

医疗保障信息平台
医保移动支付中心两定机构接口规范
(V1.1.1)

版本	修订章节	修订内容功能描述	修订日期	修订人	修订前版本号	批准人	备注
V1.0		新建	2020-6	陈仁地	无	管方	
V1.1	3.2.3.1	新增“类别代码”16, 门诊特殊病	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.1	新增“类别代码”71, 家庭病床	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.26	新增“险种类型”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.27	新增“个人结算方式”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.28	新增“中药使用方式”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.29	新增“生育费用标识”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.30	新增“出院带药标志”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.31	新增“外检标识”	2021-01-05	陈仁地	V1.0	管方	
V1.1	3.2.3.32	新增“医院审批标志”	2021-01-05	陈仁地	V1.0	管方	
V1.1	4.2.3.1	新增“请求入参”字段: chrgBchno、psnSetlway、psnNo、insuType	2021-01-05	陈仁地	V1.0	管方	
V1.1	4.2.3.1	新增“condList 定义”字段: mainCondDscr	2021-01-05	陈仁地	V1.0	管方	
V1.1	4.2.3.1	新增“rxList 定义”字段: medinsListCodg、rxTime、rxCircFlag、acordDeptCodg、acordDeptName、ordersDrCode、ordersDrName、hospApprFlag、tcmdrugUsedWay、etipFlag、etipHospCode、dscgTkdrugFlag、matnFeeFlag	2021-01-05	陈仁地	V1.0	管方	
V1.1.1	4.2.3.1	rxList 定义中“invoItemNo”、	2021-01-13	张景庄	V1.1	管方	

版本	修订章节	修订内容功能描述	修订日期	修订人	修订前版本号	批准人	备注
		“hiItem” 字段删除。					
V1.1.1	3.2.3.23	说明更新	2021-01-15	张景庄	V1.1	管方	
V1.1.1	3.2.3.24	说明更新	2021-01-15	张景庄	V1.1	管方	
V1.1.1	4.8.1.1	说明文字修订	2021-01-18	陈仁地	V1.1	管方	
V1.1.1	4.8.2.1	说明文字修订	2021-01-18	陈仁地	V1.1	管方	
V1.1.1	4.2.3.1	新增 rxCircFlag 字段用于电子处方场景	2021-01-19	陈仁地	V1.1	管方	

目次

1	范围	5
2	业务流程	5
3	接口规则	5
3.1	协议规则	5
3.2	格式规定	5
3.2.1	日期、时间格式	5
3.2.2	交易金额格式约定	5
3.2.3	数据字典	6
4	接口定义	13
	终端获取支付令牌(DLL)	13
4.1.1	接口概述	13
4.1.2	请求方式	13
4.1.3	出入参说明	14
4.1.4	DLL 方法	14
4.2	费用上传(DLL)	14
4.2.1	接口概述	14
4.2.2	请求方式	14
4.2.3	出入参说明	15
4.2.4	DLL 方法	18
4.3	支付下单(DLL)	18
4.3.1	接口概述	18
4.3.2	请求方式	18
4.3.3	出入参说明	18
4.3.4	DLL 方法	19
4.4	查询订单结算状态(SDK)	19
4.4.1	接口描述	19
4.4.2	请求地址	19
4.4.3	请求方式	19
4.4.4	出入参说明	19
4.4.5	SDK 方法	20
4.5	撤销费用明细上传(DLL)	21
4.5.1	接口描述	21
4.5.2	请求方式	21
4.5.3	出入参说明	21
4.5.4	DLL 方法	21
4.6	医保冲正(SDK)	21
4.6.1	请求地址	21
4.6.2	接口概述	22
4.6.3	请求方式	22
4.6.4	出入参说明	22

4.6.5	SDK 方法.....	22
4.7	医保退费(DLL)	23
4.7.1	接口概述	23
4.7.2	请求方式	23
4.7.3	出入参说明	23
4.7.1	DLL 方法.....	24
4.8	支付结果推送	24
4.8.1	后端回调	24
4.8.2	前端回调	26
4.9	对账文件文件下载	27
4.9.1	接口地址	27
4.9.2	接口描述	27
4.9.3	请求方式	27
4.9.4	出入参说明	27
4.10	参保人员信息查询(DLL)	28
4.10.1	接口地址	28
4.10.2	接口概述	28
4.10.3	请求方式	28
4.10.4	出入参说明	28
4.10.5	DLL 方法.....	29
附录 1	安全规范	30
1.1	签名算法 (SM2)	30
1.1.1	概述	30
1.1.2	请求参数签名	30
1.1.3	返回参数验签	31
1.2	加密算法 (SM4)	32
1.2.1	概述	32
1.2.2	请求报文加密	32

医保移动支付中心两定机构接口规范

1 范围

本文档适用于两定机构调用接入医保移动支付中心服务，主要表述了电子凭证结算涉及的接口出入参调用示例。

2 业务流程

请参考《医疗保障信息平台医保移动支付技术规范》。

3 接口规则

3.1 协议规则

规则	规则描述
传输方式	为保证交易安全性，采用 HTTPS 传输
提交方式	采用 POST 方法提交
数据格式	提交和返回数据都为 JSON 格式
字符编码	统一采用 UTF-8 字符编码
签名算法	SM2
加密算法	SM4
签名要求	请求和接收数据均需要校验签名，详细方法请参考安全规范-签名算法
加密要求	请求和接收数据均需要校验签名，详细方法请参考安全规范-加密算法
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

3.2 格式规定

3.2.1 日期、时间格式

日期：YYYYMMDD；

时间：HHMMSS。

3.2.2 交易金额格式约定

以元为单位，具体根据接口示例约定保留位数。

3.2.3 数据字典

3.2.3.1 诊疗类别定义字典 (medType)

类别代码	类别说明	备注
11	普通门诊	
12	门诊挂号	
13	急诊	
14	门诊慢特病	
15	门诊统筹	
16	门诊特殊病	
21	普通住院	
22	外伤住院	
23	转外诊治住院	
41	定点药店购药	
51	生育门诊	
52	生育住院	
53	计划生育手术费	
60	互联网问诊	新增
71	家庭病床	

3.2.3.2 门诊类别定义字典 (otpType)

类别字典	类型名称	备注
1	普通门急诊	
2	门诊慢特病	
3	其他	

3.2.3.3 费用类型

类别字典	类型名称	备注
01	门诊就诊	
02	住院	
03	体检	
04	家庭医生签约	
05	互联网医院问诊	
06	长处方续方	
07	药店在线购药	
08	终端认证问诊	
09	药店线下购药	

3.2.3.4 订单状态字典

订单状态	状态名称	备注
0	已保存	
1	预结算完成	
2	结算中	
3	自费完成	
4	医保支付完成	
5	院内结算完成	
6	结算完成	
7	已退款	
8	已医保全部退款	
9	仅自费全部退款	
10	仅自费部分退款	
11	医保全部退自费部分退款	
12	已撤销	
13	医保已撤销	
14	异常	
15	结算失败	
16	医保结算失败自费冲正失败	

3.2.3.5 回调类型

类别字典	类别名称	备注
1	支付授权回调	
2	支付成功回调	
3	退款授权回调	
4	预结算成功回调	
5	密码验证及预结算回调	

3.2.3.6 证件类型

证件代码	证件说明	备注
01	居民身份证（户口簿）	
02	中国人民解放军军官证	
03	中国人民武装警察警官证	
04	香港特区护照/港澳居民来往内地通行证	
05	澳门特区护照/港澳居民来往内地通行证	

06	台湾居民来往大陆通行证	
07	外国人永久居留证	
08	外国人护照	
11	外国人就业证	
12	外国专家证	
13	外国人常驻记者证	
14	台港澳人员就业证	
15	回国（来华）定居专家证	
16	出生医学证明	
17	港澳台居民居住证	
99	其他身份证件	

3.2.3.7 人员类别

类别代码	说明	备注
11	在职	
21	退休	
31	离休	
32	老红军	
33	一至六级残疾军人	
41	学龄前儿童	
42	中小學生	
43	大学生	
50	成年居民（非从业）	
60	老年居民	
91	其他人员	

3.2.3.8 离院方式

代码	说明	备注
1	医嘱离院	
2	医嘱转院	
3	医嘱转社区卫生服务机构/乡镇卫生院	
4	非医嘱离院	
5	死亡	
9	其他其他	

3.2.3.9 生育手术类别

代码	说明	备注
1	放置宫内节育器	
2	取出宫内节育器	
3	流产术	
4	引产术	
5	绝育手术	
6	绝育复通手术	
9	其他	

3.2.3.10 生育类别

代码	说明	备注
1	正常产	
2	助娩产	
3	剖宫产	

3.2.3.11 险种定义

代码	说明	备注
310	职工基本医疗保险	
320	公务员医疗补助	
350	一至六级残废军人医疗补助	
360	老红军医疗保障	
380	新型农村合作医疗	
391	城镇居民基本医疗保险	
330	大额医疗费用补助	
340	离休人员医疗保障	
390	城乡居民基本医疗保险	
392	城乡居民大病医疗保险	
510	生育保险	

3.2.3.12 公务员标识

代码	说明	备注
0	否	
1	是	

3.2.3.13 公务员等级

代码	说明	备注
101	国家级正职	
102	国家级副职	
111	省部级正职	
112	省部级副职	
121	厅局级正职	
122	厅局级副职	
131	县处级正职	
132	县处级副职	
141	乡科级正职	
142	乡科级副职	
150	科员级	
160	办事员级	
199	未定职	

3.2.3.14 缴费档次

代码	说明	备注
1	一档	
2	二档	
3	三档	

3.2.3.15 灵活就业标识

代码	说明	备注
0	否	
1	是	

3.2.3.16 新生儿标识

代码	说明	备注
0	否	
1	是	

3.2.3.17 门诊诊断类别

代码	说明	备注
1	西医诊断	
2	中医主病诊断	

代码	说明	备注
3	中医主证诊断	

3.2.3.18 出入院诊断

代码	说明	备注
1	入院诊断	
2	出院诊断	

3.2.3.19 是否主诊断标识

代码	说明	备注
0	否	
1	是	

3.2.3.20 结算类别

代码	说明	备注
3	补充报销	
2	联网结算	
1	中心报销	

3.2.3.21 待遇状态

代码	说明	备注
0	正常	
1	封锁	

3.2.3.22 收费项目类别

代码	说明	备注
01	西药	
02	中成药	
03	中草药	
04	常规检查	
05	CT	
06	核磁	
07	B超	
08	治疗费	
99	其他费用	

3.2.3.23 急诊标志

代码	说明	备注
0	否	
1	是	

3.2.3.24 外伤标志

代码	说明	备注
0	否	
1	是	

3.2.3.25 住院类别

代码	说明	备注
1	普通住院	
2	急诊或抢救住院	
3	转院住院	

3.2.3.26 险种类型

代码值	代码名称	代码值	代码名称
310	职工基本医疗保险	390	城乡居民基本医疗保险
320	公务员医疗补助	392	城乡居民大病医疗保险
330	大额医疗费用补助	510	生育保险
340	离休人员医疗保障		

3.2.3.27 个人结算方式

代码值	代码名称	代码值	代码名称
01	按项目结算	02	按定额结算

3.2.3.28 中药使用方式

代码值	代码名称	代码值	代码名称
1	复方	2	单方

3.2.3.29 生育费用标识

代码值	代码名称	代码值	代码名称
0	否	1	是

3.2.3.30 出院带药标志

代码值	代码名称	代码值	代码名称
0	否	1	是

3.2.3.31 外检标识

代码值	代码名称	代码值	代码名称
0	否	1	是

3.2.3.32 医院审批标志

代码值	代码名称	代码值	代码名称
0	无须审批	2	审批不通过
1	审批通过		

4 接口定义

4.1 终端获取支付令牌(DLL)

4.1.1 接口概述

用户在医保业务综合服务终端上刷脸成功后，两定机构处理业务后，使用业务流水号来进行换取终端支付令牌。

4.1.2 请求方式

POST。

4.1.3 出入参说明

4.1.3.1 请求入参

名称	类型长度	可空	说明	备注
orgCodg	Varchar2(40)	N	机构编码	医保分配
orgId	Varchar2(40)	Y	电子凭证机构号	电子凭证中台分配,待机构电子凭证建设完毕后可获取该机构号
idNo	Varchar2(40)	N	证件号码	
userName	Varchar2(40)	N	用户姓名	
idType	Varchar2(3)	N	证件类型	
ecToken	Varchar2(64)	N	电子凭证授权 ecToken	
feeType	Varchar2(3)	N	费用类型	见费用类型字典定义,该方法固定传08
authNo	Varchar2(64)	N	实名认证流水号	每一次请求都要求不同,人脸识别返回

4.1.3.2 响应出参

名称	类型长度	可空	说明	备注
payToken	Varchar2(40)	N	支付授权码	费用上传时使用
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.1.4 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

4.2 费用上传 (DLL)

4.2.1 接口概述

医院主动上传费用明细到医保结算中心,院方需要修改处方时,需要先撤销上传,修改完成之后重新上传。

4.2.2 请求方式

POST。

4.2.3 出入参说明

4.2.3.1 请求入参

名称	类型长度	可空	说明	备注
orgCodg	Varchar2(40)	N	机构编码	医保分配
orgId	Varchar2(40)	Y	电子凭证机构号	电子凭证中台分配,待机构电子凭证建设完毕后可获取该机构号
ecToken	Varchar2(64)	Y	电子凭证授权 ecToken (普通扫电子凭证码返回)	当 feeType 不为 08 时,可为空
payToken	Varchar2(64)	Y	支付令牌 (使用医保业务终端时返回)	当 feeType=08 时,不可为空
insuCode	Varchar2(6)	N	参保人所在统筹区编码	
idNo	Varchar2(40)	N	证件号码	
userName	Varchar2(40)	N	用户姓名	
idType	Varchar2(3)	N	证件类型	
medOrgOrd	Varchar2(40)	N	医疗机构订单号	院内产生惟一流水,可关联到一次结算记录,结算成功回调入参返回
initRxOrd	Varchar2(40)	Y	要续方的原处方流水	目前未开始校验
erFlag	Varchar2(3)	Y	急诊标志	
trumFlag	Varchar2(3)	Y	外伤标志	
feeType	Varchar2(3)	N	费用类型	见费用类型字典定义
otpType	Varchar2(3)	N	门诊类别	见门诊类别定义字典
medType	Varchar2(3)	N	诊疗类别	见字典定义
feeSumamt	number(12,2)	N	费用总金额	保留两位小数
chrgDate	Varchar2(8)	N	收费日期	yyyyMMdd
chrgTime	Varchar2(6)	N	收费时间	HHmmss
rgstSn	Varchar2(40)	Y	医保挂号流水号	为空时平台重新挂号
rgstFee	number(12,2)	N	挂号费用	保留两位小数
rgstDeptName	Varchar2(40)	Y	挂号科室名称	-
drName	Varchar2(40)	N	医生姓名	-
medreformDot	Varchar2(1)	N	是否医改网点	Y/N
drDeptCodg	Varchar2(40)	N	医生科室编号	-
drCertNo	Varchar2(40)	N	医生证件号码	-
rxItemVal	Number(3)	N	明细上传数量	-
iptType	Varchar2(3)	Y	住院类别	住院病人时不允许为空
iptOpNo	Varchar2(40)	Y	住院/门诊号	住院病人时不允许为空
iptDeptCodg	Varchar2(40)	Y	住院科室编码	住院病人时不允许为空
iptDeptName	Varchar2(40)	Y	住院科室名称	住院病人时不允许为空
iptBegnDate	Varchar2(8)	Y	住院起始日期	住院病人时不允许为空
iptEndDate	Varchar2(8)	Y	住院截止日期	住院病人时不允许为空

dscgWay	Varchar2(3)	Y	离院方式	见字典定义 住院病人时不允许为空
iptDays	Number(3)	Y	住院天数	住院病人时不允许为空
birctrlType	Varchar2(3)	Y	计划生育手术类别	见字典定义 生育住院类别时必传
birmtid	Varchar2(3)	Y	生育类别(方式)	见字典定义 生育住院类别时必传
babyNum	Number(3)	Y	胎儿数	生育住院类别时必传
birctrlDate	Varchar2(8)	Y	计划生育手术或生育日期	生育住院类别时必传
prgDays	Number(3)	Y	怀孕天数	生育住院类别时必传
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容
chrgBehno	Varchar2(30)	N	收费批次号	见字典定义
psnSetlWay	Varchar2(2)	N	结算方式	见字典定义
psnNo	Varchar2(30)	N	人员编码	见字典定义
insuType	Varchar2(6)	N	险种类型	见字典定义
rxCircFlag	Varchar2(1)	Y	电子处方流转标志	1: 电子处方, 0 不是电子处方, 默认 0,
diseList	JSONArray	N	诊断或症状明细	见下方 diseList 定义
rxList	JSONArray	N	费用明细	见下方 rxList 定义
condList	JSONArray	Y	病情编码列表	见下方 condList 定义

extData 定义 (示例)

名称	类型长度	可空	说明	备注
crtChrgCnt	Number(3)	Y	本次收费次数	
crtRgstCnt	Number(3)	Y	本次挂号次数	

condList 定义

名称	类型长度	可空	说明	备注
condCodg	Varchar2(40)	N	病情编码	-
condName	Varchar2(40)	N	病情名称	-
mainCondDscr	Varchar2(1000)	N	主要病情描述	8包增加

diseList 定义

名称	类型长度	可空	说明	备注
diseDetlType	Varchar2(3)	Y	诊断类别	见字典定义
diseDetlSrtNo	Varchar2(3)	Y	诊断排序号	见字典定义
diseDetlCodg	Varchar2(40)	N	诊断或症状明细编码	-
diseDetlName	Varchar2(40)	N	诊断或症状名称	-

rxList 定义

名称	类型长度	可空	说明	备注
rxno	Varchar2(40)	N	处方号	-
rxDetlNo	Varchar2(40)	N	处方明细流水号	院内系统每条明细惟一标识
itemNo	Varchar2(40)	N	项目编号	医疗目录编码
medinsListCodg	Varchar2(150)	N	医药机构目录编码	
itemName	Varchar2(40)	N	项目名称	-
itemPric	Number(12,2)	N	项目单价	-
itemEmp	Varchar2(40)	N	项目单位	-
itemSpec	Varchar2(40)	N	项目规格	-
itemCnt	Int	N	项目数量	-
itemAmt	Number(12,2)	N	项目金额	-
prodBarc	Varchar2(40)	Y	商品条形码	-
drugFrqu	Varchar2(40)	Y	药品频率	-
drugDos	Varchar2(40)	Y	药品用量	-
drutDays	int	Y	药品天数	-
dosform	Varchar2(40)	Y	剂型	-
empMedcEmp	Varchar2(40)	Y	单位用药单位	-
drugTotlnt	Varchar2(40)	Y	取药总量	-
drugTotlntEmp	Varchar2(40)	Y	取药总量单位	-
drugDelvWay	Varchar2(40)	Y	给药途径	-
drugCntDays	int	Y	药量天数	-
drName	Varchar2(40)	Y	医生姓名	-
drCertNo	Varchar2(40)	Y	医生证件号码	-
rxDate	Varchar2(8)	Y	处方日期	-
rxTime	Varchar2(6)	Y	处方时间	
rsDeptCodg	Varchar2(40)	Y	处方科室编码	-
rsDept	Varchar2(40)	Y	处方科室	-
rxCircFlag	Varchar2(3)	N	外购处方标志	
acordDeptCodg	Varchar2(30)		受单科室编码	
acordDeptName	Varchar2(100)		受单科室名称	
ordersDrCode	Varchar2(30)		受单医生编码	
ordersDrName	Varchar2(50)		受单医生姓名	
hospApprFlag	Varchar2(3)	N	医院审批标志	
tcmdrugUsedWay	Varchar2(6)		中药使用方式	见字典
etipFlag	Varchar2(3)		外检标志	见字典
etipHospCode	Varchar2(30)		外检医院编码	见字典
dscgTkdrugFlag	Varchar2(3)		出院带药标志	见字典
matnFeeFlag	Varchar2(6)		生育费用标志	见字典
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求

				传不同数据内容
--	--	--	--	---------

4.2.3.2 响应出参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	医保结算中心订单号
payToken	Varchar2(40)	N	支付 token	下单支付使用
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.2.4 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

4.3 支付下单 (DLL)

4.3.1 接口概述

对已上传过费用明细的订单进行支付下单，医保结算中心返回一个支付 H5 收银台地址，医药机构打开收银台地址进行授权密码验证后可进行自费部分支付及医保部分报销。

4.3.2 请求方式

POST。

4.3.3 出入参说明

4.3.3.1 请求入参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	处方上传出参
payToken	Varchar2(40)	N	支付 token	
feeType	Varchar2(6)	N	费用类型	见字典
orgBizSer	Varchar2(40)	N	机构流水号	
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.3.3.2 请求出参

名称	类型长度	可空	说明	备注
cashierUrl	Varchar2(2000)	N	收银台地址	医保 H5 收银台地址，医药机构打开该地址完成医保支付业务
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.3.4 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

4.4 查询订单结算状态 (SDK)

4.4.1 接口描述

医药机构打开医保收银台 H5 之后，根据处方上传返回的 payOrdId 主动查询医保支付状态。

4.4.2 请求地址

/ordstat/query

4.4.3 请求方式

POST。

4.4.4 出入参说明

4.4.4.1 请求入参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	处方上传的出参订单号
orgCodg	Varchar2(40)	N	机构编号	原结算处方机构编号
payToken	Varchar2(40)	N	支付 token	授权的出参
ecAuthCode	Varchar2(64)	N	电子凭证授权码	ecAuthCode
ecChnlUserId	Varchar2(40)	N	电子凭证应用渠道用户 id	ecChnlUserId
ecChnlAppId	Varchar2(40)	N	电子凭证应用编号	ecChnlAppId

extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容
---------	------------	---	--------	------------------

4.4.4.2 响应出参

名称	类型长度	可空	说明	备注
ordStas	Varchar2(40)	N	订单状态	见订单状态字典
状态为 REFUND 时				
hiFefdSn	Varchar2(40)	Y	医保退费流水号	
hiTrnsDate	Varchar2(8)	Y	医保退费日期	
hiTrnsTime	Varchar2(6)	Y	医保退费时间	
appRefdSn	Varchar2(40)	Y	应用退款流水号	
状态为 SETTLED 时				
traceTime	Varchar2(40)	Y	交易时间	交易成功时间
ownpayAmt	Number(12,2)	Y	个人现金自付	-
psnAcctPay	Number(12,2)	Y	个人账户支付	-
fundPay	Number(12,2)	Y	其中基金支付	含商保
hiChrgTime	Varchar2(40)	Y	医保收费时间	
hiDocSn	Varchar2(40)	Y	医保交易流水号	
hiRgstSn	Varchar2(40)	Y	医保挂号流水号	
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求返回不同数据内容

4.4.5 SDK 方法

```

@Test
public void testQuery() {
    PmcClient client = new PmcClient(pmcReqUrl, appId, appSecret, appPrivateKey,
appPublicKey, serverPublicKey, signType, encType, version);
    MmpOrderQueryParamDTO paramDTO = new MmpOrderQueryParamDTO();
    paramDTO.setPayOrdId(payOrdId);
    paramDTO.setOrgCodg("000004");
    MmpOrderQueryResultDTO resultDTO = null;
    try {
        resultDTO = client.queryOrdStat(paramDTO);
        System.out.println(JSON.toJSONString(resultDTO));
    } catch (SDKException e) {
        //必须捕获这个异常, SDK 返回失败 (code != 0) 直接抛出
        System.out.println(e.getMessage());
    }
}

```

4.5 撤销费用明细上传 (DLL)

4.5.1 接口描述

医院对已经上传费用明细但未结算确认的费用进行撤销操作后可进行修改再次上传。

4.5.2 请求方式

POST。

4.5.3 出入参说明

4.5.3.1 入参说明

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	处方上传的出参订单号
orgCodg	Varchar2(40)	N	机构编号	原结算处方机构编号
payToken	Varchar2(40)	N	支付 token	授权的出参
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.5.3.2 出参说明

名称	类型长度	可空	说明	备注
success	boolean	N	回调通知结果	true/false

4.5.4 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

4.6 医保冲正 (SDK)

4.6.1 请求地址

/pmc/api/revs_set1

4.6.2 接口概述

医药机构接收到结算成功回调之后处理自费支付业务失败之后进行医保已收费业务费用冲正。

4.6.3 请求方式

POST。

4.6.4 出入参说明

4.6.4.1 请求入参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	处方上传的出参订单号
revsToken	Varchar2(40)	N	冲正 token	结算成功回调的出参
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.6.4.2 请求出参

名称	类型长度	可空	说明	备注
success	boolean	N	回调通知结果	true/false

4.6.5 SDK 方法

```
public void revsSetl() {
    try {
        PmcClient client = new PmcClient(pmcReqUrl, appId, appSecret, appPrivateKey,
            appPublicKey, serverPublicKey, signType, encType, version);
        RevsSetlParamDTO dto = new RevsSetlParamDTO();
        RevsSetlResultDTO retDto = client.revsSetl(dto);

    } catch (SDKException e) {
        //一定要捕获这个异常
        System.out.println(e.getMessage());
    }
}
```

4.7 医保退费(DLL)

4.7.1 接口概述

医药机构根据业务要求对已收费费用进行费用原路退回。

4.7.2 请求方式

POST。

4.7.3 出入参说明

4.7.3.1 请求入参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	处方上传的出参订单号
appRefdSn	Varchar2(40)	N	应用退款流水号	应用退费流水号
appRefdTime	Varchar2(40)	N	应用退费时间	yyyyMMddHHmmss
totlRefdAmt	Number(12,2)	N	总退费金额	原交易记录总金额
psnAcctRefdAmt	Number(12,2)	Y	医保个人账户支付	
fundRefdAmt	Number(12,2)	Y	基金支付	含商保
cashRefdAmt	Number(12,2)	N	现金退费金额	
ecToken	Varchar2(64)	N	电子凭证授权 Token	
refdType	Varchar2(40)	N	退费类型	ALL:全部, CASH:只退现金 HI:只退医保
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.7.3.2 响应出参

名称	类型长度	可空	说明	备注
refdSn	Varchar2(40)	N	结算中心流水号	
hiFefdSn	Varchar2(40)	N	医保退费流水号	现金退费不返回
hiTrnsDate	Varchar2(8)	N	医保退费日期	现金退费不返回
hiTrnsTime	Varchar2(6)	N	医保退费时间	现金退费不返回
refStatus	Varchar2(40)	N	退费状态	SUCC:成功 FAIL:失败 EXP:异常, 存在退医保及自费时有可能出现这个状态
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.7.1 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

4.8 支付结果推送

4.8.1 后端回调

4.8.1.1 接口描述

调用方：医保移动支付中心

接口提供方：两定机构

说明：医保结算成功之后，调用方主动向接口提供方发起结算结果通知，接口提供方把医保结算结果数据回写自己系统及完成自己系统内的结算确认，成功之后返回结算成功标识或结算失败标识。

4.8.1.2 请求地址

开通应用渠道接入时配置的回调地址。

4.8.1.3 请求方式

POST。

4.8.1.4 出入参说明

4.8.1.5 结算成功回调入参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	支付订单号	医保结算中心订单号
callType	Varchar2(40)	N	回调类型	见回调类型字典定义
medOrgOrd	Varchar2(40)	N	医院订单号	医院订单号
traceTime	Varchar2(40)	N	交易时间	交易成功时间
feeSumamt	number(12,2)	N	费用总金额	保留两位小数
ownpayAmt	Number(12,2)	N	个人现金自付	
psnAcctPay	Number(12,2)	N	个人账户支付	
fundPay	Number(12,2)	N	其中基金支付	
hiChrgTime	Varchar2(6)	N	医保收费时间	
hiDocSn	Varchar2(40)	N	医保交易流水号	

hiRgstSn	Varchar2(40)	N	医保挂号流水号	
orgName	Varchar2(40)	N	机构名称	
ecCode	Varchar2(200)	Y	电子凭证码值	
setlType	Varchar2(40)	N	结算类型	ALL:医保自费全部, CASH:只结现金 HI:只结医保
revsToken	Varchar2(40)	N	用于院内结算失败对医保的 冲正授权	1小时内有效
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求返回不同数据 内容

4.8.1.6 结算成功回调出

名称	类型长度	可空	说明	备注
success	boolean	N	回调通知结果	true/false
message	Varchar2(1000)	N	结果说明	

4.8.1.7 退款成功回调入参

名称	类型长度	可空	说明	备注
refdSn	Varchar2(40)		结算中心流水号	
hiFefdSn	Varchar2(40)		医保退费流水号	
hiTrnsDate	Varchar2(8)		医保退费日期	
hiTrnsTime	Varchar2(6)		医保退费时间	
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.8.1.8 退款成功回调出参

名称	类型长度	可空	说明	备注
success	boolean	N	回调通知结果	true/false
message	Varchar2(1000)	N	结果说明	

4.8.1.9 退款成功回调入参

名称	类型长度	可空	说明	备注
refdSn	Varchar2(40)	N	结算中心流水号	
refdType	Varchar2(40)	N	退费类型	ALL:全部, CASH:只退现金 HI:只退医保, 与请求 入参一致
hiFefdSn	Varchar2(40)	Y	医保退费流水号	只退现金时为空
hiTrnsDate	Varchar2(8)	Y	医保退费日期	只退现金时为空
hiTrnsTime	Varchar2(6)	Y	医保退费时间	只退现金时为空
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.8.1.10 退款成功回调出参

名称	类型长度	可空	说明	备注
success	boolean	N	回调通知结果	true/false
message	Varchar2(1000)	N	结果说明	

4.8.2 前端回调

4.8.2.1 接口描述

数据加密方：医保移动支付中心

调用方：移动渠道应用系统

说明：医保结算中心在完成授权、预结算或结算确认之后，需要通知调用方结果数据，数据加密方会把需要给到调用方的数据进行加密，通知到事先配置好的前端回调地址，前端回调参数 signData 使用 SM4，需要调用方自行使用申请接入时分配的密钥解密。

4.8.2.2 请求地址

开通应用渠道接入时配置的回调地址。

4.8.2.3 请求方式

前端重定向。

4.8.2.4 支付成功回调

重定向地址：预结算成功回调入参的 forntCallUrl

forntCallUrl 示例：<https://地址/abc?encData=encData>

拼上下表参数数据加密后数据放在 callData 里进行回调

示例：forntCallUrl&callData=callData

名称	类型长度	可空	说明	备注
payChnlName	Varchar2(40)	N	支付渠道名称	
payChnlSer	Varchar2(40)	N	支付渠道流水号	
revsToken	Varchar2(40)	N	冲正 token	
payTime	Varchar2(40)	N	支付时间	yyyyMMddHHmmss
payOrdId	Varchar2(40)	N	支付订单号	处方上传的出参订单号
code	int	N	结算成功标识	0 表示成功，其他失败

4.9 对账文件文件下载

4.9.1 接口地址

/pmc/api/down/bill

4.9.2 接口描述

通过该接口，可下载指定两定机构指定日期的交易数据

前置条件：下载对应账单日期的数据需要在当地清算行提交了全部的对账文件之后可下载

4.9.3 请求方式

POST。

4.9.4 出入参说明

4.9.4.1 请求入参

名称	类型长度	可空	说明	备注
orgCodg	Varchar2(40)	N	机构编码	医保分配
billDate	Varchar2(40)	N	账单日期	要下载对账单的日期，格式 yyyyMMdd

4.9.4.2 响应出参

名称	类型长度	可空	说明	备注
payOrdId	Varchar2(40)	N	平台流水号	支付中台订单号，费用上传时的出参
medOrgOrd	Varchar2(40)	N	医疗机构订单号	院内产生惟一流水，费用上传时传入流水号
chnlSn	Varchar2(40)	Y	渠道流水号	现金支付金额为零时，可为空
mertNo	Varchar2(40)	Y	商户号	医院在对应渠道开的结算商户号，现金支付金额为零时，可为空
ordStas	Varchar2(40)	N	订单状态	见订单状态字典
psnAcctPay	Number(12,2)	N	个账支出金额	保留两位小数，单位元
fundPay	Number(12,2)	N	基金支出金额	保留两位小数，单位元
cashPayAmt	Number(12,2)	N	现金支付金额	保留两位小数，单位元
feeSumamt	Number(12,2)	N	交易总金额	保留两位小数，单位元
trnsDate	Varchar2(40)	N	交易时间	格式：“YYYY-MM-DD HH:MI:SS”，支付中台交易时间

chnlTrnsDate	Varchar2(40)	Y	渠道交易时间	格式：“YYYY-MM-DD HH:MI:SS”， 现金支付金额为零时，可为空
chnlPayAmt	Number(12, 2)	Y	渠道支付金额	单位分，现金支付金额为零时，可为空
chnlName	Varchar2(40)	Y	渠道名称，如 CCB 等	现金支付金额为零时，可为空
payChnl	Varchar2(3)	Y	支付渠道，如建行等	现金支付金额为零时，可为空
oriAppRefdSn	Varchar2(40)	Y	原应用退款流水号	退费时传入，交易状态为退费时不为空

4.10 参保人员信息查询(DLL)

4.10.1 接口地址

/pmc/api/hos/query_insu_info

4.10.2 接口概述

向医保获取用户的参保信息，以便费用预结算和结算的时候能够请求到对应的医保系统处理。

4.10.3 请求方式

POST。

4.10.4 出入参说明

4.10.4.1 请求入参

名称	类型长度	可空	说明	备注
orgCodg	Varchar2(40)	Y	医保机构编号（医保局分配）	
medType	Varchar2(40)	Y	诊断类别	见字典定义
ecToken	Varchar2(40)	N	电子凭证授权 token	医保核心系统核验电子凭证身份
idNo	Varchar2(40)	N	证件号码	
userName	Varchar2(40)	N	用户姓名	
idType	Varchar2(3)	N	证件类型	见字典定义
insuCode	Varchar2(6)	Y	统筹区编码	参保人所在统筹区编码
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.10.4.2 响应出参

名称	类型长度	可空	说明	备注
acctBalc	Number (12, 2)	N	个人账户余额	
insuStatus	Varcahr2 (6)	N	参保状态	0 表示状态正常可进行医保支付,其他表示不允许医保支付
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容
参保险种<insuList>开始				
insuOptins	Varchar2 (40)	Y	参保所属机构	
insuType	Varchar2 (40)	Y	险种	见字典定义
psnType	Varchar2 (8)	Y	人员类别	见字典定义
insuTrtStatus	Varchar2 (6)	Y	医保待遇状态	见字典定义
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容
特殊病种登记信息<condList>开始				
insuType	Varchar2 (3)	Y	险种	见字典定义
condCodg	Varchar2 (40)	Y	疾病编号	
condName	Varchar2 (40)	Y	疾病名称	
orgCodg	Varchar2 (40)	Y	医药机构编码	
hiPayQuota	Number (12, 4)	Y	医保支付限额	
curTolQuota	Number (12, 4)	Y	当前累计额度	
begnTime	Varchar2 (8)	Y	开始时间	
endTime	Varchar2 (8)	Y	结束时间	
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容
异地就医登记信息<mdtrtprovList>开始				
insuType	Varchar2 (3)	Y	险种	见字典定义
poolarea	Varchar2 (6)	Y	统筹区	
poolareaName	Varchar2 (40)	Y	统筹区名称	
trafoutMedinsName	Varchar2 (100)	Y	转出医疗服务机构名称	
outFilType	Varchar2 (3)	Y	异地备案类型	
begnTime	Varchar2 (8)	Y	开始时间	
endTime	Varchar2 (8)	Y	结束时间	
extData	JSONObject	Y	医保扩展数据	根据各地方医保要求传不同数据内容

4.10.5 DLL 方法

参见《医保移动支付中心与医药机构端数据交互规范》。

附录 1 安全规范

1.1 签名算法 (SM2)

1.1.1 概述

根据 SM2 算法，签名报文。通过对报文数据筛选、排序和拼接，组成待签名报文数据。

1.1.2 请求参数签名

1.1.2.1 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 signData、encData、extra 字段。

1.1.2.2 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。

1.1.2.3 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 appSecret 在“…参数=参数值…”后，此时生成的字符串为待签名字符串，将待签名字符串 SM2 运算，即是签名（signData）的值。（“signData”、“encData”、“extra”参数不参与签名）。

JSON 对象签名规范（如 data）： 内部按字母顺序升序排列 空值不参与签名 将整理好的 JSON 内容，输出 JSON 字符串后拼接参与签名，例如下面的示例请求报文，参数值都是示例，开发者仅参考报文格式即可。

加签报文示例：

```
{
  "appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB",
  "data": {"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "appUserId": "o8z4C5avQXqC0aWFPf1Mzu6D7W
CQ_bd", "idNo": "350181199011193519", "idType": "01", "phoneNumber": "13763873033", "userName": "
测试"},
  "encType": "SM4",
  "signData": "URVQNdVnN5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJup
HRGmyO5w==",
  "signType": "SM2", "timestamp": "20200207175759",
  "transType": "ec. gen. index",
  "version": "1.0.0"
```

```
}
```

组成的待签名字符串：

```
appId=43AF047BBA47FC8A1AE8EFB232BDBBCB&data={"appId":"43AF047BBA47FC8A1AE8EFB232BDBBCB","appUserId":"o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd","idNo":"350181199011193519","idType":"01","phoneNumber":"13763873033","userName":"测试"}&encType=SM4&signType=SM2&timestamp=20200207175759&transType=ec.gen.index&version=1.0.0&key=4117E877F5FA0A0188891283E4B617D5
```

1.1.2.4 签名结果

使用各自语言对应的 SM2 签名函数，对拼接得出的待签名字符串使用私钥进行 SM2 签名后，再将字节码进行 Base64 编码，即是签名结果，如签名结果。

签名结果示例：

```
URVQNdVnN5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHRGmy05w=
```

1.1.3 返回参数验签

1.1.3.1 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 signData、encData、extra 字段。

1.1.3.2 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。

1.1.3.3 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 appSecret 在“…参数=参数值…”，此时生成的字符串为待签名字符串，将待签名字符串 SM2 运算，即是签名（signData）的值。（“signData”、“encData”、“extra”参数不参与签名）。

请求报文示例：

```
{  
  "appId":"43AF047BBA47FC8A1AE8EFB232BDBBCB",  
  "data":{"appId":"43AF047BBA47FC8A1AE8EFB232BDBBCB","appUserId":"o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd","idNo":"350181199011193519","idType":"01","phoneNumber":"13763873033","userName":"测试"},  
  "encType":"SM4",
```

```
"signData": "URVQNdVn5mz2EhKZhLT1XNwAWTSncFoSe8I1x7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJup  
HRGmyO5w==",  
"signType": "SM2", "timestamp": "20200207175759",  
"transType": "ec. gen. index",  
"version": "1.0.0"  
}
```

组成的待签名字符串:

```
appId=43AF047BBA47FC8A1AE8EFB232BDBBCB&data={"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "a  
ppUserId": "o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd", "idNo": "350181199011193519", "idType": "01", "pho  
neNumber": "13763873033", "userName": "测试"}  
&encType=SM4&signType=SM2&timestamp=20200207175759&transType=ec. gen. index&version=1.0.0&ke  
y=4117E877F5FA0A0188891283E4B617D5
```

1.1.3.4 签名结果

使用对应的 SM2 验签函数，对拼接得出的待签名字符串使用公钥进行 SM2 进行验签，对比验签内容的签名与返回报文里的 signData 字段比较是否验签通过。

1.2 加密算法 (SM4)

1.2.1 概述

根据 SM4 加密算法，加密报文。通过对报文数据筛选、排序和拼接，组成待加密报文数据。

1.2.2 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

加密报文示例:

```
{  
"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB",  
"data": {"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "appUserId": "o8z4C5avQXqC0aWFPf1Mzu6D7W  
CQ_bd", "idNo": "350181199011193519", "idType": "01", "phoneNumber": "13763873033", "userName": "  
测试"},  
"encType": "SM4",
```

```
"signData": "URVQNdvNn5mz2EhKZhLT1XNwAWTSncFoSe8I1x7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJup  
HRGmyO5w==",  
"signType": "SM2", "timestamp": "20200207175759",  
"transType": "ec.gen.index",  
"version": "1.0.0"  
}
```

2、将 data 字段值，转换为 JSON 字符串 jStr

待加密串示例：

```
{"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "appUserId": "o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd",  
"idNo": "350181199011193519", "idType": "01", "phoneNumber": "13763873033", "userName": "测试"}
```

3、根据 SM4 加密算法，加密报文。通过对报文数据筛选、排序和拼接，组成待加密报文数据（补充：传入 sm4 加密算法长度密钥为 32 位，实际底层算法密钥应用长度为前 16 位）报文加密密钥示例：

```
Varchar2 newPassword=SM4Util.encryptCbc(appId, appSecret).subVarchar2(0, 32).toUpperCase();  
  
//appSecret 待加密内容  
  
//appId 密钥
```

4、根据 encType 声明加密算法 SM4，使用 3 获得的报文加密密钥，截取 newPassword 前 32 位作为 SM4 密钥，如 newPassword.subVarchar2(0, 32)加密 jStr 字符串（补充：传入 sm4 加密算法密钥长度为 32 位，实际底层算法密钥应用长度为前 16 位），并将加密结果转换为大写，获得加密密文 encData

密文示例：

```
4470B6B96A8E0BADA051A318E6B6FBED66B9FC5AB2A4A3C66FDDD3C70BCADD6EF526AB57DC1DC916385CEF3484  
3AABFCBAF8F1FDEA9DC51A2A56AB3EA3E170201E4EDD3137D6D1BA6A4A773F6F4872A718F56742E5052AD1C04E  
99C91EA048990F06A96E6E1E534E40BD28DFDC20ACA03CAE0DFE0DE5229EDADBD27BBD32DD4C3F9ADC833CD3C  
F01CD012CE1799BB6F
```

5、将加密结果 encData，赋值 encData，并清空 data 明文 JSON，将 encData 放入 data，将新获取报文发送服务器。

加密请求报文示例：

```
{  
"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB",  
"encData": "64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBC6AB7914898A23A9"
```

```
9C97EBEFE5277247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E06B08E
151362301659FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB736BA3BB98F
3540962552F40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D63B2D387A87F
42130F0D47B9445F9D729566FE183F9A959",
"encType": "SM4",
"signData": "URVQNdvNn5mz2EhKZhLTIXNwAWTSncFoSe8I1x7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJup
HRGmyO5w==",
"signType": "SM2",
"timestamp": "20200207175759",
"transType": "ec. gen. index",
"version": "1.0.0"
}
```

6、返回报文解密

响应报文示例：

```
{
"encData": "64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBC6AB7914898A23A9
9C97EBEFE5277247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E06B08E
151362301659FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB736BA3BB98F
3540962552F40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D63B2D387A87F
42130F0D47B9445F9D729566FE183F9A959"
,
"encType": "SM4",
"respCode": "0",
"respMsg": "处理成功",
"signData": "
OTkOMUYwREIyODk1RDhDRDQ5NjQzRTU1RENCNOZGMzdCRUY4MzFFNDMxMTM1OTY0MEM1MDk3NOE4REE2Nzk2QQ==",
"signType": "SM2",
"timestamp": "20161226093147927"
}
```

加密密文数据 enctData 示例:

```
64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBC6AB7914898A23A99C97EBEFE52
77247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E06B08E15136230165
9FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB736BA3BB98F3540962552F
40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D63B2D387A87F42130F0D47B
9445F9D729566FE183F9A959
```

7、根据 encType 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，即获得报文解密密钥

解密密钥示例:

```
Varchar2 newPassword = SM4Util.encryptCbc(appId, appSecret).subVarchar2(0,
32).toUpperCase();

//appSecret 待加密内容

//appId 密钥
```

8、根据 encType 声明加密算法，使用 3. 获取的报文解密密钥，解密 enctData 获取 JSON 字符串明文 jStr 明文示例:

```
{"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "appId": "o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd",
"idNo": "350181199011193519", "idType": "01", "phoneNumber": "13763873033", "userName": "测试"}
```

9、将 jStr 转换为 JSON 赋值 data，获取解密后返回报文

设置明文示例:

```
{
  "data": {"appId": "43AF047BBA47FC8A1AE8EFB232BDBBCB", "appId": "o8z4C5avQXqC0aWFPf1Mzu6D7W
CQ_bd", "idNo": "350181199011193519", "idType": "01", "phoneNumber": "13763873033", "userName": "
测试"},
  "encType": "SM4",
  "respCode": "0",
  "respMsg": "处理成功",
  "signData": "
OTkOMUYwREIyODk1RDhDRDQ5NjQzRTU1RENCNOZGMzdCRUY4MzFFNDMxMTM1OTYOMEM1MDk3NOE4REE2Nzk2QQ==",
  "signType": "SM2",
```

```
"timestamp": "20161226093147927"
```

```
}
```