Certificate Authority Authorization

Objective: Tell Certificate Issuers who is authorized to issue

- Not just commercial CAs
  - Must support private cert issue
- Three moving parts
  - DNS Records (DNSEXT)
  - PKI Mechanism (PKIX)
  - Legal & Practices (CA-Browser Forum)
  - Would like to only move one at a time

Current Status

- Draft: draft-ietf-pkix-caa-01
  - Can be deployed now
    - example.com IN TYPE257 \# 70 0204617574683 03e3039060a2b06010401d6790203010…
  - Have implemented extensions to BIND
    - (Not too difficult)
    - Could be simpler
- Does not
  - Mention CA accountability mechanism
  - Fully back out client validation

Issue

- How to represent the Cert issuer being granted issue rights:
  - Human readability
  - Accountability
    - Can CA X tell if CA Y is operating in compliance?
  - Stability
    - Does customer need to make changes when CA changes configuration?
  - Ambiguity
    - Can a CA plausibly claim it has authorization rights?
    - Some CAs issue under brands they do not own
  - Fine Grained Control
    - Only the xxx.edu RA can issue for XXX University

Options

- Function of signing key
  - Completely unambiguous but not stable
  - Allows fine grain control
  - Can be verified
- Policy OID
  - Well defined binding to CPS
  - Allows sub-classing
  - Opaque
- Human friendly string
  - Easy to use (once extensions deployed)
  - Do we need a registry?

Proposal

- Syntax only for ‘a string’
  - Choice of string is for issuer to decide
    - CA-Browser MAY make a decision for public Cas
      - Might be an OID
      - Might be a registered string
      - Might be an unregistered string
    - Private CAs MAY chose a digest
      - Digest may be a function of the signing key/cert