



中华人民共和国国家标准化指导性技术文件

GB/Z 185.3—2026

人工智能 智能体互联 第 3 部分：身份管理

Artificial intelligence—Agent interconnection—Part 3: Identity management

2026-05-22 发布

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..... III

引言..... IV

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 智能体身份管理框架..... 2

6 身份注册及核验..... 3

7 身份账户管理..... 4

8 凭证管理..... 5

9 身份鉴别..... 6

附录 A（资料性） 智能体身份注册及核验的实现示例..... 8

附录 B（资料性） 智能体身份核验证明材料示例..... 10

附录 C（资料性） 智能体身份鉴别的实现示例..... 11

参考文献..... 13

前 言

本文件为规范类指导性技术文件。

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。

本文件是 GB/Z 185《人工智能 智能体互联》的第 3 部分。GB/Z 185 已经发布了以下部分：

- 第 1 部分：总体架构；
- 第 2 部分：身份码；
- 第 3 部分：身份管理；
- 第 4 部分：智能体描述；
- 第 5 部分：智能体发现；
- 第 6 部分：智能体交互；
- 第 7 部分：智能体工具调用。

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。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、蚂蚁科技集团股份有限公司、中移互联网有限公司、北京邮电大学、阿里云计算有限公司、华为技术有限公司、华北电力科学研究院有限责任公司、北京浩瀚深度信息技术股份有限公司、中金金融认证中心有限公司、中兴通讯股份有限公司、北京快手科技有限公司、江苏金服数字集团人工智能科技有限公司、浪潮通信信息系统有限公司、昆仑数智科技有限责任公司、浙江大华技术股份有限公司、北京兴云数科技术有限公司、亚信科技(中国)有限公司、中移九天人工智能科技(北京)有限公司、成都理工大学、北京火山引擎科技有限公司、中国移动通信集团有限公司、南京理工大学、青岛港国际股份有限公司、北京宝兰德软件股份有限公司、厦门市美亚柏科信息安全研究所有限公司、中移(杭州)信息技术有限公司、杭州高新区(滨江)区块链与数据安全研究院、中移雄安信息通信科技有限公司、中国移动通信集团广东有限公司、晨曦数智(北京)科技有限公司、浪潮通用软件有限公司、咪咕文化科技有限公司。

本文件主要起草人：张士宗、孙曦、鲍薇、刘军、高歌、庄仁峰、文军、徐浩、朱锦涛、张熙、闫冬、卢令令、庞韶敏、李闯、赵孝武、谷晨、管俊明、茹宏格、袁明明、尚云云、孔维生、李玉国、张联华、孙昊、程晗蕾、杜宁、刘伟东、戚湧、郭乙运、陆仲达、阙锦龙、谢小燕、魏遵博、杨佳丽、朱建、邵俊谦、丁一凡、刘卫文、陈波、马丽萌。

引 言

随着人工智能技术迅猛发展,智能体作为人工智能从概念转化为实际生产力的关键载体,在各领域应用日益广泛,对赋能新型工业化、塑造新质生产力作用显著。然而,当前智能体产业发展面临诸多挑战,不同智能体间存在互联互通互操作难题,在基于协议的智能体互联领域,国际上已有 MCP、A2A、ANP 等智能体通信协议,但并未形成行业完全共识的方案,亟需制定适合国内智能体产业发展的行业统一共识方案。

为系统化解决上述问题,引导和规范智能体互联技术发展,提升智能体系统的互操作性、可组合性与整体产业效能,特制定本指导性技术文件。GB/Z 185《人工智能 智能体互联》旨在规定智能体互联的技术要求和流程,其编制遵循系统性、先进性和可操作性原则,为智能体之间实现跨平台、跨架构的互联、互通、互操作提供统一的技术框架和标准依据,GB/Z 185 拟由七个部分构成。

- 第 1 部分:总体架构。目的在于给出智能体互联环境中的概念模型、功能模型。
- 第 2 部分:身份码。目的在于给出智能体身份码定义和应用,给出身份码代码结构和分配原则的建议。
- 第 3 部分:身份管理。目的在于给出智能体互联环境中的身份管理框架和全生命周期过程,描述身份管理的技术要求。
- 第 4 部分:智能体描述。目的在于给出智能体的描述方法,提供智能体描述注册、变更和发布的参考流程。
- 第 5 部分:智能体发现。目的在于给出智能体互联的发现流程。
- 第 6 部分:智能体交互。目的在于给出智能体海量互联时的交互模式,描述交互基础元素及接口定义。
- 第 7 部分:智能体工具调用。目的在于给出基于大模型的智能体调用工具的标准化架构、流程及工具描述,支持智能体与外部工具的无缝集成。

人工智能 智能体互联

第3部分：身份管理

1 范围

本文件规定了智能体在互联环境中的身份管理框架及要求,涵盖了智能体身份注册及核验、身份账户管理、凭证管理、身份鉴别等。

本文件适用于智能体身份管理功能/系统的开发、应用及测评。

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/Z 185.2—2026 人工智能 智能体互联 第2部分：身份码
GB/T 25069—2022 信息安全技术 术语
GB/T 41867—2022 信息技术 人工智能 术语
GB/T 45288.1—2025 人工智能 大模型 第1部分：通用要求

3 术语和定义

GB/T 45288.1—2025、GB/T 25069—2022 和 GB/T 41867—2022 界定的以及下列术语和定义适用于本文件。

3.1

智能体身份 agent identity

可验证的数字身份,用于标识一个智能体。

3.2

智能体委托方 agent delegator

授权智能体代表其执行任务的实体。

3.3

智能体身份依赖方 agent identity relying party

依赖对智能体进行身份鉴别的结果决定是否建立信任关系的实体。

3.4

智能体身份注册服务方 agent identity registration service provider

处理智能体身份注册请求、执行智能体身份核验并管理智能体身份账户的实体。

3.5

智能体凭证发行方 agent credential issuer

负责为智能体生成、发行并管理身份凭证的实体。

3.6

智能体身份验证方 agent identity verifier

能够对智能体身份合法性进行验证的实体。