

《智能体互联网治理 智能体交互技术要求》编制说明

（征求意见稿）

标准起草小组
2026年6月

1. 标准“范围”的内容

本文件规定了智能体交互的技术能力标准框架，确立主体均等、复合核验、按需开放、全程可溯四项基本原则，围绕交互信任、交互数据、交互安全三个维度，对身份可信、行为可信、模式可信、数据处理与技能封装及身份、权限、数据安全等要求作出统一规范。

本文件适用于智能体交互系统的设计、开发、部署、运维、安全评测全阶段，覆盖简单交互、跳转交互、A2A链式协同等全部交互场景，适用对象包括智能体开发者、协议设计者、服务提供商、平台运营方及行业应用单位，可作为产品研发、合规自查、安全检测与能力认证依据。

2. 工作简况，主要包括：任务来源、主要工作过程、各起草单位和起草人及其在起草标准过程中所承担的工作等情况、对标准草案进行会议讨论范围、征求意见的范围、审查的范围

2.1. 立项阶段

根据中国互联网协会团体标准管理相关规定，经立项评审，《智能体互联网治理 智能体交互技术要求》团体标准符合立项要求，现予以立项，项目计划号为XXX-T/ISC-XX。

2.2. 起草阶段

本标准任务下达后，中国信通院筹备成立标准起草组，为保证标准的内容符合国内行业发展的技术需求，客观地提出合理、适用的技术指标，编制前期起草组成员对提供智能体交互过程防护产品的云服务厂商和安全厂商，以及使用智能体交互过程防护产品的企业进行了相关调研。

标准在编制过程中起草组内部组织召开了多次的技术讨论会，在标准编写过程中征求国内厂家以及用户单位的意见，形成了征求意见稿。

2.3. 征求意见稿阶段

2026年6月26日在会议上进行第一次征求意见，会议进行了此次征求意见稿的讨论，会后根据专家意见建议进行了修改。

2.4. 送审阶段

XX

2.5. 报批阶段

XX

2.6. 起草单位和起草人

本文件起草单位：中国信息通信研究院、北京邮电大学、中国电信云网操作系统研发中心、中国联合网络通信有限公司网络运营事业部、中移九天人工智能科技（北京）有限公司、中电信人工智能科技（北京）有限公司、中移（苏州）软件技术有限公司、联通数据智能有限公司、天翼安全科技有限公司、中国移动通信集团甘肃有限公司、国网信息通信产业集团有限公司、华为技术有限公司、中兴通讯股份有限公司、用友网络科技股份有限公司、北京金山云网络技术有限公司、北京知道创宇信息技术股份有限公司、安徽星盾智能科技有限公司、深信服科技股份有限公司、网宿科技股份有限公司（洋哥确定）、三六零数字安全科技集团有限公司、云从科技集团股份有限公司、广东省城乡规划设计研究院科技集团股份有限公司、数字广东网络建设有限公司、天翼数字生活科技有限公司。

本文件主要起草人：郭雪、卫斌、马铭洋、景韩愈、李忠权、刘逸凡、孙琼、宋欣、曹斌、费宗灏、严仍义、刘志伟、鞠小龙、胡皓然、高宏民、孟繁宇、汪洋、宋志明、黄绍莽、郑琳、魏巍、李苗苗、贾琨、后润李、刘金朋、姜燕、崔浩、徐国胜、刘一赫、张永波、毛帅、黄爽、殷标、李艳杰、康和、王长金、孟伟、罗启汉、康涛、孔令昊、王萃娟、田翠翠、王振兴、安东冉、杨雄、王振强、高明、程盛琪、杨俊才、吕士表、胡钢伟、李东旭、汤磊、韩福海、廖瑞毅、邱柠、李祖金、贺学尧、陈鑫、丁嘉嘉。

3. 标准编制的意义；标准原则和确定标准主要内容（如技术指标、参数、公式、性能要求、试验方法、检验规则等）的依据（包括试验、统计数据）

标准编制的意义：适用于企业在构建智能体交互安全体系、制定身份认证策略、落地智能体访问调用能力时提供技术指导，同时适用于企业在评估智能体交互技术水平、建设全流程权限管控体系、落实安全合规自查与风险验证时参照使用。

标准制依据 GB/T 1.1-2020《标准化工作准则 第一部分：标准的结构和编写》的规则编制。

本标准通过规范智能体交互技术能力要求，为厂商研发相关产品、用户建设或完善智能体交互安全体系提供统一指引与技术参考。

4. 主要试验(或验证)的分析、综述报告

本标准起草过程中，对数十家云计算厂商、安全厂商、行业用户及科研机构开展调研，汇总梳理智能体交互技术现状、痛点及能力短板；通过分析智能体交互安全事件与身份权限风险案例，提炼关键安全问题，形成相应技术能力要求与规范。

针对十家典型厂商的智能体应用平台的身份认证、交互调用相关服务，通过实测数据与应用反馈优化指标体系，完善技术要求、测试方法和评价准则，最终形成本标准。

5. 标准在起草过程中遇到的问题及解决办法；重大分歧意见的处理经过和依据；有无重要技术问题需要说明

在本标准的修订过程中，无重大分歧意见和技术问题。

6. 与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异

该项目没有完全对应的国际标准或国外先进标准。

7. 修订标准时，说明与标准前一版本的重大技术变化，并列出新、旧版本的有关条款(可引用标准前言的内容)；废止/代替现行有关标准的建议

本标准制定标准，非修订标准。

8. 说明标准与其他标准或文件的关系(可引用标准前言的内容)，特别是与有关的现行法律、法规和强制性国家标准的关系

本标准非系列标准。

9. 标准作为强制性标准或推荐性标准的建议

建议本标准作为推荐性团体标准。

10. 贯彻国家标准的要求和措施建议(包括组织措施、技术措施、过渡办法等内容)；标准发布后，对国内外业界可能产生的影响

建议本标准作为协会标准发布实施，为智能体交互安全防护产品设计者在设计和开发阶段、使用智能体交互安全防护产品的用户在选择和采购阶段以及第三方评估机构对智能体交互安全能力评估阶段提供依据。

11. 标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程

本标准未涉及。

12. 其他应予说明的事项

本标准未涉及。