CAA Revisited

Rick Andrews

Current State

- **BRs say:**
  - **2.2 Publication of Information**:
  - Effective as of 15 April 2015, section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state whether the CA reviews CAA Records, and if so, the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA SHALL log all actions taken, if any, consistent with its processing practice.
- At Meeting 34 (March 2015 in Cupertino), we had a short discussion about what "checking CAA" means, is it a do-not-issue flag? The RFC does not state what to do.

Previously-stated Pros and Cons

- **Pros:**
  - Relatively simple CA-only mis-issuance check
  - Can be used to enforce corporate policy
  - It's a preventative measure, check before mis-issuance, not after
- **Cons:**
  - Lack of CAA support in popular DNS servers and DNS hosting
  - It's not effective unless all CAs check
  - Doesn't allow for complex or multi-national corporate needs
  - Potential for abuse (CA insists customer must remove CAA records allowing competitors to issue, etc.)

CAs Currently Checking CAA Records

- Comodo
- Digicert
- Entrust
- Izenpe
- LetsEncrypt
- Symantec
- TrustCor
- WoSign

Support for CAA

- BIND 9.9.6 and 10.1.2
- NSD 4.0.1
- LDNS 1.6.17
- PowerDNS (under consideration, by request of LetsEncrypt)
- Neustar (managed DNS)
- Infoblox (managed DNS, in progress)
- Akamai informing customers about CAA

Current State

- Critical mass of CAs now checking CAA records
- Good support in popular DNS servers and hosts
- Walking up DNS hierarchy allows for complex or multi-national corporate needs
- Mis-issuances still possible

Next Steps

- CAA support should be required of all CAs (straw poll)
- Better define CAA process in BRs
- Address possible anti-competitive practices

Standardize CAA Exception Handling Process

- Check for CAA record at `a.b.c.example.com`, then `b.c.example.com`, then `c.example.com`, then `example.com`
  - *No record at any level*: write to audit log, proceed with issuance process
  - *Matching record at any level*: save record in audit log, proceed with issuance process, stop looking for other CAA records up the hierarchy
- Exceptions
  - *No response or error from DNS call*: write to audit log, proceed with issuance process, stop looking for other CAA records up the hierarchy
  - *Non-matching record at any level*: stop with issuance process, stop looking for other CAA records up the hierarchy. Contact customer, discuss options, write conclusion to audit log, approve or reject issuance.