能源管理平台开放接口规范

1 功能描述

公共接口共支持1个功能，分别是：

- 查询电表实时数据

2 公共信息对象

2.1 电表历史数据（historyElectricityInfo）

用于描述电表实时数据的一些基础信息

运营商	字段	描述	必填	类型	长度
设备编码	pointId	设备编码	是	字符串	<=20 字符
当前表码	bm	默认：0.00	是	浮点数	保留小数点后两位
数据时间	dataTime	yyyy-MM-dd HH:mm:ss	是	字符串	

表1.1 电表历史数据

3 接口规范

3.1 概述

为了满足上述业务流程的定义，一共有1个接口，分别为：

- 查询电表历史数据

3.2 查询电表最近历史数据

3.2.1 概述

此接口用于查询电表最近一条的历史数据。

3.2.2 接口定义

接口名称：query_lastHistoryElectricity_info
接口使用方法：由设备运营商方实现此接口，数据需求方调用。

3.2.3 输入参数

输入参数定义请参见表1.1：

参数名称	定义	参数类型	描述

用户编码	pointId	字符串	设备编码信息

表1.2 查询电表最近历史数据输入参数

3.2.4 返回值

返回值定义请参见表2.9：

参数名称	定义	参数类型	描述
用户账户信息	historyElectricityInfo	historyElectricityInfo	类型“historyElectricityInfo”参照 2.5

表1.2 查询电表最近历史数据返回值

3.2.5 示例

```
{
    "pointId": "000000000004",
    "bm": 555.55,
    "dataTime": "2017-06-01 09:02:55"
 }
```

4 数据传输体系

4.1 概述

数据传输体系要求了参与能源管理服务的各角色和实体之间应在正常、安全、有效的原则下通过规范的接口进行信息交换，相互协同地向用电用户提供服务。

能源管理服务信息通过数据传输接口进行交换，数据传输接口众多，既存在于各个服务逻辑层之间，也存在于同一逻辑层的不同管理域之间，数据传输接口可通过身份认证、访问控制、数据加密、数字签名等安全措施，保障数据传输过程中要保障所传输数据的机密性和安全性。

4.2 数据传输一般流程

能源管理服务信息交换一般需要经过平台认证、数据请求和数据返回3个步骤。

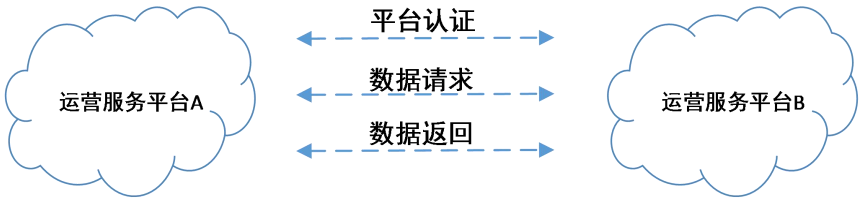

图 1 数据传输

4.3 数据传输接口的基本要求

运营商须提供严格的系统安全保密机制，保障信息交换接口安全、稳定、可靠地运行，包括信息的存取控制、应用系统操作的安全等。基本要求：

1)采用身份认证、访问控制、数据加密、数字签名等安全措施；

2)采用安全可靠并且普遍使用的加密算法；

3)密钥的存贮和交易信息的加密／解密需要在安全的环境中；

4)遵循数据安全保密的国家和行业标准；

5)定期更换密钥；

6)具备对报文做来源正确性鉴别的机制（HMAC）。

4.4 密钥体系

每个运营商交互前需要分配运营商标识（operatorId）、运营商密钥（operatorSecret）、消息密钥（dataSecret）、消息密钥初始化向量（dataSecretIV）和签名密钥（sigSecret）。

1)运营商标识（operatorId）：固定9位，运营商的组织机构代码，作为运营商的唯一标示。

2)运营商密钥（operatorSecret）:可采用32H、48H和64H，由 0-F字符组成，为申请认证使用。

3)消息密钥（dataSecret）:用于对所有接口中Data信息进行加密。

4)消息密钥初始化向量（dataSecretIV）：固定16位，用户AES加密过程的混合加密。

5)签名密钥（sigSecret）：可采用32H、48H和64H，由 0-F字符组成，为签名的加密密钥。

5 平台认证方式及规则

5.1 概述

能源管理服务信息交换应具备平台认证服务提供平台之间的鉴权认证功能。平台之间在信息交换前，需完成平台认证，获得平台交换能力。

5.2 平台认证模式

平台认证支持分布式认证模式。

分布式认证模式由运营商之间进行鉴权认证，运营商之间确定运营商标识（operatorID）、运营商密钥（operatorSecret）、消息密钥（dataSecret）、消息密钥初始化向量（dataSecretIV）和签名密钥（sigSecret），具体认证方式可由运营商协商确定。

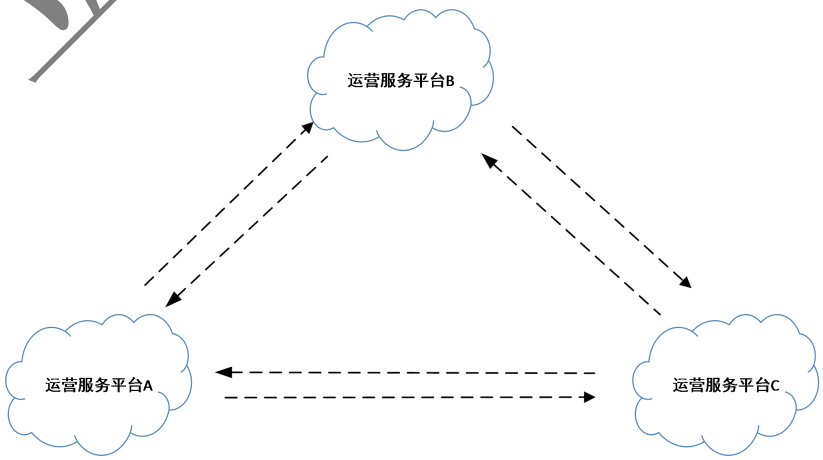

图 2 分布式认证模式

5.3 平台认证方法

平台认证宜采取身份认证和访问控制相结合的方式进行。

身份认证可采取用户名/口令认证、密钥认证或数字证书认证等方式进行；访问控制可采取IP访问控制、时间访问控制等多种手段结合。

用户身份认证成功后授予token，每次向服务端请求资源的时候需要带着服务端签发的token，服务端验证token成功后，才返回请求的数据。token的有效期由服务方确定，最长不应超过7天，token丢失或失效后需要再次发起认证服务。

图 3　平台认证方式

6　数据传输方式及规则

6.1　数据传输接口规则

所有数据传输接口均采用HTTP(S)接口，每个接口的URL均采用如下格式定义：

http(s)://[域名]/emcp/v[版本号]/[接口名称]

1)域名：各接入运营商所属域名。

2)版本号：代表接口版本号，不同的版本地址对应相应版本代码。系统升级期间，新旧版本可同时存在，待所有接入方都切换到新接口，旧接口即可下线。从而达到平滑升级的目的。

3)接口名称：所请求/调用接口的名称，具体接口名称见接口规范部分。

为保证各接口的功能明确清晰，每个URL只允许对应一种功能。

6.2　接口调用方式

所有接口均使用HTTP(S)/POST方式传输参数，传输过程中应包含消息头和消息主体两部分。

6.3　消息头规范

消息头一般需包含内容类型和授权信息（authorization）。

内容类型（Content-Type）字段用于标识请求中的消息主体的编码方式，本标准中所规范的信息交换内容均采用JSON的方式，参数信息采用utf-8编码，因此需要配置消息头中的Content-Type 为application/json;charset=utf-8。

授权信息（authorization）字段用于证明客户端有权查看某个资源，本标准中所规范的授权信息采用凭证(token)的方式，因此需要在配置消息头中的authorization 为token。

6.4　消息主体规范

消息主体是信息交换过程中的具体内容。

6.4.1 申请服务规则

一般由运营商标识（operatorId）、参数内容（data）、时间戳（timeStamp）、自增序列（seq）和数字签名（sig）组成。

表 1 消息主体内容表

参数名	说明	举例
operatorId	运营商标识	
data	各接口具体请求参数信息	data: 密文
timeStamp	时间戳	接口请求时时间戳信息,格式为 yyyyMMddHHmmss
seq	自增序列	4 位自增序列取自时间戳，同一秒内按序列自增长，新秒重计。如 0001
sig	参数签名	

6.4.2 返回参数规则

表 2 返回消息主体内容表

参数名	说明	举例
operatorId	运营商标识	
data	各接口返回信息	data: 密文
msg	返回信息戳	msg：系统繁忙
ret	返回值	ret:-1
sig	参数签名	

数据传输接口的返回参数一般由运营商标识（operatorId）、返回值（ret）、返回信息（msg）、参数内容（data）和数字签名（sig）组成。

1)ret:必填字段，返回编码参考下表。

2)msg:必填字段，有错误表示具体错误信息，无错误返回成功信息。

3)data:参数内容，具体返回参数见接口规范部分，采用utf-8编码，JSON格式。

表 3 返回参数编码表

Ret 值	说明
-1	系统繁忙，此时请求方稍后重试
0	请求成功
4001	签名错误
4002	token 错误
4003	POST 参数不合法,缺少必须的示例：

	operatorId,sig,timeStamp,data，seq 五个参数
4004	请求的业务参数不合法，各接口定义自己的必须参数
500	系统错误

7 密钥的使用及管理

各运营商系统间在消息传递时，需要保障传输和接收数据的安全和完整。

7.1 基本安全要求

运营商必须满足数据安全传输控制方面的要求。

运营商必须提供严格的系统安全保密机制，保障信息交换接口安全、稳定、可靠地运行，包括信息的存取控制、应用系统操作的安全等。

7.2 密钥的安全要求

密码算法用于密钥的产生、分发、HMAC以及加密等安全功能，相关的算法模块在其生命周期内不能被修改、导出至安全环境外部。

指定功能的密钥仅能做指定功能使用，不能被其他任何功能使用。

7.2.1 密钥的产生

数据密钥应具备随机产生特性，密钥产生后要检查密钥的有效性，弱密钥和半弱密钥需被剔除。

运营商加入信息交换时，必须申请独立的密钥文件，密钥可由运营商协商产生。

7.2.2 密钥的分发

密钥的分发应该由安全方式进行，可通过线下分发、联机报文或数字信封的方式加密传输。

7.2.3 密钥的存储

密钥宜保存在硬件加密机内。如果出现在硬件加密机外，则必须密文方式出现。

密钥注入、密钥管理和密钥档案的保管应由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。

7.2.4 密钥的销毁

当新密钥产生后，生命期结束的旧密钥必须从数据库和内存中清除，防止被替换使用；同时所有可能重新构造此密钥的信息也必须清除。新密钥成功启用和旧密钥自动销毁的记录将被更新。

7.3 数据的加密处理

7.3.1 数据加密规则

消息发送方需要对data字段中涉及交易及隐私等数据利用消息密钥（dataSecret）进行加密。

消息接收方收到消息之后，根据消息密钥（dataSecret）对消息体中的data数据进行解密，校验参数合法性等后续业务处理。

7.3.2 数据加/解密方法

数据传输的加密使用对称加密算法AES 128位加密，加密模式采用CBC，填充模式采用PKCS5Padding方式。

7.3.3 数据加/解密示例

消息密钥：1234567890abcdef

消息密钥初始化向量：1234567890abcdef

示例明文信息：

```
{
        "totalMoney": 555.55,
        "usableMoney": 555.55,
        "freezeMoney": 0,
 }
```

示例秘文：

```
CyXjEvuZudqhb21eCEtgfMimRHZQiJ2c22aLw90ZvtNV4XUkCWQKU22SSWkcJbUIt7kr
oudB/PZVFG6ICfmjJQ==
```

8 参数签名规范

8.1 参数签名要求

参数签名采用HMAC-MD5算法，采用MD5作为散列函数，通过签名密钥（sigSecret）对整个消息主体进行加密，然后采用Md5信息摘要的方式形成新的密文，参数签名要求大写。

参数签名顺序按照消息体顺序拼接后执行，

申请服务方：拼接顺序为运营商标识（operatorId）、参数内容（data）、时间戳（timeStamp）、自增序列（seq）。

返回参数方：拼接顺序为返回值（ret）返回信息（msg）返回内容（data）

8.2 参数签名方法

（1）HMAC-MD5算法

HMAC（K，M）=H（K⊕opad∣H（K⊕ipad∣M））

其中:K是密钥（sigSecret），长度可为64字节，若小于该长度，在密钥后面用“0”补齐。

M是消息内容;

H是散列函数;

opad和Ipad分别是由若干个0x5c和0x36组成的字符串;

⊕表示异或运算;

∣表示连接操作。

（2）HMAC-MD5流程

1）在签名密钥（sigSecret）后面添加0来创建一个长为64字节的字符串(str);

2)将上一步生成的字符串(str)与ipad(0x36)做异或运算，形成结果字符串(istr)；
3)将消息内容data附加到第二步的结果字符串(istr)的末尾；
4)做md5运算于第三步生成的数据流(istr)；
5)将第一步生成的字符串(str)与opad(0x5c)做异或运算，形成结果字符串(ostr)；
6)再将第四步的结果(istr)附加到第五步的结果字符串(ostr)的末尾；
7)做md5运算于第六步生成的数据流(ostr)，输出最终结果(out)。

8.3 参数签名示例

示例签名密钥：1234567890abcdef

示例运营商标识（operatorId）：123456789

示例明文信息：

```
{
        "userId": "1"
 }
```

示例密文信息（data）：

57bvzaVpNVS7HXimcMsq0g==

示例时间戳（timeStamp）：20170729142400

示例自增序列（seq）：0001

示例签名（sig）：575D190DF112C17FAACBF847477BF62F

附 录 A
（规范性附录）

A.1 概述

此接口用于平台之间认证token的申请，token作为全局唯一凭证，调用各接口时均需要使用。

A.2 接口定义

接口名称：query_token
接口使用方法：由服务端实现此接口，需求端调用。

A.3 输入参数

参数名称	定义	参数类型	描述
运营商标识	operatorId	字符串	运营商组织机构代码
运营商密钥	operatorSecret	字符串	运营商分配的唯一识别密钥

A.4 返回值

参数名称	定义	参数类型	描述
运营商标识	operatorId	字符串	运营商组织机构代码
成功状态	succStat	整型	0:成功; 1:失败
获取的凭证	accessToken	字符串	全局唯一凭证
凭证有效期	tokenAvailableTime	整型	凭证有效期，单位秒
失败原因	failReason	整型	0:无; 1:无此运营商; 2:密钥错误; 3~99:自定义