Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 5 April 2026

A. Sogomonian
Artificial Intelligence Internet Foundation (AIIF)

2 October 2025

AI URI Scheme
draft-sogomonian-ai-uri-scheme-01

Abstract

This document specifies the experimental ai Uniform Resource Identifier (URI) scheme. The scheme provides a dedicated access point for Artificial Intelligence (AI) resources, enabling autonomous systems and robots to connect natively while allowing human-facing applications to interoperate via HTTPS gateways.

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 5 April 2026.

Table of Contents

1. Introduction

The ai URI scheme identifies AI-addressable resources such as agents, models, tools, and tasks. Deployments *MAY* resolve ai: identifiers natively within AI systems and robots, or via HTTPS gateways for compatibility with existing web stacks.

For clarity, this document uses the term AIIP to denote the _Artificial Intelligence Internet Protocol_, the operational protocol by which ai:// resources are addressed, resolved, and invoked. While ai:// is the URI scheme, AIIP defines resolution and interaction semantics.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. URI Syntax (Non-Normative)

The scheme follows [RFC3986]. An informal summary is shown:

```
ai-uri = "ai:" hier-part [ "?" query ] [ "#" fragment ]
; hier-part, query, fragment per RFC 3986
```

Examples (illustrative only):

```
ai:/agent/forklift-42?task=load&zone=A3
ai://factory.example/pay?amount=10&currency=USD
```

3. Web Integration and HTTPS Gateway Access

Many user agents will not natively implement the ai scheme or the Artificial Intelligence Internet Protocol (AIIP). To enable immediate interoperability, deployments *MAY* expose ai:// resources via HTTPS gateways so that end users remain on conventional websites while backends or trusted intermediaries invoke AIIP. In this model, a relying party (for example, an online bank) advertises an ai:// endpoint and resolves it server-side or through a gateway; the user continues to interact over HTTPS without needing to understand ai://.

3.1. Discovery from HTTPS

HTTPS origins that rely on AIIP *SHOULD* advertise their ai:// endpoints using one or more of:

* *HTTP Link header* on responses:

  ```
  Link: <ai://bank/service/payments>; rel="aiip"
  ```

* *HTML link relation* for progressive enhancement:

  ```
  <link rel="aiip" href="ai://bank/service/payments">
  ```

* *Well-known resource* at /.well-known/aiip:

  ```
  {
    "endpoint": "ai://bank/service/payments",
    "jwks":
      "https://www.bank.example/.well-known/aiip.jwks.json",
    "scopes": [
      "initiate-payment",
      "check-balance"
    ],
    "policy": {
      "auth": "oauth2",
      "mtls": true,
      "requireSignedResults": true
    }
  }
  ```

* *DNS bootstrap (optional)*, for example, SRV or TXT records:

  ```
  _aiip._tcp.bank.example.  300 IN SRV 0 0 443
                            aiip.bank.example.
  _aiip.bank.example.       300 IN TXT
                            "endpoint=ai://bank/service/payments"
  ```

3.2. HTTPS to AIIP Gateway Behavior

A conforming HTTPS to AIIP gateway *MUST* map an embedded ai:// URI to an HTTPS URL under its control, perform AIIP resolution, and translate the result back into HTTPS semantics for the client. For example:

Original:
ai://bank/service/payments?amount=10&currency=USD
Gateway :
https://ai.example/gateway/bank/service/payments
?amount=10&currency=USD

Gateways *MUST*:

* Parse and normalize the ai:// URI; reject malformed or ambiguous inputs.

* Authenticate to the AI endpoint and verify provenance of responses (for example, JWS with a key discoverable via the origin’s JWKS).

* Enforce authorization consistent with the user’s web session (for example, token exchange, DPoP, or mTLS constraints).

* Preserve confidentiality and integrity at least equivalent to TLS 1.3 [RFC8446] and obey HTTP semantics [RFC9110].

* Prevent downgrades; do not weaken authentication or authorization versus native AIIP.

3.3. No Native AIIP Requirement for User Agents

Web user agents *NEED NOT* implement AIIP. Sites may perform all AI resolution server-side or via a trusted gateway. This enables gradual deployment: users remain on HTTPS while services invoke ai:// under the hood to complete actions (for example, initiating a payment).

3.4. Provenance and Result Integrity

Responses returned from AIIP resolution *MUST* include verifiable provenance (for example, a detached or embedded signature). Gateways and relying parties *MUST* reject unverifiable or policy-incompatible results. Implementations *SHOULD* publish a JWKS for verification and rotate keys per operational policy.

4. Namespace Administration

To support global uniqueness and safe operation of autonomous systems, namespace administration for ai: identifiers is expected to be coordinated by the _Artificial Intelligence Internet Foundation (AIIF)_, which serves as the umbrella governance body. The _AIIF Registry Authority for Identifiers (AIID)_ operates the AI Root Registry and administers identifier allocation and operational policy for ai:// namespaces. This administrative role is separate from the technical specification of the scheme and protocol.

5. Security Considerations

Implementations that dereference ai: identifiers *MUST* authenticate endpoints and apply authorization and safety policies, especially when actions may control physical devices or financial operations. Gateways translating ai: to HTTPS *MUST* preserve provenance and provide transport security per [RFC8446] and semantics conforming to [RFC9110].

6. Privacy Considerations

Accessing ai:// resources through HTTPS gateways may expose metadata such as target identifiers, origin site, and timing information to intermediaries. Gateways *SHOULD* minimize logging, apply strict data retention limits, and avoid retaining identifiers longer than operationally necessary. Provenance and result signatures may contain linkable identifiers; deployments *SHOULD* apply least-privilege scopes and anonymization where appropriate.

7. Internationalization Considerations

Identifiers in ai:// URIs follow [RFC3986]. Non-ASCII characters appearing in the path or query components *MUST* be percent-encoded. Any authority components mapped from DNS *MUST* follow IDNA processing where applicable. No additional internationalization mechanisms are defined by this document.

8. IANA Considerations

This document requests Provisional registration of the ai URI scheme per [RFC7595].

8.1. URI Scheme Registration

This section provides the registration template for the ai URI scheme in accordance with [RFC7595] Section 3.4.

Scheme name: ai
Status: Provisional
Applications/protocols that use this scheme:
AIIP (Artificial Intelligence Internet Protocol)
Contact:
Aram Sogomonian <waterbottling@icloud.com>
Change controller:
The author of this document (or a designated successor)
References:
This document; RFC 3986; RFC 7595; RFC 8446; RFC 9110
Security considerations:
See "Security Considerations" of this document

9. Normative References

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC7595] Thaler, D., Hansen, T., and T. Hardie, "Guidelines and Registration Procedures for URI Schemes", RFC 7595, June 2015, <https://www.rfc-editor.org/info/rfc7595>.

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

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9110] Fielding, R. and J. Reschke, "HTTP Semantics", RFC 9110, June 2022, <https://www.rfc-editor.org/info/rfc9110>.

Author’s Address

Aram Sogomonian
Artificial Intelligence Internet Foundation (AIIF)
United States of America
Email: waterbottling@icloud.com