CAA considerations
IETF 81, Quebec

Paul Hoffman
VPN Consortium

Two considerations

- Getting rid of relying party text (again)
- How should the CA be identified in the CAA record

CAA and relying parties (1)

- draft-ietf-pkix-caa-00 had description of how relying parties might use the CAA records
- There was a request on the list to remove discussion of relying parties
- WG co-chair: “I think it best to remove the discussion of RP use of this feature, and focus instead on how CAs are expected to use it”

CAA and relying parties (2)

- But draft-ietf-pkix-caa-01 still discusses relying parties
  - It is still defined, there is still a protocol item relating to relying parties, ...
- Proposal: really, let's actually get rid of all mention of relying parties

Identifying CAs (1)

- Current properties:
  - The CA's certificate policy OID in binary format
  - Hash of the CA's signing certificate or key
- Proposed property:
  - Free text in UTF8 to identify the CA
- Note that proposed identifier would replace the two current ones, but can hold those values as well

Identifying CAs (2)

- With the current draft, zone admins probably need to ask their current CA exactly how to fill in the DNS record
- With the proposal, a zone admin can enter what the CA tells them, or just the CA's common name, and so on
  - www.example.com CAA "1.3.6.1.4.1.35405.666.1"
  - www.example.com CAA "a8f1624810cb..."
  - www.example.com CAA "GutmannCA"

Identifying CAs (3)

- Advantages of current draft:
  - More precise
  - Less guessing when the CA checks the CAA record
- Advantages of proposal:
  - DNS admin doesn't need to contact CA before creating record
  - Less guessing about what to use because there is just one type of property

Identifying CAs (4)

- The CAA protocol should be optimized for DNS admins, not for the CAs
- The anticipated overhead for CAs is small: it's a table lookup, maybe with alerts for when they see something unexpected
- Policy OID and hash-of-cert are trivial to represent in free text
- Just make it easy to understand and use