CAA

Phillip Hallam-Baker

Status

- IETF Last Call
  - 1 Outstanding issue – Tree Walking
- Currently in IESG Review
  - 1 Comment, 3 Discuss
    - Descriptive...
    - IANA Registrations...
    - Wording of DNS tree walking
    - Decision on DNS tree walking

DNS Tree Walking

- Where should CA look for CAA records?
- What should the CA do if none are found?

- How many CAs are likely to be compliant?

Original Proposal

- Check x.y.z.example.com
  - x.y.z.example.com
  - example.com
  - Accept
- Why?
  - CP requires that the CA validate *only* example.com
  - Allows for exceptions to be specified if needed

Current Specification

- Check x.y.z.example.com
  - x.y.z.example.com
  - y.z.example.com
  - z.example.com
  - example.com
  - Accept

- Why?
  - Proposed in WGLC, seemed reasonable
  - Automatically supports unknown public suffixes

Proposal 1

- Check x.y.z.example.com
  - x.y.z.example.com
  - Reject

- Not acceptable
  - No public CA is going to accept a requirement that imposes a burden on every customer

Proposal 2

- Check x.y.z.example.com
  - x.y.z.example.com
  - Accept

- Cons:
  - Requires use of DNS wildcards to establish blanket policy
    - DNS wildcards <> PKIX wildcards
  - Requires CA to have access to internal side of split DNS

Conclusion

- Can we go back to my original proposal?
  - Simple