**京东数科交易数据对接白皮书**

**2019/04/03**

目录

[1. 文档概述 3](#_Toc5292519)

[2. 文档对象 3](#_Toc5292520)

[3. 安全与协议约定 3](#_Toc5292521)

[3.1. 传输安全 3](#_Toc5292522)

[3.2. 数据安全 3](#_Toc5292523)

[3.3. 通讯签名 5](#_Toc5292524)

[3.4. 协议 6](#_Toc5292525)

[3.5. 其它约定 6](#_Toc5292526)

[4. 概要 6](#_Toc5292527)

[5. 资方需要提供的接口 6](#_Toc5292528)

[5.1. 公共请求结构（CommonRequest） 6](#_Toc5292529)

[5.2. 公共响应结构（CommonResponse） 7](#_Toc5292530)

[5.3. 接口-交易数据 8](#_Toc5292531)

# 文档概述

该文档用于京东与资方侧进行实时的数据交互，主要包括贷款和回款等数据。.京东侧在相关事件发生后，将交易数据推送到资方侧。

# 文档对象

京东、银行/资方的项目业务、产品、研发、测试人员使用，该文档请注意保密。

# 安全与协议约定

## 传输安全

目前使用专线或VPN方式来保证传输安全，建议使用更稳定的专线。

使用专线或者VPN需要提前申请网络，请提前确认好IP地址和端口。

IP地址请不要随意变更（变更流程比较繁琐耗时）。

请填写如下表并邮件到京东业务侧，待流程走完后京东侧会分配对应地址。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 业务信息 |  | | 访问方向 | 客户端\_源IP | 服务端\_目的IP | 目的端口 |
| 交易数据推送 |  | 京东→银行 | | 京东侧填写 （无需提供） | 资方提供  一个IP 这个IP应该是一个VIP，避免因服务扩容导致变化 | 资方提供  一个端口 |

如使用专线，请额外提供如下信息：

**专线对端所在地  
专线运营商  
专线带宽**

如使用VPN，请额外提供如下信息：

**用于对接VPN的公网IP**

## 数据安全

传输的数据需要加密

加密规则：则使用AES算法加密，采用CBC工作模式，使用PKCS5Padding填充方式。

例：使用key=21f2q678fas234dr对 "被加密的字符串"进行加密，得到加密后的结果为：FAhtOHhphIGfIqyDVdEXjmF6scKR68rcvhqEUkksSTY=

*例： AesUtils为java版加密工具，其它语言自行开发。*

**import** **org.apache.commons.codec.binary.Base64**;

**import** **javax.crypto.Cipher**;

**import** **javax.crypto.spec.IvParameterSpec**;

**import** **javax.crypto.spec.SecretKeySpec**;

**import** **java.security.MessageDigest**;

**public** **class** **AesUtils** {

**private** **static** **final** String[] HEX\_DIGITS = {"0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "a", "b", "c", "d", "e", "f" };

**public** **static** String encryptAES(String encryptKey, String plainTextData) **throws** Exception {

Cipher cipher = Cipher.getInstance( "AES/CBC/PKCS5Padding" );

byte[] raw = encryptKey.getBytes("utf-8");

IvParameterSpec iv = **new** IvParameterSpec(raw);

cipher.init( Cipher.ENCRYPT\_MODE, **new** SecretKeySpec( raw, "AES" ), iv );

byte[] encryptedData = cipher.doFinal( plainTextData.getBytes( "UTF-8" ) );

**return** Base64.encodeBase64String( encryptedData );

}

**public** **static** String decryptAES(String encryptKey, String encryptedData) **throws** Exception {

Cipher cipher = Cipher.getInstance( "AES/CBC/PKCS5Padding" );

byte[] raw = encryptKey.getBytes("utf-8");

IvParameterSpec iv = **new** IvParameterSpec(raw);

cipher.init( Cipher.DECRYPT\_MODE, **new** SecretKeySpec( raw, "AES" ), iv );

byte[] decryptedData = cipher.doFinal( Base64.decodeBase64( encryptedData ) );

**return** **new** String( decryptedData, "UTF-8" );

}

**public** **static** String sign(String data, String salt) **throws** Exception {

data = data + "|" + salt;

byte[] bytes = MessageDigest.getInstance( "MD5" ).digest( data.getBytes( "UTF-8" ) );

**return** byteToString( bytes );

}

**private** **static** String byteToString(byte[] bByte) {

StringBuilder sb = **new** StringBuilder();

**for** (byte aBByte : bByte) {

sb.append(byteToArrayString(aBByte));

}

**return** sb.toString();

}

**private** **static** String byteToArrayString(byte bByte) {

int iRet = bByte;

**if** (iRet < 0) {

iRet += 256;

}

int iD1 = iRet / 16;

int iD2 = iRet % 16;

**return** HEX\_DIGITS[iD1] + HEX\_DIGITS[iD2];

}

}

## 通讯签名

双方约定通讯签名密钥，需要按此签名密钥生成签名，签名验证通过后，才可进行后续逻辑。

签名规则：

第一步，将请求json加密，获得requestData字符串

第二步，requestData拼接上|salt 得到stringSignTemp字符串，并对stringSignTemp进行MD5运算，得到签名值sysSign

*例：AesUtils.java类的sign (String data, String salt)方法提供了签名算法。*

*例：*使用salt=123321123*对*FAhtOHhphIGfIqyDVdEXjmF6scKR68rcvhqEUkksSTY=进行签名，其中stringSignTemp=FAhtOHhphIGfIqyDVdEXjmF6scKR68rcvhqEUkksSTY=|123321123，得到签名sysSign=06215d8246c917dc9cf62457f5bc35f7

## 协议

传输协议：HTTP/HTTPS

报文格式：JSON

请求方法：以POST方式提交请求体中的json

*例：POST* [*http://ip:port/xxxx*](http://ip:port/xxxx)

请求体：{“key1”:“value1”,“key2”:“value2”}

响应体： {“key1”:“value1”,“key2”:”value2”}

*注：接收交易方提供请求路径URL。*

## 其它约定

字符集编码：UTF-8

时间格式：yyyyMMddHHmmss

金额单位：分

利率：支持6位小数

加密：测试开发环境**encryptKey**=1234561234561234，生产环境另行约定

签名：测试开发环境**salt**=789789，生产环境另行约定

# 概要

需要资方提供稳定可靠的接口，京东主动推送交易数据到资方，如果推送失败则会进行重试，对于资方接口故障导致长时间（6小时）仍无法推送过去的请求则会被废弃，所以请务必保证接口的简单快速。

京东侧不保证推送的顺序与业务发生顺序一致。

# 资方需要提供的接口

## 公共请求结构（CommonRequest）

公共请求结构是最外层JSON结构，用于封装请求数据，其中的requestData属性是被加密的业务数据，sysSign是对requestData的签名。

? 表示可选，! 表示必填，\* 表示有 0 到多， + 表示 1 到多个

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **参数** | **名称** | **类型** | **长度** | **约束** | **说明** |
|  | requestNo | 请求号 | String | 64 | ! | 请求唯一标识，每次请求唯一，由京东指定，无业务意义 |
|  | txCode | 交易码 | String | 32 | ! | 交易数据：**TRADE** |
|  | version | 版本号 | String | 32 | ! | 固定值：1.0 |
|  | channelCode | 渠道编号 | String | 16 | ! | 京东：JD |
|  | requestTime | 请求发送时间 | String | 14 | ! | 格式：yyyyMMddHHmmss |
|  | requestData | 请求数据封装 | String | 不限 | ! | 被加密的json格式数据。  将输入参数序列化为json字符串，将json字符串加密，即可得到requestData  **输入参数见各接口说明** |
|  | sysSign | 签名 | String | 64 | ! | requestData的MD5签名 |

说明：示例结构与数据

{

"requestNo":"xxxxx",

"txCode":"TRADE",

"version":"1.0",

"channelCode":"JD",

"requestTime":"20170717113038",

"requestData":"被加密的数据字符串",

"sysSign":"MD5签名"

}

## 公共响应结构（CommonResponse）

公共响应结构是最外层JSON结构，用于封装响应数据，其中responseData属性是被加密的业务相关数据，sysSign是对responseData的签名。

? 表示可选，! 表示必填，\* 表示有 0 到多， + 表示 1 到多个

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **参数** | **名称** | **类型** | **长度** | **约束** | **说明** |
|  | responseNo | 响应流水号 | String | 64 | ! | 请求号 相互透传回来 |
|  | responseTime | 响应时间 | String | 14 | ! | 格式：yyyyMMddHHmmss |
|  | code | 返回编码 | String | 8 | ! | 00000：成功  40000：请求非法，返回具体原因（通常是因为请求参数不合法或秘钥错误导致）  50000：服务内部错误，不返回具体原因（通常是因为服务器无法处理此请求）  99999：未知错误 |
|  | msg | 返回信息 | String | 不限 | ? | **失败情况下必填** |

说明：示例结构与数据

{

"responseNo":"1480905026153",

"responseTime":"20161205103026",

"code":"00000",

"msg":"成功"

}

## 接口-交易数据

接口地址：[http://ip:port/xxx/xxx（](http://ip:port/xxx/xxx（银行/)资方提供）

京东侧将以下结构对象转为json字符串，加密后填充到CommonRequest实例的requestData属性中，将CommonRequest实例序列化为json作为请求体传输。

其中requestData 信息要素如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **参数** | **名称** | **类型（长度）** | **约束** | **说明** |
|  | requestData |  |  | ! |  |
|  | pin | 客户标识 | String(256) | ！ | 用户在京东侧唯一标识 |
|  | businessType | 业务场景 | String(16) | ！ | XB-小白条  DB-大白条  JT-金条  XB\_QX-小白条取现 |
|  | loanNo | 贷款编号 | String(64) | ！ | 贷款编号 |
|  | type | 事件类型 | String(16) | ！ | Loan-借款 LoanSuccess-借款成功  Repayment-还款 Refund-退款 Reverse-冲销 Undertake-兜底代偿PartUndertake-部分兜底 Cancel-取消借款 |
|  | principal | 本金金额 | String(16) | ！ | 本金金额，单位-分 |
|  | interest | 息费金额 | String(16) | ！ | 息费金额，单位-分 |
|  | businessTime | 事件发生时间 | String(16) | ！ | yyyyMMddHHmmss |
|  | serial | 借款流水号 | String(16) | ? | 借款流水号-对账码  仅借款和出资事件有值 |