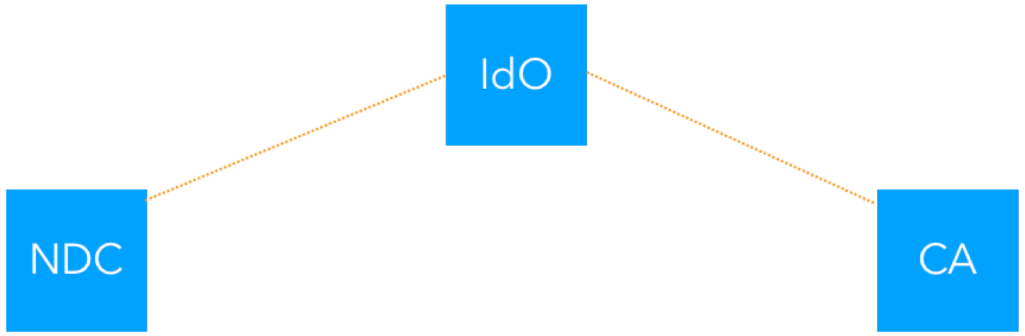
draft-ietf-acme-star-delegation

Moving forward, aligned with use cases

As a Reminder – The Goal



- IdO: Identity Owner (think Content Provider)
- NDC: Name Delegation Client (think CDN)
- CA: ...

- NDC need to terminate HTTPS using the IdO name and *really* want to avoid handover of IdO's private key between IdO and NDC
  - In CDN / CP case, the scope is DNS-based redirection, as opposed to HTTP 302 redirection or URL rewriting techniques
- STAR Request, coupled with a cert issuance protocol *equivalent* to ACME STAR, allows IdO-controlled name delegation without key sharing
- Why bother standardising it?
  - IdO and NDC typically belong to different organisations

As a Reminder – The Status

- Alignment with the main STAR draft
  - Authors focused on its final stages in the pipeline
- Discussions with documented use cases
    - STIR: draft-ietf-stir-cert-delegation
    - CDNI: draft-ietf-cdni-interfaces-https-delegation
- Understand requirements before making a new submission
  - And the draft expired (sigh)
  - But it is alive and kicking anyway

Open Questions

- Message flow
  - Looks OK to us
  - But it would be much better if it could get a pair of (pairs of) additional eyes
- Other original targets for -01
  - Composition patterns with the ACME STAR flow
  - DNS interactions (CNAMEs and other possibilities)
  - CSR validation procedures
  - The need for a CSR template
    - In the light of use case requirements

Ongoing Analysis of Use Cases

- STIR:
  - From a quick analysis of draft-ietf-stir-cert-delegation it looks like STAR-delegation might work, modulo a couple of things:
    - Abstracting DNS into a generic “naming authority”
    - Making the DNS-specific bits (CNAME mapping) optional
- CDNI
  - Modes of redirection from Content Provider to uCDN
    - HTTP 302 - looks seamless
    - DNS CNAMEs - A chain of STAR-delegation seems impractical – Authorization mechanisms under consideration
- Specific meetings on their way