CAA Discovery Options

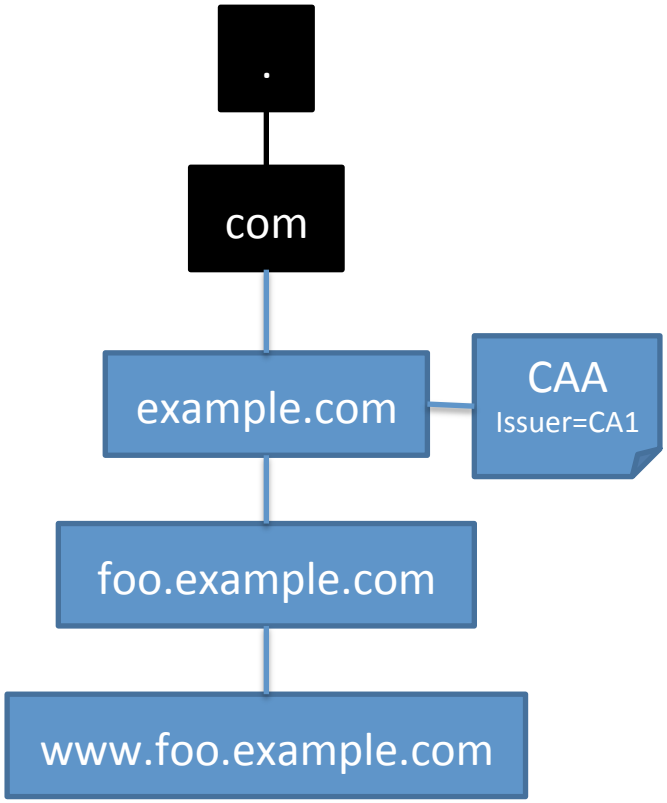
Richard Barnes

Discovery Question

- CAA “issuer” record says “the indicated issuer is allowed to issue certificates for [this name]”
- Where should an issuer look for CAA records for a given subject name?
- Equivalently, which CAA records apply to a given subject name?

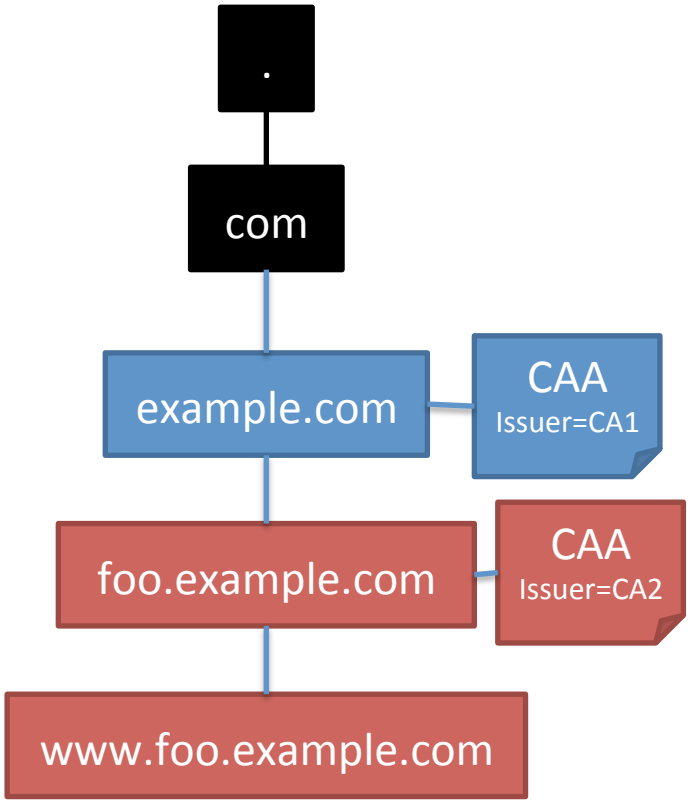
Current CAA

- CAs climb up from subject name looking for CAA
  - Use first CAA found
  - Stop at “public delegation point”
- Equivalently, authorization flows downward
  - … but not quite



Confusion

- Current document **seems** to have authorization flow downward
  - … but it stops if someone provisions CAA below
- Difficult to predict whether CAA applies to a given descendant domain

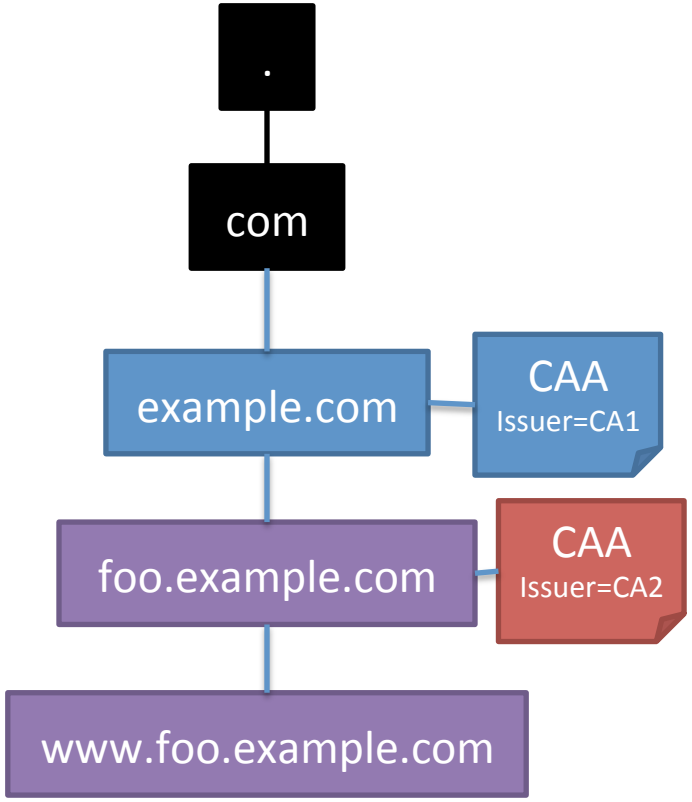


Options

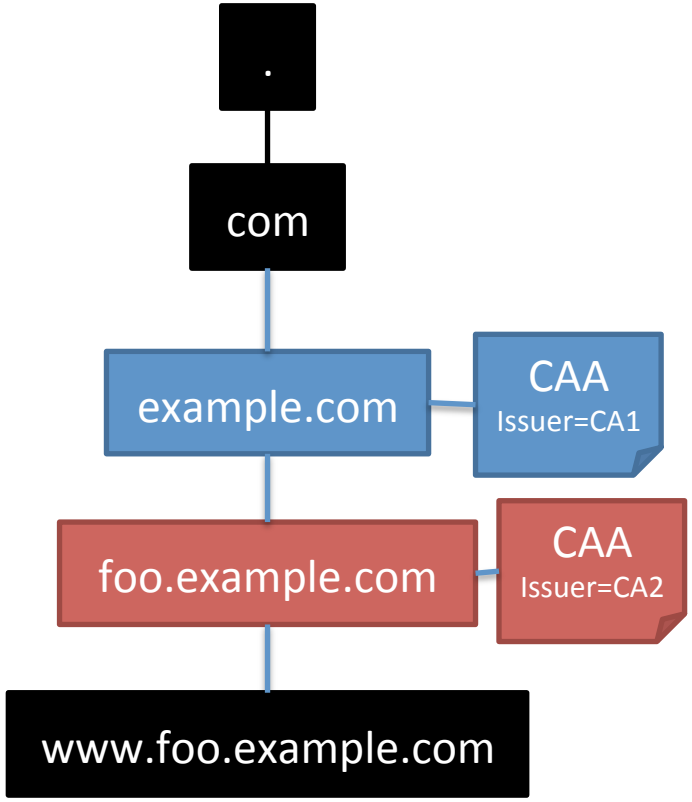
- OPTION 1: Climb all the way and union
  - Issuer is authorized if **any** ancestor domain has a CAA for that issuer
  - (Possibly stopping at a public delegation point)
- OPTION 2: No climbing
  - Just look at the name you're goint to put in the certificate

Options

Option 1: Union



Option 2: No Climbing



Wildcards

- Related question: Where do you look to authorize a wildcard cert (*.example.com)
- Options:
  - Sample names within wildcard space
  - *.example.com as QNAME
  - _star.example.com