

ACME Persistent DNS Challenge

draft-ietf-acme-dns-persist-01

Shiloh Heurich (Fastly)

Henry Birge-Lee (Crosslayer Labs)

Michael Slaughter (Amazon Trust Services)

IETF 125 ACME WG — Shenzhen

Since IETF 124 (Montreal)

Merged

- **PR #35 — accounturi decoupled from challenge object** — DNS record is self-contained; enables pre-provisioning and JIT validation; many-to-one URI model for privacy
- **PR #36 — Case-handling rules** explicit for all parameters
- **PR #41 — Renamed** "Authorization Domain Name" → "Validation Domain Name" (BR term conflict)

Implementation & Status

- **Pebble** testing CA — dns-persist-01 **merged**; **lego** client — **merged**
- **cert-manager** — **community feature request** open; **author prototype**
- -01 publication pending editorial fixes; four open issues on today's agenda

Subdomain Validation Gap (Issue #33)

The problem

Client has a record at `_validation-persist.example.com` with `policy=wildcard`

Wants a cert for `server.dept.example.com`

`policy=wildcard` authorizes subdomains, but the CA **does not know which level the client intended**

Validation Domain Name lookup

```
_validation-persist
  .server.dept.example.com
  └─ query: nothing found      x

_validation-persist.dept.example.com
  └─ query: nothing found      x

_validation-persist.example.com
  └─ record: policy=wildcard   ✓
```

Proposal: New `adn` response field directs the CA to the ancestor record.

Proposed: `adn` Response Field

RFC 8555 §7.5.1 extension point — future specs may define additional response fields

```
POST /chall/PAniVnsZcis/dns-persist-01 → payload: { "adn": "example.com" }
```

- CA confirms `example.com` is a valid Authorization Domain Name for `server.dept.example.com`
- CA looks up `_validation-persist.example.com` → finds `policy=wildcard` → validates

Open questions:

1. **Depth limits:** Restrict label pruning? (*BRs allow pruning to base domain*)
2. **Scope:** Same draft, targeting -02?

TTL as Validation Ceiling (Issue #42)

Ceiling	Controlled by	Proposal
CA Validation Reuse Period	BRs / root programs	✓ Keep
<code>persistUntil</code> timestamp	Domain owner (explicit)	✓ Keep
DNS TXT Record TTL	DNS cache config	✗ Remove

Why remove?

- **Layer confusion** — TTL governs DNS caching, not CA policy; resolvers return *remaining* cache time, not authoritative TTL
- **Already bypassed** — Let's Encrypt already caps TTL to 1 min
- **Operational breakage** — default TTLs of 30–60s silently block issuance
- **Author correction** — We wrote this MUST; mailing list analysis changed our position

Proposal: Remove TTL ceiling (currently a §9.5 MUST) in -02.

IP Validation via Reverse DNS (Issue #32)

Context

- **Proposed new scope** — not yet in draft text
- CA/BF ballot SC-91 **passed** (Nov 2025) — new BR DCV method based on dns-persist for IP addresses via `in-addr.arpa` / `ip6.arpa`
- Uses `_ip-validation-persist` label (distinct from `_validation-persist`)
- Same mechanism, different validation target and IANA registration
- **Google Trust Services** supports same-draft approach

Question: Same draft or companion document?

Option	Pro	Con
Same draft	Less overhead, same mechanism	WGLC blocked if IP text not ready
Companion	Independent timeline, cleaner IANA	Extra coordination overhead

Quick Items

Client-Side `persistUntil` Check (Issue #38)

- Should clients check `persistUntil` before responding to a challenge?
- **Concern:** Split-horizon DNS — enterprise clients may not see the record
- *Trade-off: early detection of stale records vs. silent failure behind split-horizon DNS*

Error Types (Issue #39)

- Deferred until `adn` failure modes are understood

Path Forward

Priorities for -02

1. Resolve TTL question — remove or keep ceiling (#42)
2. Spec `adn` field for subdomain validation (#33)
3. Decide IP validation scope — same draft or companion (#32)
4. Editorial cleanup from review findings

Timeline

- **-01:** Editorial fixes → **-02:** Subdomain + TTL
- **WGLC** at -02; slips to -03 if IP validation is same-draft

Implementation

- **Pebble** testing CA — merged; **lego** client — merged
- **Let's Encrypt** — **implementing**; **Fastly** — committed; **ATS** — assessing

Questions & Discussion

Thank you!

Contact:

- Mailing list: acme@ietf.org
- GitHub: <https://github.com/ietf-wg-acme/draft-ietf-acme-dns-persist>
- Draft: <https://datatracker.ietf.org/doc/draft-ietf-acme-dns-persist/>