# TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-XX

# 数据基础设施 区域/行业功能节点技术要求

**Data infrastructure—Technical requirements for Regional/Sectoral Functional Nodes**

（征求意见稿）

2025-XX-XX 发布　　2025-XX-XX 实施

全国数据标准化技术委员会　发布

# 目　　次


前　　言 ..... III
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 区域功能节点与行业功能节点的关系 ..... 2
6 功能架构 ..... 3
6.1 区域功能节点功能架构 ..... 3
6.2 行业功能节点功能架构 ..... 4
7 功能要求 ..... 5
7.1 区域/行业功能节点门户 ..... 5
7.2 区域/行业功能节点管理平台 ..... 5
7.2.1 主体身份管理 ..... 5
7.2.2 接入连接器管理 ..... 5
7.2.3 业务节点管理 ..... 6
7.2.4 数据资源与数据产品管理 ..... 6
7.2.5 标识管理 ..... 7
7.2.6 智能服务 ..... 7
7.2.7 存证服务 ..... 7
7.3 区域/行业功能节点运营平台 ..... 8
7.3.1 监测运维管理 ..... 8
7.3.2 计费清算 ..... 8
7.3.3 运营分析 ..... 8
7.3.4 行业功能节点-行业主数据服务 ..... 8
7.3.5 行业功能节点-语义模型服务 ..... 9
7.3.6 行业功能节点-行业知识中枢 ..... 9
8 互操作要求 ..... 9
9 安全要求 ..... 9
9.1 基本要求 ..... 9
9.2 平台系统 ..... 9
9.2.1 平台系统基本要求 ..... 9
9.2.2 访问控制 ..... 9
9.2.3 数据库系统 ..... 10
9.2.4 身份认证 ..... 10
9.3 运行环境 ..... 10
9.3.1 运行环境基本要求 ..... 10

9.3.2 网络与边界.....10
9.3.3 操作系统.....10
9.3.4 设施设备.....10
9.4 数据安全.....11
9.5 应急处置.....11
参 考 文 献.....12

# 前　言

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：

# 数据基础设施 区域/行业功能节点技术要求

## 1 范围

本文件规范了区域/行业功能节点的相互关系、功能架构以及在产品和资源管理、标识管理、身份管理、运营管理、监测分析等方面的技术要求，适用于指导具备条件的省份、行业主管部门、龙头企业按照标准化架构建设区域/行业功能节点。

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 2887-2011 计算机场地通用规范
GB/T 20270-2006 信息安全技术 网络基础安全技术要求
GB/T 20272-2019 信息安全技术 操作系统安全技术要求
GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 31168-2023 信息安全技术 云计算服务安全能力要求
GB/T 32905-2016 信息安全技术 SM3密码杂凑算法
GB/T 32907-2016 信息安全技术 SM4分组密码算法
GB/T 39276-2020 信息安全技术 网络产品和服务安全通用要求
GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
NDI—TR—2025—02 数据基础设施 互联互通基本要求
NDI—TR—2025—03 数据基础设施 用户身份管理和接入要求
NDI—TR—2025—04 数据基础设施 标识管理规范
NDI—TR—2025—06 数据基础设施 数据目录描述规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**全域功能节点 global function node**

数据基础设施中面向全域提供统一标识管理、统一身份管理、统一目录管理和运行监测等服务的节点。

3.2

**区域功能节点 regional function node**

数据基础设施中面向特定区域提供身份注册和核验、数据登记、数据目录查询、数据标识解析、运行监测等服务的节点。

3.3

**行业功能节点 industrial sector function node**

数据基础设施中面向特定行业提供身份注册和核验、数据登记、数据目录查询、数据标识解析、运行监测等服务的节点。

3.4

**业务节点 service node**

数据基础设施中各区域、行业及企业的数据流通利用平台。

3.5

**接入主体 access entity**

数据基础设施中参与数据流通利用的节点运营方、数据提供方、数据使用方、数据经纪、数据评估方以及第三方存储、算力服务商等。

3.6

**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、接入主体与区域/行业功能节点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。

3.7

**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。

3.8

**三统一 Three Unifications**

在数据基础设施领域中，“三统一”常指的是统一标识管理、统一身份管理和统一数据目录管理。

## 4 缩略语

下列缩略语适用于本文件。

WEB：全球广域网（World Wide Web）

MFA：多因素身份验证（Multi-Factor Authentication）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

## 5 区域功能节点与行业功能节点的关系

区域功能节点与行业功能节点的关系见图1。

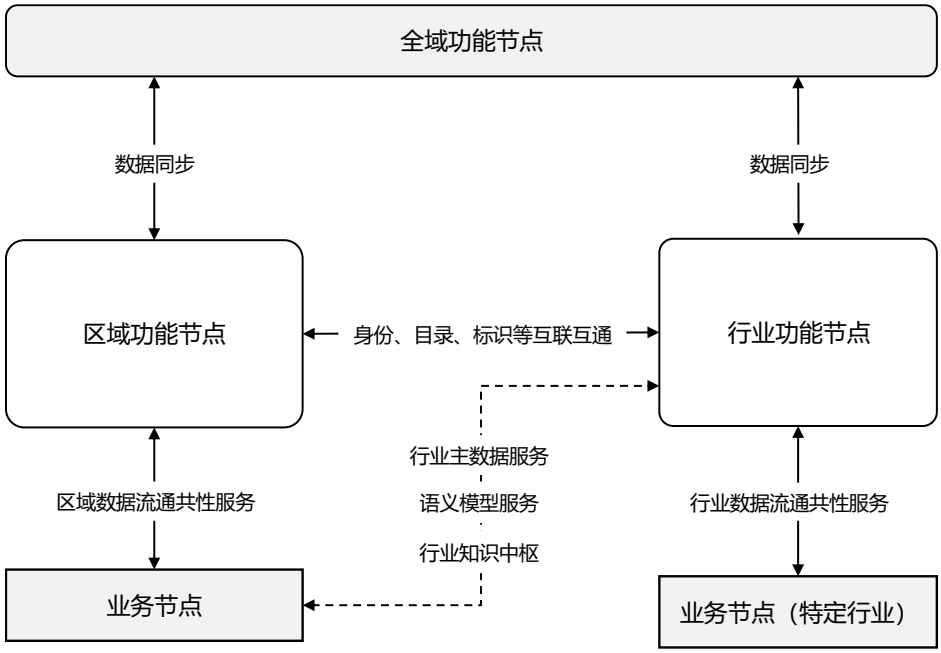


图1　区域功能节点与行业功能节点关系图

a) 区域功能节点面向特定区域提供“三统一”共性管理服务、运营服务等区域数据流通共性服务；
b) 行业功能节点面向特定行业提供“三统一”共性管理服务、运营服务等行业数据流通共性服务，其中，行业功能节点的运营服务比区域功能节点增加行业主数据服务、语义模型服务、行业知识中枢服务等行业数据服务能力；
c) 区域功能节点应与行业功能节点互联，两节点应与全域功能节点互通；
d) 通过区域功能节点开展数据流通服务的业务节点，可根据需要调用多个行业功能节点的行业主数据服务、语义模型服务、行业知识服务等行业数据服务能力，来满足特定行业数据流通服务需要；通过行业功能节点开展数据流通服务的业务节点，不需对接区域功能节点，可根据需要调用其他行业功能节点的行业数据服务能力，来满足特定行业数据流通服务需要。

## 6　功能架构

### 6.1　区域功能节点功能架构

区域功能节点由区域功能节点门户、区域功能节点管理平台、区域功能节点运营平台构成，功能架构如图3所示。

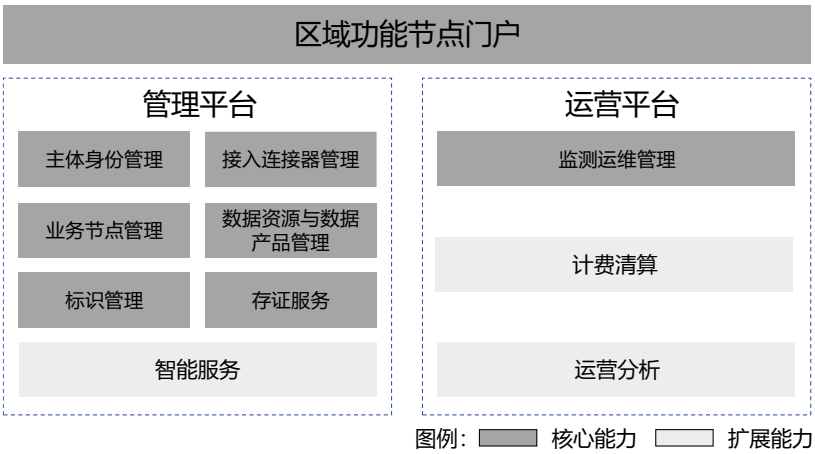


图2　区域功能节点功能架构图

区域功能节点门户应面向区域的数据流通利用主体、业务节点运营主体、接入连接器供应厂商等提供统一门户服务能力。

区域功能节点管理平台提供身份管理、接入连接器管理、业务节点管理、数据资源与数据产品管理、标识管理、智能服务、存证服务能力，面向区域提供数据基础设施“三统一”服务，支撑跨层级、跨地域、跨系统、跨部门、跨业务的数据有序流通和共享应用。

区域功能节点运营平台提供监测运维管理、计费清算、运营分析能力，支撑区域功能节点稳定高效运行。

区域功能节点应具备身份管理、接入连接器管理、业务节点管理、数据资源与数据产品管理、标识管理、存证服务、监测运维管理等核心能力。区域功能节点可根据自身实际情况，参考建设和提供其他扩展能力。

## 6.2　行业功能节点功能架构

行业功能节点由行业功能节点门户、行业功能节点管理平台、行业功能节点运营平台构成，功能架构如图4所示。

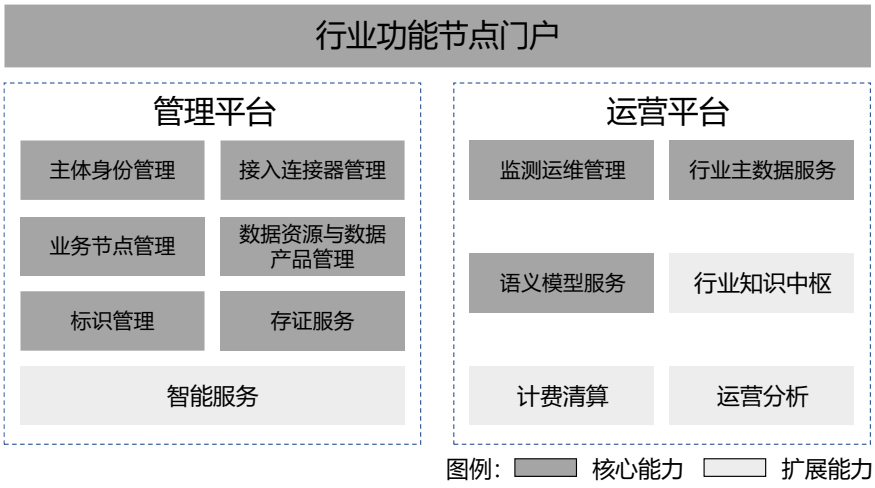


图3　行业功能节点功能架构图

行业功能节点门户应面向特定行业的数据流通利用主体、业务节点运营主体、接入连接器供应厂商等提供统一门户服务能力。

行业功能节点管理平台功能与区域功能节点相同，面向特定行业提供数据基础设施“三统一”服务和运营支撑。

行业功能节点运营平台比区域功能节点增加行业主数据服务、语义模型服务、行业知识中枢能力，支撑行业功能节点稳定高效运行。

行业功能节点应具备身份管理、接入连接器管理、业务节点管理、数据资源与数据产品管理、标识管理、存证服务、监测运维管理、行业主数据服务、语义模型服务等核心能力。行业功能节点可根据自身实际情况，建设和提供其他扩展能力。

## 7 功能要求

### 7.1 区域/行业功能节点门户

区域/行业功能节点门户的功能包括但不限于：

a) 应支持为数据流通利用主体、业务节点、接入连接器提供注册、更新、注销服务能力；
b) 应提供业务节点目录展示与检索服务，支持业务节点链接跳转；
c) 应提供数据资源登记、检索服务能力；
d) 应提供数据产品登记、检索服务能力；
e) 可提供应用市场服务，支持应用上架、更新、下载等功能，可上架的类型包括组件、工具、服务、应用等，应支持用户在此市场内自主购买或获取所需应用，若支持交易功能，需符合国家金融安全规范；
f) 可提供接入主体目录、检索服务能力；
g) 可提供智能检索、智能推荐、数据互认等服务；
h) 行业功能节点在以上功能基础上应提供行业主数据服务、语义模型服务，可支持行业知识服务。

### 7.2 区域/行业功能节点管理平台

#### 7.2.1 主体身份管理

主体身份管理的功能包括但不限于：

a) 应支持接入主体进行身份注册、更新、注销管理，应符合 NDI-TR-2025-03 数据基础设施 用户身份管理和接入规范的要求；
b) 应提供用户登录认证服务，可通过账号口令、数字证书、密钥登录等方式实现，并结合多因素认证安全策略，验证用户身份合法性与有效性；
c) 应支持将身份信息报送至全域功能节点，并接收全域功能节点同步的失效身份信息；
d) 应支持全域功能节点、其他区域/行业功能节点查询与核验主体身份信息；
e) 应支持按照 NDI-TR-2025-02 数据基础设施 互联互通基本要求进行跨域身份互认，基于其他区域/行业功能节点身份信息查询与核验服务进行跨域身份核验，基于全域功能节点提供的可信根证书查询服务，实现对其他区域/行业功能节点签发的可信身份凭证的核验与认可；
f) 应定期检查身份有效性，并同步信息至全域功能节点和相应的业务节点；
g) 应支持通过页面或者接口等形式，面向业务节点、接入连接器等提供身份注册、登录等服务；
h) 应支持接入第三方可信身份提供商，为区域接入主体签发可信身份凭证。

#### 7.2.2 接入连接器管理

接入连接器管理的功能包括但不限于：

a) 应支持接入连接器提交接入申请，提交信息包括主体身份信息、接入连接器名称、供应商名称、产品版本号等，支持运营人员对接入申请进行审核；
b) 应支持接入连接器网络接入管理，可支持固定 IP、动态 IP 等多种方式组网；
c) 应支持为审核通过的接入连接器分配唯一标识、获取身份凭证，作为接入连接器接入的合法性验证凭证。分配的唯一标识应符合 NDI-TR-2025-04 数据基础设施 标识管理规范要求，获取的身份凭证应符合 NDI-TR-2025-03 数据基础设施 用户身份管理和接入规范要求；
d) 应支持接入连接器更新/注销，接入连接器需重新提交身份信息至区域/行业功能节点审核，注销后该接入连接器停止同步数据资源和数据产品目录；
e) 应支持本区域/行业内的接入连接器通过接口获取本区域/行业或其他区域/行业内的接入连接器信息；
f) 应提供接入连接器的身份凭证验证能力；
g) 应支持获取接入连接器的运行状态信息，包括应用系统、服务运行状态信息及操作信息，对失效的接入连接器进行提示、停用或删除管理；
h) 应支持向全域功能节点上报接入连接器身份，支持其他区域/行业功能节点、业务节点、接入连接器等组件查询接入连接器信息；
i) 可支持接入连接器目录管理功能，可提供接入连接器版本管理与下载能力；
j) 应支持通过接口或页面形式，面向业务节点提供接入连接器接入服务。

### 7.2.3 业务节点管理

业务节点管理的功能包括但不限于：
a) 应支持按照 NDI-TR-2025-02 数据基础设施 互联互通基本要求和 NDI-TR-2025-03 数据基础设施 用户身份管理和接入规范确定的业务节点接入、发现、服务流程和要求，为本区域/行业业务节点提供平台名称、所属法人或其他组织名称、平台 IP 地址列表等信息的登记、上传、审核管理功能。审核通过后，应按照 NDI-TR-2025-04 数据基础设施 标识管理规范的业务节点编码要求为区域/行业业务节点发放唯一标识和认证证书；
b) 应支持对登记审核通过后的业务节点自动生成业务节点目录，经审核后进行发布，并支持业务节点目录管理，包括目录的查询、查看、导出等功能；
c) 应支持按照 NDI-TR-2025-02 数据基础设施 互联互通基本要求，将本区域/行业审核发布后的业务节点目录信息实时上报至全域功能节点，并将全域功能节点中其他区域/行业的业务节点的目录信息同步至本区域/行业业务节点目录中，实现全域业务节点目录信息的互联互通；
d) 应支持向其他区域/行业功能节点提供在本区域/行业完成认证的业务节点的身份凭证验证能力；
e) 应支持获取本区域/行业内各业务节点的运行状态信息（包括应用系统、服务运行状态信息及操作信息），对失效的业务节点进行提示、停用管理；
f) 可支持以可视化界面方式查询、浏览全域的业务节点目录信息；
g) 可支持向其他区域/行业功能节点提供业务节点目录查询服务；
h) 行业功能节点在以上功能基础上应支持已在其他区域/行业功能节点完成认证的业务节点通过跨域验证后完成接入。

### 7.2.4 数据资源与数据产品管理

数据资源与数据产品管理的功能包括但不限于：
a) 应支持接入连接器、业务节点向区域/行业功能节点通过标准接口/页面嵌入的方式或各类用户通过区域功能节点系统界面方式登记数据资源和数据产品信息，登记的数据资源和数据产

品的基本信息应该包含NDI-TR--2025-06 数据基础设施 数据目录描述规范中附录表A.1数据资源目录字典、表A.2数据产品目录字典（产品登记信息）中内容，并支持对登记信息进行合规性检测；

b) 应支持接入连接器、业务节点向区域/行业功能节点通过标准接口/页面嵌入的方式或各类用户通过区域功能节点系统界面方式获取数据资源和数据产品登记的审核结果，如果审核通过则获取对应的流程ID和标识信息；

c) 应支持接入连接器、业务节点向区域行业功能节点通过标准接口/页面嵌入的方式或各类用户通过区域功能节点系统界面方式更新已登记的资源或产品信息，区域/行业功能节点需要对更新的信息进行审核，并提供审核结果查询；

d) 应支持接入连接器、业务节点向区域/行业功能节点通过标准接口/页面嵌入的方式或各类用户通过区域功能节点系统界面方式申请撤销已登记数据资源和下架数据产品信息，并提供审核结果查询；

e) 应支持业务节点通过区域/行业功能节点提供的标准接口方式或各类用户通过区域功能节点系统界面方式检索、查看当前已在区域功能节点已登记的数据资源、数据产品信息；

f) 应支持区域/行业功能节点调用全域功能节点提供的数据目录标准上报接口,将数据产品目录、数据资源目录上报给全域功能节点；

g) 应支持区域/行业功能节点调用全域功能节点提供的数据资源和数据产品标准同步接口，获取全域功能节点当前的数据资源和数据产品目录信息；

h) 可支持向其他区域/行业功能节点提供数据目录查询服务。

### 7.2.5 标识管理

标识管理的功能包括但不限于：

a) 应支持本区域/行业参与数据流通利用的企业/个人、接入连接器、业务节点、数据资源、数据产品进行标识赋码管理，应符合NDI-TR-2025-04 数据基础设施 标识管理规范的要求；

b) 应支持向业务节点、接入连接器提供标识解析服务，支持基于数据资源、数据产品、接入连接器、业务节点、区域/行业功能节点、全域功能节点标识进行对应对象检索、定位；

c) 应支持将注册的标识信息同步至全域功能节点；

d) 可支持标识规则配置管理，可设置标识码生成规则，对存量的标识配置规则，完成原有标识与新标识的转换；

e) 可支持通过页面或接口的形式面向业务节点、接入连接器等提供标识赋码服务；

### 7.2.6 智能服务

智能服务的功能包括但不限于：

a) 可提供智能检索和智能推荐服务。可支持智能化的数据产品推荐；可支持用户搜索语义模糊匹配所需数据资源或数据产品；可根据数据提供方和数据使用方的标签分析，自动推荐潜在合作方；

b) 行业功能节点可在此基础上基于行业知识中枢能力提供行业知识智能服务。

### 7.2.7 存证服务

存证服务的功能包括但不限于：

a) 应提供存证服务，支持业务节点、接入连接器将数据使用控制策略、数据交易控制指令、数据交付过程等信息进行可信存证；

b) 应使用密码技术、可信计算技术或对接区块链平台等方式保证存证信息的完整性和不可否认性、可追溯性和不可篡改性；
c) 应提供存证信息查询服务，支持业务节点、接入连接器通过控制指令编号、数据交付过程标识等查询存证信息；
d) 应提供交付过程存证溯源服务，可基于存证信息还原完整的合约生效和数据交付过程全程记录，保证交付过程可信，为争议解决提供数据支撑。

## 7.3 区域/行业功能节点运营平台

### 7.3.1 监测运维管理

监测运维管理的功能包括但不限于：
a) 应支持对本区域/行业功能节点、业务节点、接入连接器运行状态进行监测与告警；
b) 可支持汇集本区域/行业功能节点、业务节点、接入连接器的业务运行信息，包括用户日活跃度、数据目录更新、数据流通频次等信息，并提供业务统计分析、异常预警等功能；
c) 可支持汇集信息的统计查询与表单管理功能，可支持汇集信息多维度可视化管理与展示；
d) 应支持一键断网或限流功能，以及时阻断指定业务节点或接入连接器的全部流量；
e) 应支持操作记录自动存证。

### 7.3.2 计费清算

计费清算的功能包括但不限于：

a) 可支持按照统一的信息格式，归集本区域/行业及跨区域/行业订单交易相关的业务数据，包括订单编号、涉及交易方标识与名称、交易标的、计量、计费等信息；
b) 可支持根据汇集的订单交易信息和交付过程计量信息，生成对账单；
c) 可支持对未平账的交易进行差异分析与处理，可通过自动补单或者人工干预等方式进行处理，并可支持差异情况统计。

### 7.3.3 运营分析

运营分析的功能包括但不限于：
a) 可支持对本区域/行业数据流通参与主体情况进行分析，包括主体类型、数量、行业领域等；
b) 可支持对本区域/行业的接入连接器的接入情况进行分析，包括接入连接器类型、连接器数量、在线状态等；
c) 可支持对本区域/行业登记的数据资源与数据产品情况进行分析，包括来源分布、类型、流通情况等；
d) 可支持对本区域/行业功能节点服务（“三统一”服务、智能服务、存证服务等）运营情况进行分析，包括服务次数、服务成效、服务对象分布等。

### 7.3.4 行业功能节点-行业主数据服务

行业主数据服务的功能包括但不限于：
a) 应支持行业主数据按要求接入、注册，支持根据行业特定的分类和编码体系进行数据管理；
b) 应支持建立行业特定的数据治理规则库，支持根据数据治理规则对行业主数据进行清洗、治理，根据业务规则建立关联关系；
c) 应支持行业主数据质量管理与监测评价；
d) 应支持行业主数据版本管理与变更追溯；

e） 应支持面向不同场景、不同客户通过行业功能节点页面提供行业主数据服务；
f） 应支持通过页面或接口的形式面向业务节点、接入连接器等提供行业主数据服务。

#### 7.3.5 行业功能节点-语义模型服务

语义模型服务的功能包括但不限于：
a） 应支持行业数据标准管理，包括行业数据元标准、代码标准等标准创建、版本管理、公示、发布、治理、废止等管理；
b） 应支持接入连接器、业务节点向行业功能节点通过标准接口/页面嵌入的方式或各类用户通过行业功能节点系统界面方式进行行业数据标准检索、查阅。
c） 应支持基于行业数据标准，建立对象、属性、关系、规则等关系，构建行业语义模型，并支持语义模型创建、版本管理、公示、发布、治理、废止等管理；
d） 应支持将行业语义模型转化为服务能力，应支持接入连接器、业务节点向行业功能节点通过标准接口/页面嵌入的方式或各类用户通过行业功能节点系统界面方式进行行业语义模型检索、查阅、导出、标准引用、工具下载等服务应用；
e） 可支持通过标准化接口（如 RESTful API）提供服务；
f） 可支持跨系统语义互操作服务。

#### 7.3.6 行业功能节点-行业知识中枢

行业知识中枢的功能包括但不限于：
a） 可支持行业标准、政策法规、行业知识等结构化数据和非结构化数据的分类存储；
b） 可支持各类行业知识创建、版本管理、公示、发布、治理、废止等管理；
c） 可支持行业知识图谱创建、版本管理、公示、发布、治理、废止等管理；
d） 可支持接入连接器、业务节点向行业功能节点通过标准接口/页面嵌入的方式或各类用户通过行业功能节点系统界面方式进行行业知识检索、查阅、行业知识图谱查阅等服务应用。

## 8 互操作要求

应满足NDI—TR—2025—02 数据基础设施 互联互通基本要求。

## 9 安全要求

### 9.1 基本要求

应至少满足GB/T 22239—2019中规定的第三级安全要求。

### 9.2 平台系统

#### 9.2.1 平台系统基本要求

平台系统基本安全要求包括但不限于：
a） 应支持对软件代码安全审计，确保不包含已公开的中高风险漏洞；
b） 应支持定期检查和更新第三方库、框架等依赖组件，防范组件漏洞风险；
c） 应在启动与升级过程中实施版本完整性校验，防止软件被篡改。

#### 9.2.2 访问控制

访问控制要求包括但不限于：

a) 应支持对用户访问资源权限进行标识和管理；
b) 应支持对用户、平台、数据等的访问控制权限分级；
c) 访问权限需遵循最小必要原则，仅授予完成业务所需的最小权限；
d) 应建立权限动态调整机制，对高风险操作（如批量数据下载）自动触发权限临时收缩，操作完成后恢复。

#### 9.2.3 数据库系统

数据库系统要求包括但不限于：

a) 应支持通过系统权限、数据权限、角色权限管理，建立数据库的权限控制机制；
b) 应支持通过WEB服务器或接口服务器访问数据库服务器，设置严格的数据库访问权限,禁止向公网发布数据库端口；
c) 应按照GB/T20273的要求，建立完备的数据修改日志，通过安全审计记录追踪用户对数据库的操作，明确数据库安全责任。

#### 9.2.4 身份认证

身份认证要求包括但不限于：

a) 应支持用户/密码、动态口令、生物特征识别、数字证书等多种身份认证方式；
b) 应支持多因素认证方式；
c) 用户/密码认证时应提供验证码。

### 9.3 运行环境

#### 9.3.1 运行环境基本要求

运行环境基本安全要求包括但不限于：

a） 运行环境需配置安全防护机制，防止恶意入侵和未授权访问；
b） 上线前需通过渗透测试，对高危漏洞实行“零容忍”原则；
c） 应建立漏洞快速响应机制，关键补丁需及时修复或采取临时隔离措施；
d） 管理员账户及敏感操作必须启用MFA（多因素身份验证）。

#### 9.3.2 网络与边界

网络与边界要求包括但不限于：

a) 网络应满足各类交易活动中使用人数和使用高峰期的并发要求；
b) 应配备防火墙、入侵监测等安全设备、部署访问控制列表（ACL）策略，，符合GB/T20270要求。

#### 9.3.3 操作系统

操作系统要求包括但不限于：

a) 应选用符合GB/T20272要求的操作系统；
b) 应选用杀毒软件和攻击防御系统软件对操作系统进行安全防护。

#### 9.3.4 设施设备

设施设备要求包括但不限于：

a) 建有独立机房的平台，其场地的消防、入侵报警、视频监控、出入口控制等应符合GB/T2887的要求；

b） 采用云计算技术架构的平台，服务安全能力应符合GB/T31168的要求。

## 9.4 数据安全

数据安全要求包括但不限于：

a） 应定时进行数据备份，包括用户信息、计费清算信息、合约信息、对账信息、身份信息、标识信息、审计信息等；

b） 敏感数据的传输与存储应进行加密处理，按照GB/T35276、GB/T32905、GB/T32907的要求采用国密算法加密；

c） 数据恢复应符合GB/T20988的要求；

d） 采用国密SSL证书或符合GM/T 0024标准的数字证书保障网络通信安全，防止数据在传输过程中被窃取或篡改。

## 9.5 应急处置

平台应建立应急处置预案，以最大限度降低突发事故对用户正常使用造成的影响。

a） 制定应急预案应包含数据泄露、服务异常等场景处置流程；

b） 至少每年开展1次应急演练，高风险场景可增加频次，演练记录留存≥3年。

# 参 考 文 献

[1] NDI—TR—2025—01 数据基础设施 参考架构
[2] NDI—TR—2025—05 数据基础设施 接入连接器技术要求
[3] RFC 7239（6/2014） 转发超文本传输协议扩展(Forwarded HTTP Extension)