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

C. Hood
Nomotic, Inc.

23 March 2026

AGTP Agent Certificate Extension
draft-hood-agtp-agent-cert-00

Abstract

The Agent Transfer Protocol (AGTP) base specification defines agent identity headers (Agent-ID, Principal-ID, Authority-Scope) that are self-asserted: present on every request and mandatory for logging, but not cryptographically verified at the transport layer. This document specifies the AGTP Agent Certificate Extension: an optional mechanism that binds Agent-ID, Principal-ID, and Authority-Scope to an X.509 v3 certificate presented during TLS mutual authentication. The extension enables infrastructure components including Scope-Enforcement Points (SEPs), load balancers, and governance gateways to verify agent identity and enforce authority scope without application-layer access, at O(1) cost per request header check. The extension also defines session-level revocation propagation via AGTP NOTIFY broadcast and a Certificate Transparency Log for tamper-evident governance metadata.

Note: Certain mechanisms described in this document may be subject to pending patent applications by the author. The licensor is prepared to grant a royalty-free license to implementers consistent with the IETF's IPR framework. See the IPR Notice and Section 7.

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.

Table of Contents

1. Introduction

1.1. The Identity Gap in Base AGTP

The AGTP base specification requires every request to carry Agent-ID, Principal-ID, and Authority-Scope headers. These headers are self-asserted: an AGTP client declares its identity and scope, and the server logs the declaration. In the base spec, there is no transport-layer mechanism to verify that the declared Agent-ID corresponds to a registered agent, that the Principal-ID is accurate, or that the Authority-Scope does not exceed what was granted.

This is a deliberate design choice in the core spec: self-asserted identity with mandatory logging provides a useful baseline and enables broad adoption. For many deployments, anomaly detection and audit trails over self-asserted headers are sufficient.

For higher-stakes deployments -- financial transactions, healthcare operations, legal actions, multi-organization agent federations -- the self-assertion model is insufficient. Infrastructure needs to verify agent identity and enforce scope at the transport layer without parsing application payloads.

1.2. The Agent Certificate Extension

The AGTP Agent Certificate Extension provides cryptographic identity binding at the transport layer. An AGTP Agent Certificate is an X.509 v3 certificate with agent-governance-specific extensions. It is presented during TLS mutual authentication, enabling the server and any AGTP-aware infrastructure component to verify the agent's identity and authority scope from the certificate alone, without inspecting the request headers or body.

This document specifies:

* The AGTP Agent Certificate schema and X.509 v3 extension fields
* The certificate issuance and renewal protocol
* The authority scope commitment mechanism for O(1) per-request scope enforcement
* Session-level revocation propagation via AGTP NOTIFY
* The AGTP Certificate Transparency Log (AGTP-CTL)

1.3. Scope

This extension is OPTIONAL. Core AGTP implementations that do not implement this extension remain fully compliant with [AGTP]. The extension is required only for Trust Tier 1 agent identity verification and for SEP-enforced scope constraint without application-layer access.

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.

AGTP Agent Certificate: An X.509 v3 certificate carrying agent-governance-specific extensions, presented during TLS mutual authentication to establish cryptographic agent identity and authority scope at the transport layer.

Scope-Enforcement Point (SEP): An AGTP-aware infrastructure component that enforces Authority-Scope constraints on AGTP requests. With the Agent Certificate Extension, SEPs verify scope from the certificate at O(1) cost per request without application-layer access.

Authority-Scope Commitment: A cryptographic binding of the agent’s declared Authority-Scope tokens to the Agent Certificate, enabling SEPs to verify scope token membership after a single session-establishment signature verification.

AGTP Certificate Transparency Log (AGTP-CTL): A Merkle-tree-based append-only log of issued AGTP Agent Certificates, providing tamper-evident public accountability for certificate issuance and revocation.

3. AGTP Agent Certificate Schema

3.1. Certificate Structure

The AGTP Agent Certificate is an X.509 v3 certificate per [RFC5280] with the following subject fields and extensions:

3.1.1. Standard Subject Fields

Field	Required	Value
CN (Common Name)	*MUST*	Human-readable agent label
O (Organization)	*MUST*	Organization name (maps to principal_org)
OU (Organizational Unit)	*MAY*	Governance zone identifier
emailAddress	*SHOULD*	Contact email of the responsible principal

Table 1: AGTP Agent Certificate Subject Fields

3.1.2. Agent-Governance X.509 v3 Extensions

The following extensions are defined for AGTP Agent Certificates. OIDs for these extensions are specified in Section 8 (IANA Considerations).

subject-agent-id (CRITICAL) The canonical AGTP Agent-ID derived from the governance-layer Birth Certificate's certificate_hash. This is the transport-layer Agent-ID used in the AGTP Agent-ID header. Format: hex-encoded 256-bit value.

principal-id (CRITICAL) The identifier of the human principal accountable for this agent's actions. Maps to the AGTP Principal-ID header. Format: UTF-8 string, maximum 256 characters.

authority-scope-commitment (CRITICAL) A cryptographic commitment to the agent's Authority-Scope token set, enabling SEPs to verify token membership without storing the full scope list per session. The commitment is computed as an Ed25519 signature over the canonical lexicographically sorted Authority-Scope token set. SEPs verify token membership by checking the token against the commitment after session-establishment signature verification.

governance-zone (NON-CRITICAL) The governance zone identifier in which the agent is registered. Format: UTF-8 string following the zone: prefix convention.

trust-tier (NON-CRITICAL) The agent's Trust Tier (1, 2, or 3) as defined in [AGTP] Section 6.2. Format: INTEGER.

archetype (NON-CRITICAL) The agent's behavioral archetype as defined in [AGTP] Section 6.7.3. Format: UTF-8 string; one of: assistant, analyst, executor, orchestrator, monitor.

activation-certificate-id (NON-CRITICAL) Cross-layer reference to the governance-layer Birth Certificate certificate_hash. Enables audit reconstruction without a cryptographic dependency between the transport certificate and the governance certificate. Format: hex-encoded 256-bit value.

agtp-ctl-sct (NON-CRITICAL) Signed Certificate Timestamp from the AGTP Certificate Transparency Log, proving the certificate was submitted to the AGTP-CTL before delivery. Format: SCT structure per [RFC6962] Section 3.2.

4. Certificate Issuance Protocol

4.1. Eligibility

Certificate Signing Requests (CSRs) for AGTP Agent Certificates *MUST* only be accepted for agents in Active lifecycle state in the AGTP registry. A governance platform *MUST* verify the agent's lifecycle state at CSR submission time and *MUST* reject CSRs for agents in Suspended, Revoked, or Deprecated state.

4.2. Issuance Steps

1. The governance platform generates a key pair for the agent (or accepts a CSR with an agent-generated key pair).

2. The governance platform populates the certificate subject fields and all AGTP-specific extensions from the agent's Birth Certificate and registry record.

3. The governance platform verifies that the proposed authority-scope- commitment does not exceed the scope granted in the agent's Birth Certificate. If it does, the CSR *MUST* be rejected.

4. The governance platform signs the certificate using its issuing CA key per [RFC5280].

5. The governance platform submits the certificate to the AGTP-CTL and obtains a Signed Certificate Timestamp (SCT).

6. The SCT is embedded in the agtp-ctl-sct extension and the certificate is delivered to the agent.

7. The governance platform publishes the new certificate to the agent’s registry record, triggering a registry state update.

4.3. Certificate Validity

AGTP Agent Certificates *SHOULD* have a validity period of no more than 90 days. Short validity periods limit the exposure window of a compromised certificate and reduce reliance on revocation mechanisms. Renewal *SHOULD* begin at 80% of the validity period.

Certificate renewal carries forward the predecessor’s subject-agent-id and activation-certificate-id unchanged. The renewed certificate receives a new serial number, new validity period, and a new SCT.

5. TLS Integration

5.1. Mutual Authentication

AGTP connections using the Agent Certificate Extension *MUST* use TLS 1.3 mutual authentication. The agent presents its AGTP Agent Certificate as the client certificate during the TLS handshake.

The server verifies the client certificate chain against the issuing CA trust anchors. Following successful handshake:

1. The server extracts the subject-agent-id extension value and verifies it matches the Agent-ID header on the first request.

2. The server extracts the principal-id extension value and verifies it matches the Principal-ID header on the first request.

3. The server extracts the authority-scope-commitment extension value and uses it to verify Authority-Scope header tokens on each request.

Any mismatch between certificate extension values and AGTP header values *MUST* cause the server to return 401 Unauthorized and *MUST* be logged.

5.2. Scope Enforcement at SEPs

A SEP operating with the Agent Certificate Extension verifies Authority- Scope at O(1) cost per request:

1. At session establishment, the SEP extracts the authority-scope-commitment from the client certificate. (One-time per session.)

2. On each request, the SEP checks whether the Authority-Scope header tokens are covered by the commitment. (O(1) per request after session setup.)

3. If any header token is not covered by the commitment, the SEP returns 451 Scope Violation without forwarding the request to the application layer.

This enables governance enforcement at line rate without application-layer parsing.

6. Revocation and Session Propagation

6.1. Revocation Events

An AGTP Agent Certificate *MUST* be revoked when any of the following occur:

* The agent’s lifecycle state transitions to Revoked or Deprecated

* The Birth Certificate’s certificate_hash is invalidated

* The agent’s authority-scope-commitment requires modification

* The principal requests revocation

* A trust violation is detected

6.2. Session-Level Revocation Propagation

Standard certificate revocation (CRL, OCSP) operates on polling cycles, leaving a window during which revoked certificates may still be used. For agent systems, this window is unacceptable for high-stakes operations.

AGTP Agent Certificate revocation *MUST* be propagated to active sessions via AGTP NOTIFY broadcast:

1. The governance platform issues a revocation event to the AGTP-CTL.

2. The governance platform broadcasts an AGTP NOTIFY to all infrastructure components holding active sessions for the revoked certificate’s subject-agent-id:

```
{
  "method": "NOTIFY",
  "parameters": {
    "recipient": "infrastructure:broadcast",
    "content": {
      "event_type": "certificate_revoked",
      "subject_agent_id": "[agent-id]",
      "certificate_serial": "[serial]",
      "revocation_reason": "[reason]",
      "effective_at": "2026-04-01T00:00:00Z"
    },
    "urgency": "critical"
  }
}
```

1. Infrastructure components receiving this NOTIFY *MUST* immediately terminate all active sessions for the identified subject-agent-id. Session termination *MUST* occur before the next request is processed on the affected session.

2. The target revocation-to-termination latency is 30 seconds. This is materially shorter than standard CRL or OCSP cache-based models.

6.3. Session Manager Responsibilities

AGTP Session Managers in deployments using the Agent Certificate Extension *MUST* maintain a per-certificate-serial active session registry. On receiving a revocation NOTIFY, the Session Manager *MUST* terminate all sessions associated with the revoked serial before processing the next request on any affected session.

7. AGTP Certificate Transparency Log

7.1. Purpose

The AGTP Certificate Transparency Log (AGTP-CTL) is an append-only, Merkle-tree-based log of all issued AGTP Agent Certificates. It provides tamper-evident public accountability for certificate issuance and revocation, enabling:

* Fleet-level analytics: population-wide trust score distributions, archetype frequencies, governance zone composition

* Anomaly detection: detection of certificates issued outside normal governance flows

* Audit reconstruction: verifiable history of certificate issuance and revocation for compliance

7.2. Log Structure

The AGTP-CTL follows the Certificate Transparency log structure defined in [RFC6962], adapted for agent governance metadata. Each leaf entry contains:

* Certificate serial number
* subject-agent-id
* principal-id
* governance-zone
* trust-tier
* archetype
* activation-certificate-id
* Issuance timestamp
* Revocation status (updated on revocation)
* Merkle leaf hash

The leaf hash covers all governance metadata fields. Any modification to a log entry is detectable by any party with access to the log.

7.3. Privacy Considerations

The principal-id field in the AGTP-CTL leaf entries *MAY* be pseudonymized to protect individual principal identity while maintaining audit integrity. Pseudonymous principal IDs *MUST* be resolvable by authorized parties (regulators, compliance auditors) via a trusted resolution service. The pseudonymization mapping *MUST* be maintained separately from the _*RECOMMENDED_ public log.

8. Security Considerations

8.1. Certificate Pinning

Deployments with strict security requirements *MAY* implement certificate pinning for known agents, rejecting connections from agents whose certificate serial or key does not match a pre-registered value. Certificate pinning interacts with renewal; pinned agents *MUST* update pins on each certificate renewal before the old certificate expires.

8.2. Scope Commitment Forgery

The authority-scope-commitment is an Ed25519 signature over the canonical scope token set, signed by the governance platform's issuing key. An attacker who compromises the issuing key can forge scope commitments. Issuing key compromise *MUST* trigger immediate revocation of all certificates issued by that key and issuance of replacement certificates from a new key pair. Issuing keys *SHOULD* be stored in hardware security modules.

8.3. Cross-Certificate Confusion

An agent MAY hold multiple certificates (e.g., during renewal overlap). Infrastructure *MUST* use the subject-agent-id extension value as the authoritative agent identifier, not the certificate subject CN, to prevent cross-certificate identity confusion during renewal windows.

8.4. IPR Notice

Certain mechanisms described in this document may be subject to pending patent applications by the author, specifically: the authority-scope-commitment mechanism and the session-level revocation propagation architecture. The licensor (Chris Hood / Nomotic, Inc.) is prepared to grant a royalty-free license to implementers for any patent claims covering these mechanisms, consistent with the IETF's IPR framework under the normative reference in [AGTP] Section 8.7.

9. IANA Considerations

9.1. X.509 Extension OID Registrations

This document requests registration of the following Object Identifiers in the IANA Private Enterprise Numbers registry or an appropriate OID arc for IETF use. Specific OID assignments are subject to IANA allocation:

Extension	OID (TBD)	Critical
subject-agent-id	TBD	Yes
principal-id	TBD	Yes
authority-scope-commitment	TBD	Yes
governance-zone	TBD	No
trust-tier	TBD	No
archetype	TBD	No
activation-certificate-id	TBD	No
agtp-ctl-sct	TBD	No

Table 2: AGTP Agent Certificate X.509 Extension OIDs

10. References

10.1. 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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[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>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/rfc/rfc8555>.

10.2. Informative References

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/rfc/rfc6962>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

Appendix A. Relationship to Birth Certificate

The AGTP Agent Certificate and the Agent Birth Certificate (defined in [AGTP] Section 6.7) are complementary but distinct:

Property	Birth Certificate	Agent Certificate
Layer	Governance / registry	Transport / TLS
Format	JSON document	X.509 v3
Issued by	Governance platform	Governance platform CA
Lifetime	Permanent (archived on revoke)	90 days (renewable)
Carries	Full identity + archetype + scope	Transport identity + scope commitment
Purpose	Genesis record, registry anchor	TLS mutual auth, SEP enforcement
Cross-reference	certificate_hash	activation-certificate-id

Table 3

The activation-certificate-id field in the Agent Certificate contains the Birth Certificate's certificate_hash, creating a verifiable cross-layer link between the transport certificate and the governance record without introducing a cryptographic dependency that would require re-issuance of the Agent Certificate whenever the governance record is updated.

Author's Address

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