Delegation of Domain Validation to the CA

Overview of Proposed Changes to 3.2.2.4.7

F2F 61 Update

Michael Slaughter
Amazon Trust Services

Background

- At F2F 59 (July 23’), the Validation Subcommittee of the Server Certificate WG presented the following conclusions on the practice of the Delegation of Domain Validation to the CA:
    - More clarity is needed around the practice
    - Applicants generally delegate the performance of many aspects of operating a website.
    - If done correctly, allowing Applicants to delegate the placement of the Random Value/ Request Token boosts agility and automation.
    - There are reasonable interpretations of the BRs that such delegation is already allowed today.

Background

- A Tiger Team was formed to threat model the practice of Delegated Domain Validation
    - The results of the threat model exercise were presented at F2F 60
- Following F2F 60, proposed ballot text was drafted and discussed within the Validation Subcommittee meetings

Overview of Changes

- New definition: **Canonical Authorization Name**
- Incorporate **Canonical Authorization Names** into section 3.2.2.4.7 (DNS Change)
- Add constraints around the usage of **Canonical Authorization Names** by CAs
  - Unique to an Applicant and not shared with multiple Applicants
  - DNS lookup results expire after 8 hours
  - CAs must not use the DNS zones for CANs for other purposes.

Open Discussion Items

- CNAME uniqueness to Applicant vs. an “Account”.
- 8 hours as a DNS query record freshness requirement
- Constraints on the usage of the CA-Operated DNS zone

Open Discussion Items

- CNAME uniqueness to Applicant vs. an “Account”.
- 8 hours as a DNS query record freshness requirement
- Constraints on the usage of the CA-Operated DNS zone

Next Steps

- Feedback is requested on the GitHub PR
    - THANK YOU for those that have already contributed!
- Resolve the remaining open issues in the ballot text
- Transition to Formal Ballot

Artifacts

- Pull Request: https://github.com/slghtr-says/servercert/pull/1/files
- Proposal Overview: https://docs.google.com/document/d/1_Shdqcj9TzMl7a_ULJ3ACJrhzYxGUB-7BVG3hv8gey4/edit?usp=sharing
- Threat Model: https://docs.google.com/document/d/1G2GYb0eg0rqE23f844J8qs7RYGU1jFVDsU5Pf7UYg3g/edit?usp=sharing