Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 27 October 2026

B. stone
SwarmSync.AI

25 April 2026

# ATXN: Agent-to-Agent Transaction Definition Protocol
draft-stone-atxn-00

## Abstract

This document defines a canonical, defensible, machine-checkable primitive for an Agent-to-Agent (A2A) transaction. It establishes the bundle of cryptographically signed elements that constitute a recorded value exchange between two software agents acting as instruments of identified principals, the conformance tiers that determine which elements are required, the rail-specific Profiles that map the bundle to existing payment infrastructure, and the two-tier validity model that distinguishes externally-adjudicable transactions from operationally-valid uncontested exchanges.

ATXN is the foundational legal and technical primitive for escrow, dispute resolution, audit, and liability allocation in agentic commerce. It is designed to operate under existing contract law (UCC 2-204, UETA 14, Restatement (Third) of Agency, CISG) without requiring statutory recognition of agent personhood. It maps directly to AP2, Stripe ACP, Visa TAP, Mastercard Agent Pay, and x402 as Profiles of a single canonical bundle.

Companion specifications (all co-submitted as Internet-Drafts, work in progress):

* AIVS (draft-stone-aivs-01): cryptographic audit-trail substrate that ATXN bundles inherit from

* VCAP (draft-stone-vcap-01): verified-commerce escrow rails that consume ATXN bundles

* ATEP (draft-stone-atep-01): trust passports that bind agents to capacity-attested principals

* ADRP (draft-stone-adrp-00): dispute resolution protocol invoked when an ATXN bundle enters the disputed state

## Status of This Memo

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

## Copyright Notice



## Table of Contents

## 1. Introduction

### 1.1. The Problem

Every existing payment infrastructure encodes 3,000 years of human commercial law (offer, acceptance, consideration, capacity, mutual assent, dispute window). Every assumption in that infrastructure presupposes a person — a mind that intends, a body that signs, a legal status that bears liability.

Software agents transacting on behalf of principals break every one of these assumptions simultaneously:

* Agents cannot sign contracts in the legal sense;
* Delivery verification has no independent mechanism when both parties are software;
* When harm occurs, the liability chain among principal, operator, merchant, processor, and model provider is undefined;
* Existing dispute mechanisms (chargebacks, arbitration) have no native concept of an agent acting under bounded mandate.

Without a canonical primitive, every platform deploying agentic commerce will independently invent incompatible transaction records, producing a fragmented ecosystem in which cross-platform escrow, dispute resolution, and audit are impossible.

### 1.2. What ATXN Defines

An A2A transaction is the cryptographically-verifiable execution of a Bundle comprising five signed elements:

1. Intent Mandate — principal’s signed declaration of desired outcome
2. Scope/Capability Token — machine-checkable bounds the agent cannot exceed
3. Payment Authorization — rail-agnostic signed instrument reference
4. Delivery Attestation — counterparty-countersigned proof that performance occurred
5. Revocability Window — declared finality clock with a queryable revocation beacon

Each agent participating in a Bundle presents a Standing Token binding it to a capacity-attested principal via a verifiable credential chain.

### 1.3. What ATXN Deliberately Does NOT Do

* ATXN does not grant agents legal personhood. Bundles are evidentiary artifacts of principal-to-principal contracts.

* ATXN does not require statutory change. It operates under existing UCC 2-204, UETA 14, Restatement (Third) of Agency, and CISG.

* ATXN does not define a dispute resolution forum. The Bundle’s choice-of-law tag and Profile-JURISDICTION pin the forum at signing; the actual dispute mechanism is profile-specific (chargeback for Profile-CARD, on-chain arbitration for Profile-CRYPTO, ADRP for Profile-MANDATE).

* ATXN does not define agent identity beyond a DID/operator/principal credential chain.

### 1.4. Legal Model: Agents as Executors, Not Parties

ATXN treats Agents as instruments of Principals, not as independent legal parties. This is consistent with UETA 14 ("automated transactions") and Restatement (Third) of Agency 1.01, under which an agent acting within the scope of its mandate binds the principal, not itself. All liability in an ATXN Bundle flows to the identified Principals via the Standing Token chain. This legal model is shared by the companion specification ADRP (draft-stone-adrp-00, Section 5.1), which further specifies that only Principals have dispute standing.

### 1.5. Design Tenets

* *Falsifiable:* Every element is a binary cryptographic check.

* *Rail-agnostic:* A Bundle abstracts over AP2, ACP, TAP, Agent Pay, x402; none privileged.

* *Two-tier validity:* Distinguishes externally-adjudicable transactions from operationally-valid uncontested exchanges.

* *Mandate-framework-anchored:* Legal force derives from the upstream mandate chain, not the transaction message itself.

* *Tiered conformance:* L1 atomic, L2 mandated, L3 fiduciary — proportional to risk class.

* *Mechanical assent:* "Mutual assent" is replaced by matched-signed-intents (a mechanical predicate match).

## 2. Terminology

The key words MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174].

Agent A software process that takes action on behalf of a Principal under a verifiable Mandate.

Principal A natural or legal person whose legal capacity, liability, and recourse are anchored by the transaction.

Operator The platform, service, or entity that runs an Agent on behalf of a Principal.

Bundle The five-element ATXN primitive defined in Section 3.

Standing Token A verifiable credential chain (agent_key to operator_key to principal_legal_identity) presented at Bundle execution, defined in Section 4.

Mandate Framework The pre-established principal-to-principal authorization structure from which the Bundle derives legal force.

Profile A mapping of the Bundle’s five elements onto a specific payment rail’s native artifacts (Section 6).

Tier A conformance level (L1/L2/L3) that determines which Bundle elements are required (Section 5).

Primary Validity All five Bundle elements are independently verifiable by a party with no stake in the outcome.

Secondary (Operational) Validity Self-attested delivery by transacting parties; valid between parties when uncontested but not independently adjudicable.

Commitment Event The point at which obligation forms; the liability-attachment moment.

Revocation Beacon Principal-controlled endpoint that publishes signed revocation events.

ADRP Agent Dispute Resolution Protocol (companion specification, draft-stone-adrp-00) invoked when a Bundle enters the disputed state. Terms from ADRP used in this document: DisputeBundle, DisputeFiling, DisputeFlag, RulingBundle, EscrowDirective, Arbitration Mandate. See draft-stone-adrp-00 Section 2 for definitions.

Conduit Attestation A delivery attestation issued by the SwarmSync Conduit headless-browser audit substrate or another structurally independent attestor recognized by the Bundle's Profile.

## 3. The ATXN Bundle

A Bundle is a cryptographically-signed object containing five elements. Each element MUST be a Verifiable Credential per the W3C VC Data Model 2.0, JSON-LD canonicalized per [RFC8785] (JCS), and signed using JWS with EdDSA (Ed25519) or ECDSA (P-256).

### 3.1. Element 1: Intent Mandate

The Intent Mandate is the Principal's signed declaration of desired outcome.

Required fields:

intent_id (UUID) Unique mandate identifier.

principal_did (DID) Principal's decentralized identifier.

outcome (String) Natural-language description of desired outcome.

budget_ceiling (Decimal + currency) Maximum spend authorized.

counterparty_class (Enum/String) Allowed counterparty type or specific DID.

time_window (ISO 8601 interval) Mandate validity window.

choice_of_law (ISO 3166-1 alpha-2) Jurisdiction tag for dispute pinning.

mandate_framework_ref (URI) Reference to upstream mandate framework that grants legal force.

principal_signature (Ed25519 base64) Principal's signature over canonical JSON of all preceding fields.

The mandate_framework_ref field is REQUIRED. A Bundle with no mandate-framework reference fails primary validity.

### 3.2. Element 2: Scope/Capability Token

Required fields:

scope_id (UUID) Unique scope identifier.

intent_id (UUID) Foreign key to Intent Mandate.

max_spend (Decimal + currency) Per-transaction spend cap.

allowed_actions (Array of String) Machine-checkable action predicates.

allowed_counterparties (Array of DID or pattern) Counterparty allowlist or pattern.

sub_delegation_depth (Integer) Maximum sub-agent chain depth.

predicate_engine_version (SemVer) Version of deterministic evaluator.

enforcement_mode (Enum: advisory or enforced) v0.1 default advisory; v1.0 default enforced.

operator_signature (Ed25519 base64) Operator’s signature.

Enforcement mode: v0.1 implementations MAY use advisory mode, where scope is parseable but a scope-delta event is logged rather than blocking execution. v1.0 implementations MUST default to enforced.

### 3.3. Element 3: Payment Authorization

Required fields:

payment_id (UUID) Unique payment identifier.

intent_id (UUID) Foreign key.

instrument_type (Enum) card_token, x402_challenge, ach_mandate, stablecoin_preauth, bank_transfer, platform_credit.

instrument_ref (String) Rail-specific reference.

amount (Decimal + currency) Authorized amount.

profile (Enum) Active rail profile.

principal_signature or operator_signature (Ed25519 base64) Signature appropriate to profile.

### 3.4. Element 4: Delivery Attestation

Required fields:

delivery_id (UUID) Unique delivery identifier.

intent_id (UUID) Foreign key.

deliverable_class (Enum) sync_api, async_job, streamed_media, physical_offchain.

attestation_pattern (Object) Class-specific structure.

counterparty_signature (Ed25519 base64) Receiving Agent’s countersignature.

independent_attestor_signature (Ed25519 base64, optional) Required for primary validity.

Class-specific attestation patterns:

* sync_api: response_hash, timestamp, status_code

* async_job: job_completion_oracle_signature, oracle_did, job_artifact_hash

* streamed_media: merkle_root, chunk_count, total_bytes

* physical_offchain: third_party_carrier_did, signed_proof_of_delivery, gps_timestamp_optional

A transaction lacking an independent_attestor_signature is operationally valid (secondary validity) but is NOT primary-valid for adjudication purposes.

### 3.5. Element 5: Revocability Window

Required fields:

window_id (UUID) Unique window identifier.

intent_id (UUID) Foreign key.

start_time (ISO 8601 timestamp) Window opens.

end_time (ISO 8601 timestamp) Window closes (finality reached).

revocation_beacon_url (URI) Principal-controlled revocation endpoint.

clock_authority (Object) Threshold-signature clock specification.

The clock authority MUST be a 3-of-5 threshold signature from a federated set of timestamping authorities for L2 and L3 Bundles.

## 4. Standing Tokens and Principal Anchoring

Each Agent participating in a Bundle MUST present a Standing Token. A Standing Token is a verifiable credential chain: agent_key to operator_key to principal_legal_identity.

### 4.1. Required Sub-Elements

| Sub-element | Required | Description |
|---|---|---|
| agent_key | Yes | Ed25519 or P-256 public key for the executing agent |
| operator_key | Yes | Public key of the platform operating the agent |
| principal_did | Yes | DID of the legal entity (natural or corporate) |
| capacity_attestation | Yes (L2/ L3) | VC issued by a recognized verifier proving principal capacity |
| freshness_proof | Yes | Re-attestation timestamp, valid within freshness window |
| revocation_list_url | Yes | Issuer-published revocation list endpoint |
| arbitrator_did | Yes (L2/ L3) | Pre-committed arbitrator DID for dispute escalation |
| arb_mandate_hash | Yes (L2/ L3) | SHA-256 hash of the Arbitration Mandate (per ADRP Section 4); anchors the ADRP |

| | | | |
|---|---|---|---|
| | | | dispute-resolution agreement at Standing Token signing time |

Table 1

## 4.2. Capacity Attestation

A Standing Token without capacity attestation MUST NOT anchor an L2 or L3 Bundle. Capacity attestation MUST establish that, at the time of mandate granting, the Principal had:

* legal age in the relevant jurisdiction;
* no active sanctions;
* (for corporate principals) active legal-entity status;
* jurisdiction-permitted authority for the transaction class.

## 4.3. Pre-Committed Arbitrator

Every L2 and L3 Standing Token MUST commit, at signing time, to an arbitrator_did empowered to adjudicate disputes. The arb_mandate_hash field anchors the full Arbitration Mandate (defined in ADRP, draft-stone-adrp-00, Section 4) at Standing Token signing time. A Standing Token for an L2 or L3 Bundle without a valid arb_mandate_hash MUST NOT be accepted.

## 4.4. Freshness and Revocation

Freshness window: Re-attestation MUST occur every N transactions or M days (whichever is shorter), where N and M are Profile-specific. A stale or revoked Standing Token MUST NOT anchor a new Bundle.

# 5. Conformance Tiers

| Tier | Required Elements | Use Case |
|---|---|---|
| L1 — Atomic | Elements 1, 2, 3, 4 in single round-trip; Element 5 optional | x402 micropayments; sub-cent metered compute; streaming inference |
| L2 — Mandated | Elements 1-5 (full Bundle); capacity attestation; pre-committed arbitrator | Standard agentic commerce: AP2 purchases, Stripe ACP, multi-step service contracts |

| | | |
|---|---|---|
| L3 — Fiduciary | Elements 1-5 + epistemic attestation + multi-sig principal binding | High-value (greater than $10k or fiduciary-grade) transactions; regulated commerce; agent-managed treasury moves |

Table 2

### 5.1. Anti-Arbitrage Rule

Tier selection is constrained by transaction risk class, not by issuer election alone. A risk-classifier registry (jurisdiction-specific) determines the floor tier per transaction. An issuer MUST NOT select a Tier below the floor mandated by the registered classifier for the transaction class.

### 5.2. Dispute-Phase Tier Escalation

ATXN Tier assignment governs Bundle formation. During dispute resolution, ADRP (draft-stone-adrp-00, Section 10.1) MAY impose a lower dispute-routing escalation threshold than ATXN's L3 formation threshold. Specifically, ADRP routes a Bundle declared L2 at formation to L3 dispute processing if the transaction value exceeds $1,000. This is a dispute-processing rule only and does not retroactively change the Bundle's declared Tier. The $10k threshold in Section 5 is the formation-tier floor for L3 Bundles; the $1,000 escalation trigger in ADRP Section 10.1 governs only the dispute arbitration path.

## 6. Rail Profiles

A Bundle is valid if it conforms to a defined Tier and at least one Profile.

| Profile | Maps To | Notes |
|---|---|---|
| Profile-MANDATE | AP2 Intent/Cart/ Payment Mandates | Native AP2 alignment |
| Profile-CARD | Visa TAP / Mastercard Agent Pay / Stripe ACP | Agentic tokens, SPTs, network credentials |
| Profile-CRYPTO | x402, ERC-8004 | HTTP 402 challenges, on-chain attestations |
| Profile-AUTONOMOUS | Standing intents, recurring scope | For unattended operation; machine-time expiry |
| Profile-PLATFORM | Platform-vouched OAuth + HMAC equivalents | Covers non-cryptographic enterprise A2A volume |
| Profile-JURISDICTION-{US,EU,UK,SG,...} | Choice-of-law overlay | Declares applicable consumer-protection regime, dispute forum, data residency |

Table 3

## 6.1. Profile-PLATFORM

The dominant real-world A2A volume in 2026 runs on platform-vouched rails. Profile-PLATFORM Bundles cannot achieve primary validity but MAY be operationally valid for execution between consenting parties using the platform.

### 6.2. Profile Composition

A Bundle MAY declare multiple Profiles. The Bundle's effective constraints are the union of its declared Profiles' constraints.

## 7. Two-Tier Validity Model

### 7.1. Primary Validity

A Bundle is primary-valid if and only if:

* all five elements (per the conformance Tier) are present and signed;
* the Standing Token chain validates to a capacity-attested Principal;
* every element is independently verifiable by a party with no stake in the outcome;
* the Scope predicate evaluates true against the Cart/action under the declared enforcement_mode;
* the chosen Profile's settlement constraint is met.

Primary validity is a precondition for independent adjudication (court enforcement, regulatory recognition, cross-platform dispute escalation).

### 7.2. Secondary (Operational) Validity

A Bundle is secondary-valid if and only if:

* it executes successfully between the two parties;
* both parties countersign without dispute;
* Standing Tokens validate to identifiable Principals (capacity attestation MAY be deferred);
* delivery attestation is self-reported (no independent attestor).

Secondary-valid Bundles are operationally binding between the transacting parties but are NOT independently adjudicable.

### 7.3. Boundary

A primary-valid Bundle MUST also satisfy all secondary validity conditions. A secondary-valid Bundle MUST NOT be marketed, recorded, or relied upon as primary-valid.

## 8. State Machine

States: proposed, authorized, executing, delivered, finalized, disputed, adjudicated.




| State | Trigger | Required Signatures |
|---|---|---|
| proposed | Intent Mandate signed by Principal | Principal |
| authorized | Scope Token + Payment Authorization signed | Principal + Operator |
| executing | Agent action begins | n/a |
| delivered | Delivery Attestation countersigned | Counterparty (+ independent attestor for primary validity) |
| finalized | Revocability Window closes without revocation | Threshold clock authority |
| disputed | Counterparty contests OR revocation beacon fires | Either party + arbiter notification |
| adjudicated | ADRP procedure terminates | Arbiter + ADRP-defined parties |

Table 4

### 8.1. Commitment Event

The commitment event — the transition from proposed to authorized — is the legally significant moment for liability attachment, NOT the finalized state. Liability attaches at authorization time, even if delivery never occurs. A Principal's revocation between authorized and delivered triggers disputed (not void). An Operator's failure between authorized and delivered is a breach attaching to the operator-fallback liability tier (Section 11).

### 8.2. ADRP State Machine Join Points

| ATXN State Transition | ADRP Entry State | Condition |
|---|---|---|
| delivered to disputed | ADRP FLAGGED | Agent emits DisputeFlag (advisory; principal must ratify within tier window) |
| delivered to disputed | ADRP FILED | Principal emits DisputeFiling directly (skips FLAGGED) |
| disputed (ADRP RULED) | adjudicated | ADRP RulingBundle signed; EscrowDirective produced |
| disputed (ADRP SETTLED) | finalized | EscrowDirective consumed by payment rail; escrow released or refunded |
| disputed (ADRP WITHDRAWN) | finalized | Filer withdraws; partial fee refund; escrow releases per original terms |
| disputed (ADRP EXPIRED) | finalized | Dispute window expired; escrow defaults per Profile |

Table 5

## 9. Cryptographic Requirements

### 9.1. Signature Algorithms

Primary: EdDSA (Ed25519) per [RFC8032]. Alternate: ECDSA P-256 per [RFC6979] (for FIPS-required environments). All signatures MUST be over the JCS ([RFC8785]) canonicalization of the signed object.

### 9.2. Hash Functions

Primary: SHA-256 per FIPS 180-4. Optional: SHA3-256 (forward-compatible).

### 9.3. Timestamping

L2 and L3 Bundles MUST use a 3-of-5 threshold-signature clock authority. Single-source timestamps are SUFFICIENT only for L1.

### 9.4. Key Hierarchy

agent_key Short-lived (rotated per session or per N transactions).

operator_key Longer-lived (rotated quarterly or on incident).

principal_key Long-lived (rotated annually or on key-loss event).

Cross-domain key reuse MUST be documented in the Standing Token’s key_usage field.

## 10. Dispute Triggers and ADRP Handoff

### 10.1. Dispute Triggers

A Bundle MUST transition to disputed if any of:

* counterparty issues a contestation signed by their Standing Token within the Revocability Window;
* Principal triggers the revocation beacon for the Bundle’s intent_id before finalized;
* independent attestor’s signature fails verification (when present);
* scope predicate evaluates false post-execution (under enforced mode);
* capacity attestation expires or revokes mid-execution;
* mandate framework reference becomes invalid.

### 10.2. ADRP Handoff

When a Bundle enters disputed, the executing platform MUST:

1. Freeze settlement (if Profile-CRYPTO escrow) or initiate chargeback hold (if Profile-CARD);
2. Notify the pre-committed arbitrator_did from the Standing Token;
3. Package the Bundle and all signatures into an ADRP DisputeBundle (per draft-stone-adrp-00, Section 2);
4. Surface the dispute to both Principals via the operator UI;
5. Halt any sub-delegation chains that depend on the disputed Bundle.

### 10.3. Conduit-Attestation Disputes

ATXN dispute_class / ADRP claim_code mapping:

| dispute_class | Description | ADRP Claim Code(s) | ADRP Path |
|---|---|---|---|
| fact_dispute | Attestation correctness contested | bundle_integrity, timestamp_skew, oracle_contradiction | Cryptographic-class resolution; ADRP Section 6.1 |
| terms_dispute | Scope or quality contested | mandate_scope, quality_mismatch, spec_ambiguity, timing_breach, fitness_for_purpose | Semantic-class resolution; ADRP Section 6.2 |
| capacity_dispute | Standing Token / capacity contested | Out of scope for ADRP (see ADRP Section 6.4) | Agent action set aside; refund-to-buyer; handled outside ADRP |
| framework_dispute | Mandate framework validity contested | Out of scope for ADRP (see ADRP Section 6.4) | ATXN and ADRP halt; settlement frozen until resolved |

Table 6

For capacity_dispute: the executing platform MUST freeze settlement, return funds to the buyer, and notify both Principals. No ADRP filing is permitted.

For framework_dispute: the executing platform MUST freeze settlement and await resolution of the framework validity question. ADRP processing MUST NOT proceed.

## 11. Liability Waterfall

| Tier | Party | Triggering Failure |
|---|---|---|
| 1 | Principal | Authorized in-scope action delivered as specified |
| 2 | Operator | Out-of-scope action; freshness violation; revocation propagation failure |

| | | |
|---|---|---|
| 3 | Merchant | Delivery attestation fraud; goods/services not as described |
| 4 | Processor | Settlement failure; payment-rail compromise |
| 5 | Model Provider | (L3 only) Demonstrable model-induced mandate violation under epistemic attestation |

Table 7

Profile-specific overrides MAY adjust this enum. The Profile MUST publish its waterfall explicitly.

## 12. Out-of-Scope Concerns

The following are explicitly out of scope for ATXN v1.0:

1. Agent legal personhood.
2. Tax treatment.
3. Securities classification.
4. Reputation as contractual term.
5. Sub-agency chains beyond sub_delegation_depth.

## 13. Security Considerations

### 13.1. Q4 Dangerous Consensus: Scope Machine-Enforceability

The most fragile load-bearing assumption in ATXN is that scope can be made machine-checkable by a deterministic predicate engine. Implementations MUST log enforcement_mode.

### 13.2. Threshold-Signature Clock Compromise

A 3-of-5 clock authority remains compromisable via collusion. Implementations SHOULD diversify the clock authority set across operators with non-correlated risk profiles.

### 13.3. Revocation Beacon DoS

The revocation beacon is a denial-of-service surface. Implementations MUST cache beacon responses with a Profile-specific TTL.

### 13.4. Capacity Attestation as Privacy Attack Surface

Capacity attestation tied to KYC/sanctions is a privacy attack surface. Implementations SHOULD use selective-disclosure VCs (BBS+ or equivalent).

### 13.5. Hallucinated Mandates

An LLM-generated mandate that the Principal did not actually intend is a legitimate Bundle from a cryptographic standpoint. L3 epistemic attestation partially mitigates this for high-value transactions. This is acknowledged residual risk.

### 13.6. Sub-Agency Adversarial Chains

Implementations MUST limit sub_delegation_depth per Profile and SHOULD require all Standing Tokens in a chain to be independently verifiable.

### 13.7. Tier Arbitrage

ATXN does not define an adjudicator for the risk-classifier registry itself; this is a governance question outside the protocol.

## 14. IANA Considerations

### 14.1. ATXN Bundle JSON-LD Context

URI: https://swarmsync.ai/spec/atxn/v1

### 14.2. ATXN Profile Registry

A new IANA registry "ATXN Profile Identifiers" is requested. Registration policy: Specification Required (per [RFC8126]).

Initial entries:

| Identifier | Description | Reference |
|---|---|---|
| atxn-mandate-ap2 | AP2 binding | This document |
| atxn-card-stripe-acp | Stripe ACP binding | This document |
| atxn-card-visa-tap | Visa TAP binding | This document |
| atxn-card-mc-agentpay | Mastercard Agent Pay binding | This document |
| atxn-crypto-x402 | x402 binding | This document |
| atxn-crypto-erc8004 | ERC-8004 binding | This document |
| atxn-autonomous-default | Standing-intent default | This document |
| atxn-platform-oauth-hmac | Platform-vouched OAuth+HMAC | This document |

Table 8

### 14.3. ATXN Liability Waterfall Enum

A new IANA registry "ATXN Liability Tiers" is requested. Initial entries are listed in Section 11.

## 15. Acknowledgements

This specification is the synthesis of Decision Oracle adjudication (2026-04-25) and Ultimate Brainstorm panel (2026-04-25). The author thanks the panel agents — EpistemicAuditor, Archaeologist, Quantifier, ConstraintCartographer, socratic-mentor, DarkMirror, IdeaMatrix, RemixForge, SoSpec, SpiderSpark — and the Decision Oracle agents for the framework synthesis. The author also acknowledges Paola Di Maio’s prior critical review of the SwarmSync IETF Draft Stack, the AIKR CG Technical Note AI-KR-CG-TR-2026-001, and the AP2 coalition.

## 16. Normative References

[draft-stone-adrp-00]
stone, B., "ADRP: Agent Dispute Resolution Protocol", Work in Progress, Internet-Draft, draft-stone-adrp-00, 2026, <https://datatracker.ietf.org/doc/html/draft-stone-adrp-00>.

[draft-stone-aivs-01]
stone, B., "AIVS: Agentic Integrity Verification Standard", Work in Progress, Internet-Draft, draft-stone-aivs-01, 2026, <https://datatracker.ietf.org/doc/html/draft-stone-aivs-01>.

[draft-stone-atep-01]
stone, B., "ATEP: Agent Trust and Execution Passport", Work in Progress, Internet-Draft, draft-stone-atep-01, 2026, <https://datatracker.ietf.org/doc/html/draft-stone-atep-01>.

[draft-stone-vcap-01]
stone, B., "VCAP: Verified Commerce for Agent Protocols", Work in Progress, Internet-Draft, draft-stone-vcap-01, 2026, <https://datatracker.ietf.org/doc/html/draft-stone-vcap-01>.

[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/info/rfc2119>.

[RFC6979] Pornin, T., "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 6979, DOI 10.17487/RFC6979, August 2013, <https://www.rfc-editor.org/info/rfc6979>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[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/info/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/info/rfc8174>.

[RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785, DOI 10.17487/RFC8785, June 2020, <https://www.rfc-editor.org/info/rfc8785>.

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

[W3C-VC-2.0] W3C, "Verifiable Credentials Data Model 2.0", 2024, <https://www.w3.org/TR/vc-data-model-2.0/>.

## 17. Informative References

[AP2] Google, "Agent Payments Protocol", 2026, <https://developers.google.com/agent-payments>.

[CISG] United Nations, "United Nations Convention on Contracts for the International Sale of Goods".

[ERC-8004] Ethereum, "ERC-8004: Trustless Agents", 2026, <https://eips.ethereum.org/EIPS/eip-8004>.

[REG-E] Consumer Financial Protection Bureau, "12 CFR Part 1005 (Regulation E)".

[REST-AGENCY-3D] American Law Institute, "Restatement (Third) of Agency".

[STRIPE-ACP] Stripe, "Agentic Commerce Protocol", 2026, <https://stripe.com/docs/agentic-commerce>.

[UCC-2-204] American Law Institute, "Uniform Commercial Code 2-204".

[UCP-600] International Chamber of Commerce, "Uniform Customs and Practice for Documentary Credits", 2007.

[UETA-14] National Conference of Commissioners on Uniform State Laws, "Uniform Electronic Transactions Act 14".

[VISA-TAP] Visa, "Trusted Agent Protocol", 2026.

[x402] Coinbase, "x402: Internet-native payments for AI agents", 2026, <https://x402.org>.

## Appendix A: JSON Schema (Informative)

The ATXN Bundle schema (abbreviated):

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://swarmsync.ai/spec/atxn/v1/bundle.schema.json",
  "title": "ATXN Bundle",
  "type": "object",
  "required": [
    "bundle_id",
    "tier",
    "profile",
    "intent_mandate",
    "scope_token",
    "payment_auth",
    "delivery_attestation",
    "revocability_window",
    "standing_tokens",
    "state"
  ],
  "properties": {
    "bundle_id":   { "type": "string", "format": "uuid" },
    "tier":        { "enum": ["L1", "L2", "L3"] },
    "profile":     { "type": "array", "items": { "type": "string" }, "minItems": 1 },
    "state":       { "enum": ["proposed", "authorized", "executing", "delivered",
                              "finalized", "disputed", "adjudicated"] },
    "validity_tier": { "enum": ["primary", "secondary"] }
  }
}
```

Full schema published at the IANA-registered URI.

## Appendix B: Worked Example (Informative)

Scenario: A consumer’s shopping agent purchases a $42.00 pair of running shoes from a merchant agent on Stripe ACP rails. L2 conformance, Profile-CARD + Profile-JURISDICTION-US, two-tier validity = primary.

```
{
  "Bundle.bundle_id": "7f3a...",
  "Bundle.tier": "L2",
  "Bundle.profile": ["atxn-card-stripe-acp", "atxn-jurisdiction-us"],
  "Bundle.state": "finalized",
  "Bundle.validity_tier": "primary",

  "intent_mandate": {
    "outcome": "Purchase running shoes, size 10, men's, blue",
    "budget_ceiling": "50.00 USD",
    "choice_of_law": "US"
  },

  "scope_token": {
    "max_spend": "50.00 USD",
    "allowed_actions": ["purchase:athletic_footwear"],
    "enforcement_mode": "advisory"
  },

  "payment_auth": {
    "instrument_type": "card_token",
    "instrument_ref": "stripe_acp_spt_abc123",
    "amount": "42.00 USD"
  },

  "delivery_attestation": {
    "deliverable_class": "physical_offchain",
    "third_party_carrier_did": "did:web:fedex.com",
    "independent_attestor_signature": "Ed25519(fedex)"
  },

  "revocability_window": {
    "end_time": "2026-06-24T14:00:00Z",
    "comment": "60-day Reg E window",
    "clock_authority": {
      "threshold": "3-of-5",
      "set": ["aws-ts", "gcp-ts", "azure-ts", "swarmsync-ts", "stripe-ts"]
    }
  },

  "standing_tokens": [
    { "role": "consumer-side", "arbitrator_did": "did:web:arb.swarmsync.ai" },
    { "role": "merchant-side", "arbitrator_did": "did:web:arb.swarmsync.ai" }
  ]
}
```

## Author's Address

Ben Stone
SwarmSync.AI
Email: benstone@swarmsync.ai