Independent Submission
Internet-Draft
Intended status: Informational
Expires: 27 November 2026

C. Hood
Nomotic, Inc.

26 May 2026

AGTP Agent Certificate Extension
draft-hood-agtp-agent-cert-01

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 27 November 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 bound to this certificate. The canonical Agent-ID is the 256-bit SHA-256 hash of the canonical-form Agent Genesis document, per [AGTP]. Format: 64 lowercase hexadecimal characters. A relying party that parses an AGTP Agent Certificate *MUST* treat the value carried in this extension as the authoritative Agent-ID for the agent.

The certificate’s public key is independent of the canonical Agent-ID: the same Agent Genesis (and therefore the same canonical Agent-ID) *MAY* back successive certificates issued with different key pairs across renewal cycles. The TLS layer *MUST NOT* require that the public key hash equal the value carried in subject-agent-id; the equality held only in earlier drafts that derived Agent-ID from the cert public key, and that derivation has been retired in favor of the Genesis-hash derivation specified in [AGTP].

Defense against substitution attacks (in which a CA-signed certificate is presented with a forged subject binding) is performed at the application layer: a relying party that cares about Agent Genesis binding *MUST* retrieve the Agent Genesis for the asserted Agent-ID (via DISCOVER /genesis on the agent’s home server, or from a local registry copy), recompute sha256(canonical_form(Agent_Genesis_without_ signature)), and

confirm the result equals the value in subject-agent-id. The relying party *MUST* additionally verify the Agent Genesis signature against the recognized issuer key for the agent's governance platform. SEPs and other transport-layer enforcers *MAY* defer this check to application-layer components but *MUST* ensure the check is performed before treating the asserted Agent-ID as authoritative for governance-sensitive decisions. A certificate whose Agent Genesis binding cannot be verified *MUST* be treated as transport-only: usable for TLS authentication but carrying no authoritative governance identity.

principal-id (CRITICAL) The identifier of the human or organizational principal accountable for this agent's actions. Carried on the wire as part of the Owner-ID identifier chain; see [AGTP]. Format: UTF-8 string, maximum 256 characters.

This field identifies the agent's _owner_ — the principal recorded on the Agent Genesis as accountable for the agent's existence. It is distinct from the acting_principal_id field on extended Attribution-Records per [AGTP-IDENTIFIERS], which identifies the principal on whose behalf the agent acts for a _specific request_, typically lifted from an external OAuth or OIDC credential per the composition section in [AGTP]. The two principals are independent: the owner is permanent and certificate-bound; the acting principal is per-request and credential-bound. A request *MAY* carry both, neither, or one without the other; their semantics do not interact.

authority-scope-commitment (CRITICAL) The agent's committed Authority-Scope as a canonical token list. The extension value is the lexicographically sorted, comma-separated, UTF-8-encoded list of Authority-Scope tokens the agent is authorized to assert. The integrity of the committed token list is provided by the certificate's enclosing CA signature; no separate signature is carried in the extension. A SEP enforces Authority-Scope at line rate by parsing the extension value once per session and checking each request's Authority-Scope header tokens against the parsed set (Section 5.2). Format: UTF-8 string of comma- separated tokens, each token matching the Authority-Scope token grammar defined in [AGTP].

governance-zone (NON-CRITICAL) The governance zone identifier in which the agent is registered. SEPs *MAY* enforce that the request's AGTP-Zone-ID header matches this value; a mismatch results in a 457 Zone Violation per Section 5.2. 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]. Format: INTEGER.

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

activation-certificate-id (NON-CRITICAL) Cross-layer reference to the Agent Genesis lifecycle event that activated this certificate. Enables audit reconstruction from a transport certificate back to the Agent Genesis activation record without introducing a cryptographic dependency that would force certificate re-issuance whenever the Agent Genesis lifecycle state is updated. Format: 64 lowercase hexadecimal characters.

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. Implementations that issue certificates carrying this extension *MUST* populate the value with a syntactically valid SCT structure; cryptographic verification of the SCT against an operating AGTP-CTL is deferred to a future revision of this document. Until that revision, relying parties *MAY* parse the extension for record-keeping purposes but *MUST NOT* treat its presence or absence as authoritative for trust decisions.

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 Agent Genesis and registry record.

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

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

5. If an AGTP Certificate Transparency Log is operating, the governance platform submits the certificate to the AGTP-CTL and obtains a Signed Certificate Timestamp (SCT). Until AGTP-CTL is operating, this step is omitted and the agtp-ctl-sct extension is not populated.

6. When an SCT is obtained, it is embedded in the agtp-ctl-sct extension and the certificate is delivered to the agent. Otherwise the certificate is delivered without the agtp-ctl- sct extension.

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 and (optionally) governance zone at O(1) cost per request:

1. At session establishment, the SEP extracts the authority-scope-commitment from the client certificate and parses the comma-separated token list once. The SEP also extracts the governance-zone extension if present and zone enforcement is configured. (One-time per session.)

2. On each request, the SEP checks whether the Authority-Scope header tokens are a subset of the parsed commitment token set. (O(1) per request after session setup.)

3. If any header token is not in the commitment token set, the SEP returns *455 Scope Violation* without forwarding the request to the application layer.

4. If governance-zone enforcement is configured and the request’s AGTP-Zone-ID header does not match the value carried in the certificate’s governance-zone extension, the SEP returns *457 Zone Violation* without forwarding the request.

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

A certificate that lacks the AGTP-specific extensions is a valid TLS client certificate but carries no SEP-enforceable governance metadata. SEP enforcement of authority-scope-commitment and governance-zone is purely additive: in the absence of those extensions, scope and zone are enforced through application-layer checks against the agent’s Agent Identity Document per [AGTP]. Deployments *MAY* mix certificates with and without AGTP extensions; the SEP layer treats each session by what its certificate carries.

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 Agent Genesis 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 extension carries the agent’s committed Authority-Scope token list. Integrity of the commitment relies on the certificate’s enclosing CA signature: tampering with the extension value invalidates the certificate signature and causes the certificate to be refused by any conforming verifier.

An attacker who compromises the issuing CA key can forge scope commitments by issuing fraudulent certificates with arbitrary extension values. 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. The AGTP Certificate Transparency Log (Section 7), once operating, provides an additional detection surface for unauthorized issuance: a forged certificate that does not appear in the log is detectable by any party that performs log-inclusion checks.

8.3. Cross-Certificate Confusion

An agent MAY hold multiple certificates simultaneously. Renewal overlap is one cause; key rotation under a stable Agent Genesis is another. Because the canonical Agent-ID is bound to the Agent Genesis rather than to any specific cert key pair, successive certificates for the same agent *MUST* carry the same value in subject-agent-id and *MAY* carry different public keys. Infrastructure *MUST* use the subject-agent-id extension value as the authoritative agent identifier, not the certificate subject CN, and *MUST NOT* treat key differences across certificates for the same Agent-ID as evidence of an identity mismatch.

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.

9. IANA Considerations

9.1. X.509 Extension OID Registrations

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

Until IANA allocation is complete, implementations *MUST* use provisional OIDs under the ITU-T UUID arc, derived deterministically by UUIDv5 ([RFC4122]) under a fixed AGTP namespace UUID and the extension’s canonical short name. The resulting integer-encoded UUID is appended to the arc prefix 2.25 to form the provisional OID (2.25.{uuid_int}). The derivation is reproducible across

implementations from the extension short name alone, allowing independent implementations to interoperate without a central allocation step. When IANA allocates standards-tree OIDs, those values replace the provisional UUID-derived OIDs in a future revision of this document; relying parties *SHOULD* accept both the provisional and the IANA-allocated OIDs through a transition window declared in that revision.

Extension	OID (provisional / IANA)	Critical
subject-agent-id	UUIDv5-derived (TBD allocation)	Yes
principal-id	UUIDv5-derived (TBD allocation)	Yes
authority-scope-commitment	UUIDv5-derived (TBD allocation)	Yes
governance-zone	UUIDv5-derived (TBD allocation)	No
trust-tier	UUIDv5-derived (TBD allocation)	No
archetype	UUIDv5-derived (TBD allocation)	No
activation-certificate-id	UUIDv5-derived (TBD allocation)	No
agtp-ctl-sct	UUIDv5-derived (TBD allocation)	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-08, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-independent-agtp-08>.

[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>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/rfc/rfc4122>.

[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

[AGTP-API] Hood, C., "AGTP-API: Verbs, Paths, Endpoints, and Synthesis", Work in Progress, Internet-Draft, draft-hood-agtp-api-01, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-api-01>.

[AGTP-IDENTIFIERS] Hood, C., "AGTP Identifier Stack and Attribution-Record", Work in Progress, Internet-Draft, draft-hood-agtp-identifiers-01, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-identifiers-01>.

[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 Agent Genesis

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

Property	Agent Genesis	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
Identifier	Canonical Agent-ID (256-bit SHA-256 of canonical Agent Genesis)	subject-agent-id extension carries the canonical Agent-ID
Cross-reference to lifecycle event	(originating issuance event in AGTP-LOG)	activation-certificate-id extension

Table 3

The subject-agent-id extension carries the canonical Agent-ID (256-bit SHA-256 hash of the canonical Agent Genesis), creating a direct binding between the transport certificate and the governance identity. The activation-certificate-id extension carries a reference to the lifecycle event that activated this certificate,

allowing audit reconstruction back to the activation record without introducing a cryptographic dependency that would force certificate re-issuance whenever the Agent Genesis lifecycle state is updated.

Appendix B. Changes from v00

Version 01 is a drift-cleanup revision. The certificate schema, issuance protocol, and revocation propagation mechanisms are unchanged. Clarifications align spec wording with deployed implementation behavior; one normative item (authority-scope-commitment representation) tracks the implementation as the working interpretation and is open to revision.

B.1. Substantive Changes

The following substantive changes were made:

1. *authority-scope-commitment representation.* The extension value is now defined as the lexicographically sorted, comma-separated, UTF-8-encoded list of Authority-Scope tokens. Integrity is provided by the certificate's enclosing CA signature, not by a separate Ed25519 signature carried in the extension. The earlier detached-signature framing is withdrawn. SEP enforcement parses the token list once per session and checks request tokens by set membership; the operational contract is unchanged for relying parties, only the encoding of the commitment value is changed.

2. *subject-agent-id decoupled from certificate public key; substitution defense moved to application layer.* Earlier drafts implied that the canonical Agent-ID could be derived from the certificate public key and that the TLS layer must refuse certificates whose subject-agent-id disagreed with that derivation. Under the current Agent Genesis taxonomy, the canonical Agent-ID is sha256(canonical_form(Agent_Genesis_without_signature)) and is independent of any specific cert key pair. The subject-agent-id extension is authoritative when present; the cert public key is independent and renewable. The substitution-attack defense is performed at the application layer by retrieving the Agent Genesis (via DISCOVER /genesis per [AGTP-API] or a local registry copy), recomputing the canonical hash, and verifying the Agent Genesis signature against the recognized issuer key. The Cross-Certificate Confusion security consideration is updated accordingly: successive certificates for the same agent *MUST* carry the same subject-agent-id and *MAY* carry different public keys.

3. *Birth Certificate terminology retired.* All references to the Agent Birth Certificate have been replaced by Agent Genesis, matching the locked taxonomy in [AGTP] (Agent Genesis is the permanent signed governance-layer origin document; the canonical Agent-ID is its 256-bit SHA-256 hash; the Agent Certificate is the X.509 v3 transport credential bound to that Agent-ID). The Relationship to Birth Certificate appendix is renamed and rewritten as Relationship to Agent Genesis.

4. *SEP status codes updated to v07 numbering.* Scope Enforcement at SEPs now returns *455 Scope Violation* (previously 451) and adds *457 Zone Violation* for certificates carrying the governance-zone extension when the request's AGTP-Zone-ID header disagrees with the certificate. The status code renumbering propagates the v06 → v07 change in [AGTP].

5. *SEP enforcement made additive.* A new paragraph in Section 5.2 makes explicit that a certificate without AGTP-specific extensions is a valid TLS client certificate and is enforced through application-layer checks against the Agent Identity Document. Deployments may mix certificates with and without AGTP extensions.

6. *activation-certificate-id semantics clarified.* The field is now defined as a cross-layer reference to the Agent Genesis lifecycle event that activated this certificate, rather than to a certificate_hash field that no longer exists under the locked taxonomy. The relying-party contract is unchanged: a 64-hex value suitable for cross-layer audit reconstruction.

7. *agtp-ctl-sct cryptographic verification deferred.* The extension may be carried and parsed for record-keeping purposes, but verification against an operating AGTP-CTL is deferred to a future revision. The Issuance Protocol is updated to make AGTP-CTL submission and SCT embedding conditional on AGTP-CTL availability.

8. *Provisional OID strategy introduced.* OIDs for the eight extensions are derived deterministically as UUIDv5 values under a fixed AGTP namespace and the extension's canonical short name, placed under the ITU-T UUID arc 2.25.{uuid_int}. This permits independent implementations to interoperate without a central allocation step. The provisional OIDs will be replaced by IANA-allocated standards-tree OIDs in a future revision.

9. *Normative reference to [AGTP] updated to v08.*
Section references that pointed at v02 / v06 section numbers (Section 6.2, Section 6.7, Section 6.7.3, Section 8.7) are

removed; cross-references now name the companion document and the concept rather than a specific section number, since section structure in [AGTP] continues to evolve. RFC 4122 added to normative references to support the OID derivation.

B.2. Wire Format Compatibility

The change to authority-scope-commitment (item 1) is the only wire-format-visible change in this revision. Verifiers that previously expected an Ed25519 signature in the extension value will not parse certificates carrying the sorted-token-list form. v00 issuers and verifiers cannot interoperate with v01 issuers and verifiers without an update. Because no production certificates were issued under the v00 commitment encoding, this revision treats the change as a clarification rather than a breaking transition.

All other changes are editorial or specify operational behavior that v00 left unspecified.

Author’s Address

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