31 March 2026

To: AI-Identity@nist.gov

Re: NIST Call for Comments on Accelerating the Adoption of Software and AI Agent Identity and Authorization

oneM2M is pleased to respond to NIST's initiative on how standards and best practices for the use of AI Agents can deliver business value while mitigating risks. We are the global standards development organization (SDO) for the Internet of Things (IoT). Our global community develops IoT standards to enable interoperable, secure, and simple-to-deploy services for the IoT ecosystem. oneM2M's technical specifications are open, accessible, and internationally recognized.

Our response to NIST, as follows, focuses on the interplay between AI Agents and IoT:

- Industry rationale for focusing on IoT specifics.
- A common-framework approach for identity, authentication, authorization, and security
- Technical challenges specific to AI Agents for IoT,
- Data licensing implications for the standardization roadmap,
- oneM2M initiatives on technical standardization for AI Agents and IoT,
- Suggestions for collaboration between NIST, U.S. businesses, and oneM2M.

Industry Rationale for Focusing on IoT Specifics

Our comments focus on the use of AI Agents in IoT systems because they have distinct characteristics when compared to systems involving humans in the loop. In IoT systems, designers must work on the basis that many IoT devices and applications will exist in the background, as unattended applications. We cannot count on there being human users to "feed and water them." Many IoT devices are designed with limited power reserves and processing capacities. That involves designing security from the outset and automating many security, remote connectivity, and communications-management functions. Doing so requires a set of dependable and foundational capabilities to enable AI Agent and IoT operations, as we describe below.

AI Agents in a System-of-Systems

Based on practical experimentation, we treat AI Agents as one of several components in a system-of-systems architecture. That is because of the interaction that will arise between AI Agents and other components. The latter include IoT sensors, connected machinery, gateways, middleware, enterprise databases, dashboards, digital twins, decision-making applications, controllers.

Interactions also apply to other AI Agents, which might belong to a different operating environment, or which separate organizations might supply. Each of the AI Agent and IoT entities need to share a common approach for identification, authorization, and security functions to enable interoperability.

AI Agents to Modernize Standardization and Speed-up Product Development

Aside from technical interactions in operational deployments, there is another and quite distinct dimension to the use of AI Agents. This arises from the integration of AI Agents into product development and software implementation activities. In the standardization domain, we envisage AI Agents interacting directly with technical specifications documents. The intention is to speed up the process of transforming technical specifications into production systems. Furthermore, as AI Agents learn through operational experience, there is a direct feedback pathway to improve the quality of technical specifications and augment human experience.

Based on this vision, oneM2M is modernizing the standardization process. Our members publish technical information (coding rules, design guides, technical specifications) in machine-readable format. Our strategy is preparing the foundation for automation through AI Agents, scripts, and syntactic and semantic checking for quality assurance.

A Common Framework for Identity, Authentication, Authorization, and Security

AI Agents will interact with other system components such as IoT sensors, enterprise databases, IoT platforms, and application-logic entities. In this context, identity, authentication, authorization, and security become common functions that all components share. When a system operator registers an IoT sensor, creates an identity, and records its credentials, that same process should apply to all system entities, be they AI Agents or IoT components. Adhering to the same process and technical parameters, better known as standardization, enables plug-and-play interoperability and economy-of-scale benefits.

oneM2M's relevance to AI Agents and IoT is grounded in a horizontal architecture that connects a wide range of communications networks, hardware, and software entities interchangeably. All entities in this framework have access to a toolkit of common service functions (CSFs). Example CSFs include Registration, Discovery, Device Management, Application Management, and Security.

An IoT sensor and an AI Agent can both use a single Registration function to create an identity and entity-specific resource profile. That makes it straightforward for an AI Agent to use the Discovery function to find accessible resources or to alter access control privileges via the common Security function.

Technical Challenges Specific to AI Agents for IoT

oneM2M's experimentation with AI Agents for IoT systems identifies two challenges. One involves communication between AI Agents, via an orchestrator agent. What allows an IoT entity to discover an AI Agent, and how can AI Agents from different providers interact?

The second challenge applies to AI Agents interacting with non-AI entities. For example, one or more smart home components might connect to an AI agent to request environmental data from a

neighboring weather station. What added functionality and API access does the AI agent need to interact with the (non-AI) station and to do so in a secure manner?

At a granular level, two security building blocks are authentication and authorization functions. They help developers to implement entity-identification and access control policies to subsystems and to IoT data. Consider the case where a system manager wants to grant unrestricted access to privileged users, while applying narrower access rights for another set of users. When multiple agents want to access data, might there be a response protocol that sends policy permissions information back to an AI Agent or is there a need for an overlay protocol that adds conditions to Model Context Protocol (MCP) requests? We are addressing these issues by developing an authN/AuthZ solution for MCP that addresses the authentication chain from an IoT platform through an MCP server and all the way to the AI Agent.

Another topic for investigation applies to notifications functions. Their purpose is to improve system efficiency and resource management. For example, one IoT entity can subscribe to receive notifications when another IoT entity satisfies a threshold condition. A “temperature exceeds threshold X” would send a notification message to a monitoring application, saving it the effort on constantly polling the sensor. This helps to conserve energy and reduce traffic on communications networks. While there exist protocols for AI Agents to send information requests and receive replies, there is a need to standardize how AI Agents manage notifications.

The notifications concept leads to the topic of time series events and data. What happens when an agent requests the current humidity level as well as corresponding data from one month and one year ago? A response is possible if historical data is accessible. If this is not the case, and the AI Agent invents a response, what are the opportunities to standardize protective measures? This leads to the possibility of attaching contextual and provenance indicators, potentially through data licensing mechanisms.

Data Licensing Implications for the Standardization Roadmap

A longer-term topic related to AI Agents deals with the issue of data licensing. Existing practices for training AI systems rely primarily on human generated data. The expected growth of IoT sensors and connected devices will make more data available, in time-series sequences, and with distinctive characteristics.

Our experience of multi-stakeholder IoT deployments covers, among others, agriculture, drone operations, intelligent transport, and smart city systems. These examples highlight the need for technical mechanisms to share data between distributed IoT entities, and across operational and organizational boundaries. This leads to the need to parametrize data sharing arrangements.

Existing oneM2M capabilities allow IoT system operators to designate access control policies for different entities and data consuming endpoints. We expect future enhancements to support data license credentials so that organizations can control and capture value from downstream uses of IoT data. These will enrich data provider identities and support data provenance reporting. Both will enhance system trustworthiness and AI-explainability.

oneM2M Initiative on Technical Standards for AI Agents and IoT

In preparation for new requirements and their impact on the standardization roadmap, oneM2M members launched a work item to study and specify technical specifications for IoT systems to interwork with the Model Context Protocol in a standardized way. The scope of this work item covers:

- basic data forwarding and API wrapping,
- semantic interworking,
- behavioral interworking,
- and aspects related to security, authentication, authorization, and licensing.

As is the case with 3GPP standardization for the mobile network industry, oneM2M follows a continuous standardization roadmap. Improvements appear through periodic Releases. oneM2M is currently at Release 4, with new capabilities for Agent AI and other topics in the pipeline for future Releases. This presents opportunity for industry and research organizations to partake in shaping technical standards.

Getting Involved in oneM2M for AI Agent and IoT Standardization

There are three avenues for industry participants to get involved in this initiative. The easiest way to take part is as an observer in oneM2M's Technical Plenaries (TPs). The University of British Columbia will host the next TP as an on-line event in the week of June 1-5, 2026.

A second avenue, for standardization bodies and industry alliances, is to set up a liaison relationship with oneM2M.

Finally, for more in-depth involvement, organizations can use their membership of national standardization bodies to participate in oneM2M activities. For this, many US-based companies take advantage of their membership of Telecommunications Industry Association and/or ETSI.

oneM2M wishes NIST every success in furthering its Software and AI Agent strategic plan and supporting initiatives. We look forward to further discussions and collaboration on NIST's future research, community building, and international outreach efforts.

On behalf of oneM2M

contact@onem2m.org