Stamps for Agents

A narrow, ownerless pricing layer for an open agentic web

If we want an open agentic web, the missing piece may be a thin, interoperable "stamp" layer: not identity, not commerce, not licensing — anti-abuse pricing for automated access, standardized before proprietary defaults harden.

Date: 2026-04-29
Mike Linksvayer (personal capacity)
Epistemic status: Speculation/brainstorm/wishful thinking; exploratory framing for an interdisciplinary workshop
Biases: increasing generative capacity » redistributing market power; love prices, externality taxes, markets are expensive and need entrepreneuers, low risk/potential big win to provide primitives that optionally enable markets, eg https
License: CC0-1.0

HTTPS: a narrow constraint that unlocked a market

- One narrow function: **secure the channel** between user-agent and named server.
  - *Not* identity-of-the-human, *not* payment, *not* content trust, *not* abuse.
- Twenty-four-year arc from possible (1994) to default (~2018).
- Frictions broke one by one: **export controls** (relaxed 1999–2000), **open-source crypto** (OpenSSL, later LibreSSL/BoringSSL/mbedTLS), CPU cost (AES-NI), cert cost & hassle (**Let's Encrypt + ACME, 2015**), shared hosting (SNI), mixed-content & migration tooling (HSTS, HTTPS Everywhere), and last — **browser UI pressure** flipped the default.
- Two-stage adoption: high-value flows (login, e-commerce) went HTTPS early because both sides wanted it. *Ubiquity* — the long tail of static sites — required user-agents to push.

> The hard problem in 1995 wasn't agreeing HTTPS was needed. It was deploying a narrow constraint cheaply, openly, and ubiquitously enough that an open-web market could rely on it.

The agentic web is not one problem — it's at least five

#	What people want	Maps to	Shape
1	**Verifiable agent identity**	TLS/PKI for agents	PKI-shaped, technically clean
2	**Anti-abuse pricing ("stamps")**	Postal stamps; HTTP 402	**Bearer-token-shaped; institutional load concentrated in issuance**
3	**Consent / delegation proofs**	OAuth-for-agents; AP2	User-context-shaped
4	**E-commerce semantics**	UCP, AP2, traditional payments	Domain-specific, fat
5	**Reputation**	CAs, credit bureaus, PageRank	Institutional, slow

These are **layered, not competing.** Identity work is well underway (RFC 9421 HTTP Message Signatures, Web Bot Auth, DPoP). Stamps is less discussed and surprisingly clean as a thin layer.

> Most "agentic web" proposals try to solve all five at once. HTTPS won by solving exactly one. The interesting question is which of these can be the next "exactly one."

Defining stamps: access pricing, not commerce

	E-commerce payment	Stamp payment
Shape	Buy a specific thing	Affix proof-of-postage per request
State	Stateful, bilateral	Stateless, bearer instrument
Needs	Identity, refunds, disputes, regulation	None of those
Verdict	**Fat**	**Thin**

Stamps are **anti-abuse pricing**, not commerce. The post office doesn't care *why* or *who* — only that the cost has been prepaid.

> *Access pricing, not rights licensing.*
> *Anti-abuse, not commerce.*
> *Bearer proof, not identity.*

Stamps fit the *institutional* shape of HTTPS

Identity is the most HTTPS-shaped *technically*: clean PKI, well-understood threat model.

Stamps may be the most HTTPS-shaped *institutionally*:

- A narrow constraint that, if standardized openly, preserves participation at adjacent layers.
- Aligned incentives: origins want abuse priced; legitimate agent operators want a way to prove they aren't abuse without bilateral deals with every site.
- Independent of identity, consent, commerce, reputation — a stamp is a bearer token.
- Standards-feasible building blocks already exist: HTTP 402, RFC 9421 signatures, Hashcash lineage, x402, L402, Cloudflare Pay-Per-Crawl.
- Real chokepoints exist for enforcement: CDNs on the receive side, agent runtimes on the send side.

> A stamp layer is a constraint. The question is whether it's an open, auditable, interoperable constraint that preserves downstream independence — or a privately owned toll layer that reallocates option value to CDNs, payment processors, and dominant agent runtimes.

Governance is the whole game

The protocol is the easy part. **Issuance is the political question.**

- **Cautionary precedent:** Goodmail (2005–2008) — paid certified email, single commercial issuer, AOL/Yahoo as gatekeepers. Killed by an EFF/MoveOn-led coalition that correctly identified it as a tax on legitimate senders enforced by inbox gatekeepers.
- **Positive precedent:** Let's Encrypt (2015) — neutral, automated, free issuance via the Internet Security Research Group. Collapsed the cost of participation in HTTPS from "annual hassle + $50–500" to zero. Without it, HTTPS adoption stalls at the well-resourced top of the web.

The institutional question for stamps:

- Who issues stamps without becoming a toll gate?
- What's the unit of account, and how is the price set?
- Origins set their own prices and waivers per-request — but a healthy regime needs at least one neutral, low-cost issuer for that to be more than theoretical.
- **How are research, accessibility, archiving, journalism, and search preserved?** Per-origin policy + shared community lists + taxpayer / philanthropic subsidy of stamps for sympathetic users — *not* a protocol-level exemption registry.
- **Buy-side discipline.** Per-request pricing creates a market: budgets, comparison shopping, walk-away — extortionate pricing is mostly self-limiting. (Side benefit: agents become more robust.)

Alternatives all centralize somewhere

Family	Examples	Where it centralizes
Default-deny + bot management	Cloudflare, Akamai, DataDome, Turnstile	Bot-mgmt vendors
Verified-bot identity (no payment)	Web Bot Auth, signed crawler IDs	Big agent vendors
Bilateral licensing deals	NYT/OpenAI, Reddit/Google, AP, News Corp	Top publishers + top AI vendors
Subscription bundles at agent platform	ChatGPT/Claude/Copilot subs cover access	Agent platforms
Crawl-as-a-service marketplaces	Bright Data, Apify, ScrapingBee	Data brokers
Voluntary signaling	robots.txt, ai.txt, AI-Preferences	Consensus contested; compliance voluntary
Legal / regulatory	Copyright suits, EU AI Act	State + well-resourced litigants
API-key / OAuth everywhere	Login required to read	Identity providers; kills unauthenticated open web

> Sender-pays stamps with multiple competing issuers is the only family that **doesn't structurally require centralization** — *if* the issuance layer stays open.

Multiple equilibria

	Open-web equilibrium	Walled-garden equilibrium
E-commerce	TLS + Let's Encrypt + open standards	Alipay / WeChat / super-apps
Agent traffic, commons-only path	Cheaper serving + norms + bulk side channels	Private default-deny + platform bundles
Agent traffic, with pricing primitive	**Open stamp standard + neutral issuers**	Bilateral deals + CDN-as-merchant + agent-platform bundles

> The easiest outcome is that the open access commons adapts: serving keeps getting cheaper, norms improve, bulk channels absorb the load, and no payment primitive is needed. *See YAGNI backlot slides.*
>
> But a stamp primitive is not only a fallback. Even if the commons holds, open pricing could make the agentic web larger by letting legitimate automated demand pay at the margin without bilateral deals.
>
> The question is whether any pricing that emerges is an open protocol layer with competing issuers and auditable rules — or whether it hardens into bilateral deals, default-deny CDNs, and agent-platform bundles.
>
> HTTPS preserved an open-web equilibrium for e-commerce by making one narrow function cheap, standard, and ubiquitous. A stamp layer wouldn't be HTTPS for everything agents do. It would be one narrow attempt to keep automated access from becoming a private toll-road architecture.

— Backlot —

The slides that follow are reserve material: the full HTTPS-shape checklist, technical flavors of stamp, prior art, alternative framings, and the YAGNI objection in detail. They expand on points that are compressed or dropped from the main deck.

Backlot: HTTPS-shape checklist for stamps

HTTPS property	Stamps?
Single, narrow problem	✅ "Make bulk unwanted traffic uneconomic."
Independent of adjacent layers	✅ No identity / consent / commerce required.
Aligned incentives	✅ Origins want abuse priced. Legit agents want a way to prove they aren't abuse without bilateral deals.
Standards-feasible building blocks	✅ HTTP 402, RFC 9421 signatures, Hashcash lineage, x402, L402, Cloudflare pay-per-crawl.
Plausible chokepoints	✅ CDNs (receive side), agent runtimes (send side).
Doesn't require resolving political fights	✅ Fair-use, liability, reputation all stay independent.

Backlot: where the HTTPS analogy breaks

- **No single agreed problem.** HTTPS had one. The agentic case has at least five.
- **Asymmetric incentives.** HTTPS had aligned incentives — site, user, browser all wanted it. Agent operators and origins are *not* aligned today.
- **Money is in the loop.** HTTPS marginal cost → 0. Anything payment-shaped structurally cannot.
- **No "browser-equivalent" with default-setting power yet.** Several candidates (CDNs, agent runtimes, OS vendors), none consolidated.

Backlot: three flavors of stamp

- **Cash-backed** — real micropayments (e.g. x402, stablecoin or card-on-file at issuer level). Closest to actual postage.
- **Compute-backed** — Hashcash-style proof-of-work. Politically attractive (no money, no regulation). Historically loses to well-funded adversaries.
- **Credential-backed** — prepaid stamp buckets from a few issuers. Pragmatically likely; risks centralization.

> Today's default is "free unless blocked." Stamps flip it to "priced unless waived."

Backlot: challenges in detail

1. **Marginal cost can't be zero.** Adoption is asymmetric, not a flag-flip.
2. **Price discovery is real.** Static page ≠ DB query ≠ purchase → denominations / postal classes. Risk: scope creep.
3. **Issuer concentration.** Three CDNs + two hyperscalers = "stamps" become "tolls." Central political question.
4. **Regulation.** Cash-backed brushes against payments regulation, KYC, tax, cross-border. Technically thin, legally not always.
5. **PoW favors well-funded adversaries.** Email-Hashcash failed for this reason.
6. **Free-tier & human exemptions.** Must not break logged-in users, accessibility, search crawlers, archive.org, research.
7. **Fragmentation before consolidation.** Pay-per-crawl, x402, L402 today — could converge or harden into silos.

Backlot: next steps

- **Make the commons-holds path work:** cheaper serving, static/dump/API paths, better caching, responsible collection defaults, shared preference signals, and public-interest funding.
- **Standards track:** IETF/W3C convergence on HTTP 402 + denomination format + stamp issuance/verification spec. Several drafts already exist.
- **A "Let's Encrypt for stamps":** neutral, automated, free-or-cheap issuance is the missing piece. Without it, this becomes a CDN toll road.
- **A "browser-equivalent" willing to set defaults:** agent runtimes (Anthropic, OpenAI, Google, MS) carry stamps by default; CDNs require them.
- **Empirical work:** what fraction of "abuse" traffic is deterred at $0.0001 / $0.001 / $0.01 per request? Cloudflare's Pay-Per-Crawl deployment is generating the first real data.

Backlot: robots.txt as the negative example

- Voluntary, low-cost, near-universal.
- Worked for ~30 years on a gentleman's agreement.
- **Decline under economic pressure:** training-data wars, AI scrapers ignoring it, bilateral licensing deals, IP block lists.
- The cleanest argument for why a technically-enforced equivalent is needed.

Backlot: prior art (chronological)

- **HTTP 402 "Payment Required"** *(1997, HTTP/1.1)* — status code reserved in the spec from day one. "Reserved for future use" for ~28 years.
- **Hashcash** *(1997, Adam Back)* — proof-of-work stamp for email. SHA-1 puzzle in a header. Spec lives on (Bitcoin's lineage); email deployment failed — asymmetric attacker advantage, no enforcement chokepoint.
- **Penny Black** *(Microsoft Research, ~2003)* — proof-of-CPU and proof-of-memory variants for email postage. Never deployed at scale.
- **Goodmail CertifiedEmail** *(2005–2008)* — paid certified email; AOL & Yahoo accepted it for inbox bypass. Killed by EFF/MoveOn "Dear AOL" backlash + commercial collapse.
- **L402** *(Lightning Labs, 2020)* — Lightning + macaroons + HTTP 402. `WWW-Authenticate: L402 macaroon=…, invoice=…`; client pays BOLT11, returns `Authorization: L402 <macaroon>:<preimage>`. Stateless cryptographic verify.
- **x402** *(Coinbase, May 2025)* — open spec; HTTP 402 with stablecoin (USDC) settlement, chain-agnostic. "Facilitator" servers handle settlement so origins don't touch crypto. Designed for agents and APIs.
- **Cloudflare Pay-Per-Crawl** *(July 2025, beta)* — CDN-edge stamp regime. Origin sets per-crawl USD price; crawler gets HTTP 402 with price; Cloudflare is merchant-of-record. Default-deny for AI bots on new sites.

> The pattern: failures targeted federated substrates (email) with no enforcement chokepoint. The current generation targets HTTP-fronted services where CDNs and agent runtimes provide chokepoints. That's the changed variable.

Backlot: are any of these "the" httpstamp standard?

Short answer: no, but the building blocks are converging.

	Best at	Why it isn't yet the standard
L402	Verification model — stateless macaroons	Lightning-only — niche audience
x402	Settlement abstraction — facilitators, agent-first	Coinbase-led, stablecoin political ceiling
Cloudflare Pay-Per-Crawl	Enforcement topology — CDN edge, neutral merchant-of-record	Single-vendor: *is* the toll-road failure mode
Hashcash / PoW	No money, no regulation, no issuer	Adversary asymmetry; companion only

Plausible synthesis: L402's verification model + x402's settlement abstraction + Pay-Per-Crawl's enforcement topology + a Let's-Encrypt-shaped neutral issuer.

Backlot: the YAGNI objection — the China case

The sharpest objection: HTTPS consensus was overstated in retrospect; China has world-leading e-commerce without ubiquitous HTTPS. Maybe stamps are YAGNI too.

What's right about it

- Pre-Snowden / pre-Firesheep, HTTPS-everywhere was contested. Consensus consolidated *after* deployment.
- Chinese top-site HTTPS adoption has lagged the West (~70–80% vs ~95%+).
- Chinese e-commerce (Alipay, WeChat Pay, Taobao, JD, Pinduoduo) is genuinely world-class.

What it misses

- **Encryption didn't disappear, it moved into apps.** Mobile-app-first means TLS-protected API calls underneath; the padlock is just invisible. Payment-bearing wire is encrypted everywhere.
- **Substitution, not absence.** Where open-web HTTPS is lower, the trust model was substituted: real-name verification, centralized settlement (Alipay/WeChat Pay), super-apps as walled trust boundaries.
- That substitution has costs: super-app dominance, no permissionless entry, privacy concentrated in platforms/state.

> HTTPS wasn't the only way to get safe e-commerce. It was the only way to get safe e-commerce **on the open web.** The same is true of stamps and the open agentic web.

Backlot: YAGNI objection — the commons adapts

The stronger YAGNI objection: maybe the open-access commons holds without a payment primitive.

That could happen if:

- Serving information keeps getting cheaper: static publishing, edge caches, object storage, better rate limits.
- Being available to agents remains valuable: discoverability, citation, narrative presence, advertising-like subsidy.
- Commons infrastructure scales: government, philanthropy, universities, private complements / exhaust.
- Responsible collection norms and tools become good enough defaults.
- Bulk/high-volume needs remain as side channels: dumps, APIs, Wikimedia Enterprise-style services.

> If this is right, stamps add transaction cost, governance risk, and financial mediation where cheaper technical and institutional adaptation would suffice.

Backlot: why now?

- Real economic pressure on origins from agent / crawler traffic; not limited by human attention.
- Bilateral licensing fragmentation: NYT/OpenAI, Reddit/Google, Stack Overflow, AP, News Corp, Axel Springer, Vox.
- Closing window before *de facto* solutions harden into proprietary tolls.
- Cloudflare Pay-Per-Crawl shipped to GA mid-2025 covering a meaningful fraction of the web.
- Agent runtimes consolidating among ~5 vendors who could default-on stamp behavior.

Backlot: Pigouvian framing

- Stamps are a **price on an externality** imposed by agent traffic on a commons (origin infrastructure).
- Not a moral judgment on agents — a market mechanism.
- Closest analogs:
  - **Congestion pricing** (London, Stockholm, Singapore)
  - **Carbon pricing** (cap-and-trade or carbon tax)
  - **Postage** itself
- Same design questions as those: who collects, who's exempt, what's the unit, how is the price set, how is it adjusted.

Backlot: what stamps deliberately don't solve

- **Training-data licensing fights.** Stamps price *access*, not *rights*. Fair-use questions stay independent.
- **Agent intent declarations.** "Is this for training / answering / transacting?" Separate proposal. Stamps don't care why.
- **Reputation.** Out of scope — different layer.
- **End-user identity / consent.** Out of scope — different layer (AP2, OAuth-for-agents).
- **Liability for agent actions.** Out of scope — legal, not protocol.

> Discipline about scope is the whole point. Stamps refuse to solve adjacent problems — that's why they're institutionally tractable.

Backlot: 5-year success picture

- A neutral issuer ("Let's Encrypt for stamps") exists, free or near-free for low volumes.
- Two or three IETF RFCs covering 402 challenge format, denomination, and signature/proof carriage.
- Major CDNs default to challenging unauthenticated agent traffic with a stamp requirement.
- Major agent runtimes default to carrying stamps from a small, interoperable set of issuers.
- Origin operators see a measurable drop in unwanted-bot load and a measurable revenue stream from legitimate paid traffic.
- Robots.txt-style voluntary signaling continues, but as a *preference* layer on top of the *enforced* stamp layer.

Backlot: buy-side dynamics — does this just become extortion?

How agents decide whether to pay:

- Per-request budgets and price caps set by the principal.
- Comparison shopping across substitutable sources.
- Anomaly detection on price spikes.
- Walk-away as the always-available default.
- Public price feeds / aggregators (expected to emerge).

Why extortion is mostly self-limiting:

- Substitutable content → comparison shopping wins.
- Unique content (court records, primary datasets) already has market power today via paywalls and bilateral licensing — stamps don't make it worse, just give it an HTTP-shaped interface.
- No agent is *obligated* to pay.

Side benefit: agents that handle 402s, varying prices, and budget exhaustion become more robust to all error states.