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`

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

How dns-persist-01 Works

Record Format

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

Key Features

✓ **Persistent** - Reuse for multiple certificates

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

✓ **CA-specific** - Issuer domain name

✓ **Multi-CA** - Separate TXT records per issuer

✓ **Expiration** - Optional `persistUntil`

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

Why We Need This

Current Challenges

http-01/tls-alpn-01

- Port 80/443 required
- Geo-blocking blocks validation
- Wildcards unsupported

dns-01

- DNS propagation delays
- API keys on servers risk compromise
- Automation complexity

dns-account-01 (draft-ietf-acme-dns-account-challenge)

Current Workarounds

"Magic CNAMEs" (acme-dns.io)

- Single point of failure
- DNS cache poisoning risk
- BGP hijacking vulnerability

Why Standardize?

CAs could deploy via pre-validation without protocol changes, but this bypasses ACME's challenge selection.

Standardization enables proper protocol integration.

Key insight: ACME account URIs provide durable, cryptographic binding

Implementation Support

Timeline:

- **Oct 9:** CA/BF SC088v3 **PASSED** (26 CAs YES, 3 consumers YES)
- **Oct 9 - Nov 8:** IP Rights Review Period
- **Oct 16:** IETF WG adoption
- **2026:** Let's Encrypt implementation

Status

Committed: Let's Encrypt (2026)

Expected: Fastly/Certainly, Amazon Trust Services

Proof of Concept: Pebble server fork, eggsampler client fork

Active WG Discussions

Security Trade-offs

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

DNSSEC Validation

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

Validation Reuse Period

How long CA relies on one DNS check

Effective period = shortest of:

- DNS record TTL (MUST respect)
- `persistUntil` parameter
- CA policy (398 days → 10 days by 2029)

Changes in -00

✓ **Pre-validation optimization**

- CA checks existing records during order creation
- Authorization becomes "valid" immediately if found
- Skips challenge flow with persistent record

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

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

✓ **Error handling** - `malformed` for syntax, `unauthorized` for auth failures

✓ **Document renamed** - `draft-ietf-acme-dns-persist`

Seeking WG Input (1/2)

Acknowledging concerns: Use case definition, trust relationships, existing validation interactions

Questions:

1. **DNSSEC requirement?**
   - Draft: SHOULD validate
   - Alternative: MUST validate
   - Which level?
2. **Protocol validation caps?**
   Beyond `persistUntil`
3. **Security considerations?**
   What else to address?

Seeking WG Input (2/2)

4. **Timeline?**
   Given industry momentum

5. **AccountURI flexibility?** (PR #30)
   Multiple URIs per account?

   - **Pro:** Privacy, access control
   - **Con:** CA cannot predict client's 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/