中国银行间市场交易商协会开放接口（iOpenAPI）系统总体技术规范

2020 年 11 月

第1章 引言

1.1 编写目的

本文档旨在通过建立统一的系统设计及功能开发规范，为开放接口系统功能建设、内部拟接入数据服务接口开发、外部机构接入接口开发过程提供规范、一致的技术指导。

1.2 阅读对象

本文档主要面向的读者和使用人员包括协会开放接口系统、外部接口接入系统及内部数据服务接口系统相关开发、测试及运维支持人员。

1.3 使用说明

本文档。

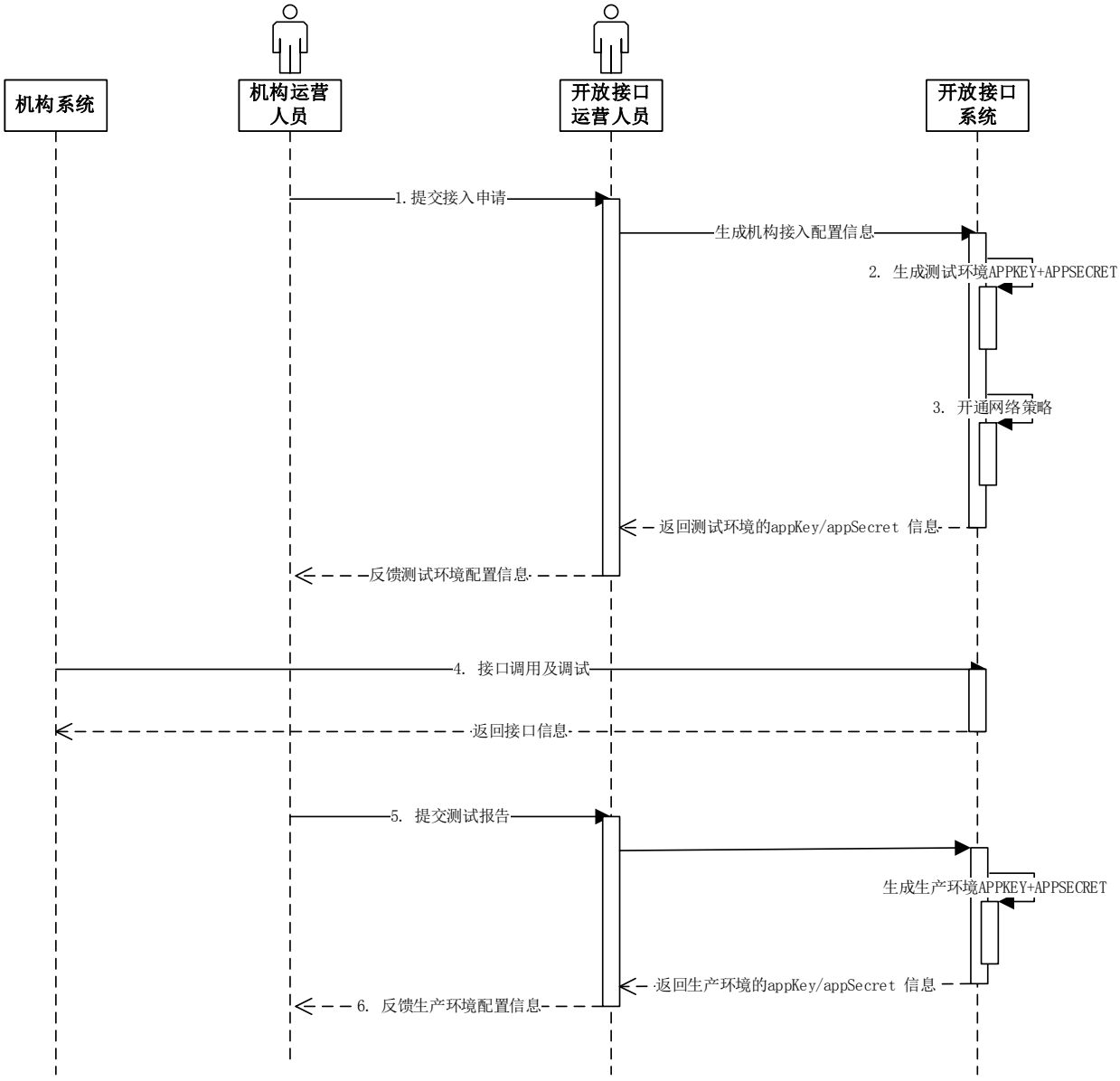
1.4 术语定义

名称	定义
机构	与协会通过开放接口系统进行业务对接的机构。
报文	协会接口系统与机构系统之间交换的结构化信息。
协会开放接口系统（简称开放接口系统）	协会与外部机构进行业务数据交互、系统对接的统一入口及数据服务管控平台。

外部接口接入方	机构端应用系统，可按照接口接入管理办法要求与协会开放接口系统进行业务数据交互。
内部数据服务接入方	结合具体业务场景中数据交互需求，按照开放接口系统基础报文规范提供相关交互接口具体功能实现的内部组件

第2章 总体方案

2.1 外部接口接入方案



1. 提交接入申请

申请接入机构填写《协会开放接口服务开通申请表》(见附件1)提出接入协会开放接口系统的申请，并由协会相关部门、单位进行审

核。

2. 获取测试环境 appKey 和 appSecret

接入申请通过审核后，协会相关单位为接入机构分配测试环境的 appKey 和 appSecret。

3. 开通网络策略

协会相关单位根据《协会开放接口服务开通申请表》中的 IP 地址，开通对应的网络策略。

4. 接口调试及验收测试

接入机构根据相关接口规范调用接口并进行调试，提出验收测试申请，进行接口验收测试，编制验收测试报告；协会相关单位进行接口验收测试。

5. 投产计划

接入机构测试环境通过接口验收测试后，制定投产计划，提交技术方案和测试报告。协会相关单位审核通过后发送正式上线通知并抄送协会相关部门。

6. 获取生产环境 appKey 和 appSecret

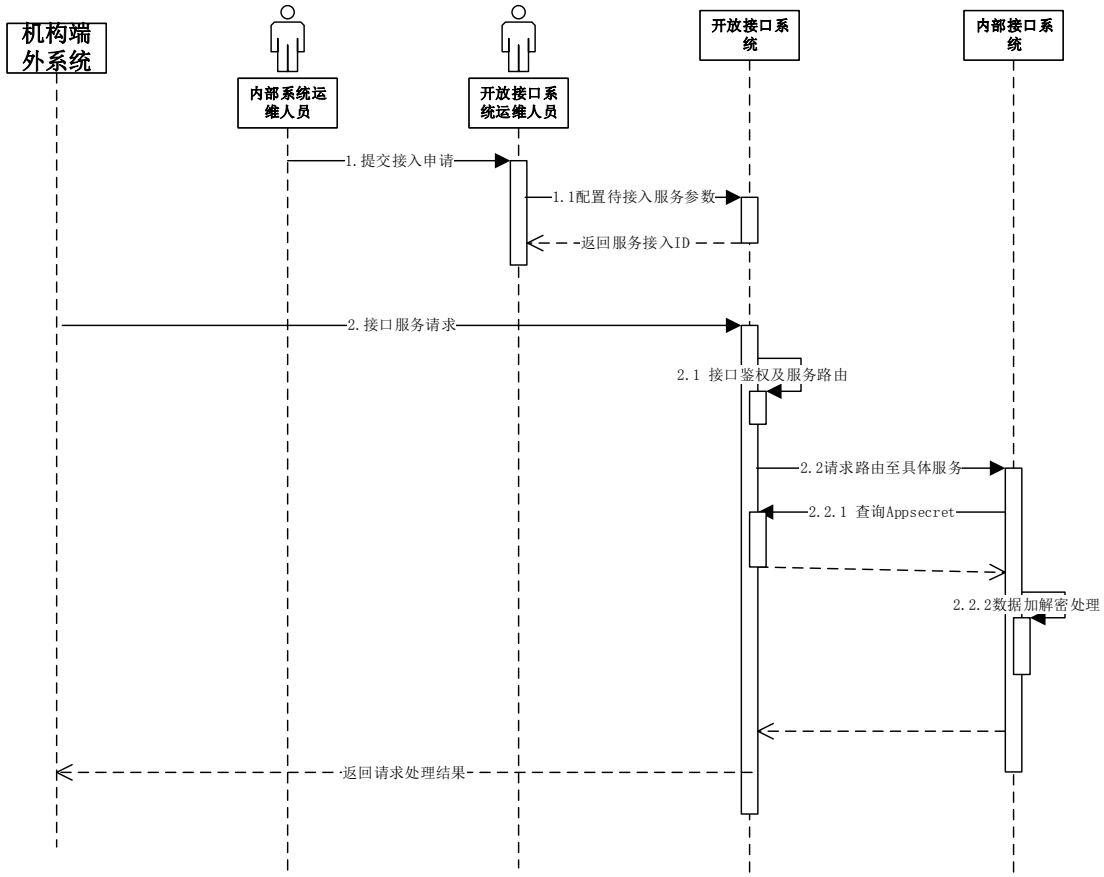
协会相关单位为接入机构分配生产环境的 appKey 和 appSecret。

7. 正式投产

协会相关单位与接入机构按照投产计划进行投产实施，与正式环境进行对接。

2.2 内部数据服务接入方案

内部数据服务接入方结合外部机构在具体业务场景中数据交互需求，按照开放接口系统基础报文规范提供相关交互接口具体功能实现，并满足以下服务接入相关要求。

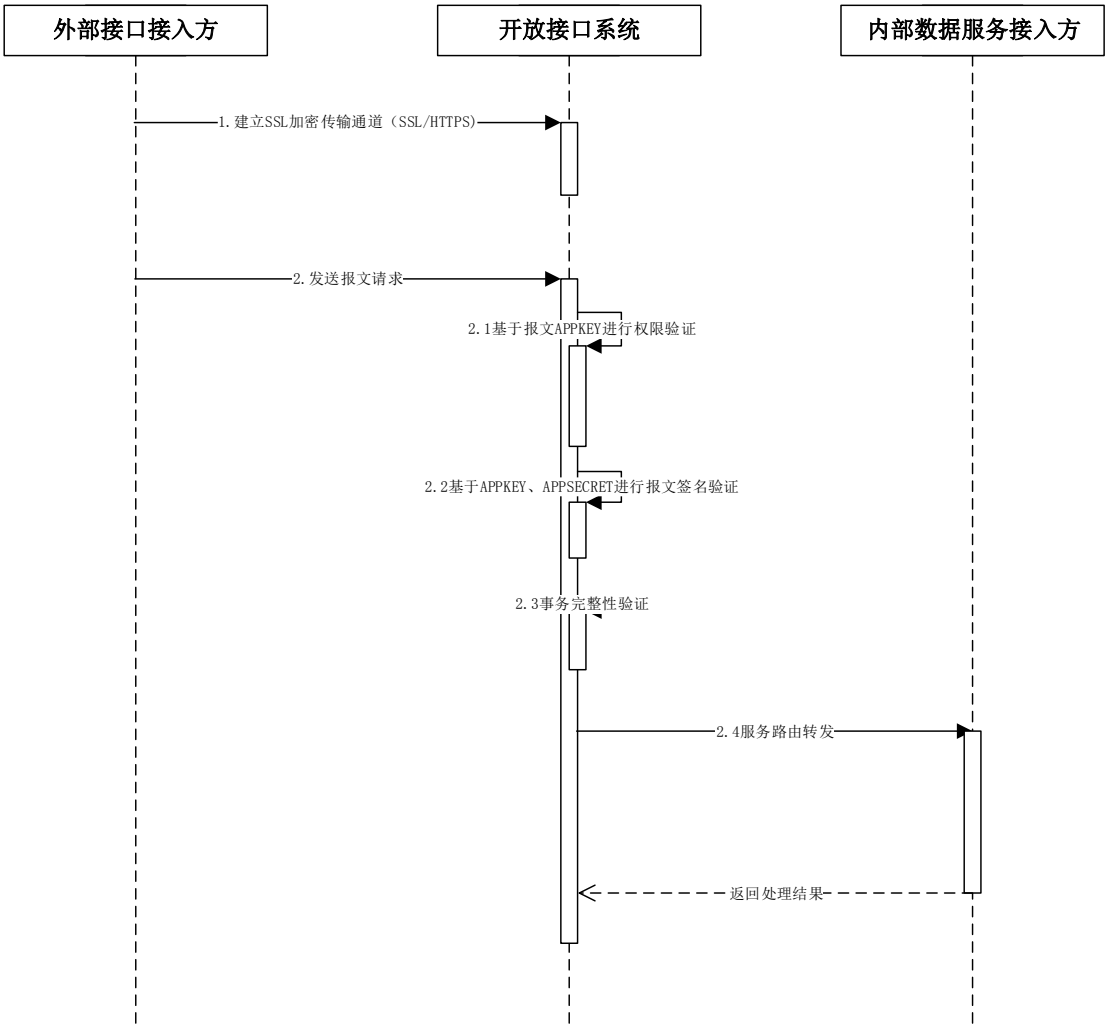


1. 开放接口系统开发服务配置功能，并建立服务接入参数配置表，覆盖业务分类、服务名、服务IP地址及端口信息。
2. 开放接口系统在配置待接入数据服务时，授权该数据服务可基于APPKEY查询相关外部接入方APPSECRET信息。

3. 外部接口接入方提交接口服务请求，经开放接口系统鉴权及服务路由至具体内部数据服务，内部数据服务组件可通过报文中APPKEY获取该机构APPSECRET并进行后续业务数据加解密处理。

2.3 开放接口系统服务鉴权、路由及管控方案

开放接口系统承担外部接口接入方接入授权、内部数据服务接入方配置管理、服务请求路由等方面管理职责，其整体交互时序如下图所示：



1. 外部接口接入方与开放接口系统间数据传输过程使用SSL加密机制，消息通道SSL加密或者采用https协议。

2. 外部接口接入方与开放接口系统间数据交互报文基于APPKEY/APPSECRET进行签名及验签。

3. 开放接口系统基于APPKEY及请求具体服务进行服务权限校验及服务路由。

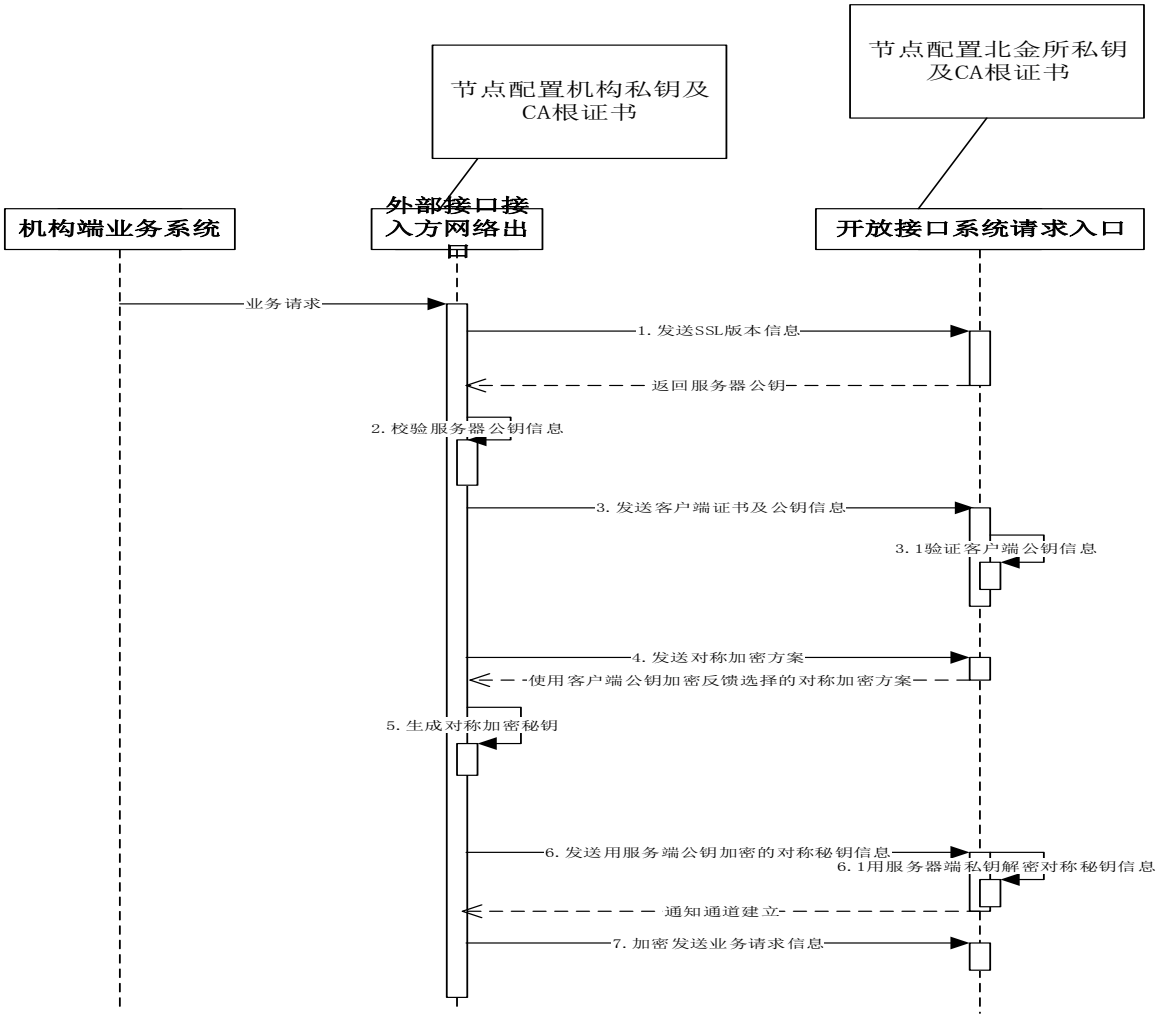
4. 开放接口系统结合报文规范中事务机制进行报文内容完整性

校验。

第3章 关键方面设计规范

3.1 通道安全

通道安全相关要求主要针对消息通道、HTTPS 协议进行数据交互场景，具体交互过程如下：



1. 机构端提交外部接口接入申请后，由开放接口系统分配 APPKEY、APPSECRET 及通道 SSL 证书。

2. 机构端网络出口及开放接口系统网络入口分别需要配置 HTTPS 双向 SSL 证书，或基于 SSL 认证建立消息传输通道。

3.2 传输机制

3.2.1 https

针对同步请求，接入机构与开放接口系统之间的通过 https 进行数据交互。https 是以安全为目标的 https 通道，在 http 的基础上通过传输加密和身份认证保证了传输过程的安全性。提供了通道级的身份验证和加密通讯方法，被广泛的用于对于安全敏感数据的交互。

3.2.2 消息通道 kafka

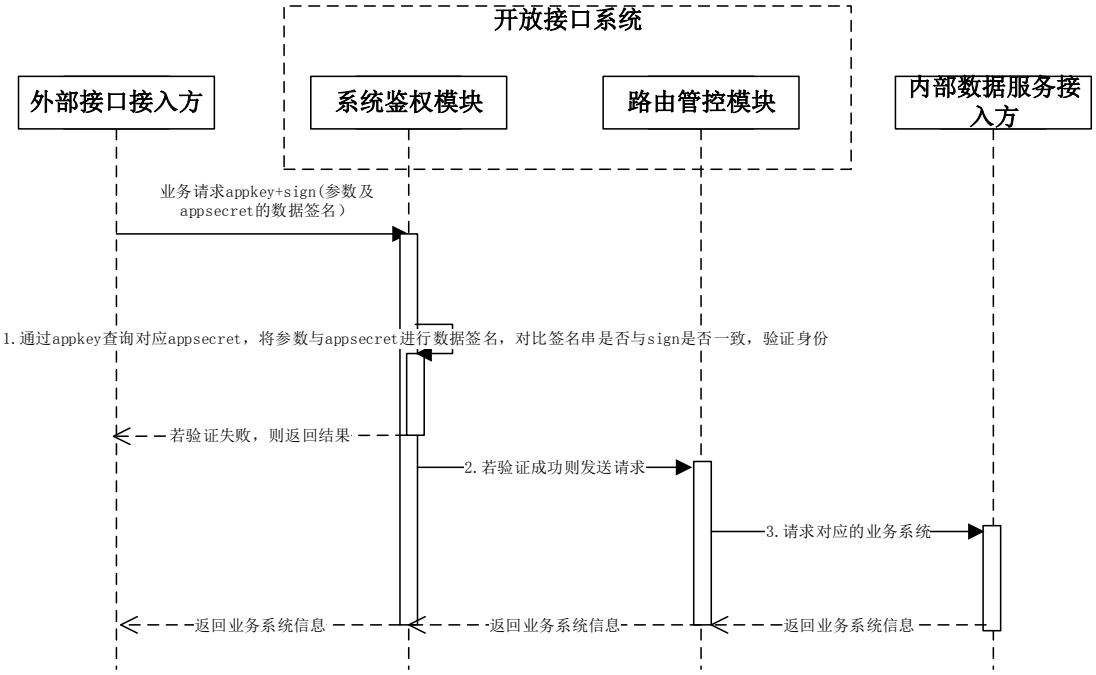
针对适合异步或需要开放接口进行数据推送等业务场景，接入机构与开放接口系统之间的交互数据通过 kafka 消息通道进行传递，保证消息传递过程中的可靠性及高可用性。

3.2.3 SFTP 文件接口技术

本规范约定双方文件数据交互过程采用 SFTP 协议。SFTP 是一种安全文件传送协议，可为传输文件提供安全的加密方法，提供足够的安全性保证。同时 SFTP 的速率也可以保证应急文件数据的实时传输。

3.3 访问授权

开放接口系统根据外部接口接入方提交的数据服务访问权限申请信息，为其分配 SSL 证书、APPKEY 及 APPSECRET，并配置该 APPKEY 访问权限及路由规则。



1. 接口接入方发送的数据请求中须包含 APPKEY 信息及签名信息。
2. 开放接口系统根据请求中 APPKEY 信息进行访问权限核验，并结合本地存储的与报文中 APPKEY 对应的 APPSECRET，进行签名核验。

3.4 加密及签名机制

申请接入机构提交的接入申请通过审核后，系统会为每个接入机

构颁发一个 appKey 和 appSecret，用户的每次请求需要上传 appKey，便于信息的确认，appSecret 用于对数据做签名和敏感信息加密。

3.4.1 加密机制

加密机制为报文中的关键域采用对称密钥加密法 3des 算法，通过颁发的密钥(appSecret)进行加密，并为加密后的信息进行 base64 的编码，服务端需要对关键域的信息进行 base64 解码后再用相同的密钥（appSecret）进行解密才可以获取正确的信息，能有效的保证信息的安全性。

如报文中需要传输债券代码(bondCode)等涉及的敏感信息字段，则采用加密手段进行传输。示例如下：

原报文

```
{
    "appKey":"63336f955e1e497a977435916e53e998",
    "bondCode":"13508081234"
}
```

加密后报文,密钥 appSecret：123456

```
{
    "appKey":"63336f955e1e497a977435916e53e998",
    "bondCode":"YTE5THVZOG9BVmQ1K2kyYU92RzRoZz09"
}
```

3.4.2 签名机制

签名机制采用{appSecret}+入参 key 值升序排序后取 value 值+{appSecret}并 md5(32 位小写)加密算法生成签名，服务端需要将接收的信息采用相同的签名机制生成签名后和接收到的签名字段进行比对，比对一致则信息传输的过程中信息没有被篡改。能有效的保证信息的不可抵赖、防止篡改。

以上节报文为例，则签名字段 sign 为：

sign:md5({appSecret}+{appKey}+{bondCode}+{appSecret})

示例如下：

原报文

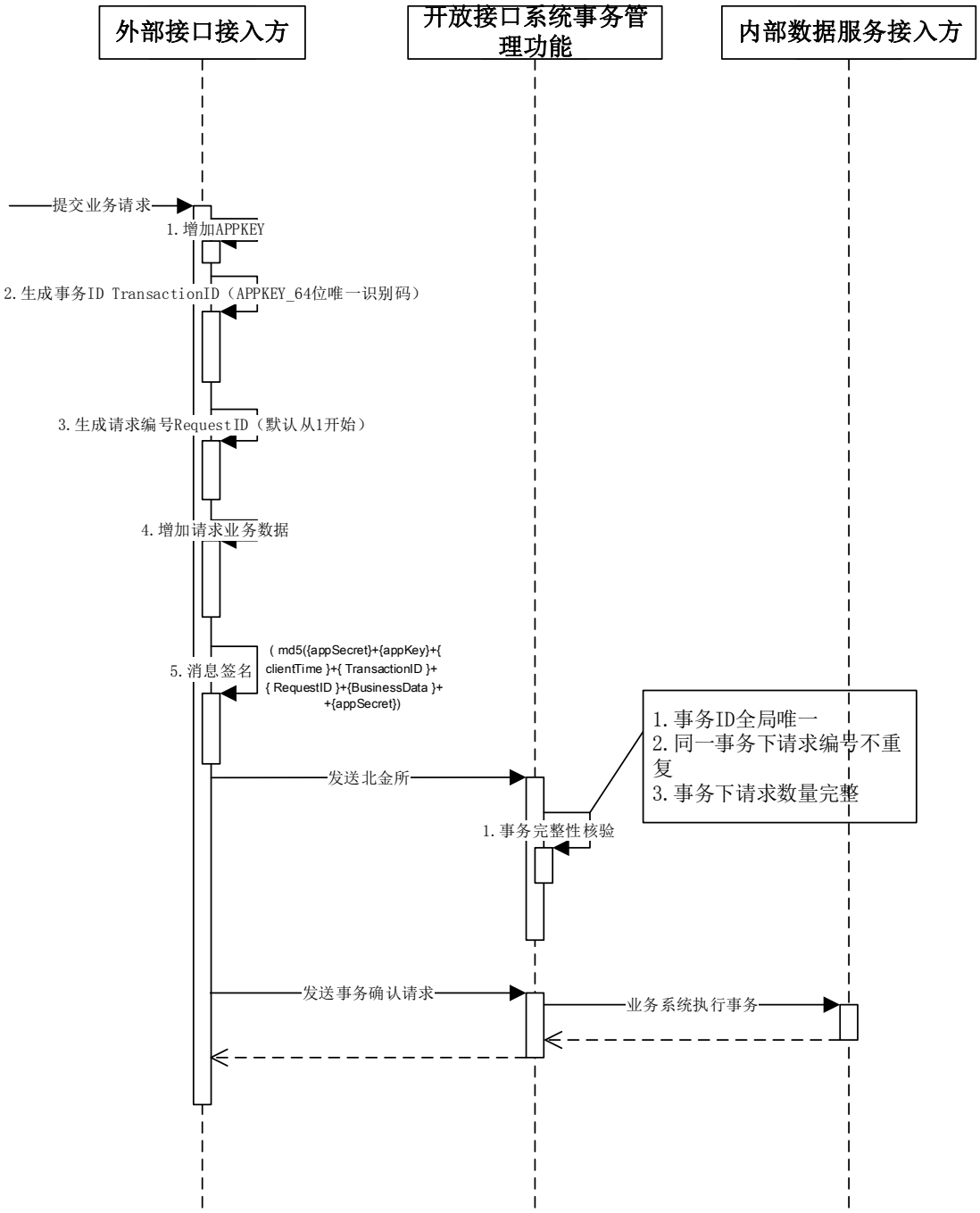
```
{
   "appKey":"63336f955e1e497a977435916e53e998",
   "bondCode": "13508081234"
}
```

签名并加密后的报文,密钥 appSecret：123456

```
{
   "appKey":"63336f955e1e497a977435916e53e998",
   "bondCode":"YTE5THVZOG9BVmQ1K2kyYU92RzRoZz09"
   "sign": "2e8e5e0cb9099f830c58796337eb0731"
}
```

3.5 事务机制

为保障双方数据交互过程可靠性，避免因网络异常、系统故障引起数据一致性、完备性问题，本规范消息交互过程设计如下事务机制：



1）若一次传输过程涉及多条业务数据记录，多条业务数据记录可以通过多个报文进行发送。

2）同一事务下各报文拥有相同的事务编号，并由报文头中msgCnt 指定事务下报文总数量。

3）各报文 msgId 从编号"00000001"开始连续递增。

4）接收端对各条报文发送反馈报文，反馈报文中事务编号及报文编号与发送方各报文对应一致。

5）对于同一事务下存在多条报文的情况，最后一条报文作为事务结束报文，事务状态须设置为 1，该报文不携带业务数据，仅作为事务结束确认。接收方将基于该报文反馈该次事务数据完整性校验及执行结果。

涉及基础技术字段如下：

中文名称	英文名称	类型	必填	描 述
报文状态	msgState	Number	是	枚举值： 0:正常报文 1：正常报文反馈 2：重发报文 3：重发报文反馈
事务编号	transUuid	str	是	该字段为技术约束，同一次传输使用相同的唯一事务编号，64 位。各次传输需使用不同的事务编号。
事务下报文数量	msgCnt	Number	是	默认值为 1
事务状态	tranState	Number	否	当 msgCnt 大于 1 时，该字段必填。 枚举值：

				0:传输中 1：确认结束，最后一条报文使用该枚举值进行事务结束确认。
报文编号	msgUuid	str	是	8 位数字，由 8 位顺序码组成，顺序编码。

3.6 事务重发机制

为保障双方数据交互过程可靠性，本规范在消息交互过程设计如下重发机制：

1）接收方在接收完毕某某次事务过程所有报文后（以接收到本次正常传输过程结束报文为准），在结束报文反馈中明确是否需要重传全部或部分报文。接收方在结束报文反馈中以“反馈状态”字段标示重传（取值 303）。

2）发送方发送重传报文时，所有报文 msgState=2，事务编号与初次发送事务编号一致，消息编号与初次发送时各报文编号一致。

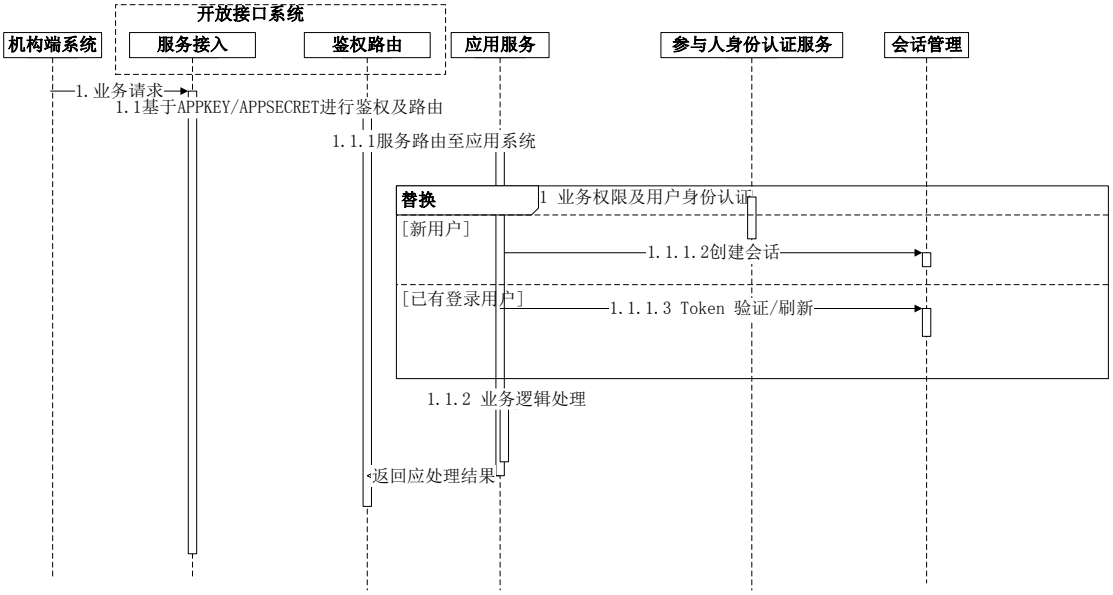
3）接收方对重传报文进行反馈时，所有报文 msgState=3，事务编号与初次发送时事务编号一致，消息编号与初次发送时各报文编号一致。

涉及基础技术字段如下：

中文名称	英文名称	类型	必填	描 述
报送机构代码	sendId	str	是	机构代码（北金所预先分配的 8 位代码）
报送机构全称	senderName	str	是	机构全称
报送机构用户名	userName	str	是	用户名

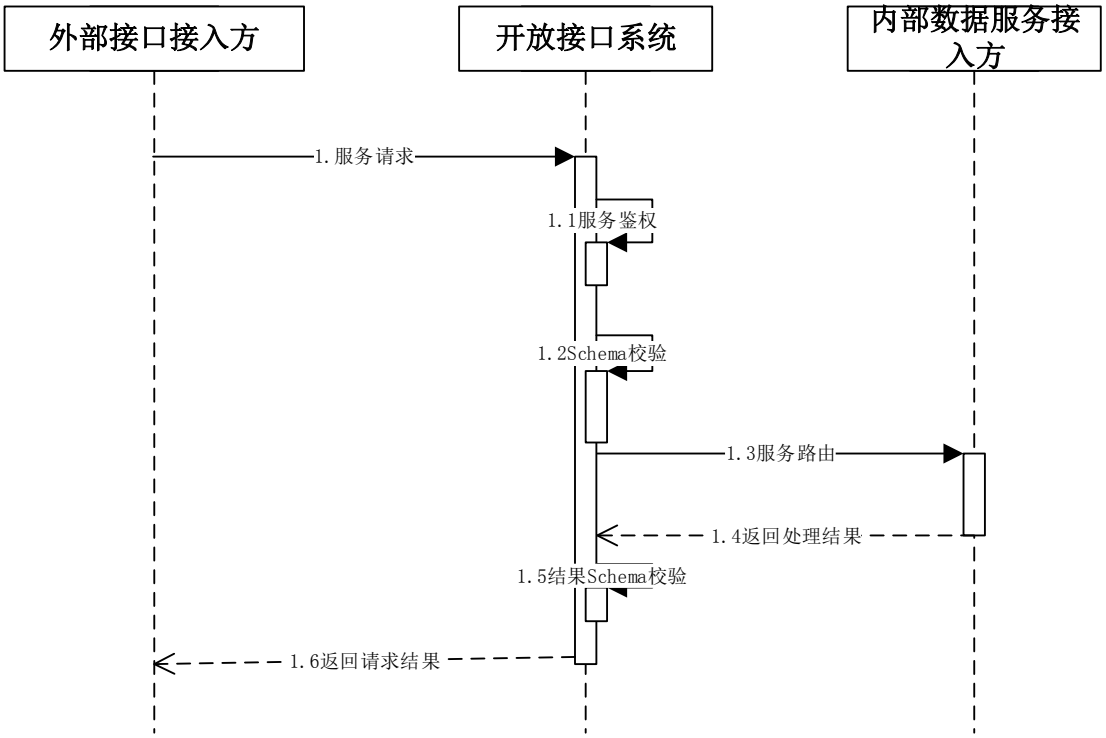
接收机构名称	targetName	str	是	接收方机构代码（北金所预先分配的 8 位代码）
报文状态	msgState	Number	是	枚举值： 0:正常报文（发送方使用） 1：正常报文反馈（接收方正常反馈时使用） 2:重发报文(发送方重发报文使用) 3：重发报文反馈（接收方对重发报文进行反馈时使用）
事务编号	transUuid	str	是	该字段为技术约束，同一次传输使用相同的唯一事务编号，64 位。各次传输需使用不同的事务编号。
报文编号	msgUuid	str	是	8 位数字，由 8 位顺序码组成，顺序编码。

3.7 会话机制



3.8 Schema 机制

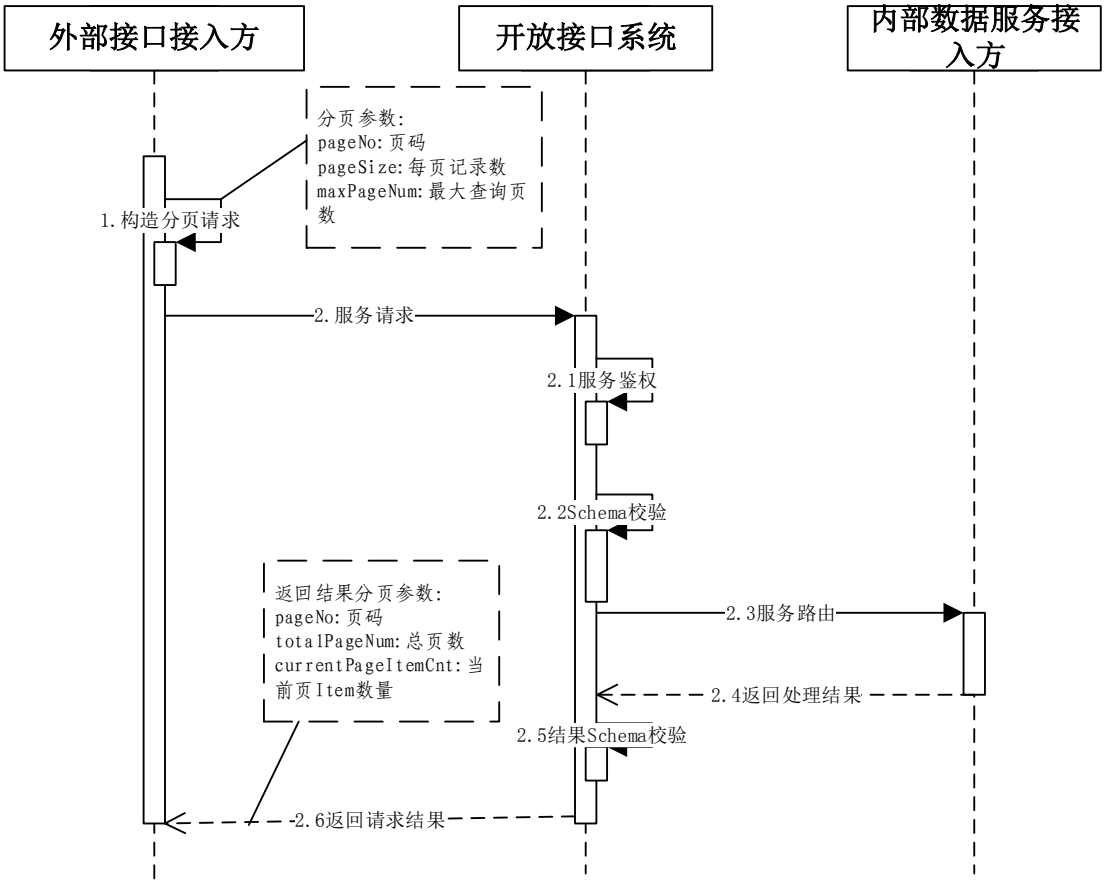
开放接口系统建立 Schema 校验机制，支持对 XML、JSON 报文进行格式校验。



1. 开放接口系统建立统一的 Schema 配置管理及 Schema 校验功能。
2. 各业务场景报文规范须建立服务请求、服务响应报文 Schema 文件，并在做服务配置时提供至开放接口系统。
3. 对于外部接口接入方相关服务请求，开放接口系统经过服务鉴权（访问授权、签名核验相关处理）后，进行报文 Schema 校验后服务路由至内部数据服务接入方进行业务处理。
4. 对于业务处理结果，开放接口系统进行 Schema 校验通过后，反馈给外部接入方。

3.9 分页机制

针对交互数据量较大场景，开放接口系统建立标准分页机制：



1. 服务请求方根据业务场景各接口报文规范构造分页查询服务请求，涉及分页请求字段如下：

中文名称	英文名称	类型	必填	描 述
页码	pageNo	Number	否	本次拟查询页码; 默认返回第一页
每页记录数	pageSize	Number	否	本次查询每页拟显示记录数: 默认一页返回所有记录
最大查询页数	maxPageNum	Number	否	拟查询最大页数

2. 内部数据服务方根据业务场景提供分页处理并返回分页结果。

中文名称	英文名称	类型	必填	描 述
页码	pageNo	Number	是	本次返回数据页码
总页数	totalPageNum	Number	是	本次返回数据总页数
当前页记录数	currentPageItemCnt	Number	是	当前页有效记录数

3.10 超时重发机制

第4章 报文语法与结构

4.1 报文数据类型

数据类型用于定义报文域的取值类型,本协议使用的数据类型由几个基本的数据类型（数值、字符串、时间）和在此基础上扩展的数据类型组成。

4.1.1 数值

数值类型（number）可表示正负（ASCII 码字符“-”,“0”至“9”和“.”组成),以及可选小数部分的数值。数值类型定义形式为(m.n)，m 表示整数位最大长度，n 表示小数位精度。

4.1.2 字符

字符类型（str）指由字母、数字以及符号组成的字符。字符类型定义形式为(n)，n 表示字符最大长度。字符类型域取值为空时用“”表示。

4.1.3 时间

时间类型（date）用来表示时间及符号组成的字符。时间类型定义形式为(YYYYMMDD-HH:MM:SS.sss)或其中节选部分如日期为（YYYYMMDD),其中,YYYY=0000-9999,MM=01-12,DD=01-31,HH=00-23,

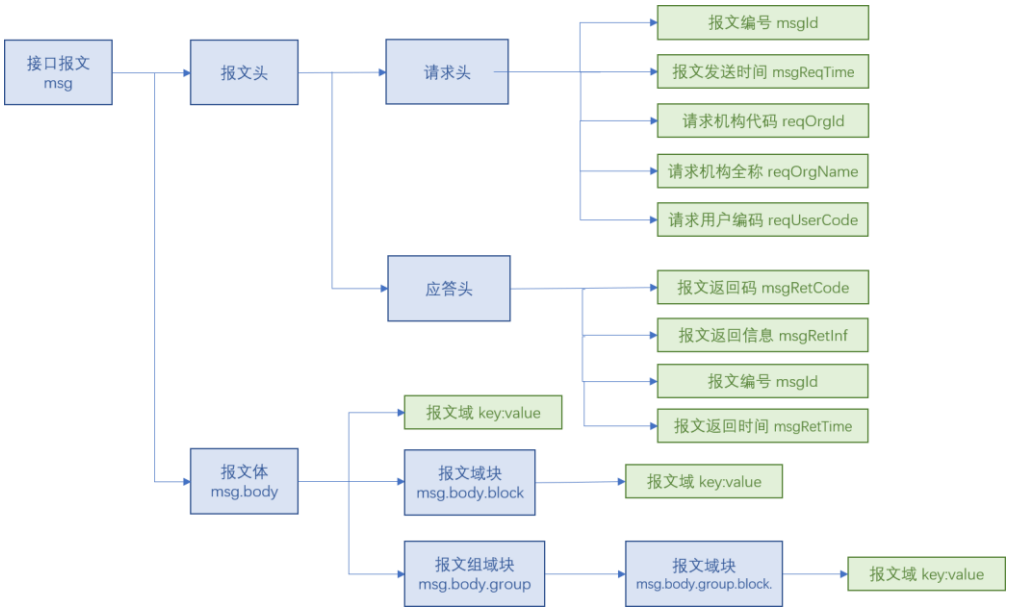
MM=00-59，SS=00-60(秒)，sss=000-999（毫秒）。

4.1.4 扩展数据类型

当数值、字符、时间类型无法满足数据类型的表示要求时，可自定义扩展数据类型。扩展数据类型需对取值的限定进行准确的说明。

4.2 报文结构

报文结构包括报文头和报文体，具体如图所示：



4.3 报文头

每个报文都应该包含报文头，用于说明报文发送方、身份认证信息、报文编号、报文发送时间、报文返回结果等内容。参考标准如下:

1. 发送方报文基础技术字段

中文名称	英文名称	类型	必填	描 述

发送机构代码	sendId	str	是	机构代码（北金所预先分配的机构代码）
发送机构全称	senderName	str	是	机构全称
发送机构用户名	userName	str	否	用户名
接收机构代码	targetId	str	是	机构代码（北金所预先分配的机构代码）
接收机构全称	targetName	str	是	机构全称
服务功能代码	funcId	str	是	服务功能代码
服务功能版本	funcVer	str	否	服务功能版本，0000 默认为最新版本
报文状态	msgState	number	是	枚举值: 0:正常报文 1：正常报文反馈 2：重发报文 3：重发报文反馈
事务编号	transId	str	是	该字段为技术约束，同一次传输使用相同的唯一事务编号，64 位。各次传输需使用不同的事务编号。
事务下报文数量	msgCnt	Number	是	默认值为 1
报文编号	msgId	str	是	8 位数字，由 8 位顺序码组成，顺序编码。
报文发送时间	msgTimeStamp	str	是	如下格式的报文发送时间戳"yyyy-MM-dd HH:mm:ss SSS"

2. 反馈报文基础技术字段

中文名称	英文名称	类型	必填	描 述
反馈报文发送机构代码	sendId	str	是	机构代码（北金所预先分配的 8 位代码）
反馈报文发送机构全称	senderName	str	是	机构全称信息
反馈报文接收机构代码	targetId	str	是	机构代码（北金所预先分配的 8 位代码）
反馈报文接收机构全称	targetName	str	是	机构全称
服务功能代码	funcId	str	是	服务功能代码

服务功能版本	funcVer	str	否	服务功能版本，默认最新版本
事务编号	transId	str	是	该字段为技术约束，同一次传输使用相同的唯一事务编号，事务编号为64位字符串。
报文编号	msgId	str	是	8位数字，由8位顺序码组成，顺序编码。同一次事务传输中报文编号递增。
报文状态	msgState	number	是	枚举值： 0:正常报文（发送方发送报文时使用该状态） 1：正常报文反馈（接收方向发送反馈报文时使用） 2：重发报文（发送方应接收方要求，重新发送全量或部分报文时使用该状态） 3：重发报文反馈（接收方对发送方发送的重发报文进行反馈时使用该状态）
反馈状态	feedBack	number	是	300:成功接收 301：异常 302：异常，部分重传（使用相同事务编号，反馈描述中以List反馈需重传报文编号列表 ） 303：异常，全部重传（使用相同事务编号）
反馈描述	feedBackDesc	str	否	消息接收状态反馈说明，当反馈状态为302时，需要以List存储拟重传报文编号。
反馈报文发送时间	msgTimeStamp	str	是	如下格式的反馈报文发送时间戳"yyyy-MM-dd HH:mm:ss SSS"

4.4 报文体

报文体主要包含业务层面需要的信息，报文体包含三个类型：报文域、报文域块、报文组域块。

4.4.1 报文域

报文域是报文中最基本的数据元素。每个报文域表是一个基本的业务元素，报文域使用域名-域值（Key-Value 键值对）的形式表示。报文域遵循如下规范：

- 报文域名（Key）为报文数据内容的名称，以字符串表示，字符串由大小写英文字母、数字或下划线组成；
- 报文域值（Value）为报文数据内容的值，每个域值具有特定的数据类型和取值范围；

报文域可分为必填、选填、条件必填三种类型，其中条件必填指根据其他报文域的内容决定该报文域是否必填。

4.4.2 报文域块

报文域块指的是在业务逻辑上存在一定关系的报文域的集合。同样的报文域块可在多个报文类型中使用，报文域块拥有固定的名称，并包含固定的报文域，便于更好的理解数据报文的结构和业务含义。

4.4.3 报文组域块

报文组域块指的是可以多次重复的报文域、报文域块或报文组域块的集合，用以表示组类的业务数据。报文组域块应遵循如下规范：

- 报文组域块中重复出现的每个单元必须是相同的报文结构；
- 报文组域块的每个单元中的第一个报文域作为这个单元的关键域，关键域是必填项且关键域的域值在该报文组域块内唯一。

报文组域块中定义的报文域在每次重复时类型必须相同，即如果该域定义为必输，每次重复时都必填；如果该域定义为可填，每次重复时都可填；如果该域定义为条件必填，每次重复时都条件必填。

4.4.4 通用编码规则

1) 百分数相关字段：传输过程中统一用小数形式，如 85% 传输为“0.85”。
2) 字段序列化方式：对于数字、浮点、日期、文本等数据类型，传输时统一采用字符串格式进行序列化。
3) 字段名称格式按照 camelCase 规范，首字母小写，后续单词首字母大写。
4) 报文所有字段数据统一采用 UTF8 编码，报文整体按照 JSON 格式组织。
5) 报文中所有引用路径的字段中使用反斜杠“/”，JSON 字符串构造过程中需要将原始数据中转义字符：斜杠，单(双)引号，回车符、换行符等进行转义处理，确保 JSON 字符串重新转换为 JSON 对象后字段值与原始值的一致性。
6) 若无法提供非必填字段相关信息，如无特殊约定，报文中省略非必填字段。