Independent Submission
Internet-Draft
Intended status: Informational
Expires: 24 September 2026

C. Hood
Nomotic, Inc.

23 March 2026

AGTP Web3 Bridge Specification
draft-hood-agtp-web3-bridge-00

Abstract

The Agent Transfer Protocol (AGTP) uses a PKI-based trust model: agent identity is anchored to DNS-verified domain ownership and CA-issued X.509 certificates. Web3 systems offer an alternative identity model based on blockchain address ownership, smart contract verification, and decentralized naming systems including the Ethereum Name Service (ENS) and Unstoppable Domains. This document specifies the AGTP Web3 Bridge: a framework for mapping Web3 identity anchors to AGTP trust tiers, resolving Web3 names to canonical AGTP Agent-IDs, and operating AGTP sessions with agents whose identity is anchored to blockchain rather than DNS. Web3-anchored agents are treated as Trust Tier 2 (Org-Asserted) in the absence of additional verification. This document also defines the conditions under which a Web3 identity MAY be elevated to Trust Tier 1 through a hybrid verification procedure.

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 24 September 2026.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Two Identity Models 2
1.2. Scope and Status 3
2. Terminology 3
3. Web3 Identity Anchors and AGTP Trust Tiers 4
3.1. Default Trust Tier Assignment 4
3.2. Trust Tier 1 Elevation for Web3 Agents 5
4. Name Resolution 5
4.1. ENS Resolution 5
4.2. Unstoppable Domains Resolution 6
4.3. DID Resolution 6
5. Operating AGTP Sessions with Web3-Anchored Agents 7
5.1. Session Establishment 7
5.2. Authority-Scope Constraints 7
5.3. Governance Token Compatibility 7
6. Security Considerations 7
6.1. Blockchain Reorganization 8
6.2. ENS Name Expiry 8
6.3. Private Key Compromise 8
6.4. Smart Contract Vulnerabilities 8
7. IANA Considerations 9
8. References 9
8.1. Normative References 9
8.2. Informative References 9
Appendix A. Web3 Ecosystem Status Note 10
Author's Address 10

1. Introduction

1.1. Two Identity Models

AGTP's default trust model is PKI-based. An agent's identity is anchored to a real-world domain (e.g., acme.tld), verified through DNS ownership challenge per, and bound to a CA-signed certificate chain. This model inherits decades of web PKI infrastructure and integrates cleanly with enterprise certificate management systems.

Web3 systems provide a different identity model. In Web3, identity is anchored to a blockchain address: a cryptographic key pair whose public address is a first-class identifier. Ownership of a

blockchain address is proven by signing a challenge with the corresponding private key. Web3 naming systems (ENS, Unstoppable Domains) map human-readable names to blockchain addresses, analogous to DNS mapping names to IP addresses.

These models are not mutually exclusive. An organization may hold both a verified DNS domain and blockchain-anchored assets. An agent may legitimately derive its identity from either model. AGTP must interoperate with both.

1.2. Scope and Status

This document is informational. The Web3 ecosystem is evolving rapidly, and a fully normative specification would risk premature standardization of mechanisms that have not stabilized. This document defines:

* The resolution_layer field values for Web3 identity anchors (already defined in [AGTP] Section 6.6)

* Mapping rules from Web3 identity to AGTP Trust Tiers

* Name resolution procedures for ENS and Unstoppable Domains

* A hybrid verification procedure for Trust Tier 1 elevation

* Security considerations specific to Web3-anchored agents

Implementers *MAY* use this document as guidance. A future normative revision will be issued as the Web3 identity landscape stabilizes.

2. Terminology

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.

Blockchain Address: A cryptographic public key hash serving as a first-class identifier on a blockchain network (e.g., an Ethereum address of the form 0x... or a Solana address in base58 encoding).

ENS (Ethereum Name Service): A distributed naming system built on the Ethereum blockchain that maps human-readable names (e.g., acme.eth) to Ethereum addresses and other records. Defined in [EIP-137].

Unstoppable Domains: A blockchain-based naming system providing human-readable domain names (e.g., acme.crypto, acme.nft) anchored to blockchain addresses.

DID (Decentralized Identifier): A globally unique identifier defined by [W3C-DID] that enables verifiable, decentralized digital identity without dependence on a centralized registry.

Web3 Trust Anchor: A blockchain address, ENS name, Unstoppable Domain name, or DID that serves as the primary identity anchor for a Web3-registered agent.

3. Web3 Identity Anchors and AGTP Trust Tiers

3.1. Default Trust Tier Assignment

[AGTP] Section 6.6 defines the resolution_layer field in the Agent Manifest Document and specifies that Web3-anchored agents *MUST* be treated as Trust Tier 2 (Org-Asserted) in the absence of additional verification:

resolution_layer Value	Default Trust Tier	Notes
dns	Tier 1 (if DNS challenge passed)	Standard AGTP default
pki	Tier 2	PKI without DNS challenge
web3-ens	Tier 2	ENS name ownership verified
web3-unstoppable	Tier 2	Unstoppable Domains ownership verified
web3-did	Tier 2	DID method-specific verification
agtp-registry	Tier 2	Direct registry registration, no domain anchor

Table 1: resolution_layer Values and Default Trust Tiers

Trust Tier 2 means the agent's identity is asserted and verifiable (ownership of the blockchain address is provable) but the agent has not been verified as representing a specific real-world organization through DNS. The trust_warning: "org-label-unverified" field *MUST* appear in the Agent Manifest Document for all Web3-anchored agents at default Trust Tier 2.

3.2. Trust Tier 1 Elevation for Web3 Agents

A Web3-anchored agent *MAY* be elevated to Trust Tier 1 through a hybrid verification procedure that combines blockchain address ownership proof with DNS ownership verification:

1. The agent operator proves ownership of the blockchain address by signing an AGTP-issued challenge with the corresponding private key.

2. The agent operator publishes a DNS TXT record at _agtp.[domain.tld] containing the blockchain address:

_agtp.acme.tld. IN TXT "agtp-web3=0x1a2b3c...; chain=ethereum"

1. The AGTP governance platform verifies both the blockchain signature and the DNS TXT record.

2. On successful dual verification, the agent is registered at Trust Tier 1 with resolution_layer: web3-ens (or equivalent) and the DNS anchor recorded in the Agent Manifest Document.

This hybrid procedure establishes that the same entity controls both the blockchain address and the DNS domain, providing a trust level equivalent to standard DNS-anchored verification.

4. Name Resolution

4.1. ENS Resolution

ENS names (e.g., acme.eth) resolve to Ethereum addresses through the ENS registry smart contract. AGTP implementations that support ENS resolution *MUST*:

1. Query the ENS registry contract for the address record associated with the ENS name.

2. Verify that the resolved address matches the blockchain_address field in the agent's registration record.

3. Verify that the agent's canonical Agent-ID is recorded in the ENS name's text records under the key agtp-agent-id.

ENS text record format:

Key: agtp-agent-id
Value: 3a9f2c1d8b7e4a6f...

AGTP resolution *MUST* treat the ENS text record as informational only. The canonical Agent-ID in the AGTP registry is authoritative. If the ENS text record conflicts with the AGTP registry, the AGTP registry value *MUST* be used.

4.2. Unstoppable Domains Resolution

Unstoppable Domains names resolve through a blockchain registry contract specific to each domain extension (.crypto, .nft, .x, etc.). AGTP implementations that support Unstoppable Domains resolution *MUST* follow the same verification procedure as ENS, adapted for the specific registry contract of the domain extension.

Unstoppable Domains record format:

Key: agent.agtp.id
Value: 3a9f2c1d8b7e4a6f...

4.3. DID Resolution

W3C Decentralized Identifiers [W3C-DID] provide a method-agnostic framework for decentralized identity. AGTP implementations that support DID resolution *MUST*:

1. Resolve the DID Document using the DID method-specific resolver.

2. Extract the AGTP-specific service endpoint from the DID Document:

```
{
  "service": [
    {
      "id": "#agtp",
      "type": "AgentTransferProtocol",
      "serviceEndpoint": "agtp://agtp.acme.tld/agents/my-agent",
      "agtp_agent_id": "3a9f2c1d8b7e4a6f..."
    }
  ]
}
```

1. Resolve the serviceEndpoint URI to the agent’s canonical AGTP Agent Manifest Document.

2. Verify that the agtp_agent_id in the DID Document matches the canonical_id in the Agent Manifest Document.

5. Operating AGTP Sessions with Web3-Anchored Agents

5.1. Session Establishment

AGTP sessions with Web3-anchored agents follow the standard AGTP session model defined in [AGTP]. The resolution_layer field in the Agent Manifest Document declares the trust anchor type; the requesting agent *MUST* retrieve and verify the manifest before establishing a session.

If the requesting agent requires Trust Tier 1 (e.g., for financial transactions or cross-organization delegation), it *MUST* reject connection attempts from Tier 2 Web3-anchored agents unless the hybrid verification described in Section 3.2 has been completed and is reflected in the agent’s Trust Tier.

5.2. Authority-Scope Constraints

Web3-anchored agents at Trust Tier 2 *MUST NOT* be granted authority scopes above documents:query and knowledge:query without AGTP-CERT cryptographic identity binding per [AGTP-CERT], as specified in [AGTP] Section 6.1.6.

AGTP-CERT binding for Web3-anchored agents follows the same certificate issuance process as for DNS-anchored agents, with the blockchain address ownership proof substituted for or supplemented by the DNS challenge.

5.3. Governance Token Compatibility

Governance Tokens issued for Web3-anchored agents follow the standard Governance Token format defined in [AGTP] Section 6.7.7. The agent_id field in the Governance Token *MUST* match the agent’s canonical AGTP Agent-ID (the 256-bit hash form), not the blockchain address or Web3 name.

6. Security Considerations

6.1. Blockchain Reorganization

Blockchain networks are subject to reorganization events in which recently confirmed transactions may be reversed. In AGTP context, a blockchain reorganization could theoretically reverse the publication of an ENS text record or Unstoppable Domains record used in agent verification.

Mitigation: AGTP implementations *SHOULD* require a minimum confirmation depth before treating blockchain-based verification as complete. The recommended minimum is 12 blocks for Ethereum mainnet. Implementations operating on proof-of-stake networks with finality guarantees *MAY* use the finality checkpoint instead of a block depth threshold.

6.2. ENS Name Expiry

ENS names require periodic renewal. If an ENS name expires and is acquired by a different party, the new owner could publish an AGTP agent ID that points to an agent the original owner registered.

Mitigation: AGTP governance platforms *MUST* monitor ENS name expiry for all registered Web3-anchored agents and treat an expired ENS name as equivalent to an expired DNS domain per [AGTP] Section 9.6. Agents under an expired ENS name *MUST* be automatically Suspended.

6.3. Private Key Compromise

A blockchain address is only as secure as its private key. Private key compromise grants an attacker the ability to prove ownership of the address and potentially re-register agents or modify ENS records.

Mitigation: Web3-anchored agent operators *SHOULD* use hardware wallets or multi-signature schemes for blockchain addresses used in AGTP registration. Private key rotation *MUST* trigger immediate agent re-registration with the new address and *MUST* be logged in the governance audit trail.

6.4. Smart Contract Vulnerabilities

ENS and Unstoppable Domains registry contracts are smart contracts. Smart contract vulnerabilities could allow attackers to modify name resolution records without controlling the associated private key.

Mitigation: AGTP implementations *SHOULD* monitor the security status of registry contracts they rely on and be prepared to treat affected resolutions as untrusted pending contract remediation. This document does not specify a normative procedure for contract vulnerability response; that is governed by the respective naming system's security policies.

7. IANA Considerations

This document defines no new IANA registrations. The resolution_layer field values web3-ens, web3-unstoppable, and web3-did are defined in [AGTP] Section 6.6.2 and do not require separate registration.

The DNS TXT record key agtp-web3 used in hybrid verification is a conventional identifier within the _agtp subdomain established by [AGTP] Section 6.1.6. No formal IANA registration is required for this key.

8. References

8.1. Normative References

[AGTP] Hood, C., "Agent Transfer Protocol (AGTP)", Work in Progress, Internet-Draft, draft-hood-independent-agtp-02, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-independent-agtp-02>.

[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/rfc/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/rfc/rfc8174>.

8.2. Informative References

[AGTP-CERT] Hood, C., "AGTP Agent Certificate Extension", Work in Progress, Internet-Draft, draft-hood-agtp-agent-cert-00, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-agent-cert-00>.

[EIP-137] Ethereum Foundation, "Ethereum Name Service", 2016, <https://eips.ethereum.org/EIPS/eip-137>.

[W3C-DID] W3C, "Decentralized Identifiers (DIDs) v1.0", 2022, <https://www.w3.org/TR/did-core/>.

Appendix A. Web3 Ecosystem Status Note

The Web3 identity landscape is evolving rapidly. ENS and Unstoppable Domains are the most widely deployed blockchain naming systems at the time of this writing, but the field is not settled. W3C DIDs provide a method-agnostic framework that may become the preferred abstraction layer for decentralized identity in agent systems.

This document is intentionally informational to avoid premature normative commitment. Implementers should treat the procedures in this document as best-current-practice guidance subject to revision as the Web3 ecosystem stabilizes.

Author’s Address

Chris Hood
Nomotic, Inc.
Email: chris@nomotic.ai
URI: https://nomotic.ai