Dispatch
Internet-Draft
Intended status: Standards Track
Expires: 7 May 2026

C. Zheng
B. Liu
N. Geng
Q. Gao
X. Shang
Z. Li
Huawei Technologies
3 November 2025

Agent Identity Managenment
draft-zheng-dispatch-agent-identity-management-00

Abstract

This document specifies agent identity management in the Internet of Agents (IOA) system. It defines the descriptive requirements for agent identities, the agent registration process, the structure and assignment of agent identifiers, and the basic and extended identity management functions performed by the agent gateway based on the agent’s descriptive information.

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 7 May 2026.

Copyright Notice

Table of Contents

1. Introduction

As intelligent agents become increasingly prevalent in distributed and interoperable systems, robust identity management is essential to ensure secure, scalable, and policy-compliant operation. In the Internet of Agents (IOA) system, agents—ranging from simple automation scripts to high-intelligence autonomous entities—must be uniquely identified, authenticated, and governed throughout their lifecycle.

This document outlines the foundational framework for agent identity management in the IOA system. It specifies the required descriptive attributes of an agent, the registration process with the agent gateway, the format and semantics of agent identifiers, and the basic and extended management capabilities enabled by the agent' s identity metadata. While security mechanisms such as authentication protocols and cryptographic binding are acknowledged as critical, their detailed specification is considered out of scope for this document.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Overview of the Agent Identity Management

The agent identity management architecture in the IOA system comprises four core functional modules: Agent Description, Agent Identity Registration, Agent Identity Management, and Security Considerations. First, an agent’s identity information MUST be represented in a normalized form. The agent then registers this normalized identity description with an Agent Gateway. Upon successful authentication of the registering agent, the Agent Gateway assigns a unique Agent ID to the agent and, using the Agent ID as a key, enforces identity management policies based on the agent’s normalized identity description.

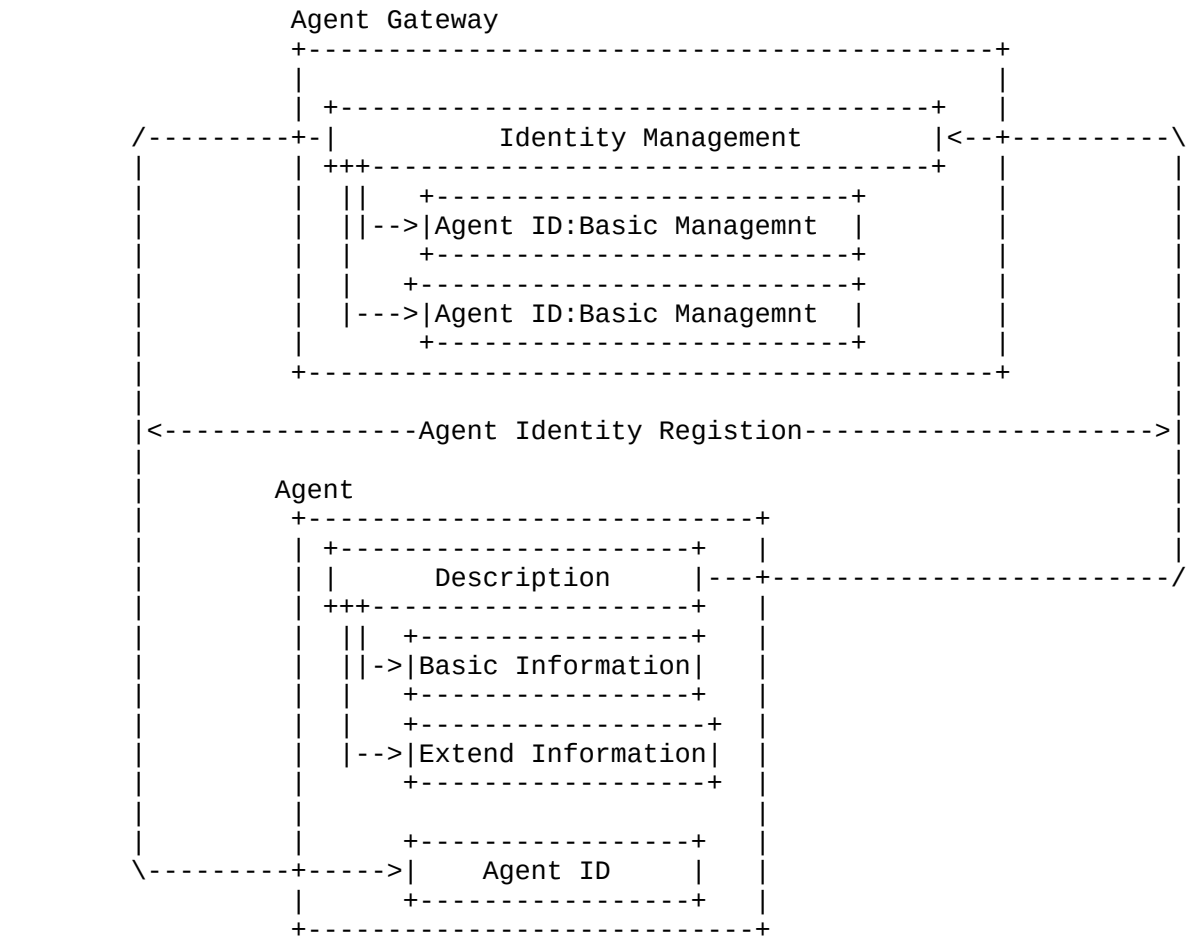

Figure 1: Agent identity management architecture

3. Agent description Requirements

To enable accurate agent identity management on the agent gateway, it is necessary to define a set of essential information elements for describing an agent.

3.1. Basic Information

The agent description MUST include the following base information elements:

* Agent name

* Agent capabilities/skills
* Agent author
* Agent version
* Agent creation time
* Agent description model version
* Agent location
* Agent communication protocol
* Agent description (human-readable)
* Agent signature

In addition, the following attributes MUST also be included as part of the base information:

* Agent validity period
* Agent form factor
* Agent intelligence level
* Agent extended profile URI
* Agent role
* Translation enablement indicator

Usecases

* Agent validity period: The validity period of an agent on the agent gateway specifies the time interval during which the agent is considered active and authorized for operation. The agent gateway MAY use this field to enforce publication and maintenance policies, automatically deactivating or removing expired or stale ("zombie") agents to reduce operational overhead and minimize the burden of agent lifecycle management.

* Agent form factor: The form of the agent, such as digital agent or embodied agent. The form field can support the interconnection of heterogeneous forms of agents in future IOA systems. For example, agent gateways may have different requirements for access authentication and policy control for agents of different forms. Communication protocols between agents of different forms may also differ.

* Agent intelligence level: The intelligence level of an agent can be defined using mainstream AI agent intelligence classification standards in the future. This will help application agents to select the final communication target among a group of candidate agents based on the required intelligence level. For example, when agents have the same capabilities, the one with a higher intelligence level can be chosen.

* Agent extended profile URI: The address accessible for the extended version of the agent. It helps to continuously and dynamically upgrade and update the agent during its online period on the extended version address.

* Agent role: The roles of agents include two types: consumer and producer. An agent can also assume both roles. This helps the agent gateway determine whether to establish a short connection or a long connection with the agent. It also assists the gateway in formulating control strategies when publishing agent information on the network, for example, by not publishing information for consumers who do not provide services.

* Translation enablement indicator: This field describes whether the agent message allows the gateway to perform message translation. It helps the agent gateway to translate heterogeneous protocol communications between agents while respecting the agent’s preferences. For example, in scenarios where semantic translation might occur, the agent can use this field to protect its data privacy.

3.2. Extended Information

The agent description SHOULD include the following extended information elements:

* Network requirements

* Trust level

* Extension

Usecases

* Network requirements: The requirements of agents for the network include three aspects: experience, monitoring, and security. These help the agent gateway implement on-demand QoS guarantee strategies (e.g., low latency assurance or high bandwidth assurance), security assurance strategies (e.g., path security, quantum encryption for communication), and agent task monitoring and maintenance strategies (e.g., agent task flow measurements at the stream level, packet level, segment level, and etc.).

* Trust level: The agent's permission scope defines the boundaries of its authorized operations and data access. This attribute enables the agent gateway to enforce fine-grained access control policies— for example, restricting agent data from leaving a specific administrative domain such as a campus or a country— thereby supporting regulatory compliance and data sovereignty requirements.

* Extension: An extensible information field is provided as a reserved mechanism to accommodate future dynamic attributes of the agent.

4. Agent Identity Registration

The agent MUST register its descriptive information with the agent gateway to enable the gateway to perform identity management based on this description. The specific registration interaction protocol between the agent and the gateway is outside the scope of this draft.

Upon receiving an agent's registration information, the agent gateway MUST first perform identity authentication. The specific authentication mechanism is outside the scope of this document. Following successful authentication, the gateway proceeds to the next step of agent identity management.

5. Agent Identity management

The agent gateway MUST first assign a unique identifier to the agent. Using this identifier as a key, the gateway can perform both basic and extended identity management functions by correlating it with the agent's descriptive information.

5.1. Agent Identifier

The agent identifier (agent ID) is used to uniquely represent an agent within the IOA system. Specific approaches for constructing this identifier MAY employ a hierarchical string scheme (e.g., incorporating domain, subdomain, and instance components) or alternatively use a standardized encoding of such a hierarchical string (e.g., via URI, UUID, or other IETF-recognized identifier formats) to ensure global uniqueness, interoperability, and ease of parsing.

Below is an example definition of an agent identifier in the form of a hierarchical string:

orgtype:org/internal enterprise namespace/client-id

Where:

* orgtype indicates the standardized type or schema that the org field conforms to. This enables consistent interpretation and validation of the organizational context associated with the agent, such as whether the organization is identified according to a public registry (e.g., PENs for orgnizations [RFC9371]), or another recognized naming authority.

* org field identifies the enterprise or organization to which the agent belongs, in accordance with the standard specified by the orgtype field.This ensures that the organizational identifier is interpreted consistently and unambiguously according to the referenced naming scheme or registry.

* internal enterprise namespace is defined and managed autonomously by the enterprise itself. It provides a private, organization-specific naming scheme for identifying agents, organizational units, or other entities within the enterprise's administrative domain, without reliance on external registries or global standards.

* client-id serves as a locally unique identifier for the agent within its administrative or operational domain. It MAY be assigned by the agent gateway upon registration, or alternatively issued by a Certificate Authority (CA) during the agent identity signing process, ensuring uniqueness and cryptographic binding to the agent's identity credentials.

5.2. Agent Identity Basic Managenment

Based on the base information contained in the agent description, the agent gateway can perform fundamental identity management functions using the agent ID as the primary key.

Agent ID : Basic Management functions

These functions include, but are not limited to:

* Identity verification management: validating the authenticity and integrity of the agent using attributes such as name, signature, and author.

* Capability classification management: categorizing agents according to their declared skills/capabilities for policy-based routing or service matching.

* Communication protocol management: enforcing or negotiating supported communication protocols to ensure interoperability.

* Lifecycle management: tracking and controlling the agent’s operational state (e.g., creation, activation, expiration, revocation) based on attributes such as creation time and validity period.

* Form factor classification management: grouping agents by their form (e.g., embedded, digital) for resource allocation or policy application.

* Intelligence level management: applying differentiated handling policies based on the agent’s declared intelligence level.For example, the agent gateway MAY apply behavior monitoring policies of varying intensity based on the agent’s declared intelligence level, thereby preventing high-intelligence agents from performing unauthorized or out-of-scope actions.

* Extended profile management: referencing and validating the agent’s extended profile URI for dynamic or context-specific attributes.

* Role-based classification management: assigning or enforcing permissions and behaviors according to the agent’s declared role.

* Communication translation management: enabling or disabling protocol or semantic translation based on the translation enablement indicator.

These management functions collectively support scalable, secure, and policy-compliant operation of agents within the IOA system.

5.3. Agent Identity Extended Management

By leveraging the extensible information included in the agent description, the agent gateway can perform enhanced identity management functions beyond the base set.

Agent ID : Extended Management functions

These extended management functions include:

* Agent network service management: dynamically provisioning, monitoring, or orchestrating network services associated with the agent (e.g., QoS requirements, connectivity policies, security assurance, and etc.).

* Agent permission management: enforcing fine-grained, context-aware access control policies based on extended permission scopes, such as data residency constraints (e.g., "data must not leave the campus or country").

* Future extensible identity management functions: supporting additional identity-related features that may be defined in future specifications, such as behavioral attestation, perfermence scoring, or integration with decentralized identity frameworks.

The extensible information field is designed to be forward-compatible, enabling the agent gateway to adapt to evolving operational, regulatory, or architectural requirements without requiring changes to the core agent description model.

6. Security Considerations

Security is a critical consideration in agent identity management. This includes authenticating and validating the agent’ s identity during registration, ensuring the integrity and non-repudiation of the agent identifier (e.g., to prevent tampering or spoofing), and enforcing access control policies for agent onboarding and interaction. However, the specific security mechanisms and detailed considerations related to these aspects are outside the scope of this document.

7. IANA Considerations

TBD

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Chong Zheng
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: zhengchong6@huawei.com

Bing Liu
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: leo.liubing@huawei.com

Nan Geng
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: gengnan@huawei.com

Qiangzhou Gao
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: gaoqiangzhou@huawei.com

Xiaotong Shang
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: shangxiaotong@huawei.com

Zhenbin Li
Huawei Technologies
No. 156 Beiqing Road
Beijing
China
Email: robinli314@163.com