全国生活垃圾焚烧厂智能管控平台

联网数据传输技术要求

软件开发单位：

编写时间

版本号：

# 前言

## 概述

针对目前接口数据接入数据格式不够统一，结合当前全国平台数据接入需求，制定本接口文档。

## 术语

### 加密方式

1. 非对称加密

非对称加密算法需要两个密钥：公开密钥（publickey:简称公钥）和私有密钥（privatekey:简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。 非对称加密算法实现机密信息交换的基本过程是：接收数据一方(接收方)生成一对密钥并将公钥公开，需要向接收方发送信息的其他角色(发送方)使用该密钥(接收方的公钥)对机密信息进行加密后再发送给接收方；接收方再用自己私钥对加密后的信息进行解密。接收方想要回复发送方时正好相反，使用发送方的公钥对数据进行加密，同理，发送方使用自己的私钥来进行解密。

1. 对称加密

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。所谓对称，就是采用这种加密方法的双方使用方式用同样的密钥进行加密和解密。密钥是控制加密及解密过程的指令。算法是一组规则，规定如何进行加密和解密。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用，但由于加密和解密都使用同一个密钥，保证密钥的安全性尤为重要

基于对称加密及非对称加密的特点，本方案采用对称加密对发送数据进行加密，采用非对称加密方式加密对称加密的密钥之后传递对称加密的密钥从而保证密钥的安全性。

### 名词

* **数据发送方（以下简称：“发送方”）**

即代表生活垃圾焚烧厂，需要将数据按本技术要求传输到全国生活垃圾焚烧厂智慧管控平台。

* **数据接收方（以下简称：“接收方”）**

即全国生活垃圾焚烧厂智慧管控平台。

* **RSA**

基于非对称加密定义，加密密钥（即公开密钥）PK是公开信息，而解密密钥（即秘密密钥）SK是需要保密的。加密算法E和解密算法D也都是公开的。虽然解密密钥SK是由公开密钥PK决定的，但却不能根据PK计算出SK，基于上述理论产生RSA算法，它通常是先生成一对RSA密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA密钥至少为500位长，一般推荐使用1024位。本方案采用java实现基于RSA算法的非对称加密，密钥长度1024位。

* **AES**

密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，对称加密采用的算法，AES算法的区块长度固定为128位，密钥长度则可以是128，192或256位，本方案采用基于java实现的AES 128位 无向量，加密模式为ECB，填充模式为PKCS7Padding，密钥长度16byte,128位的对称加密。

* **ECB(Electronic Code Book电子密码本)模式**

最基本的加密模式，也就是通常理解的加密，相同的明文将永远加密成相同的密文，无初始向量，将加密的数据分成若干组，每组的大小跟加密密钥长度相同。然后每组都用相同的算法和密钥加密, 如果最后一个分组长度不够128位，需要填充。

* **PKCS7Padding填充模式**

PKCS7Padding模式，对于块的大小是不确定的，可以在1-255之间，填充值的算法都是一样的： value=k - (l mod k) ,K=块大小，l=数据长度，如果l=8, 则需要填充额外的8个byte的8

# 接口规则

## 协议规则

发送方将数据传输给接收方必须遵循以下规则：

|  |  |
| --- | --- |
| **传输方式** | 为了保证无差错、不丢失、不重复传递数据，采用TCP协议传输 |
| **数据格式** | 请求响应数据都为json格式 |
| **字符编码** | 统一采用UTF-8字符编码 |
| **身份认证** | 接收方需要对厂家标识进行身份认证，认证通过之后方可传输数据 |
| **数据加密算法** | AES与RSA两种算法相结合 |

## 参数规定

### 请求与响应协议结构

|  |  |
| --- | --- |
| 报文长度(4个字节) | 报文内容 |

每次请求或响应消息的前四个字节传递的为整个消息内容的长度，消息长度之后为消息内容。

### 公共的请求响应参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数名称** | **类型** | **长度(单位字节)** | **是否必填** | **参数说明** |
| msgType | byte | 1 | 是 | 消息类型，定义参看[消息类型定义](#_消息类型定义) |
| msgId | String | 8 | 否 | 每次请求唯一标识 |
| facKey | String | 128 | 是 | 发送方发送数据所需密钥(线下获取) |
| facId | String | 50 | 是 | 发送方注册唯一标识(线下获取) |
| msgContent | String | 不限长 | 是 | 请求或响应内容,json格式的字符串，不同消息类型对应的内容，由各个消息类型接口 |

请求时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| secretKey | String | 否 | 使用RSA公钥加密的AES密钥参数，传递数据时该参数必须传递 |
| data | String | 否 | 传递的数据信息，由各个接口自己定义 |

响应时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| success | Boolean | 是 | 成功时返回true，失败时返回false |
| message | String | 是 | 成功或失败原因 |
| data | String | 否 | 返回的数据，由各个接口自己定义 |

备注：以上为各个接口定义通用参数，每个接口只需定义msgContent里data参数的格式即可，接口定义章节定义的接口只针对msgContent json串中的data字段进行定义。

### 消息类型定义

|  |  |
| --- | --- |
| **标识** | **说明** |
| 1 | 身份认证消息 |
| 2 | 响应消息 |
| 3 | PING消息 |
| 4 | PONG消息 |
| 5 | 地磅数据消息 |
| 6 | 测点数据消息 |

## 安全规范

### 身份认证

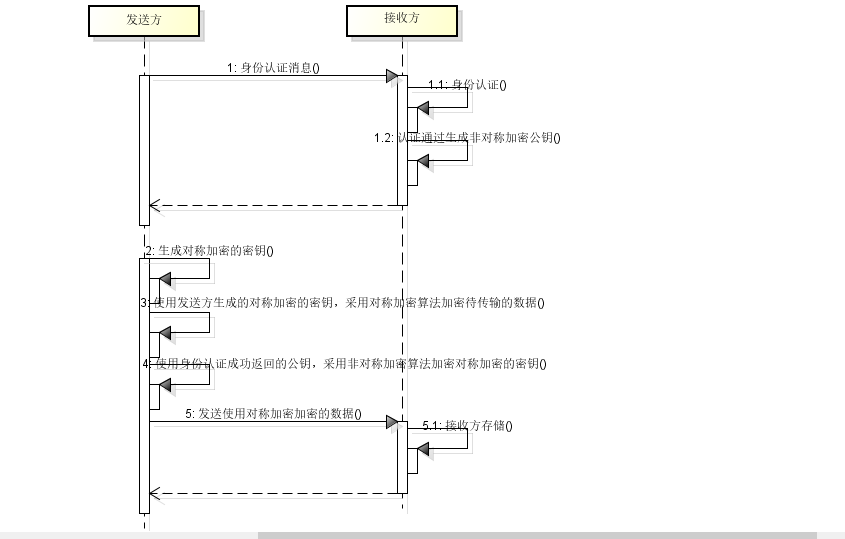
发送方联系接收方进行线下备案发送方相关信息，备案之后接收方给发送方提供facKey，facId两个请求参数值，发送方在发送数据之前需要带着备案之后拿到的两个参数发送消息类型为1的身份验证消息，接收方收到该消息会对发送方的身份进行校验，校验通过之后方可正常发送数据信息。

### 数据加密

发送方发送身份认证消息认证通过之后，接收方会返回给发送方一个RSA生成的公钥给发送方，发送方采用AES加密算法生成AES加密密钥，并使用该密钥对待传递的数据进行加密，为了保证AES加密所使用的密钥在传输过程中的安全性，发送方需使用RSA算法及身份认证通过之后收到的接收方返回的公钥进行加密，最后发送方使用采用AES加密过的数据及使用RSA算法加密过的AES加密密钥与接收方进行数据传递。为了保证AES加密的密钥的安全性，发送方也可以每次请求都随机生成一个AES加密的密钥对传递数据进行加密。

## 整体调用序列

发送方与接收方交互说明：



# 数据联网要求

## DCS、其它工控数据联网要求

DCS、其它工控数据均应以数字信号从DCS工控系统采集，通过正向网闸隔离，将采集的数据传入网闸外侧的接口机，由网闸外侧接口机将数据传输至全国管控平台（即数据接收方）。

数据采集和传输频率要求为1分钟。



## 地磅数据联网要求

地磅系统数据仅包括地磅称重明细，即榜单明细。

地磅系统数据均从地磅系统的数据库直接采集，数据采集设备将采集的数据输至全国管控平台（即数据接收方）。

数据采集和传输频率要求为5分钟。



# 接口定义

## 身份认证接口

### 使用场景

此接口用于发送方与接收方进行身份认证，发送方按照接口定义格式将facKey及facId信息发送给接收方，接收方会根据facKey及facId信息进行身份认证，认证通过之后按接口定义的返回格式返回给发送方一个使用RSA算法产生的公钥供发送方使用。

### 请求参数

请求响应公共字段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数名称** | **类型** | **长度(单位字节)** | **是否必填** | **参数说明** |
| msgType | byte | 1 | 是 | 本接口请求与响应该字段传递的值都为1 |
| msgId | String | 8 | 否 | 每次请求唯一标识 |
| facKey | String | 128 | 是 | 发送方发送数据所需密钥(线下获取) |
| facId | String | 50 | 是 | 发送方注册唯一标识(线下获取) |
| contentLength | int | 4 | 是 | 内容长度,即msgContent消息内容对应的字节数 |
| msgContent | String | 不限长 | 是 | 本接口msgContent对应的两个字段值都可以为空 |

msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| secretKey | String | 否 | 本接口无需填值 |
| data | String | 否 | 本接口无需填值，也可以传递说明性的描述 |

请求样例报文：

{

"msgType": 1,

"msgId": "000001",

"facKey": "1\_86h6Yhx16Ni634n",

"facId":”NWSP.SXJG01”,

"msgContent": "{\"secretKey\":null,\"data\":\"this is my authentication message.\"}"

}

### 响应参数

响应时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| success | Boolean | 是 | 成功时返回true，失败时返回false |
| message | String | 是 | 成功或失败原因 |
| data | String | 是 | 身份认证成功之后返回RSA加密对应的公钥信息 |

响应样例报文：

{

"msgType": 1,

"msgId": null,

"contentLength": 0,

"msgContent":"{\"success\":true,\"message\":\"成功\",

\"data\":\"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCSSCxvghVE0rtQWCIeqBJDq3MLwOnqOSIJ4HFJnL+Yo6Bwcvn4A50Eh8IaE/nmFm43nhAxWA6K9i7J2f5gNYmfRt8HmuwtkWh3Td5eJUnSEDw+IXA3OzAPgcMwbFGR6O1wv2jLbZPzUQVw2bfTG9Ba4yOOJC2kx4udUUSsJN2JKwIDAQAB\"}"

}

## 心跳检测

### 使用场景

本接口用于接收方探测发送方服务是否还正常，接收方在没有收到发送任何请求时，每隔固定时间就会发送一次心跳消息(消息类型为ping消息)给发送方，发送方接收到接收方的心跳消息需要给接收方一个响应(消息类型为pong消息)，如发送方长时间不给接收方任何响应，接收方则会自动断开与发送方的链接，断开连接之后发送方再次发送数据给接收方需要重新建立连接。

### 请求参数

请求响应公共字段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数名称** | **类型** | **长度(单位字节)** | **是否必填** | **参数说明** |
| msgType | byte | 1 | 是 | 本接口接收方发送心跳消息给发送方时需传3,发送方响应心跳需传4 |
| msgId | String | 8 | 否 | 每次请求唯一标识 |
| facKey | String | 128 | 是 | 发送方发送数据所需密钥(线下获取) |
| facId | String | 50 | 是 | 发送方注册唯一标识(线下获取) |
| contentLength | int | 4 | 是 | 内容长度,即msgContent消息内容对应的字节数 |
| msgContent | String | 不限长 | 是 | 本接口msgContent对应的两个字段值都可以为空 |

msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| secretKey | String | 否 | 本接口无需填值 |
| data | String | 否 | 本接口无需填值，也可以传递说明性的描述 |

请求样例报文：

{

"msgType": 3,

"msgId": "000001",

"facKey": "1\_86h6Yhx16Ni634n",

"facId":”NWSP.SXJG01”,

"contentLength": 0,

"msgContent": "{\"secretKey\":null,\"data\":\"ping\"}"

}

### 响应参数

响应时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| success | Boolean | 是 | 成功时返回true，失败时返回false |
| message | String | 是 | 成功或失败原因 |
| data | String | 否 | 本接口该字段返回可为空 |

响应样例报文：

{

"msgType": 4,

"msgId": null,

"contentLength": 0,

"msgContent":"{\"success\":true,\"message\":\"成功\",

\"data\":\"pong\"}"

}

## 地磅数据传输

### 使用场景

该接口用于持续传输地磅称重流水的增量数据，地磅数据以具备进、出厂信息为完整信息，每次传输的称重流水信息必须是完整。

如实际运行存在修改场景（如补单、更正、作废），监管平台会根据每条称重信息的流水号作为本记录的唯一标识进行验证是否已同步。如在监管平台中存在，则进行修改；如在监管平台中不存在，则进行新增。

### 请求参数

请求响应公共字段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数名称** | **类型** | **长度(单位字节)** | **是否必填** | **参数说明** |
| msgType | byte | 1 | 是 | 本接口发送方发送数据时需传5,接收端响应该字段传递的值为2 |
| msgId | String | 8 | 否 | 每次请求唯一标识 |
| facKey | String | 128 | 是 | 发送方发送数据所需密钥(线下获取) |
| facId | String | 50 | 是 | 发送方注册唯一标识(线下获取) |
| contentLength | int | 4 | 是 | 内容长度,即msgContent消息内容对应的字节数 |
| msgContent | String | 不限长 | 是 | 本接口传递地磅的数据信息，json格式 |

msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| secretKey | String | 是 | 本接口该字段传递的值为：身份认证成功之后收到的RSA公钥加密AES加密地磅数据所使用的密钥 |
| data | String | 否 | 地磅数据，json格式，一次可以传递多条地磅数据 |

单条地磅数据格式定义：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| lsh | String | 是 | 流水号(唯一) |
| carNo | String | 是 | 车牌号 |
| cardNo | String | 是 | ic卡号 |
| proCode | Integer | 是 | 1：生活垃圾；2：飞灰；3：炉渣；4：渗滤液；5：活性炭；6：消石灰；7：螯合剂；8：水泥；9：氨水；10：盐酸 |
| originalSourceArea | String | 否 | 地磅系统中的货物来源 |
| transportUnit | String | 否 | 运输单位 |
| firstWeightTime | Date | 是 | 进厂时间，精确到时分秒 |
| secondWeightTime | Date | 是 | 出厂时间，精确到时分秒 |
| gross | Double | 是 | 毛重，单位：kg |
| tare | Double | 是 | 皮重，单位：kg |
| net | Double | 是 | 净重，单位：kg |
| operator | String | 否 | 称重员 |
| tradeSysId | Long | 否 | 地磅系统id，如存在多个地磅称重系统，可用序号：1、2……来区分 |
| orgId | Long | 否 | 组织id |
| dataStatus | int | 否 | 数据状态 1:生效 2:作废 |
| statDateNum | Integer | 是 | 磅单归属日期，值为出厂时间(secondWeightTime)的日期格式化，格式为：yyyyMMdd，样例：20210630 |

未加密的地磅明文数据样例格式：

[{

"lsh": "流水号1",

"carNo": "车牌号1",

"cardNo": "车牌卡号1",

"proCode": 1,

"originalSourceArea": null,

"transportUnit": null,

"firstWeightTime": null,

"secondWeightTime": null,

"gross": 4000.00,

"tare": 1900.00,

"net": 2100.00,

"operator": null,

"tradeSysId": 1,

"orgId": null,

"dataStatus": 0

},

{

"lsh": "流水号2",

"carNo": "车牌号2",

"cardNo": "车牌卡号2",

"proCode": 1,

"originalSourceArea": null,

"transportUnit": null,

"firstWeightTime": null,

"secondWeightTime": null,

"gross": 4000.00,

"tare": 1900.00,

"net": 2100.00,

"operator": null,

"tradeSysId": 1,

"orgId": null,

"dataStatus": 0

}]

请求的原始报文(数据被加密的)：

{

"facKey": "1\_86h6Yhx16Ni634n",

"facId": “NWSP.SXJG01”,

"msgType": 5,

"msgId": null,

"contentLength": 0,

"msgContent": "

{

\"secretKey\":\"jE5OjpHEJlng5HOvp0fQn0OJiL+K+aI0utEMuxk1bJhp8PNGXq7C47XhxBh5odykdP8bS8TZEdKO6/lgKMoVoVid/mRS0UNvoqeyKn/zhnuliCXUniJkDeujvJzc8i04IWv8LIhrV8pmUakElRXpm/bf49anWugWdFQFla32vtE\\u003d\",

\"data\":\"AES加密的上述地磅明文数据\"}"

}

### 响应参数

响应时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| success | Boolean | 是 | 成功时返回true，失败时返回false |
| message | String | 是 | 成功或失败原因 |
| data | String | 否 | 本接口该字段返回为空 |

响应样例报文：

{

"facKey": “1\_86h6Yhx16Ni634n”,

"facId": “NWSP.SXJG01”,

"msgType": 2,

"msgId": null,

"contentLength": 0,

"msgContent": "{\"success\":true,\"message\":\"成功\",\"data\":null}"

}

## 运行测点数据传输

### 使用场景

本接口用于接收运行的实施测点数据。

### 请求参数

请求响应公共字段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数名称** | **类型** | **长度(单位字节)** | **是否必填** | **参数说明** |
| msgType | byte | 1 | 是 | 本接口发送方发送数据时需传6,接收端响应该字段传递的值为2 |
| msgId | String | 8 | 否 | 每次请求唯一标识 |
| facKey | String | 128 | 是 | 发送方发送数据所需密钥(线下获取) |
| facId | String | 50 | 是 | 发送方注册唯一标识(线下获取) |
| contentLength | int | 4 | 是 | 内容长度,即msgContent消息内容对应的字节数 |
| msgContent | String | 不限长 | 是 | 本接口传递测点的数据信息，json格式 |

msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| secretKey | String | 是 | 本接口该字段传递的值为：身份认证成功之后收到的RSA公钥加密AES加密地磅数据所使用的密钥 |
| data | String | 否 | 测点数据，json格式，一次可以传递多条测点数据 |

单条测点数据格式定义：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| itemCode | String | 是 | 测点在管控平台的CODE |
| itemValue | String | 是 | 测点的值 |
| sourceCode | String | 是 | 测点在源系统的code |
| instanceTime | Date | 是 | 测点数据的监测时间 |
| sysId | int | 否 | 系统编号(用于区分同一个电厂的一期、二期) |

未加密的测点明文数据样例格式：

[{

"itemCode":”测点CODE值”,

"itemValue":”测点值”,

"instanceTime":null,

"sourceCode":”测点在源系统的code”,

"sysId":1

},

{

"itemCode":“测点CODE值”,

"itemValue":”测点值”,

"instanceTime":null,

"createTime":null,

"equipmentId":null,

"sysId":1,

"orgId":null

}]

请求的原始报文（数据被加密的）

{

"facKey":"1\_86h6Yhx16Ni634n",

"facId":”NWSP.SXJG01”,

"msgType":6,

"msgId":null,

"contentLength":0,

"msgContent":"{

\"secretKey\":\"Zm6o62cal/w7czL0q/Y9yw1ynWC4BC8GLb/u657I9Y0ghpKMkRC1vB41iqqyMJhpUEYsNIx1LNORdeqDNrPL+94PKKAbHrKhDrpAQEWnC1q8GYJvDvY92mTloMCjmkc/qY3UN6p4TJv/SJ5+ddfFBiS50kv95MuYJN2Ne9DjNyE\\u003d\",

\"data\":\"AES加密的上述测点明文数据\"

}"

}

### 响应参数

响应时msgContent对应的json数据参数定义如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数名称** | **类型** | **是否必填** | **参数说明** |
| success | Boolean | 是 | 成功时返回true，失败时返回false |
| message | String | 是 | 成功或失败原因 |
| data | String | 否 | 本接口该字段返回为空 |

响应样例报文：

{

"facKey":”1\_86h6Yhx16Ni634n”,

"facId":”NWSP.SXJG01”,

"msgType":2,

"msgId":null,

"contentLength":0,

"msgContent":

"{\"success\":true,\"message\"：\"成功\",\"data\":null}"

}

# 修订记录

|  |  |  |
| --- | --- | --- |
| **修订日期** | **版本** | **修订原因** |
| 2020-09-29 | 1.0 | 创建文档草案，定义接口协议及规范，并定义测点及地磅数据接入接口定义。 |
| 2021-07-06 | 1.1 | 调整地磅数据传输接口的请求报文字段名，并增加一个磅单归属日期字段 |
| 2021-07-29 | 1.2 | 调整文档中测点数据发送报文字段参数定义与样例报文不一致 |