ICS 35.xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

智能体互联网治理 智能体交互技术要求

Intelligent Agent Internet Governance: Technical Requirements of Agent Interaction

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中 国 互 联 网 协 会　　发布

目　　次

前　言

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。

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。

本文件由中国互联网协会提出并归口。

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。

引　言

随着“人工智能+”行动深度落地，智能体技术从单一人机对话转向多智能体协同执行复杂任务，智能体对智能体交互成为端云协同、跨平台服务的核心形态，广泛应用于金融、医疗、智能交通、工业控制、办公协作等领域。

当前国内智能体交互生态存在显著短板：一是交互协议、消息格式、技能规范碎片化，不同厂商智能体无法高效互通，形成技术孤岛；二是交互信任体系缺失，身份伪造、恶意协作、行为不可控等问题频发；三是跨域数据流转缺乏统一管控规则，数据泄露、违规处理风险突出；四是交互权责模糊，异常行为难以追溯，制约智能体产业规模化、规范化发展。

为统一智能体交互技术能力底线，规范智能体对智能体全流程交互行为，防范各类安全风险，本标准立足国内产业现状与监管要求，以主体均等、复合核验、按需开放、全程可溯四大原则为核心，构建“交互信任、交互数据、交互安全”三位一体技术框架，明确智能体交互各环节技术要求、实施规范与评估标准。

本标准旨在为智能体开发者、协议设计者、服务提供商、平台运营方提供可落地的技术指引，打通跨厂商、跨平台智能体协同壁垒，建立动态可信的交互体系，保障数据安全流转与交互行为合规，推动智能体互联网治理体系完善，助力人工智能产业健康有序发展。

智能体互联网治理 智能体交互技术要求

1 范围

本文件规定了智能体交互的技术能力标准框架，包含了智能体交互必须遵循的核心原则、交互信任要求、交互数据规范、以及身份、权限、数据等维度的基础安全技术要求。

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链式协同等所有交互场景。适用对象包括智能体应用开发者、交互协议设计者、智能体服务提供商、平台运营方，以及金融、医疗、交通、工业、电商等行业应用单位。

本文件可作为智能体交互产品研发、合规自查、第三方安全检测、能力认证的技术依据。

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 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 32400-2015 信息技术 云计算 概览与词汇

GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法

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）

具备感知环境、处理信息、执行任务和自主决策能力的软件系统，能够模拟人类智能完成特定或复杂任务。智能体通常包括模型推理、知识管理、多模态交互等模块，支持连续学习与个性化服务。

3.2 智能体交互（Agent Interaction）

智能体与被调用方、用户之间为达到特定目的，协同作业而进行的访问和操作过程。

3.3 A2A 交互（Agent-to-Agent Interaction）

智能体对智能体交互，不同智能体基于统一协议开展通信、任务委托、协同执行的链式交互形态，包含客户端智能体与服务端智能体两类核心角色。

3.4 A2A 客户端（A2A Client/A）

发起交互请求、承接用户指令，向其他智能体提交任务的智能体，是交互流程的发起方。也称作智能体服务请求方，以下简称“客户端”或“服务请求方”。

3.5 A2A服务端（A2A Server）

接收外部智能体请求、执行业务任务并反馈结果的智能体，对外暴露标准化交互端点。也称作智能体服务提供方，以下简称“服务端”或“服务提供方”。

3.6 智能体名片（Agent Card）

存储智能体身份、技能、服务端点、认证规则等元数据的标准化JSON文档，用于智能体能力发现与身份声明。

3.7 智能体技能（Skills）

智能体具备的可对外提供的功能、服务与处理能力，是智能体交互的核心业务单元。

3.8 简单交互

单次请求-响应模式的智能体交互，无多级委托、无长周期任务，交互链路单一。

3.9 跳转交互

智能体根据任务需求，主动跳转至第三方智能体/服务完成阶段性工作的交互模式。

3.10信任等级

基于智能体历史交互行为、安全合规记录、能力可信度，动态划分的交互信任层级，用于差异化管控交互权限。

3.11智能体链（Agent Chain）

由多个智能体依次组成的A2A链式委托结构，其中前一个智能体的客户端本身也是A2A智能体，可将授权请求或任务进一步委托给其自身的客户端，形成任务或凭证沿链传递的协作链路。

注1：智能体交互场景包括智能体通过接口、操作系统权限、通信协议等方式代理用户访问 被调用方的数据、调用被调用方的功能等场景。

注2:被调用方包括APP、其他智能体等。

4 符号和缩略语

下列符号和缩略语适用于本文件。

API	应用程序编程接口（Application Programming Interface）
ID	身份标识号（Identity Identifier）
IP	互联网协议（Internet Protocol）
A2A	智能体到智能体（Agent-to-Agent）
SSE	服务器推送事件（Server-Sent Events）
Skill	智能体技能

5 智能体互联网治理 智能体交互技术要求标准框架

5.1 框架模型

本标准从交互信任、交互数据、交互安全三个维度出发，三者相互支撑、协同管控智能体全流程交互行为。

交互信任：聚焦身份、行为、交互模式的可信性，构建动态信任体系；

交互数据：规范数据流转、技能封装、数据处理的统一规则；

交互安全：覆盖身份、权限、数据三类安全能力，筑牢交互安全底线。

智能体交互全流程需同时满足三大维度技术要求，适配简单交互、跳转交互、A2A智能体链等所有场景。智能体交互身份与访问控制安全要求框架如图1所示。

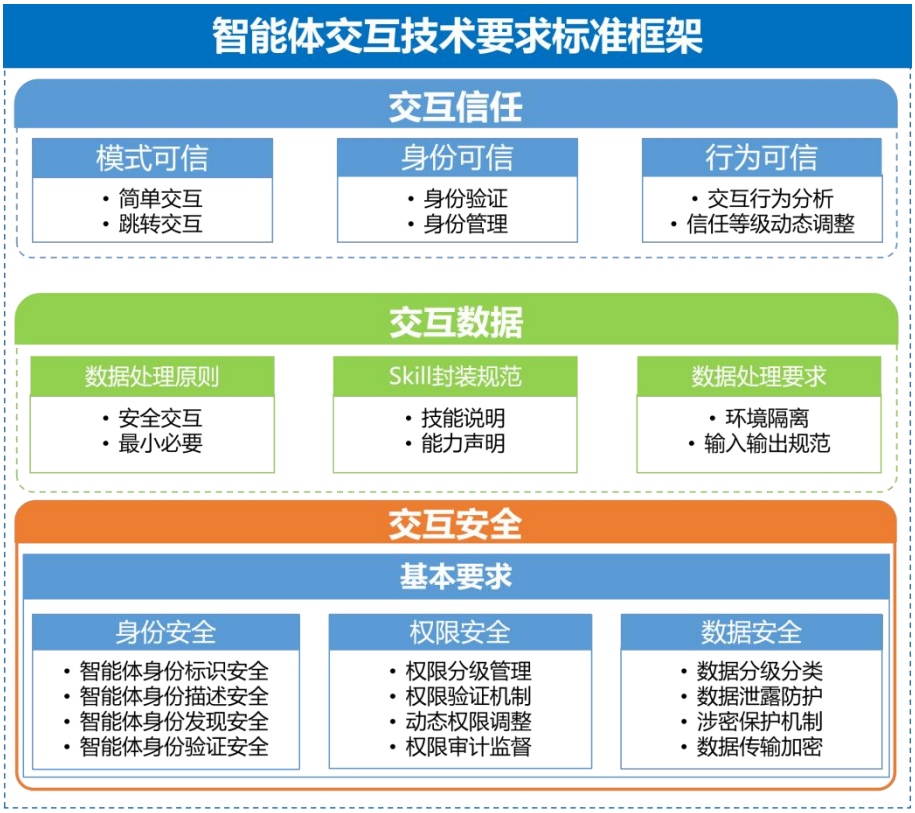

图 1 智能体交互技术能力标准框架

5.2 A2A 交互流程概述

客户端（智能体A）接到用户意图后进行初步分析，识别出涉及服务提供方（智能体B），将用户意图传递给服务提供方（智能体B）。智能体A和智能体B可根据需要提供直接跳转、简单交互等用户服务模式。跳转交互模式下，智能体A把用户原始意图传递给智能体B，用户将跳转到智能体B的服务界面，智能体B与用户直接交互直至完成用户意图，把意图结果直接反馈给用户；简单交互模式下，智能体B对接收到的用户简单意图进行处理，处理后将意图结果返回服务请求方（智能体A）并最终反馈给用户，用户也可以跳转到服务提供方（智能体B）中获取意图结果。交互流程如图2所示。

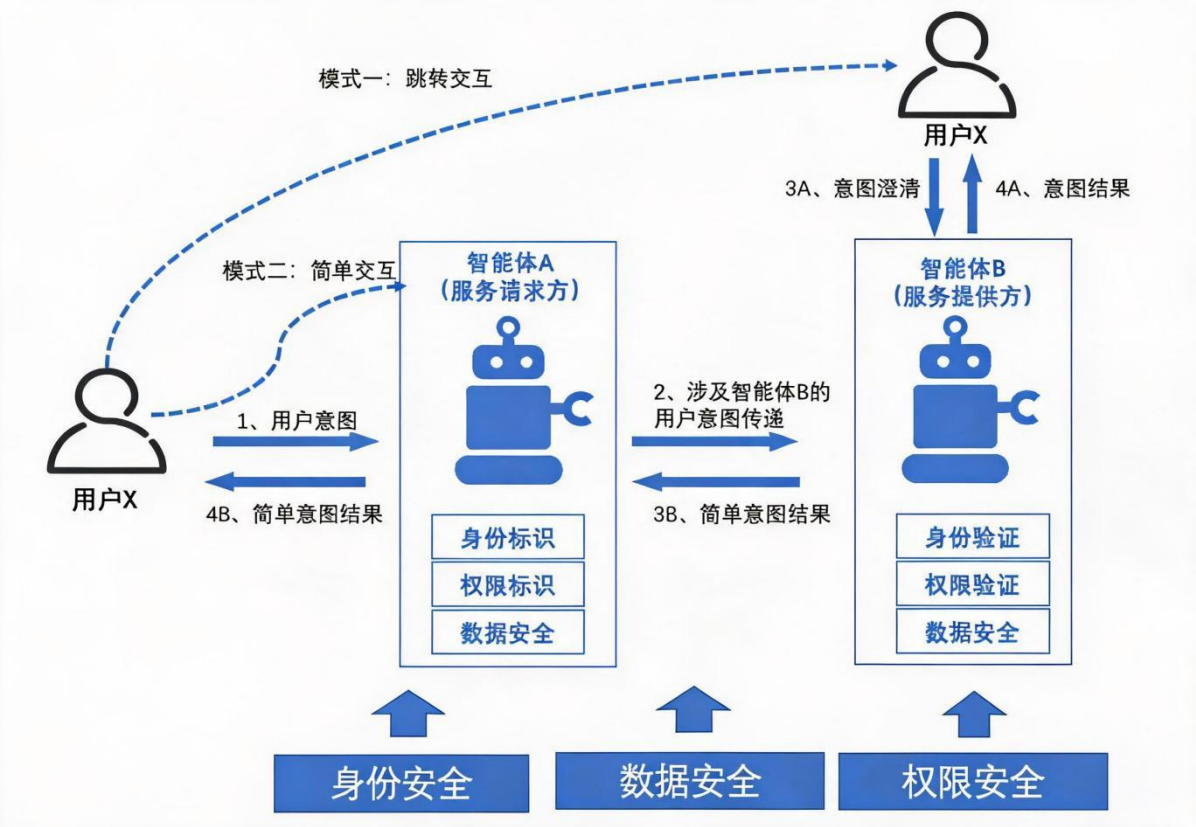

图 2　A2A 交互技术逻辑示意

5.3 基本要求

a）主体均等：所有参与交互的智能体、平台、用户等主体地位平等、权利与责任对等，统一交互规则，不设置差异化特权，明确各方责任归属，保障交互生态公平有序。

b）复合核验：针对身份变更、数据调取、跨端操控、权限修改、A2A 权限委托等高风险操作，执行多层级、多主体、多轮次校验，杜绝单一核验漏洞。

c）按需开放：严格恪守业务刚需边界，在权限分配、接口开放、数据共享、技能调用等环节，仅开放业务运行必需的能力与资源，遵循最小必要准则。

d）全程可溯：交互身份、操作行为、数据流转、权限变更全流程留痕，轨迹可追踪、日志可查询、责任可界定，支撑风险排查与合规审计。

e）客户端/服务请求方在访问服务端/服务提供方前，应当满足透明化要求，并以可识别、可验证的方式主动声明其作为智能体的身份，不得以伪装用户主体的方式实施访问；

f）客户端/服务请求方在访问服务端/服务提供方前，应获得服务提供方的授权，不得以绕开服务提供方授权和权限验证机制的方式实施访问；

g）客户端/服务请求方和服务端/服务提供方之间的交互数据应加强安全防护，保障数据传输过程中不被窃取、篡改。

6　交互信任技术要求

包括对智能体身份的认证、用户身份的认证以及被调用方身份的认证。

6.1 身份可信要求

6.1.1 身份管理

a）为每一个智能体分配全局唯一身份标识，标识与智能体名片、身份凭证强绑定；

b）身份信息、凭证采用加密存储，严禁明文留存，定期开展身份凭证有效性核查；

c）智能体注销、下线时，同步注销身份标识与关联凭证，阻断后续交互能力；

d）身份信息变更需留存操作日志，变更后同步更新全链路关联数据。

6.1.2 身份验证

a）所有参与 A2A 交互的智能体，必须基于标准化协议完成双向身份验证，禁止匿名交互、身份伪装；

b）智能体名片（Agent Card）需公开真实身份信息、认证方式，元数据不可篡改，更新后及时同步至交互网络；

c）A2A 智能体链场景下，链路内每一个节点智能体均需独立完成身份验证，不得继承上游身份豁免校验；

d）跨域交互场景应采用统一认证网关，实现身份一次校验、全域认可，避免重复认证智能体应和被调用方协商身份认证方式，如采用基于数字证书的身份凭证、API 密钥等认证方式；

6.2 行为可信要求

6.2.1 交互行为分析

a）建立智能体交互行为监测机制，实时识别异常行为，包括高频恶意请求、越权调用、违规数据抓取、循环委托等；

b）区分正常业务交互与异常攻击行为，针对违规行为触发告警、临时阻断等处置动作；

c）A2A 链式交互需逐跳分析行为合规性，任一节点行为异常则终止整条链路交互。

6.2.2 信任等级动态调整

a）基于历史合规记录、异常行为次数、安全评级，为智能体划分多级信任等级；

b）信任等级与交互权限、核验强度挂钩：高信任等级智能体可适度简化常规核验，低信任等级智能体执行强化复合核验；

c）智能体出现违规行为时，自动下调信任等级；连续合规交互可逐步提升信任等级，等级调整全程留痕；

d）信任等级评估周期按照评估协议执行，评估结果对外可查询（脱敏展示）。

6.3 模式可信要求

6.3.1 简单交互

a）遵循“请求-响应”标准化流程，消息格式统一适配 JSON 等通用格式，兼容 HTTP 基础协议；

b）单次交互任务边界清晰，禁止在简单交互中附加多级任务委托、跨域数据批量传输等高风险行为；

c）交互超时机制生效，超时未响应则自动终止任务，释放资源并记录日志。

6.3.2 跳转交互

a）智能体发起跳转前，需向用户/上游主体明示跳转目标、跳转用途、数据流转范围，获取显

式授权；

b）跳转链路全程记录节点信息，禁止无溯源的隐蔽跳转；

c）跳转后权限遵循“权限不放大”原则，下游智能体权限不得超出上游授权范围；

d）跳转失败、目标服务异常时，及时向上游反馈状态，不得静默中断交互。

7 交互数据技术要求

7.1 数据处理通用原则

a）严格遵循按需开放、最小必要原则，仅采集、传输、处理完成任务必需的数据；

b）区分公开数据、一般敏感数据、高敏感数据，实行分级差异化处理规则；

c）跨智能体数据流转必须获得数据主体授权，禁止未经授权共享、转发用户隐私数据；

d）交互产生的临时数据、缓存数据，任务结束后自动清理，留存周期不超过 24 小时；

e）所有数据交互过程需加密传输，禁止明文传输敏感数据。

7.2 智能体 Skills 封装规范

7.2.1 技能说明

a）每一项 Skill 需编写标准化说明文档，明确技能名称、功能描述、适用场景、输入输出格式、依赖资源；

b）标注技能风险等级（低/中/高），高风险技能（如资金操作、隐私数据查询）需单独标识；

c）技能说明内容需通俗易懂，同时适配机器解析与人工查阅，禁止模糊描述功能边界；

d）Skills 版本迭代时，同步更新说明文档，旧版本技能标注淘汰时限。

7.2.2 能力声明

a）智能体对外声明的能力必须与实际 Skills 一一对应，禁止虚假声明、夸大能力；

b）能力声明嵌入智能体名片，对外公开可查询，作为交互双方能力匹配的依据；

c）能力变更、下线时，提前公示并同步更新声明信息，过渡期不超过 7 天；

d）A2A 交互中，调用方需校验目标智能体的能力声明，禁止调用未声明的隐藏技能。

7.3 数据处理专项要求

a）多模态数据（文本、音频、视频、文件）交互时，遵循对应格式规范，做好数据解析与校验，拦截恶意畸形数据；

b）涉密数据、个人敏感信息不得在 A2A 公网链路中传输，需采用专属加密通道；

c）数据聚合、二次加工需保留原始数据来源溯源信息，确保数据流转可追溯；

d）禁止利用智能体交互批量爬取、缓存第三方平台非公开数据。

8 交互安全技术要求

智能体在访问被调用方前，应向被调用方申请权限并获得被调用方的授权。只有通过授权的智能体，才允许访问被调用方。

8.1 交互安全基本要求

a）所有智能体交互必须同时完成身份认证与权限校验，双重校验通过后方可执行业务操作；

b）接口调用遵循安全规范，防范接口注入、越权调用、重放攻击等常见网络攻击；

c）A2A 智能体链实行“全链路权限校验”，任一节点权限失效则整条链路终止访问；

d）高风险交互操作（资金交易、医疗数据调取、账户修改）强制启用复合核验；

e）交互环境实现逻辑隔离，不同智能体、不同任务的运行环境相互隔离，防止横向渗透。

8.2 身份安全要求

8.2.1 身份标识安全

a）智能体、用户、被调用方身份标识均具备唯一性、不可篡改性，加密存储，脱敏展示；

b）A2A 交互链路中，每跳身份标识全程记录，用于审计追溯；

c）身份标识变更后，同步更新全链路绑定关系，避免标识失效导致交互异常。

8.2.2 身份描述与发现安全

a）智能体身份描述仅对外公开非敏感信息，隐私内容禁止对外披露；

b）智能体能力发现仅开放授权查询接口，禁止非法遍历、批量探测全网智能体信息；

c）限制身份发现的访问频率，防范爬虫、恶意探测行为。

8.2.3 身份验证安全

a）优先选用数字证书、动态令牌等强认证方式，高风险场景禁用简单密钥、明文传输等弱认证；

b）身份凭证设置有效期，临近有效期自动提醒更新，凭证失效立即终止交互；

c）认证失败仅返回统一提示，不泄露凭证错误、有效期过期等细节信息，防止信息泄露。

d）交互过程中，定期核验智能体、用户和被调方身份凭证信息。

8.3 权限安全要求

8.3.1 权限分级管理

a）结合技能风险、数据敏感度，将权限划分为一般权限、敏感权限、高危权限三个等级；

b）按照智能体信任等级、能力等级匹配对应权限，低能力、低信任智能体禁止分配高危权限；

c）A2A 权限传递遵循“受限传递”原则，下游权限不得大于上游授予范围，禁止权限逐级放大。

8.3.2 权限验证机制

a）每一次技能调用、数据访问均需实时验证权限，不依赖缓存权限；

b）权限变更、撤销后即时生效，全链路同步更新，杜绝延迟生效漏洞；

c）智能体链场景下，基于整条链路最小权限执行访问控制。

d）服务端为区分自然人用户访问或智能体访问，可按照自身安全管理要求设置合理、必要的核验措施。服务请求方在访问服务提供方时，应当遵循服务提供方的核验规则，不得通过模拟用户行为、伪造交互事件、自动生成用户响应或其他方式绕过核验措施；

e）客户端和服务端应当提供授权管理功能，用于用户开启、关闭客户端对服务端的访问能力；

f）交互过程中，主动定期进行权限认证检测，防止权限变更。

8.3.3 动态权限调整

a）根据交互行为、风险态势动态调整权限：异常行为自动收缩权限，长期合规可适度优化权

限范围；

b）临时任务授予临时权限，任务结束后自动回收，临时权限有效期最长不超过 24 小时。

8.3.4 权限审计监督

a）完整记录每一次权限调用、变更、撤销日志，日志留存时长不少于 90 天；

b）定期开展权限审计，清理冗余权限、僵尸权限；

c）发现超权限调用、未授权访问等行为，立即阻断并告警，留存审计证据。

8.4 数据安全要求

8.4.1 数据分级分类

参照国家数据安全相关规范，将交互数据划分为公开数据、一般数据、敏感数据、核心涉密数据，分类制定防护策略。

8.4.2 数据泄露防护

a）部署数据防泄露机制，拦截敏感数据违规外发、批量导出；

b）跨智能体数据共享前做脱敏处理，隐藏手机号、身份证、银行卡等个人敏感信息；

c）监测异常数据传输行为，对超大流量、高频敏感数据传输触发阻断与告警。

d）交互过程中，涉及个人信息的，应符合《个人信息保护法》的要求，并通过隐私政策、合同协议等方式明确责任划分。

e）涉及知识产权、商业秘密的，应通过合同协议、开发者协议等方式明确责任归属。

f）客户端与服务端均应形成 A2A 交互的审计日志，包括且不限于时间戳、客户端、服务端、被调用技能、操作结果等内容。

8.4.3 涉密保护机制

a）核心涉密数据禁止通过公网 A2A 链路传输，仅限内网专属通道交互；

b）涉密数据交互全程加密，操作人员、智能体身份严格管控；

c）涉密数据交互日志单独归档，提升日志访问权限等级。

8.4.4 数据传输加密

a）所有网络交互数据采用端到端加密，基于 HTTPS、加密 RPC 等安全协议传输；

b）密钥定期轮换，密钥存储于专用安全介质，禁止嵌入代码或明文配置；

c）断点续传、流式传输（SSE）场景下，保持加密状态不中断。

附 录 A

1. 常见交互场景安全示例

场景名称	交互示例	技术与安全管控要求	交互模式、是否允许外部智能体自动化操作
金融理财（资产查询）	用户发起资产查询指令，客户端理财智能体作为发起方，依次调用资产汇总智能体、账户明细智能体，逐级拉取账户余额、交易流水等信息，整合数据后向用户反馈结果。	1.全链路节点智能体逐一完成双向身份验证，不得豁免校验；2.遵循权限受限传递原则，下游智能体仅开放查询类最小权限；3.账户流水、资产数据作为敏感数据，全程加密传输并做脱敏展示；4.记录完整调用链路日志，日志留存不少于90天；5.限制接口访问频率，防范批量爬取账户数据。	A2A智能体链 经过完整身份认证与权限校验后允许
金融理财（资金交易）	用户通过理财分析智能体制定投资方案，由该智能体委托支付交易智能体完成转账、理财产品申购等资金操作。	1.启用复合核验机制，身份、权限、操作内容三重校验；2.高危资金权限单独划分等级，临时权限有效期不超过24小时；3.禁止权限在链路中放大，上游撤销授权后下游凭证级联失效；4.每笔交易强制留存全流程轨迹，异常交易实时告警并阻断；5.高风险操作禁止单纯依赖自动化，关键节点需人工确认。	A2A智能体链（高危场景） 严格限制，仅基础查询可自动化，资金交易类操作不允许全自动化
办公协同（日程&差旅联动）	日程管理智能体检测到用户已有外出日程，主动跳转至差旅预订智能体，自动匹配行程时间、出行地点，完成机票、酒店初步筛选并推送至用户确认。	1.跳转前明示跳转目标、数据流转范围，获取显式授权；2.双方智能体能力声明与实际Skill保持一致，禁止隐藏功能调用；3.仅同步日程时间、地点等必要公开数据，不流转用户隐私信息；4.任务结束后自动清理临时缓存数据，留存时长不超过24小时；5.基于信任等级动态调整核验强度，高信任智能体简化常规校验。	跳转交互+简单交互 经过身份与权限校验后允许
出行服务（综合出行预订）	综合出行智能体根据用户出行需求，依次调用火车票智能体、网约车智能体、酒店预订智能体，串联完成全流程出行服务；同时识别恶意刷票、高频重复请求等异常行为。	1.逐跳校验链路节点身份与权限，异常行为立即终止整条交互链路；2.对订票、下单接口设置访问频次上限，拦截恶意刷票、批量操作；3.用户手机号、证件信息等敏感数据脱敏传输，不对外原始展示；4.遵循按需开放原则，仅开放行程预订必需的功能权限；5.建立行为分析机制，多次违规下调智能体信任等级。	A2A智能体链+跳转交互 正常出行预订：校验通过后允许；恶意刷票、批量占位类操作：禁止

电子商务（客服&物流联动）	用户咨询订单物流状态，客服智能体跳转至物流查询智能体，获取物流轨迹、配送节点等信息并回复用户；若发起售后退款，则跳转至售后处理智能体。	1.普通查询场景执行基础身份与权限校验，售后退款启用二次核验；2.订单编号、收货信息等敏感数据加密传输，跨智能体流转必做脱敏；3.禁止智能体私自篡改订单状态、发起无授权退款操作；4.区分正常咨询与恶意售后申诉，高频异常请求触发访问限制。	跳转交互 物流信息查询：允许；售后退款、订单修改等高风险操作：不允许全自动化
医疗健康（报告解析&问诊辅助）	问诊辅助智能体接收用户咨询，委托检查报告解析智能体读取电子检查报告、解读指标，并将分析结果回传至问诊智能体，为用户提供健康参考。	1.全链路采用强身份认证，仅内网专属加密通道传输医疗涉密数据；2.医疗数据划为核心涉密数据，禁止在公网 A2A 链路中流转；3.严格执行最小权限原则，仅开放报告读取、指标解析权限；4.全程复合核验，所有操作轨迹单独归档，提升日志访问权限；5.智能体仅做辅助解读，诊断、诊疗建议等核心环节必须人工介入。	A2A 智能体链（高涉密场景） 仅基础报告查询允许有限自动化，诊疗、诊断类操作全面禁止自动化
工业运维（设备监测&故障处置）	设备监测智能体实时采集设备运行数据，发现异常后推送至故障分析智能体；若判定为轻微故障，再委托运维处置智能体执行基础参数调整。	1.交互环境物理+逻辑双重隔离，防止运维链路被横向渗透；2.设备操控权限划为高危权限，与智能体信任等级、能力等级强绑定；3.运行数据分级处理，核心设备参数禁止对外流转；4.设备启停、参数大幅修改等高危操作，强制人工确认，阻断纯自动化执行；5.故障处置全流程留痕，用于事后运维审计。	简单交互+A2A 智能体链 设备状态查询、数据监测：允许；设备操控、参数修改、停机启动：禁止全自动化

附 录 B

B.1 模式介绍

服务提供方将自身提供的各种能力封装成SDK，供服务请求方集成。

B.2 交互流程

1）服务请求方到服务提供方处申请“开发者权限”，获取“开发者身份标识”；

2）服务请求方在服务提供方处下载SDK，并在自身代码中集成SDK，完成SDK集成的测试、上线；

3）用户通过服务请求方发起对服务提供方的调用指令；

4）服务提供方识别用户指令涉及服务提供方后，把用户指令通过SDK传递给服务提供方；

5）服务提供方验证服务提供方的身份和权限，通过后完成用户意图的准确识别、决策和操作，并将结果通过SDK反馈给服务请求方；

6）服务请求方将收到的服务提供方结果数据返回给用户。

附录 C：网关交互模式

C.1 模式介绍

服务请求方对服务提供方的访问，所有请求都经过网关统一验证和处理。

C.2 交互流程

1）网关实现对服务申请方的请求接收、对服务申请方的身份认证和权限鉴权、用户意图的精准识别、对服务提供方的功能路由、对服务提供方返回数据的接收等功能；

2）服务提供方部署网关，将自身提供的各种功能封装在网关后端，并将网关地址提供给服务申请方；

3）服务请求方配置网关地址，测试网关的连通性；

4）用户通过服务请求方发起对服务提供方的调用指令；

5）服务提供方识别用户指令涉及服务提供方后，把用户指令通过网关传递给服务提供方；

6）网关验证服务申请方的身份和权限，通过后完成用户意图的准确识别、决策，调用服务提供方具体的功能，并将结果通过网关反馈给服务请求方。