

TC609

全国数据标准化技术委员会技术文件

TC609-6-2026-XX

数据基础设施 智能体交互技术要求

Data infrastructure—Technical requirements for agent interaction

（征求意见稿）

2026-XX-XX 发布

2026-XX-XX 实施

全国数据标准化技术委员会 发布

目 次

前 言	II
1 范围	3
2 规范性引用文件	3
3 术语和定义	3
4 缩略语	3
5 总体概念	4
5.1 概述	4
5.2 概念模型	4
5.3 概念域	4
6 功能要求	5
6.1 概述	5
6.2 功能描述	5
7 互操作要求	7
7.1 总体要求	7
7.2 重要功能设施互操作要求	7
7.3 业务节点互操作要求	8
7.4 接入连接器互操作要求	8
7.5 智能体互操作要求	8
7.6 算力设施互操作要求	8
8 安全要求	9
8.1 智能体系统安全	9
8.2 智能体通信安全	9
8.3 资源访问安全	9
8.4 智能体调度安全	10
8.5 审计与存证安全	10
附 录 A （规范性） 基于 MCP 协议的智能体交互参考实现	11
参 考 文 献	17

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 智能体交互技术要求

1 范围

本文件规定了智能体在接入数据基础设施时与各个功能组件之间的交互关系、以及智能体之间通过基础设施功能组件的交互。

本文件适用于指导智能体的设计、研发企业如何利用数据基础设施中的相关资源以提升智能体能力并将智能体接入到数据基础设施中。

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。

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能体 agent

能感知环境，并主动采取行动以实现特定目标的实体。

注：一般为软件系统。

[来源： GB/Z 185.1-2026 人工智能 智能体互联 第 1 部分：总体架构]

3.2

智能体交互 agent interaction

智能体以远程接口调用的形式访问数据基础设施中接入的数据、工具或其他智能体等资源。

3.3

智能体标识 agent identifier

用于在网络环境、分布式系统或数字生态中，唯一识别、定位和关联智能体身份、属性及行为特征的标准化信息载体。

4 缩略语

下列缩略语适用于本文件。

A2A：智能体交互协议（Agent to Agent）

ANP：智能体网络协议（Agent Network Protocol）

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

DOIP：数字对象接口协议（Digital Object Interface Protocol）

gRPC：一种轻量级的远程过程调用协议（google Remote Procedure Call）

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

MCP：模型上下文协议（Model Context Protocol）

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

RESTful API: 符合REST风格的应用程序接口, 一般基于HTTP协议实现

5 总体概念

5.1 概述

对数据基础设施而言, 智能体一方面可作为一种产品服务, 通过接入连接器接入数据基础设施, 形成产品并在业务节点中发布, 供需求方发现和使用智能体能力; 另一方面, 智能体也是一种数据应用, 能够充分利用数据基础设施中接入的数据、工具和其他智能体资源, 解决实际的场景问题。作为数据产品时, 智能体应按照数据基础设施中对数据产品相关要求, 在数据基础设施的各个系统组件中进行登记、发布及交付; 作为数据应用时, 智能体可基于数据基础设施各系统中提供的各类服务接口发现、订购、使用数据基础设施中的各类资源, 同时数据基础设施还应面向智能体提供相应的功能及接口扩展。

5.2 概念模型

概念模型描述了智能体在接入数据基础设施并使用其已接入的各类数据、工具和智能体资源时, 所涉及的与数据基础设施相关的交互模块以及交互关系。



图1 数据基础设施中智能体交互概念模型图

5.3 概念域

5.3.1 智能体

智能体域是不同类型智能体的身份维护、元数据维护、智能体交互和认证鉴权等自有功能的集合。智能体是智能体交互中的核心执行单元, 由具有服务供给能力的相关主体提供。

5.3.2 重要功能设施

重要功能设施域是20255408-T-907中规定的重要功能设施所具备的功能集合。重要功能设施基于已有接口面向智能体提供身份、标识、目录等相关服务, 并提供面向智能体的相关功能扩展, 见6.2.2。

5.3.3 业务节点

业务节点域是20255408-T-907以及20262814-T-907等业务节点相关标准中规定的业务节点所具备的功能集合。业务节点基于已有接口面向智能体提供自身所具备的相关服务, 并提供面向智能体的相关功能扩展, 见6.2.3。

5.3.4 接入连接器

接入连接器域是20255408-T-907以及20255402-T-907中规定的接入连接器所具备的功能集合。接入连接器基于已有接口面向智能体提供自身具备的基础及扩展能力，并应提供面向智能体的相关功能扩展，见6.2.4。

5.3.5 算力设施

算力设施域是20255408-T-907中规定的算力设施所具备的功能集合。算力设施基于已有接口面向智能体提供算力服务，并应提供面向智能体的相关功能扩展，见6.2.5。

6 功能要求

6.1 概述

智能体交互功能架构以概念模型为基础，给出各个概念域面向智能体的功能扩展，以及智能体域与数据基础设施各个域的互操作关系。其中，数据基础设施各系统面向智能体产品或应用扩展的功能亦有所差异，见图2。

注：智能体身份唯一标识一般由重要功能设施分配。

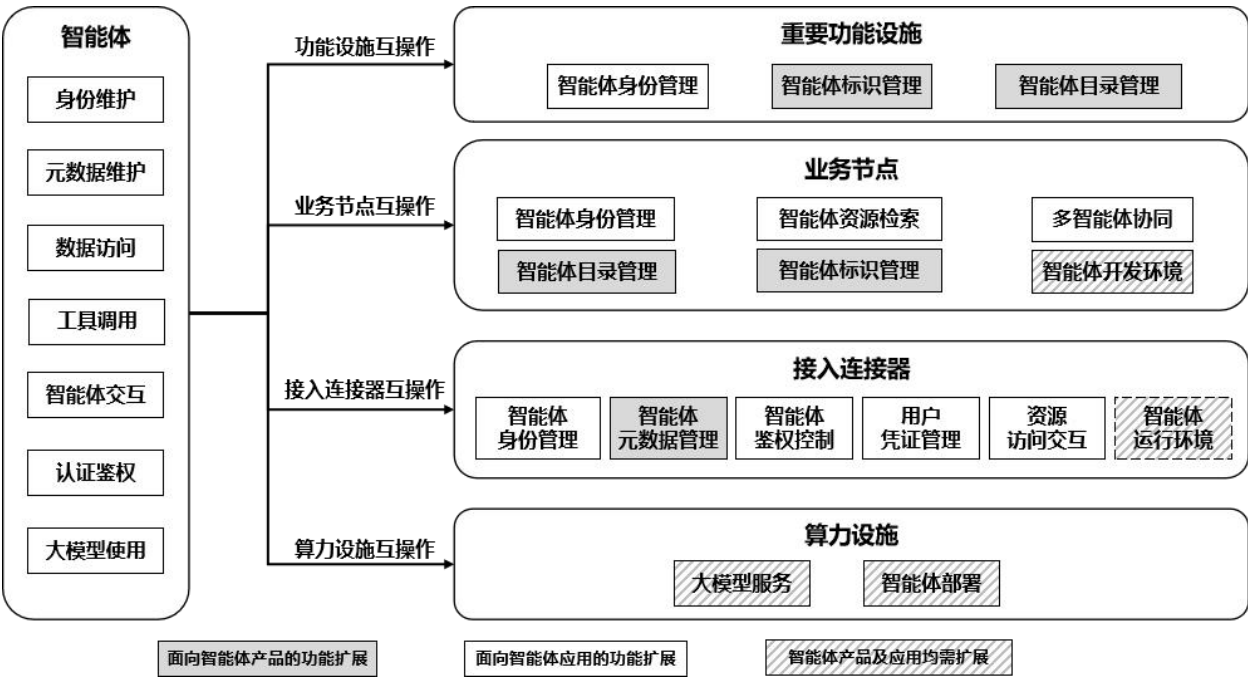


图2 数据基础设施 智能体交互功能架构

6.2 功能描述

6.2.1 智能体

作为一种接入数据基础设施的软件系统，智能体的功能应包括：

- a) 身份维护：维护由相关主体为智能体颁发的身份信息，如：智能体标识、证书、密钥等；
- b) 元数据维护：维护智能体本身的描述信息，用于其他人发现并了解智能体的基本能力；

- c) 数据访问：能够以常见的数据访问接口协议，如：RESTful API、DOIP等提供标准访问接口的数据资源；
- d) 工具调用：能够基于常见协议，如：gRPC、MCP等，调用以API形式提供服务的远程工具；
- e) 智能体交互：能够基于常见的智能体交互协议，如：A2A、ANP等，访问其他智能体提供的服务接口并与之交互；
- f) 认证鉴权：对接收到的访问请求具备身份认证和权限鉴别的能力，判断其是否有权访问自身提供的服务；
- g) 大模型使用：能够按需使用本地部署或远程部署的大模型服务，规划或完成用户指定的任务；
- h) 智能体宜具备基于所感知的数据、状态和规则，对任务执行路径、资源使用策略及风险处置方式进行判断和选择的能力，其决策结果可通过语义化任务请求或建议的方式传递给其他系统或人工参与者。

6.2.2 重要功能设施

重要功能设施负责管理、维护全局智能体的身份、标识及目录信息。面向智能体交互，重要功能设施在TC609-6-2025-11规定的功能基础上应扩展的功能包括：

- a) 智能体身份管理：面向智能体应用提供身份注册、身份验证、身份注销等服务；
- b) 智能体标识管理：提供面向智能体产品的编码规则以及标识注册、标识解析等服务；
- c) 智能体目录管理：提供面向智能体产品的编目规则，编制智能体目录并提供目录浏览和检索功能。

6.2.3 业务节点

业务节点作为重要功能设施在区域/行业层面的业务代理，其智能体身份管理、目录管理等功能应基于重要功能设施提供的基础服务进行扩展和业务化封装。业务节点宜作为智能体发现、调度全网数据、工具、智能体资源的入口及枢纽，各业务节点宜结合自身业务特征按需提供智能体相关服务。业务节点在已有标准文件中规定的功能基础上，宜扩展的功能包括：

- a) 智能体身份管理：提供面向智能体应用的身份注册、身份验证、身份注销等服务。智能体在业务节点注册身份时，可代理向重要功能设施申请全局身份或在全局身份基础上分配业务场景相关的本地身份；
- b) 智能体目录管理：提供面向智能体产品的编目规则，编制智能体目录并提供目录浏览和检索功能；
- c) 智能体资源检索：提供适用于智能体应用的数据、工具、智能体等资源的检索服务，支持基于联邦检索、语义向量、知识图谱以及多轮交互的深度搜索等能力增强面向智能体的资源检索服务；
- d) 智能体标识管理：提供适用于智能体产品的编码规则以及标识注册、标识解析等服务。业务节点为智能体分配标识时应符合20255409-T-907相关要求；
- e) 多智能体协同：提供面向智能体应用的多智能体协调服务，能够针对智能体处理的复杂任务，按需匹配业务节点上可发现的其他智能体并编排任务协同流程，并协助完成智能体消息分发和任务调度；
- f) 智能体开发环境：提供面向智能体应用及产品的开发环境，支持利用数据基础设施中接入、购买的数据、工具及智能体资源组合开发出新的智能体，并接入数据基础设施提供服务。

6.2.4 接入连接器

接入连接器可作为智能体接入数据基础设施并与数据基础设施中各类资源交互的入口。面向智能体，接入连接器应在20255402-T-907规定的的能力基础上，扩展如下功能：

- a) 智能体身份管理：管理在本地接入的智能体应用在数据基础设施中的身份信息，包括身份标识、证书等。同时，宜支持连接器代理向重要功能设施申请智能体身份；
- b) 智能体元数据管理：管理在本地接入的智能体产品的描述信息，包括但不限于：智能体名称、描述、服务地址、提供者信息、版本、文档链接、能力、认证要求、默认交互模式以及智能体具备的技能集合；
- c) 智能体鉴权控制：能够识别访问本连接器智能体应用的用户身份信息，并根据凭证鉴定是否具有访问相应智能体的权限，凭证一般包括：智能体应用的身份凭证以及终端请求用户的身份凭证；
- d) 用户凭证管理：管理利用本地智能体应用访问数据基础设施相关资源的用户的凭证信息，当本地智能体访问其他数据基础设施中的数据、工具、智能体资源时，应携带请求发起者的用户身份凭证以及智能体本身的身份凭证；
- e) 资源访问交互：支持本地智能体应用远程访问其他连接器中接入的数据资源、工具资源并支持被其他连接器中接入的智能体访问，从而实现智能体协同交互；
- f) 智能体运行环境：接入连接器可提供智能体产品及应用的运行环境，支持智能体直接本地部署在接入连接器中。

6.2.5 算力设施

算力设施为智能体产品及应用提供大模型推理和算力服务。面向智能体产品及应用，算力设施应在20255408-T-907规定的的能力基础上，扩展如下功能：

- a) 智能体部署：提供PaaS（平台即服务 Platform as a Service）服务与大语言模型平台，支持智能体提供方利用算力设施中相关资源完成智能体和大模型的部署；
- b) 模型服务：提供模型即服务MaaS（模型即服务 Model as a Service）的能力，支持智能体产品及应用按需调用算力设施提供的大模型资源，完成任务规划和执行。

7 互操作要求

7.1 总体要求

智能体作为数据产品时按照20255402-T-907、20255410-T-907等标准中数据产品相关规范进行登记、上架及交付，与数据基础设施的交互不设额外要求。当智能体作为数据应用时，需要从数据基础设施中发现、订购、使用相关产品服务，此时会与数据基础设施的各个系统产生交互，基础设施应提供适应于智能体的交互接口，接口应基于现有成熟的智能体互操作协议进行实现，如：MCP、A2A等。

智能体应用与数据基础设施其他系统构件之间的交互分为两类：一是基于各个数据基础设施技术文件中已规定的互操作能力进行交互；二是在此基础上，各个功能构件应面向智能体扩展的互操作能力。基于已有互操作能力的交互要求应遵循相应技术文件中的有关要求，在此基础上应扩展的互操作能力。

7.2 重要功能设施互操作要求

除利用20255405-T-907规定的互操作能力进行交互外，重要功能设施还应面向智能体扩展如下接口：

- a) 智能体身份接口：支持智能体向区域/行业重要功能设施注册、修改、注销身份，以及获取其他主体及智能体的身份凭证；
- b) 智能体目录接口：支持智能体查询区域/行业重要功能设施中已注册的智能体服务信息；

- c) 智能体标识接口：支持智能体解析区域/行业重要功能设施中已注册的智能体标识信息。

7.3 业务节点互操作要求

除利用业务节点提供的基本服务接口使用业务节点功能外，面向智能体业务节点宜提供如下接口：

- a) 智能体身份接口：支持智能体通过业务节点注册、修改、注销身份，业务节点应按需调用重要功能设施相应接口完成身份同步。
- b) 智能体目录接口：支持智能体向业务节点发布自身元数据信息形成目录，或查询其他智能体元数据信息；
- c) 智能体标识接口：支持智能体业务节点发布自身标识信息，或查询其他智能体标识信息；
- d) 智能体资源检索：支持智能体基于用户需求以适应智能体的方式检索数据基础设施中的资源；
- e) 智能体资源寻址：支持智能体基于所需资源标识定位目标资源所在网络位置及访问接口信息；

7.4 接入连接器互操作要求

智能体与接入连接器的互操作可分为以下两种情况：一是接入连接器具备智能体运行环境，支持智能体部署在接入连接器中，此时智能体与接入连接器的交互以STDIO（标准输入输出 Standard Input/Output）等本地接口调用模式；二是接入连接器与智能体分开部署，此时接入连接器作为智能体与数据基础设施中其他功能模块交互的代理，此时接入连接器与智能体之间应通过远程接口调用模式交互。面向智能体，接入连接器应提供的接口包括：

- a) 接入连接器能力查询接口：支持智能体域查询指定接入连接器的硬件配置、安全芯片型号、当前负载等基础及扩展能力信息，确认连接器具备处理智能体请求的相应能力；
- b) 智能体身份管理接口：支持智能体将通过业务节点、重要功能设施获取到的身份信息交由接入连接器进行管理；
- c) 智能体元数据管理接口：支持智能体向接入连接器发布、修改、删除自身元数据信息；
- d) 资源请求接口：支持智能体将对数据基础设施中的资源访问需求发送给接入连接器，并由接入连接器转发或代理向资源所在目标接入连接器访问相应数据、工具及智能体资源；
- e) 资源访问接口：数据供方连接器应支持面向智能体基于常见协议提供标准化的资源访问接口，如：基于MCP的函数工具访问接口，基于A2A、ANP的智能体服务访问接口等。

7.5 智能体互操作要求

智能体在以远程形式接入数据基础设施提供服务时，应提供如下接口，允许接入连接器按需调用智能体服务：

- a) 智能体身份获取接口：支持接入连接器获取智能体的身份信息；
- b) 智能体元数据获取接口：支持接入连接器获取智能体的元数据信息；
- c) 智能体交互接口：支持接入连接器向智能体转发接收到的任务需求，并支持智能体的异步响应。

7.6 算力设施互操作要求

智能体与算力设施的交互主要用于计算资源的申请，以及模型服务的调用。前者一般由智能体提供者通过用户界面操作完成，不需提供额外接口；后者则可基于以下接口提供大模型即服务的互操作能力：

- a) 模型服务调用接口：支持智能体按需调用算力设施中部署的大模型服务，请求模型推理、生成或微调等服务，应支持标准的模型调用协议（如OpenAI Chat Completions API等），并具备身份认证与计量机制；
- b) 算力资源查询接口：算力设施通过统一元数据模型对外暴露其计算能力，智能体可通过服务发现协议实时查询可调用的算力资源。

8 安全要求

8.1 智能体系统安全

8.1.1 智能体接入安全

接入数据基础设施的智能体系统应进行有效的安全评估，并由具备资质的身份授权方对智能体及其提供者的身份进行安全合规检验，颁发智能体身份标识及证书，确保接入数据基础设施的智能体的安全合规。

8.1.2 智能体行为监控

接入连接器应实时监督本地智能体行为是否符合其角色定义与操作边界，限制其生成外部链接或调用高危接口的能力。采用多重防护机制（如安全护栏、审核API、备用验证模型）过滤可能被篡改的响应内容。同时监测是否存在诱导人类执行非预期操作的策略性行为。

对可能影响现实系统运行结果的智能体行为，应通过权限分级、人工确认或仿真验证等机制进行约束，防止智能体在无人工监督的情况下形成不可控的现实影响。

8.1.3 恶意智能体处置

接入连接器应开展对智能体异常行为的检测，自动识别违反安全策略的智能体实例。一经确认，立即隔离其网络连接、撤销系统权限，并终止相关进程。对尝试更换身份或重建会话以规避管控的恶意实体，应实施持续追踪与阻断，确保威胁彻底清除。

8.2 智能体通信安全

智能体在数据基础设施中通信应采用传输链路加密与消息完整性校验机制，防止未经授权的访问、数据泄露和恶意攻击。接入连接器作为传输链路的可信安全节点（TLS终止点），负责在其管辖范围内对通讯内容进行安全审计和合规检查，数据在接入连接器处解密、审计后重新加密转发。加密算法强度不应低于SM4/AES-256。

应引入动态信任评分模型评估交互方的可靠性。关键操作应通过多智能体协同验证或交叉验证确认，避免单点决策风险。通信范围应依据角色职责实施细粒度隔离，限制非必要跨域交互。系统应配置速率限制与专属资源配额，防范请求泛洪或DDoS类攻击，并优先选用开放、安全、可互操作的通信协议。

8.3 资源访问安全

8.3.1 资源访问安全

智能体使用过程中存在三种典型数据流向：

- a) 本地数据访问：智能体与所需数据位于同一平台（业务节点或接入连接器）内，数据访问在平台内部完成，应通过平台内部的访问控制机制和权限管理确保数据安全；
- b) 跨平台数据访问：智能体需调用其他平台的数据资源（如业务节点中运行的智能体需访问其他接入连接器中的数据），数据跨平台流转时，应在每个传输节点实施身份验证和加密保护，确保数据在跨平台传输过程中的安全性和完整性。
- c) 智能体协同交互：智能体之间通过A2A/ANP等协议进行跨连接器的服务调用与数据交换，应在交互双方实施双向身份认证、权限验证和数据加密，确保跨连接器智能体协同过程中的安全性和数据隐私。

智能体调用数据基础设施中的资源或与其他接入数据基础设施中的智能体进行交互时，须实施最小权限原则，严格限定其可访问的工具集合，并在每次调用前完成函数级身份认证。同时，须实施严格的访问控制策略，确保只有经过授权的智能体能够访问特定资源或执行特定操作。当接入连接器与智能体分开部署时，接入连接器作为智能体与数据基础设施中其他功能模块交互的网关，应对跨连接器的资源访问请求实施双向身份认证、权限委托验证和访问范围控制，防止未授权的跨域资源访问。所有工具交互行为应完整记录于不可篡改的日志系统中，支持全链路审计与异常回溯。对涉及金融交易、医疗诊断、行政许可等高风险功能的操作，必须引入强制性人工审批机制。

8.3.2 资源使用安全

智能体使用数据基础设施数据的关键过程应执行于隐私保护计算、数据沙箱等安全环境中，防止越权操作影响主营业务系统。系统应基于实时风险评分动态调整工具调用权限，对包含提权、系统修改等敏感操作的AI生成代码，须经人工复核后方可执行。

8.3.3 输入输出安全

智能体接收的所有输入（包括文本、图像、音频及多模态数据）应进行内容过滤与语义验证，有效防范提示注入、角色伪装、语义混淆及隐写攻击等新型威胁。输出内容须通过合规性校验，自动拦截包含违法不良信息、伦理违规或安全敏感指令的响应。

8.4 智能体调度安全

具备智能体调度能力的业务节点应持续监控智能体间的任务委派、角色切换与权限变更行为，识别未授权提权或异常协作模式。记录全部交互日志，检测非常规请求序列、重复被拒后绕过审批的行为，以及同类场景下决策结果不一致等异常现象。对潜在的恶意智能体实施自动标记与行为限制。

8.5 审计与存证安全

数据基础设施应建立覆盖智能体全生命周期的审计与存证机制，包括：

- a) 行为日志：完整记录智能体的身份认证、资源访问、工具调用、数据传输等全部交互行为，日志内容应包含操作时间、操作主体、操作对象、操作类型及操作结果；
 - b) 不可篡改存储：审计日志应存储于不可篡改的日志系统中，支持基于哈希链等技术手段保障日志的完整性和真实性；
 - c) 全链路追溯：支持基于智能体标识和交互会话标识的全链路追溯能力，能够还原智能体完整的行为轨迹和决策过程；
- 异常告警：基于审计日志实施实时异常检测，对异常行为模式（如频繁的权限提升尝试、异常的数据访问模式等）自动告警并触发相应的安全响应措施。

附录 A
(规范性)
基于 MCP 协议的智能体交互参考实现

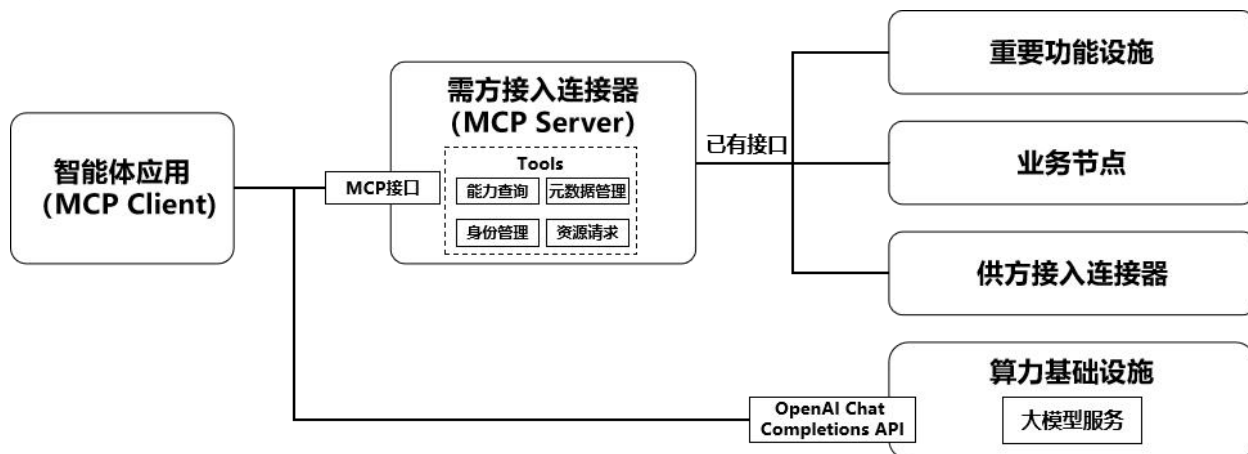
A.1 目标

本标准仅涉及智能体与数据基础设施交互的基本要求，不限定具体实现。为进一步指导数据基础设施建设方与智能体开发方的技术实践，本小结以MCP协议为例，展示如何基于MCP协议在符合标准的情况下实现智能体与数据基础设施各个系统的交互。

A.2 以连接器为网关访问数据基础设施资源

A.2.1 参考架构

连接器是用户访问数据基础设施资源的入口，数据基础设施标准体系中已经对连接器与数据基础设施各个系统之间的交互接口进行了基本规范，智能体应用可以连接器为网关，访问数据基础设施中的各类数据资源。以MCP为例，此时智能体与基础设施的交互关系如图A.2-1所示。



图A. 2-1 以连接器为网关的MCP参考实现

智能体应用作为MCP Client，需方连接器作为MCP Server，二者之间基于MCP协议进行交互。按照标准要求，此时需方连接器需要以MCP Tools的方式实现能力查询、元数据管理、身份管理、资源请求四类工具。连接器作为MCP Server，对外提供统一访问接口，智能体可基于tool/list了解接入连接器的基本能力，并由连接器为代理，基于已有接口访问重要功能设施、业务节点、供方接入连接器中的各类资源。

A.2.2 接口要求

A.2.2.1 接入连接器接口要求

接入连接器MCP Server提供以下四类工具，分别对应7.4规定的：能力查询（发现可用的服务和资源）、元数据管理（维护智能体描述信息）、身份管理（维护智能体身份凭证）、资源请求（发起数据资源访问）。其接口应满足如下要求：

a) 能力查询（capability_query）

查询接入连接器及其后端系统对外提供的服务能力清单，供智能体在接入前评估可用的服务和资源类型。表A.2-1 capability_query 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
能力类型	capability_type	string	否	按能力类型过滤，如 identity、directory、resource、compute 等；不填则返回全部
返回值：能力列表	capabilities	array	—	能力清单，每项含 capability_id、capability_type、description、endpoint 等

b) 元数据管理（metadata_manage）

管理智能体在接入连接器中的描述元数据，支持注册、更新、查询和注销操作。

表 A.2-2 metadata_manage 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
操作类型	action	string	是	管理操作：register（注册）、update（更新）、query（查询）、deregister（注销）
智能体标识	agent_id	string	条件必填	智能体标识；update、query、deregister 操作时必填
智能体元数据	agent_metadata	object	条件必填	智能体描述元数据，包含名称、功能描述、能力标签等；register 和 update 操作时必填
返回值：操作结果	result	object	—	操作结果对象，含 status（状态码）、message（描述信息）及操作相关的返回数据

c) 身份管理（identity_manage）

管理智能体在接入连接器中的身份信息与凭证，支持注册身份、更新凭证、查询身份、注销身份操作。

表 A.2-3 identity_manage 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
操作类型	action	string	是	管理操作：register（注册）、update_credential（更新凭证）、query（查询）、deregister（注销）
智能体标识	agent_id	string	条件必填	智能体标识；update_credential、query、deregister 操作时必填
身份凭证	credential	string	否	注册或更新时提供新的身份凭证，由重要功能设施签发
返回值：操作结果	result	object	—	操作结果对象，含 status（状态码）、message（描述信息）及操作相关的返回数据

d) 资源请求（resource_request）

通过接入连接器向数据基础设施请求访问数据资源，获取资源访问会话及凭据。连接器根据资源标识路由到对应业务节点，完成访问授权后返回访问端点。

表 A.2-4 resource_request 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
资源标识	resource_id	string	是	目标数据资源的全局标识
访问模式	access_mode	string	是	访问模式：read（只读）、write（写入）、stream（流式读取）
访问参数	access_params	object	否	访问附加参数，如数据过滤条件、字段投影、分

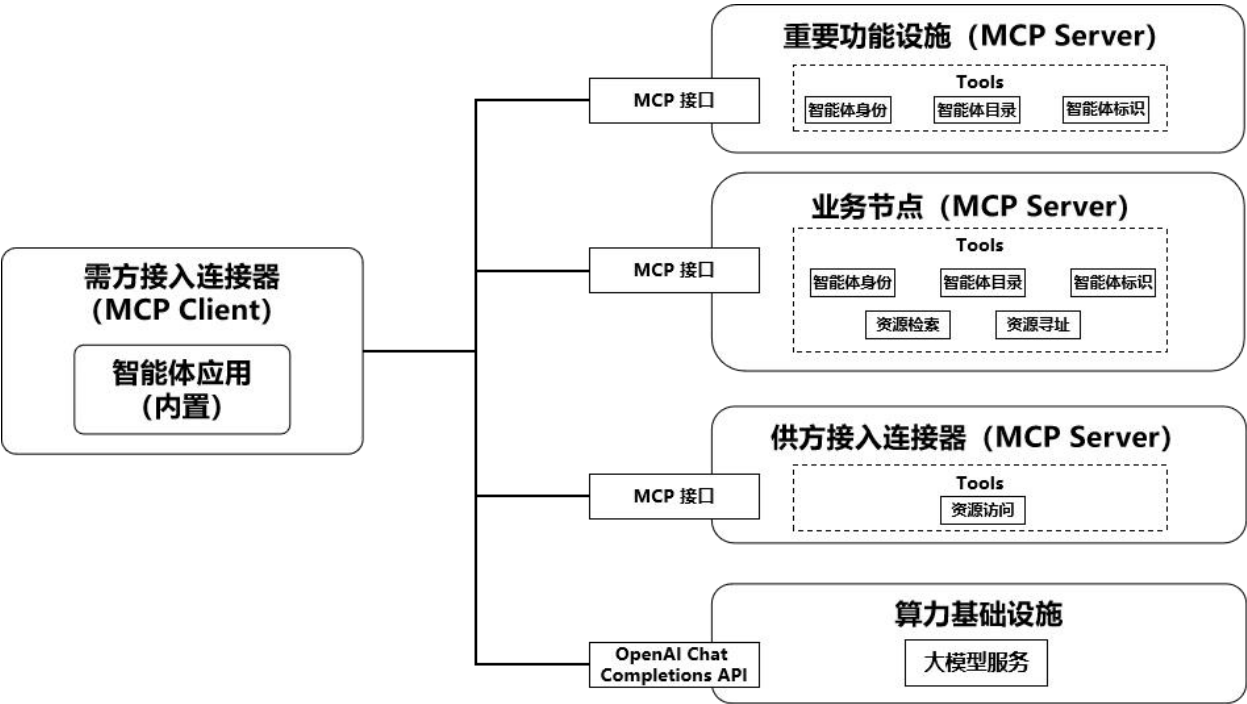
				页设置等
返回值：资源标识	resource_id	string	—	访问的资源标识（原值返回）
返回值：资源内容	resource_content	object	—	访问的资源内容

A.3 连接器部署智能体直接访问数据基础设施

A.3.1 参考架构

当智能体应用直接部署在连接器上时，连接器作为Client，与重要功能设施、业务节点、连接器以及算力设施之间进行交互。除通过已有的HTTP接口进行交互外，数据基础设施的各个系统还应提供专用于智能体的访问接口，交互关系如图A.3-1所示。

内置智能体的连接器作为MCP Client，重要功能设施、业务节点、供方连接器作为MCP Server，二者之间基于MCP协议进行交互。按照标准要求，此时重要功能设施需要以MCP Tools的方式实现智能体身份、智能体目录、智能体标识三类工具；业务节点需要实现智能体身份、智能体目录、智能体标识、资源检索、资源寻址、编排调度六类工具；供方接入连接器需实现能力查询、元数据管理、身份管理、资源请求四类工具，这三个系统均为MCP Server，对外提供统一访问接口，需方智能体应用可基于tool/list了解各系统的基本能力，并直接访问重要功能设施、业务节点、供方接入连接器中的各类资源。提供大模型服务的算力设施可基于OpenAI Chat Completions API提供推理服务，供智能体访问。



图A.3-1 以连接器为网关的MCP参考实现

A.3.2 接口要求

A.3.2.1 重要功能设施接口要求

重要功能设施作为MCP Server，提供以下三类工具，分别对应6.2.2规定的智能体身份管理、智能体目录管理、智能体标识管理功能。

- a) 智能体身份注册 (agent_identity_register)

向重要功能设施注册智能体身份。智能体首次接入数据基础设施时调用此工具，获取全局唯一的智能体身份标识及数字身份凭证。

表 A.2-1 agent_identity_register 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
智能体名称	agent_name	string	是	智能体的注册名称，宜具有业务可辨识性
提供方标识	provider	string	是	智能体提供方的主体标识，如组织机构代码
功能描述	description	string	否	智能体功能与能力的简要描述
公钥	public_key	string	是	智能体的公钥，用于后续签发和验证数字身份凭证
返回值：智能体标识	agent_id	string	—	全局唯一的智能体身份标识
返回值：凭证	credential	string	—	由重要功能设施签发的智能体数字身份凭证

b) 智能体目录查询（agent_directory_query）

查询重要功能设施管理的智能体目录，获取已注册智能体的基本信息列表。

表 A.2-2 agent_directory_query 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
查询类型	query_type	string	是	查询方式，可选值：agent_id（按标识查询）、provider（按提供方查询）、capability（按能力查询）
查询关键字	query_value	string	是	与查询类型匹配的检索关键字
每页记录数	page_size	integer	否	每页返回记录数，默认 20
页码	page_number	integer	否	分页页码，默认 1
返回值：智能体列表	agents	array	—	符合条件的智能体信息列表，每项包含 agent_id、agent_name、provider 等字段
返回值：记录总数	total	integer	—	满足查询条件的总记录数

c) 智能体标识解析（agent_identifier_resolve）

解析智能体标识，获取智能体的访问地址及元信息，支持智能体间的寻址与路由。

表 A.2-3 agent_identifier_resolve 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
智能体标识	agent_id	string	是	待解析的智能体全局标识
返回值：智能体标识	agent_id	string	—	解析的智能体标识（原值返回）
返回值：访问地址	access_endpoint	string	—	智能体的网络访问地址（URL 或 IP:Port 格式）
返回值：元信息	metadata	object	—	智能体元信息，含 agent_name、provider、capabilities 等

A.3.2.2 业务节点 MCP Tools

业务节点MCP Server提供以下六类工具。其中智能体身份、智能体目录、智能体标识三类工具的接口定义与A.4.2基本一致，此处仅列出与重要功能设施版本的主要差异；资源检索、资源寻址、编排调度为业务节点的专有工具，完整列出。

a) 智能体身份注册（agent_identity_register）

与表A.2-1一致，不同之处在于工具注册到业务节点MCP Server，且工具描述中服务对象为"本业务节点"。

b) 智能体目录查询（agent_directory_query）

与表A.2-2一致，查询范围为业务节点管辖域内的智能体目录。参数定义同表A.2-2。

c) 智能体标识解析（agent_identifier_resolve）

与表A.2-3一致，解析范围为业务节点管辖域内的智能体标识。参数定义同表A.2-3。

d) 资源检索（resource_search）

在业务节点管理的资源目录中检索数据资源，支持关键词检索和按资源类型、数据格式等多维过滤。

表 A.3-4 resource_search 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
检索关键词	query	string	是	资源检索关键词，支持自然语言描述。关键字为空串时，则返回整个列表。
资源类型	resource_type	string	否	资源类型过滤，如 dataset、api、model、report 等
附加过滤条件	filters	object	否	扩展过滤条件，键值对格式，如 {"data_format":"csv","update_time":"2026-01"}
每页记录数	page_size	integer	否	每页返回记录数，默认 20
页码	page_number	integer	否	分页页码，默认 1
返回值：资源列表	resources	array	—	符合条件的资源信息列表，每项含 resource_id、resource_name、resource_type 等
返回值：记录总数	total	integer	—	满足检索条件的总记录数

e) 资源寻址（resource_locate）

根据资源标识定位资源的物理存储地址，返回一个或多个可用的访问端点。

表 A.3-5 resource_locate 工具参数

参数名称	英文变量名	参数类型	是否必须	描述
资源标识	resource_id	string	是	待寻址的数据资源全局标识
返回值：资源标识	resource_id	string	—	寻址的资源标识（原值返回）
返回值：访问端点列表	storage_endpoints	array	—	资源的物理访问端点列表，每项含 endpoint_url、protocol、region 等字段

A.3.2.3 接入连接器接口要求

接入连接器作为MCP Server应提供本地接入数据资源及产品的访问工具，对应7.4规定的资源访问（访问本地接入数据资源及产品）。其接口应满足如下要求：

参数名称	英文变量名	参数类型	是否必须	描述
资源标识	resource_id	string	是	待寻址的数据资源全局标识
返回值：资源标识	resource_id	string	—	访问的资源标识（原值返回）
返回值：资源内容	resource_content	object	—	访问的资源内容

参 考 文 献

- [1] GB/T XXXXX-XXXX 数据基础设施 参考架构
 - [2] GB/T XXXXX-XXXX 数据基础设施 互联互通基本要求
 - [3] GB/T XXXXX-XXXX 数据基础设施 用户身份管理和接入规范
 - [4] GB/T XXXXX-XXXX 数据基础设施 标识要求
 - [5] GB/T XXXXX-XXXX 数据基础设施 连接器技术要求
 - [6] GB/T XXXXX-XXXX 数据基础设施 数据目录描述要求
 - [7] OpenAI. Chat Completions API. <https://platform.openai.com/docs/api-reference/chat/create>.
 - [8] Anthropic. Model Context Protocol Specification. <https://spec.modelcontextprotocol.io/>.
-