

W3C AI Agent Protocol CG 项目组进展

W3C AI Agent Protocol CG Project Progress

构建开放、互操作的AI智能体网络

Building an Open, Interoperable AI Agent Network

社区组的工作范围

Scope of Work of the Community Group

智能体间通信协议： 允许智能体相互发现、交换意图和能力信息、协商角色，并动态建立或解除协作。

Inter-agent Communication Protocol: Allows agents to discover each other, exchange intent and capability information, negotiate roles, and dynamically establish or dissolve collaborations.

智能体身份/授权模型： 基于开放标准的AI智能体身份框架，支持跨域智能体间的安全、可互操作的身份验证，以及授权。

Agent Identity/Authorization Model: An open standards-based AI agent identity framework that supports secure, interoperable authentication and authorization between cross-domain agents.

标准化元数据格式： 智能体能力、接口、目标和状态的结构化描述，实现智能体行为的自动化推理和编排。

Standardized Metadata Format: Structured descriptions of agent capabilities, interfaces, goals, and states, enabling automated reasoning and orchestration of agent behaviors.



社区组白皮书

Community Group Whitepaper

从语义网到智能体网络： 随着LLM等现代AI技术的发展，智能体现在能够自主执行任务、进行复杂推理和解决多步骤问题。

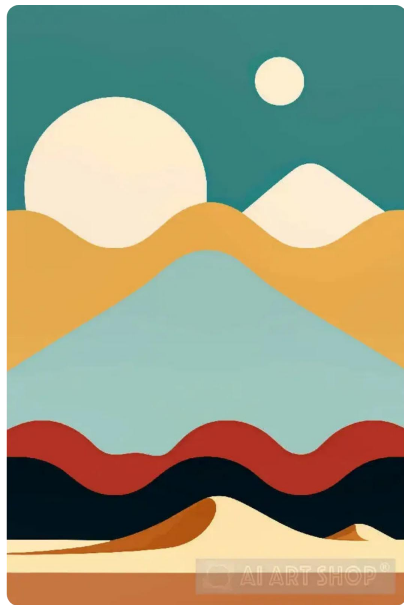
From Semantic Web to Agent Network: With the development of modern AI technologies such as LLMs, agents can now autonomously execute tasks, perform complex reasoning, and solve multi-step problems.

智能体网络四大趋势： 智能体取代传统软件成为互联网基础设施、智能体间普遍互联、基于协议的原生连接模式、智能体自主组织和协作。

Four Major Trends of Agent Network: Agents replacing traditional software as internet infrastructure, universal connectivity between agents, protocol-based native connection modes, and autonomous organization and collaboration among agents.

标准化协议的必要性： 打破数据孤岛、实现异构智能体协作、构建AI原生数据网络，最终实现开放高效的智能体网络。

Necessity of Standardized Protocols: Breaking data silos, enabling heterogeneous agent collaboration, building AI-native data networks, ultimately achieving an open and efficient agent network.



社区组的用例

Community Group Use Cases

个人智能体 (Personal Agent) : 直接服务于个人用户，代表用户利益，管理偏好、日程、通信和个人任务，同时保护用户隐私和控制权。

Personal Agent: Directly serves individual users, represents user interests, manages preferences, schedules, communications, and personal tasks, while protecting user privacy and control.

服务智能体 (Service Agent) : 向其他智能体提供服务，而非直接服务个人用户。提供专业能力，可通过标准化协议被个人智能体或其他服务智能体调用。

Service Agent: Provides services to other agents rather than directly to individual users. Offers specialized capabilities that can be invoked by personal agents or other service agents through standardized protocols.

搜索智能体 (Search Agent) : 促进智能体发现和连接。维护可用智能体及其能力的目录，使智能体能够相互查找和连接，形成动态智能体网络。

Search Agent: Facilitates agent discovery and connection. Maintains a directory of available agents and their capabilities, enabling agents to find



用例：酒店预订、即时通信

Use Cases: Hotel Booking, Instant Messaging

社区组协议文档

Community Group Protocol Document

智能体身份模块： 解决任意两个智能体之间的互连和互操作性挑战，使它们能够相互识别、建立信任和传输身份信息。

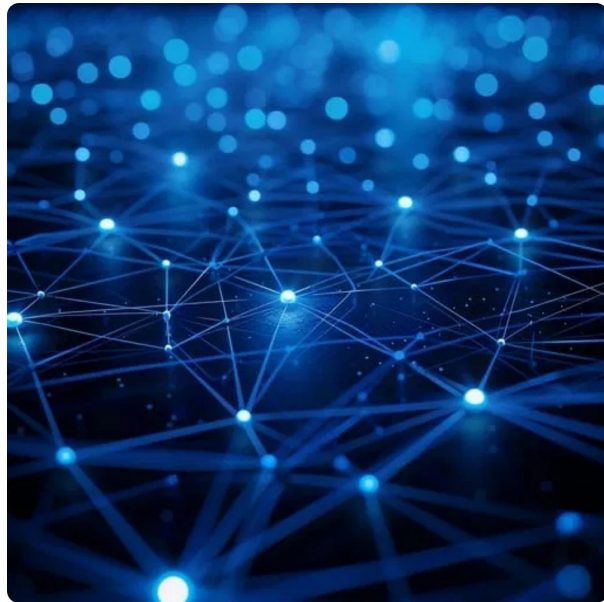
Agent Identity Module: *Addresses the interconnection and interoperability challenges between any two agents, enabling them to recognize each other, establish trust, and transmit identity information.*

去中心化标识符 (DID)： 为智能体提供基于标准的、可验证的身份原语，以便在异构生态系统中相互识别、认证和授权。

Decentralized Identifiers (DID): *Provides agents with standards-based, verifiable identity primitives for mutual recognition, authentication, and authorization in heterogeneous ecosystems.*

基于Web的DID方法 (did:wba)： 具有高安全性、操作简单性和利用现有Web基础设施的优势，支持跨平台身份验证。

Web-based DID Method (did:wba): *Features high security, operational simplicity, and leverages existing web infrastructure, supporting cross-platform identity verification.*



协议信息交互模型： 基于Linked-data模型，设计智能体之间的信息交互模型，基于现有的web，构建便于AI访问的数据网络。

Protocol Information Interaction Model: *Based on the Linked Data model, it designs an information exchange model between agents and builds a data network on the existing Web that facilitates AI access.*

社区组未来规划

Community Group Future Plans

完善核心协议： 与社区成员共同完成协议的所有未完成部分，包括智能体身份认证/授权机制、智能体描述模型和智能体发现机制。

Improving Core Protocols: Working with community members to complete all unfinished parts of the protocol, including agent authentication / Authorization , mechanisms agent description models, and agent discovery mechanisms.

增强互操作性： 增强智能体数据交换格式，确保语义一致性和结构标准化，开发更完善的智能体能力调用机制。

Enhancing Interoperability: Enhancing agent data exchange formats, ensuring semantic consistency and structural standardization, and developing more comprehensive agent capability invocation mechanisms.

推动标准化进程： 加强协议的安全性、隐私保护、可扩展性和灵活性，推动更多组织和开发者参与W3C标准化进程。

Promoting Standardization Process: Strengthening protocol security, privacy protection, scalability, and flexibility, and encouraging more organizations and developers to participate in the W3C standardization process.

