北京市充电设施公共服务管理平台互联互通技术对接实施细则

第 4 部分：数据传输与安全

目　　次

前　　言

《北京市充电设施公共服务管理平台互联互通技术对接实施细则》本次制定共分为四个部分：

——第 1 部分：总则；

——第 2 部分：公共信息交换规范；

——第 3 部分：业务信息交换规范；

——第 4 部分：数据传输及安全；

本部分为第4部分。

编制说明：

为普及充电设施快速推广，提高行业整体服务质量，提升用户充电服务体验，加大政府监管及扶持力度，为支撑政府信息监管平台的实际需求，特基于行业一致认可的《T / CEC 102.4—2016 电动汽车充换电服务台信息交换》为蓝本进行了修订和扩充，本稿中蓝色字体为修订内容。

北京市充电设施公共服务管理平台互联互通技术对接实施细则

第4部分：数据传输与安全

1 范围

本部分确立了北京市充电设施公共服务管理平台互联互通技术对接实施细则的数据传输和安全防护的一般原则，包含充换电服务信息交换的数据传输体系、平台认证要求、密钥的管理和使用要求。

本部分适用于不同运营商服务平台之间的充换电服务信息交换,以及电动汽车充换电运营服务平台与第三方服务及政府监管平台之间的信息交换。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2260-2007 中华人民共和国行政区域代码

GB/T 7408-2005 数据元和交换格式信息交换日期和时间表示法

GB/T 9387.1-1998 信息技术 开放系统互联 基本参考模型 第1部分：基本模型

GB/Z 19027-2005 统计技术指南

GB/T 19596-2004 电动汽车术语

GB/T 18391.1-2002 信息技术 数据元的规范与标准化 第1部分：数据元的规范与标准化框架

GB/T 25070-2010 信息安全技术信息系统等级保护安全设计技术要求

GB/T 20271-2006 信息安全技术信息系统安全通用技术要求

GB/T 20988-2007 信息安全技术信息系统灾难恢复规范

GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求

GB/T 29317-2012 电动汽车充换电设施术语

3 术语和定义

GB/T 19596、GB/T 29317、GB/Z 19027-2005以及《北京市充电设施公共服务管理平台互联互通技术对接实施细则 第1部分：总则》中定义的术语和定义适用于本文件。

4 数据传输体系

4.1 数据传输一般流程

北京市充电设施公共服务管理平台互联互通技术对接实施细则一般需要经过平台认证、请求和应答3个步骤。

4.2 数据传输接口

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]/evcs/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《北京市充电设施公共服务管理平台互联互通技术对接实施细则 第2部分：公共信息交换规范》和《北京市充电设施公共服务管理平台互联互通技术对接实施细则 第3部分：业务信息交换规范》。

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。

4.3 接口调用方式

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

4.4 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令牌（Token）的方式，因此需要在配置消息头中的Authorization 为Bearer Token。

4.5 消息主体规范

4.5.1 服务申请

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	各接口具体参数信息	"Data":{
		"ItemSize":1,
		"PageCount":1,
		"PageNO":1,
		"StationInfos":{
		"OperationID":"123456789",
		"PlatformID":"123456789",
		"StationID":"000000000000001",
		"StationName":
		"\U5145\U7535\U7ad9\U540d\U79f0",
		"CountryCode":"Cn",
		"AreaCode":"441781",
		"Address":"\U5730\U5740",
		"ServiceTel":"123456789",
		"StationType":1,
		"StationStatus":50,

		"ParkNums": 3,
		"Lng": 119.97049,
		"Lat": 31.717877,
		"Construction": 1,
		"EquipmentInfos": [
		{
		"EquipmentID": "10000000000000000000003",
		"ManufacturerID": "123456789",
		"EquipmentModel": "P3",
		"ProductionDate": "2016-04-26",
		"EquipmentType": 3,
		"ConnectorInfos": [
		{
		"ConnectorID": "1",
		"ConnectorType": 1,
		"VoltageUpperLimits": 220,
		"VoltageLowerLimits": 220,
		"Current": 15,
		"Power": 3.3
		}
		]
		}
		]
		}
		}

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	

4.5.2 参数返回

数据传输接口的返回参数一般由返回值（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《北京市充电设施公共服务管理平台互联互通技术对接实施细则 第2部分：公共信息交换规范》、《北京市充电设施公共服务管理平台互联互通技术对接实施细则 第3部分：业务信息交换规范》，采用utf-8编码，JSON格式。

4)Sig:必填字段，按签名规则， 用Ret+Msg+Data生成返回签名。

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

4.6 重发机制

数据传输过程中应设置重发机制，重发次数应大于3次，重发周期宜为1分钟。

4.7 批量数据传输

数据传输接口中的Data字段可为数组型的JSON格式，数据发送方可通过该字段实现批量数据的传输。

5 平台认证要求

5.1 基本要求

北京市充电设施公共服务管理平台互联互通技术对接实施细则应根据国家信息安全等级保护相关要求。

北京市充电设施公共服务管理平台互联互通技术对接实施细则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。

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；

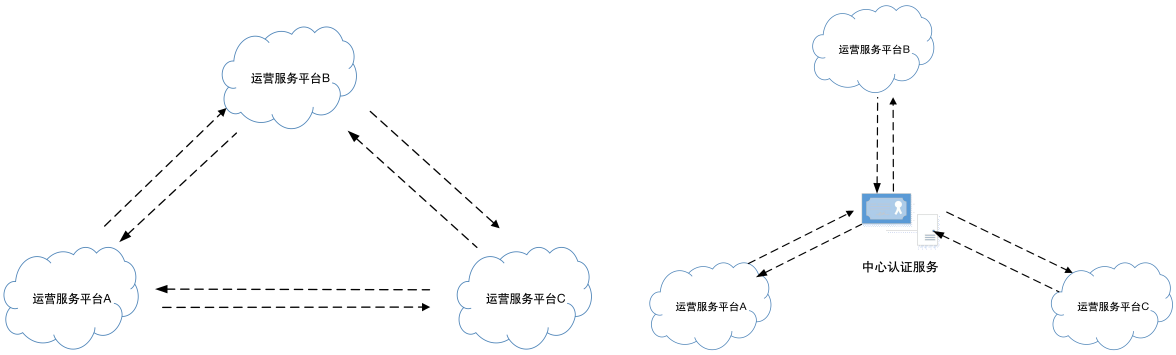
6)具备对报文做来源正确性鉴别的机制 （HMAC） 。

5.2 平台认证方式及规则

5.2.1 平台认证模式

平台认证应支持分布式认证模式或中心交换认证模式，具体结构参见图1。

分布式认证模式由运营商之间进行鉴权认证，具体认证方式可由运营商协商确定。中心交换认证模式由统一的认证服务方提供鉴权认证服务，具体认证方式由各运营商和认证服务方共同确定。



a） 分布式认证模式　　b）中心交换认证模式

图 1　认证模式

5.2.2　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，相关流程参见图2。

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。认证接口规范参见附录A。

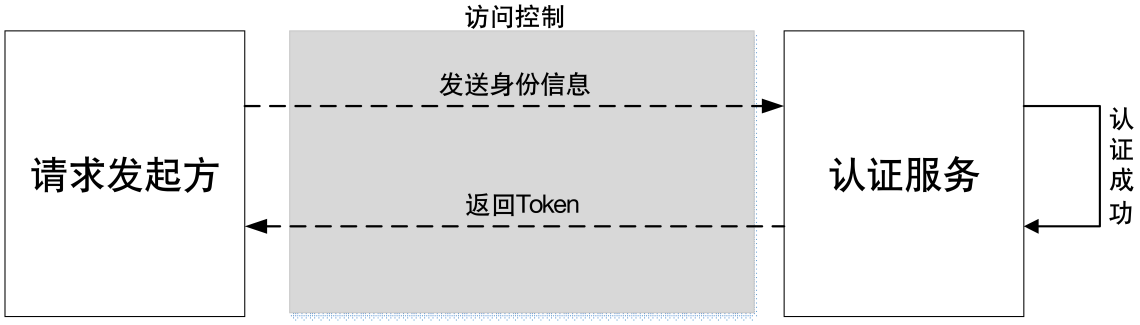


图 2　平台认证方式

6　密钥的管理和使用

6.1　基本要求

运营商应满足数据安全传输控制方面的要求。

运营商应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。

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。

6.2　密钥的分类

每个运营商交互前需要分配运营商标识、运营商密钥、消息密钥、消息密钥初始化向量和签名密钥。具体要求如下：

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。

6.3 密钥的管理

6.3.1 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。

6.3.2 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。

6.3.3 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。

6.3.4 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。

6.4 密钥的使用

6.4.1 数据的加解密处理

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。具体加解密方法和示例见附录B。

6.4.2 参数签名规范

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，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）。具体参数签名方法和示例见附录C。

附　录　A
（规范性附录）
分布式认证的认证接口规范

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	请求方组织机构代码
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	返回方组织机构代码
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

A.5　示例

无

附 录 B
（资料性附录）
数据加密方式

B.1 数据加密方法

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。

B.2 数据加密示例

示例密钥：1234567890abcdef

示例初始向量：1234567890abcdef

示例明文信息：

示例：{"OperatorSecret": "1234567890abcdef", "OperatorID": "123456789"}

示例秘文：

BmuQPtmtMfSqKqTPqiWVUJsPzr3E/HcaBHBkRN5yqdjkQAEzz1H9SHq+/NCa3XLLIo3o019uPEH3qHPCXiFgrUkqIicd8AFWszg1moI9Mzo=

附 录 C
（资料性附录）
HMAC-MD5 参数签名方式

C.1 HMAC-MD5 参数签名算法

HMAC（K，M）=H（K⊕opad｜H（K⊕ipad｜M））

其中:K是密钥（OperatorSecret），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。

C.2 HMAC-MD5 参数签名流程

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)。

C.3 参数签名示例

示例签名密钥：1234567890abcdef

示例运营商标识（OperatorID）：123456789

示例参数信息（Data）：

il7B0BSEjFdzpyKzfOFpvg/Se1CP802RItKYFPfSLRxJ3jf0bVl9hvYOEktPAYW2nd7S8MBcyHYy

acHKbISq5iTmDzG+ivnR+SZJv3USNTYVMz9rCQVSxd0cLlqsJauko79NnwQJbzDTyLooYoIwz7

5qBOH2/xOMirpeEqRJrF/EQjWekJmGk9RtboXePu2rka+Xm51syBPhiXJAq0GfbfaFu9tNqs/e2Vjj

a/ltE1M0lqvxfXQ6da6HrThsm5id4ClZFIi0acRfrsPLRixS/IQYtksxghvJwbqOsbIsITail9Ayy4tKcoge

EZiOO+4Ed264NSKmk7l3wKwJLAFjCFogBx8GE3OBz4pqcAn/ydA=

示例时间戳（TimeStamp）：20160729142400

示例自增序列（Seq）：0001

示例签名（Sig）：745166E8C43C84D37FFEC0F529C4136F
