Domain Attest

DomainAttest: An Open Protocol for Domain Ownership Verification

White paper · July 2026 · domainattest.org

Abstract

Domain marketplaces must establish that a seller controls a domain before listing it. The prevailing method, demonstration of DNS control through TXT records or name server changes, is slow, error-prone, and proves the wrong thing: control of a zone file at one moment, rather than current ownership of the domain. In practice these costs cause marketplaces either to skip verification, enabling fraudulent listings, or to verify once and treat the result as permanent, producing stale verifications that persist after domains change hands.

DomainAttest is an open protocol through which a sponsoring registrar issues a short-lived, cryptographically signed attestation that an authenticated account controls a specific domain. The protocol is a profile of the OAuth 2.0 authorization code flow with PKCE and introduces no new cryptographic primitives or identity infrastructure. Verification completes in seconds, reflects ownership at the time of issuance, and can be repeated at negligible cost. This paper describes the problem, the protocol, its design rationale, and considerations for each participant. The normative specification is published separately.

1. Background

Proof of domain control is among the most frequently performed verification rituals on the internet. SaaS platforms require it at onboarding, email authentication depends on it, advertising and payment systems use it to validate counterparties, and emerging identity systems anchor identifiers to domains. Nearly all of these rely on the same mechanism: the requester publishes a challenge value in the domain's DNS, and the verifying service polls for it. The IETF's ongoing work on best practices for DNS-based domain control validation reflects both the ubiquity of the pattern and its known operational problems.

This paper concerns the setting where those problems are most acute: domain marketplaces, where verification gates a transaction, failure enables fraud, and the party being verified is often a portfolio holder performing the ritual repeatedly.

The registrar of record for a domain maintains authoritative knowledge of which account controls it. No standard mechanism exists for a third party to query that knowledge with the owner's

consent. Marketplaces therefore rely on the same indirect proxy as everyone else: the seller demonstrates control of the domain's DNS by publishing a nonce in a TXT record or repointing name servers, and the marketplace polls until the change propagates.

This method has known deficiencies:

1. Latency. DNS propagation introduces delays from minutes to 48 hours between the seller's action and confirmation.

2. Error rate. Manual record entry fails often enough that marketplaces maintain support processes for it, and registrars receive the resulting tickets.

3. Weak proof. DNS control is not ownership. A compromised zone or hijacked name server satisfies TXT verification. Conversely, an owner whose domain runs production email or a live site bears risk when editing its records.

4. No freshness. The proof is valid only at the instant of the check, but is typically recorded as a permanent attribute of the listing.

5. Conflict with delegation. Actively listed domains commonly delegate their name servers to a marketplace's landing-page or DNS service. The registrar's zone is then not authoritative, and a TXT record added there is invisible to the verifying party. To verify with an additional service, the holder must re-delegate the domain to the registrar, wait for propagation, complete verification, then restore the original delegation and wait for propagation again, with the landing page and any purchase traffic it carries unavailable in the interim. This burden falls most heavily on the most active sellers, precisely those who verify most often.

2. Related work

Domain Control Validation using DNS (IETF). An active IETF dnsop working group draft, draft-ietf-dnsop-domain-verification-techniques, defines best current practices for DNS-based domain control validation, recommending TXT-based challenges that are time-bounded, randomized, and targeted to a specific application service. The draft addresses the operational deficiencies of ad hoc TXT verification within the DNS-based model. DomainAttest shares its conclusions about validation hygiene, in particular that proofs should be time-bounded and scoped to a single consumer, but applies them outside the DNS-based model entirely: the assertion is obtained from the sponsoring registrar's authoritative records with the holder's consent, rather than inferred from zone contents.

Domain Connect. Domain Connect is an open standard, with an IETF working group formed toward its formalization, through which a service provider applies DNS configuration templates at a user's DNS provider with the user's consent, using an OAuth-based flow. It is the closest architectural precedent for consent-mediated interaction between a domain holder's provider and a third-party service, and its registrar adoption demonstrates that the integration model is

practical. Its purpose is orthogonal: Domain Connect configures a domain's DNS; it does not produce a portable assertion of ownership consumable by a third party. DomainAttest addresses that distinct trust object, and its attestations are signed and audience-bound because they are presented to parties outside the flow that produced them.

Commercial registrar-marketplace networks. Afternic's Fast Transfer network and the Sedo MLS integrate marketplaces with registrars bilaterally, using pre-authorized EPP transfer credentials to enable listing distribution and immediate post-sale transfer. These systems demonstrate registrar-integrated marketplace flows at scale, but they are proprietary, pairwise, and oriented toward transfer execution rather than ownership proof; participation requires a commercial relationship with the network operator, and neither defines an open, marketplace-neutral verification mechanism. DomainAttest standardizes the verification layer these networks each implement privately, and is available to any relying party without a relationship with any network operator.

Registration data services. RDAP provides authoritative, structured access to registration data and is used by DomainAttest for registrar discovery. RDAP responses describe the registration; they do not establish, with the holder's participation, that a particular authenticated party controls the domain, and privacy services redact the registrant data that might otherwise be compared. DomainAttest is complementary: RDAP locates the authority, and the protocol obtains the authority's consent-based assertion.

3. Problem statement

Because each verification is costly, the industry has converged on two practices, each with distinct harms.

Unverified listings. Some marketplaces do not verify ownership at all. Any party can list any domain. This enables front-running, in which a party lists a domain it does not own and attempts to acquire it only after finding a buyer, as well as outright fraudulent sales. Buyers cannot distinguish verified from speculative listings, and owners discover their domains listed by third parties.

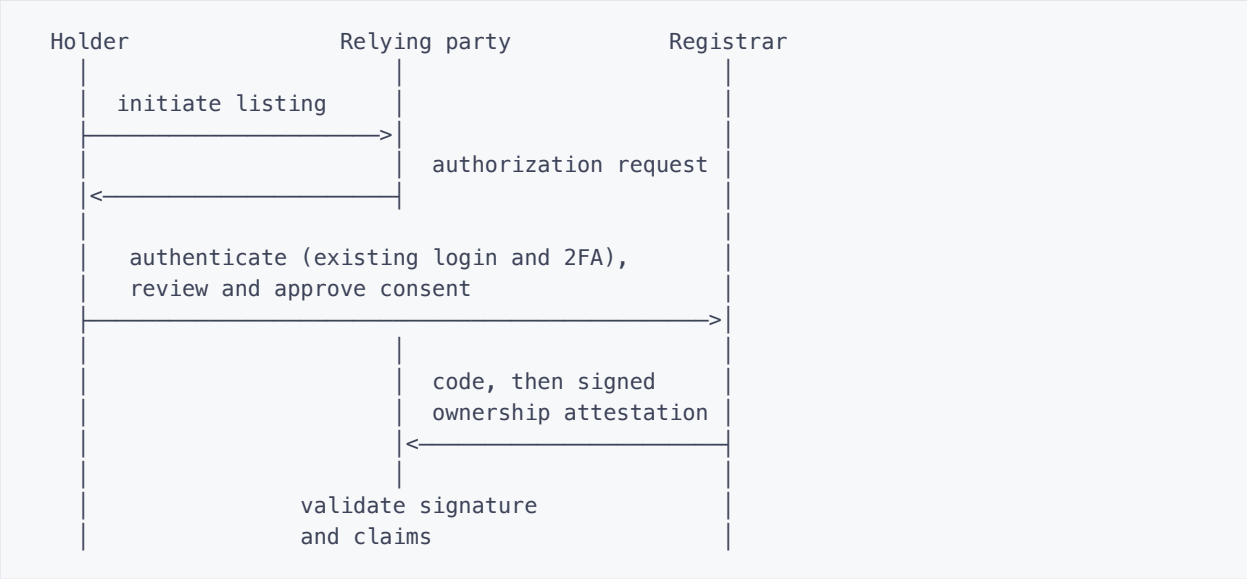
Stale verification. Marketplaces that verify typically do so once, at listing creation. When the domain is subsequently sold or transferred, the verification is not invalidated. The listing persists under the previous owner's account, often at an obsolete price. The current owner, seeking to list the same domain, must displace the earlier verification through manual support processes, with the burden of proof falling on the party who actually owns the domain.

Both practices share a root cause: verification is expensive relative to its useful lifetime, so it is either omitted or never repeated.

4. Protocol overview

DomainAttest defines four roles: the holder (the party with an authenticated registrar account controlling the domain), the registrar (issuer of attestations), the relying party (consumer of attestations, typically a marketplace), and an optional hub (an aggregation service that transports, but cannot create or modify, attestations).

The flow is an OAuth 2.0 authorization code exchange with PKCE:



1. The relying party discovers the domain's sponsoring registrar via RDAP and retrieves the registrar's protocol metadata from a well-known endpoint.

2. The relying party redirects the holder to the registrar's authorization endpoint, identifying the domain and the requesting relying party.

3. The registrar authenticates the holder through its normal login, including any second factor on the account, verifies that the account controls the domain, and presents a consent screen naming the relying party and the domain.

4. On approval, the registrar issues an ownership attestation: a JWS-signed token asserting that the authenticated account controls the domain, bound to the requesting relying party, with a validity period not exceeding 15 minutes.

5. The relying party validates the signature against the registrar's published keys and the token's claims, and proceeds accordingly.

The attestation contains no registrant identity data. It asserts control, not identity, and leaves Whois privacy unaffected.

5. Design rationale

Authorization flow rather than static keys. A simpler design, in which the registrar displays a verification key that the holder pastes into a marketplace, was considered and rejected. A static key is a bearer credential, and the domain industry has extensive experience with the social engineering of bearer credentials in the form of transfer authorization codes. A key that proves ownership to any relying party is a key that attackers will extract from owners to list stolen domains. The authorization flow leaves no copyable secret: consent occurs on the registrar's own property under the account's existing protections, and the resulting attestation is useless to any party other than the named relying party.

Short validity by design. Attestations expire within minutes. This is a deliberate response to the stale-verification problem described in Section 3. Ownership is a time-dependent fact; a proof mechanism that records it as permanent will diverge from reality. Because re-attestation costs the holder a single approval, relying parties can re-verify at operationally significant moments, such as a price change, an incoming offer, or the opening of escrow, and can automatically retire listings whose sellers no longer control the domain. The protocol deliberately defines no long-lived token in version 1.

Existing standards only. The protocol is composed entirely of deployed, well-understood mechanisms: OAuth 2.0 authorization code flow, PKCE, JWS-signed JWTs, and JWKS key publication. A registrar with a contemporary authentication stack can implement the required endpoints in a small number of engineering weeks. No new trust infrastructure is required beyond the registrar's existing relationship with its customers.

Incremental adoptability. The protocol requires no coordinated adoption. A single registrar and a single relying party provide complete functionality to their shared customers. Each additional registrar extends coverage; each additional relying party increases the value of registrar participation. DNS-based verification remains available as a fallback for domains at non-participating registrars.

6. Considerations by participant

Registrars. Participation positions the registrar as the authoritative source relying parties depend on for the ownership question, rather than solely the custodian of the registration. Practical effects include portfolio consolidation by sellers toward participating registrars, and elimination of verification-related support volume, including stale-listing disputes currently routed to registrars. As adoption extends to relying parties beyond marketplaces, such as software-as-a-service platforms that verify customer domains, the same effect reaches retail registrants: a business that repeatedly verifies its domain across services has a durable reason to remain with a registrar where each verification is a single click.

Relying parties. Verification friction currently suppresses supply at the point of highest seller intent, and unverified supply carries fraud risk. Registrar-signed attestations remove the friction

while strengthening the proof: a hijacked zone can satisfy TXT verification but cannot produce a registrar signature. Relying parties also retire their polling infrastructure, propagation handling, and manual dispute processes, and gain the ability to keep verification current over the life of a listing.

Holders. Verification completes in seconds within the registrar account the holder already controls, with no DNS changes and no risk to live services on the domain, and independently of where the domain's name servers point: a domain delegated to a marketplace's landing service verifies without disturbing that delegation. A holder who acquires a domain previously listed elsewhere can verify immediately, since current attestations supersede any earlier owner's stale verification.

Buyers. Listings carry registrar-level proof that reflects control at or near the present time, rather than DNS-level proof recorded at listing creation.

7. Comparison with DNS-based verification

Property	DNS-based verification	DomainAttest
Completion time	Minutes to 48 hours	Seconds
Holder action	Manual DNS record changes	Authorization via existing login
Assertion	Control of zone file at time of check	Registrar-of-record account control at issuance
Validity model	Recorded as permanent in practice	Explicit expiry; repeatable on demand
Resistance to DNS compromise	None	Requires registrar signature
Relying party infrastructure	Polling, propagation handling, disputes	Signature and claim validation
Standardization	Per-marketplace implementations	Single open specification

8. Security and privacy summary

The full analysis appears in the specification. In summary: the protocol defines no bearer secrets; attestations are audience-bound to a single relying party and expire within 15 minutes; relying parties reject replayed token identifiers; the consent surface is the registrar's existing login, introducing no new location where credentials are entered; compromise of a registrar signing key affects only that registrar's domains and is bounded by key rotation and token lifetime; and attestations exclude all registrant contact data.

9. Deployment model

Two integration paths are defined, and they interoperate.

Direct. A registrar implements the authorization and token endpoints and publishes its keys; a relying party integrates registrars individually and validates attestations against published keys. No relationship with any third party is required.

Hub. A hosted aggregation service exposes the same flow across all connected registrars behind a single integration. Attestations returned through the hub are the registrar-signed tokens, unmodified; the hub holds no signing authority and its output is independently verifiable. Registrars declare whether they accept traffic directly, through a hub, or both.

10. Machine-mediated transactions

An increasing share of domain discovery and acquisition is conducted by software agents acting on behalf of buyers and sellers. Verification workflows that depend on manual DNS edits and propagation delays serve such actors poorly: they require human intervention at an arbitrary point in an otherwise programmatic transaction and introduce unbounded latency. A signed attestation is machine-verifiable by construction, and the protocol's discovery and validation steps require no human judgment on the relying party's side. Ownership verification is therefore available as a programmatic primitive to agent-mediated commerce from version 1, with agent-initiated flows under delegated holder consent identified as a candidate extension. Absent a standard, this layer would likely emerge as a set of incompatible per-platform workarounds.

11. Scope and limitations

Version 1 attests that an authenticated registrar account controls a single domain at a point in time. It does not assert registrant identity, does not effect transfers, and does not address domains at non-participating registrars, for which DNS-based verification remains the fallback. Bulk attestation, standing verification, agent-initiated flows with delegated consent, and an optional settlement path for sales between accounts at the same registrar are identified as candidate extensions in the specification.

The protocol standardizes one layer: proof of domain control. Nothing in the attestation format or flow is specific to marketplaces; any service that currently verifies domain control through DNS challenges can act as a relying party, and applications beyond the domain aftermarket are natural extensions as registrar coverage grows. Within the marketplace setting, discovery, pricing, negotiation, escrow, and the remainder of marketplace function are unaffected and remain points of differentiation among relying parties.

12. Conclusion

The ownership question that DNS verification approximates has always had an authoritative answer held by the registrar of record. DomainAttest provides the standard mechanism, built from existing and well-understood components, by which that answer is issued with the owner's consent and verified by any party in seconds. The specification is published, stable at version 1, and open for implementation without permission or fee.