

TC609

全国数据标准化技术委员会技术文件

TC609-6-2025-11

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

2025-08-29 发布

2025-08-29 实施

全国数据标准化技术委员会 发布

目 次

前言	II
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	6
7.3 区域/行业功能节点运营平台	9
7.4 区域/行业功能节点公共服务平台	10
8 互操作要求	12
9 流程要求	12
9.1 身份管理流程	12
9.2 数据资源和产品目录管理流程	12
9.3 标识管理流程	13
10 安全要求	13
10.1 基本要求	13
10.2 平台系统	13
10.3 运行环境	14
10.4 数据安全	15
10.5 应急处置	15
参考文献	16

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：国家信息中心、浪潮云信息技术股份公司、北京国信新网通讯技术有限公司、杭州趣链科技有限公司、北京数网链通科技有限公司、杭州市数据集团有限公司、云上陕西科技运营有限公司、北京新材道数智科技有限公司、北京国际大数据交易所有限责任公司、浙江织数数字科技有限公司、杭州金智塔科技有限公司、西北大学、中国信息通信研究院、国家数据发展研究院、中国电子技术标准化研究院、中国移动通信集团有限公司、中国移动研究院、联通数据智能有限公司、杭州数梦工场科技有限公司、上海数据集团有限公司、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、华为技术有限公司、杭州安恒信息技术股份有限公司、华控清交信息科技(北京)有限公司、江西省大数据中心、中国南方电网有限责任公司、杭州景联文科技有限公司、杭州拓数派科技发展有限公司、嘉兴市文诺财经大数据技术研究院、京东科技信息技术有限公司、领信数科信息技术有限公司、上海零数众合信息科技有限公司、数梦工厂科技有限公司、温州市数据集团、中国科学院深圳先进技术研究院、中通服咨询设计研究院有限公司、云上(江西)大数据发展有限公司、云基华海信息技术股份有限公司、浙江蚂蚁密算科技有限公司、北京大数据先进技术研究院、北京大学、中国南方航空股份有限公司、中电数创、中科斯欧(合肥)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、北京华盛智数科技有限公司、北京可信华泰科技有限公司、北京绿都畅达人才科技发展有限公司、北京天融信网络安全技术有限公司、北京易华录信息技术股份有限公司、北京熠智科技有限公司、北京域智科技有限公司、沧州市大数据中心、洞见智慧科技有限公司、烽火通信科技股份有限公司、公安部第三研究所、广电运通信息科技有限公司、广州芳禾数据有限公司、广州维视达数字科技有限公司、广州信息协会、广州智能科技发展有限公司、国机数字科技有限公司、国家工业信息安全发展研究中心、国家管网集团智网数科、哈尔滨工程大学、南京南瑞信息通信科技有限公司、全国组织机构代码数据服务中心、煤炭科学研究总院有限公司、软通智慧科技有限公司、三未信安科技股份有限公司、山大地纬软件股份有限公司、上海计算机软件技术开发中心、上海芯超数据科技有限公司、深圳市洞见智慧科技有限公司、深圳市尚数网科技有限公司、深圳数据交易所有限公司、生命奇点(北京)科技有限公司、首都信息发展股份有限公司、数据空间研究院、数融智联(徐州)信息科技有限公司、数族科技(南京)股份有限公司、中移雄安信息通信科技有限公司、中汽数据(天津)有限公司、太极计算机股份有限公司、文诺研究院、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、下一代互联网国家工程中心、兴唐通信科技有限公司、亚信科技(中国)有限公司、中国信息协会、数字广东网络建设有限公司。

数据基础设施 区域/行业功能节点技术要求

1 范围

本文件规定了区域/行业功能节点的相互关系、功能架构以及在主体身份管理、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、智能服务、监测运维管理、计费清算、运营分析、行业主数据服务、语义模型服务、行业知识中枢、数据授权运营、应用市场、数据协作开发、高质量数据集公共服务、人才实训、测试验证方面的技术要求。

本文件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，建设基于数场、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数据基础设施，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
GM/T 0024-2023 SSL VPN技术规范
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-2025-05 数据基础设施 接入连接器技术要求
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，提供数据采集、数据加工、数据交易、数据开发、数据流通、数据运营、数据通道管理、公共数据授权运营、区块链、隐私保护计算等服务。

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

数据资源 data resource

指具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合。

3.8

数据产品 data product

指自然人、法人或者非法人组织对其合法获取的数据资源，经过实质性加工和创新性劳动后形成的，可满足特定需求的数据加工品和数据服务。

3.9

三统一 Three Unifications

在数据基础设施领域中，“三统一”指统一目录标识、统一身份登记和统一接口要求。

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）

DID：去中心化身份（Decentralized Identifier）

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

SSL：安全套接层（Secure Sockets Layer）

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。

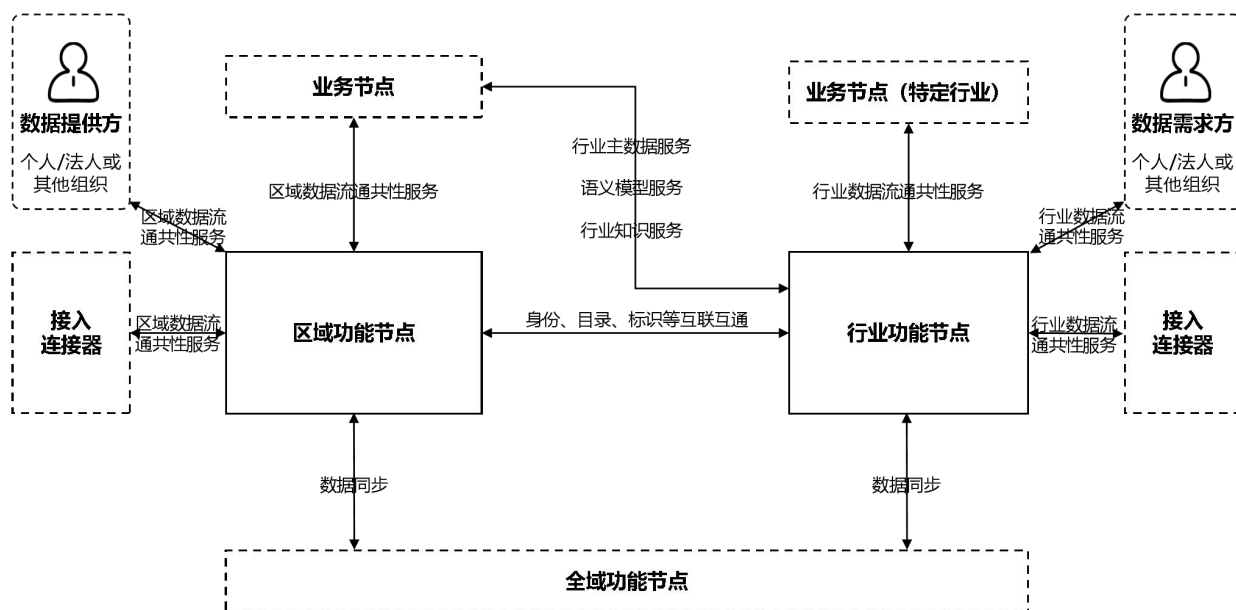


图 1 区域功能节点与行业功能节点关系图

- 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、公共服务等区域数据流通共性服务；
- 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、公共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；
- 区域/行业功能节点应与其他区域/行业功能节点互联，并与全域功能节点互通；
- 行业功能节点应面向业务节点提供行业主数据服务、语义模型服务、行业知识中枢服务等行业数据服务能力，支撑特定行业数据流通服务需求。

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、区域功能节点公共服务平台构成，功能架构如图2所示。

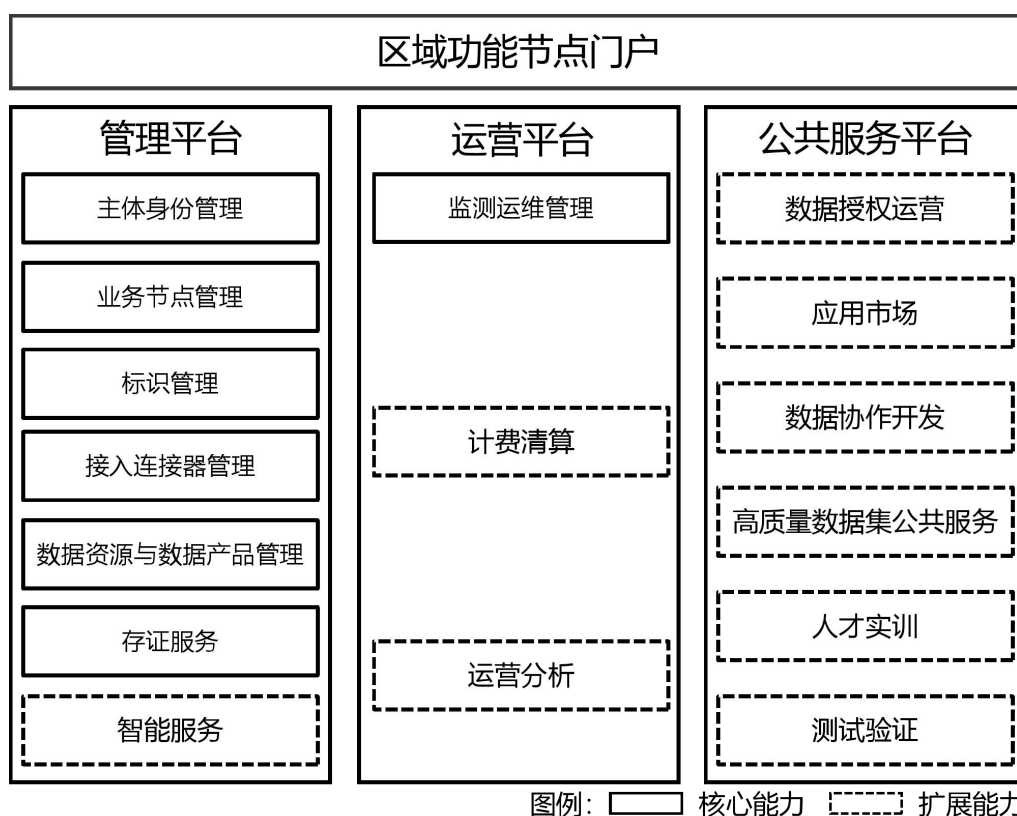


图 2 区域功能节点功能架构图

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主体身份管理、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。

区域功能节点公共服务平台提供数据授权运营、应用市场、数据协作开发、人才实训、测试验证等服务能力，推进数据资源合规利用与价值释放。

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，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、行业功能节点公共服务平台构成，功能架构如图3所示。

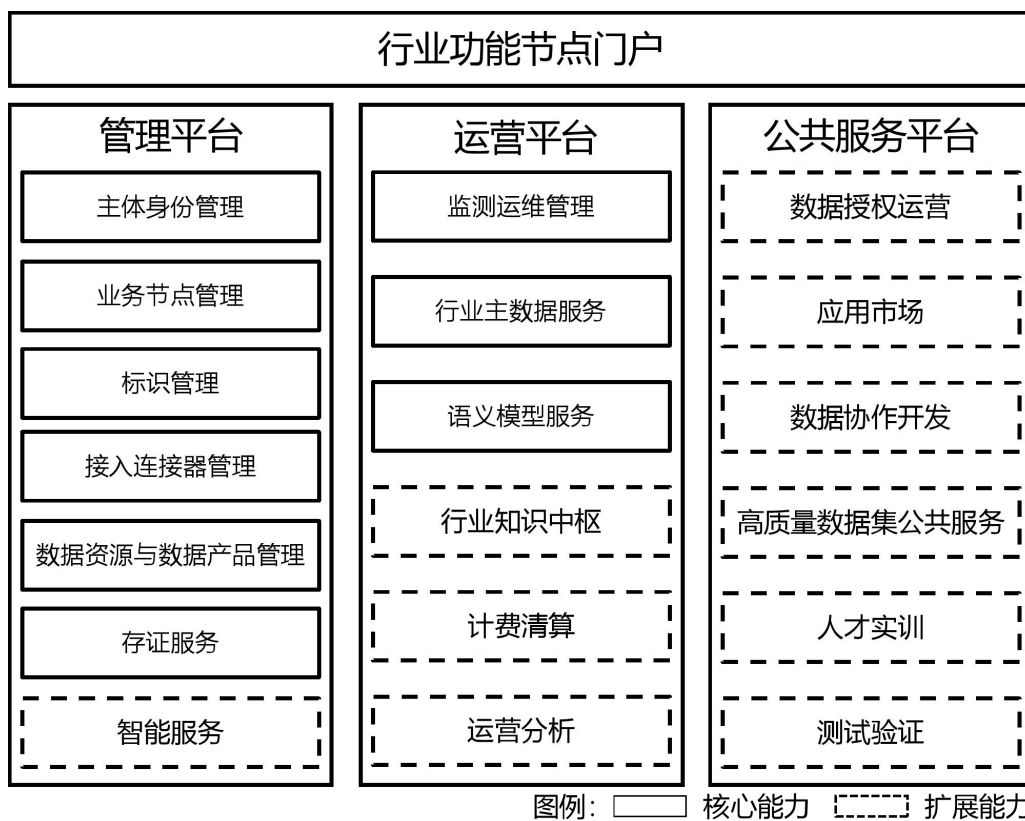


图 3 行业功能节点功能架构图

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。

行业功能节点公共服务平台与区域功能节点相同，面向特定行业提供数据授权运营、应用市场、数据协作开发、人才实训、测试验证等公共服务。

行业功能节点应提供主体身份管理、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、分类展示、检索服务能力；
- d) 应提供数据产品登记、分类展示、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、分类展示、检索服务能力;
- g) 可提供智能检索、智能推荐、智能问答等服务;
- 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) 应按照 NDI-TR-2025-03 的要求进行接入主体(个人/法人或其他组织、法人或其他组织经办人)身份注册、更新、注销管理,并支持对接入主体注册、更新、注销信息进行审核,审核不通过可退回;支持接入主体修改后再次提交,审核通过后颁发身份凭证;可支持接入第三方可信身份提供商,为区域/行业接入主体签发可信身份凭证;
- b) 应提供用户登录认证服务,可通过账号口令、数字证书、DID、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) 应支持按照 NDI-TR-2025-02 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、业务节点查询与核验主体身份信息;
- e) 应支持按照 NDI-TR-2025-03 和 NDI-TR-2025-02 的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、更新、注销、登录、认证等服务。

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,可提供多网域的组网服务,支持具备固定 IP 或动态 IP 的接入连接器在不同网络环境间互联互通;
- c) 应支持为审核通过的接入连接器获取身份凭证,作为接入连接器接入的合法性验证凭证。获取身份凭证应符合 NDI-TR-2025-03 的相关要求;
- 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) 应面向业务节点、接入连接器、其他区域/行业功能节点、全域功能节点提供接入连接器的身份凭证验证能力,应按照 NDI-TR-2025-03 的相关要求支持接入连接器与区域/行业功能节点间双向认证、接入连接器之间双向认证;

- g) 应支持实时监控接入连接器运行状态，按照 NDI-TR-2025-05 确定的接入连接器运行状态上报要求，收集、汇总接入连接器运行状态，监测接入连接器的运行情况，每间隔 5 秒接收接入连接器上报的心跳数据，超时未收到心跳数据则判定该接入连接器已停止运行，支持对断开连接的接入连接器进行筛选、提示、停用等管理；
- h) 应支持按照 NDI-TR-2025-02 的相关要求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 和 NDI-TR-2025-03 确定的业务节点接入、发现、服务流程和要求，为本区域/行业的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 的业务节点编码要求为区域/行业的业务节点发放唯一标识和身份凭证；
- 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 的相关要求，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/行业的业务节点目录中，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包含 NDI-TR-2025-06 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，检测不通过可退回，支持修改后再次提交，并对检测通过的数据资源和数据产品调取标识管理能力进行标识赋码；
- 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，如审核通过则获取对应的标识信息；
- 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服务；

- d) 应支持接入连接器通过标准接口/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向业务节点上架数据产品，数据产品上架信息应符合 NDI-TR-2025-06 中附录表 A.3 数据产品目录字典（产品上架信息）要求，并支持对产品上架信息进行合规性检测；
- e) 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的数据资源和数据产品信息，并提供审核结果查询服务；
- f) 应支持接入连接器通过标准接口/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下架业务节点上已发布的数据产品信息，并提供审核结果查询服务；
- g) 应支持区域/行业功能节点调用全域功能节点提供的标准接口，将数据产品目录、数据资源目录上报全域功能节点；
- h) 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；
- i) 应支持业务节点、接入连接器通过区域/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/行业功能节点登记的数据资源、数据产品信息以及全域数据目录信息；
- j) 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) 应支持对本区域/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 的相关要求；
- 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对应象检索、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 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。

7.2.7 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) 可支持通过语义、文本解析等功能提供数据库、表、字段的查询、关联服务；
- c) 可支持知识存储、处理、构建等能力，为智能体提供知识库服务；
- d) 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。

7.3 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，及时阻断指定业务节点或接入连接器与区域/行业功能节点间的数据流量；
- 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) 应提供主数据服务，支持在行业功能节点页面直接使用，或通过接口形式供业务节点、接入连接器调用；

- c) 可支持对行业主数据进行统一的生命周期管理,包括建立数据治理规则、进行质量监控与评价、实现版本控制与变更追溯,确保数据的准确性与可靠性。

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) 应支持基于行业数据标准,构建行业语义模型,包括对象、属性、关系、规则等关系,并支持语义模型更新和版本管理;
- b) 应支持语义模型的在线检索与查阅;
- c) 应支持通过标准化接口向接入连接器、业务节点提供语义模型的检索、查阅、导出、工具下载等服务。

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、半结构化以及非结构化数据存储;
- 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) 可提供行业知识检索服务,支持在行业功能节点页面直接使用,或通过接口形式供业务节点、接入连接器调用。

7.4 区域/行业功能节点公共服务平台

7.4.1 数据授权运营

数据授权运营的功能包括但不限于:

- a) 可支持公共数据采集、清洗、分类分级和目录管理,形成标准化的物理上或逻辑上的公共数据资产库;
- b) 可支持公共数据授权运营全流程管理和运营服务,包括授权申请、多级审核、协议生成与签署、流通使用监控等功能,确保数据汇集、流通、使用全过程合规可控,实时监控数据流向并防范数据滥用风险;
- c) 可支持个人和企业数据回流、汇聚、治理、分类分级和目录管理,形成物理上或逻辑上的个人和企业数据资产库;
- d) 可支持个人和企业一站式管理自身数据,可在办理业务或享受服务时,授权提供服务的系统使用自身数据,可支持授权第三方机构查阅或使用自身数据;
- e) 可支持应用个人或企业数据进行模型训练,为个人提供医疗健康提醒、旅游路线规划等个性化智能服务,为企业经营分析、客户行为分析等个性化智能服务。

7.4.2 应用市场

应用市场的功能包括但不限于:

- a) 可支持对接入连接器相关软件、数据开发工具、数据应用软件等应用进行上架管理,支持对申请上架的应用进行审核管理,审核通过后可上架应用市场;
- b) 可支持对上架应用进行管理,支持应用检索、信息查看、更新管理、下架管理、版本管理等功能;
- c) 可提供应用检索、应用推荐、应用购买、下载安装卸载、应用更新通知等服务,支持多方主体可在应用市场自行购买、获取所需应用。

7.4.3 数据协作开发

数据协作开发的功能包括但不限于：

- a) 可支持多方主体间数据沙箱、隐私计算等技术开发协议的规范统一，支持跨域数据联合分析、模型训练、数据产品开发等功能；
- b) 可根据用户身份体系提供动态权限分配、匿名化处理、数据动态脱敏、多方共管等服务；
- c) 数据协作开发环境应包含测试环境与生产环境，并支持两种开发环境之间模型、脚本的同步与管理；
- d) 可支持数据模型、算法的安全合规审核管理功能，提供流程审批、血缘追踪、审计追溯等服务；
- e) 可支持数据模型创建、导入、发布、版本管理、废止等功能。

7.4.4 高质量数据集公共服务

高质量数据集公共服务的功能包括但不限于：

- a) 可支持区域/行业内高质量数据集以专题库形式进行统筹管理，提供数据集分级分类管理、供需管理、标签管理、检测规则管理、图谱关联管理等功能；
- b) 可支持接入连接器、业务节点向区域/行业功能节点通过标准接口/页面嵌入/系统界面的方式上传、更新、撤销高质量数据集，区域/行业功能节点需要对相关信息进行审核，并提供审核结果查询；
- c) 可支持从数据质量、合规、安全等维度提供数据集动态评估与评测服务，包括测评申请、测评执行、报告生产、报告核验等功能；
- d) 可支持业务节点通过区域/行业功能节点提供的标准接口/页面嵌入/系统界面的方式检索、查看当前已在区域/行业功能节点登记的高质量数据集信息；
- e) 可支持区域/行业功能节点调用全域功能节点提供的高质量数据集上报接口，将高质量数据集目录上报给全域功能节点；
- f) 可支持区域/行业功能节点调用全域功能节点提供的高质量数据集标准同步接口，获取全域功能节点当前的高质量数据集目录信息；
- g) 可支持向其他区域/行业功能节点提供高质量数据集目录查询服务。

7.4.5 人才实训

人才实训功能包括但不限于：

- a) 可支持数据要素基础设施相关培训资源上传、存储、分类管理功能，支持文档、视频、课件等多种格式资源管理；
- b) 可提供课程管理功能，应记录用户学习进度，提供历史学习课程和进度查询；
- c) 可提供在线考评能力，支持题库管理、成绩统计等功能；
- d) 可提供证书认证服务，按照规定的要求完成课程后，可生成证书，并提供证书的生成、查询、验证、下载等功能。

7.4.6 测试验证

测试验证的功能包括但不限于：

- a) 可支持为业务节点、接入连接器等平台提供功能测试与互联互通测试服务；
- b) 可提供区域功能节点、业务节点、接入连接器测试桩，提供测试验证环境；
- c) 可支持测试用例和标准接口查看与下载；
- d) 可支持测试任务的创建、编辑、删除等管理功能；
- e) 测评的任务可包括但不限于页面测评、接口自动化测评等，其中接口自动化测评需满足互联互通

f) 可支持测试报告的自动化生成,可在线查看和下载。

区域/行业功能节点与全域功能节点、业务节点、接入连接器的互操作要求应满足NDI-TR-2025-02的相关要求。

9.1 身份管理流程

9.2 数据资源和产品目录管理流程

The diagram illustrates the data resource management and distribution process flowchart, showing the interaction between various components within a 'Global Functional Node' (全域功能节点) and the flow of data between 'Data Provider' (数据提供方) and 'Data Demander' (数据需求方).

Global Functional Node (全域功能节点):

- 3. Data Catalog Reporting (数据目录上报)
- 4. Global Catalog Synchronization (全域目录同步)
- 2.7 Data Product Listing (数据产品上架)
- 2.5 Data Resource/Product Registration (数据资源/产品登记)
- 2.1 Data Resource/Product Registration (数据资源/产品登记)

Data Provider (数据提供方): (Individual/Enterprise/Other Organization)

- 1.1 Local Data Resource Access (本地数据资源接入)
- 1.2 Packaging Data Products and Inclusion in Local Data Catalog (封装数据产品并纳入本地数据目录)
- 2.4 Identification/Labeling (标识赋码)
- 2.3 Compliance Check (合规检测)
- 5.2 Data Catalog Query (数据目录查询)

Regional/Industry Functional Node (区域/行业功能节点):

- 2.2 Data Resource/Product Registration (数据资源/产品登记)
- 2.8 Data Product Listing (数据产品上架)
- 5.1 Data Catalog Query (数据目录查询)
- 2.6 Data Resource/Product Registration (数据资源/产品登记)
- 5.3 Data Catalog Query (数据目录查询)

Business Node (业务节点):

- 5.4 Data Discovery Access (数据发现访问)

Data Demander (数据需求方): (Individual/Enterprise/Other Organization)

- 5.2 Data Catalog Query (数据目录查询)

Access Connectors (接入连接器):

- 5.3 Data Catalog Query (数据目录查询)

Flow Summary:

- Data Provider connects to the Regional/Industry Functional Node via 1.1 and 1.2.
- Data Provider sends 2.4 and 2.3 to the Regional/Industry Functional Node.
- Data Provider queries the Regional/Industry Functional Node via 5.2.
- Regional/Industry Functional Node sends 2.2 and 2.8 to the Business Node.
- Regional/Industry Functional Node sends 5.1 to the Business Node.
- Regional/Industry Functional Node sends 2.6 to the Access Connector.
- Regional/Industry Functional Node queries the Access Connector via 5.3.
- Business Node sends 5.4 to the Data Demander.
- Data Demander queries the Access Connector via 5.2.
- Access Connector queries the Data Demander via 5.3.
- Data Provider sends 2.5 and 2.7 to the Global Functional Node.
- Global Functional Node sends 3 and 4 to the Regional/Industry Functional Node.
- Global Functional Node sends 2.1 to the Business Node.

上述流程如下：

- 12

- e) 各类用户可通过区域/行业功能节点、接入连接器进行数据目录查询，通过业务节点进行数据发现访问。

9.3 标识管理流程

标识管理的核心业务流程见下图：

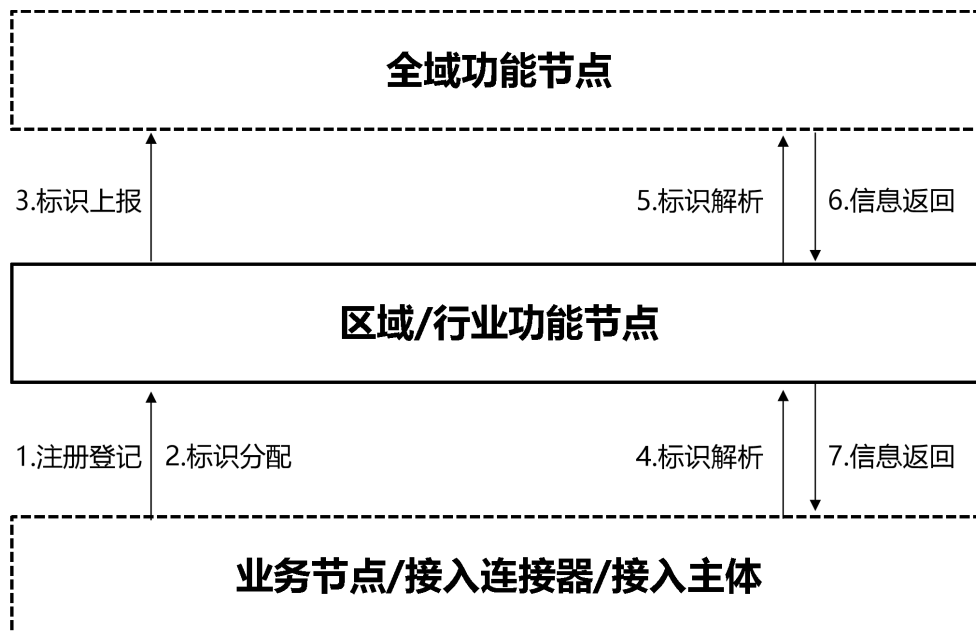


图5 标识管理业务流程图

上述流程如下：

- 业务节点/接入连接器/接入主体等向区域/行业功能节点进行身份、数据等注册登记；
- 区域/行业功能节点审核通过后为其分配相应标识，业务节点/接入连接器/接入主体等可通过门户或接口查询到相应标识；
- 区域/行业功能节点向全域进行标识等用户信息上报，将标识汇总至全域功能节点；
- 业务节点/接入连接器/接入主体等可通过标识解析接口向区域/行业功能节点查询该标识详细信息；
- 区域/行业功能节点提供本区域标识解析，若本地不存在则通过全域标识解析接口获取全域中该标识详细信息；
- 区域/全域依次返回标识详细信息，供业务节点/接入连接器/接入主体查看使用。

10 安全要求

10.1 基本要求

各平台应至少满足 GB/T 22239-2019中规定的第三级安全要求。

10.2 平台系统

10.2.1 平台系统基本安全要求

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。

10.2.2 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。

10.2.3 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/T 20273-2006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。

10.2.4 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) 宜支持多因素认证方式；
- c) 用户/密码认证时应提供验证码。

10.3 运行环境

10.3.1 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) 平台上线前应通过渗透测试；
- 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）。

10.3.2 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/T 20270-2006要求。

10.3.3 操作系统

操作系统要求包括但不限于：

- a) 应选用符合GB/T 20272-2019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。

10.3.4 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/T 2887-2011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/T 31168-2023的要求。

10.4 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/T 32905-2016、GB/T 32907-2016的要求采用国密算法加密；
- c) 数据恢复应符合GB/T 20988-2007的要求；
- d) 采用国密SSL证书或符合GM/T 0024-2023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。

10.5 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件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
-