Identifying Delegated Third Parties in the context of domain validation

The domain validation process

- The vast majority of domain validation methods employed today leverage one or more network connections made over the Internet
  - The CA provides Random Value/Request Token (RVRT) to the Applicant
  - The Applicant either makes the RVRT publicly available or returns it to the CA
    - In the case where the RVRT is made publicly available, the CA performs a request to fetch the RVRT and compare it with the expected value
- The Internet infrastructure is not run by a single entity, and certainly not by a single CA
- Several entities are involved in conveying these connections
- The components operated by these entities may not always be trustworthy or reliable
  - The MPIC work is a testament to this reality

What the BRs say

- The BRs prohibit the use of Delegated Third Parties for performing domain validation

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

“With the exception of Section 3.2.2.4 and Section 3.2.2.5, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.”

So, a few questions…

- Is the CA's Internet Service Provider (which provides Internet connectivity for the CA) a DTP?
- Are the operators of routing infrastructure along the network path to the Applicant considered a DTP?
- Is the Applicant itself (who operates their own network infrastructure) considered a DTP?
- Is the publisher of software or operating systems installed on CA validation systems considered a DTP?
- Is the manufacturer of CA server hardware considered a DTP?
- If interaction of the CA with any of these entities is audited but not necessarily the operation of these components, are they no longer DTPs?

Goal-setting

- The CA should use a reliable, compliant, and auditable process to perform validations
- The risk introduced by the use of components provided by external entities should be minimized
- The risk introduced by the CA replicating components outside of its core responsibilities should be minimized

Are any of these not goals, or are there any that were missed?

Process for improving clarity in domain validation methods

1. Identify methods we want to evaluate
2. Prioritize methods for evaluation
3. For each method:
    1. Identify external components that can be potentially used
    2. Identify potential risks introduced by the use of this external component
    3. Establish guardrails or restrict the use of external components
    4. Codify changes in the BR text