Network Working Group
Internet-Draft
Intended status: Informational
Expires: 31 October 2026

L. Zhang
H. Yang
Y. Li
S. Wang
AsiaInfo Technologies (China) Inc.

29 April 2026

Gateway Capability Directory and Synchronization for Internet of Agents
draft-zhang-dmsc-gateway-directory-sync-01

Abstract

This document describes a gateway capability-directory framework for the Internet of Agents (IoA) in deployments that use Agent Gateways. In such deployments, a gateway-managed capability directory is a necessary control-plane function for maintaining validated capability information beyond transient advertisements, static endpoint bindings, or external descriptions alone. This document defines requirements and a common object model for gateway-managed capability information, including the Agent Capability Specification (ACS), Capability Digest, and directory entry lifecycle. It also specifies synchronization, freshness, provenance, and validation requirements for capability information exchanged across gateways.

This document clarifies the relationship between gateway-managed ACS objects and externally published descriptions such as the A2A Agent Card, and briefly compares this framework with broader distributed directory-service approaches. It does not define a discovery query protocol, ranking algorithm, storage substrate, distributed lookup algorithm, task orchestration protocol, or agent-to-agent session protocol. It can inform subsequent DMSC protocol work, including capability digest synchronization and related gateway procedures.

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 31 October 2026.

Table of Contents

1. Introduction

As agent systems become increasingly distributed across heterogeneous networks and administrative domains, a gateway-based deployment needs a gateway-managed capability directory as a stable control-plane view of capability information. A gateway cannot rely only on transient advertisements, static endpoint bindings, or external descriptions if it is expected to support capability visibility, semantic resolution, policy enforcement, routing input, and interconnection across gateways.

This document therefore describes a framework for gateway capability directories and synchronization in IoA. It focuses on what information a gateway-managed directory entry needs to contain, how that information is derived and maintained, how much of it can be synchronized across gateways, and what validation and provenance guarantees are required before the information can be used by routing, task invocation, or other collaboration functions.

Adjacent work is separating discovery from other interoperability layers. DAWN is focusing on discovery problem statements, terminology, and requirements, while explicitly excluding registration processes, capability negotiation, task orchestration, and agent-to-agent communication protocols [DAWN-PS] [DAWN-REQ]. This leaves DMSC-specific work on the gateway-side capability directory that supports registration, synchronization, validation, and handoff to collaboration protocols.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174].

The following terms are used in this document:

Agent Capability Specification (ACS): A gateway-managed, structured capability description associated with an Agent Identity Code (AIC) and constrained by local authorization and policy.

Capability Digest: A gateway-generated summary derived from one or more ACS objects, intended for inter-gateway visibility and synchronization rather than full capability disclosure.

Directory Entry: A versioned object stored or managed by a gateway capability directory. A directory entry MAY contain a full ACS, a derived digest, or related validation metadata.

Handoff Reference: Information returned by a gateway that enables a subsequent interaction, invocation, or session establishment step.

Source Description: An externally or internally supplied capability description that a gateway can ingest, normalize, or constrain. Examples include an A2A Agent Card, a local registration payload, or an operator-managed descriptor.

Freshness: The degree to which synchronized or cached information is still valid for operational use.

Provenance: Evidence indicating where a directory entry originated, how it was transformed, and what authority or gateway asserted it.

3. Scope and Non-Goals

This document specifies:

- A common framework for gateway capability directory objects in IoA deployments.

- Requirements for ACS objects, capability digests, and directory entry lifecycle.

- Requirements for synchronization, freshness, provenance, and validation across gateways.

- The relationship between gateway-managed ACS objects and externally published descriptions such as the A2A Agent Card.

This document does not specify:

- A discovery query protocol, query syntax, ranking algorithm, or candidate selection policy.

- A naming system, global identifier resolution protocol, or generic registry architecture for all entities.

- Agent-to-gateway advertisement messages, intent submission messages, candidate-list response messages, routing-feedback messages, or other wire-format exchanges of an intent-routing protocol.

- Task orchestration, session establishment, or agent-to-agent message exchange procedures.

- A domain-specific ontology or a full semantic negotiation protocol, although semantic hooks MAY be carried by directory objects.

- A complete identity framework, trust framework, or credential issuance system.

4. Architecture Overview

Within a gateway-based IoA deployment, the capability directory is a gateway-side control-plane function. It receives or derives capability descriptions during onboarding, associates them with an AIC and authorized operational scope, maintains local directory entries, and exposes suitable information to later functions such as semantic resolution, task-based invocation, and inter-gateway visibility.

The capability directory sits between registration/authorization and collaboration/runtime procedures, as illustrated in Figure 1.

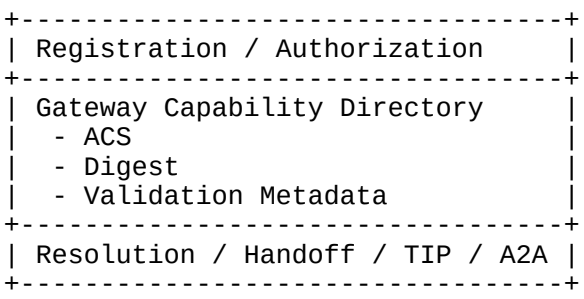

Figure 1

Figure 1: Capability Directory Position

A gateway capability directory manages directory entries. A directory entry may carry a full ACS, a derived Capability Digest, or related validation metadata, depending on local use and disclosure scope.

5. Directory Object Model

5.1. Agent Capability Specification

An ACS is the primary full directory object. An ACS MUST be bound to a single AIC or equivalent local agent identity reference. An ACS SHOULD be sufficient for local directory use, semantic resolution input, handoff preparation, and policy evaluation.

An ACS SHOULD contain at least:

- a stable local identifier for the ACS entry;

- the bound AIC or equivalent identity reference;

- one or more capability references;

- input/output or modality references relevant to invocation and compatibility;

- interface binding references and handoff references, if available;

- local status and version information;

- provenance and integrity metadata; and

- optional semantic hooks such as ontology identifier, ontology version, or semantic-profile reference.

An ACS MAY additionally carry local policy constraints, region or domain scope, deployment visibility, or runtime limitations. Such information SHOULD be clearly distinguished from core capability assertions.

5.2. Capability Digest

A Capability Digest is a derived object intended for synchronization and visibility across gateways. A digest MUST be smaller in disclosure scope than the corresponding ACS. It SHOULD reveal enough information for coarse-grained matching, routing preparation, or further query forwarding, while minimizing unnecessary internal detail.

A Capability Digest SHOULD contain:

- a digest identifier and version;

- the asserting gateway or administrative domain identifier;

- one or more abstracted capability references or categories;

- visibility scope and freshness metadata; and

- provenance and integrity metadata.

A digest MAY contain handoff hints, interface categories, trust indicators, or semantic summary references, provided these do not disclose more information than permitted by local policy.

5.3. Directory Entry States

Directory entries SHOULD support an explicit lifecycle. The following states are RECOMMENDED:

- active: entry is valid for operational use;

- suspended: entry is temporarily not usable but retained;

- deprecated: entry remains visible for compatibility but SHOULD be replaced; and

- revoked: entry MUST NOT be used for new operational decisions.

Implementations MAY define equivalent states, but the effect on visibility and use MUST be clear.

6. Lifecycle Requirements

A gateway MUST be able to create, update, deprecate, suspend, revoke, and remove directory entries under local lifecycle control. Registration and credential issuance themselves are out of scope, but this document defines what the directory layer requires after onboarding has completed.

At a minimum:

- a new ACS entry MUST be versioned at creation time;

- changes to bound identity, capability references, interface binding references, semantic hooks, or integrity metadata SHOULD create a new version or equivalent version transition;

- state changes MUST be auditable;

- revoked entries MUST be excluded from new handoff or resolution results; and

- deprecated entries SHOULD indicate replacement or migration information if available.

If an ACS is derived from an external source description such as an A2A Agent Card, the gateway SHOULD distinguish source changes from gateway-local changes. A source refresh that does not alter accepted operational semantics MAY update freshness metadata without changing the ACS semantic version.

7. Synchronization Requirements

Gateways in the same collaboration environment or across federated domains MAY synchronize capability visibility information. Synchronization MUST be policy-aware and SHOULD default to Capability Digest exchange rather than full ACS replication.

A synchronization mechanism for directory information SHOULD support:

- initial establishment of baseline visibility;

- incremental updates for entry creation, modification, withdrawal, and state transitions;

- version comparison or ordering sufficient to detect stale updates;

- explicit acknowledgement or equivalent delivery confirmation;

- conflict detection and local conflict resolution policy; and

- recovery after disconnection or partial state loss.

When multiple gateways provide conflicting information about the same effective capability or identity reference, the receiving gateway SHOULD consider provenance, signature status, administrative trust policy, lifecycle state, and update freshness before accepting the new information.

Synchronization procedures SHOULD be able to carry, or reference, the following metadata:

- source gateway identifier;

- entry identifier and version;

- operation type;

- effective time or update time;

- optional replacement or revocation information; and

- integrity and provenance evidence.

8. Freshness, Validation, and Provenance

A gateway MUST evaluate whether directory information is still suitable for operational use before returning it to semantic resolution, handoff preparation, or task-routing logic.

Directory validation SHOULD include:

- integrity validation of the entry or synchronized update;

- freshness validation against local policy or advertised validity information;

- lifecycle-state validation, including revocation awareness;

- provenance validation indicating which gateway or source asserted the information; and

- semantic or profile reference validation when semantic hooks are present.

Validation failure handling SHOULD distinguish between:

- invalid entry content;

- unverifiable provenance;

- stale information;

- revoked information; and

- locally disallowed disclosure or use.

An implementation MAY retain invalid or stale entries for audit or troubleshooting purposes, but such entries MUST NOT be used for new operational decisions unless explicitly allowed by local policy.

9. DMSC Integration

Within DMSC architecture, the capability directory is a gateway-side control-plane function that supports other DMSC functions such as semantic resolution, task-based invocation, and inter-gateway visibility [MACP-02] [ACPS-ARC] [IOA-TASK].

This document is intended to be complementary to other DMSC work. It refines the control-plane objects and requirements needed by protocol-suite elements such as ACS/CDSP in MACP, by capability-management and discovery functions in ACPs Architecture, and by gateway functions such as delegated discovery, ID-based resolution, and task-based searching [MACP-02] [ACPS-ARC] [GW-REQ].

It also provides a substrate that can be used by task-level procedures and semantic-interoperability work, while remaining below gateway-facing intent-routing behavior such as IAIP [IOA-TASK] [IOA-SEM] [IAIP-00]. Accordingly, this document does not define discovery query syntax or routing algorithms. Instead, the capability directory defined here is intended to support other DMSC functions as follows:

- semantic resolution procedures MAY use ACS or digest content as inputs to capability matching and route preparation;

- task-based invocation procedures MAY use handoff references and capability constraints derived from ACS content;

- gateway policy enforcement MAY use lifecycle state, provenance, and local constraints stored with the directory entry; and

- semantic interoperability procedures MAY use optional ontology or semantic-profile hooks carried by ACS content without redefining the semantic layer itself.

10. Relationship to External Descriptions

A gateway capability directory can ingest or reference externally supplied descriptions. Such external descriptions MAY be published by an agent endpoint, a management system, or another authoritative source. They are treated by this document as source descriptions rather than as gateway-native directory objects.

A2A defines the Agent Card as one example of such an external description. The Agent Card is a self-describing object published by an agent endpoint for discovery and interaction setup, and includes information such as identity, skills, supported interfaces, security requirements, and other public metadata [A2A-SPEC].

An ACS is not the same object as an external description such as an A2A Agent Card. An external description states what an agent claims or offers for publication or exchange, while an ACS is a gateway-managed, normalized, and policy-constrained directory object used by DMSC infrastructure. A Capability Digest is a further abstraction derived from ACS content for inter-gateway visibility.

A gateway MAY ingest an A2A Agent Card as one source description when constructing an ACS. However, externally supplied description content is not automatically suitable for directory synchronization or operational use; it remains subject to local validation, normalization, provenance tracking, and policy application.

11. Relationship to Other Directory Approaches

Other proposals are considering broader directory-service mechanisms for agents. For example, the ADS draft discusses a distributed agent directory service with content-addressed storage, taxonomy-based discovery, content-routing, and peer-to-peer synchronization [ADS-01].

This document has a narrower focus. It defines the gateway-managed control-plane directory objects and requirements that a DMSC Gateway needs in order to maintain validated capability information for local use and inter-gateway visibility.

Accordingly, this document does not define a storage substrate, content-addressed artifact model, distributed lookup algorithm, taxonomy design, or generic search architecture. Such mechanisms could be complementary if they are used as one backend, one exchange environment, or one visibility mechanism for gateway-managed directory information.

12. Security Considerations

Capability directories and synchronization channels are attractive targets for poisoning, replay, downgrade, and unauthorized disclosure attacks. Implementations SHOULD consider:

- integrity protection for ACS entries and synchronized digests;

- provenance continuity for derived objects, especially when ingesting external descriptions such as A2A Agent Cards;

- freshness enforcement to prevent stale or replayed capability visibility;

- access control over which entries may be disclosed, synchronized, or returned for operational use; and

- auditability of lifecycle changes and synchronization decisions.

If semantic hooks are carried, implementations SHOULD also consider risks related to ontology substitution, invalid alignment references, or use of inconsistent semantic-profile versions.

13. IANA Considerations

This document makes no request for IANA action.

14. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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, 2017, <https://www.rfc-editor.org/info/rfc8174>.

15. Informative References

[A2A-SPEC] Foundation, L., "A2A Protocol Specification", 2026, <https://a2a-protocol.org/latest/specification/>.

[ACPS-ARC] Liu, J., Yu, K., Li, K., and K. Chen, "Agent Collaboration Protocols Architecture for Internet of Agents", Work in Progress, Internet-Draft, draft-liu-dmsc-acps-arc-03, 2026, <https://datatracker.ietf.org/doc/draft-liu-dmsc-acps-arc/03/>.

[ADS-01] Muscariello, L. and R. Polic, "Agent Directory Service", Work in Progress, Internet-Draft, draft-mp-agntcy-ads-01, 2026, <https://datatracker.ietf.org/doc/draft-mp-agntcy-ads/01/>.

[DAWN-PS] Akhavain, A., Moussa, H., and D. King, "Problem Statement for the Discovery of Agents, Workloads, and Named Entities (DAWN)", Work in Progress, Internet-Draft, draft-akhavain-moussa-dawn-problem-statement-00, 2026, <https://datatracker.ietf.org/doc/draft-akhavain-moussa-dawn-problem-statement/00/>.

[DAWN-REQ] King, D. and A. Farrel, "Requirements for the Discovery of Agents, Workloads, and Named Entities (DAWN)", Work in Progress, Internet-Draft, draft-king-dawn-requirements-00, 2026, <https://datatracker.ietf.org/doc/draft-king-dawn-requirements/00/>.

[GW-REQ] Liu, B., "Gateway Requirements for Dynamic Multi-agents Secured Collaboration", Work in Progress, Internet-Draft, draft-liu-dmsc-gw-requirements-00, 2026, <https://datatracker.ietf.org/doc/draft-liu-dmsc-gw-requirements/00/>.

[IAIP-00] Sun, S. and X. Zhang, "Intent-based Agent Interconnection Protocol at Agent Gateway", Work in Progress, Internet-Draft, draft-sz-dmsc-iaip-00, 2026, <https://www.ietf.org/archive/id/draft-sz-dmsc-iaip-00.txt>.

[IOA-SEM] Zhang, L., Yang, H., Li, Y., and S. Wang, "Ontology-based Semantic Interaction for Internet of Agents", Work in Progress, Internet-Draft, draft-zhang-dmsc-ioa-semantic-interaction-02, 2026, <https://datatracker.ietf.org/doc/draft-zhang-dmsc-ioa-semantic-interaction/02/>.

[IOA-TASK] Yang, C., Wang, P., Wu, J., and T. Huang, "Internet of Agents Task Protocol for Heterogeneous Agent Teaming and Cross-domain Collaboration", Work in Progress, Internet-Draft, draft-yang-dmsc-ioa-task-protocol-01, 2026, <https://datatracker.ietf.org/doc/draft-yang-dmsc-ioa-task-protocol/01/>.

[MACP-02] Li, X., Liu, J., Du, C., and L. Zhang, "Multi-agent Collaboration Protocol Suite", Work in Progress, Internet-Draft, draft-li-dmsc-macp-02, 2026, <https://datatracker.ietf.org/doc/draft-li-dmsc-macp/02/>.

Authors' Addresses

Lianhua Zhang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: zhanglh2@asiainfo.com

Huiling Yang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: yanghl10@asiainfo.com

Yun Li
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: liyun9@asiainfo.com

Shoufeng Wang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: wangsf11@asiainfo.com