CAA (Re)Discovery

Phillip Hallam-Baker

Comodo Group Inc.
Some DNS records are private

• [This is not up for debate]
• CAs regularly issue certificates for sites with hidden DNS entries
  • classified.example.com
  • [This is not going to change, this is not up for debate]
  • [CT does not change matters either]

• CAA addresses this requirement by tree climbing
  • classified.example.com
  • example.com
  • .com
The problem...

• CAA records are intended to be
  • A communication from the domain name holder to the CA

• DNS records are
  1. Published by domain name holders
     • (Directly or through a third party)
     • CNAME used to map a set of names onto a single target.
  2. Delegated by domain name holder to third party service providers
     • MX, SRV (for individual services)
     • CNAME (for HTTP CDNs)
(Digression) DNAME is not a DNS Record

• DNAME is a DNSSEC record
  • DNAME is a form of DNS wildcard record
  • Queries in the scope of a DNAME result in CNAMEs being synthesized

• A CAA client should:
  • Process DNAME as part of CNAME validation
    • The NSEC3 record indicates a DNAME should have been returned
    • The DNAME record indicates a CNAME should have been returned.
  • The CNAME returned is valid
  • The CNAME returned is invalid

• Process the synthesized CNAME records.
Use of CNAME is restricted

• A DNS node that contains a CNAME MUST NOT contain anything else

• This limits CAA, this is not legal:
  • web.example.com CNAME www.example.com
  • web.example.com CAA ....

• This led to the requirement that CAA clients follow CNAME
Use case

• web.example.com CNAME www.example.com
  • Administrative redirect internal

• www.example.com CNAME cdn.example.net
  • Redirect to third party
RFC 6844 algorithm

• Assumes CNAME mapping are administrative:

• Discovery path
  • web.example.com
  • www.example.com
  • `cdn.example.net`
  • `example.net`
  • `.net`
  • example.com
  • `.com`
RFC 6844 Errata 5065 (in production)

- Assumes CNAME mapping are administrative:

- Discovery path
  - web.example.com
  - www.example.com
  - cdn.example.net
  - example.com
  - .com
Possible solution: Use prefix record

- Ignore CNAMEs entirely

- Discovery path
  - web.example.com
  - _prefix.web.example.com
  - www.example.com
  - _prefix.www.example.com
  - example.com
  - _prefix.example.com
  - .com
  - _prefix.com
Remaining problem: DNAME

• No records are allowed under a DNAME

• example.net DNAME example.com
• _prefix.example.net CAA...
• example.net CAA ...
  • Allowed in RFC 2672 (DNAMEs don’t match themselves)
  • Unclear in RFC 6672

• It might be that there is no solution since DNAME does not work.