ACME Persistent DNS Challenge Update

draft-ietf-acme-dns-persist-00

Shiloh Heurich (Fastly)
Henry Birge-Lee (Crosslayer Labs)
Michael Slaughter (Amazon Trust Services)

IETF ACME WG - Montreal

Status Update

WG adopted October 16, 2025

`draft-sheurich-acme-dns-persist` → `draft-ietf-acme-dns-persist`

Industry Progress:

- **Oct 9:** CA/BF SC088v3 **PASSED** (26 CAs YES, 3 consumers YES)
- **Nov 8:** IP Rights Review completed

Implementation Commitments:

- **2026:** Fastly/Certainly, Let's Encrypt
- **Assessing:** Amazon Trust Services

Proof of Concept: pebble server, eggsampler client

- Interoperates with regular and wildcard issuance

How dns-persist-01 Works

Record Format

```
_validation-persist.example.com. IN TXT
  "ca.example; accounturi=https://ca.example/acct/123"
```

Key Features

✓ **Persistent** - Reuses across certificates

✓ **Account-bound** - Uses `accounturi` parameter

✓ **CA-specific** - Contains issuer domain name

✓ **Multi-CA** - Supports multiple issuers

✓ **Expiration** - Optional `persistUntil` timestamp

✓ **Scope** - `policy=wildcard` covers subdomains

Why We Need This

Current Challenges

http-01/tls-alpn-01

- Requires ports 80/443
- Geo-blocking prevents validation
- Cannot validate wildcards

dns-01

- DNS propagation delays validation
- Server-stored API keys risk compromise
- Complex automation

dns-account-01

- Account-scoped labels
- Handles multi-region needs
- Requires per-validation provisioning

Current Workarounds

"Magic CNAMEs" (acme-dns.io)

- Single point of failure
- Vulnerable to DNS cache poisoning
- Vulnerable to BGP hijacking

Why Standardize?

CAs could check persistent DNS records outside ACME, but this bypasses the protocol's challenge negotiation where clients choose validation methods.

Standardization ensures proper protocol integration.

Key insight: ACME account URIs provide durable cryptographic binding

Design Principles

Strong Account Binding

- **ACME accounturi**: Durable identity
- Prevents unauthorized use via DNS alone
- Survives account key rotation
- Requires no new trust anchors

Multi-CA Architecture

- **Per-issuer TXT records**
- Each CA validates its own records
- Requires no CA coordination
- Domain owners control authorization

Flexibility & Extensibility

- **Optional parameters:**
  - `persistUntil` - sets expiration
  - `policy=wildcard` - enables subdomains
- **Ignores unknown parameters**
- Enables future extensions

Security Constraints

- **MUST respect DNS TTL**
- CA policy limits apply
- DNSSEC validation recommended

Active WG Discussions

Security Trade-offs

- Freshness vs. operational simplicity
- Account key becomes long-lived credential
- **Key compromise:** Enables issuance without DNS access
- **Privacy:** `accounturi` exposed in public DNS

Validation Reuse Period

Effective period = shortest of:

- DNS record TTL (mandatory)
- `persistUntil` parameter
- CA/BF policy (398d → 10d by 2029)

DNSSEC Validation

- **Draft:** SHOULD validate signatures
- **Alternative:** MUST use validating resolver
- **Trade-off:** Security vs. private PKI flexibility

Evolution to WG Draft

Changes from `draft-sheurich-acme-dns-persist-00` through WG adoption:

Just-in-Time Validation

- CA checks existing DNS records upon authorization request
- Valid record → instant "valid" status (no challenge)
- No record → normal challenge flow

Security Considerations expanded - Record risks, account binding, subdomain validation

Long TXT record guidance - Multi-string format for >255 characters

Error handling - `malformed` for syntax errors, `unauthorized` for auth failures

Document renamed - `draft-ietf-acme-dns-persist` (WG adoption)

Seeking WG Input

Acknowledging concerns: Use cases, trust relationships, validation interactions

Questions:

1. **DNSSEC requirement?**
   - Draft: SHOULD validate
   - Alternative: MUST validate
   - Which approach?
2. **Security considerations?**
   What else needs coverage?
3. **Timeline?**
   Given industry momentum
4. **AccountURI flexibility?** (PR #30)
   Allow multiple URIs per account?
   - **Pro:** Privacy, access control
   - **Con:** Unpredictable client choice
   - Trade-off: Privacy vs. simplicity

Path Forward

- Incorporate Montreal feedback
- Expand security considerations
- Resolve PR #30 (accounturi flexibility)
- Address use case and trust concerns
- Target WGLC after 1-2 revisions
- Coordinate with CA/Browser Forum

Feedback → Revision → WGLC → RFC

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/