智能体交互身份与访问控制安全能力要求

编制说明
（征求意见稿）

标准起草小组
2026年4月

1. 标准“范围”的内容

本文件针对智能体参与的各类交互场景，明确了智能体自身、操作用户以及服务被调用方等多方主体的身份认证机制与访问控制规则，规范了身份核验、权限分配、操作鉴权、行为审计等安全技术与管理要求，保障交互过程中身份可信、权限可控、操作可追溯。

本文件适用于智能体全生命周期过程中的身份安全与权限管理工作，覆盖智能体的设计研发、集成部署、上线运行及运维优化等阶段，可为相关产品研发、系统建设、安全测评与监管管理提供技术依据和实施指引。

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，《智能体交互身份与访问控制安全能力要求》3项团体标准符合立项要求，现予以立项，项目计划号为164-T/ISC-26。

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

xx

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、北京金山云网络技术有限公司、天翼安全科技有限公司。

本文件主要起草人：郭雪、卫斌、马铭洋、李忠权、景韩愈。

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、部署访问控制能力时提供技术指导，同时适用于企业在评估智能体身份安全水平、建设全流程权限管控体系、开展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场景下身份认证与访问控制安全能力要求，为厂商研发相关安全产品、用户建设或完善智能体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身份认证与访问控制安全现状、技术痛点及能力短板；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，形成相应安全能力要求与技术规范。

针对十家典型厂商的智能体应用平台的身份认证、访问控制相关服务，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，并列出所涉及的新、旧版本的有关章条(可引用标准前言的内容)；废止/代替现行有关标准的建议

本标准为制定标准，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行业标准。

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。