YB

医保网络安全和信息化标准

福建医疗保障平台

商业补充医疗保险接入标准规范

修订版 1.7

技术支持：易联众信息技术股份有限公司

变更记录

序号	日期	更改内容	版次	起草人或修订人	医保经办/对接
1	2021/11/01	修订稿	V0.1	颜荣华	黄栋雄
2	2021/11/06	修订稿：支付流程优化，增加对账接口等	V0.2	颜荣华	黄栋雄
3	2021/11/16	修订稿：新增查询对账明细接口，新增异步通知参数定义，新增结算接口部分字段等	V0.3	卢灿鹏	
4	2021/11/17	修订稿：明细对账新增分页相关字段	V0.4	卢灿鹏	
5	2021/11/19	修订稿：明细对账字段调整，异步回调新增第三方流水号等	V0.5	卢灿鹏	
6	2021/12/02	字典修改及字段确认	V0.6	卢灿鹏	
7	2021/12/04	错误编码补充	V0.7	卢灿鹏	
8	2021/12/14	地市编码补充	V0.8	卢灿鹏	
9	2022/05/11	返回参数优化和部分业务流程调整	V0.9	卢灿鹏	
10	2023/02/27	CI00.02.00.01 新增 sub_his_pay_no 子订单号， CI00.02.00.02 回参信息 setId 字段	V1.1	卢灿鹏	
11	2023/03/15	去掉 CI00.02.00.05， CI00.02.00.06 接口 新增 CI00.02.00.08 明细对账 新增 CI00.02.00.09 总对账	V1.2	卢灿鹏	
12	2023/06/15	明细对账接口（ CI00.02.00.0）外围新增人员证件号限定	V1.3	卢灿鹏	
13	2023/10/31	调整回参三要素，支付，退款新增用户 id 等	V1.4	卢灿鹏	黄栋雄
14	2024/07/08	资格校验接口新增 CI00.01.00.03 新增 companyName 基层医保区划名称（街道信息），insutypeName 参保类型	V1.6	卢灿鹏	
15	2024/09/25	CI00.02.00.08 回参描述调整	V1.7	卢灿鹏	

目录

1 范围

本文档主要表述福建医疗保障平台与有关第三方平台进行商业补充医疗保险（如惠闽保等）相关数据交互的标准服务接口出入参调用示例、业务流程及接口交互安全规范等。

2 使用对象

服务使用者：可能是企业、定点机构、社会组织、公共事业单位等。

服务提供者：可能是社会组织、公共事业单位、应用开发商、其它服务提供商、平台运维商、城市管理部门。

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	SM3
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 公共参数说明

3.2.1.1 请求共通报文结构

接口请求时，需根据渠道接入平台的安全等级配置，增加以下参数。

序号	参数代码	参数名称	数据类型	必填	说明
1	chs_fjs_appid	渠道 id	varchar(20)	Y	医保分配固定值
2	chs_fjs_appsecret	渠道私钥	varchar(100)	N	医保分配固定值
3	chs_fjs_token	渠道 token	varchar(100)	N	请求时携带的动态令牌，详细方法请参考安全规范-渠道认证-授权码模式

4	chs_fjs_funid	服务编号	varchar(20)	Y	平台分配的统一管理服务编号
5	chs_fjs_timestamp	请求时间戳	Integer	N	精确到毫秒（ms）
6	chs_fjs_encdata	请求加密数据串	varchar(max)	N	请求数据需要校验签名，详细方法请参考安全规范-签名算法
7	chs_fjs_sign	请求签名数据串	varchar(100)	N	请求数据需要校验签名，详细方法请参考安全规范-加密算法

3.2.1.2 响应共通报文结构

序号	参数代码	参数名称	数据类型	必填	说明
1	chs_fjs_timestamp	请求时间戳	Integer	N	精确到毫秒（ms）
2	chs_fjs_encdata	请求加密数据串	varchar(max)	N	接收数据需要校验签名，详细方法请参考安全规范-签名算法
3	chs_fjs_sign	请求签名数据串	varchar(100)	N	接收数据需要校验签名，详细方法请参考安全规范-加密算法

3.2.2 数据字典

3.2.2.1 加解密方式（encType）

类别代码	类别说明	备注
SM4	国密 SM4 算法	
RSA	RSA 算法	
PKCS7	PKCS7 算法	
AES	AES 算法	

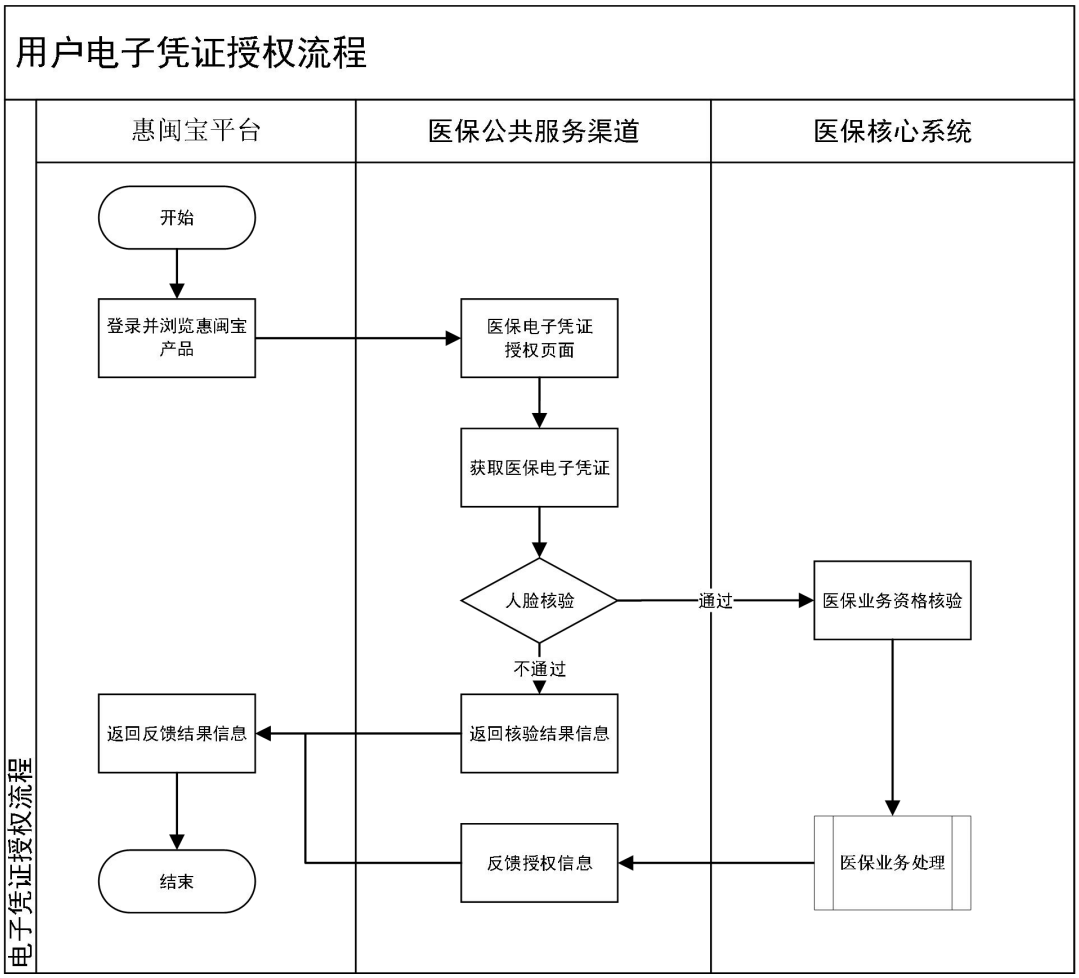
3.2.2.2 签名方式（signType）

类别代码	类型说明	备注
SM3	国密 SM3 算法	
MD5	MD5 算法	
RSA	RSA 算法	

4 应用接入说明

4.1 业务流程图

4.1.1 用户电子凭证授权流程



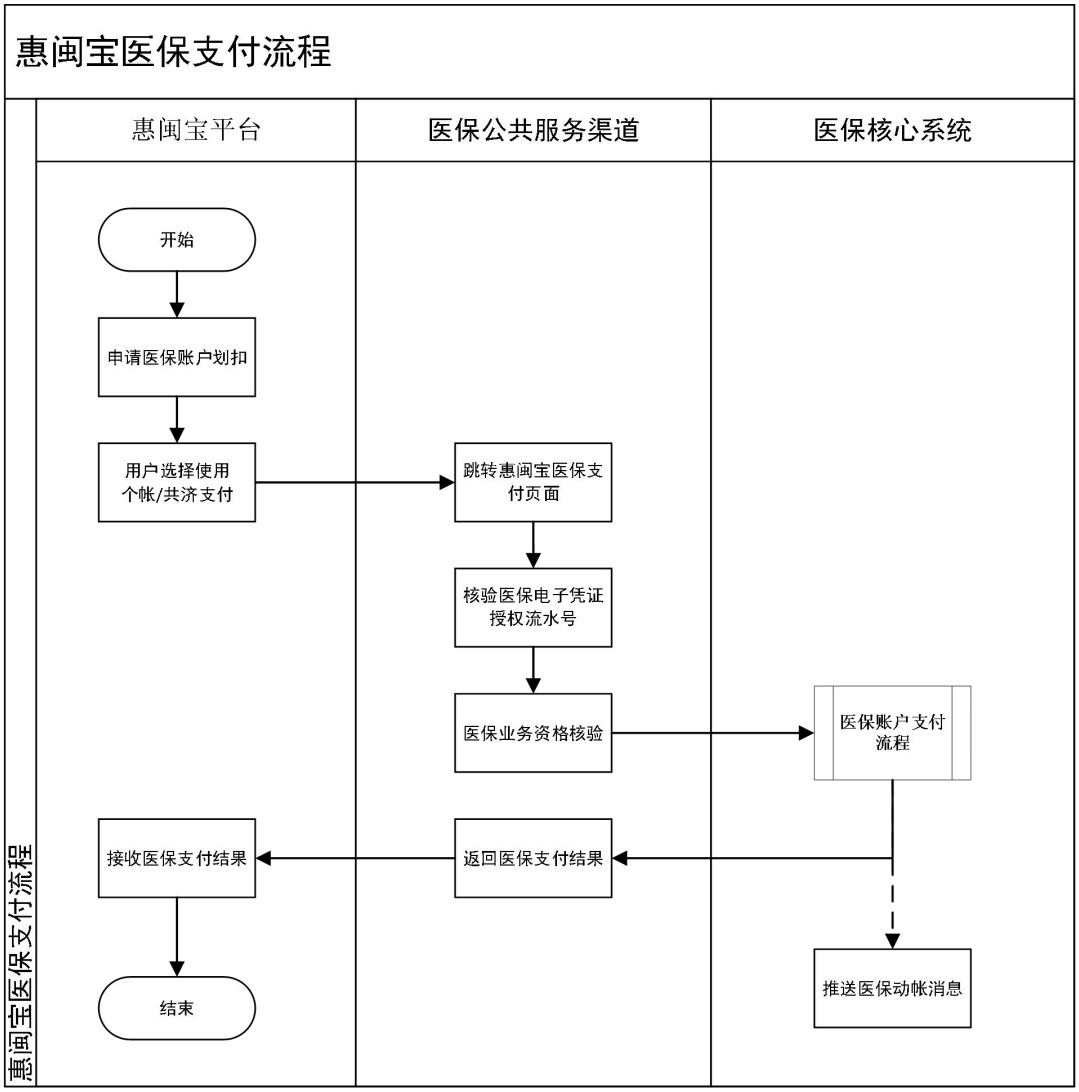
流程说明:

1、用户登录并浏览惠闽保产品时，通过接入医保电子凭证授权服务进行过医保在线服务授权。

2、先获取用户医保电子凭证，进行人脸核验，若用户人脸通过，则进行医保业务资格核验（用户待遇资格核验，共济关系是否正常等）。

3、医保业务处理，后返回反馈授权信息给第三方平台，授权流程结束。

4.1.2 惠闽保医保支付流程



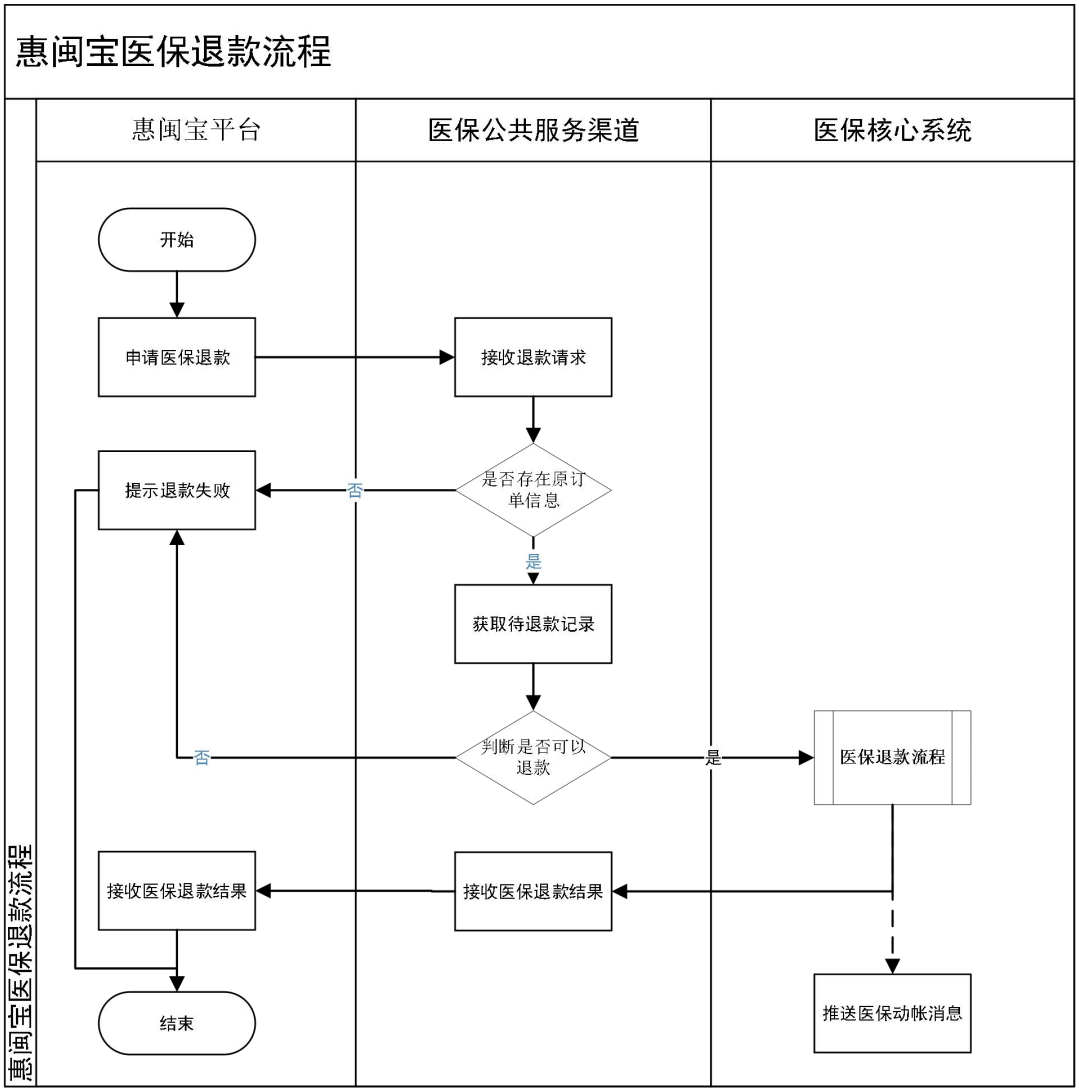
流程说明:

1、用户申请医保账户划扣申请，选择使用个人账户支付/家庭共济支付方式。

2、 跳转惠闽保医保支付页面， 医保核验医保电子凭证授权信息，发起医保业务资格核验（进行业务授权号核验、共济关系核验等），核验成功后，进行医保账户支付流程。

3、医保账户支付成功后，返回医保支付结果，同时异步推送医保支付结果消息给各参保人。

4.1.3 惠闽保医保退款流程



流程说明:

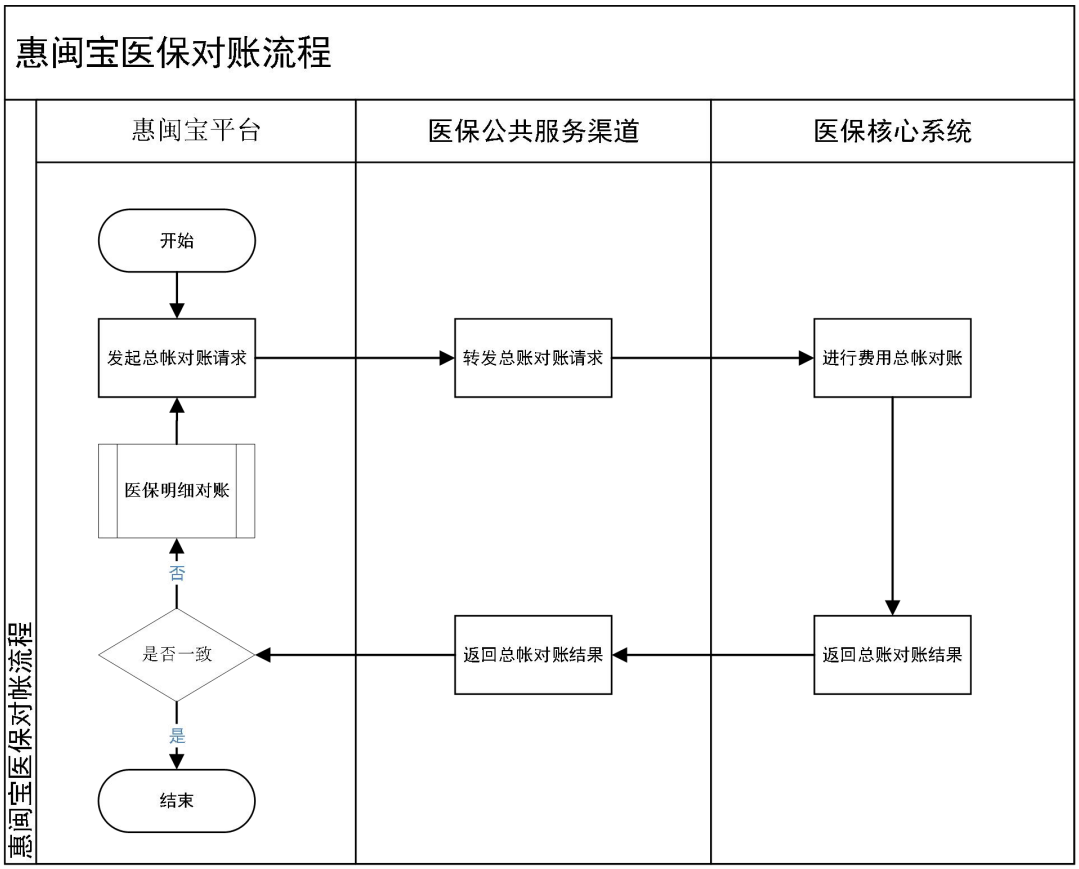
1、用户申请医保退款。

2、医保接收到医保退款请求后，判断是否存在原订单信息，不存在则直接提示失败。

3、存在订单信息，获取待退款记录，并判断是否可以退款，不能退款则提示退款失败

4、若可以退款，发起医保退款流程，返回医保退款结果，同时异步推送医保动帐结果消息给各参保人。

4.1.4 惠闽保医保对账流程



流程说明:

1、机构发起总帐对账请求，医保核心系统进行费用总帐对账，返回对账结果给机构。

2、机构核对总账是否一致，若不一致，则发起医保明细对账。

3、明细帐核对完成后，再次发起总帐对账请求，直至总账对账完成。

4.2 服务鉴权

4.2.1 获取医保在线服务授权页面表单 CI00.01.00.01

逻辑：根据获取信息获取页面表单

返回地址会附带令牌 authcode，用来查询医保用户信息

令牌 authcode90 天内有效，若支付完成，令牌失效，只能用于退款操作。

如果重复授权，旧令牌则失效。以新令牌为准。

存在多人时，授权列表用户只有同一个家庭网人员才会授权成功。

请求参数

名称	描述	类型	必填	备注
appid	应用编号	String	Y	固定分配
service_id	服务编号	String	Y	固定分配
org_code	第三方平台编号	String	Y	固定分配
user_id	惠闽保的用户唯一码	String	Y	
name	申请人姓名	String	Y	
idcard	申请人证件号	String	Y	
cert_type	申请人证件类型	String	Y	
phone	申请人手机号	String	Y	
redirect_url	回调地址	String	Y	授权成功后，回调返回鉴权令牌
fail_url	失败回调地址	String	N	
url_type	回调地址类型	String	Y	1、微信 h5 2、微信小程序 3、支付宝小程序 4、闽政通 5、支付宝 h5 6、i 厦门 7、莆田惠闽保 8、e 福州
被投保人列表 paylist				
name	姓名	String	Y	
idcard	证件号	String	Y	
cert_type	证件类型	String	Y	
phone	手机号	String	N	
hser_rlts	与共济户主的关系	String	Y	见附录《共济关系》
被投保人列表 paylist				

响应参数

名称	描述	类型	必填	备注
link_url	生成链接地址	String	Y	通过调用该地址，医保唤起相应渠道的医保电子凭证校验

返回码

返回码	描述	说明

注: 1、如果使用小程序, 见小程序跳转 见《附录 2 应用跳转》

4.2.2 根据授权令牌获取用户医保信息- CI00.01.00.02

逻辑：查询授权情况，返回失败成功授权人员信息

请求参数

名称	描述	类型	必填	备注
auth_code	用户授权令牌	String	Y	4.2.1 回调地址携带的令牌，有效期内可多次调用

响应数据

名称	描述	类型	必填	备注
用户信息 userlist				
treatment_type	参保状态	String	Y	
insurance_type	险种类型	String	Y	
insurance_type_name	险种类型名称	String	Y	
is_family	是否共济关系	String	Y	只返回投保人的
auth_psn	授权人标识	String	Y	1 是 0 否
isSuccess	授权是否成功	String	Y	1 成功 0 失败
failMsg	失败原因	String	N	
failCode	错误码	String	N	
user_id	用户 id	String	Y	通过国密加密，第三方进行私钥解密，加密串包含身份证，姓名，证件类型
用户信息 userlist				

4.2.3 获取用户是否参保- CI00.01.00.03

逻辑：查询用户是否参保

查询福建省参保信息。

请求参数

名称	描述	类型	必填	备注
用户信息 userlist				
name	姓名	String	Y	
idcard	证件号	String	Y	
cert_type	证件类型	String	Y	
region	参保行政区划	String	N	
用户信息 userlist				

响应数据

名称	描述	类型	必填	备注
结果 list				
region	参保行政区划	String	Y	
is_insu	是否参保	String	Y	1=是，0=否
user_id	用户 id	String	Y	通过国密加密，第三方进行私钥解密，加密串包含身份证，姓名，证件类型
companyName	基层医保区划名称（街道信息）	String	N	有居民参保才会返回
insutypeName	参保类型	String	Y	

结果 list

5 接口规范

5.1 医保交易

5.1.1 获取医保支付划扣页面表单- CI00.02.00.01

逻辑：通过相关入参获取支付页面
分为共济支付和个账支付。
共济支付如果人员信息不在一个家庭网，则整笔支付失败。
共济余额不足，则整笔支付失败。

请求参数

名称	描述	类型	必填	备注
appid	应用编号	String	Y	
service_id	服务编号	String	Y	
org_code	第三方平台编号	String	Y	
user_id	惠闽保的用户唯一码	String	Y	
auth_code	业务授权流水号	String	Y	
hi_pay_no	第三方平台支付流水号	String	Y	长度 32
hi_pay_date	实际支付时间	String	Y	
medfee_sumamt	医保支付总金额	String	Y	
pay_kind	结算方式	String	Y	1=个帐支付，2=共济支付
redirect_url	支付回调地址	String	Y	医保支付成功后，回调返回医保结算数据 code
notify_url	异步回调通知地址	String	N	
url_type	回调地址类型	String	Y	1、微信 h5 2、微信小程序 3、支付宝小程序 4、闽政通 5、支付宝 h5
fail_url	支付失败回调地址	String	Y	
代扣信息 paylist				
name	姓名	String	Y	
idcard	证件号	String	Y	
cert_type	证件类型	String	Y	
region	参保行政区划	String	Y	
pay_amt	划扣金额	String	Y	
sub_his_pay_no	子订单号	String	Y	新增

代扣信息 paylist

响应数据

名称	描述	类型	必填	备注
link_url	唤起支付返回页面	String	Y	回传 code 参数

5.1.2 获取医保结算结果- CI00.02.00.02

逻辑：通过结算 code 获取支付情况。

请求参数

名称	描述	类型	必填	备注
code	医保结算回传 code	String	Y	

响应数据

名称	描述	类型	必填	备注
auth_code	业务授权流水号	String	Y	
pay_no	医保支付流水号	String	Y	长度 64
hi_pay_no	第三方平台支付流水号	String	Y	
pay_date	实际医保支付时间	String	Y	
pay_kind	结算方式	String	Y	1=个帐支付，2=共济支付
medfee_sumamt	医保支付总金额	String	Y	
代扣信息 paylist				
region	参保行政区划	String	Y	
pay_amt	划扣金额	String	Y	
acct_pay	个人账户支付金额	String	Y	
acct_mulaid_pay	家庭共济账户支付	String	Y	
psn_cash_pay	个人现金支出	String	Y	
pay_result	结算结果	String	Y	1 成功 0 失败
failMsg	支付异常信息	String	N	支付成功为空
failCode	错误码	String	N	支付成功为空
setId	医保支付 id	String	Y	第三方后续对账用
user_id	用户 id	String	Y	通过国密加密，第三方进行私钥解密，加密串包含身份证，姓名，证件类型
代扣信息 paylist				

5.1.3 医保支付退款- CI00.02.00.03

逻辑：根据订单信息进行退款操作

请求参数

名称	描述	类型	必填	备注

auth_code	业务授权流水号	String	Y	
pay_no	医保支付流水号	String	Y	
hi_refund_no	第三方平台退款流水号	String	Y	
hi_refund_date	惠闽保退款时间	String	Y	
refund_amt	退款总金额	String	Y	
退款信息 paylist				
name	姓名	String	Y	
idcard	证件号	String	Y	
cert_type	证件类型	String	Y	
region	参保行政区划	String	Y	
refund_amt	退款金额	String	Y	
退款信息 paylist				

响应数据

名称	描述	类型	必填	备注
hi_refund_no	第三方平台退款流水号	String	Y	
pay_no	医保支付流水号	String	Y	
refund_no	医保退款流水号	String	Y	
refund_date	医保退款时间	String	Y	
refund_amt	退款总金额	String	Y	
paylist	退款信息	List	Y	
paylist 开始				
pay_amt	退款金额	String	Y	
setId	医保退款 id	String	Y	明细对账用
region	地市	String	Y	
user_id	用户 id	String	Y	通过国密加密，第三方进行私钥解密
paylist 结束				

5.1.4 单笔结算单查询- CI00.02.00.04

逻辑：查询单笔结算数据

请求参数

名称	描述	类型	必填	备注
appid	应用编号	String	Y	
service_id	服务编号	String	Y	
org_code	第三方平台编号	String	Y	
pay_no	医保支付流水号	String	N	两选一
hi_pay_no	第三方平台支付流水号	String	N	两选一

响应数据

名称	描述	类型	必填	备注
hi_pay_no	第三方平台支付流水号	String	Y	
pay_no	医保支付流水号	String	Y	
pay_date	实际医保支付时间	String	Y	
代扣信息 paylist				
is_use_pay	是否使用医保支付	String	Y	
pay_stat	订单状态	String	Y	1=支付，2=退款
pay_amt	账单金额	String	Y	
acct_pay	个人账户支付金额	String	Y	
acct_mulaid_pay	家庭共济账户支付	String	Y	
psn_cash_pay	个人现金支出	String	Y	
hi_refund_no	第三方平台退款流水号	String	N	
refund_no	医保退款流水号	String	N	
refund_date	医保退款时间	String	N	
refund_amt	退款金额	String	Y	
user_id	用户 id	String	Y	通过国密加密，第三方进行私钥解密，加密串包含身份证，姓名，证件类型
代扣信息 paylist				

5.1.1 明细对账- CI00.02.00.08

请求参数

名称	描述	类型	必填	备注
appid	应用编号	String	Y	
service_id	服务编号	String	Y	
org_code	第三方平台编号	String	Y	
stmt_begndate	对账开始日期	String	Y	yyyy-MM-dd
stmt_enddate	对账结束日期	String	Y	yyyy-MM-dd
idcard	证件号	String	N	有传明细信息会限制此人员的，没有传明细信息是对账开始日期-对账结束日期所有人的订单信息
setlDDTOList	医保结算明细信息	List		
setlDDTOList				
setlId	医保支付/退款 id	String	Y	
pay_amt	划扣金额	String	Y	退款的传负数
acct_pay	个人账户支付金额	String	Y	退款的传负数

acct_mulaid_pay	家庭共济账户支付	String	Y	退款的传负数
psn_cash_pay	个人现金支出	String	Y	
name	姓名	String	Y	
idcard	证件号	String	Y	
hi_pay_no	第三方平台支付/退款流水号	String	Y	
setlDDTOList				

响应数据

名称	描述	类型	必填	备注
返回 data 数组				
setlId	医保支付/退款 id	String	Y	
stmtRslt	对账结果	String	Y	0 平 1 不平 101 中心多 102 机构多 103 数据不一致
memo	备注	String	Y	

5.1.1 总对账- CI00.02.00.09

请求参数

名称	描述	类型	必填	备注
appid	应用编号	String	Y	
service_id	服务编号	String	Y	
org_code	第三方平台编号	String	Y	
stmt_begndate	对账开始日期	String	Y	yyyy-MM-dd
stmt_enddate	对账结束日期	String	Y	yyyy-MM-dd
pay_amt	划扣金额	String	Y	总额
acct_pay	个人账户支付金额	String	Y	总额
acct_mulaid_pay	家庭共济账户支付	String	Y	总额
psn_cash_pay	个人现金支出	String	Y	总额
fixmedins_setl_cnt	结算笔数	String	Y	

响应数据

名称	描述	类型	必填	备注
memo	备注	String	Y	
stmtRslt	对账结果	String	Y	0 平 1 不平 101 中心多 102 机构多 103 数据不一致

5.2 异步回调

请求方式 post 数据格式为 json，对方提供内网接口，并采用一定的加密方式

Json 数格式如下：

名称	描述	类型	必填	备注
medfee_sumamt	医保总支付	String	Y	
acct_pay	个账支付	String	Y	
acct_mulaid_pay	家庭共济金支付	String	Y	
psn_cash_pay	现金支付	String	Y	
pay_result	支付结果	String	Y	1 成功 0 失败
redirect_url	回调地址	String	Y	
fail_msg	支付失败信息	String	Y	
hi_pay_no	第三方订单	String	Y	
failCode	失败错误码	String	Y	

6 报文示例

渠道 id: ldxt

渠道密钥：67b082f9d58045619a4ef05147b87659

分配 bizkey: testkey

加解密 salt: f2313d85601342b8b15c872286c6aaff

原始请求报文


```
{
    "chs_fjs_appid":"ldxt",
    "chs_fjs_appsecret":"67b082f9d58045619a4ef05147b87659",
    "chs_fjs_funid":"F04.05.13.09",
    "chs_fjs_timestamp":"1631685457000",
    "psnBasicInfoDTO": {
        "psnNo": "543212343",
        "name": "王二",
        "gend": "1",
        "brdy": "19800101",
        "certType": "01",
        "certNo": "650101198001010032",
        "naty": "01",
        "natRegnCode": "CHN",
        "survStas": "1",
        "poolarea": "660100"
    }
}
```


入参报文：


```
{
    "chs_fjs_appid":"ldxt",
    "chs_fjs_appsecret":"67b082f9d58045619a4ef05147b87659",
```

"chs_fjs_funid":"F04.05.13.09",
"chs_fjs_timestamp":"1631685457000",
"chs_fjs_encdata":"738yYxU+RHC3er8nWI8JtzfQxeAXWJWJtMGubi6AHKRkiYa7GZx9n/AX2TABkiGlPuhAK6PFroKRbxGjui8BKL6QSH6jEjACYCOeYxz1zeCsmyafGo4FF1x8POfhzsZiJK2vlybUolHTAChQKTbSajZz48z5Ic+igwl1BrtW8bUoEx5KHx3ududrg8TdFOMJmWftL2d5u/aJ+5sryZLbp2pxmLMdDtY47ytcwTshUsLltOpBYhW6AZR4yhoagYMFFueEdpy+xfHyJtVUysRv/CVEailYHewcXaoox0RlJru19Mqm6/IrBW4CTvTMyX623+xxRrTAG2ppYkheODwmkvJex3c7A48wGdvtNm2gZMOOyk1AXfpoJhfLmJGbSqg5+UBAY10QaCfLHLM101U9UKArgihUnqNIJm2s/lKkYYCHnRbqtVieRLoKAG59j6y/L980bgr5FNsGbRktyXvMw8OKVQ5l1JVkm2d8n+hj9jy2IspTrLcRBqOKPvefbK/Kavb5IzhC+fuLksGlopNO6Q==",
"chs_fjs_sign":"37A299CF9B627EABB920D3314324031B",

原始出参报文：


```
{
    "code": 0,
    "type": "success",
    "message": "成功",
    "data": {
        "psnBasicInfoDTO": {
            "psnNo": "1000000001",
            "name": "王二",
            "gend": "1",
            "brdy": "19791201",
            "certType": "01",
            "certNo": "650101198001010032",
            "naty": "01",
            "natRegnCode": "CHN",
            "survStas": "1",
            "poolarea": "660100"
        }
    }
}
```


出参报文


```
{
    "code": 0,
    "type": "success",
    "chs_fjs_sign":"682FD1B29011DFE68DB4FCAA35901D6F",
    "chs_fjs_encdata":"DB71ufMpR08XAPA5AtubOGT1aXmUi1jm/+o4Kuk91DrP1W9Xx0w0iJ7/WraEfSszlmuusnXnxtjFfQsGi0rBjEYvmkFfU/IUsFag5Yl8z1VgJdG7Ztws2wg+xLtDVZKxyhF1M2pmDUcA/Nsil5DsYjFATfKhMf0R6VQy9tf8bQudfp5+BnZ5rIl4GFxiqW1Eshf8F+ZF4V94cXVG0nVBGa2K+2FekKui8XHLCAZDpInBPlIcDr8v0M51ZYdN4Abb9MfIOsGd+J3u+Lvj8XztgvV5+G8cM/8UbXcweMTp+QJn2YXy2FYeSFV0vyKMcltW4TRK36AfPs3F4KM4InMV7kTFjNaUeupMAlfEPUotd9uTAw35pCf0YeDtInICOS8USdh3KVdOf1LILYZXvMk8BBqqvXCG91GHgMEtU+kiRLQ="
}
```

附录 1 安全规范

1.1 时间戳校验

1.1.1 概述

可用于防钓鱼校验，主要实现原理如下：

1、在发出 http 请求前先调用终端的当前时间 T1，把时间 T1 作为请求的一个参数传递给医保服务器。

2、服务器接收到请求后先取出时间参数 T1，然后取一下当前服务器当前的系统时间 T2，计算两个时间的间隔，如果时间差超过一定范围，则时间戳检查失败，拒绝服务。

3、时间间隔的设定默认是 600 秒，可以根据配置灵活的调整。

1.2 渠道认证

1.2.1 概述

平台需对接入渠道的身份进行统一的安全校验，目前支持 User 认证（密钥模式）、OAuth2.0 认证(授权码模式)、匿名认证三种模式。

1.2.2 认证模式

1.2.2.1 User 认证(密钥模式)

通过医保平台分配给不同渠道的渠道编号 chs_fjs_appid 和渠道密钥 chs_fjs_appsecret 直接进行接口鉴权访问，类似于账号密码登录模式，主要适用于应用直接都是受信任的。

1.2.2.2 OAuth2.0 认证(授权码模式)

提供一种无需加密的认证方式，此方式是基于现存的 cookie 验证架构，token 本身将自己作为 secret，通过 HTTPS 发送，从而替换了通过 HMAC 和 token secret 加密并发送的方式，主要适用于在服务端应用之间的认证。

1.2.2.3 匿名认证

主要用于医保内部各业务系统间的交互通信等。

1.3 签名算法

1.3.1 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。

1.3.2 请求参数签名

1.3.2.1 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。

1.3.2.2 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。

1.3.2.3 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）。

JOSN 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":"o8z4C5avQXqC0aWFPf1Mzu6D7WCQ
_bd","idNo":"350181199011193519","idType":"01","phoneNumber":"13763873033","userName":"测试"},
"encType":"SM4",
"signData":"URVQNdVNn5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHR
GmyO5w==",
"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","phoneN
umber":"13763873033","userName":"测试"}
```

```
&encType=SM4&signType=SM2&timestamp=20200207175759&transType=ec.gen.index&version=1.0.0&key=4
117E877F5FA0A0188891283E4B617D5
```

1.3.2.4 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：

```
URVQNdVNn5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHRGmyO5w=
```

1.3.3 返回参数验签

1.3.3.1 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。

1.3.3.2 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。

1.3.3.3 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":"URVQNdVNn5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHR
GmyO5w==",
"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
```

1.3.3.4 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。

1.4 加密算法

1.4.1 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。

1.4.2 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":"o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd","idNo":"350181199011193519","idType":"01","phoneNumber":"13763873033","userName":"测试"},
"encType":"SM4",
"signData":"URVQNdVNn5mz2EhKZhLTlXNwAWTSncFoSe8Ilx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHRGmyO5w==",
"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 加密算法长度秘钥为 32 位，实际底层算法秘钥应用长度为前 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 加密算法秘钥长度为 32 位，实际底层算法秘钥应用长度为前 16 位），并将加密结果转换为大写，获得加密密文 encData

密文示例：

```
4470B6B96A8E0BADA051A318E6B6FBED66B9FC5AB2A4A3C66FDDD3C70BCADD6EF526AB57DC1DC916385CEF34843AABFCBAF8F1FDEA9DC51A2A56AB3EA3E170201E4EDD3137D6D1BA6A4A773F6F4872A718F56742E5052AD1C04E99C91EA048990F06A96E6E1E534E40BD28DFDC204ACA03CAE0DFE0DE5229EDADBD27BBD32DD4C3F9ADC833CD3CF01CD012CE1799BB6F
```

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":"64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBCB6AB7914898A23A99C97EBEFE5277247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E06B08E151362301659FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB736BA3BB98F3540962552F40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D63B2D387A87F42130F0D47B9445F9D729566FE183F9A959",
"encType":"SM4",
"signData":"URVQNdVNn5mz2EhKZhLTlXNwAWTSncFoSe8llx7jhn81eABJ46sdRRN1ZiAiQjPUTixG9bwqEhiJupHRGmyO5w==",
```

```
"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":"64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBCB6AB7914898A2
3A99C97EBEFE5277247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E
06B08E151362301659FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB73
6BA3BB98F3540962552F40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D6
3B2D387A87F42130F0D47B9445F9D729566FE183F9A959"
,
"encType": "SM4",
"respCode": "0",
"respMsg": "处理成功",
"signData": "
OTk0MUYwREIyODk1RDhDRDQ5NjQzRTU1RENCN0ZGMzdCRUY4MzFFNDMxMTM1OTY0MEM1MDk3N0E4REE2
Nzk2QQ==",
"signType": "SM2",
"timestamp": "20161226093147927"
}
```


加密密文数据 enctData 示例：


```
64A9C5A7AB3AEA5FC01DE87025F999521C08D25DA13BD715D7E036A7D7C1DBCB6AB7914898A23A99C97EBE
FE5277247AD7D0DD9B18F4DCC71A2C280C5143F25B857C795E6BA9F399652C3A4264FC2CBBA7E06B08E1513
62301659FC3F3773480966E8D19AB082B64A4F9B9BDBABCE57DC2CA95C9975090885AB286BB736BA3BB98F3
540962552F40C8350926B93CD21CB7A624E6C4E41E349627E7B36B5C1B5F94604EDC42EA6034D63B2D387A8
7F42130F0D47B9445F9D729566FE183F9A959
```

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 encData 获取 JSON 字符串明文 jStr

明文示例：


```
{"appId":"43AF047BBA47FC8A1AE8EFB232BDBBCB","appUserId":"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","appUserId":"o8z4C5avQXqC0aWFPf1Mzu6D7WCQ_bd","idNo":"350181199011193519","idType":"01","phoneNumber":"13763873033","userName":"测试"},
"encType": "SM4",
"respCode": "0",
"respMsg": "处理成功",
"signData": "OTk0MUYwREIyODk1RDhDRDQ5NjQzRTU1RENCN0ZGMzdCRUY4MzFFNDMxMTM1OTY0MEM1MDk3N0E4REE2Nzk2QQ==",
"signType": "SM2",
"timestamp": "20161226093147927"
}
```

附录 2 应用跳转

2.1 **跳转小程序**

2.1.1 接入方跳到小程序

使用 wx.navigateToMiniProgram() 跳转到我们小程序，相关参数如下：
appid：wx0c13e701f68315c4
page：pages/internetHospital/healthcareOnlineServiceAuth
示例代码：

```
uni.navigateToMiniProgram({
   appid: 'wx0c13e701f68315c4',
   path: 'pages/healthcareOnlineServiceAuth/index'
})
```

2.1.2 小程序回跳到接入方

电子凭证授权成功后回跳到接入小程序，在 app.js 的 onShow 函数里获取返回数据。

证件类型表

居民身份证（户口簿）	01
中国人民解放军军官证	02
中国人民武装警察警官证	03
香港特区护照/港澳居民来往内地通行证	04
澳门特区护照/港澳居民来往内地通行证	05
台湾居民来往大陆通行证	06
外国人永久居留证	07
外国人护照	08
残疾人证	09
军烈属证明	10
外国人就业证	11
外国专家证	12
外国人常驻记者证	13
台港澳人员就业证	14
回国（来华）定居专家证	15
中国护照	16
港澳台居民居住证	17
暂住证	9901

错误码

20001	结算 code 不能为空
20002	电子凭证授权已过期，请重新授权
20004	被投保人列表不能为空
20005	服务 id 不存在
20006	应用编号不能为空
20007	服务编号不能为空
20008	第三方平台编号不能为空
20009	第三方平台支付流水号不能为空
20010	医保支付总金额不能为空
20011	医保支付流水号和第三方平台支付流水号不能同时为空
20013	code 不能为空
20014	订单【】不存在
20015	订单【】人员【】不能重复冲销
50101	系统服务异常
20016	总价格与支付信息价格不一致
20017	支付人员信息不是在一个家庭网
20018	未查询到家庭共济信息
20019	共济余额不足
20020	其他支付异常
20021	非户主不能邀请临时惠闽保成员
20022	其他授权异常
20023	此用户与户主不在同一个家庭网,此用户家庭网 id 为【】
20024	订单数据插入异常
20025	个账余额不足
20026	个账冲销失败
20027	证件类型不一致
20028	个账支付退款只允许单人退款
20029	证件类型不能为空
20030	姓名不能为空
20031	证件号码不能为空
20032	授权异常
20033	授权码错误
20034	未查询到参保信息

地市编码

福州市	350100
厦门市	350200
莆田市	350300
三明市	350400
泉州市	350500
漳州市	350600
南平市	350700
龙岩市	350800
宁德市	350900
平潭实验区	350128

共济关系编码

户主	0
配偶	1
外祖父	10
外祖母	11
配偶祖父	12
配偶祖母	13
配偶外祖父	14
配偶外祖母	15
孙子	16
孙女	17
外孙子	18
外孙女	19
父亲	2
女婿	20
儿媳	21
母亲	3
配偶父亲	4
配偶母亲	5
儿子	6
女儿	7
祖父	8
祖母	9