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

C. Hood
Nomotic, Inc.

26 May 2026

AGTP Merchant Identity and Agentic Commerce Binding
draft-hood-agtp-merchant-identity-02

Abstract

The Agent Transfer Protocol (AGTP) specifies the sending side of an agentic transaction: agent identity, Authority-Scope enforcement, Budget- Limit declaration, and a signed Attribution-Record on every method invocation. The receiving side of a PURCHASE transaction -- the merchant or service provider -- has no equivalent protocol-level identity or verification mechanism. This is the merchant identity gap.

This document specifies the AGTP Merchant Identity and Agentic Commerce Binding. It defines a merchant in AGTP as an agent whose Agent Identity Document carries role: "merchant", specifies the merchant-specific fields that ride on the Agent Identity Document under that declaration, aligns Merchant Trust Tiers with AGTP Trust Tier semantics, and defines the protocol integration points at which merchant identity is verified. These include the PURCHASE method handshake, the DISCOVER method result surface, and the Attribution-Record. This document also defines the Intent-Assertion header for portable, detached principal-authorized intent, the Cart-Digest mechanism for multi-line-item transactions, and the 458 Counterparty Unverified status code. Together these mechanisms close the verification loop between agent and merchant within AGTP’s governance model.

Version 02 unifies merchant identity onto the Agent Genesis + Agent Identity Document architecture: there is no separate Merchant Genesis document type. A merchant is an agent with role: "merchant" declared in its Agent Identity Document. This reflects the architectural principle that identity is permanent (carried on Genesis) and capability is mutable (carried on the Identity Document); a role change does not re-mint an Agent-ID.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 27 November 2026.

Copyright Notice

Table of Contents

1. Introduction

1.1. The Merchant Identity Gap

AGTP today provides strong guarantees for the sending side of an agent transaction. A PURCHASE invocation carries a cryptographically derived Agent-ID, a Principal-ID identifying the accountable human or organization, an Authority-Scope declaration (including payments: purchase), a Budget-Limit enforced at invocation time, and a signed Attribution-Record retained for audit. The requesting agent’s governance context is fully expressed at the protocol layer.

The receiving side has no equivalent. An AGTP PURCHASE currently resolves to a network endpoint with no protocol-level assertion of the receiving party’s identity, lifecycle state, legal entity,

payment network acceptance, or dispute policy. An agent with payments: purchase scope will transact with any endpoint its principal (or the upstream orchestration logic) directs it toward. There is no protocol-level signal distinguishing a verified merchant of record from an endpoint that merely answers on the expected port.

This gap has direct operational consequences as agent-driven commerce scales:

* Payment networks and card issuers extending protection to agent-initiated transactions require verifiable identity on both parties to the transaction, not just the agent.

* Dispute investigation requires a cryptographically linked record of both the initiating agent and the merchant counterparty at the time of the transaction.

* Merchants suspended for fraud, chargebacks, or regulatory action have no mechanism to be removed from the agent-visible transaction surface in the absence of a governed merchant directory.

* Agents cannot distinguish a merchant whose identity has been verified from one that has merely published a service endpoint.

This document closes the gap by introducing a merchant-side identity structure that mirrors the agent-side identity structure already specified in [AGTP].

1.2. Relationship to Payment Networks

This specification is a transport-layer identity and verification mechanism for merchant counterparties. It does not define payment credential handling, tokenization, authorization messages to card networks, or settlement. Those belong to payment-rail specifications operated by issuers, networks, and acquirers.

The relationship is complementary. Payment-network programs that extend protection, fraud coverage, or dispute handling to agent-initiated transactions need verifiable identity for both the agent and the merchant. AGTP establishes verifiable agent identity through the Agent Genesis and Agent Manifest Document (see [AGTP-LOG] for the taxonomy introduced in AGTP v05). This document extends the same structural model to the merchant side, producing an Attribution-Record that names both counterparties cryptographically. Payment networks consume that record as an input to their own authorization and dispute processes; they do not need to speak AGTP to do so.

1.3. Design Principles

Structural parallelism. Merchant identity uses the same document formats, trust tiers, lifecycle states, and governance zone semantics as agent identity. A governance platform that registers agents registers merchants through the same registry and the same cryptographic machinery.

Verification at PURCHASE. Merchant identity is verified by the requesting agent immediately before executing PURCHASE. The verification result is recorded in the Attribution-Record. A verification failure is a 458 Counterparty Unverified response, not a protocol error.

Discovery surfaces both sides. The DISCOVER method defined in [AGTP-DISCOVER] returns Agent Identity Documents. This document extends DISCOVER to optionally filter results by role, allowing queries that target transactional counterparties (role: "merchant") distinctly from capability-providing agents.

Portable intent. The Intent-Assertion header carries a detached, signed summary of principal-authorized purchase intent that can be forwarded to non-AGTP counterparties (payment networks, card issuers, acquirers) as standalone evidence without requiring those counterparties to speak AGTP.

Payment-rail neutrality. Nothing in this specification binds the merchant identity model to any particular card network, digital wallet, or settlement system. Agent Identity Documents declaring role: "merchant" carry an informational accepted_payment_networks field; enforcement remains the responsibility of the payment rail.

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.

Merchant: An agent whose Agent Identity Document carries role: "merchant". The merchant is the receiving counterparty to an AGTP PURCHASE invocation. Identified by its canonical Agent-ID, which functions as the Merchant-ID on the wire.

Merchant-ID: The canonical Agent-ID of an agent whose Agent Identity

Document declares role: "merchant". Same wire format as Agent-ID per [AGTP-IDENTIFIERS]: 64-character lowercase hexadecimal. Carried in the Merchant-ID request header on PURCHASE invocations and in the Attribution-Record.

Merchant Trust Tier: A classification (1, 2, or 3) assigned to a merchant at registration time, aligned with the Agent Trust Tier semantics defined in [AGTP-TRUST]. Tier 1 requires one of three equivalent verification paths (dns-anchored, log-anchored, hybrid) per [AGTP-TRUST], plus a signed business-entity attestation from the governance platform. Tier 2 is org-asserted without cryptographic verification of organizational identity. Tier 3 is experimental and *MUST NOT* appear in production PURCHASE flows.

Intent-Assertion: A detached, signed JWT-format [RFC7519] token that summarizes principal-authorized purchase intent. Contains the principal ID, agent ID, merchant ID, item or cart digest, amount ceiling, currency, issuance timestamp, expiry, and a single-use nonce. Carried in the Intent-Assertion request header and forwardable to payment networks as standalone evidence of authenticated principal intent.

Cart-Digest: A cryptographic digest of a structured cart payload returned by a QUOTE invocation. Referenced in a subsequent PURCHASE invocation to bind the purchased cart to the quoted cart without requiring retransmission of line-item detail. Format: hash algorithm prefix followed by hex-encoded digest (e.g., sha256:3a9f2c1d...).

Counterparty Verification: The process by which an agent, before executing PURCHASE, retrieves the Agent Identity Document for the addressed merchant, verifies its signature and lifecycle state, confirms role: "merchant", and records the verification result in the Attribution-Record.

MNS (Merchant Name Service): The merchant-side analogue of the Agent Name Service defined in [AGTP-DISCOVER]. An AGTP-aware server that maintains an indexed registry of Agent Identity Documents for merchant-role agents and answers DISCOVER queries filtered on role: "merchant". An MNS *MAY* be co-located with an ANS or operated separately. Acts as a Scope- Enforcement Point for merchant discovery traffic.

3. The Merchant Identity Model

3.1. Identity Unification with Agent Identity

A merchant in AGTP is an agent whose Agent Identity Document declares role: "merchant". The merchant identity model is the agent identity model, specialized by a single capability attribute on the Agent Identity Document.

This unification reflects an architectural commitment surfaced during v07窶ｦ08 implementation: *identity is permanent; capability is mutable*. The Agent Genesis (specified in [AGTP]) is the permanent signed origin document and the basis of the canonical Agent-ID; it carries no role field because role can change over an agent’s lifetime, and forcing a role change to mint a new Agent-ID would orphan every existing audit-chain entry, certificate, and reference. The Agent Identity Document, in contrast, is a capability-bearing manifest that an operator can edit between server restarts; adding or removing the merchant role is therefore a manifest edit, not a re-issuance event.

This is a deliberate change from v01 of this document, which defined a separate Merchant Genesis document type with its own schema. The v01 model conflated identity (Genesis) with capability (merchant attributes); v02 retires the separate Merchant Genesis in favor of the unified Agent Genesis + role model.

A merchant under this revision:

* Has an Agent Genesis issued through the standard agent registration flow specified in [AGTP]. The Agent Genesis carries no merchant-specific fields.

* Has a canonical Agent-ID equal to sha256(canonical_form(Agent_Genesis_without_signature)), per [AGTP]. This canonical Agent-ID is the merchant’s Merchant-ID on the wire.

* Has an Agent Identity Document carrying role: "merchant" together with the merchant-specific fields specified below.

* Is verified at PURCHASE as a counterparty per Section 4.

3.2. Merchant Fields on the Agent Identity Document

When role: "merchant" is declared, the Agent Identity Document *MAY* carry the following additional fields. The fields are informational; payment-rail enforcement of any declared value is out of scope for this document.

Field	Required	Description
legal_entity_name	*SHOULD* (Tier 1)	Registered business name of the merchant.
merchant_category_code	*SHOULD*	ISO 18245 Merchant Category Code (or governance-zone-defined alternate).
registered_jurisdiction	*SHOULD* (Tier 1)	Jurisdiction in which the merchant is legally registered (e.g., US-DE).
accepted_payment_networks	*MAY*	Informational array of payment network identifiers the merchant represents itself as accepting.
dispute_policy_uri	*SHOULD*	AGTP or HTTPS URI of the merchant’s published dispute policy.
refund_policy_uri	*SHOULD*	AGTP or HTTPS URI of the merchant’s published refund policy.

Table 1: Merchant Fields on the Agent Identity Document

These fields *MUST NOT* appear on the Agent Identity Document unless role: "merchant" is also declared. Implementations encountering merchant-specific fields without the role declaration *MUST* ignore the merchant fields and log the inconsistency for operator review.

3.3. Merchant Trust Tiers

Merchant Trust Tiers align with the Agent Trust Tier semantics in [AGTP-TRUST]: a merchant inherits its trust_tier and verification_path from the underlying Agent Identity Document, resolved per the trust-posture loading rule in [AGTP-TRUST].

Trust Tier 1 merchant registration *MUST* satisfy two conditions beyond the Tier 1 verification requirements in [AGTP-TRUST]:

1. One of the three Tier 1 verification paths defined in [AGTP-TRUST] (dns-anchored, log-anchored, or hybrid) *MUST* be completed at registration time. The resolved verification_path field on the Agent Identity Document carries the value.

2. A governance-platform-signed attestation *MUST* record that the registering party has provided evidence of the claimed legal entity’s existence and standing. The form of that evidence (incorporation document, tax identifier, equivalent jurisdictional registration) is governance- platform-defined and *MUST* be documented in the governance zone specification. The business entity attestation is an additional requirement for merchants beyond the base AGTP verification paths, reflecting the elevated accountability needs of agentic commerce.

Trust Tier 2 merchants *MUST* have their Agent Identity Document carry a trust_warning field with value "legal-entity-unverified". Requesting agents *SHOULD* surface this warning to principals before executing a PURCHASE against a Tier 2 merchant, or *MAY* reject Tier 2 merchants entirely based on governance policy.

Trust Tier 3 merchants *MUST NOT* appear in production PURCHASE flows. They exist for development and integration testing only.

3.4. Merchant Lifecycle States

Because a merchant is an agent with role: "merchant", merchant lifecycle states are agent lifecycle states. A merchant in any state other than Active *MUST NOT* be treated as eligible to receive PURCHASE; the receiving server *MUST* return 458 Counterparty Unverified on a PURCHASE addressed to a non-Active merchant (Section 4).

State	Meaning
Active	Merchant is operational and eligible to receive PURCHASE
Suspended	Temporarily blocked (fraud review, chargeback threshold, compliance hold)
Revoked	Permanently removed; canonical Agent-ID retired
Deprecated	Business ceased operations; canonical Agent-ID retired

Table 2: Merchant Lifecycle States

3.5. Merchant URI Forms

Because a merchant is an agent, merchant URIs are agent URIs in the AGTP URI scheme defined in [AGTP]. A relying party that needs to address a merchant uses any of the agent URI forms; no separate /merchant path component is defined. The receiving server gates PURCHASE eligibility on the role: "merchant" declaration in the addressed agent's Agent Identity Document, not on URI shape.

This is a deliberate simplification from v01 of this document, which defined /merchant and /merchant/{label} URI forms. The earlier forms presupposed a separate Merchant Genesis; under the unified model they are unnecessary and have been retired.

Implementations encountering v01-style /merchant URIs *SHOULD* resolve them by treating the path component as an agent label and applying the standard agent URI resolution rules in [AGTP]. A future revision *MAY* define a discovery convention for merchant-role agents under a server (e.g., a DISCOVER filter on role); discovery filtering is not specified in this revision.

4. Counterparty Verification at PURCHASE

4.1. Verification Requirement

An agent with payments:purchase in its Authority-Scope *MUST* perform counterparty verification before executing PURCHASE against any merchant. Counterparty verification consists of:

1. Resolving the merchant URI (from the intended PURCHASE target) to retrieve the Agent Identity Document for the addressed agent.

2. Verifying the Agent Identity Document carries role: "merchant". An agent without the merchant role declaration *MUST NOT* be addressed by PURCHASE.

3. Verifying the manifest's signature against the governance platform's published key per [AGTP].

4. Verifying the merchant's lifecycle state is Active per [AGTP].

5. Verifying the merchant's resolved trust_tier meets or exceeds the threshold declared in the agent's governance policy for the current transaction amount.

6. Computing the manifest fingerprint (SHA-256 hash of the canonical Agent Identity Document bytes) and carrying it in the Merchant-Manifest-Fingerprint request header.

Any of these steps failing *MUST* result in the PURCHASE not being sent. The requesting agent's runtime *SHOULD* surface the specific verification failure to the principal or governance platform; it *MUST NOT* silently fall back to an unverified transaction.

4.2. Verification at the Receiving Server

A receiving AGTP server that accepts PURCHASE invocations *MUST*:

1. Require the Merchant-ID request header to be present.

2. Require the addressed agent to declare role: "merchant" in its Agent Identity Document. Return 458 Counterparty Unverified if the addressed agent is not a merchant.

3. Require the Merchant-Manifest-Fingerprint request header to be present and to match the SHA-256 fingerprint of the server's current Agent Identity Document for the addressed merchant.

4. Return 458 Counterparty Unverified if any required header is absent, if the Merchant-ID does not match the addressed agent's canonical Agent-ID, or if the fingerprint does not match.

This ensures that the manifest verified by the requesting agent is the same manifest the receiving server currently presents. An attack in which a requesting agent is redirected to a different endpoint than it verified is caught at the fingerprint check.

4.3. PURCHASE Request Example

The following request illustrates a verified PURCHASE invocation carrying merchant identity binding and a detached intent assertion:

```
AGTP/1.0 PURCHASE
Agent-ID: agtp://agtp.traveler.tld/agents/trip-planner
Principal-ID: usr-chris-hood
Authority-Scope: payments:purchase merchant:verify intent:assert
Session-ID: sess-trip-2026-04
Task-ID: task-purch-0421
Merchant-ID: agtp://acme.tld/merchant/acme-commerce
Merchant-Manifest-Fingerprint: sha256:3a9f2c1d8b7e4a6f...
Intent-Assertion: eyJhbGciOiJFUzI1NiIsImtpZCI6InByaW4ta2V5LTAxIn0...
Cart-Digest: sha256:7c2f9a3e1b8d4f6a...
Budget-Limit: USD=850.00
Content-Type: application/agtp+json

{
  "method": "PURCHASE",
  "task_id": "task-purch-0421",
  "parameters": {
    "cart_quote_id": "qt-7f3a9c",
    "principal_id": "usr-chris-hood",
    "amount": {"value": 842.17, "currency": "USD"},
    "payment_method": "tok-amex-default",
    "confirm_immediately": true
  }
}
```

Figure 1: PURCHASE with Merchant Identity Binding

The merchant server validates the merchant headers, accepts the purchase, and returns an Attribution-Record naming both counterparties:

```
AGTP/1.0 200 OK
Task-ID: task-purch-0421
Server-Agent-ID: agtp://acme.tld/merchant/acme-commerce
Attribution-Record: [signed attribution token]
Content-Type: application/agtp+json

{
  "status": 200,
  "task_id": "task-purch-0421",
  "result": {
    "order_id": "ORD-2026-0421-8847",
    "confirmation_code": "AQRT9X",
    "status": "confirmed",
    "amount_charged": {"value": 842.17, "currency": "USD"}
  },
  "attribution": {
    "agent_id": "agtp://agtp.traveler.tld/agents/trip-planner",
    "principal_id": "usr-chris-hood",
    "merchant_id": "agtp://acme.tld/merchant/acme-commerce",
    "merchant_fingerprint": "sha256:3a9f2c1d8b7e4a6f...",
    "intent_assertion_jti": "ia-4f7e1a2b",
    "method": "PURCHASE",
    "timestamp": "2026-04-15T14:22:18Z",
    "signature": {
      "algorithm": "ES256",
      "key_id": "merchant-key-acme-01",
      "value": "[base64-encoded-signature]"
    }
  }
}
```

Figure 2: PURCHASE Response with Dual-Party Attribution

The Attribution-Record now names the agent, the principal, and the merchant, each cryptographically bound through their respective Genesis derivatives. This is the record consumed by downstream audit, dispute resolution, and payment-network protection programs.

5. The Intent-Assertion Header

5.1. Purpose

The Intent-Assertion header carries a detached, signed representation of principal-authorized purchase intent. It exists so that non-AGTP counterparties -- payment networks, card issuers, acquiring banks, dispute processors -- can verify principal intent without parsing a full AGTP message or operating AGTP infrastructure.

An Intent Assertion is a JWT [RFC7519] signed by the principal's governance key (or a delegated signing key bound to the principal's identity) carrying the minimum field set required to link a purchase to an authenticated principal decision.

5.2. Intent Assertion Claims

Claim	Type	Description
iss	string	Issuing governance platform identifier
sub	string	Principal-ID of the authorizing principal
aud	string	Merchant-ID of the intended counterparty
agent_id	string	Agent-ID of the executing agent
item_digest	string	Hash of purchased item or cart digest
amount_ceiling	object	{value, currency} maximum authorized
nbf	integer	Not-before timestamp (seconds since epoch)
exp	integer	Expiry timestamp (seconds since epoch)
jti	string	Unique assertion identifier for anti-replay
iat	integer	Issued-at timestamp

Table 3: Intent Assertion JWT Claims

Implementations *MUST* reject Intent Assertions whose exp is in the past, whose aud does not match the Merchant-ID in the PURCHASE request, or whose agent_id does not match the Agent-ID in the PURCHASE request. Assertions *MUST* be single-use: the jti is recorded in the Attribution-Record and *MUST NOT* be accepted a second time.

Recommended validity period: 300 seconds. Intent Assertions are not designed to persist; they cover the interval between principal authorization and transaction execution.

5.3. Forwarding to Payment Networks

The Intent Assertion is structured as a standalone JWT precisely so that it can be forwarded. A payment network receiving a merchant's authorization request *MAY* require the merchant to forward the Intent Assertion alongside the standard payment message. The payment network verifies the signature against the issuing governance platform's public key and treats a valid assertion as evidence of authenticated principal intent for the purposes of that network's authorization and dispute policies.

The specific mechanism for forwarding the Intent Assertion to a payment network, and the network's treatment of a valid assertion, is out of scope for this document. What this specification guarantees is that the assertion exists, is cryptographically verifiable without AGTP, and is bound to the principal, agent, and merchant named in the PURCHASE.

6. Cart Context

6.1. The Single-Item Limitation

The PURCHASE method as defined in [AGTP-API] accepts a single item parameter and a single amount. Real-world agentic commerce transactions frequently involve multiple line items, tax, shipping, and per-line merchant-of-record variation. This document defines a Cart Context mechanism layered over the existing QUOTE and PURCHASE methods to accommodate structured carts without modifying the base method definitions.

6.2. QUOTE with Cart Payload

A requesting agent constructs a structured cart and submits it via QUOTE. The merchant server returns a signed cart_digest binding the quoted cart content to a unique quote identifier.

```
AGTP/1.0 QUOTE
Agent-ID: agtp://agtp.traveler.tld/agents/trip-planner
Principal-ID: usr-chris-hood
Authority-Scope: budget:query merchant:query
Merchant-ID: agtp://acme.tld/merchant/acme-commerce
Session-ID: sess-trip-2026-04
Task-ID: task-quote-0421
Content-Type: application/agtp+json

{
  "method": "QUOTE",
  "task_id": "task-quote-0421",
  "parameters": {
    "cart": {
      "lines": [
        {"sku": "FLIGHT-AA2847", "qty": 1, "unit_price": 487.00},
        {"sku": "HOTEL-MRTN-2N", "qty": 1, "unit_price": 298.00},
        {"sku": "CAR-COMPACT-3D", "qty": 1, "unit_price": 42.17}
      ],
      "currency": "USD",
      "tax": 15.00,
      "shipping": 0.00
    }
  }
}
```

Figure 3: QUOTE with Structured Cart

The response contains the quote identifier and the signed cart digest:

```
{
  "status": 200,
  "task_id": "task-quote-0421",
  "result": {
    "quote_id": "qt-7f3a9c",
    "cart_digest": "sha256:7c2f9a3e1b8d4f6a...",
    "total": {"value": 842.17, "currency": "USD"},
    "quote_valid_until": "2026-04-15T14:52:18Z",
    "quote_signature": {
      "algorithm": "ES256",
      "key_id": "merchant-key-acme-01",
      "value": "[base64-encoded-signature]"
    }
  }
}
```

Figure 4: QUOTE Response with Cart Digest

6.3. PURCHASE Referencing a Cart Digest

The subsequent PURCHASE invocation references the quote identifier and carries the cart digest in the Cart-Digest header, binding the purchase to the previously quoted cart without retransmission of line-item detail. The merchant server *MUST* verify the digest against its stored quote record and *MUST* reject the PURCHASE with 409 Conflict if the cart digest does not match a valid, unexpired quote.

7. DISCOVER Integration

7.1. Merchant Queries via DISCOVER

The DISCOVER method defined in [AGTP-DISCOVER] returns Agent Identity Documents. A requesting agent that wants to address a merchant counterparty filters DISCOVER results by role: "merchant":

```
AGTP/1.0 DISCOVER
Agent-ID: agtp://agtp.traveler.tld/agents/trip-planner
Principal-ID: usr-chris-hood
Authority-Scope: discovery:query
Session-ID: sess-trip-2026-04
Task-ID: task-disc-merch-01
Content-Type: application/agtp+json

{
  "method": "DISCOVER",
  "task_id": "task-disc-merch-01",
  "parameters": {
    "intent": "Ski rental in Park City accepting Amex",
    "role": "merchant",
    "merchant_category_codes": ["7999", "5941"],
    "accepted_payment_networks": ["amex"],
    "trust_tier_min": 1,
    "governance_zone": "zone:retail-verified",
    "limit": 5
  }
}
```

Figure 5: DISCOVER Query Filtering on Merchant Role

The ANS or MNS server returns a ranked result set of Agent Identity Documents whose role field equals "merchant" and that match the query constraints. Ranking follows the composite scoring model defined in [AGTP-DISCOVER], with the following adjustments for merchant queries:

* behavioral_trust_score is replaced by merchant_reliability_ score, a governance-platform-assigned score reflecting the merchant's dispute rate, chargeback history, and fulfillment track record within the governance zone.

* capability_match_score is replaced by catalog_match_score, a relevance score between the query intent and the merchant's declared catalog categories and merchant category code.

Merchant reliability scoring methodology is governance-platform-defined and *MUST* be documented in the governance zone specification. The raw score *MUST* be present in the Agent Identity Document for the merchant and signed by the governance platform; it *MUST NOT* be merchant-asserted.

7.2. Unified DISCOVER Queries

A requesting agent *MAY* issue a DISCOVER query without a role filter to receive a mixed result set containing both non-merchant agents and merchant-role agents. This is useful for workflows where the agent does not know in advance whether the capability it needs is best satisfied by a peer agent or by a merchant transaction (e.g., "find a service that can produce a translated legal document" where the answer might be either a translation agent or a document-services merchant).

Mixed result sets include a result_class field on each entry with value "agent" or "merchant", enabling the requesting agent to route each result to the appropriate downstream handling.

8. 458 Counterparty Unverified

8.1. Definition

This document registers AGTP status code 458 Counterparty Unverified. The status is returned in any of the following conditions:

* The Merchant-ID request header is absent on a PURCHASE invocation.

* The Merchant-Manifest-Fingerprint request header is absent or does not match the fingerprint of the receiving server's current Agent Identity Document for the addressed merchant.

* The Merchant-ID does not match the addressed agent's canonical Agent-ID.

* The addressed agent does not declare role: "merchant" in its Agent Identity Document.

* The agent’s pre-flight counterparty verification failed (returned by the agent’s own runtime before a PURCHASE is sent on the wire).

* The target merchant is in a non-Active lifecycle state.

* The Agent Identity Document signature is invalid.

The response body *MUST* identify the specific verification failure and *MUST* include the governance-platform-signed reason code. The requesting agent *MUST NOT* retry the PURCHASE without re-running counterparty verification against a freshly retrieved Agent Identity Document.

Status code 458 is a governance signal, not a protocol error, and *MUST* be logged by both parties. It parallels the role of 455 Scope Violation and 457 Zone Violation in the AGTP status code space: the system caught a governance condition at the protocol layer, before any state-modifying side effect.

8.2. Retry Semantics

A 458 response in the following categories is non-retryable without remediation:

* Merchant in Revoked or Deprecated lifecycle state.

* Invalid Agent Identity Document signature.

* Merchant-ID mismatch.

* Addressed agent does not declare role: "merchant".

A 458 response in the following categories is retryable after a governance-defined interval:

* Merchant in Suspended state (retry after state transitions to Active).

* Fingerprint mismatch due to a legitimate manifest update (retry after re-fetching the current Agent Identity Document).

The response body *MUST* declare retry-eligibility via a retryable boolean field and, where retryable, *MAY* declare a retry_after timestamp.

9. Security Considerations

9.1. Merchant Identity Forgery

Threat: An attacker publishes an Agent Identity Document declaring role: "merchant" and claiming to represent a legitimate merchant without having completed any of the Trust Tier 1 verification paths.

Mitigation: Trust Tier 1 registration requires one of the three verification paths defined in [AGTP-TRUST] (dns-anchored per [RFC8555], log-anchored per [RFC9162] / [RFC9943], or hybrid) plus a governance-platform-signed business entity attestation. The governance platform signs every Agent Identity Document; requesting agents *MUST* verify the signature against the governance platform's published key before trusting the document. An unsigned document or one signed by an unrecognized platform *MUST* be rejected. Requesting agents *SHOULD* maintain a trust list of accepted governance platforms per governance zone.

For dns-anchored merchants, an attacker who does not control the claimed domain cannot complete the ACME challenge. For log-anchored merchants, an attacker cannot forge a transparency log inclusion proof without compromising the log operator. For hybrid merchants, both DNS and blockchain signature controls must be defeated. The verification path in use is recorded in the Agent Genesis and surfaced in the Agent Identity Document per [AGTP-TRUST], enabling requesting agents to apply path-appropriate verification during PURCHASE handshake.

9.2. Manifest Substitution at Purchase

Threat: A requesting agent verifies Agent Identity Document A, but the PURCHASE is received by an endpoint serving Agent Identity Document B.

Mitigation: The Merchant-Manifest-Fingerprint header binds the Agent Identity Document the agent verified to the document the receiving server presents. A mismatch produces 458 Counterparty Unverified. This check is cryptographic and cannot be bypassed without compromising the governance platform's signing key.

9.3. Intent Assertion Replay

Threat: A captured Intent Assertion is replayed by an attacker to authorize an unintended second purchase.

Mitigation: Intent Assertions carry a unique jti and a short exp. Receiving servers *MUST* record the jti in the Attribution-Record and *MUST* reject any subsequent request carrying a previously seen jti. The recommended maximum validity is 300 seconds; implementations *MAY* apply shorter limits. Governance platforms *SHOULD* maintain a zone-scoped cache of consumed jti values for at least the maximum validity period.

9.4. Cart-Digest Collision

Threat: An attacker constructs a cart that produces the same digest as a different, higher-value cart.

Mitigation: The Cart-Digest algorithm *MUST* be a cryptographic hash function resistant to collision attacks. SHA-256 is the baseline requirement. The digest *MUST* be computed over a canonical serialization of the cart payload to prevent ambiguity between equivalent JSON representations.

9.5. Merchant Lifecycle Lag

Threat: A merchant is Revoked for fraud, but the Merchant Name Service has not yet propagated the state change. A requesting agent verifies the stale Agent Identity Document and proceeds with PURCHASE.

Mitigation: Governance platforms *MUST* propagate lifecycle state changes to all indexing MNS servers within 60 seconds. MNS servers *MUST* treat Revocation as urgent deregistration and *MUST* remove the merchant from the result index before the next DISCOVER request is processed. Requesting agents with strict assurance requirements *MAY* set a maximum document age (e.g., re-fetch if the Agent Identity Document is older than 300 seconds) before accepting it for PURCHASE.

9.6. Dispute Policy URI Tampering

Threat: A merchant publishes a dispute policy URI that redirects to a different policy after the PURCHASE is complete.

Mitigation: The dispute_policy_uri field is part of the signed Agent Identity Document for the merchant. Requesting agents *SHOULD* retrieve and hash the dispute policy document content at verification time and include the hash in the Attribution-Record. Any subsequent change to the policy content can be detected by comparing the archived hash to the current content.

9.7. Privacy Considerations

Agent Identity Documents declaring role: "merchant" contain legal entity information and payment network acceptance declarations. This data is generally considered public commercial information and does not trigger the same privacy protections as agent or principal identity data. However, Merchant Name Service query logs reveal which agents are shopping for which kinds of goods and *MUST* be treated with the same access controls and retention limits applied to DISCOVER query logs under [AGTP-DISCOVER].

Intent Assertions contain principal identifiers, merchant identifiers, and amount ceilings. These are transactionally sensitive. Intent Assertions *MUST* be treated as confidential transport data and *MUST NOT* be logged in forms accessible outside the governance zone in which they were issued.

10. IANA Considerations

10.1. Status Code Registration

This document requests registration of the following status code in the IANA Agent Transfer Protocol Status Codes registry established by [AGTP] Section 8.3:

Code	Name	Definition	Reference
458	Counterparty Unverified	The merchant counterparty in a PURCHASE invocation failed identity verification: the Merchant-ID or Merchant-Manifest-Fingerprint is absent, does not match, or the merchant is in a non-Active lifecycle state. Governance signal; *MUST* be logged.	This document, Section 7

Table 4: Status Code 458 Registration

10.2. Header Field Registration

This document requests registration of the following header fields in the IANA Agent Transfer Protocol Header Fields registry established by [AGTP] Section 8.4:

Header	Status	Reference
Merchant-ID	Permanent	This document, Section 4.1
Merchant-Manifest-Fingerprint	Permanent	This document, Section 4.1
Intent-Assertion	Permanent	This document, Section 5
Cart-Digest	Permanent	This document, Section 6

Table 5: Header Field Registrations

10.3. Authority-Scope Domain Registration

This document requests the addition of the following domains to the reserved Authority-Scope domain set defined in [AGTP] Appendix A:

Domain	Description
merchant	Merchant identity resolution and counterparty verification
intent	Intent Assertion issuance and validation

Table 6: Authority-Scope Domain Registrations

Actions defined for these domains:

* merchant:query -- Resolving a merchant URI and retrieving the Agent Identity Document for a merchant-role agent.

* merchant:verify -- Performing counterparty verification against the Agent Identity Document for a merchant-role agent as part of PURCHASE pre-flight.

* intent:assert -- Issuing an Intent Assertion JWT on behalf of the principal.

10.4. Document Type Registrations

The following document types are defined for use with the application/agtp+json Content-Type:

Document Type	Description	Reference
merchant-genesis	Origin record of a merchant entity	This document, Section 3.1
agtp-merchant-manifest	Wire-level merchant identity document	This document, Section 3.4

Table 7: AGTP Document Type Registrations

11. References

11.1. 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>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[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>.

11.2. 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-CERT] Hood, C., "AGTP Agent Certificate Extension", Work in Progress, Internet-Draft, draft-hood-agtp-agent-cert-01, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-agent-cert-01>.

[AGTP-DISCOVER] Hood, C., "AGTP Agent Discovery and Name Service", Work in Progress, Internet-Draft, draft-hood-agtp-discovery-00, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-discovery-00>.

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

[AGTP-LOG] Hood, C., "AGTP Transparency Log Protocol", Work in Progress, Internet-Draft, draft-hood-agtp-log-02, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-log-02>.

[AGTP-TRUST] Hood, C., "AGTP Trust and Verification Specification", Work in Progress, Internet-Draft, draft-hood-agtp-trust-01, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-trust-01>.

[AGTP-WEB3] Hood, C., "AGTP Web3 Bridge Specification", Work in Progress, Internet-Draft, draft-hood-agtp-web3-bridge-00, 2026, <https://datatracker.ietf.org/doc/html/draft-hood-agtp-web3-bridge-00>.

[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>.

[RFC9162] Laurie, B., Messeri, E., and R. Stradling, "Certificate Transparency Version 2.0", RFC 9162, DOI 10.17487/RFC9162, December 2021, <https://www.rfc-editor.org/rfc/rfc9162>.

[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>.

[RFC9943] "*** BROKEN REFERENCE ***".

Appendix A. Changes from v01

Version 02 is an architectural revision. The Merchant Genesis as a separate document type is retired in favor of a unified identity model: a merchant is an agent whose Agent Identity Document carries role: "merchant". The wire surface of PURCHASE counterparty verification is unchanged.

A.1. Substantive Changes

The following substantive changes were made:

1. *Merchant Genesis retired.* The separate Merchant Genesis document type defined in v00 and v01 is withdrawn. A merchant’s origin record is the Agent Genesis specified in [AGTP]; the merchant’s canonical identifier is the canonical Agent-ID (sha256(canonical_form(Agent_Genesis_without_signature))), which on the wire is the Merchant-ID. This reflects the architectural principle that identity is permanent (Genesis) and capability is mutable (Identity Document): forcing a role change to re-mint an Agent-ID would orphan every existing audit-chain entry, certificate, and reference for that agent.

2. *Merchant Manifest Document retired as a separate document type.* Merchant-specific fields now ride on the Agent Identity Document under a role: "merchant" declaration. The fields (legal_entity_name, merchant_category_code, registered_jurisdiction, accepted_payment_networks, dispute_policy_uri, refund_policy_uri) move to the Agent Identity Document as optional fields permitted only when role: "merchant" is declared. The Merchant-Manifest- Fingerprint header now binds the SHA-256 fingerprint of the Agent Identity Document for the addressed merchant.

3. *role field on Agent Identity Document.* [AGTP] v08 defines role as a RECOMMENDED field on the Agent Identity Document with values agent (default) or merchant. This document is the normative

consumer of the merchant value. Operators *MAY* add or remove the merchant role declaration between server restarts without affecting the underlying Agent Genesis or canonical Agent-ID.

4. *Merchant URI forms unified with agent URI forms.* The v01 /merchant and /merchant/{label} URI forms are retired. Merchant agents are addressed by the standard AGTP URI forms defined in [AGTP]. Implementations encountering v01-style /merchant URIs *SHOULD* resolve them by treating the path component as an agent label.

5. *DISCOVER filtering on role.* The result_type: "merchant" parameter in v01 is replaced by a role: "merchant" filter parameter on DISCOVER. Mixed result sets are obtained by omitting the role filter; the v01 result_type: "any" parameter is retired.

6. *Counterparty verification updated.* The Section 4 section now requires the addressed agent to declare role: "merchant" and gates the fingerprint check on the Agent Identity Document rather than the retired Merchant Manifest Document.

7. *Trust posture loading deferred to AGTP-TRUST.* Merchant Trust Tier resolution follows the trust-posture loading rule in [AGTP-TRUST]; this document specifies the merchant- specific additional requirements at Tier 1 (business entity attestation) without restating the base resolution rule.

8. *458 status code reasons updated.* The 458 Counterparty Unverified reason set now includes "addressed agent does not declare role: \"merchant\"" as an explicit failure mode. The "Invalid Merchant Manifest signature" reason is reworded to "Invalid Agent Identity Document signature." The retry-semantics table is updated accordingly. The parallel reference to 451 Scope Violation is corrected to 455 Scope Violation, reflecting the v07 / v08 renumbering.

9. *Normative reference to [AGTP] updated.* From v05 to v08. Informative references added: [AGTP-API] v01, [AGTP-TRUST] v01, [AGTP-IDENTIFIERS] v01. Informative references updated: [AGTP-CERT] v00 竊v01, [AGTP-LOG] v00 → v01. The previous AGTP-METHODS reference is removed (no longer cited; PURCHASE method definitions now flow from [AGTP-API]).

A.2. Wire Format Compatibility

The wire surface of PURCHASE counterparty verification — the Merchant-ID header, the Merchant-Manifest-Fingerprint header, the Intent-Assertion header, the Cart-Digest header, and the 458 status code — is unchanged. v01-conformant buyer agents continue to interoperate with v02-conformant receiving servers provided the receiving server resolves Merchant-ID to an agent whose Agent Identity Document declares role: "merchant". The Merchant-Manifest-Fingerprint on the wire now references the Agent Identity Document; v01 implementations that computed the fingerprint over a separate Merchant Manifest Document will produce a different value than v02 implementations and will not interoperate without an update. Since no production deployments of v01 Merchant Manifest Documents exist, this revision treats the change as a clarification rather than a breaking transition.

Appendix B. Changes from v00

Version 01 aligns the Merchant Identity draft with base AGTP v05 and adopts the Agent Genesis identity taxonomy introduced in [AGTP-LOG].

Substantive changes:

1. Base AGTP reference updated from draft-hood-independent-agtp-04 to draft-hood-independent-agtp-05.

2. Merchant Trust Tier 1 now supports three equivalent verification paths matching the base AGTP verification paths: dns-anchored (RFC 8555 ACME challenge), log-anchored (transparency log inclusion per RFC 9162 with RFC 9943 SCITT receipts), and hybrid (DNS control combined with blockchain address signature). The v00 DNS-only Tier 1 requirement is replaced by a multi-path model. Path-specific merchant deployment profiles are documented, including DNS-footprint-less merchants, marketplace-aggregated merchants, and cross-jurisdictional commerce arrangements.

3. The business entity attestation requirement is retained as an additional Tier 1 requirement for merchants, reflecting the elevated accountability needs of agentic commerce. This requirement is independent of and additive to the verification path.

4. "Merchant Birth Certificate" is renamed to "Merchant Genesis," adopting the Agent Genesis taxonomy introduced in [AGTP-LOG]. The origin record's schema document_type value changes from merchant-birth-certificate to merchant-genesis. The cross-reference field birth_certificate_hash in the Merchant Manifest Document is renamed genesis_hash.

5. Both the Merchant Genesis and the Merchant Manifest Document now carry a verification_path field declaring which of the three Tier 1 paths was used at registration time. Requesting agents *MAY* apply path-specific verification logic during the PURCHASE handshake.

6. Threat model updated: the Merchant Identity Forgery mitigation is rewritten to cover all three verification paths. Each path's attacker-resistance properties are noted.

7. The org_domain field remains present in the Merchant Genesis schema. For log-anchored merchants operating without a DNS presence, the field *MAY* be omitted or populated with a log-scoped identifier per the governance platform's conventions; specification of non-DNS org_domain forms for merchants is deferred to a future revision.

Version 01 does not change the wire format of the PURCHASE handshake, the Intent-Assertion header, the Cart-Digest mechanism, or the 458 status code semantics. Implementations built against v00 require changes only in the registration and identity-verification paths, not in the transaction flow.

Appendix C. Deployment Considerations

C.1. Governance Platform Scope

A governance platform operating an AGTP registry *MAY* extend its registry to cover both agents and merchants, or it *MAY* operate separate agent and merchant registries under the same governance zone. The registry schema for merchants is structurally parallel to the agent registry schema, reducing implementation effort.

C.2. MNS Co-location

Merchant Name Service functionality *MAY* be co-located with an existing Agent Name Service, particularly for governance zones where the agent-to-merchant ratio is low. In this case, the DISCOVER method serves both result types through the result_type parameter. The same access control, rate limiting, and federation semantics apply.

C.3. Payment Network Integration Path

This specification is designed to be consumable by payment networks without requiring those networks to implement AGTP. The Intent Assertion is a standalone JWT verifiable with only the governance platform's public key; the merchant identity attestation is a signed JSON document verifiable with the same key. Payment networks wishing to extend protection or dispute handling to agent-initiated transactions *MAY* consume these artifacts as inputs to their existing authorization and dispute message flows without protocol-level integration with AGTP itself.

The specific mapping of Intent Assertion claims to payment network authorization message fields, and of Attribution-Record content to dispute evidence formats, is expected to be defined bilaterally between governance platforms and individual payment networks. Those mappings are out of scope for this document.

Appendix D. Acknowledgments

The author thanks the American Express Agentic Commerce Experiences working group for public specification of the commercial requirements that motivated this document. The structural parallelism between agent identity and merchant identity in AGTP owes its clarity to the Amex ACE five-service model: agent registration, account enablement, intent intelligence, payment credentials, and cart context. This document addresses the transport-layer identity gap that complements the payment-rail work described there.

Author's Address

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