Internet Engineering Task Force H. Yu
Internet-Draft China Internet Network Information Center
Intended status: Informational 20 May 2026
Expires: 21 November 2026

An RDAP Profile for Agent Identifier Registration Data
draft-yu-agent-identifier-rdap-00

Abstract

AI agents may need stable identifiers that are independent from their current network locations. In agent deployments, an Agent identifier may be associated with IPv6 locators, IPv6 prefixes, Agent Gateways, public key references, policy references, lifecycle state, and revocation status. Applications, gateways, controllers, and operators need a trusted way to query this registration data.

This document defines an RDAP profile for querying Agent identifier registration data. The profile reuses the Registration Data Access Protocol (RDAP) query model and JSON response format, and defines an RDAP object class and extension members for Agent identifiers, IPv6 locator bindings, Agent Gateway bindings, and related operational metadata.

This document does not define a new agent discovery protocol, a new agent interaction protocol, or a new authentication mechanism. It defines a registration data access profile that can be used by agent deployments and by other agent-related systems that need trusted Agent identifier metadata.

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 21 November 2026.

Table of Contents

1. Conventions Used in This Document

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. Introduction

AI agents are increasingly expected to interact across platforms, organizations, clouds, edge environments, and administrative domains. A stable Agent identifier can help identify an agent independently from the agent's current network location. However, a relying party may still need to know which entity is responsible for the Agent identifier, whether the identifier is active, which IPv6 locators or Agent Gateways are authorized to represent the agent, and whether a binding has expired or been revoked.

The companion IPv6 networking considerations draft discusses what networking information may be needed after agent discovery, including Agent-ID to IPv6 locator or Agent Gateway binding. This document explores one possible way to provide stable registration data for Agent identifiers using RDAP.

RDAP provides a RESTful query model and JSON responses for registration data [RFC7480] [RFC9082] [RFC9083]. Reusing RDAP allows agent deployments to use an existing registration data access model rather than defining a new query protocol.

3. Scope and Non-Goals

This document specifies:

* an RDAP object class for Agent identifiers;
* query paths for Agent identifier lookup;
* JSON members for Agent lifecycle state and responsible entity references;
* JSON members for IPv6 locator and Agent Gateway bindings;
* JSON members for policy, certificate, validity, and revocation metadata;
* security and privacy considerations for exposing Agent registration data.

This document does not specify:

* a new Agent identifier syntax;
* a new agent discovery or collaboration protocol;
* a new authentication, authorization, or attestation protocol;

* a mandatory global registry for all Agent identifiers;

* real-time presence, health, load, capability ranking, or endpoint selection;

* a replacement for RDAP domain, nameserver, entity, autnum, or IP network objects.

4. Terminology

Agent:
A software entity that can perceive context, reason, plan, invoke tools, communicate with other agents, and perform tasks on behalf of a user, organization, or system.

Agent Identifier:
A stable identifier used to identify an agent independently from its current network location.

Agent Networking Considerations:
Considerations related to the use of IP networking mechanisms to support agent communication after discovery.

Agent Gateway:
A network or application gateway that represents one or more agents and provides controlled access, address mapping, policy enforcement, protocol adaptation, or telemetry collection.

Agent Binding:
An association between an Agent identifier and one or more IPv6 locators, IPv6 prefixes, or Agent Gateways.

Agent RDAP Object:
An RDAP object representing registration data for an Agent identifier.

5. RDAP Extension Identifier

RDAP responses that use the extensions defined in this document MUST include the extension identifier "agent_identifier_rdap" in the "rdapConformance" array.

```
{
  "rdapConformance": [
    "rdap_level_0",
    "agent_identifier_rdap"
  ]
}
```

The extension identifier is used provisionally in this version. Future versions may request IANA registration if this approach receives community interest.

6. Query Path

This profile defines the following RDAP query path for exact Agent identifier lookup:

/agent/{agentIdentifier}

The "agentIdentifier" path component is the Agent identifier being queried. The value MUST be percent-encoded when required by URI syntax.

Servers MAY also support search paths in a future version. This document defines only exact lookup.

7. Agent RDAP Object

An Agent RDAP Object is an RDAP response object that describes an Agent identifier and related registration data. It reuses common RDAP members such as "objectClassName", "handle", "entities", "events", "links", "notices", and "remarks" as defined by RDAP.

The "objectClassName" member for an Agent RDAP Object MUST be "agent".

The following agent-specific members are defined:

agentIdentifier:
: The stable Agent identifier represented by this object.

agentStatus:
: The lifecycle state of the Agent identifier or binding. Example values include "active", "inactive", "suspended", "revoked", and "expired".

responsibleEntity:
: An RDAP entity handle, URI, or opaque reference identifying the entity responsible for the Agent identifier.

agentDomains:
: An array of administrative or operational domains associated with the Agent identifier.

ipv6Locators:
An array of IPv6 locator objects associated with the Agent identifier.

agentGateways:
An array of Agent Gateway objects authorized to represent the Agent identifier.

certificateRefs:
An array of certificate, key, or trust document references.

policyRefs:
An array of policy references associated with the Agent identifier or binding.

revocationStatus:
Information about revocation state and revocation checking endpoints.

8. IPv6 Locator Object

An IPv6 Locator Object describes an IPv6 address or prefix through which an agent instance, service, or gateway can be reached.

The following members are defined:

locator:
An IPv6 address or prefix.

locatorType:
The type of locator. Example values include "instance", "service", "gateway", and "prefix".

priority:
An integer used to express selection priority. Lower values indicate higher preference.

weight:
An integer used for weighted selection among locators of equal priority.

region:
A deployment region, availability zone, site, or other operational location label.

validFrom:
The time from which this locator binding is valid.

validUntil:
The time after which this locator binding is no longer valid.

status:
The status of the locator binding. Example values include "active", "inactive", "revoked", and "expired".

9. Agent Gateway Object

An Agent Gateway Object describes a gateway that is authorized to represent one or more Agent identifiers.

The following members are defined:

gatewayIdentifier:
A stable identifier for the Agent Gateway.

gatewayLocator:
An IPv6 address, IPv6 prefix, URI, or other locator used to reach the gateway.

representedAgents:
An array of Agent identifier references or patterns represented by the gateway.

authorizationRef:
A reference to authorization data showing that the gateway may represent the Agent identifier.

policyRefs:
An array of policy references enforced by or associated with the gateway.

status:
The status of the gateway binding.

10. Example Response

The following example shows an Agent RDAP Object for an agent that is reachable through an Agent Gateway.

```
{
  "rdapConformance": [
    "rdap_level_0",
    "agent_identifier_rdap"
  ],
  "objectClassName": "agent",
  "handle": "AGENT-EXAMPLE-0001",
```

```
    "agentIdentifier": "agent:warehouse.example.cn:agv-001",
    "agentStatus": "active",
    "responsibleEntity": "CNIC-EXAMPLE-ENTITY",
    "agentDomains": [
      "warehouse.example.cn"
    ],
    "ipv6Locators": [
      {
        "locator": "2001:db8:100:20::1",
        "locatorType": "gateway",
        "priority": 100,
        "weight": 100,
        "region": "warehouse-site-a",
        "validFrom": "2026-05-20T00:00:00Z",
        "validUntil": "2026-11-20T00:00:00Z",
        "status": "active"
      }
    ],
    "agentGateways": [
      {
        "gatewayIdentifier": "warehouse-gateway-001",
        "gatewayLocator": "2001:db8:100:20::1",
        "representedAgents": [
          "agent:warehouse.example.cn:agv-001"
        ],
        "authorizationRef": "https://example.net/agent/authz/warehouse-gw-001",
        "policyRefs": [
          "policy:warehouse-dispatch"
        ],
        "status": "active"
      }
    ],
    "certificateRefs": [
      "https://example.net/agent/certs/agv-001"
    ],
    "policyRefs": [
      "policy:warehouse-dispatch"
    ],
    "revocationStatus": {
      "status": "notRevoked",
      "revocationCheck": "https://example.net/agent/status/agv-001"
    },
    "events": [
      {
        "eventAction": "registration",
        "eventDate": "2026-05-20T00:00:00Z"
      },
      {
```

```
        "eventAction": "last changed",
        "eventDate": "2026-05-20T00:00:00Z"
      }
    ],
    "links": [
      {
        "value": "https://rdap.example.net/agent/agent%3Awarehouse.example.cn%3Aagv-001"
,
        "rel": "self",
        "href": "https://rdap.example.net/agent/agent%3Awarehouse.example.cn%3Aagv-001",
        "type": "application/rdap+json"
      }
    ]
  }
```


11. Use with Agent Networking

An agent networking implementation can use this RDAP profile to verify Agent-ID binding data before selecting an IPv6 locator, Agent Gateway, or network policy. For example, an Agent Gateway can query the Agent RDAP Object to determine whether it is authorized to represent a target Agent-ID. A controller can query the same object to select a locator or policy for a given communication, such as an SRv6 policy in a controlled domain.

This RDAP profile is not a real-time reachability protocol. It provides registration data. Implementations that require live reachability, health, or load information should combine this profile with other mechanisms such as Agent registries, service discovery systems, controllers, telemetry, or application-layer health checks. Online/offline state, live load, health, capability ranking, and endpoint selection are out of scope for this profile.

12. Conformance and Error Handling

Servers implementing this profile MUST follow RDAP transport and response requirements. RDAP error responses, including status codes, notices, and remarks, are used as defined by RDAP.

If the requested Agent identifier does not exist, the server SHOULD return an RDAP not-found response. If the Agent identifier exists but the client is not authorized to view the requested data, the server SHOULD return an appropriate authorization error or a redacted response according to local policy.

A server MAY return different field sets to different clients based on authentication, authorization, local policy, and privacy requirements. Clients MUST NOT assume that absence of a field means absence of the corresponding registration data.

13. Relationship to Audit and Accountability

Agent identifier registration data can be useful to audit and accountability systems. For example, an audit record may contain an Agent identifier and later need to determine the responsible entity, lifecycle state, revocation state, authorized Agent Gateway, or associated IPv6 locator for that identifier.

This profile can provide stable registration data that audit systems may reference. It does not define audit records, distributed audit log formats, audit context propagation, attestation evidence, transparency logs, or non-repudiation mechanisms.

14. Security Considerations

Agent registration data can influence routing, gateway selection, access control, and policy enforcement. Servers providing Agent RDAP Objects MUST authenticate update operations and MUST ensure that an Agent identifier cannot be bound to an unauthorized IPv6 locator or Agent Gateway.

RDAP clients MUST use HTTPS as specified by RDAP over HTTP. Clients MUST validate the server identity according to the applicable TLS validation rules.

Agent Gateway authorization data is security-sensitive. A gateway MUST NOT be treated as authorized to represent an Agent identifier solely because it appears in an unauthenticated or stale response. Implementations SHOULD check validity periods, revocation status, and policy references before relying on gateway binding information.

Replay and stale-data attacks are possible if old registration data is accepted after a binding has changed or been revoked. Servers SHOULD include update events and validity intervals. Clients SHOULD apply local freshness policies and re-query when cached data is stale.

This profile does not define how Agent identifiers are created, delegated, or cryptographically controlled. Deployments MUST define the authority model used to issue and manage Agent identifiers.

15. Privacy Considerations

Agent RDAP Objects may reveal information about organizations, internal deployments, gateways, network locations, operational regions, policy names, and relationships between domains. Servers SHOULD minimize disclosed data and apply access control where appropriate.

Some Agent identifiers may be pseudonymous or scoped to a domain. Servers SHOULD avoid exposing unnecessary personally identifiable information, user data, prompts, task descriptions, or sensitive application payload information in Agent RDAP Objects.

Public RDAP responses and authenticated RDAP responses may have different disclosure levels. Deployments SHOULD define which fields are public and which require authorization.

16. IANA Considerations

This initial version does not request any IANA action.

Future versions may request registration of an RDAP extension identifier if this approach receives community interest.

17. 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>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

18. Informative References

[RFC7482] Newton, A. and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format", RFC 7482, DOI 10.17487/RFC7482, March 2015, <https://www.rfc-editor.org/info/rfc7482>.

[RFC7483] Newton, A. and S. Hollenbeck, "JSON Responses for the Registration Data Access Protocol (RDAP)", RFC 7483, DOI 10.17487/RFC7483, March 2015, <https://www.rfc-editor.org/info/rfc7483>.

[I-D.yu-ai-agent-ipv6-networking-considerations] Yu, H., "IPv6 Networking Considerations for AI Agent Communication", <https://datatracker.ietf.org/doc/draft-yu-ai-agent-ipv6-networking-considerations/>.

Author's Address

Haisheng Yu
China Internet Network Information Center
Email: yuhaisheng@cnnic.cn