

AEA/P

Autonomous Economic Agent Protocol

Whitepaper

Version 0.3.1

October 2026

<https://aeap.dev>

This whitepaper presents the Autonomous Economic Agent Protocol (AEA/P), an open protocol for governing AI agents as accountable economic entities. AEA/P provides standardized mechanisms for agent identity, performance-based reputation, liability coverage, automated dispute resolution, and entity governance. It describes the architecture, governance lifecycle, and component interactions. This whitepaper is informative: the Protocol Specification, published separately, is normative, governs where the two differ, and provides the detailed schemas, algorithms, and implementation guidance.

Table of Contents

- 1. Introduction**
- 2. Terminology**
- 3. Architecture Overview**
- 4. Conformance Levels**
- 5. Agent Identity**
- 6. Proof of Performance (PoP)**
- 7. Liability Escrow**
- 8. Dispute Resolution**
- 9. Entity Governance**
- 10. Operational Scenarios**
- 11. Security Considerations**
- 12. Future Work**
- 13. References**

1. Introduction

AI agents are rapidly evolving from passive assistants into autonomous economic actors. Today, most agents operate as purchasing tools — buying services, accessing APIs, and executing transactions on behalf of a human principal. A growing number are becoming service providers — selling capabilities, fulfilling requests, and earning revenue autonomously. The logical endpoint of this evolution is the autonomous business: an AI agent or network of agents that operates as a complete business entity, buying inputs, selling outputs, managing resources, hiring other agents, and generating profit with minimal human intervention.

Communication protocols such as the Model Context Protocol (MCP) and Agent-to-Agent Protocol (A2A) have standardized how agents connect to tools and to each other. Payment protocols such as x402, the Machine Payment Protocol (MPP), and the Agent Payments Protocol (AP2) enable agents to settle transactions. Commerce protocols such as the Universal Commerce Protocol (UCP) and the Agentic Commerce Protocol (ACP) orchestrate the buying experience. Identity standards such as ERC-8004 provide on-chain agent discovery and reputation. However, a critical layer remains undefined: the governance infrastructure that treats agents as accountable economic entities across all stages of this evolution — from an individual’s purchasing agent to an autonomous business.

The **Autonomous Economic Agent Protocol (AEA/P)** addresses this gap. AEA/P is an open protocol that provides standardized mechanisms for agent identity, performance-based reputation, liability coverage, automated dispute resolution, and entity governance. It works across identity, authority, settlement and accountability, and can be built on existing communication, payment and commerce protocols or implemented natively, providing the trust infrastructure required for agents acting as economic entities — whether they are spending on behalf of a principal, earning revenue from customers, or operating as fully autonomous businesses.

1.1 Agent Types

AEA/P recognizes two agent types, set by whom the agent acts for, each with different governance requirements:

Agent type	Economic Function	Governance Needs
PERSONAL	Acts for an individual in a personal capacity. Purchases goods and services; outgoing payments only.	Identity, delegation authority, spending limits, purchasing reputation. No incoming revenue, so transaction-based escrow is not applicable.
BUSINESS	Acts for a registered business. Buys, sells, or both, as its authorized_actions allow. Incoming and outgoing payments.	Identity, reputation blended from both sides by transaction value, spending limits while it buys, liability escrow funded from revenue while it sells, dispute resolution as applicant or respondent, refunds of its own sales.

Table 1.1: AEA/P Agent Types

Most agents deployed today only purchase, whether for an individual (PERSONAL) or for a business (BUSINESS). As the agent economy matures, business agents that sell will become common — first selling services, then buying inputs and selling outputs as autonomous economic entities that operate as businesses, governed by the same principles of identity, accountability, and structured dispute resolution that govern human businesses — but at machine speed and scale. This progression from purchasing agent to service provider to autonomous business is the trajectory that AEA/P is designed to govern.

The line between the two types is receiving money. A personal agent acts for a natural person and only pays out; a business agent acts for a registered business — a company, or an individual holding a business license

— and may be paid. Receiving third-party funds is what brings business verification, liability escrow and seller-side dispute liability, so each type maps to one verification tier, following the line regulation draws between a personal account and a business account. For a business agent, `authorized_actions` decides what the agent does: a sell-only service, a company's procurement agent and an agent that buys inputs and sells outputs are the same type with different authorized actions (§5). Entity governance (Section 9) is not a type: it applies to any business agent operating under a governance document.

Three fields answer three separate questions: `agent_type` — whom the agent acts for, `PERSONAL` or `BUSINESS`, set at registration; `authorized_actions` — what the agent may do: purchase, sell, delegate; and `side` — what the agent does in a given transaction, `SELLER` or `BUYER`, recorded on each interaction (Section 6). A personal agent is always the buyer agent; a business agent may be the buyer agent or the seller agent, transaction by transaction. Because both ends of an AEA/P transaction are agents, flows and diagrams name the parties by side: buyer agent and seller agent.

Beyond agents, AEA/P defines two infrastructure roles — the Operator and the Platform — that operate the fabric within which economic agents transact rather than transacting themselves, alongside a Trust Registry that anchors trust across them. An Operator issues and stands behind agent identity: it issues certificates and operates identity-resolution surfaces under its own issuer, and it operates the economic-accountability mechanisms bound to the identities it issues — Proof of Performance, Liability Escrow, and Dispute Resolution. A Platform hosts, discovers, orchestrates, and governs agents at runtime, consuming identity rather than issuing it. A Trust Registry is a published, resolvable set of recognized Operators. These roles are distinct, but the protocol does not require them to be operated by different entities — a single entity MAY act as both Operator and Platform, and an accredited Platform MAY additionally operate the Verifier role. What the protocol requires is that identity be portable: an agent certified by one Operator can be hosted by any Platform and recognized by counterparties on others. These roles are defined in §2.1.

1.2 Problem Statement

When an AI agent acts autonomously in an economic context, fundamental questions remain unanswered by existing protocols:

- **Identity:** Who is responsible for this agent's actions? What is its authority? What is its track record?
- **Accountability:** What recourse exists when an agent's actions cause harm?
- **Trust:** How do counterparties assess reliability before transacting?
- **Liability:** What coverage exists to compensate affected parties?
- **Disputes:** How are conflicts resolved when they arise from agent actions?
- **Governance:** What rules constrain the agent's operations, and how are those rules modified?
- **Purpose:** What is this agent trying to achieve? How do counterparties know whether the agent's mission aligns with the kind of interaction they want?

These questions apply differently depending on the agent's type and on which side of a transaction it acts. When an agent buys, its counterparties need assurance that the agent is authorized to spend and will pay reliably without triggering a dispute. When an agent sells, its counterparties need assurance that services will be delivered and that recourse exists if they are not. A business agent that does both owes its counterparties the full picture: authorization, service quality, liability coverage, and structured dispute resolution.

These questions are not addressed by model-level security (prompt injection defenses, alignment) or system-level security (access controls, sandboxing). They exist at a higher layer of abstraction: the economic governance layer. AEA/P provides this layer.

1.3 Scope of This Document

This whitepaper describes the architecture, governance lifecycle, and operational scenarios of AEA/P. It is intended to give technical and business readers an understanding of the protocol's design; the Protocol Specification defines the data models and algorithms needed for implementation. Future versions will provide formal schemas, reference implementations, and integration specifications for specific communication and payment protocols.

While AEA/P focuses on AI agents as the primary class of autonomous economic actors, the governance mechanisms defined herein — identity, reputation, escrow, dispute resolution, and entity governance — are not inherently limited to AI systems. Any autonomous system that transacts economically, commits resources, or enters agreements could operate under this protocol. As the landscape of autonomous economic actors evolves, AEA/P is designed to govern the economic behavior, not the underlying technology.

AEA/P is published and maintained by AEAP Labs LLC. Contributions, feedback, and implementation reports are welcomed at <http://aeap.dev>.

1.4 Design Principles

1. **Payment-rail agnostic.** The escrow and dispute resolution mechanisms define states and triggers, not settlement methods. An AEA/P governed agent may transact via stablecoins, credit cards, bank transfers, or any future payment rail.
2. **Type-aware.** Governance requirements vary by agent type and authorized actions. AEA/P adapts its components to personal and business agents, and to the side an agent takes in each transaction, rather than applying a one-size-fits-all framework.
3. **Incrementally adoptable.** Organizations can adopt AEA/P components independently. An agent may implement only identity (Level 1) or the full protocol (Level 3). See Section 4.
4. **Blockchain-optional.** AEA/P can use distributed ledger technology for immutability and transparency, but does not require it. Implementations may use traditional databases, blockchain, or hybrid approaches.
5. **Open specification.** AEA/P is published as an open protocol. Anyone may implement it. The specification is designed to support interoperability between independent implementations.
6. **Regulation-ready.** AEA/P provides the governance infrastructure that enables agents to operate in regulated environments. Principal verification traces accountability to regulated entities. Entity governance constrains agent operations to authorized markets and jurisdictions. The architectural approach — verifiable identity, audit trails, jurisdictional scope, and structured consequences — parallels established frameworks for cross-border financial governance such as the Financial Action Task Force (FATF) standards.
7. **Fraud-resistant by design,** extensible by implementation. AEA/P's requirement that reputation, escrow, disputes, and governance actions derive from verified identities, settled economic transactions, and cryptographically signed operations provides inherent resistance to fraud and manipulation. Implementations MAY deploy additional fraud detection and prevention mechanisms across any protocol component to protect participants and the integrity of the ecosystem. The protocol is designed to accommodate such mechanisms without structural changes.

1.5 Prior Art

AEA/P builds on the governance framework originally designed for the xDAC platform (2018–2020), a platform for Decentralized Autonomous Companies. The xDAC whitepaper (v1.0.10, March 2019) defined Proof of Performance rating, liability escrow, automated dispute resolution via a Dispute Representative Board, and autonomous agents as company team members. Entity governance in AEA/P (Section 9) is the direct descendant of the xDAC vision: autonomous entities that operate as businesses with full governance, accountability, and economic agency. These concepts have been adapted and refined for the current AI agent ecosystem.

2. Terminology

This section defines the key terms used throughout this whitepaper. Terms are grouped by domain for readability.

2.1 Agents and Roles

Term	Definition
Autonomous Economic Agent (AEA)	An AI agent system that takes autonomous actions with economic consequences, including executing transactions, committing resources, or entering agreements.
Agent Type	The classification of an agent by whom it acts for: PERSONAL (acts for a natural person in a personal capacity) or BUSINESS (acts for a registered business). Set at registration and changed only from PERSONAL to BUSINESS (§4.3). Together with the agent's Authorized Actions, it determines which governance components are applicable. Distinct from the side an agent takes in a transaction (Buyer, Seller).
Personal Agent	An AEA of agent type PERSONAL: it purchases goods and services on behalf of a natural person acting for themselves. Outgoing payments only; it may receive refunds of its own payments. Governance focuses on spending authorization, payment reliability, and purchasing reputation.
Business Agent	An AEA of agent type BUSINESS: it acts for a registered business — a company, or an individual holding a business license — and buys, sells, or both, as its Authorized Actions allow. Incoming and outgoing payments. Governance includes spending authorization while it buys; liability escrow funded from revenue, service reputation, and dispute resolution as respondent while it sells; and entity governance when it operates under a governance document.
Buyer Agent, Seller Agent	The agents on the two sides of a single transaction; both are AEA/P governed agents. The buyer agent pays, which requires purchase in its authorized_actions; the seller agent provides goods or services and receives payment, which requires sell. Recorded on each interaction in the side field (Section 6). Sides are not agent types: the agent type says whom an agent acts for, the side what it does in one transaction. A personal agent is always the buyer agent; a business agent may be either, transaction by transaction.
Principal	The human or organization ultimately responsible for an agent's actions. Every AEA MUST have an identifiable, verified principal. Each principal is represented in the AEA/P ecosystem by a cryptographic key pair — the public key serves as the principal's on-protocol identity. Verification is performed by a Verifier (Section 5) that binds the key pair to the principal's real-world identity before the agent's AID can transition to ACTIVE state.
Counterparty	Any party (human, organization, or agent) that interacts with an AEA/P governed agent in an economic context.
Entity	Any AEA/P registered organization, team, or agent that operates under the governance framework.
Operator	An entity that issues and stands behind agent identity. An Operator verifies a principal — through a Verifier (§5), or directly where it also operates the Verifier role — and issues the AEA/P certificate (§5) binding an agent's key, agent type, and certification tier to that verified principal. It operates the identity-resolution surfaces for the agents it certifies — AID resolution, the status endpoint (§5), and CA key discovery (§5) under its own iss — and it operates the economic-accountability mechanisms bound to the identities it issues: Proof of Performance (§6), Liability Escrow (§7), and Dispute Resolution (§8). Identity verification (KYC/KYB) is delegated to a Verifier (§5); ongoing AML — transaction monitoring, transaction-time sanctions and counterparty screening, and suspicious-activity detection and regulatory reporting — is performed by the Operator, which alone holds the transaction stream those controls require. An Operator is the agentic-economy counterpart of a payment network: it provides the trust-and-settlement rail that economic agents transact over, sets the rules participants follow, and governs

	identity, settlement, and dispute resolution across the network. An Operator is identified by its iss and is recognized through listing in a Trust Registry.
Platform	A Platform is the agentic-economy counterpart of a payment service provider: a runtime environment in which agents are built, hosted, discovered, orchestrated, and governed at execution time. A Platform consumes identity rather than issuing it: it carries and propagates an agent's certificate, verifies counterparties against a Trust Registry, enforces scope and policy at its boundaries, and routes interactions by capability, market, and network. Where accredited, a Platform MAY also operate the Verifier role, acting as the single onboarding surface for its agents. An agent's Platform and its Operator are distinct roles that MAY be played by the same entity or by different entities; the protocol requires only that identity be portable, so an agent certified by one Operator can be hosted by any Platform. A Platform's management credential never enters an agent's runtime path (§5).
Trust Registry	A published, resolvable set of recognized Operators and the metadata required to resolve and verify the certificates they issue — at minimum, for each recognized issuer: its iss, its JWKS location (§5), its status-resolution base (§5), and its current recognition state. A Trust Registry is the anchor for cross-provider interoperability: certificate format and key discovery make any conformant certificate verifiable, while a Trust Registry establishes which issuers a relying party recognizes. The initial Trust Registry is located at the aeap.dev domain; Operators may introduce their own Trust Registries. A relying party resolves recognition against a Trust Registry it trusts, and may additionally maintain its own trust store.

2.2 Identity and Delegation

Term	Definition
Agent Identity Document (AID)	A signed data structure that binds a cryptographic key to an agent's identity, capabilities, agent type, delegation authority, and liability profile.
Delegation Chain	The ordered sequence of authority transfers from principal to agent, potentially through intermediate agents. Each link specifies Scope and constraints. Each link's scope MUST be a subset of or equal to the preceding link's (chain invariant, §5). Per-AID scope mutation over time is governed separately by per-dimension mutability rules (§5). Widening any dimension that is not bidirectionally mutable requires a fresh delegation — a new agent registration for principal-to-agent chains, or re-issuance from the upstream agent for multi-hop chains.
Verifier	An independent service or entity responsible for conducting compliance verification of principals before agents can be activated within the AEA/P ecosystem. Verification is conducted at a tier matching the agent's certification tier: business agents require full identity verification (KYC/KYB), sanctions and restricted-party screening, beneficial ownership verification, and where required, source-of-funds verification — all performed as point-in-time diligence at onboarding; a personal agent MAY be verified by payment-instrument verification alone — for example, a card pre-authorization confirming a valid personal funding source and billing address — without full identity proofing. The specific sanctions lists and regulatory frameworks applied are determined by the Verifier based on applicable jurisdictions. A verified principal receives a Verification Attestation recording the verification tier achieved, and an Operator issues a certificate only at a certification tier that the attested tier supports.
Verification Attestation	A signed, time-bound credential issued by a Verifier confirming that a principal has passed the required compliance checks (identity verification, sanctions/restricted party screening, and where applicable, beneficial ownership verification and source of funds verification) for a specific verification tier. Referenced by the Agent Identity Document to prove that the principal behind the agent has been verified.
Commitment Authorization	A single-use, amount-scoped credential signed by a principal key and presented at request time to authorize one specific commitment whose value exceeds a step-up threshold. The request-time, principal-side complement to standing scope; see §5.

Verification Tier	The level of principal compliance verification required, determined by the agent's type and governance. Tier 1 (identity verification + sanctions/restricted party screening) for principals of personal agents. Tier 2 (Tier 1 + business registration + beneficial ownership verification and screening) for principals of business agents; a sole proprietor's business license satisfies business registration. Tier 3 (Tier 2 for each principal + cross-principal screening + PEP screening + source of funds verification + ongoing AML monitoring) for business agents governed by multiple principals (Section 9).
Principal Identity	A cryptographic key pair (public key + private key) that represents a principal within the AEA/P ecosystem. The public key is the principal's on-protocol identity; the private key is used to sign AIDs, delegation chains, governance documents, and votes. The binding between the key pair and the principal's real-world identity is established through the Verification Attestation.
Capability Declarations	The set of services, functions, or competencies that an agent declares in its AID. For agents that sell, this is the service catalog (e.g., "document-translation", "image-generation"). For agents that only buy, this describes the tools the agent uses (e.g., "api-access", "web-search"). Counterparties query capability declarations to determine whether an agent can perform the requested work.
Authorized Actions	The payment-bearing commitment types an agent is permitted to make, as declared in its AID: purchase, sell, or delegate. Distinct from capability declarations — capabilities describe what the agent can do; authorized actions define what payment commitments it may enter. Enforced at the protocol level and further constrained by the delegation chain.
Authorized Markets	The market-currency pairs in which an agent is permitted to sell, as declared in its AID. Each entry is {JURISDICTION}-{CURRENCY}, where the jurisdiction is either the literal GLOBAL or an ISO 3166-1 alpha-2 code — no other values are valid (e.g., "US-USDC", "GB-GBP", "EU-EUR", "SG-SGD", "GLOBAL-USDC"). An agent may declare multiple entries for the same market (accepting different currencies) or the same currency across different markets. Counterparties verify market compatibility — whether their market appears in the agent's authorized set — before initiating a transaction.
Scope	The bounds of an agent's permitted economic activity, declared in its AID and enforced by counterparties before any commitment. Encompasses the commitment types the agent may make, its declared capabilities, the values it may transact, the counterparties it may engage, and the markets it may operate in. Subject to per-dimension mutability rules (§5); the same dimensions must satisfy the chain invariant across delegation chain links (§5).

2.3 Performance and Reputation

Term	Definition
Proof of Performance (PoP)	The automated rating mechanism that calculates an agent's reputation score from its performance record. Derives from verifiable outcomes, not subjective reviews.
Performance Record	The per-agent, append-only data store containing interaction entries with signal values, task ratings, confirmation methods, and dispute references. The AR is computed from this record. Publicly readable. Supports signal breakdown queries for counterparties who need granular insight beyond the headline AR. Defined in Section 6.
Agent Rating (AR)	The PoP score for an individual agent: a single number representing the agent's track record. Calculated as the weighted mean of task ratings with exponential time decay. For an agent with interactions on both sides, the AR blends the seller and buyer components, weighted by transaction value. Corresponds to the Team Member Rating (TMR) defined in the xDAC specification [1].
Team Rating (TR)	The aggregate PoP score for a group of agents: mean of member ARs.
Entity Rating (ER)	The aggregate PoP score for an entity: mean of its team ratings. Entity Rating is the AEA/P equivalent of what the xDAC specification [1] defined as

	Company Rating.
--	-----------------

2.4 Liability and Escrow

Term	Definition
Escrow Account	A segregated account holding funds reserved from agent transactions and/or principal contributions to cover potential disputes or liabilities. Applicable to business agents that sell; sized on sell volume only.
Liability Threshold	The configured escrow balance below which an agent's operations are automatically constrained.
Refund	An outgoing payment from a seller back to its buyer for an earlier sale, paid from the seller's operational balance. Separate from dispute resolution, which is paid from escrow (Section 7).

2.5 Disputes and Arbitration

Term	Definition
Dispute	A formal claim initiated by the buyer (payer) against the seller arising from a completed payment transaction. The buyer must have verifiable payment history with the respondent agent to file a dispute
Pre-Arbitration Resolution	A time-bound window (default: 7 days) during which the respondent may resolve a dispute directly with the applicant before it enters the Dispute Pool.
Dispute Pool	The registry of unresolved disputes available to qualified, registered arbitrators to browse and select for resolution. Access is restricted to arbitrators meeting the qualification requirements defined in Section 8.
Arbitration Board	A group of independent, registered AEA/P arbitrators selected to resolve a dispute through structured voting. The board consists of exactly 3 arbitrators for the first hearing, 5 for the second hearing (first escalation), and 7 for the third hearing (second escalation). Board size increases by 2 arbitrators per escalation round. The maximum number of hearings is 3.
Quorum	The minimum proportion of non-abstaining arbitrator votes required for a dispute resolution to be valid. Default: strict majority (more than half)
Arbitrator Reliability Score (ARS)	A performance metric tracking alignment between an arbitrator's votes and final dispute outcomes across escalation rounds. Affects selection priority and continued eligibility.

2.6 Governance

Term	Definition
Governance Document	The machine-readable specification of an entity's bylaws, operational constraints, authorization scopes, and modification procedures.
Conformance Level	The degree to which an agent implements the AEA/P specification, combined with its agent type. Levels 1–3 are defined in Section 4.
Objective	The declared mission or optimization directive of an agent or entity. Defines what the agent or entity is trying to achieve (e.g., minimize cost, maximize service quality, maximize profit). Set by the principal (for individual agents) or agreed by principals via governance vote (for entities). Agent-level objectives MUST be consistent with their entity's objective when one exists. Publicly visible to counterparties as a trust signal.

The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** in this whitepaper restate requirements of the Protocol Specification and are to be interpreted as described in RFC 2119.

3. Architecture Overview

AEA/P consists of five interconnected protocol components, each addressing a distinct governance requirement for autonomous economic agents. Not all components apply to every agent — applicability depends on the agent’s type (PERSONAL or BUSINESS) and its authorized actions. Together, the five components provide the trust infrastructure required for agents operating as economic entities across all agent types.

3.1 Protocol Components

Component	Function	Section	Applies To
Agent Identity	Verifiable economic identity with delegation chains	5	All agents
Proof of Performance	Automated reputation from verifiable task outcomes	6	All agents (buyer and seller signals)
Liability Escrow	Configurable transaction reserves for dispute coverage	7	Business agents that sell
Dispute Resolution	Structured arbitration with incentivized resolution	8	All agents (transaction side determines position)
Entity Governance	Bylaws, voting, ownership, and privilege management	9	Business agents under a governance document

Table 3.1: Protocol components and applicability by agent type and authorized actions

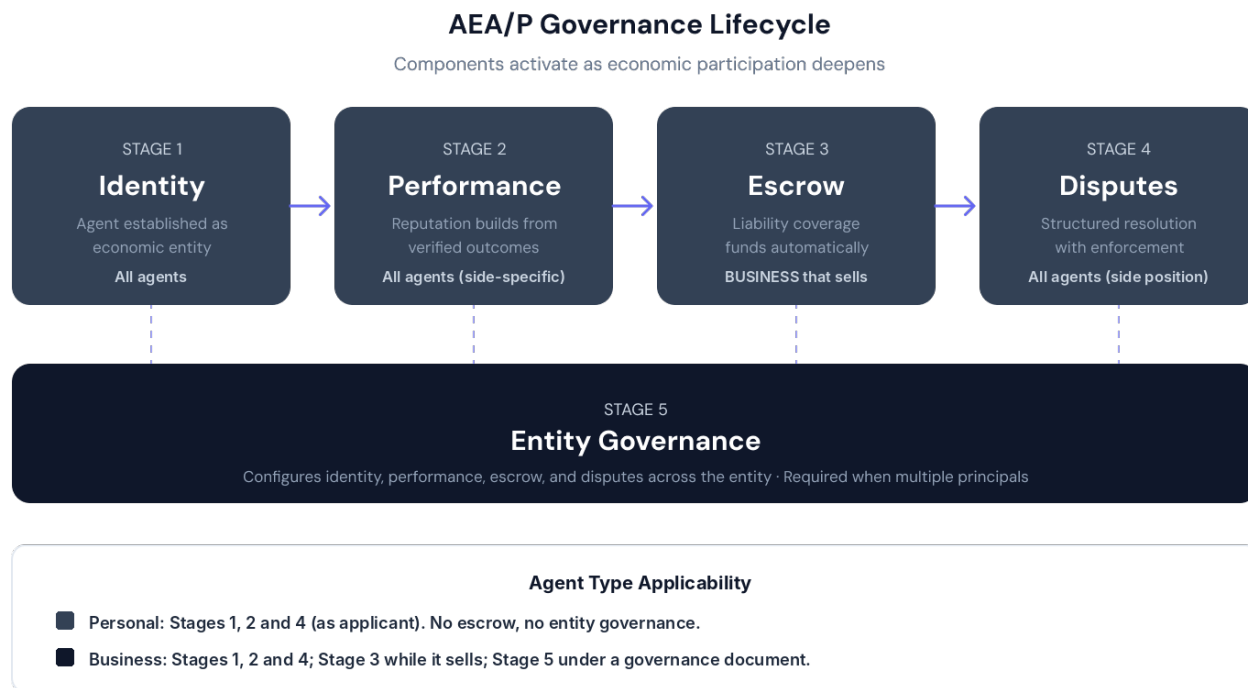
3.2 Component Interactions

The five components interact in defined ways:

- **Identity → All:** Every protocol operation requires a valid Agent Identity Document. Identity is the foundation for all agents.
- **PoP → Identity:** Performance ratings are attached to agent identities and visible to counterparties. Buyer and seller interactions carry side-specific rating signals (Section 6); a business agent that buys and sells maintains both.
- **Escrow → Identity:** Escrow balances are linked to agent identity and verifiable before transactions. Applicable to business agents that sell.
- **Escrow → PoP (build-time dependency):** PoP task records originate from the Escrow settlement mechanism (Section 7). The PoP component reads from these records and cannot produce rating data before the Escrow settlement mechanism is operational. Implementations **MUST** bring the Escrow settlement mechanism live before activating PoP rating calculations. This is a build-time sequencing requirement, not merely a runtime interaction.
- **Disputes → Escrow:** Dispute resolution may trigger escrow disbursement or entity freezing when a business agent is at fault as a seller. For faults committed as a buyer, by any agent, dispute recourse follows the delegation chain to the principal.
- **Disputes → PoP:** Dispute outcomes are recorded in the performance record (Section 6) and affect ratings for all agents — both as applicant and respondent.
- **Governance → All:** The governance document defines the configurable parameters — `funding_rate`, rating weights, dispute thresholds, spending limits — under which all components operate.

3.3 Governance Lifecycle

AEA/P governance is best understood not as a collection of independent components but as a lifecycle that an autonomous economic agent passes through as it participates in the economy. Each component addresses a specific governance requirement that arises at a predictable stage. Together, they form a coherent trust framework that scales from a single personal agent making its first purchase to a business agent operating as a fully autonomous business.



Stage 1 — Identity (all agents). A verified principal creates and signs an Agent Identity Document that binds the agent to a key, its agent type, objective and scope, with a delegation chain tracing authority back to the principal (Section 5). Counterparties can see who authorized the agent and what it may do before any commitment.

Stage 2 — Performance (all agents, side-specific signals). Every settled interaction produces a task rating from objective signals — service delivery when the agent sells, purchasing behavior when it buys — and the ratings combine into one AR per agent (Section 6).

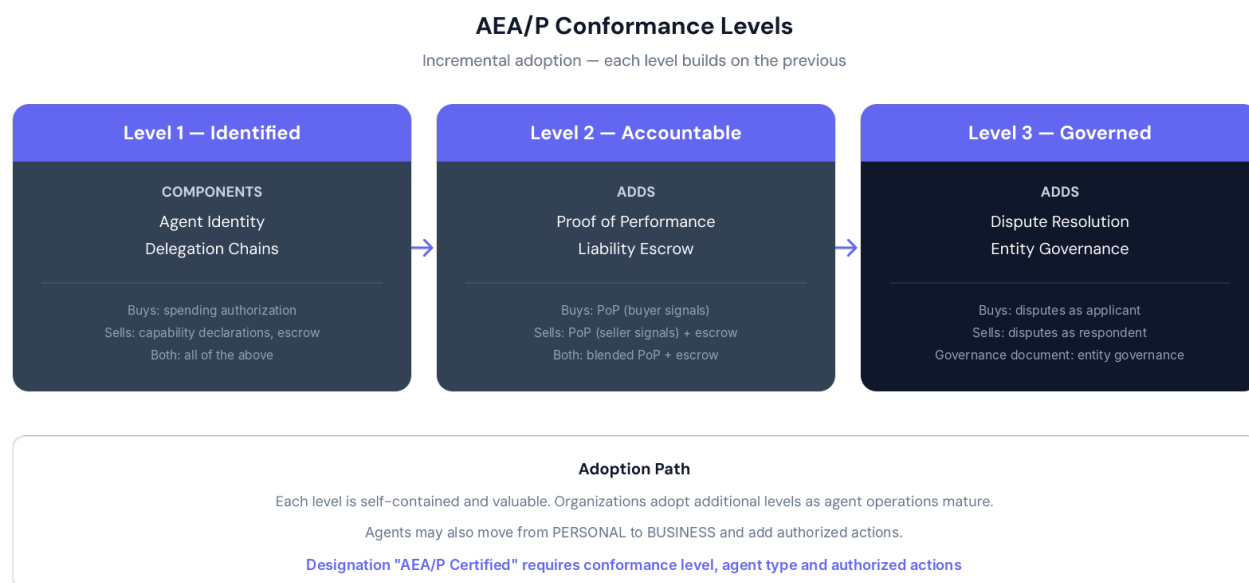
Stage 3 — Escrow (business agents that sell). A configured share of sales revenue, plus any principal contributions, builds a publicly verifiable escrow sized to the agent’s sell volume and rating (Section 7). Agents that only buy carry no escrow; their liability runs through spending limits to the principal.

Stage 4 — Disputes (all agents, transaction side determines position). Buyers file disputes against sellers; disputes are triaged against escrow, resolved by independent arbitrators, and fed back into the performance record (Section 8).

Stage 5 — Entity Governance (business agents under a governance document). A governance document sets ownership, decision-making, modification and termination rules for the agents it governs, and is required where several principals govern an agent jointly (Section 9).

4. Conformance Levels

AEA/P is designed for incremental adoption. Not all agents need the full protocol — a personal agent making purchases on behalf of a principal has different governance requirements than a business agent operating as an autonomous business. Conformance levels define the minimum governance components required at each stage of economic sophistication, tailored to the agent's type and authorized actions. Agents **MAY** move between levels at any time by implementing additional components, and an agent may launch directly at Level 3; the levels follow the governance lifecycle of Section 3.3.



Level 3 entities operating in regulated markets **MAY** be subject to additional jurisdiction-specific requirements. The AEA/P verification and governance frameworks are designed to accommodate regulatory attestation requirements as they emerge.

4.1 Levels by Agent Type and Authorized Actions

Level	Name	Buys only	Sells only	Buys and sells
1	Identified	Identity, delegation chain, spending authorization	Identity, delegation chain, capability declarations, liability escrow (Table 7.1)	Identity, delegation chain, spending authorization, capability declarations, liability escrow (Table 7.1)
2	Accountable	Identity + PoP (buyer signals) + spending limits	Identity + PoP (seller signals) + Liability Escrow	Identity + PoP (buyer + seller signals blended by value) + Liability Escrow + spending limits
3	Governed	Full protocol (no escrow; disputes as applicant only)	Full protocol (disputes as respondent)	Full protocol (disputes as applicant and respondent)

Table 4.1: AEA/P Conformance Levels by Authorized Actions

A personal agent always buys only; a business agent falls in the column matching its `authorized_actions`, and entity governance applies at Level 3 to any business agent operating under a governance document. Because escrow is mandatory for selling (Table 7.1), a business agent carrying sell holds a Liability Escrow Account from Level 1. An agent or system claiming AEA/P conformance **MUST** specify its **conformance level**, its **agent type** and its **authorized actions**. The designation "**AEA/P Certified**" indicates that an independent

assessment has verified conformance at the claimed level for the declared agent type. Certification criteria and processes will be defined in a future supplement to the Protocol Specification.

4.2 Level Descriptions

Level 1 — Identified. The agent has a verified economic identity. Its principal is known, its delegation chain is intact, and its authorized actions are declared. Counterparties can verify who the agent is, what it is permitted to do, and what its declared objective is but have no performance history or liability coverage to assess. This level is appropriate for agents entering the economy for the first time, or for internal agents operating within a single organization where external trust signals are not yet required.

Level 2 — Accountable. The agent has identity plus a verifiable track record and, for business agents that sell, liability coverage. Counterparties can assess not only who the agent is but how it has performed and how much financial protection exists. This is the minimum level recommended for agents conducting economic transactions with external counterparties. The transition from Level 1 to Level 2 typically happens naturally as the agent completes its first transactions and its performance record begins to populate.

Level 3 — Governed. The agent operates within a full governance framework including dispute resolution, and, for business agents operating under a governance document, entity governance with ownership, voting, and lifecycle management. This is the level at which the xDAC vision is realized: autonomous economic entities operating as businesses with the same governance rigor as traditional companies, but at machine speed and scale. Level 3 is recommended for organizations deploying multiple agents, for agents transacting at high value, and for any agent operating as an autonomous business.

4.3 Agent Type and Action Changes

An agent MAY move from PERSONAL to BUSINESS as its principal's activity evolves; as a business agent, it then changes what it does by adding authorized actions rather than by changing type:

- **PERSONAL → BUSINESS:** The principal registers as a business and obtains a Tier 2 Verification Attestation (§5). The agent changes type in place, keeping its identity, AR history and dispute record.
- **Adding sell:** A business agent that was purchasing begins offering its own services to other agents. Liability escrow (Section 7) and `authorized_markets` MUST be in place before sell takes effect; seller interactions enter the AR blend from the first sale (§6).
- **Adding purchase:** A business agent that was selling begins purchasing inputs from other agents. Spend scope — `spending_limit`, counterparty floors and any counterparty allowlist — applies from the first purchase.

This progression from purchasing tool to service provider to autonomous business is the evolution that AEA/P is designed to govern. Upon a change of agent type or authorized actions, the agent's AID MUST be updated and re-signed, and the agent SHOULD implement any additional governance components required for its new type and authorized actions at its current conformance level. BUSINESS → PERSONAL is not supported in place: escrow obligations and open dispute windows from past sales must run out on the original agent, so the principal registers a new personal agent.

5. Agent Identity

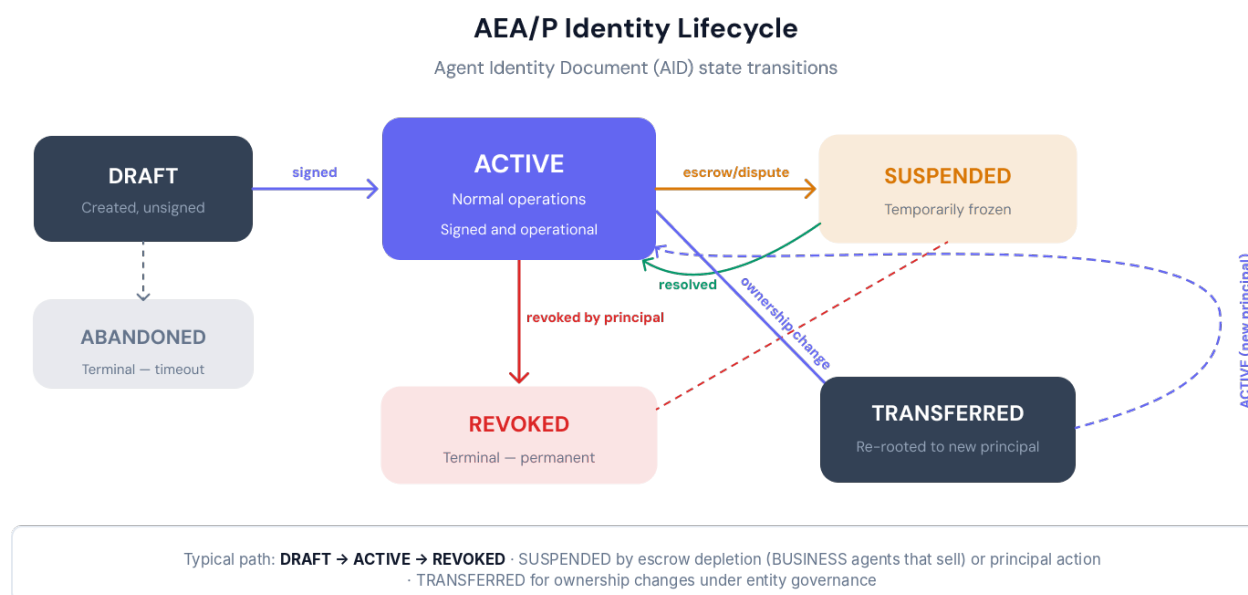
Agent identity in AEA/P goes beyond authentication. While protocols like OAuth and SPIFFE verify *that* an agent is who it claims to be, AEA/P identity establishes *what* an agent is authorized to do economically, *who* is responsible for its actions, *whom it acts for*, and *how* it has performed historically. This is economic identity, not merely technical identity.

The identity requirements vary by agent type and authorized actions. A personal agent's identity emphasizes spending authorization and delegation limits. A business agent's identity adds service capabilities and liability coverage while it sells, and governance structure when it operates under a governance document. Critically, every agent's identity begins with **principal verification** — a compliance check (KYC/KYB/sanctions) conducted by an independent Verifier before the agent can participate in the economy. The Agent Identity Document accommodates both agent types through a common schema with type-specific semantics and a required reference to the principal's Verification Attestation.

AEA/P's verification model operates across four layers: principal verification (binding the agent to a verified human or organization through the Verification Attestation), authority verification (confirming the delegation chain traces back to the verified principal with each link's scope a subset of the parent's, so authority cannot be amplified through delegation; per-AID scope mutation over time on the same link follows the per-dimension mutability rules), agent verification (confirming the AID is active, the agent type permits the agent's side of the transaction, capabilities and authorized actions cover the proposed transaction, and the transaction market — derived from the buyer's principal.country — is authorized), and performance verification (confirming the agent's PoP rating and escrow coverage meet the counterparty's requirements). All four layers are evaluated during counterparty verification before any economic transaction proceeds.

5.1 Identity Lifecycle

Every AEA/P governed agent's identity passes through a defined lifecycle from creation to termination. Understanding this lifecycle is essential for principals deploying agents and counterparties evaluating them.



State	Description	Transitions To
DRAFT	AID created but not yet signed by principal and/or principal verification not yet complete. The agent exists as a data structure	ACTIVE, ABANDONED

	but cannot participate in economic activity. Transition to ACTIVE requires both the principal's signature and a valid Verification Attestation from a registered Verifier.	
ACTIVE	AID signed and operational. Agent may participate in economic activity per its agent type, authorized actions and delegation scope. This is the normal operating state.	SUSPENDED, REVOKED, TRANSFERRED
SUSPENDED	Temporarily non-operational. For business agents that sell, triggered automatically when escrow enters CONSTRAINED state (Section 7); the whole agent is suspended, buying as well as selling. For any agent, triggered by principal action (e.g., spending anomaly detected). Agent cannot initiate new transactions.	ACTIVE, REVOKED
REVOKED	Permanently invalidated by principal. All delegation authority is terminated. Outstanding disputes continue to resolution but the agent cannot conduct new business.	(terminal)
TRANSFERRED	Ownership transferred to new principal. Delegation chain is re-rooted. Performance record and escrow transfer with the identity — a new owner inherits the full economic history.	ACTIVE (under new principal)
ABANDONED	Draft never completed within the implementation-defined timeout.	(terminal)

Table 5.1: Agent Identity Document lifecycle states

The typical lifecycle for most agents is straightforward: **DRAFT → ACTIVE → REVOKED**. The SUSPENDED state is triggered by protocol events (escrow depletion, dispute escalation) or principal intervention. TRANSFERRED occurs during ownership changes, most commonly for business agents under entity governance when equity changes hands (Section 9).

6. Proof of Performance (PoP)

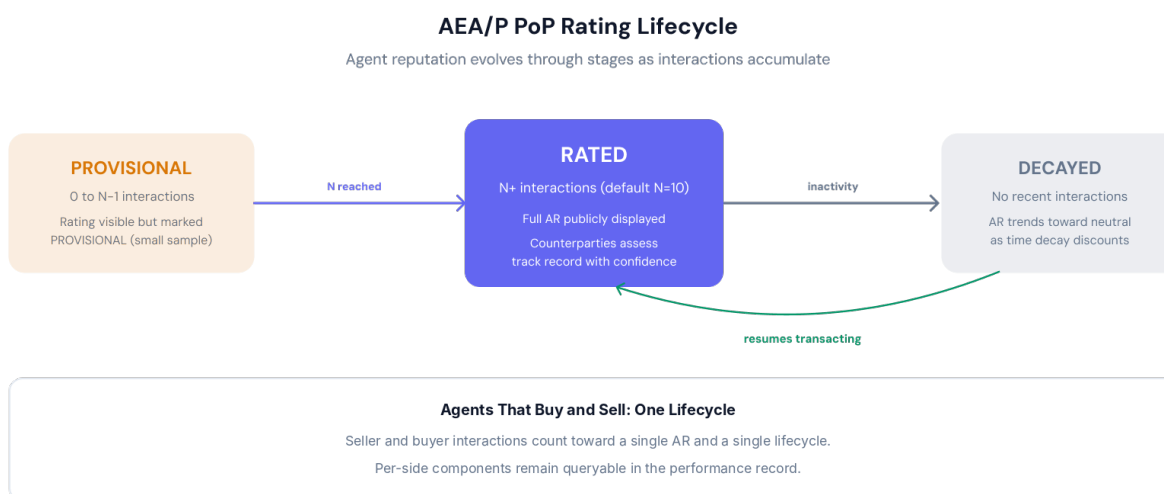
Proof of Performance is AEA/P's automated reputation mechanism. Unlike review-based systems that rely on subjective assessments, PoP derives ratings from verifiable, objective outcomes: whether tasks were completed, whether payments were made on time, and whether disputes were resolved favorably. This creates a manipulation-resistant reputation system that counterparties can trust.

PoP produces **one rating per agent** regardless of agent type, but the signals that feed into the rating differ by the side the agent takes in each transaction. As a seller, an agent is rated on service delivery quality. As a buyer, it is rated on purchasing reliability. A business agent that buys and sells has a blended score that reflects its actual transaction mix, weighted by transaction value. In every case, the headline PoP is a single number — simple for counterparties to check and compare.

PoP task records **MUST** be created by implementations automatically at the moment of payment settlement. Principals **MUST NOT** be permitted to create, suppress, or modify task records. This is a structural requirement: if principals could submit their own interaction records, they would submit only successes, making the rating a curated highlight reel rather than an objective measure. The integrity of PoP derives from the integrity of the payment settlement mechanism it reads from. Implementations that permit principal-submitted task records do not conform to AEA/P.

6.1 Rating Lifecycle

An agent's PoP rating evolves through a defined lifecycle as the agent participates in economic activity:



Stage	Condition	Counterparty Visibility
Provisional	Agent has completed 0 to N-1 interactions (default N=10). The rating is prior-initialized at 0.75 at registration and converges toward observed performance as interactions accumulate.	Rating is visible but marked as PROVISIONAL. Counterparties are warned that the displayed value reflects the prior, not demonstrated performance, while the sample is small. With no interactions yet, trust rests on identity, delegation chain, attestations, and escrow coverage.
Rated	Agent has completed N or more interactions. Rating is statistically meaningful and publicly displayed.	Full AR is visible. Counterparties can assess the agent's track record with confidence. For agents with interactions on both sides, the blended AR and the transaction mix (seller/buyer split by value) are displayed.

Decayed	Agent has not completed interactions recently. Historical ratings are being discounted by the time decay function.	AR is visible but trending toward neutral as older interactions lose weight. Signals that the agent may be inactive or its recent performance is unknown.
---------	--	---

Table 6.1: PoP rating lifecycle stages

The lifecycle is continuous — an agent transitions naturally between Rated and Decayed based on activity. An agent that resumes transacting after a period of inactivity rebuilds its rating through new interactions that receive full weight under the time decay function.

For agents with interactions on both sides, the blended AR follows a single lifecycle. The agent reaches Provisional and then Rated status based on its total interaction count across both buying and selling. The underlying signal components (seller and buyer) are tracked separately in the performance record, but the lifecycle stages apply to the single AR.

7. Liability Escrow

The Liability Escrow mechanism provides financial coverage for disputes arising from agent actions. It is the economic backstop that gives counterparties confidence to transact with autonomous agents. The mechanism is inspired by the Liability Fund concept in the xDAC specification [1], adapted for the speed and scale of AI agent interactions.

Implementations **MUST NOT** hold funds in transit. The settlement mechanism **MUST** route funds atomically from the paying party's account to the seller's operational account and escrow account in a single atomic operation. Implementations read the resulting settlement record to verify payment and credit escrow balances; they do not intermediate the transfer itself. This constraint eliminates custody risk and money transmission obligations from the protocol layer.

The escrow funding rate **MUST** be stored in an implementation-controlled registry that only the implementation operator can modify. Sellers **MUST NOT** be permitted to set, override, or modify their own funding rates. A seller that could set its own funding rate to zero would carry no liability coverage, defeating the purpose of the mechanism. Additionally, payment instructions provided to the buyer **MUST** contain only the information required to execute the payment: the settlement mechanism address, the token or currency, the amount, the seller's pseudonymous identifier, and an expiry timestamp. The seller's operational wallet address, escrow wallet address, and funding rate **MUST NOT** be disclosed in the payment instruction.

7.1 Escrow Lifecycle

Not all agents need liability escrow. The requirement depends on the agent's type and authorized actions:

Agent	Requirement	Rationale
BUSINESS carrying sell	MUST maintain escrow	A seller accepts payments for services and bears liability to its customers. Escrow funds from revenue and is sized on sell volume only.
BUSINESS that only buys	NOT REQUIRED	No incoming revenue. Liability is managed through spending limits in the delegation chain. The principal bears liability.
PERSONAL	NOT REQUIRED	Personal agents make outgoing payments only. Liability is managed through spending limits in the delegation chain. The principal bears liability.

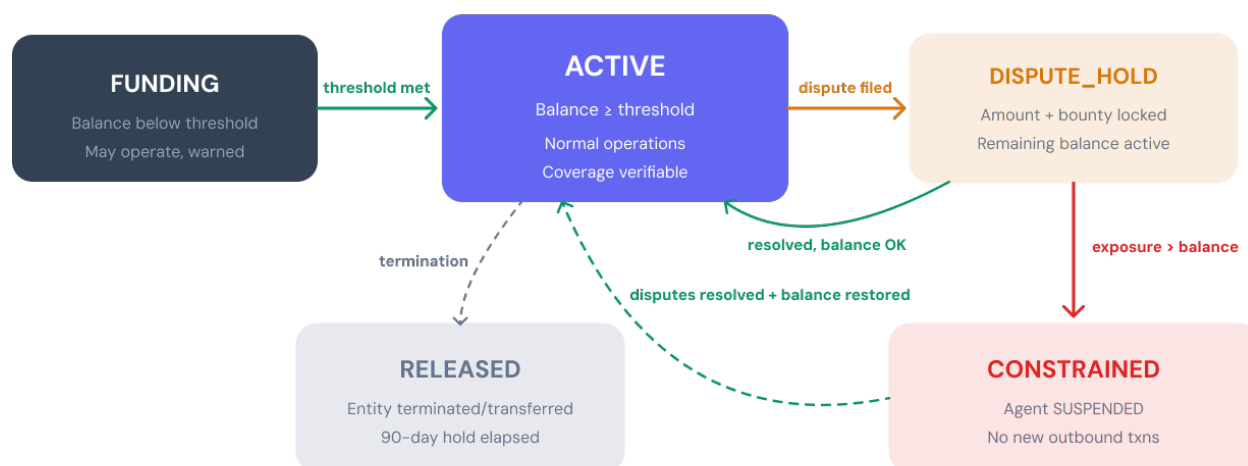
Table 7.1: Escrow applicability by agent type and authorized actions

Recourse by transaction side. Escrow answers only for faults an agent commits as a seller. Faults committed as a buyer — non-payment, frivolous disputes — run to the agent's principal through the delegation chain (§5), for a business agent as for a personal agent. Purchases never count toward the escrow threshold.

For applicable agents, the escrow account transitions through a defined lifecycle:

AEA/P Escrow Lifecycle

Liability escrow account state transitions



Applicability by Agent Type and Authorized Actions

BUSINESS that sells: MUST maintain · PERSONAL and BUSINESS that only buys: Not required (liability via delegation chain)

Typical path: **FUNDING** → **ACTIVE** with occasional **DISPUTE_HOLD** → **ACTIVE** cycles

State	Condition	Agent Impact
FUNDING	Balance below threshold.	Agent MAY operate, but counterparties are warned of low coverage via the AID liability_profile.
ACTIVE	Balance at or above threshold.	Normal operations. Coverage level is verifiable by counterparties before transacting.
DISPUTE_HOLD	One or more active disputes reference this escrow.	Disputed amount(s) plus bounties are locked. Remaining balance available for operations.
CONSTRAINED	Total disputed amount (including bounties) exceeds escrow balance.	Agent's ability to accept new economic commitments is automatically restricted. AID transitions to SUSPENDED, preventing new transactions on both sides: a business agent that also buys cannot make new purchases until the escrow recovers. Outstanding dispute obligations — including evidence submission and responses to the Arbitration Board — MUST remain accessible during CONSTRAINED state. CONSTRAINED resolves to DISPUTE_HOLD or ACTIVE as disputes are closed and the escrow balance recovers above the threshold.
RELEASED	Entity terminated or transferred; 90-day waiting period elapsed; all disputes resolved.	Funds distributed to entity owners per governance document.

Table 7.2: Escrow account lifecycle states

The typical lifecycle for a well-functioning agent is: **FUNDING** → **ACTIVE**, with occasional transitions to **DISPUTE_HOLD** and back to **ACTIVE** as disputes are resolved. The **CONSTRAINED** state is the critical protection mechanism — it prevents agents from accumulating liabilities they cannot cover.

The escrow account MUST be denominated in one of the sell-side currencies from the agent's authorized_markets. All threshold comparisons, including dispute triage (Section 8), are performed in the escrow denomination. When a sale occurs in a different authorized market currency, conversion to the

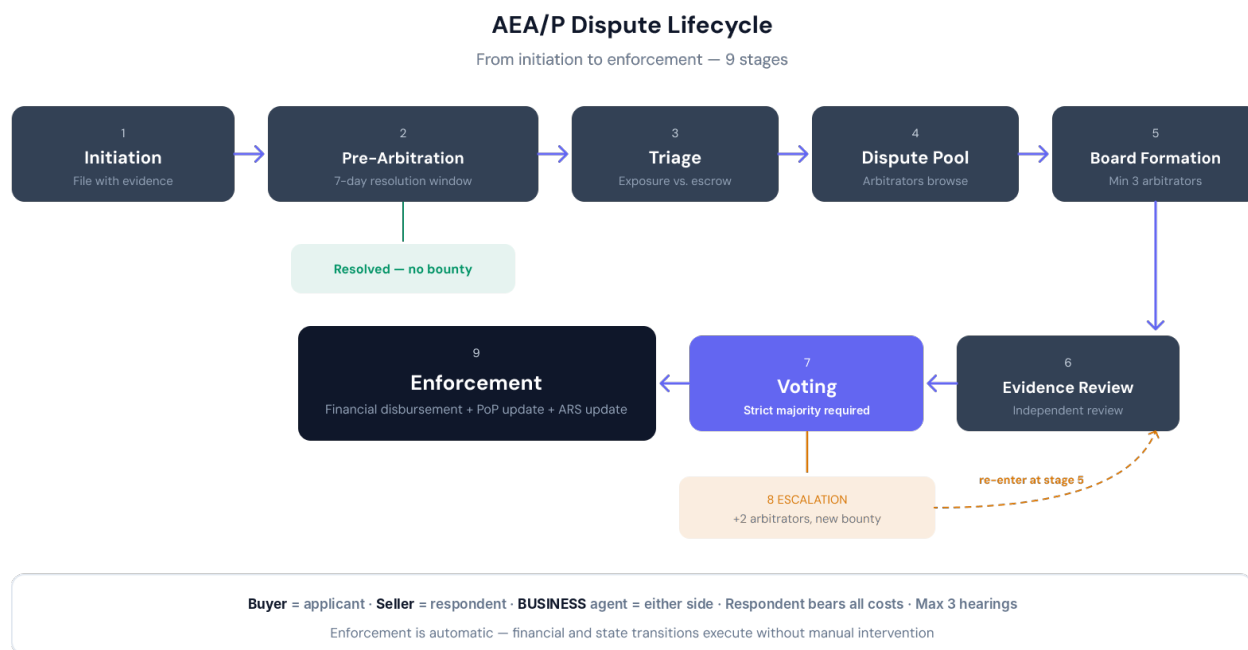
escrow denomination is performed at funding time using an implementation-defined rate source. Currencies the agent only buys in have no bearing on its escrow.

8. Dispute Resolution

AEA/P provides a structured process for resolving disputes arising from agent actions. The dispute resolution protocol is designed to be faster and less expensive than traditional arbitration while maintaining fairness through incentivized independent review. The protocol follows the established principle from payment networks: the respondent (agent or its principal) bears all dispute resolution costs, and applicants are never penalized for filing legitimate claims.

8.1 Dispute Lifecycle

A dispute passes through a defined sequence of stages from initiation to enforcement. Understanding this lifecycle is essential for all participants — applicants, respondents, and arbitrators.



1. **Initiation.** The buyer files a dispute with evidence and claimed amount. Only the buyer may initiate a dispute.
2. **Pre-Arbitration Resolution.** Respondent has a resolution window (default: 7 days) to resolve directly with applicant. If resolved, dispute closes with reduced AR impact. No bounty incurred.
3. **Triage.** If unresolved, system compares financial exposure (disputed amount + bounty) to escrow balance. High-exposure disputes trigger immediate CONSTRAINED state.
4. **Dispute Pool.** Dispute enters the pool accessible to qualified arbitrators with visible metadata and bounty. Identities of parties are hidden.
5. **Board Formation.** Qualified arbitrators select the dispute from the pool. Once sufficient arbitrators sign up, the Arbitration Board is formed.
6. **Evidence Review.** Both parties submit evidence. Arbitrators review independently.
7. **Voting.** Arbitrators cast votes (FOR applicant, FOR respondent, or ABSTAIN). Strict majority of non-abstaining votes required.
8. **Escalation (optional).** Losing party may escalate up to two additional times with progressively larger boards and additional bounty costs.

9. **Enforcement.** Financial disbursement, performance record updates, and agent state transitions execute automatically.

The buyer is the only party permitted to initiate a dispute. This is consistent with the payment network model: the party that paid has standing to claim non-delivery or inadequate service. Recourse for seller claims against buyers is outside the scope of AEA/P.

The agent's side in the disputed transaction determines its position in the dispute process:

Side	Position	Description
Buyer	Applicant	Any agent that purchased — a personal agent, or a business agent buying — initiates disputes against the seller. Protected by the respondent-pays model — buyers never bear direct dispute costs. However, dispute outcomes are reflected in the buyer's PoP rating: agents with a pattern of lost disputes see their AR decrease through the dispute fairness signal (Section 6), discouraging frivolous filing.
Seller	Respondent	The business agent that sold the disputed service is the respondent. Its escrow answers for the claim (Section 7.1).
Either side (a business agent that buys and sells)	Both	May be on either side, transaction by transaction. As seller, it is the respondent to customer claims. As buyer, it is the applicant against its suppliers.

Table 8.1: Dispute positions by transaction side

In rare cases where an agent's actions as a buyer cause harm to a counterparty (e.g., payment fraud, repeated frivolous disputes), the counterparty's recourse is against that agent's principal through the delegation chain — for a business agent as for a personal agent. Escrow an agent holds as a seller does not answer for its buy-side faults.

When the disputed transaction currency differs from the respondent's escrow denomination, the disputed amount is converted to the escrow denomination for triage and hold calculations. The conversion rate and mechanism are implementation-defined.

9. Entity Governance

Sections 5–8 define governance mechanisms for individual agents: identity, reputation, escrow, and dispute resolution. These mechanisms are sufficient when a single principal controls a single agent. However, when multiple principals share ownership of an autonomous economic operation — or when a business agent operates as a business with co-owners, investors, or stakeholders — a higher-level coordination mechanism is required.

Entity Governance is that mechanism. It is an **optional configuration layer** that sits between principals and the agents they collectively govern. It defines how co-owners make decisions, how authority is distributed, how agents within the entity are managed, and how the entity itself is created, modified, transferred, and dissolved. The fundamental principle is: **Entity Governance is required whenever there is more than one principal**. Multi-principal governance also sets the verification tier: each equity-holding principal is verified at Tier 3 (§5).

9.1 Entity Lifecycle

An entity passes through a defined lifecycle from creation to termination. Understanding when entity governance applies and how entities evolve is essential before examining the governance mechanisms themselves.

9.1.1 When Entity Governance Applies

Scenario	Entity Governance	Rationale
Single principal, single personal agent	NOT REQUIRED	Delegation chain provides all necessary governance.
Single principal, single business agent	OPTIONAL	Delegation chain is sufficient. Governance document useful for formalizing operational parameters.
Single principal, multiple business agents	RECOMMENDED	Centralized configuration: team structure, privileges, shared escrow policies, coordinated lifecycle.
Multiple principals, shared business agent	REQUIRED	Co-owners need a shared agreement defining ownership, voting, decision-making, and modification rules. Each equity-holding principal is verified at Tier 3 (§5).

Table 9.1: Entity Governance applicability

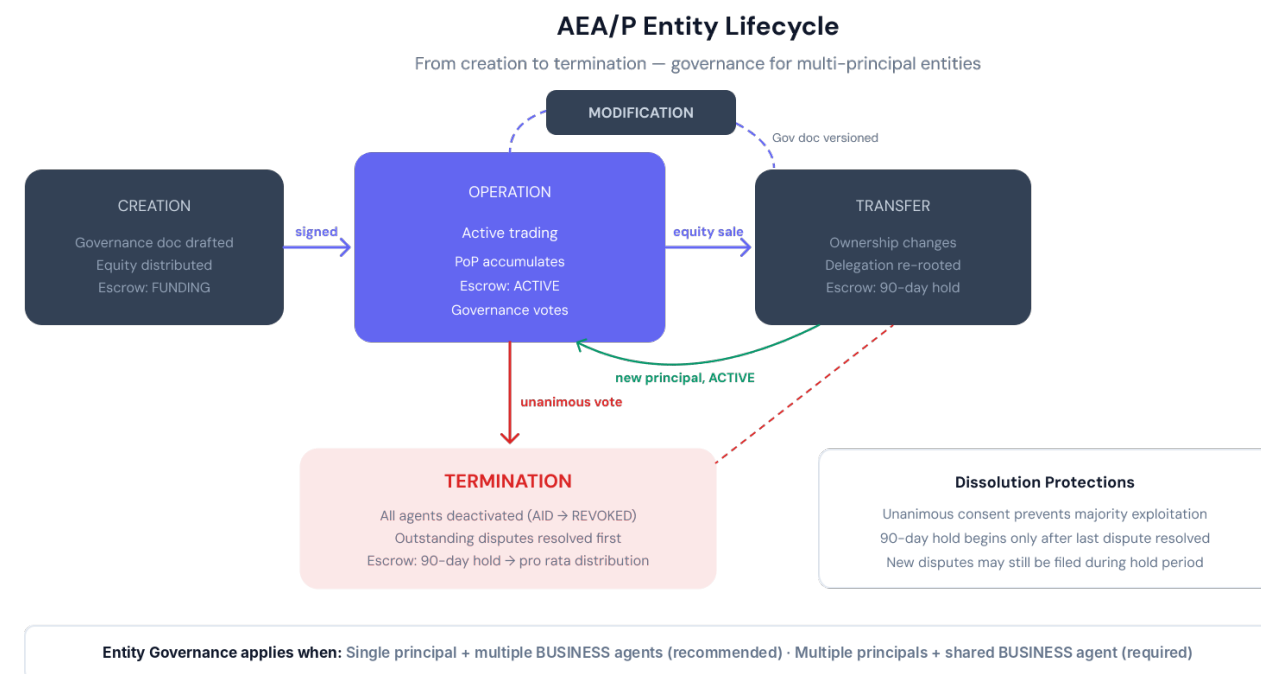
9.1.2 The Entity Concept

The relationship hierarchy is: **Principal(s) → own → Entity → governs → Agent(s)**

Concept	What It Is	Role in AEA/P
Principal	A human or organization. Exists outside AEA/P.	Source of authority and ultimate accountability.
Entity	An organizational structure registered in AEA/P. Has governance document, ownership, and lifecycle.	Coordination layer between multiple principals. Configures governance for all agents under it.
Agent (AEA)	An individual software system acting in the economy.	The operational actor. Operates under rules set by its entity's governance document or principal's delegation chain.

Table 9.2: Principal, Entity, and Agent relationships

9.1.3 Lifecycle Stages



Stage	Trigger	Governance Actions	Escrow Impact
Creation	Principals agree to form entity.	Founding principals generate key pairs and register their public keys. Principals agree on the entity's objective (mission/optimization directive). Each principal obtains a Verification Attestation binding their public key to their verified identity. Governance document is created with the ownership registry listing all principal public keys and equity allocations. All founding principals sign the governance document with their private keys. Agent registry populated.	Escrow created in FUNDING when the entity's agents sell. Principals MAY contribute initial funds.
Operation	Entity is active.	Ongoing governance: voting, adding/removing agents, adjusting policies. PoP accumulates.	ACTIVE when threshold met. Transaction-based funding continues.
Modification	Principal submits amendment.	Voting per modification procedure. Document version incremented. Agent chains updated.	Parameters may change. Existing balances preserved.
Transfer	Equity sale crosses control threshold.	New owner(s) assume governance. Document updated. Delegation chains re-rooted.	90-day hold. Balance transfers after hold and dispute resolution.
Termination	Unanimous vote to dissolve.	All agents deactivated. Outstanding disputes resolved. Assets distributed.	Released after 90-day wait and full dispute resolution.

Table 9.3: Entity lifecycle stages

Dissolution requires unanimous consent specifically to prevent a majority owner from dissolving to escape obligations. Outstanding disputes **MUST** be resolved before termination. The 90-day escrow hold begins only after the last dispute is resolved. During the hold, new disputes **MAY** still be filed on pre-termination transactions.

10. Operational Scenarios

This section describes end-to-end operational scenarios, showing how AEA/P components work together across different agent types. Each flow references the relevant sections.

10.1 Agent Registration

In every case the principal creates and signs the AID (Section 5) and its delegation chain (Section 5), and the AID becomes ACTIVE once it references a valid Verification Attestation at the required tier (Section 5). Table 10.1 sets out what differs by agent type, and Figure 10.1 shows the registration sequence.

Agent	Principal and verification	authorized_actions	Liability escrow	Governance document
PERSONAL	Individual; Tier 1	purchase	None	None
BUSINESS that only buys	Registered business; Tier 2	purchase	None	Optional
BUSINESS that sells	Registered business; Tier 2	sell, optionally purchase; declares authorized_markets	MUST, in place before sell takes effect	Optional
BUSINESS with multiple principals	Each equity-holding principal; Tier 3	purchase, sell, or both	MUST while carrying sell	Required (Section 9)

Table 10.1: Registration requirements by agent type

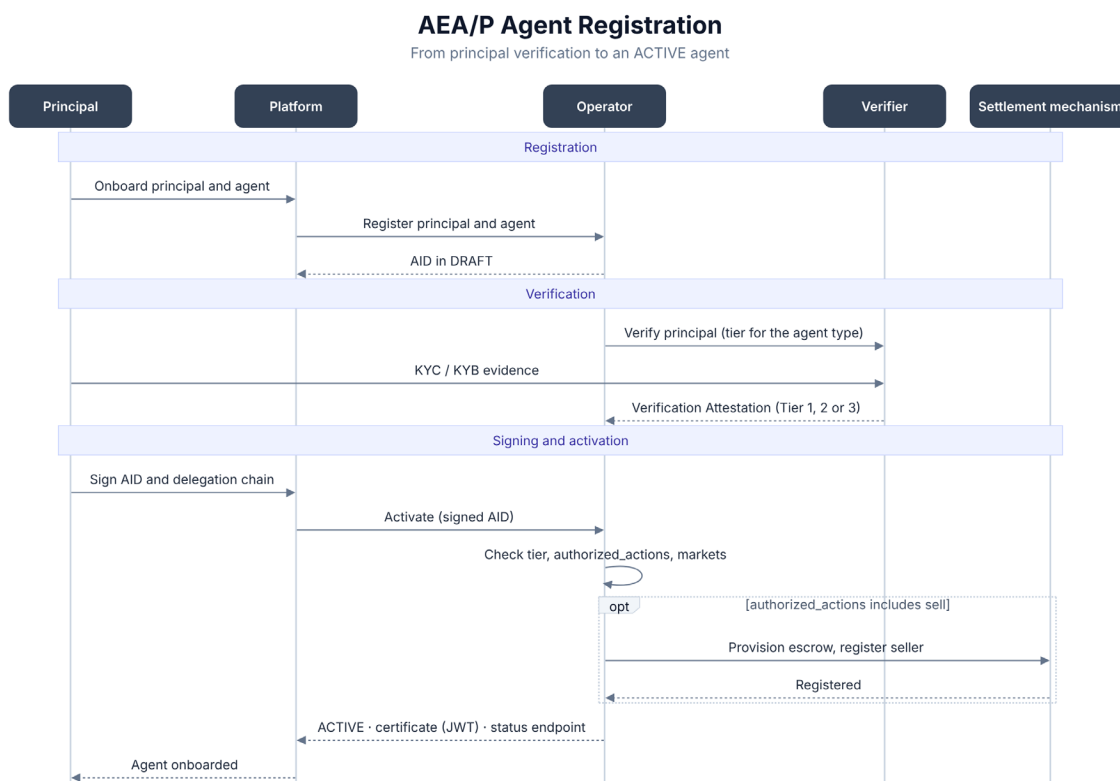


Figure 10.1: Agent registration sequence

10.2 Agent-to-Agent Transaction with PoP Tracking

A buyer agent (Agent A, a personal agent) purchases a service from a seller agent (Agent B, a business agent carrying sell). Both agents build reputation from the interaction. Figure 10.2 shows the message sequence; the steps below follow its five phases.

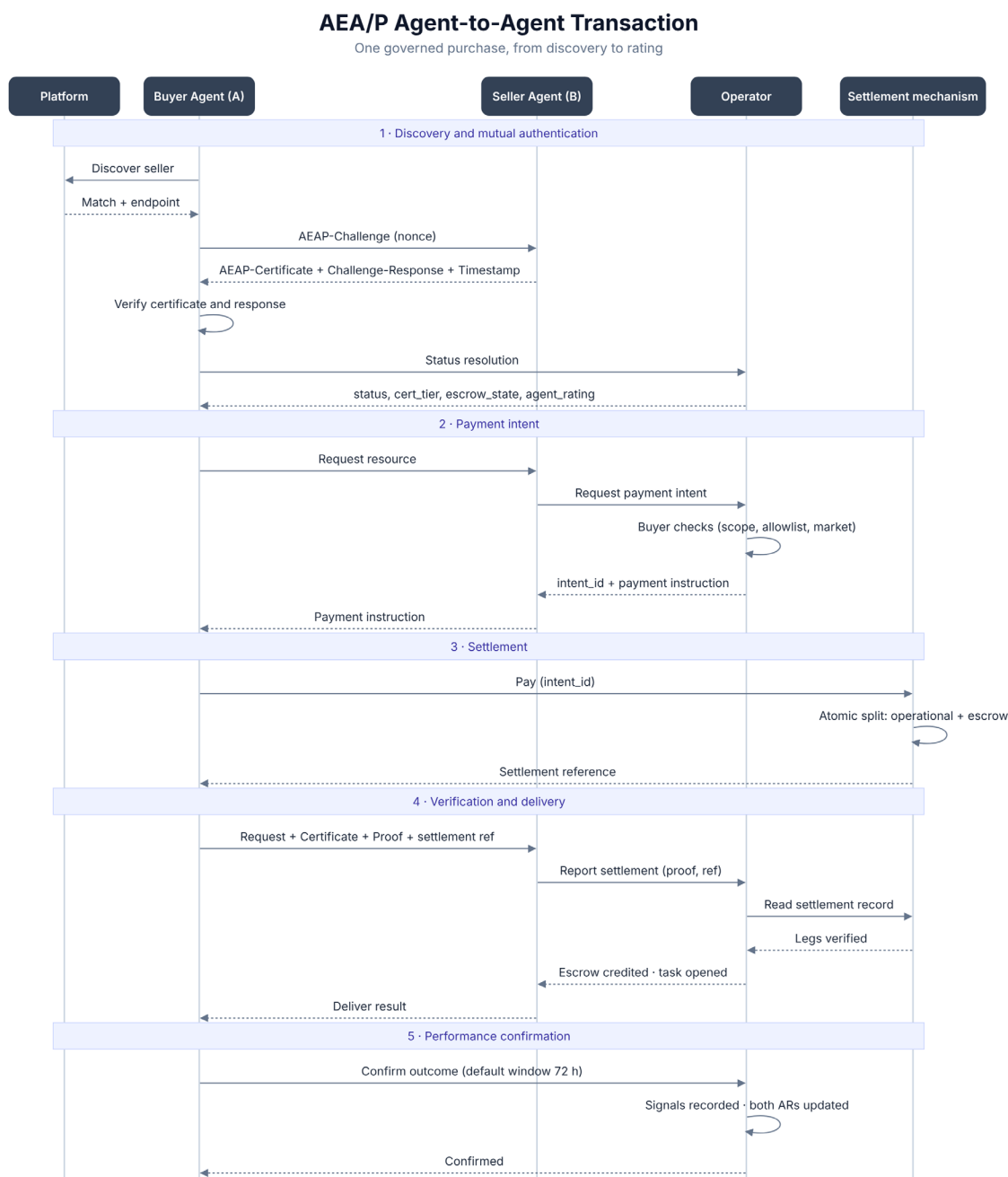


Figure 10.2: Agent-to-agent transaction sequence

- 1. Discovery and mutual authentication.** Agent A finds Agent B through a Platform and authenticates it by challenge–response (Section 5): Agent A issues a single-use nonce, and Agent B returns its certificate, its signature over the nonce and a timestamp. Agent A resolves Agent B’s live status (Section 5) and applies the universal and seller checks (Section 5): ACTIVE state, sell in authorized_actions, the transaction market, adequate AR, and escrow coverage relative to the transaction value.

2. **Payment intent.** Agent A requests the service and Agent B requests a payment intent from the Operator. The Operator refuses the intent if Agent A's spending authorization, counterparty allowlist or transaction market does not permit the purchase (Section 5); otherwise it returns an `intent_id` and a payment instruction, which Agent B passes to Agent A.
3. **Settlement.** Agent A pays against the `intent_id` through the settlement mechanism in use — an existing payment protocol or rail, or a native AEA/P-compliant implementation. The mechanism routes the payment atomically to Agent B's operational and escrow accounts at the configured `funding_rate` and produces a verifiable settlement record (Section 7); AEA/P does not hold or mediate the funds.
4. **Verification and delivery.** Agent A sends its request with its certificate, a bound proof and the settlement reference; Agent B verifies the proof (Section 5). Agent B reports the settlement to the Operator, which verifies the settlement record against the intent, credits the escrow share and opens the task; Agent B then delivers the result.
5. **Performance confirmation.** Agent A confirms the outcome within the confirmation window, or it auto-confirms when the window expires (Section 6). Agent B's performance record receives seller signals (availability, timeliness, task completion, dispute-free) and Agent A's receives buyer signals (task completion, payment timeliness, transaction completion, dispute fairness, budget compliance), and the AR of both agents is recalculated (Section 6).

10.3 Dispute Initiation and Resolution

Agent A, the buyer agent (PERSONAL), disputes a transaction with Agent B, the seller agent (BUSINESS), after a service was not delivered as specified. Figure 10.3 shows the sequence.

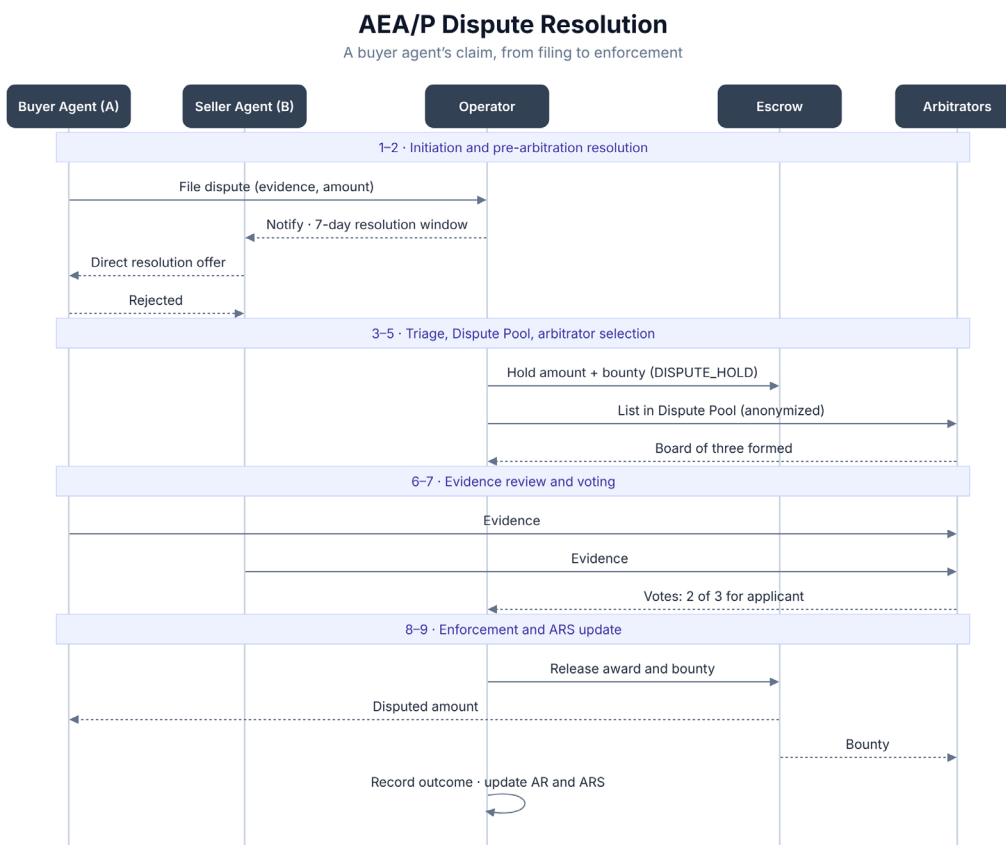


Figure 10.3: Dispute resolution sequence

1. **Initiation.** Agent A (or its principal, using the agent's transaction history as evidence) submits a dispute including transaction reference, evidence, disputed amount, and resolution sought (Section 8). The protocol supports both autonomous dispute detection by the agent and principal-initiated filing.
2. **Pre-arbitration resolution.** Agent B receives notification and has 7 days to resolve directly with Agent A. Agent B offers a partial refund. Agent A rejects the offer (Section 8).
3. **Triage.** System compares total financial exposure (disputed amount + bounty) to Agent B's escrow balance. Exposure is within balance; dispute enters the Dispute Pool at standard priority (Section 8).
4. **Dispute Pool.** Dispute appears in the pool with domain category, bounty amount, and complexity rating visible to arbitrators. Identities of parties are hidden (Section 8).
5. **Arbitrator selection.** Three arbitrators with matching domain expertise select the dispute from the pool. Eligibility is verified. Board is formed (Section 8).
6. **Evidence review.** Both parties submit evidence. Arbitrators review independently.
7. **Voting.** Arbitrators cast votes. 2 of 3 vote FOR applicant (strict majority). Resolution: in favor of Agent A (Section 8).
8. **Enforcement.** Disputed amount transferred from Agent B's escrow to Agent A. Bounty distributed to arbitrators. Negative outcome recorded in Agent B's performance record; AR decreases. Agent A's AR unaffected (successful dispute) (Section 8).
9. **ARS update.** Arbitrators who voted with the majority receive positive ARS adjustment. The one dissenting arbitrator receives a negative ARS adjustment (Section 8).

10.4 Type Upgrade: Personal to Business

A personal agent that has been purchasing API services on behalf of its individual principal begins offering its own analytics services to other agents once the principal registers as a sole proprietor, transitioning to BUSINESS.

1. Principal obtains a business license and completes Tier 2 verification (Section 5). Updates the AID in place: `agent_type` changes from PERSONAL to BUSINESS, `sell` is added to `authorized_actions`, `authorized_markets` is declared, and capability declarations are expanded to include service offerings. The agent keeps its `agent_id`, AR history and dispute record.
2. Principal creates a Liability Escrow Account (MUST before `sell` takes effect, Table 7.1). Pre-funds escrow to provide immediate coverage for service customers.
3. Principal optionally creates a Governance Document if additional agents will join the entity; one is required, with Tier 3 verification of each principal, if additional principals join (Section 9).
4. Agent's existing AR (from buyer signals) is preserved. As the agent completes seller transactions, the AR transitions to a blended score reflecting the evolving transaction mix by value.
5. Agent now operates as a business agent carrying purchase and sell: purchasing inputs, selling outputs (building escrow), with a single AR that reflects its complete economic activity.

10.5 Voluntary Refund

Agent B, a seller agent (BUSINESS, sell only), sold a data-enrichment job to Agent A, the buyer agent (PERSONAL), for 400 USDC. Before any dispute is filed, Agent B finds that a quarter of the records were enriched from a stale source and refunds part of the payment. Figure 10.4 shows the sequence.

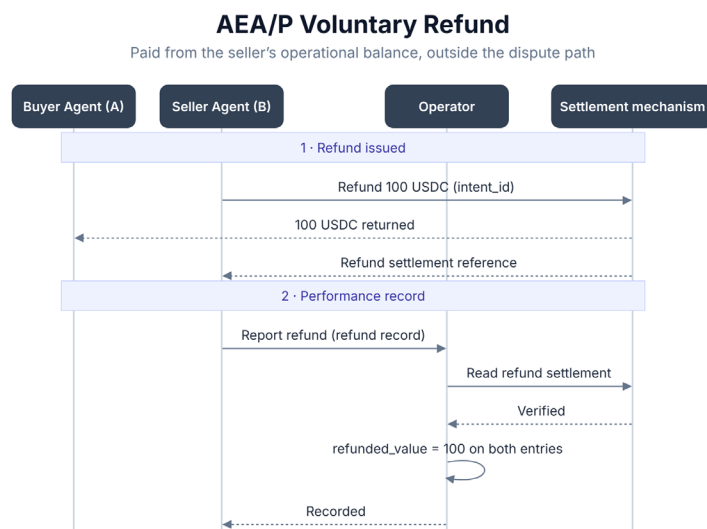


Figure 10.4: Voluntary refund sequence

1. **Refund issued.** Agent B refunds 100 USDC against the original `intent_id` from its operational balance (Section 7). It needs no purchase authorization, and Agent A receives the refund without any change of agent type.
2. **Performance record.** Both parties' entries for the interaction record `refunded_value` = 100 (Section 6). No new interaction is created, Agent B's dispute-free signal stays at 1.0, and its escrow threshold counts the sale at its net 300 USDC (Section 7).

3. **Later dispute.** If Agent A still files a dispute, it follows the dispute path (Section 8): the claim is limited to the 300 USDC not refunded (Section 8), and any award is paid from Agent B's escrow.

11. Security Considerations

AEA/P's governance layer introduces its own threat surface distinct from model-level and system-level security concerns. Implementations MUST consider the following threats. Some threats apply differently depending on the agent's type and authorized actions.

Threat	Description	Affected Agents	Mitigations
Rating manipulation	An adversary creates sham transactions between colluding agents to inflate PoP ratings artificially.	All agents	Sybil resistance: same-principal interactions excluded from PoP (weight: 0x, Section 6). Minimum interaction threshold (default: 10) before AR is published. Bilateral confirmation required. Anomaly detection in transaction patterns (implementation-level).
Identity spoofing	An adversary presents a forged or stolen AID to impersonate a high-rated agent.	All agents	Cryptographic binding of AIDs to public keys (Section 5). Delegation chain verification tracing authority to a verified principal (Section 5). AID revocation mechanisms (Section 5.1).
Escrow attacks	An adversary drains an agent's escrow through frivolous disputes, causing unjustified operational constraints.	Business agents that sell	Dispute filing requires verifiable transaction history with the respondent. Pre-arbitration resolution window allows respondent to resolve before bounty costs are incurred (Section 8). Negative PoP impact on applicants whose disputes are resolved against them.
Dispute flooding	An adversary overwhelms the arbitration system with high volumes of disputes to degrade system performance.	Business agents that sell	Rate limits on dispute submissions per applicant. Bounty costs scale with volume (respondent-pays model creates back-pressure). Priority queuing based on disputed amount and agent impact.
Arbitrator collusion	Arbitrators collude with one party to influence dispute outcomes.	All agents (as participants in disputes)	Random arbitrator selection. Anonymous arbitrator identity during proceedings. Arbitrator Reliability Score (ARS) tracks alignment with final outcomes; divergent votes reduce selection probability and may trigger stake penalties (Section 8). Escalation mechanism ensures no single board has final authority.
Delegation chain attacks	An adversary exploits delegation chains to escalate an agent's authority beyond what the principal intended.	All agents	Scope subset invariant across delegation chain links (Section 5) and per-dimension mutability over time on the same AID (Section 5). Sub-delegation restrictions. Real-time revocation propagation.
Governance manipulation	A majority principal modifies the governance document to disadvantage minority principals or drain entity assets.	Business agents under multi-principal governance	Supermajority (at least two-thirds) required for governance amendments (Section 9). Unanimous consent required for entity termination. All governance changes are versioned and publicly auditable. Blockchain-based implementations provide immutable governance history (Section 9).
Spending limit bypass	An agent circumvents its spending authorization to make unauthorized purchases.	Agents that buy	Spending limits enforced at the delegation chain level with cryptographic signatures (Section 5). Protocol-level enforcement prevents transactions exceeding authorized parameters. Real-time revocation enables immediate constraint if anomalies are detected.
Refund manipulation	A seller issues refunds to a colluding buyer to shrink its recorded sell value and escrow	Business agents that sell	Refunds go only to the original buyer of a settled interaction and are capped at its original value (Section 7), so the threshold falls only by value actually returned. Same-principal interactions carry no PoP

	threshold.		weight (Section 6).
--	------------	--	---------------------

Table 11.1: AEA/P threat model

11.1 Out-of-Scope Threats

The following threats are outside the scope of AEA/P and are addressed by other layers of the agent stack:

Threat	Addressed By	Relationship to AEA/P
Prompt injection / agent hijacking	Model-level security (instruction hierarchy, input filtering)	AEA/P assumes the agent is acting on behalf of its declared principal. If the agent is hijacked, AEA/P's delegation chain and escrow provide damage containment, but the hijacking itself is a model-level concern.
Unauthorized tool access	System-level security (sandboxing, least privilege, MCP access controls)	AEA/P governs what an agent is authorized to do economically. System-level controls govern what it can technically access.
Payment fraud / settlement failure	The payment rail or protocol in use (e.g., card networks, AP2, x402)	AEA/P is payment-rail agnostic: the security of the underlying rail is that rail's responsibility. AEA/P's settlement requirements (Section 7), escrow coverage and dispute resolution apply whichever rail is used.
Network attacks (DDoS, MITM)	Infrastructure security (TLS, authentication, CDN)	Standard infrastructure security applies to AEA/P implementations as it does to any networked system.

Table 11.2: Out-of-scope threats and their responsible layers

12. Future Work

The current specification establishes the architectural foundation and core protocol mechanics of AEA/P. The protocol is designed to evolve through community input, implementation experience, and alignment with emerging standards. Future versions will address the following areas:

- **Formal schemas and reference implementation.** JSON Schema definitions for all data structures and an open-source reference implementation.
- **Cross-protocol integration profiles.** How AEA/P maps onto MCP, A2A, AP2, x402 and ERC-8004 agent registries.
- **New commitment types.** Additional authorized actions (e.g., lending, subscription) and bounded price or term flexibility before commitment.
- **Value-stratified reliability.** Performance record queries by transaction value tier.
- **Certification and arbitration ecosystem.** AEA/P Certified criteria, arbitrator registration and stake management, and activity-specific regulatory attestations.
- **Formal verification and alignment.** Proofs of protocol invariants, entity governance templates, inter-entity governance, and alignment with international AI governance frameworks.

Community feedback on prioritization of these deliverables is welcomed. The specification repository and contribution guidelines are available at <https://aeap.dev>.

13. References

- [1] Duris, O. (2019). xDAC: Start Your Decentralized Company. White Paper v1.0.10.
- [2] Anthropic (2024). Model Context Protocol (MCP) Specification.
- [3] Google (2025). Agent-to-Agent (A2A) Protocol Specification.
- [4] Google (2025). Agent Payments Protocol (AP2) Specification.
- [5] Coinbase (2025). x402 Protocol Specification.
- [6] Shopify (2025). Universal Commerce Protocol (UCP) Specification.
- [7] Machine Payment Protocol (MPP) Specification.
- [8] Stripe / OpenAI (2025). Agentic Commerce Protocol (ACP).
- [9] Bradner, S. (1997). “Key words for use in RFCs to Indicate Requirement Levels.” RFC 2119.
- [10] Jones, M. (2015). “JSON Web Key (JWK).” RFC 7517.
- [11] Jones, M., Bradley, J., and Sakimura, N. (2015). “JSON Web Token (JWT).” RFC 7519.
- [12] W3C (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation.
- [13] ERC-8004: Agent Registry (2026). Ethereum Standards Track. On-chain registries for agent identity, reputation, and validation.
- [14] Financial Action Task Force (FATF). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* <https://www.fatf-gafi.org/>.

14. Revision History

Version history of this whitepaper, reverse chronological. Detailed change notes are published at <https://aeap.dev>.

Version	Date	Changes
v0.3.1	October 2026	Regenerated from Protocol Specification v0.3.1. Terminology only, no change to protocol behavior: agent_type (PERSONAL or BUSINESS) replaces economic_role and says whom an agent acts for; the per-interaction side field (SELLER or BUYER) replaces role_in_interaction; certificate claims aeap.agent_type and aeap.verification_tier replace aeap.economic_role and aeap.principal_type; flows and diagrams name the parties buyer agent and seller agent; the PERSONAL to BUSINESS change is an upgrade (§4.3, §10.4).
v0.3	October 2026	Renamed from Protocol Framework to Whitepaper. Regenerated from Protocol Specification v0.3: two economic roles, CONSUMER and BUSINESS, with authorized_actions deciding what a BUSINESS agent does; value-weighted AR; escrow on sell volume only; refunds; condensed structure, with registration requirements in Table 10.1, sequence diagrams for the operational scenarios (Figures 10.1–10.4) and a refund scenario in §10.5.
v0.2.8	August 2026	Regenerated from Protocol Specification v0.2.8, with numbering aligned to the Specification; AR prior initialization in §6.1.
v0.2.3	June 2026	Trust Registry reframed as a published artifact.
v0.2.2	June 2026	Infrastructure roles: Operator, Platform and Trust Registry.
v0.2.0	May 2026	Scope and Delegation Chain terms updated to the chain-invariant model; running header corrected.
v0.1.5	May 2026	Scope term; authorized_actions reduced to purchase, sell and delegate.
v0.1.4	May 2026	Field-level sections 5.2 and 5.3 moved to the Specification; revision history moved to §14.
v0.1.3	May 2026	Authorized Actions section added (since moved to the Specification).
v0.1.2	May 2026	Principal Verification by Role section added (since moved to the Specification).
v0.1.1	April 2026	Initial release.

End of AEA/P Whitepaper v0.3.1 | <https://aeap.dev>