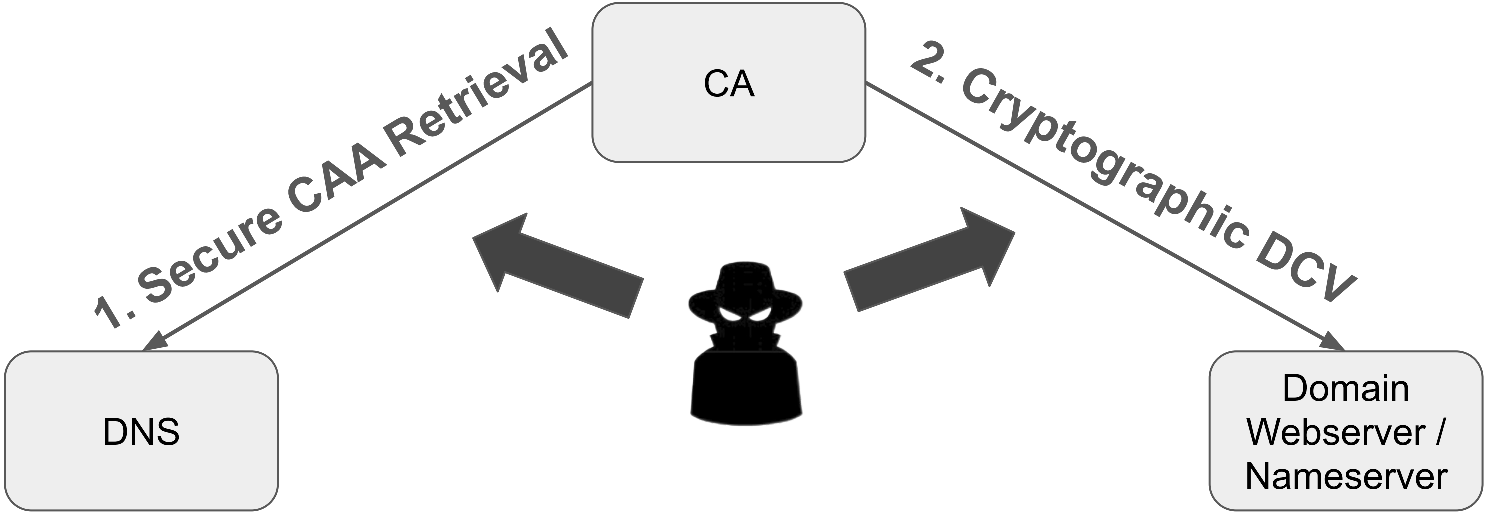
draft-ietf-lamps-caa-security Progress

IETF 124, November 2025

Henry Birge-Lee	Princeton University
Grace Cimaszewski	Princeton University
Cyrill Krähenbühl	Princeton University
Liang Wang	Princeton University
Aaron Gable	ISRG
Prateek Mittal	Princeton University

Draft Overview

The draft introduces a new “security” CAA tag that mandates CA to perform a **cryptographic domain control validation** that is resilient against network adversaries



1. Secure CAA Retrieval is Feasible

Downgrade protection is enabled by setting the critical flag in security CAA tags and retrieving CAA records securely via:

- DNSSEC:
  - Mandated by the CA/Browser Forum starting from March 2026
- Secure channels to authoritative nameservers:
  - Ongoing deployment effort with Let’s Encrypt
  - Can secure **~50% of domains** by deploying channels to the **8 largest authoritative nameservers**
  - **No domain owner opt-in** necessary

2. Cryptographic Domain Validation Methods are Feasible

1. http-validation-over-tls (✅):
   - perform regular http-01 validation over port 443 instead of port 80 and **verify certificate validity**
2. known-account-specifier (✅):
   - ACME CAs supporting **RFC 8657** already implement most of the necessary functionality, only requires synchronization between CAA retrieval code and validation code
   - SC-088 ballot allowing DNS-persist validation may further promote use of account-uri
3. secure-dns-record-change ⏳:
   - similar to dns-01 but all **DNS records are retrieved securely** (DNSSEC or via secure channels) with additional restrictions, e.g., no CNAME to an unprotected domain
4. private-key-control ⏳:
   - specify public key in DNS record and perform interactive challenge-response protocol to **prove private key ownership**

Next Steps

- Continue implementation efforts (OpenMPIC & Let's Encrypt)
- Add details on secure-dns-record-change and private-key-control
- Academic paper on the security tag is under peer review

- Get feedback from working group: github.com/birgelee/draft-caa-security-tag
- Other interested CAs as early adopters of security CAA tag?

Cyrill Krähenbühl
cyrill.k@princeton.edu

Additional Slides

Hybrid deployment of DNSSEC and Secure Channels:

- Channel (.) -> Channel (.com) -> Channel (example.com) ✅
- DNSSEC (.) -> DNSSEC (.com) -> Channel (example.com) ❌ (example.com NS records stored at the .com zone are not secure)
- DNSSEC (.) -> **DNSSEC + Channel (.com)** -> Channel (example.com) ✅
- DNSSEC (.) -> **DNSSEC + DELEG (.com)** -> Channel (example.com) ✅ (example.com DELEG records at the .com zone are DNSSEC-signe)