Network Working Group
Internet-Draft
Intended status: Informational
Expires: 2 January 2026

K. Yao
P. Liu
China Mobile

1 July 2025

Digital Identity Management for AI Agent Communication Protocols
draft-yl-agent-id-requirements-00

Abstract

AI agents are rapidly and massively transitioning from cutting-edge technology into real life. The AI agent communication protocol will establishing a critical means to connect agents with different users, tools, and other agents. Among all the features of AI agent communication protocol, digital identity is one of the most important components. Developing a cross-industry, universal, flexible, interoperable, and secure AI agent digital identity protocol is the foundation for achieving communication between agents and other entities in future network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 January 2026.

Copyright Notice

Table of Contents

1. Introduction

In recent years, large model-based generative AI is rapidly advancing, paving the way for the arrival of AGI. Technically, the large model has evolved from the single-modal LLMs like ChatGPT to multi-modal Vision-Language Models (VLMs) such as DALL-E, SORA, and GPT-4o. It now evolves to the Vision-Language-Action (VLA) models for robot control, like Google's RT-2 and RT-H.

A large number of new intelligent terminals emerge, and embodied AI is poised to become the most valuable application of AI. A plethora of traditional terminals are being upgraded to AI ones through embedded large models and AI agents, for example, AI phones, AI

wearables, and AI PCs. In addition, embodied AI comes in. It refers to intelligent agents that can understand, reason, and interact with the physical world, such as intelligent robots, self-driving cars, and robot dogs. Humanoid robots are one of the core scenarios of embodied AI. According to the prediction of GGII, the global humanoid robot market is projected to grow from USD 1.017 billion in 2024 to USD 15 billion in 2030, increasing at a compound annual growth rate (CAGR) of 56%. The global sales volume of humanoid robots will increase from 11,900 to 605,700.

Everyone may have a virtual intelligent assistant. AI agents understand user needs, schedule tasks, and invoke and combine massive applications autonomously. AI agents will revolutionize application-centric development mode and Graphic User Interface (GUI)-based human-machine interaction. This innovation leads to entries for super applications and super traffic. Many relavant use cases have been mentioned in [I-D.rosenberg-ai-protocols].

These AI agents are poised to be the "new citizens" of future network connections, heralding an economic boom and ushering human social life into a new era of collaboration between humans and AI agents, as well as among AI agents themselves.

2. Digital Identity Management Related Use Cases in the Context of AI Agent Communications

2.1. General

According to ITU-T [Digital-identity], the digital identity is defined as follows:

Digital Identity: The International Telecommunication Union (ITU) defines the concept of identity as a ‘representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context’. Building on this definition, we might state that a digital identity is the digital representation of an entity detailed enough to make the individual distinguishable within a digital context.

According to 3GPP [TR22.870], an AI agent is defined as follows:

Al Agent: an automated intelligent entity capable of e.g. interacting with its environment, acquiring contextual information, reasoning, self-learning, decision-making, executing tasks (autonomously or in collaboration with other Al Agents) to achieve a specific goal.

Thus the digital identity of an AI agent could be defined as “the digital representation of an AI agent detailed enough to make individual distinguishable within an AI agent communication context.” The digital identity contains mainly 3 parts: identifier, attribute and key credential.

2.2. Use Cases

According to 3GPP TR 22.870, there are some use cases discussing AI agent that communicate from/to terminal side with the support of digital identity.

AI agents communication: - As communication serves as a common mechanism for sharing information, there will be more and more users and their AI agents that need to be supported in a near future. A group could be established for users and their AI agents to communicate with each other. To complete a complex task involving multiple users and triggered by a user, AI agent or application, communication domain for multiple groups could be established, the users and AI agents working for the same task can be explicitly identified by the task request or implicit identified based on location area or relative distance. Communication domain could be dynamically created for users and AI agents from multiple groups to communicate with each other for a specific task during a specific time. Only the AI agents in the same domain can communicate with each other. If authenticated / authorized, users and AI agents could join this group via various access technologies, including the cellular network, Wi-Fi and Ethernet, etc.

Intelligent Communication Assistants: - Overall, intelligent communication assistant provided by the operators natively is a customized service. It can interact with end users through voice, text, gesture or other modalities to provide enhanced experience. The assistant can be customized for each particular user by accessing user data stored in the network. With user’s consent, it can provide various communication services and support individual users based on user’s intention and requirement. The provided services include intent-based search, personalized recommendations, voice-controlled smart home devices, and interaction with various services (including 3rd party AI assistant or capabilities) or devices. The customization can be achieved by providing different levels of the intelligent communication assistant service, based on the authorization from the user for user data.

3. Potential Digital Identity Management Requirements for AI Agent Communication

3.1. General

Digital Identity in the context of AI agent communication involves several common requirements to ensure effective, efficient, and secure interactions. Here is a list of potential key requirements derived from the illustrative use cases provided in the previous sections. They are not yet formally approved by 3GPP and only provided for information/discussion.

3.2. Identifier

3.2.1. Global Unique Identifier

AI agents SHOULD have a global unique identifier in an universal interoperable format to ensure the identifier can be used to dynamically identify and locate the AI agent.

3.2.2. User Binding

AI agents are designed to provide services for the human user, sometimes on behalf of the user. The digital identity of an AI agent MUST support the description of its associated user, so that the AI agent communication protocol can further support user authorization when needed.

3.3. Attribute

3.3.1. Skill

AI Agents can support multiple skills, and these skills may not be provided by a single manufacturer or provider. Considering that skill is the nature of AI agent communication and one of the most important properties of an AI agent. The definition of skills with different origins for an AI agent SHOULD be supported.

3.3.2. Capability

AI agent are able to communicate with other agents through multi-modal capabilities, e.g. text, image, voice, video, real-time communication. These capabilities are pre-requisites for the communication channel establishment. The definition of these multi-modal capabilities SHOULD be supported.

3.3.3. Service

AI Agent SHOULD be able to obtain long-term or short-term service verifiable credentials from different service providers, these credentials can be used for access control purposes. The AI agent identity SHOULD support the definition of dynamic service attributes.

3.3.4. Key Credential

AI Agent SHOULD be able to support transmit, share, store its digital identity in a secure way. Usually the public key credential is used to ensure the integrity of digital identity. Also the key credential can be used by the target entity of the AI agent to verify its identity information. The AI agent identity SHOULD support the usage of key credential.

3.4. Security

3.4.1. Authentication

In addition to traditional user authentication, the authentication of the agent should also be considered in AI agent identity management. More AI agent authentication related considerations have been mentioned in [I-D.yao-agent-auth-considerations]. The digital identity SHOULD contain at least one corresponding credential for the unique identifier for the identification.

3.4.2. Authorization

According to different scenarios, there will be three different authorization requirements, the digital identity of AI agent SHOULD support these authorization requirements.

* Agent Authorization:

The agent authorization is the common authorization that agent A provides authorized information from its own digital identity needed by agent B, and then agent B verifies and authorize the request. This is REQUIRED when an agent is on-behalf-of(OBO) itself or other agents.

* Delegation Authorization:

The agent authorization is the common authorization that Agent A provides authorized information from its user’ s and own digital identity needed by Agent B, and then Agent B verifies and authorize the request. This is REQUIRED when an agent is OBO its user, itself, or other agents.

* User Authorization:

The agent authorization is the common authorization that agent A provides authorized information from its user’ s and own digital identity needed by agent B, and then agent B still thinks that it’ s not sufficient, then agent B require agent A to help get a direct authorized information from the user to avoid risk. This is REQUIRED when an agent is OBO its user.

3.5. Discovery

3.5.1. Intra-domain

* Registration: In order for a successful discovery, the AI agent SHOULD be able to register its digital identity in an intra-domain repository. So that the AI agent can be discovered by the intra-domain entities (e.g. user/other agents).

3.5.2. Inter-domain

* Discovery mechanism: AI agent should be able to find needed resource (user/tool/agent) dynamically through discovery mechanism depending on identifier or attribute, from intra-/inter-domain repositories to meet its task requirements. The digital identity of AI agent should be the bearer of discovery information.

* Repository Update and Synchronization: In order for a successful discovery, different AI agent repositories SHOULD be able to update the digital identity information of AI agents that can be discovered.

4. Security Considerations

As discussed in previous sections, security plays a key roles in the definition of digital identity of AI agent. A comprehensive consideration of the potential impact of the various specific technologies that may be involved on the overall AI agent communication protocol is required.

5. Conclusions

AI agent communication requires the participation of partners from the industry, academia, and research sectors, including terminal vendors, network service providers, cloud service suppliers, AI base model providers, and application developers. Through technical workshops, project collaboration, and innovation pilots, all parties should join efforts to make AI agent communication an essential part of AI agent economic growth in the future. Furthermore, the industry

should advance the standardization progressively to formulate globally unified standards for the AI agent communication and prosper the industry ecosystem.

In summary, while AI agents have impressive autonomy and intelligence, they are ultimately tools that serve the needs of individuals or organizations. Each AI agent possesses a unique digital identity bound to the user identity they serve on the network. After AI agents are authenticated and authorized, their autonomous communication activities can be supervised, controlled, and traced on the network by the user. Also, diverse AI agents possess varying levels of sensing, decision-making, and operational capabilities. Besides autonomy, these properties can be shared with other AI agents through discovery and orchestration, facilitating task collaboration and achieving the effect of collective intelligence.

Standard solutions will be required to support the management of digital identity for AI agent communications. To ensure the global interoperability between heterogeneous AI agents, a standardized AI agent communication protocol including the digital identity management needs to be introduced for the session establishment and multi-modal data transmission. It is expected that IETF could be the place to develop such standard.

6. IANA Considerations

TBD.

7. Acknowledgements

8. Informative References

[Digital-identity]
ITU-T, "Digital Identity Roadmap Guide, D-STR-DIGITAL.01-2018-PDF-E.", n.d..

[I-D.rosenberg-ai-protocols]
Rosenberg, J. and C. F. Jennings, "Framework, Use Cases and Requirements for AI Agent Protocols", Work in Progress, Internet-Draft, draft-rosenberg-ai-protocols-00, 5 May 2025, <https://datatracker.ietf.org/doc/html/draft-rosenberg-ai-protocols-00>.

[I-D.yao-agent-auth-considerations]
Yao, K., "Further considerations on AI Agent Authentication and Authorization Based on OAuth 2.0 Extension", Work in Progress, Internet-Draft, draft-yao-

agent-auth-considerations-00, 30 June 2025, <https://datatracker.ietf.org/doc/html/draft-yao-agent-auth-considerations-00>.

[TR22.870] 3GPP, "Study on 6G Use Cases and Service Requirements", n.d..

Authors' Addresses

Kehan Yao
China Mobile
Email: yaokehan@chinamobile.com

Peng Liu
China Mobile
Email: liupengyjy@chinamobile.com