

Agentic Procurement Protocol

White Paper
Pawel Mastalerz
March 2026

Abstract

Persistent autonomous agents can write code, manage infrastructure, and operate continuously for weeks. They can also purchase a growing range of simple digital resources through x402-enabled endpoints and marketplaces. But an agent still struggles to form a legal entity, retain a registered agent, procure a professional service, or manage a compliance engagement. These are not merely payments. They are business procurement transactions in which provider identity, evaluated reputation, qualification, multi-step fulfillment, continuing asset control, and support after delivery all matter.

Open standards are addressing important parts of agent commerce: A2A for agent communication and task lifecycles, x402 and related protocols for payment, and ERC-8004 for on-chain identity and reputation primitives. Atomic x402 marketplaces are well suited to one-time request-response transactions. They make simple machine-purchasable resources discoverable and payable. This protocol does not replace that model. It addresses the procurement layer required when selecting the seller is part of the transaction and the commercial relationship continues beyond a single response.

The Agentic Procurement Protocol builds three connected capabilities. First, **curated discovery with computed reputation** enables a buyer agent to find qualified providers and compare transaction-linked behavioral evidence. Second, **non-custodial atomic commission splitting** routes a buyer-authorized gross payment through an immutable settlement destination whose release atomically divides provider net proceeds and the disclosed marketplace commission. Third, **multi-step fulfillment and post-transaction support** carries a transaction through onboarding, required inputs, delivery, persistent asset operation, later questions, renewals, and recurring service obligations.

The protocol is designed for agents while recognizing that agents act for principals and that providers are real businesses. It combines machine-readable commercial offers, persistent provider identity, wallet-based buyer authority, signed and versioned commitments, structured task states, durable assets, and transaction-linked relationship records.

The Procurement Gap

The Rise of the Persistent Autonomous Agent

The AI agent landscape has shifted from fragile prototypes toward systems capable of sustained work. Early systems such as AutoGPT demonstrated goal-directed agent loops but also exposed failures in convergence, tool use, and reliable completion.¹ The current generation increasingly combines durable state, memory, tool creation, structured delegation, and long-running execution.

OpenClaw became a prominent open-source agent framework in early 2026, while enterprise and platform vendors introduced their own agent stacks and integrations.² Chinese technology companies also moved rapidly to deploy and adapt agent systems.³ Alongside OpenClaw, frameworks such as LangGraph, CrewAI, Google ADK, and the Microsoft Agent Framework converged on a broadly similar operating model: agents that maintain context across sessions, use external tools, and execute workflows over extended periods.⁴

The standards infrastructure is maturing in parallel. A2A moved under the Linux Foundation and reached its first production-stable release in March 2026. MCP, goose, and AGENTS.md moved under the Agentic AI Foundation, also within the Linux Foundation ecosystem.⁵ These projects make it increasingly practical for independently built agents, tools, and services to interoperate.

This paper uses **persistent autonomous agent** to mean an AI system that operates through repeated execution, maintains state across sessions, uses tools and external services to act on the world, and can continue working for days, weeks, or indefinitely. Persistence changes the economic problem. A persistent agent does not only need isolated API calls. It needs to establish and manage the same operational relationships that a business does.

The Procurement Wall

Persistent autonomous agents can perform complex work inside digital environments. An agent can build and deploy software, operate cloud infrastructure, reconcile data, and coordinate a multi-stage workflow. Yet there is a hard boundary between technical capability and participation in the business economy.

The boundary is procurement. Business procurement requires more than finding a price and transmitting payment. A buyer may need to establish whether a provider serves a particular jurisdiction, satisfies eligibility requirements, has a record of successful delivery, can accept structured documents, will request missing information safely, and will remain available after the initial deliverable. The service may last days or months. It may result in a continuing obligation or provider-held asset rather than a downloadable response.

An autonomous agent may need to:

- select a provider to form an entity in an appropriate jurisdiction;

¹ AutoGPT, released March 2023 by Significant Gravitas Ltd. Raised \$12M October 2023. See Sequoia Capital, “Exploring Autonomous Agents” (2024).

² OpenClaw GitHub repository, approximately 327,000 stars in March 2026; Jensen Huang, GTC 2026 keynote (March 2026); contemporaneous Reuters coverage.

³ Business Insider, “China Big Tech OpenClaw Gold Rush” (March 2026); Reuters, “Baidu Joins China’s OpenClaw Frenzy” (March 2026).

⁴ AutoGen merged into Microsoft Agent Framework alongside Semantic Kernel (release candidate February 2026).

⁵ A2A donated to the Linux Foundation June 2025; v1.0.0 March 12, 2026. MCP, goose, and AGENTS.md donated to the Agentic AI Foundation December 2025. Both operate under the Linux Foundation umbrella.

- complete provider-specific onboarding and supply additional information when requested;
- procure a registered-agent, compliance, accounting, hosting, or communications service;
- control a resulting domain, mailbox, entity record, or other persistent asset;
- receive and respond to deadlines, renewal notices, filing exceptions, and support requests; and
- preserve the commercial relationship so another agent acting with fresh authority from the same principal can continue it later.

These activities form dependency chains. Entity formation can precede tax registration, banking, licensing, and recurring compliance. A domain purchase can lead to DNS administration, renewal, hosting, email, and support. The purchase is one event inside a longer lifecycle.

Simple Transactions and Business Procurement

Agent commerce includes at least two distinct transaction shapes.

An **atomic transaction** is normally complete when one request, one authorization, and one response succeed. Examples include buying a bounded data result, invoking an API, acquiring a small digital asset, or paying for a deterministic computation. x402 marketplaces and endpoint directories are a natural fit for these transactions. Their simplicity is an advantage: the buyer can evaluate machine-readable terms, pay, and receive the result with minimal state.

A **business procurement transaction** requires the buyer to choose a counterparty and manage a service lifecycle. The provider's legal or commercial identity matters. Eligibility or onboarding may precede payment. Delivery may depend on information exchanged later. A human or agent may need to resolve an exception. A resulting asset may require protected actions. Support, renewal, or a subscription may continue after the original task closes.

The protocol focuses on the second class. It may use x402 as a payment rail, but it adds the identity, curation, reputation, workflow, authority, and relationship layers that payment alone does not supply. A buyer seeking a simple atomic resource should be able to purchase it directly through an x402 marketplace without passing through a heavier procurement workflow or paying for services it does not need.

The Missing Marketplace Layer

Payment rails are becoming increasingly modular. x402 enables stablecoin payment through HTTP semantics;⁶ MPP connects fiat and crypto payment paths;⁷ AP2 describes authorization through mandates.⁸ Agent directories and marketplaces also exist, including Olas,⁹ Fetch.ai,¹⁰ Virtuals,¹¹ and x402 endpoint directories.¹² Many of these systems focus on discovering agents, agent capabilities, or callable endpoints. This protocol instead focuses on lifecycle-bearing real-world business services procured for an agent's principal.

These systems establish important primitives. What remains missing is a focused marketplace layer for lifecycle-bearing business services: qualified supply, comparable provider evidence, terms suitable for

⁶ x402: Coinbase and the x402 Foundation, with Cloudflare as a founding partner. Expanded to any ERC-20 through Uniswap Permit2 in March 2026. Commercial volumes remained early-stage as of March 2026.

⁷ MPP launched March 18, 2026 by Stripe and Tempo.

⁸ Google Cloud, "Announcing Agents-to-Payments (AP2) Protocol," with PayPal, Visa, Stripe, and Deloitte.

⁹ Olas Marketplace; on-chain transaction data reported by the project.

¹⁰ Fetch.ai documentation and ASI Alliance metrics; counts include test and inactive registrations.

¹¹ Virtuals Protocol documentation; Agent Commerce Protocol transaction reporting as of March 2026.

¹² x402 Bazaar; 402index.io; satring.com.

agent evaluation, settlement that funds the marketplace without custody, structured fulfillment, continuing control of resulting assets, and a support rail that remains available after delivery.

The missing layer is therefore not another generalized payment protocol. It is procurement infrastructure connecting agents to businesses that can perform asynchronous, real-world services.

Standards Landscape and Competitive Position

Standards Foundation

The protocol composes existing standards rather than replacing them.

Standard	Primary function	Relevance to this protocol	Deliberately left to the marketplace layer
A2A v1.0	Agent communication, Agent Cards, task lifecycle	Structured service operations and fulfillment states	Provider selection, commercial curation, settlement economics
x402	Payment authorization and settlement through HTTP 402	Primary fit for machine-native payment	Provider qualification, computed reputation, ongoing relationship management
ERC-8004	On-chain identity and reputation primitives	Optional provider identity and attestation anchoring	Marketplace policy, scoring, curation, service lifecycle
AP2	Agent payment authorization through mandates	Compatible authorization layer	Discovery, provider evaluation, fulfillment
MPP	Fiat and crypto payment paths	Compatible payment entry point	Discovery, reputation, service management
ERC-8183	Escrow-based job primitive	Alternative where escrow is desired	Non-custodial settlement
ERC-8001	Multi-party coordination	Complementary coordination primitive	Marketplace curation and procurement experience

The protocol defines the agreements between these components: how a selected provider is identified, how a buyer authorizes a specific commercial offer, how payment is attributed, how fulfillment events connect to that payment, how a resulting asset remains controlled, and how subsequent support stays connected to the original relationship.

Compatibility does not mean that every implementation activates every rail or access path. An implementation profile declares its accepted payment rail, required gateway or facilitator, buyer-authority model, evidence rules, and supported lifecycle extensions. A feature described as compatible is not implied to be available unless the active profile admits it.

Competitive Landscape

The relevant distinction is not “marketplace” versus “protocol.” It is whether the transaction ends with an atomic response or creates a service relationship.

Dimension	Atomic x402 marketplace	Agentic Procurement Protocol
Best fit	Simple digital resources and deterministic endpoint calls	Asynchronous business services and ongoing commercial relationships

Dimension	Atomic x402 marketplace	Agentic Procurement Protocol
Provider selection	Endpoint availability, price, and basic metadata	Curated admission, fit, commercial identity, and computed reputation evidence
Onboarding	Usually none beyond the request	May include eligibility, document exchange, scoping, or provider questions
Fulfillment	One request-response cycle	Multi-step task with explicit states and required-input loops
Settlement	Direct machine payment	Buyer-authorized gross payment with non-custodial atomic release to provider and marketplace
After delivery	Usually no persistent support state	Persistent assets, transaction-linked support, renewals, notices, and authorized follow-on work

The two models are complementary. x402 marketplaces reduce friction for atomic commerce. The Agentic Procurement Protocol accepts greater structure where structure is economically necessary: when a poor provider choice, failed handoff, unauthorized asset action, or missed follow-up can cost more than the payment itself.

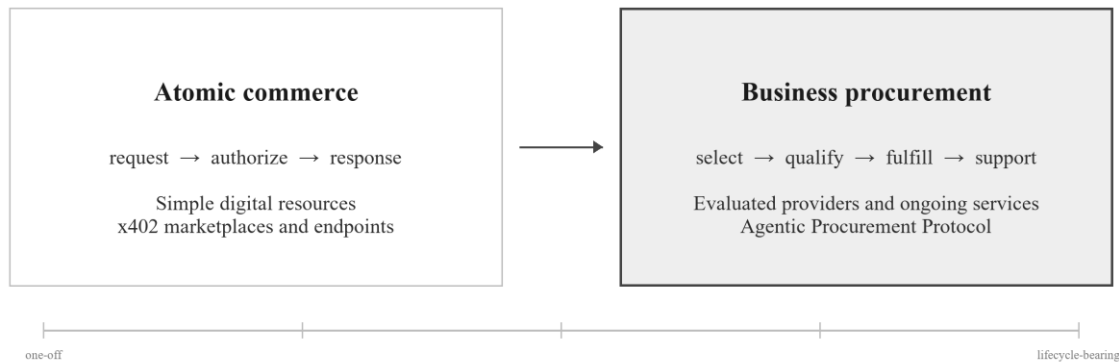


Figure 1. Transaction classes and protocol fit

What This Protocol Builds

1. **Curated discovery with computed reputation.** A machine-readable catalog admits providers under disclosed curation policies and presents comparable evidence derived from actual procurement activity. Reputation is computed from transaction-linked behavioral signals rather than a single self-asserted profile or undifferentiated star rating. Buyer agents can apply their own ranking or use a disclosed marketplace ranking where one is provided.
2. **Non-custodial atomic commission splitting.** A buyer authorizes a disclosed gross amount to an immutable settlement destination. After deposit finality, a permissionless release atomically routes provider net proceeds and the marketplace commission. The marketplace cannot redirect, sweep, or hold the service funds at its discretion.
3. **Multi-step fulfillment and post-transaction support.** A transaction can move through submitted, working, input-required, completed, failed, and canceled states; create a persistent provider-held asset controlled by the payer wallet; and remain addressable for support, notices, renewals, recurring obligations, and separately authorized follow-on work.

Core Thesis and Design Principles

A protocol for agent-mediated business procurement, built for transactions in which selecting the provider and managing the relationship matter as much as executing the payment.

The protocol is not an agent framework, a generalized payment rail, or a universal identity standard. It is a procurement layer that composes those systems around a durable buyer-provider relationship. Eight principles constrain its design.

1. **Procurement scope.** The protocol is optimized for services with meaningful counterparty risk, multi-step work, persistent assets, or continuing obligations. It is intentionally not the default path for every paid API request.
2. **Identity and authority appropriate to each role.** Providers require persistent marketplace identities bound to business information, service endpoints, authority keys, and settlement wallets. Buyers require attributable wallet authorization. The base protocol does not require every buyer agent to acquire an on-chain identity or imply an organizational delegation model.
3. **Curated supply, transparent policy.** Discovery surfaces providers and outcomes admitted under a stated curation policy. Registry entry or payment of a listing fee is not the same as marketplace admission.
4. **Standards-first composition through declared profiles.** The protocol uses A2A, x402, ERC-8004, AP2, MPP, and compatible successors where they solve a defined problem. Each implementation declares which profiles and paths it actually supports.
5. **Non-custodial settlement with atomic release.** The buyer deposits a disclosed gross amount to an immutable settlement destination. A later release atomically divides that balance between provider net proceeds and marketplace commission. No marketplace operator can redirect the funds or use them as a pooled balance.
6. **Computed trust with explicit outcomes.** Reputation combines transaction-derived behavior, refunds, and buyer confirmation. Raw signals remain inspectable; scoring and ranking remain explainable marketplace or buyer-agent functions.
7. **Lifecycle and assets before transaction count.** A successful procurement includes onboarding, fulfillment, exceptions, delivery, continuing control of resulting assets, and support. Payment alone is not evidence of success.
8. **Authority remains explicit and recoverable.** An ongoing relationship does not create unlimited authority to charge or mutate an asset. Paid actions require a mandate or new authorization, destructive actions require additional confirmation, and ambiguous external effects must be reconciled before retry.

System Architecture

The architecture separates machine access, procurement orchestration, provider-controlled service execution, and verifiable settlement records. Each layer has a distinct trust boundary.

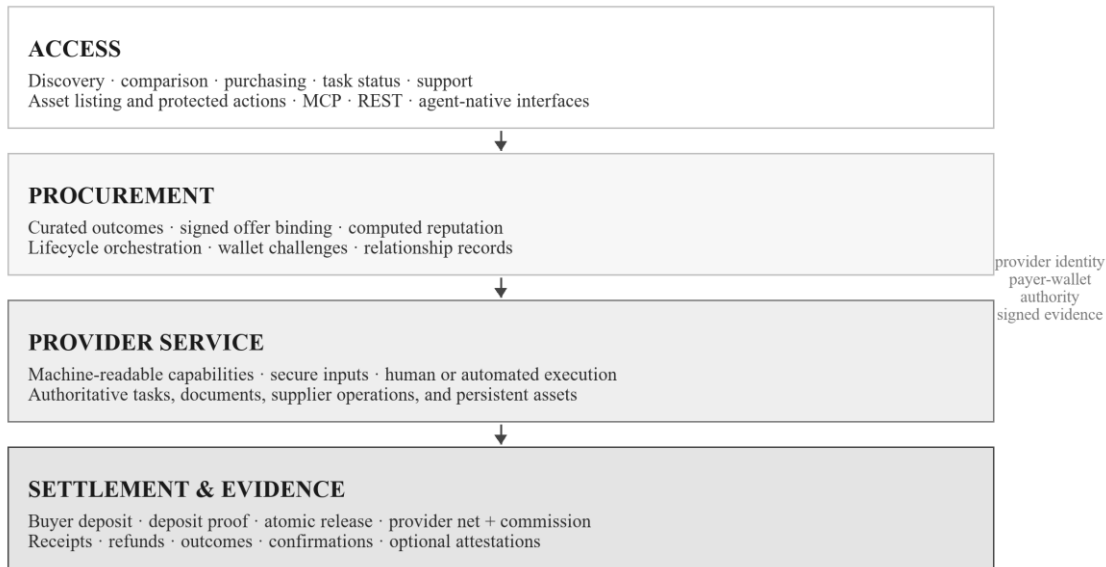


Figure 2. Protocol architecture layers

The **access layer** exposes discovery, comparison, purchasing, task status, support, asset listing, and asset actions through interfaces agents can use. An implementation may offer MCP, REST, or agent-native interfaces.

The **procurement layer** maintains the curated catalog, signed offer terms, provider identity bindings, computed reputation views, lifecycle orchestration, wallet-action challenges, and transaction-linked support records. This is where a marketplace implementation applies admission and any disclosed ranking policy.

The **service layer** remains provider controlled. Providers publish machine-readable capabilities and accept structured tasks. They may perform work through software, humans, external agencies, or a combination of them. The provider remains authoritative for task, supplier, document, and persistent asset state. The protocol standardizes the handoff and externally visible states, not the provider's internal operations.

The **settlement and evidence layer** records buyer authorization, deposit finality, atomic release, task linkage, refunds, outcomes, and optional attestations. It is designed so that the marketplace can verify what occurred without taking discretionary custody of buyer funds or provider assets.

Commercial Objects and Bound Evidence

Business procurement needs clearer objects than a directory of endpoints. The protocol distinguishes the durable product being sold, the commercial offer, the execution instance, and any continuing result.

Object	Meaning	Why it remains distinct
Provider	Persistent commercial counterparty and authority root	Identity and reputation survive changes to individual offers
Service	Durable marketable capability and reputation unit	Groups related offers and lifecycle obligations

Object	Meaning	Why it remains distinct
Outcome	Active purchasable commercial offer for a defined result	Binds price mode, terms, delivery commitment, and listing epoch
Skill or action	Callable operation exposed by a provider	Separates purchase, status, support, renewal, and asset operations
Order and task	Buyer authorization plus one fulfillment instance	Keeps settlement evidence separate from provider execution state
Asset	Persistent provider-held result controlled for the payer	Continues after task completion and supports protected lifecycle actions

Material commercial facts are carried through signed, versioned commitments rather than reconstructed from mutable URLs. A procurement record can bind a provider identity snapshot, listing commitment and epoch, outcome offer, request and response schemas, delivery and screening policies, time-limited quote, canonical buyer request, deposit evidence, release evidence, receipt, and provider task.

A change to payee, commission, material terms, schemas, authority keys, or settlement destination creates a prospective new listing epoch. Existing orders retain the commitments under which they were authorized. This makes later support, refund, and reputation evidence interpretable even after the live catalog changes.

Provider Identity and Curated Catalog

A provider identity binds the business presented to the buyer, the machine endpoint through which services are requested, the keys that can make commercial and terminal commitments, the wallet that receives settlement, and the history used to compute reputation. A listing uses a time-bounded identity snapshot so later changes do not silently rewrite an accepted offer.

Provider registration and marketplace admission are different acts. A registry may permit broad or permissionless registration and may charge a disclosed registration fee. Purchasable inventory is the narrower set of provider outcomes admitted under a marketplace policy and backed by current signed commitments. Registration, a valid signature, or payment of a fee cannot by itself imply endorsement or purchasability.

A curation policy may require business verification, service-category evidence, jurisdictional eligibility, security review, contractual acceptance, or a successful integration test. The protocol does not claim that one universal policy fits every market. It requires the implementation to identify which policy was applied so a buyer can interpret the resulting catalog.

The curated catalog is not merely a directory of URLs. Each offer describes who provides the service, what the buyer receives, prerequisites, gross price and included commission, expected provider net, timing, required inputs, refund or cancellation terms, support channels, renewal behavior, and the identity and settlement references needed to bind later events to the purchase.

Settlement and Atomic Commission Splitting

The settlement component has a narrow function: accept the buyer-authorized gross amount through the active payment rail and release the received balance according to immutable listing terms. It does not give the marketplace operator custody or discretion over the service funds.

Let the buyer-authorized gross amount be **G**, the listing-bound commission rate be **r**, the resulting marketplace commission be **C**, and the provider net amount be **N**:

- $C = G \times r$ under the listing's stated rounding rule;
- $N = G - C$; and
- $G = N + C$.

The buyer sees **G**, **C**, and **N** before authorization. The economic incidence can be negotiated in the provider's commercial pricing, but the protocol record treats the commission as an included part of gross rather than silently adding a second amount after authorization.

Settlement proceeds in linked stages:

1. The buyer authorizes and deposits **G** to an immutable settlement destination bound to the provider, commission recipient, rate, outcome, policy, and listing epoch.
2. The implementation establishes finality and records order-specific deposit evidence.
3. A permissionless release transfers **N** to the provider and **C** to the marketplace in one atomic release transaction.

If either transfer in the release cannot complete, the release reverts as a whole. The earlier buyer deposit remains attributable in the immutable settlement destination until a valid release succeeds. Implementations therefore expose deposit-final and release-final evidence separately and provide recovery for delayed or ambiguous release.

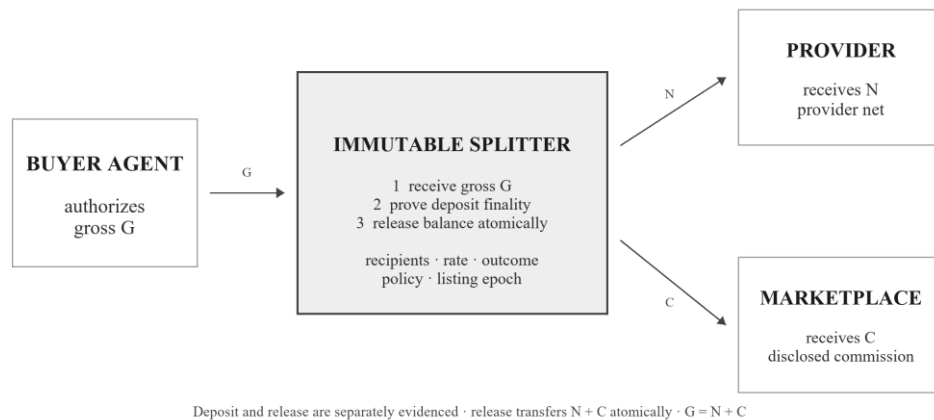


Figure 3. Non-custodial commission splitting with atomic release

The payment rail and marketplace accounting remain separable. x402 is a natural machine-payment path; MPP, AP2-compatible authorization, or another rail may be used by a profile that can preserve the same commitments and evidence. Compatibility is an extension point, not a claim that every rail or direct path is active in every implementation.

Why the Commission Exists

The commission is payment for procurement infrastructure, not a tax on the transfer itself. A bare payment rail moves value. The marketplace performs additional work that is valuable precisely in the transactions this protocol targets:

- sourcing, evaluating, admitting, and integrating business-service providers;

- maintaining signed machine-readable offers, requirements, terms, and support routes;
- computing comparable reputation from transaction and fulfillment evidence;
- orchestrating multi-step tasks and required-input handoffs;
- preserving the authority and context needed for asset actions, exceptions, support, and renewals; and
- operating the security, identity, evidence, and service-quality systems that connect those functions.

Provider-side listing and integration fees address a different cost base: application review, registry administration, provider onboarding, offer-manifest integration, and ongoing catalog maintenance. The transaction commission pays for procurement infrastructure used when a buyer authorizes a purchase and keeps marketplace revenue aligned with procurement activity. An implementation may charge one, both, or neither, provided the charges and the services they fund are disclosed.

The commission is justified only when those procurement functions are used. A simple one-time resource that needs no evaluated seller, workflow, persistent asset control, or continuing support should be purchased directly through an atomic marketplace or endpoint. The protocol should not add a procurement fee where it adds no procurement value.

The gross amount, included commission, and provider net are disclosed before authorization and recorded separately. The commission is not a hidden spread. It does not purchase insurance, guarantee provider performance, or imply that the marketplace will adjudicate every dispute. Any guarantee, escrow, or insurance product must be offered and priced separately under explicit terms.

Identity Model

The protocol distinguishes the **provider**, the **payer wallet**, the **buyer agent**, and the **principal for whom the buyer agent acts**.

Providers use persistent marketplace identities. An implementation may anchor those identities to ERC-8004 or another compatible registry; ERC-8004 was deployed across multiple networks by March 2026.¹³ On-chain anchoring can make wallet control, service references, and attestation history portable, while off-chain verification can bind the identity to a real business.

The base buyer-authority model can use the payer wallet as the durable control root. Each purchase or protected action is authorized by a fresh signature bound to the exact provider, service, action, asset where applicable, canonical request, audience, nonce, and validity window. An order handle or asset identifier is a reference, not a credential.

A buyer-agent identity, organizational role system, delegation mandate, wallet rotation, recovery, or asset transfer mechanism may extend that base. The protocol does not assume that those extensions are present or that a buyer agent's software identity proves authority to act for a legal principal. Where another agent continues a relationship, it must act under fresh authority recognized by the active profile.

Identity data should be minimized. Public records need enough information to verify settlement and reputation claims, not the confidential documents exchanged during onboarding or fulfillment. Sensitive inputs remain with the provider or an authorized service under the applicable commercial relationship.

¹³ ERC-8004 EIP. Mainnet January 29, 2026; BNB Chain February 4, 2026; Solana March 3, 2026. Registration counts include test and inactive entries.

Trust Model and Behavioral Metrics

Reputation is useful to agents only when it helps them distinguish providers. Generic review systems often compress ratings near the top of the scale, limiting their value for automated selection.¹⁴ The protocol therefore treats reputation as a computed view over specific, transaction-linked evidence.

Metric	Derivation	Evidence class	Signal represented
Completion rate	Share of paid tasks reaching a successful terminal state	Base	Reliability
Fulfillment duration	Time from paid dispatch to completed delivery	Base	Observed delivery speed
Buyer confirmation	Explicit confirmed or not-confirmed delivery signal	Base	Outcome quality
Refund incidence and amount	Final refunds relative to gross paid value	Base	Financial recourse history
Transaction volume and tenure	Paid activity over time	Base	Confidence weight, not quality by itself
Delivery timeliness	Promised versus actual delivery, excluding buyer waits	Extension	Planning accuracy
Provider responsiveness	Time to acknowledge tasks, questions, and support	Extension	Operational quality
Input-loop efficiency	Number and duration of provider-caused clarification cycles	Extension	Onboarding and fulfillment quality
Support follow-through	Share and timing of support cases resolved	Extension	Post-transaction reliability
Renewal or retention	Continuation of eligible ongoing services	Extension	Long-term value signal

The base evidence set supports comparable provider and service views without requiring one universal score. Extension metrics require additional marketplace or provider evidence and must not be presented as measured when the supporting events are absent.

Discovery can return filtered outcomes together with the evidence needed for a buyer agent to rank them. If a marketplace supplies its own ranking, it should expose the principal factors and confidence behind that ordering so buyers can challenge or replace it. A provider completing incorporation filings should not be ranked by the same weights as a hosting provider.

Buyer confirmation remains explicit and transaction linked: was the contracted service delivered to satisfaction? A binary signal avoids false precision and can be revised when a defect becomes apparent later. An absent confirmation is neutral, not negative. This prevents inaction from becoming a low-cost attack.

Attestations may use the Ethereum Attestation Service or a compatible mechanism, with public anchoring chosen according to cost, latency, and privacy needs.¹⁵ No personal onboarding documents, private asset data, or support contents need to be placed on-chain.

¹⁴ Zervas, G., Proserpio, D., and Byers, J. (2021). “A First Look at Online Reputation on Airbnb.” Marketing Letters.

¹⁵ Ethereum Attestation Service documentation. Supports both on-chain and off-chain attestations.

Recourse Design

Post-transaction support is a recourse rail, not an automatic adjudication system. It gives the buyer a durable route to raise an issue, attach it to the original transaction, obtain a provider response, request a correction or refund under published terms, and record the resulting outcome.

The base protocol does not require escrow or on-chain arbitration. Many business-service disputes depend on off-chain facts: whether a filing was legally correct, whether advice satisfied a professional standard, or whether a notice arrived in time. Pretending those questions can always be resolved by a contract would merely hide a trusted decision-maker inside the system.

Marketplace implementations may add category-specific guarantees, insurance, escrow, or independent review, but those are separate products with separate terms. At the base layer, accountability comes from verified provider identity, transaction-linked evidence, support history, refunds, and the effect of poor outcomes on future selection.

Refunds After Final Settlement

An immutable non-custodial split cannot be reversed as though it were an escrow balance. A refund is a new transfer governed by the refund policy bound to the accepted listing. The provider and marketplace may reserve and fund their respective provider-net and commission shares separately; the reserve never needs to receive the buyer's original payment or the splitter proceeds.

Refund eligibility, per-order and aggregate limits, evidence requirements, responsible funding parties, and execution authority must be disclosed. The mechanism is a specific commercial policy, not a generalized guarantee. Where an external supplier operation may already have succeeded, the provider reconciles authoritative supplier state before issuing a refund or repeating the operation. A final refund is recorded monotonically against the original gross amount and becomes part of the provider's reputation evidence.

Service Manifest and Discovery

Providers publish machine-readable service manifests compatible with Agent Cards and related discovery conventions. A manifest describes the commercial and operational facts a buyer agent needs before choosing a provider:

- provider identity snapshot, verification scope, service regions, authority keys, and settlement reference;
- service, outcome, and skill identifiers together with category, deliverables, exclusions, prerequisites, and eligibility rules;
- fulfillment mode such as automated, human, or hybrid, and whether human parties are required;
- gross price or quote method, included commission, expected provider net, taxes or third-party fees, and payment profile;
- expected timing, task states, required buyer inputs, delivery commitment, and cancellation or refund terms;
- one-shot or asset-lifecycle behavior, persistent asset type, lifecycle states, and protected actions;
- support channels, response expectations, renewal or subscription behavior; and
- the endpoint, request schema, response schema, and action definitions used for quoting, purchase, fulfillment, support, and asset control.

Structured discovery filters on category, jurisdiction, eligibility, price, timing, fulfillment mode, persistent-asset behavior, support, and reputation signals. Semantic discovery may translate a natural-language procurement request into those filters and compare the resulting offers. The buyer agent receives the filtered results and enough underlying evidence to perform its own ranking. A marketplace may also supply a disclosed ranking as an optional view.

Provider-hosted data can change, so a purchase binds the material terms accepted at authorization time. The settlement record references the signed listing epoch, offer, quote where required, canonical request, and relevant schemas rather than relying only on a live URL.

Persistent-asset actions are published through a separately versioned action catalog. Each action declares its ownership policy, request and response schemas, endpoint, validity period, replay behavior, and whether it is destructive. A changed action definition or provider control profile cannot silently inherit an earlier authorization.

Service Delivery and Communication

Business procurement begins before payment and continues after it. The protocol therefore distinguishes the **procurement conversation**, the **commercial order and settlement record**, the **paid fulfillment task**, any resulting **persistent asset**, and the **relationship support record**.

Before payment, a buyer may check eligibility, submit non-sensitive scoping information, receive a fixed or time-limited quote, or learn that additional review is required. The quote binds the canonical request, gross amount, settlement destination, listing and offer references, nonce, and expiry so the provider cannot reinterpret the paid request later.

After release finality, the provider creates or confirms a task linked to the order. A2A-compatible states represent the externally visible work:

State	Meaning	Example: entity formation
submitted	Paid order received and validated	Formation request accepted
working	Provider execution or internal review is underway	Name search, filing preparation, or operator review
input-required	The buyer can supply a concrete correction or choice	Proposed name unavailable; alternative required
completed	Contracted deliverables and any asset record are available	Formation evidence and managed entity created
failed	Provider cannot complete the service	Filing rejected and no permitted correction remains
canceled	Task ended under cancellation terms	Buyer withdraws before committed filing spend

The order record separately captures authorization, payment verification, deposit finality, release finality, dispatch, and recovery states. A legal, sanctions, compliance, or committed-spend review is not mislabeled as buyer input-required merely because a human decision is pending.

An input-required state includes a machine-readable request, a secure response route, and the effect of delay on the target completion date. The task record should distinguish provider processing time from buyer waiting time so reputation metrics do not assign responsibility incorrectly.

Completion attaches deliverable metadata and starts the buyer-confirmation window without ending the relationship. Follow-on paid work creates a new authorization and task linked to the same provider relationship and, where applicable, the same persistent asset.

Persistent Assets and Continuing Control

Many procurement outcomes create a durable provider-held asset: a domain, mailbox, entity record, registered-agent relationship, hosting account, or similar resource. The provider remains authoritative for the asset's operational state. The procurement layer stores only the identity, authorization, and routing information needed to let the payer discover and act on it.

Each private read or mutation requires a fresh payer-wallet authorization scoped to the exact provider, service, action, asset, request, audience, nonce, and expiration. The provider independently verifies the marketplace grant and current action definition. A leaked asset identifier, order handle, email, or support message cannot by itself authorize a mutation.

Destructive actions use staged confirmation. The first authorization produces an exact effect summary, confirmation hash, earliest execution time, and expiry. After the delay, a second fresh authorization confirms or cancels that exact staged effect. This protects agents and principals from accidental deletion, dissolution, transfer, or other irreversible changes.

The base control root is the payer wallet. Delegation, organizational roles, wallet rotation, recovery, and asset transfer are profile extensions and must not be inferred from possession of an identifier or from the existence of a prior relationship.

Relationship Communications

The protocol does not attempt to replace every communication channel. Machine-executable, priceable, or authorization-sensitive actions use structured skills and explicit task events. Routine questions, human-readable explanations, and service notices may use provider-declared channels such as authenticated email or a secure portal.

The support rail preserves routing and context. A buyer agent can identify the relevant transaction, open a support request, receive status changes, and let another agent continue the case only when that agent presents fresh authority recognized for the same payer or principal. Providers can issue renewal notices, compliance reminders, and service-required alerts through declared channels while linking any action requiring payment back to a new authorization.

Subscriptions follow the same rule. The existence of an ongoing service permits communication and state continuity; it does not grant unlimited debit authority. The base profile uses a new authorization for each renewal or paid action. A visible, revocable mandate with amount and timing limits may be added by a profile that explicitly supports recurring authorization.

Gateway and Access Layer

Some implementations use a gateway to expose wallet-agnostic tools, issue challenges, validate payment attempts, establish chain evidence, release settlement, and sign provider dispatch or asset-action grants. Others may support enterprise accounts, managed wallets, or fiat-compatible entry points. The active profile declares which gateway, facilitator, or signer dependencies are required.

A gateway is not the authoritative store for provider tasks or assets and does not take discretionary custody of service funds. It can nevertheless be a required orchestration and trust component for paid purchases and protected actions. A direct crypto-native path exists only where the provider and active profile accept equivalent signed commitments, evidence, and lifecycle grants; protocol compatibility alone does not create a bypass.

If an access provider becomes unavailable, on-chain settlement and signed commercial records should remain provable. Continuing the relationship through another interface may still require an admitted replacement profile, fresh buyer authority, and provider-recognized grants. Portability is therefore an explicit recovery property, not an automatic consequence of using a wallet.

End-to-End Example: Entity Formation

Entity formation illustrates why procurement cannot be reduced to a single request and response.

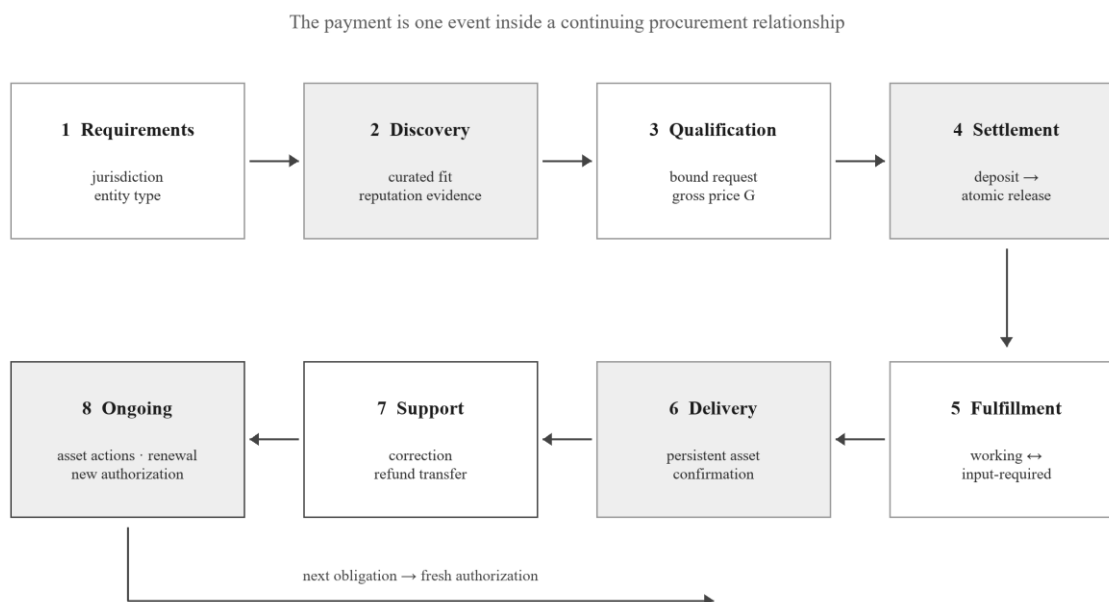


Figure 4. Entity formation procurement and relationship lifecycle

1. **Requirement definition.** A buyer agent identifies the principal, target jurisdiction, desired entity type, timing, continuing-service needs, and constraints on information disclosure.
2. **Curated discovery.** The agent queries the catalog for admitted outcomes, applies jurisdiction and eligibility filters, examines transaction-linked reputation evidence, and selects or ranks the eligible providers according to the principal's risk preferences.

3. **Pre-purchase qualification.** The selected provider checks basic eligibility and returns the required inputs, exclusions, expected timeline, signed terms, gross price, included marketplace commission, expected provider net, government or third-party fees, and support policy. A time-limited quote binds the canonical request. Sensitive documents are not placed on a public registry.
4. **Authorization and settlement.** The agent verifies the identity snapshot, listing epoch, offer, quote, and settlement destination before authorizing the gross amount. The buyer deposit becomes final, then an atomic release transfers provider net proceeds and the disclosed commission. The order retains separate deposit and release evidence.
5. **Multi-step fulfillment.** After release finality, the provider accepts the signed dispatch and moves the task from submitted to working. If a name is unavailable or information is incomplete, the task enters input-required with a structured request. The authorized buyer agent responds and the task returns to working. Provider or compliance review remains separately attributable.
6. **Delivery, asset creation, and confirmation.** The provider marks the task completed, delivers formation evidence and access instructions, and records the managed entity as a persistent asset controlled for the payer wallet. The buyer checks the artifacts and may submit a revisable delivery confirmation. The transaction contributes evidence to the provider's computed reputation.
7. **Post-transaction support and refund.** If a filing detail appears incorrect, the buyer opens support against the original transaction. The provider can correct the work, explain the result, or apply the bound refund policy. A refund is a separately funded transfer recorded against the original gross amount, not a reversal of the splitter.
8. **Ongoing relationship.** Registered-agent service, annual reports, amendments, dissolution, licenses, or other recurring obligations continue against the same entity asset. Notices can reach an agent acting with current authority. Each new paid or destructive action requires a fresh, appropriately scoped authorization.

Protocol Threat Model

The protocol narrows some risks and makes others visible. It does not eliminate the commercial risk inherent in purchasing real-world services.

False provider identity. A bad actor could present a fabricated or borrowed business identity. Curated admission binds the provider profile, authority keys, settlement wallet, endpoints, and verification evidence. Material changes trigger a new identity snapshot and listing epoch. The catalog states the scope and freshness of the checks rather than implying universal certification.

Registration confused with admission. A registry-only provider could appear equivalent to an admitted marketplace seller. Discovery exposes only outcomes admitted under the current curation policy. Explicit provider lookup identifies a registry-only provider as non-purchasable. A listing fee or valid registry signature does not purchase trust.

Reputation farming and Sybil behavior. Colluding buyers and providers can attempt to manufacture positive outcomes. Every counted signal must link to an actual settlement and task, which imposes cost but does not mathematically eliminate profitable manipulation.¹⁶ Buyer or marketplace ranking can reduce the weight of circular activity, repeated counterparties, low-value transactions, and abrupt identity changes.

¹⁶ Cheng, Y. et al. (2021). "On the Limits of Reputation-Based Mechanisms." AAMAS 2021.

Confirmation grieving. A competitor could purchase a service and submit a negative confirmation. The attack requires a real purchase, and the signal is evaluated alongside the provider's broader history, refunds, value, and counterparty pattern. A single binary signal is evidence, not a verdict.

Catalog manipulation and stale terms. A provider may change a live manifest after discovery. Authorization binds a signed listing epoch, offer, quote where required, canonical request, and material schemas. Discovery interfaces show when identity, pricing, and service commitments were last refreshed.

Payment-component exploitation or delayed release. The buyer deposit and splitter release are separately evidenced. The settlement destination has immutable recipients and policy bindings, while the release transfers provider net and commission atomically. Implementations still defend against replay, token incompatibility, reentrancy, unexpected balance deltas, false finality, duplicate deposits, and a deposit that becomes final before release succeeds.

Ambiguous external fulfillment. A supplier request may have succeeded even when a network timeout or process failure hides the response. The provider records durable intent and a request fingerprint before an at-most-once mutation. It reconciles authoritative supplier state before retry, refund, or terminal failure. Blind repetition of a potentially successful filing, registration, renewal, or deletion is forbidden.

Unauthorized persistent-asset actions. An attacker may acquire an asset identifier or stale support context and attempt a private read or mutation. Every protected action requires fresh, scoped wallet authority and a provider-recognized grant. Destructive effects are staged, delayed, and separately confirmed or canceled.

Provider-output and support-content prompt injection. Provider results, uploaded documents, web content, and inbound email can contain text intended to override a buyer agent's instructions. Implementations treat external content as untrusted data, enforce closed schemas and size limits, reject active content, isolate provider payloads from model instructions, and require explicit scoped authorization for any resulting mutation.

Improper autonomous decision-making. An agent may attempt to approve compliance judgments, committed supplier spend, refunds, or irreversible actions beyond its authority. The fulfillment model distinguishes buyer-supplied input from provider review and human-only decisions. Fail-closed gates preserve the responsible human or commercial authority where the service requires it.

Access-layer compromise or outage. A required gateway or signer may issue invalid challenges, grants, or evidence, or become unavailable. Short-lived audience-bound signatures, independent provider verification, immutable settlement evidence, signer rotation through new profiles, and explicit recovery states limit the effect. An implementation must disclose the access dependencies that remain trust anchors.

Support-channel impersonation. Attackers may imitate a provider and send urgent payment or credential requests. Support routes are declared in the provider identity and service records, and any paid or authorization-sensitive action returns to a bound request and fresh signature. Informal messages cannot silently change settlement destinations or asset authority.

Unauthorized recurring charges. A continuing service could be used to justify charges outside the buyer's intent. Recurring payments require a scoped, revocable mandate with amount and timing limits or a new authorization. Renewal notices alone do not authorize payment.

Privacy leakage. Business services may require personal, legal, or confidential documents. Public records contain identifiers, hashes, timing, and outcome evidence only where necessary. Documents, asset details, credentials, and support contents remain off-chain with access controlled by the parties.

Lifecycle abandonment. A provider may accept payment but stop responding during a multi-step task, asset lifecycle, or support case. Task timers, input attribution, support escalation, renewal notices, refunds, and computed reputation make abandonment observable. Category-specific guarantees may add financial recourse, but they are not implied by the base protocol or its commission.

Use Cases and Service Categories

The protocol is most useful where the seller's reputation, the quality of the handoff, the control of a resulting asset, and the continuing relationship materially affect the buyer's outcome.

Category	Typical lifecycle	Why provider reputation matters	Protocol capabilities used
Entity formation	Qualification, filing, corrections, delivery, continuing entity actions	Errors can create legal and operational consequences	Curated discovery, secure inputs, task states, persistent asset, support
Registered agent and compliance	Ongoing service with event-driven notices and recurring filings	Missed notices or deadlines can impair the entity	Persistent identity, notices, fresh authorization, support history
Accounting, tax, and professional services	Scoping, document exchange, analysis, revisions	Competence and responsiveness are central to value	Qualification, reputation evidence, input loops, deliverables, follow-on work
Domain and digital presence	Purchase followed by administration, transfer, and renewal	Control, continuity, and recovery matter after checkout	Settlement, wallet-controlled asset actions, renewal notice, support
Hosting, email, and operational infrastructure	Provisioning plus continuing service	Reliability, security, and response quality accumulate over time	Manifest, protected asset actions, renewals, service notices, support
Licensing, filings, and physical mail	Jurisdictional workflow with deadlines and exceptions	The provider acts across external systems the buyer cannot directly observe	Curated fit, task states, reconciliation evidence, post-transaction routing

These services often compose into procurement plans. An agent may form an entity, obtain required registrations, establish communications and infrastructure, and then maintain recurring compliance. The protocol lets each service remain separately authorized while preserving the relationships, assets, and evidence needed to manage the whole plan.

The protocol is deliberately less focused on one-time, self-contained digital purchases. A bounded API result, deterministic computation, single downloadable asset, or other atomic resource is generally better served by direct x402 payment and an atomic marketplace. The boundary is functional, not ideological: use the least complex transaction model that safely completes the job.

Administration and Economic Model

Protocol implementations require accountable administration of provider admission, catalog policy, listing epochs, settlement configuration, signer profiles, software updates, security response, and commission destinations. Those controls should be documented, access-limited, auditable, and appropriate to the implementation's legal and operational environment. This paper does not require a native token or a separate political-governance system.

Interoperability does not require every marketplace to make identical choices. Different implementations may curate different providers, apply different scoring models, select different access profiles, or serve

different jurisdictions while using compatible manifests, commitments, settlement records, and task links. Buyers can evaluate those policies just as they evaluate providers.

Revenue Model

The protocol supports two complementary marketplace revenue streams: a disclosed transaction commission and provider-side listing or integration fees. For a purchase, the buyer authorizes the displayed gross amount G . The immutable release records the marketplace commission C and provider net N separately, with $G = N + C$. The commission is therefore included in the authorized gross amount rather than introduced as an undisclosed second charge.

Provider-side fees can cover registry administration, application review, provider onboarding, offer-manifest integration, and ongoing catalog maintenance. A registration fee may be charged once. A recurring listing, integration, or maintenance fee exists only where an implementation expressly offers it and discloses its renewal terms; recurrence is not implied by the base protocol.

Registration and admission remain separate. Listing and integration fees purchase defined marketplace services; they do not purchase trust. Payment must not guarantee admission, imply marketplace endorsement, increase computed reputation, or improve marketplace ordering. Purchasability, reputation computation, and any ranking remain governed by disclosed criteria and active signed outcomes.

Commission configuration is bound to the listing epoch and changes prospectively. Categories requiring deeper provider qualification, integration, workflow support, protected asset operations, or continuing relationship infrastructure may justify a different rate from lighter services. An implementation may also set the rate to zero where it does not add sufficient procurement value. The gross amount, commission rate and amount, provider net, and any category rule must be visible before authorization.

The commission funds the marketplace functions described in this paper: curated provider supply, machine-readable commercial integration, computed reputation, fulfillment orchestration, persistent authority, support continuity, and secure settlement evidence. It does not convert the marketplace into the service provider, custodian, insurer, or universal dispute arbiter.

No native token is required for settlement, service access, listing, or commission payment. The protocol's economic test is straightforward: providers should pay listing or integration fees only when defined registry, admission-review, integration, or catalog services are supplied; agents should authorize the commission when the marketplace reduces the cost and risk of business procurement; and agents should use a simpler direct payment path when it does not.