注),截取 appId 前 16 位作为 AES 密钥,如 appId.substring(0, 16)加密 appSecret,并将加密结果转 16 进制,再将 16 进制串转换为大写,即获得报文加密密钥:(appId 密钥需根据不同的加密算法取不同的长度做密钥,如 AES 截取前 16 位,DES 截取前 8 位)

第一次 AES 加密, encrypt(appSecret, appId) 得到新密钥 newPassword=614B2607FB83D8109298D163D48CFDFBF1861835315DC357423460181B225BE371723F368437B754EBDOCEC1B01935C6

根据 ALG 声明加密算法 AES,使用 3 获得的报文加密密钥,截取 newPassword 前 16 位作为 AES 密钥,如 newPassword.substring(0, 16)加密 jStr 字符串,并将加密结果转 16 进制,再将 16 进制串转换为大写,获得加密密文 encData: 第二次 AES 加密 encrypt(jStr, newPassword) 得到密文 5EDEB902E459E3AD900E406A8E86A1D6AF6846E49271BF420AA652B508BAF35C437B8D001C819A141E87CF0709B8A61DAB698ABFFDCB74A84895F0AD96E19415AC892B9C03E1BABC79EA4E4AEC4179F168E864EAAAA006347B00DA5084F50F87984F84A5599F21555AAD861CC27A20873C2109BDBAA9E478F90CE0F504898619E003CFB107E4A74A166351A6352F63FBE614FFCD53230BAC103F9108F33C9DF5D32D7C1F30C5EDBF71B49B915AB26F203E9ACF92B8C1DD551D4F15E8308F5C5B137C97F65E9F07C817AF9CFD447ECD776D27DA4DC481AEBEF54C98AE0CF49A419D29AF60B6443D3C1229A097E388B44C5376C4D711404349BDDDBD1D5A8DDA05BB3D9C0A75F5D408FDEAD46432D816867CBF30C6EEA671086A2AAA75C4B5A4DA95403925B0E9D4A73DB21A34CFEAB581520A736C70F7E90E018A48FD3355BE9C22FEE19E7DB252B730F3D6DA5F5642E7546B1E4C7E94E26554EFA6CADCEF8637461AC8C6944F7BE0F34FDAFD5D2788DD60175C32D6BB0678729E3F54CFCCFA5006140DA153E8D6F5DA815407A226506287E51C51A09F5B033E5A2B98100F975FE666B8DA1A4E369C10AA6B33A6AAAB25E991C6979FD4C914C58187F403B52F930DDF35A57BDF46D140E96980DD5E33EB12E58639B9AFFB2396B208F965BDDFEF4F1F4DEDE968ED3D63BC912DBEECB024E31FC9746F4063B03A6B88E5BD03535D4487C08FA81335263708AE395BEA6F9EC3CFA7B878EB41F2323DB5B800C7030A67CA054BD18F1E87B04D70F3EE7DA70C880317E38AFE1D5D652F9AEF6780CB9E68E6299EC0E9CB1A32C03BACBA5482168C974C737051082435778F56B5D2914F84EBE15B9C594066E99A81430BC41BE0A4B5DF458E527C3C7F626BC89B79171ED60EC4F5E15A4FE453ACB73DC5194C9357C61411C7B69F41F252FDEB9E05B1D84D2273E87B7605DC815333C4E97DC775645292COD5EADB660BD4F642B0A5E

CA49A4065E7797C3B5811D36A696C322

然后把密文赋值给 params 得到请求报文

```
{
  "alg": "AES. MD5",
  "appId": "8a8a87106b72a440016b72bf44a10000",
  "id": "47485F619033464DBB58586735710BC5",
  "params":
    "5EDEB902E459E3AD900E406A8E86A1D6AF6846E49271BF420AA652B508BAF35C437B8D001C819A141E87CF0
    709B8A61DAB698ABFFDCB74A84895F0AD96E19415AC892B9C03E1BABC79EA4E4AEC4179F168E864EAAAA0063
    47B00DA5084F50F87984F84A5599F21555AAD861CC27A20873C2109BDBAAA9E478F90CE0F504898619E003CF
    B107E4A74A166351A6352F63FBE614FFCD53230BAC103F9108F33C9DF5D32D7C1F30C5EDBF71B49B915AB26F
    203E9ACF92B8C1DD551D4F15E8308F5C5B137C97F65E9F07C817AF9CFD447ECD776D27DA4DC481AEBEF54C98
    AE0CF49A419D29AF60B6443D3C1229A097E388B44C5376C4D711404349BDDDBD1D5A8DDA05BB3D9C0A75F5D4
    08FDEAD46432D816867CBF30C6EEA671086A2AAA75C4B5A4DA95403925B0E9D4A73DB21A34CFEAB581520A73
    6C70F7E90E018A48FD3355BE9C22FEE19E7DB252B730F3D6DA5F5642E7546B1E4C7E94E26554EFA6CADCEF86
    37461AC8C6944F7BE0F34FDAFD5D2788DD60175C32D6BB0678729E3F54CFCCFA5006140DA153E8D6F5DA8154
    07A226506287E51C51A09F5B033E5A2B98100F975FE666B8DA1A4E369C10AA6B33A6AAAB25E991C6979FD4C9
    14C58187F403B52F930DDF35A57BDF46D140E96980DD5E33EB12E58639B9AFFB2396B208F965BDDFEF4F1F4D
    EDE968ED3D63BC912DBEECB024E31FC9746F4063B03A6B888E5BD03535D4487C08FA81335263708AE395BEA6
    F9EC3CFA7B878EB41F2323DB5B800C7030A67CA054BD18F1E87B04D70F3EE7DA70C880317E38AFE1D5D652F9
    AEF6780CB9E68E6299EC0E9CB1A32C03BACBA5482168C974C737051082435778F56B5D2914F84EBE15B9C594
    066E99A81430BC41BE0A4B5DF458E527C3C7F626BC89B79171ED60EC4F5E515A4FE453ACB73DC5194C9357C6
    1411C7B69F41F252FDEB9E05B1D84D2273E87B7605DC815333C4E97DC775645292C0D5EADB660BD4F642B0A5
    ECA49A4065E7797C3B5811D36A696C322",
  "serviceId": "hos.recipe.main.createRecipeFromHIS",
  "sign": "F2F279E2058688F6B18C03C40CA3AD2F",
  "termId": "1234",
  "timestamp": "20190801091631",
  "version": "V.SDK"
}
```

1.2.2 返回报文解密

获取响应报文

```
{
  "id": "CF89E83C5CEC457D8B341F5E5A5611CF",
  "alg": "AES. MD5",
  "version": "V.SDK",
  "result":
    "1E4C34F171718D05B560C9C960AABC2B124FD8F6775EEB7D5415C813EC39F169A42031681AC3F231ECD19C4
    EFE917D7F662AE4BBBA8ABAF87BB26F63F2BA93ED30A9EDEF8A874880F610F20589E07F0978186BA8254ECD0
    96F455D2D467241DC79B21F46455FF5811F6E134A21607AB4DBD6A2621C82EAAA82AD091FDFAE159D07BB80
    2CD9F321D07813AA3BE8C0A029A405E2BFD9B4F19C11330579648362EEC01E55A5ED9EF89311035E13098B92
    BA333DA5C67E54E7AFC0609B584031A28B301EC2A06649F5C47DABA79410D9A00D76A7737561A04E1EB0ACFC
    "
```

B10FC53FB7E38F06E58989499AAE0BCC32DF9269872ADB695C92202B9A3CAACC2921923017272CF1D623C2D0
9119F81CA9C11F69DD3C1DE84D389C135D2DF1B95498FD4E4451C67502E9405F4DD652FE9C02B81AF572AA5E
69B585E6FF2C705630AF07DCA9E8D5F54767092A261B92C7D69F90B134D3D62003BD9221A1BF29D7F93F27AA
AC0032588E794596B7E55D17D705BDAA641C57DED4237A348DCF642D262FE6DA8A550AB5266CF445A2955566
73703EBC9548FD311771E2A26AD4CF9DC82C7C83347B16F40DD807D5DEFEE62B9FF760EE82E27DBCCAA76007
97D51B33D589394BFFAC7D9BE27A1E22FF9D14947B5DF2F8AC33504D8F67A711A5289067E064C25136736567
CE8E940BF409A66DCEA379AD6E1769EFB96B3409719783606B205805D66E9C6F942A2FC6A25A3C5C1E289070
815E3A01BA9B56A406FFEE023851AA17B7FAC560661B8221C7EC1EC6B681CB0C99D9C5D8E5C924EBFE62E7F0
89321FBCDEA3CE20082516A8DEA9010425334F52CAFBA80EBA21CEEE6EF86C5D4CF9BF8809F13AD5DFAE3CD
4D3A4BF75499CA620197FB8F117E73EFBE674A7EB7789ED6CCC16BD3414560DE82119EC7EA2A25F1A8DB7843
2D07965260EF80298D185CE3E0FD8B2CBD04E107C06254AA6FFB8365555C2C7728F0046B0BCD554946F3913F
8D61B39329EE45B88F50DCF1495203339FB38C3928F3FD6BA2172B4C3F101D965FDE5D4DC1421886AB4AE05F
B791FBAE80FEB14E21465C9678A252BB801F5FE5C011A60A0DD6517EFB380CCF4B565CBFCC09D9EA2D95BFE4
944E8AA613C846F71EBE1754B60C03EB5733E2E96FC284CDEFA22F61AF4832A0068BD32D735D43B7C884FBF2
37B2AC7259124FA3DF73BA509964C479B98F1BA666A8778591F2810ACDDFBDE39BAD7DE0A20A02528A372D0F
A0FB88F347C49AEA9233A0662C20331884E6996A3F814DCOD9566F7E2896EC31284E31E8438D54E23060025F
28688CC41EF3D4B04FBF54C6F8164AC96B1983798D083FB75CBB8F54BA8E2D6ADEAC5B38E",

"code": "000000",
"timestamp": "20190801101236",
"appId": "8a8a87106b72a440016b72bf44a10000",
"termId": "1234",
"sign": "F468133FA6B10CD283A8E19C148CCCC4",
"msg": "处理成功"

}

2. 获取加密密文数据 result

jStr=

1E4C34F171718D05B560C9C960AABC2B124FD8F6775EEB7D5415C813EC39F169A42031681AC3F231ECD19C4E
FE917D7F662AE4BBBA8ABAF87BB26F63F2BA93ED30A9EDEFAA874880F610F20589E07F0978186BA8254ECD09
6F455D2D467241DC79B21F46455FF5811F6E134A21607AB4DBD6A2621C82EAAA82AD091FDFAE159D07BB802
CD9F321D07813AA3BE8C0A029A405E2BFD9B4F19C11330579648362EEC01E55A5ED9EF89311035E13098B92B
A333DA5C67E54E7AFC0609B584031A28B301EC2A06649F5C47DABA79410D9A00D76A7737561A04E1EB0ACFCB
10FC53FB7E38F06E58989499AAE0BCC32DF9269872ADB695C92202B9A3CAACC2921923017272CF1D623C2D09
119F81CA9C11F69DD3C1DE84D389C135D2DF1B95498FD4E4451C67502E9405F4DD652FE9C02B81AF572AA5E6
9B585E6FF2C705630AF07DCA9E8D5F54767092A261B92C7D69F90B134D3D62003BD9221A1BF29D7F93F27AAA
C0032588E794596B7E55D17D705BDAA641C57DED4237A348DCF642D262FE6DA8A550AB5266CF445A29555667
3703EBC9548FD311771E2A26AD4CF9DC82C7C83347B16F40DD807D5DEFEE62B9FF760EE82E27DBCCAA760079
7D51B33D589394BFFAC7D9BE27A1E22FF9D14947B5DF2F8AC33504D8F67A711A5289067E064C25136736567C
E8E940BF409A66DCEA379AD6E1769EFB96B3409719783606B205805D66E9C6F942A2FC6A25A3C5C1E2890708
15E3A01BA9B56A406FFEE023851AA17B7FAC560661B8221C7EC1EC6B681CB0C99D9C5D8E5C924EBFE62E7F08
9321FBCDEA3CE20082516A8DEA9010425334F52CAFBA80EBA21CEEE6EF86C5D4CF9BF8809F13AD5DFAE3CD4
D3A4BF75499CA620197FB8F117E73EFBE674A7EB7789ED6CCC16BD3414560DE82119EC7EA2A25F1A8DB78432
D07965260EF80298D185CE3E0FD8B2CBD04E107C06254AA6FFB8365555C2C7728F0046B0BCD554946F3913F8
D61B39329EE45B88F50DCF1495203339FB38C3928F3FD6BA2172B4C3F101D965FDE5D4DC1421886AB4AE05FB
791FBAE80FEB14E21465C9678A252BB801F5FE5C011A60A0DD6517EFB380CCF4B565CBFCC09D9EA2D95BFE49

44E8AA613C846F71EBE1754B60C03EB5733E2E96FC284CDEFA22F61AF4832A0068BD32D735D43B7C884FBF23
7B2AC7259124FA3DF73BA509964C479B98F1BA666A8778591F2810ACDDFBDE39BAD7DE0A20A02528A372D0FA
0FB88F347C49AEA9233A0662C20331884E6996A3F814DC0D9566F7E2896EC31284E31E8438D54E23060025F2
8688CC41EF3D4B04FBF54C6F8164AC96B1983798D083FB75CBB8F54BA8E2D6ADEAC5B38E

3. 报文解密密钥

根据 alg 声明加密算法，使用 appId 密钥加密 appSecret，并将加密结果转换为大写，再根据不同加密算法截取长度（AES 截取前 16 位、DES 截取前 8 位），即获得报文解密密钥；（appId 密钥是根据不同的加密算法取不同的长度做密钥，如 AES 截取前 16 位，DES 截取前 8 位）
614B2607FB83D8109298D163D48CFDFBF1861835315DC357423460181B225BE371723F368437B754EBD0CEC1
B01935C6

4. 根据 alg 声明加密算法，使用 3. 获取的报文解密密钥，解密 result 获取 JSON 字符串明文 jStr

```
{  
  "sfrq00": "20190731",  
  "updateDate": "20190801",  
  "bqmc00": "高血脂",  
  "infoId": "11C72A53E8A84E41BD83968F0501DCE2",  
  "yszjhm": "212484154654",  
  "ysxm00": "张麟经",  
  "crtTime": "101235",  
  "operId": "crd",  
  "bcghcs": 1,  
  "cardNo": "DD3558167",  
  "idNo": "35052619900316453X",  
  "orderState": "0",  
  "appId": "8a8a87106b72a440016b72bf44a10000",  
  "operName": "陈仁地",  
  "yszjdj": "111",  
  "state": "init",  
  "ysbh00": "326562",  
  "ksmc00": "内一科",  
  "appName": "测试医院",  
  "bcsfcs": 1,  
  "crtDate": "20190801",  
  "ksbm00": "255222",  
  "updateTime": "101235",  
  "zdxxList": [{  
    "bqzdms": "头痛",  
    "bqzdbm": "MLIL.OLKL"  
  }],  
  "userName": "陈仁地",  
  "xtgzh0": "HIS20190801101234",  
  "cfly00": "0",  
  "cfxms0": "1",  
  "detailList": [{
```

```

        "cfhao0": "sfsdfs",
        "xmgg00": "g/g",
        "dcyydw": "个",
        "sfybxm": "Y",
        "ysxm00": "dsfdf",
        "ypl00": "3 次/日",
        "ypts00": 3,
        "qyzl00": "25",
        "ylts00": "3",
        "sptxbm": "2555555",
        "xmmc00": "大力丸",
        "fpxmbh": "02",
        "xmsl00": 2,
        "qyzldw": "25",
        "ypyf00": "口服",
        "xmdw00": "包",
        "jx0000": "药品"
    }],
    "termNo": "1234",
    "sfygwd": "Y",
    "age": "23"
}

```

5. 设置明文

将 jStr 转换为 JSON 赋值 result，获取解密后返回报文

```

{
    "alg": "AES.MD5",
    "appId": "8a8a87106b72a440016b72bf44a10000",
    "code": "000000",
    "id": "CF89E83C5CEC457D8B341F5E5A5611CF",
    "msg": "处理成功",
    "result": {
        "sfrq00": "20190731",
        "updateDate": "20190801",
        "bqmc00": "高血脂",
        "infoId": "11C72A53E8A84E41BD83968F0501DCE2",
        "yszjhm": "212484154654",
        "ysxm00": "张麟经",
        "crtTime": "101235",
        "operId": "crd",
        "bcghcs": 1,
        "cardNo": "DD3558167",
        "idNo": "35052619900316453X",
        "orderState": "0",
        "appId": "8a8a87106b72a440016b72bf44a10000",
    }
}

```

```

    "operName": "陈仁地",
    "yszjdj": "111",
    "state": "init",
    "ysbh00": "326562",
    "ksmc00": "内一科",
    "appName": "测试医院",
    "bcsfcs": 1,
    "crtDate": "20190801",
    "ksbm00": "255222",
    "updateTime": "101235",
    "zdxList": [{
        "bqzdms": "头痛",
        "bqzdbm": "MLIL.OLKL"
    }],
    "userName": "陈仁地",
    "xtgzh0": "HIS20190801101234",
    "cfly00": "0",
    "cfxms0": "1",
    "detailList": [{
        "cfhao0": "sfsdfs",
        "xmgg00": "g/g",
        "dcyydw": "个",
        "sfybxm": "Y",
        "ysxm00": "dsfdf",
        "yppl00": "3 次/日",
        "ypts00": 3,
        "qyzl00": "25",
        "ylts00": "3",
        "sptxbm": "2555555",
        "xmmc00": "大力丸",
        "fpxmbh": "02",
        "xmsl00": 2,
        "qyzldw": "25",
        "ypyf00": "口服",
        "xmdw00": "包",
        "jx0000": "药品"
    }],
    "termNo": "1234",
    "sfygwd": "Y",
    "age": "23"
},
"sign": "F468133FA6B10CD283A8E19C148CCCC4",
"termId": "1234",
"timestamp": "20190801101236",

```

```
    "version": "V.SDK"  
}
```