



# 中华人民共和国国家标准

GB/T XXXXX—XXXX

## 数据基础设施 连接器技术要求

Data infrastructure—Technical requirements for connector

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

国家市场监督管理总局  
国家标准化管理委员会 发布

目 次

前 言 ..... IV

引 言 ..... V

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 总体要求 ..... 2

6 能力要求 ..... 3

    6.1 总体架构 ..... 3

    6.2 标准能力 ..... 4

        6.2.1 身份认证 ..... 4

        6.2.2 网络接入 ..... 4

        6.2.3 数据交付 ..... 4

        6.2.4 数据访问控制 ..... 4

        6.2.5 日志记录 ..... 4

        6.2.6 运行状态上报 ..... 5

    6.3 扩展能力 ..... 5

        6.3.1 数据资源管理 ..... 5

        6.3.2 数据产品管理 ..... 5

        6.3.3 数字合约管理 ..... 5

        6.3.4 数据产品目录服务 ..... 5

        6.3.5 数据使用控制 ..... 5

        6.3.6 隐私保护计算能力集成 ..... 6

        6.3.7 高速数据网接入 ..... 6

        6.3.8 其他关键技术组件扩展 ..... 6

7 互操作要求 ..... 6

    7.1 接入连接器身份认证要求 ..... 6

    7.2 数据产品目录查询要求 ..... 6

        7.2.1 数据产品目录检索服务 ..... 6

        7.2.2 数据产品详情查询服务 ..... 6

    7.3 数据接口要求 ..... 6

        7.3.1 API 数据接口方式 ..... 7

        7.3.2 批量数据流方式 ..... 7

        7.3.3 数据传输协商 ..... 7

8 安全保障要求 ..... 8

    8.1 标识和鉴别 ..... 8

    8.2 访问控制 ..... 8

    8.3 系统安全 ..... 8

8.4 数据安全 .....	8
8.5 用户信息安全 .....	8
参 考 文 献 .....	10

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：国家信息中心、北京国信新网通讯技术有限公司、浪潮云信息技术股份公司、中国电子技术标准化研究院、中国信息通信研究院、中国联合网络通信集团有限公司、中国移动通信集团有限公司、中国移动通信有限公司研究院、华为技术有限公司、杭州安恒信息技术股份有限公司、深圳数鑫科技有限公司、紫金山实验室、中电数据产业集团有限公司、杭州趣链科技有限公司、数据空间研究院、浙江大学、蚂蚁科技集团股份有限公司、蓝象智联（杭州）科技有限公司、云基华海信息技术股份有限公司、苏州数据资产运营有限公司、深圳市智慧城市科技发展集团有限公司、中国农业大学、江苏未来网络集团、中电云计算技术有限公司、航天信息股份有限公司、上海零数众合信息科技有限公司、中电（浙江）数据产业有限公司、太极计算机股份有限公司、联通数据智能有限公司、中国科学院深圳先进技术研究院、浪潮软件科技有限公司、上海数据集团、杭州市数据集团有限公司、深圳数据交易所、陕西云创网络科技股份有限公司、三未信安科技股份有限公司、北京邮电大学、煤炭科学研究总院有限公司、北京熠智科技有限公司、山西数据交易中心有限公司、丝绸之路信息港股份有限公司、北京数风科技有限公司、深圳市尚数网科技有限公司、领信数科信息技术有限公司、山东未来集团有限公司、中国电信集团有限公司、中国人民大学、浙江科正电子信息产品检验有限公司、中关村科学城城市大脑股份有限公司、杭州金智塔科技有限公司、北京易华录信息技术股份有限公司、中通服咨询设计研究院有限公司、西北大学、电子科技大学、北京交通大学、北京腾云天下科技有限公司、江西省大数据中心、中国信息协会、北京华宇软件股份有限公司、云宏信息科技股份有限公司、杭州铭威信息科技有限公司、哈尔滨工程大学、北京国润信达信息科技有限公司、高颂数科（厦门）智能技术有限公司、南湖实验室、中航信数智科技（北京）有限公司、清华大学社会科学学院经济学研究所、华控清交信息科技（北京）有限公司、下一代互联网关键技术和评测北京市工程研究中心有限公司、清雁科技（北京）有限公司、杭州数美科技有限公司、中科斯欧（合肥）科技股份有限公司、机械工业经济管理研究院、湖北省标准化与质量研究院、天津市天河数字产业科技有限公司、中国汽车工程研究院股份有限公司、视联动力、中国南方电网有限责任公司、山西云时代技术有限公司、软通智慧科技有限公司、地纬智能科技股份有限公司、中国联合健康医疗大数据有限责任公司、四川数通智汇数据科技有限公司、中兴通讯股份有限公司、国家工业信息安全发展研究中心、中关村工信二维码技术研究院、深圳市机密计算科技有限公司、西安交通大学等单位负责起草。

本文件主要起草人：马英、徐春学、张立峰、许晓非、张群、王亦澎、张鹏、王为中、司宏伟、胡馨月、景越、徐文静、喻炜、茹志强、赵丽丽、陈星、廖炳才、刘运强、陈平平、国丽、胡麦芳、王佐成、纪守领、樊建平、赵灵晰、宫大庆、昌文婷、王超、鲁胜强、杨红、王刚、钱锐、王皓磊、张紫萱、孙婧、赵彬彬、赵进延、许紫媛、袁博、贾轩、杨靖世、孙骞、张艺贝、梁超、马万钟、张帆、李征、李崇、王吾冰、胡成盛、李岑、张宝龙、邱炜伟、张晓蒙、曾成、江金菁、罗笑、王俊颀、马韵洁、杨仁慧、李鸿阔、王芳、宋若宁、兰春嘉、杨珍、周福春、苏仁玲、刘长周、孙辉、刘海潮、辛卫民、周强、张凯、李榕、黄徽川、鹿淑煜、何帅、苏上海、戚文婷、王儒、王俊祥、朱纯超、吴桂荣、张震宇、王春庆、张鑫、黄科满、孙璐、李豫、宋键、程宏、夏琦、闫晓杰、张亚东、孙杨、韩金丽、魏丽丽、朱敏健、李帜、王小芳、陈昊洁、林建兴、张磊、孙晓峰、汤珂、靳晨、张旭东、赵富春、念灿华、于万钦、宣秀芳、李鹏、丁凡、乔晗、全代勇、亓娜、杨秋勇、戎劲光、林镇阳、陈曦、王敏虾、张永奇、缪贵海、王福焱、牛小兵、蓝晏翔、惠维。

## 引 言

本文件主要规范接入连接器的总体要求，明确接入连接器的用户对象和角色；明确接入连接器的类型、产品形态；明确接入连接器于业务平台、接入连接间的对接关系；规范接入连接器的能力要求，明确接入连接器在身份认证、网络接入、数据交付、数据访问控制、日志记录、数据资源管理、数据使用控制、数据产品目录服务、隐私计算集成、高速数据网接入以及互操作和安全保障方面的能力要求，旨在为行业提供接入连接器的技术规范，为企业设计生产和应用符合标准的接入连接器产品提供参考，为构建高效、安全、可持续的数据基础设施提供指引。



# 数据基础设施 接入连接器技术要求

## 1 范围

本文件规范了接入连接器的标准能力要求、扩展能力要求、安全保障要求以及互操作要求，用于指导接入连接器的设计和开发、异构接入连接器的对接和测试。

本文件适用于数场、可信数据空间、数联网、数据元件、隐私保护计算、区块链等技术体系支撑的各类层级的数据基础设施建设，包括区域、城市、行业、企业、个人等数据基础设施。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 AAAAA-20XX 数据基础设施 参考架构
- GB/T BBBBB-20XX 数据基础设施 互联互通基本要求
- GB/T CCCCC-20XX 数据基础设施 用户身份管理和接入要求
- GB/T DDDDD-20XX 数据基础设施 数据目录描述规范
- TC609-6-2025-01 可信数据空间 技术架构
- TC609-6-2025-11 数据基础设施 区域/行业功能节点技术要求
- TC609-6-2025-12 数据基础设施 接入管理
- TC609-6-2025-13 数据基础设施 安全能力通用要求
- TC609-6-2025-14 可信数据空间 数字合约技术要求
- TC609-6-2025-15 可信数据空间 使用控制技术要求

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**接入连接器** access connector

连接接入主体与接入主体、接入主体与业务节点、接入主体与重要功能设施的规范化软硬件系统，数据供需双方均可通过接入连接器接入数据基础设施。

[来源：20255407-T-907，3.4.19]

### 3.2

**访问策略** access policy

指可在接入连接器内自动化解析执行的机器可读的指令语言，用于控制接入连接器在许可范围内访问、使用数据。

### 3.3

**数据使用控制策略** data usage control policy

用于管理和约束数据使用方在处理、流通、销毁等各阶段内使用数据的一系列方法和技术。

### 3.4

#### 智能服务 smart service

指以大模型、智能体、具身智能、决策引擎等智能技术单元为核心能力载体，通过API、MCP、SDK等交互方式，对外提供智能感知、理解、生成、决策、执行、协同与调度等全链路智能化能力服务的统称。

## 4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表(Access Control List)

API：应用程序编程接口(Application Programming Interface)

HTTPS：有安全套接层的超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)

JSON：JavaScript对象表示法(JavaScript Object Notation)

REST：表述性状态传递(Representational State Transfer)

XML：可扩展标记语言(Extensible Markup Language)

TLS：传输层安全协议(Transport Layer Security)

SSL：安全套接层(Secure Sockets Layer)

MCP：模型上下文协议(Model Context Protocol)

## 5 总体要求

接入连接器在数据基础设施中的连接逻辑如图1所示，总体要求包括：

- a) 接入连接器应支持对接重要功能设施，实现接入连接器的身份注册、身份认证、监测信息和运行状态信息上报。
- b) 接入连接器应支持对接业务节点，实现运行状态信息上报和控制指令信息获取。
- c) 接入连接器应支持对接数据提供方、数据使用方本地应用、数据库、大模型、智能体，实现数据和智能服务的接入与获取，接入连接器在业务节点的协调下，可实现点对点相互连通，并按照控制指令信息完成数据传输、智能服务的协同交互。



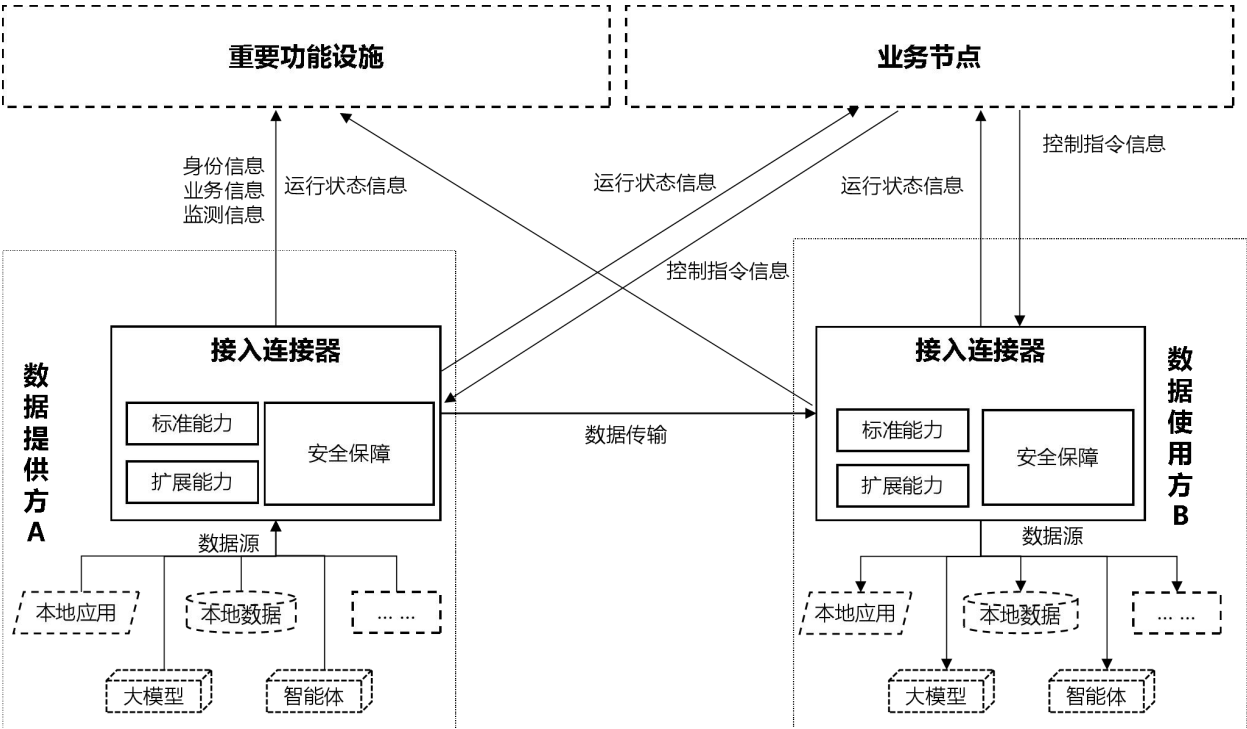


图1 接入连接器的连接逻辑示意图

6 能力要求

6.1 总体架构

接入连接器可以多种形态体现，如Ukey、软件系统、软硬件结合的终端等，不同形态的接入连接器具备的功能维度也不同；

身份认证是接入连接器的基础能力，可以Ukey形态作为最小化的接入连接器，支撑用户接入数据基础设施；

身份认证、网络接入、数据交付、数据访问控制、日志记录、运行状态上报组成了接入连接器的标准能力集，支撑用户流通和利用数据的接入连接器类产品应具备全部标准能力；

接入连接器扩展能力包括数据产品目录服务、数据使用控制、数据资源管理、数字合约管理、隐私保护计算能力集成、高速数据网接入、数据产品管理、智服务接入以及其他关键技术组件扩展能力等。

接入连接器能力总体架构见图2。

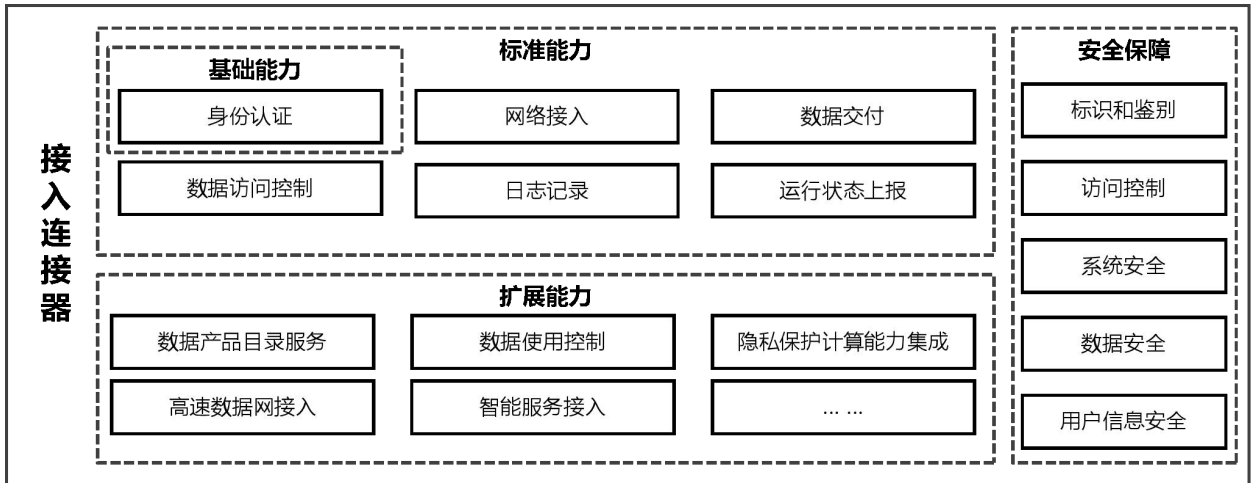


图 2 接入连接器能力总体架构图

## 6.2 标准能力

### 6.2.1 身份认证

接入连接器的身份认证能力包括：

- a) 接入连接器应支持可信身份凭证的管理，可信身份凭证技术要求应符合 GB/T CCCCC-20XX 《数据基础设施 用户身份管理和接入要求》第 XXX 条的规定；
- b) 接入连接器应支持基于可信身份凭证的用户身份认证。

### 6.2.2 网络接入

接入连接器应支持不同类型的网络接入，包括但不限于互联网、专线等，以连接业务节点、其它接入连接器、连接重要功能设施，实现不同网络接入主体的数据参与方快速连通（网络物理隔离情况除外）。

### 6.2.3 数据交付

接入连接器数据交付能力要求包括：

- a) 接入连接器应支持 API 数据接口、批量数据流等方式进行数据交付；
- b) 接入连接器可提供 API 数据接口、批量数据流鉴权信息等配置能力；
- c) 接入连接器应支持按照数字合约要求交付原始数据，可支持交付脱敏后数据或计算结果数据等。

### 6.2.4 数据访问控制

在数据交付过程中，数据提供方接入连接器应通过获取、解析数据交易控制指令识别待交付数据产品、数据访问控制策略等信息，并根据策略对数据使用方的访问进行权限检查，确保按权限访问数据。控制指令信息的要求应满足 GB/T BBBB-20XX 《数据基础设施 互联互通基本要求》第 xxx 条的要求。

### 6.2.5 日志记录

接入连接器日志记录能力要求包括：

- a) 接入连接器应支持记录系统日志、操作日志、业务日志等信息，支撑审计、运维工作；
- b) 接入连接器应支持按照用户定义的规则记录数据调用次数、使用时长、使用量等信息；
- c) 日志的留存时间应满足国家相关法律法规要求。

### 6.2.6 运行状态上报

接入连接器应支持根据业务需要定时将运行状态上报至重要功能设施和业务节点,以支撑重要功能设施或业务节点掌握接入连接器的状态。

## 6.3 扩展能力

### 6.3.1 数据资源管理

接入连接器应支持数据提供方接入自身数据系统中的数据资源,作为封装数据产品的基础,能力要求包括:

- a) 接入连接器应支持本地多样数据资源接入能力,包括但不限于对象存储、数据库、本地文件服务器等;
- b) 接入连接器应支持对已接入的数据资源进行删除、修改。

### 6.3.2 数据产品管理

接入连接器应支持数据提供方管理、上架数据产品。接入连接器应支持数据提供方基于接入数据资源封装数据产品,并对本地数据产品进行管理,能力要求包括:

- a) 接入连接器应支持基于已接入的数据资源,配置数据产品定价、交付方式、数据访问与使用策略等信息,将其封装为可流通的数据产品;
- b) 接入连接器应支持数据提供方将已封装且登记后的数据产品通过业务节点上架。

### 6.3.3 数字合约管理

接入连接器可提供数字合约管理功能,支持数据提供方、数据使用方直接通过接入连接器签订数字合约,并管理已签订的数字合约,能力要求包括:

- a) 接入连接器应支持在数据使用方发起数据产品使用申请时,由数据使用方接入连接器基于数据产品要求及策略模板创建数字合约,用户也可通过业务节点创建数字合约后下发到接入连接器;
- b) 接入连接器应支持数据提供方、数据使用方、数据服务方之间就数据的使用策略形成的数字合约进行协商;数字合约协商可进行多轮,协商完成后签订数字合约;
- c) 接入连接器应支持数据提供方和数据使用方,在数字合同签订完成时,依据合约内容触发数据交付和数据使用的履约操作。

### 6.3.4 数据产品目录服务

接入连接器数据产品目录服务能力要求包括:

- a) 接入连接器可支持数据提供方创建、管理数据产品目录;
- b) 接入连接器可在无需平台参与的情况下提供接入连接器之间的数据产品目录服务,以供其他接入连接器查询。

### 6.3.5 数据使用控制

接入连接器可支持加载解析数据使用控制策略并按策略执行,以支持数据提供方通过使用次数限制、使用周期限制等策略,约束数据使用方使用数据,能力要求包括:

- a) 接入连接器应提供使用数据的软硬件环境,支持数据使用方按照数字合约中的使用控制策略要求,通过算法或应用使用数据提供方交付的数据产品;

- b) 接入连接器可集成隐私保护计算、数据沙箱、数据匿名化、智能合约等技术，增强数据使用的安全性；
- c) 接入连接器应支持与数据使用环境联动，对数据使用方的数据使用行为进行实时监测与控制，保证数据的使用符合数字合约要求；
- d) 接入连接器应将数据使用过程日志进行细粒度的存证，并按照要求上报给业务节点或重要功能设施的存证审计系统，同时提供日志的查询及溯源服务。

#### 6.3.6 隐私保护计算能力集成

接入连接器可通过对接隐私保护计算节点，将控制指令信息同步给该节点，并将隐私保护计算过程中需要交互的信息在各接入连接器间、接入连接器与业务节点间传输；或集成多方安全计算、联邦学习等相关模块以实现隐私保护计算能力。

#### 6.3.7 高速数据网接入

接入连接器可通过维护下一跳网络地址、高速数据网接入服务地址等配置，快速接入高速数据网。

#### 6.3.8 智能服务接入

接入连接器可接入大模型、智能体，可通过API或流访问大模型和智能体的服务，可通过MCP协议接入工具集，可通过A2A协议实现智能体协作。

#### 6.3.9 其他关键技术组件扩展

接入连接器可通过接口配置、能力集成等方式，根据用户需求动态扩展各类关键技术组件。

### 7 互操作要求

#### 7.1 接入连接器身份认证要求

接入连接器应支持基于可信身份凭证实现接入连接器之间的双向认证，技术要求应满足GB/T CCCCC-20XX《数据基础设施 用户身份管理与接入规范》第6.2.2.2 接入连接器之间双向认证的要求。

#### 7.2 数据产品目录查询要求

##### 7.2.1 数据产品目录检索服务

接入连接器之间进行数据产品目录检索时遵循统一的参数要求：

- a) 请求参数应包含检索关键字、排序规则、开始偏移量、限制条数、目标接入连接器编码、发起接入连接器编码、发起时间、扩展信息等；
- b) 响应参数应包含状态码、消息描述、消息体、所有页记录总数、本页结果、数据产品唯一标识、数据产品名称、产品描述、接入连接器编码等信息。

##### 7.2.2 数据产品详情查询服务

接入连接器之间进行数据产品详情查询时遵循统一的参数要求：

- a) 请求参数应包含数据产品唯一标识、数据产品名称；
- b) 响应参数应包含状态码、消息描述、消息体、接入连接器编码、数据产品对象信息等信息。

#### 7.3 数据接口要求

### 7.3.1 API 数据接口方式

接入连接器间API数据接口应符合统一的传输协议、请求参数和返回参数要求。

#### 7.3.1.1 传输协议

接入连接器间应支持 HTTPS 作为 API 接口传输协议，应支持 RESTful 类型的接口。

#### 7.3.1.2 请求头参数

请求头中应包括请求唯一标识、目标接入连接器、发起接入连接器、数据产品唯一标识、控制指令编号等参数；可包括请求内容摘要、鉴权信息、X-Forwarded-For等参数；包括：

- a) 请求唯一标识：使用方 32 位随机字符串。用于核对调用请求，进行故障排查。
- b) 接入连接器唯一标识：发起请求的接入连接器唯一标识，用于明确请求来源。
- c) 接入连接器鉴权信息：根据数据使用方与数据提供方协商的身份验证手段生成，可选数字证书签名、APP 调用凭证等，用于向请求目标证明接入连接器的请求合法性。
- d) 请求内容摘要：由发起请求的接入连接器生成，使用哈希加密算法对请求 Body 参数进行摘要计算，用于验证请求内容的完整性。
- e) 数据产品唯一标识：从控制指令信息中获取。数据使用方接入连接器调用时传递，用于提供方接入连接器确定被调用产品。
- f) 控制指令编号：从控制指令信息中获取。数据使用方接入连接器调用时传递，用于提供方接入连接器执行访问控制。
- g) X-Forwarded-For：在 RFC 7239 中定义的 HTTP 扩展头字段，表示 HTTP 请求端真实 IP。

#### 7.3.1.3 Body 参数

API接口请求Body参数由数据产品提供方自主定义，传递参数为中文字符时，应使用UTF-8方式进行编解码。

#### 7.3.1.4 返回参数

API数据查询返回参数时遵循统一的要求：

- a) API 接口调用结果应通过返回码反馈；
- b) API 接口调用返回参数应包含状态码、消息描述、原始 API 响应头和原始 API 响应报文等信息。

### 7.3.2 批量数据流方式

接入连接器间批量传输数据时遵循统一的参数要求：

- a) 请求参数应包含目标接入连接器编码、发起接入连接器编码、发起时间、数据产品标识、数据产品名称等信息；
- b) 响应参数应包含状态码、消息描述、消息体、接入连接器编码等信息。

### 7.3.3 数据传输协商

数据传输协商的过程和接口要求包括：

- a) 使用方和提供方未从控制指令信息中获取足够的数据传输协议或参数的情况下，可先协商再传输，协商分为两步：
  - 1) 使用方接入连接器通过数据传输协商接口向提供方接入连接器协商数据传输协议、授权码、地址等详细传输参数；
  - 2) 协商完成后，双方使用达成一致的数据传输标准协议进行数据传输。

- b) 数据传输协商接口的传输协议、请求头参数、Body 参数以及返回参数应按照第 7.3.1 的要求。

## 8 安全保障要求

接入连接器应符合《TC609-6-2025-13 数据基础设施 安全能力通用要求》中对接入连接器的通用安全要求，在此基础上扩展以下安全保障能力。

### 8.1 标识和鉴别

接入连接器满足以下标识与鉴别能力要求：

- a) 接入连接器应基于数字证书实现双向身份验证、唯一标识比对等方式核验所对接的接入连接器身份，确保对接的接入连接器身份可信；
- b) 接入连接器可支持对用户的多因素认证（如动态口令、短信验证码等）和密钥核验等方式，验证用户身份的真实性，确保只有授权用户能够访问系统；
- c) 应保障用户和接入连接器自身的标识和鉴别信息在传输和存储过程中的保密性和完整性；
- d) 使用口令鉴别方式时，应提供口令的强度验证和定期更换功能，并支持首次接入连接器时强制修改默认口令。

### 8.2 访问控制

接入连接器满足以下访问控制能力要求：

- a) 对接入连接器的用户分配账户和权限，区分管理员角色，实现管理权限相互制约；
- b) 对接入连接器自身应支持通过配置 ACL 策略、白名单管控等方式，控制网络访问权限；
- c) 应配备必要的网络安全能力，防止被攻击或入侵。

### 8.3 系统安全

接入连接器满足以下系统安全要求：

- a) 支撑接入连接器的软件代码应经过严格的安全审计，不应包含已公开的中、高风险漏洞；
- b) 应定期检查和更新依赖的第三方库、框架等组件，防止因组件漏洞导致的安全风险；
- c) 接入连接器的运行环境应具备安全防护机制，防止恶意软件入侵或未经授权的访问。在启动与升级部署过程中，应具备版本完整性校验功能，防止软件被篡改；
- d) 接入连接器应对安全事件数据进行完整记录，并上传至区域功能节点；
- e) 接入连接器应具备应用程序和系统的可信保障体系，通过完整性度量、可信启动与持续验证等手段，确保连接器运行环境未被篡改。

### 8.4 数据安全

接入连接器满足以下数据安全要求：

- a) 采用加密协议（如 TLS/SSL）保障网络通信的安全与可信，防止数据在传输过程中被窃取或篡改；
- b) 接入连接器可通过报文签名、数据加密等方式，保障对接、传输过程中的数据安全，防止传输的数据被篡改、泄漏；
- c) 接入连接器应支持在识别到数据存在风险时终止交付。

### 8.5 用户信息安全

接入连接器满足以下用户信息安全要求：

- a) 接入连接器仅收集实现功能所必需的用户信息；
- b) 在涉及个人信息传输和存储的过程中保障个人信息的保密性和完整性；
- c) 在涉及个人信息存储时提供对超出保存期限个人信息的处理功能。

## 参 考 文 献

- [1] RFC 7239 (6/2014) 转发超文本传输协议扩展(Forwarded HTTP Extension)
-