A historical look at Delegated Third Parties

DISCLAIMER

- I have been in this industry for less than a decade
- I was not in this industry when these initial events transpired or these topics were discussed during writing v1.1 of the BRs (what happened to v1.0, anyway?)
- Please correct me if I'm wrong about anything (or everything)

The problem

- A reseller for a major CA was compromised
  - https://groups.google.com/g/mozilla.dev.security.policy/c/bDOrEipMt2M/m/MxASBGayo6oJ
- The reseller functioned as a RA, including domain validation
- The compromise of reseller systems allowed the issuance of fraudulent certificates

- This event was around the timeframe of DigiNotar and other notable attacks

The “solution”

- It was proposed that the initial version of the BRs was supposed to allow delegation of all activities, except for domain validation
- This didn’t make it to the published version
- Instead, there were contractual and audit requirements established for any delegated function

The solution

- With Ballot 204, the practice of delegating domain validation was finally banned in the BRs
  - However, there was some problematic language that was present until Ballot 215 passed: https://cabforum.org/2017/10/04/ballot-215-fix-ballot-190-errata/

The thinking behind the solution

- The discussion during the development of Ballot 204 as captured on the mailing list archive provides the thinking behind the current wording:
  - Discussion at F2F 40: https://cabforum.org/2017/03/22/minutes-of-the-f2f-40-meeting-in-research-triangle-park-north-carolina-21-23-march-2017/#mozilla-proposal-forbidding-delegation-of-validation-to-third-parties
  - https://lists.cabforum.org/pipermail/public/2017-March/041879.html

From these discussions, it is clear that the intent of the ballot was not to prohibit the use of any third-party service, but rather prohibit a CA from "delegating away" the responsibility for correct performance of domain validation

Some doubts on the thinking behind the solution

- Or maybe the use of third party services is a DTP?
  - https://lists.cabforum.org/pipermail/public/2017-May/027300.html
  - https://lists.cabforum.org/pipermail/public/2017-April/026842.html

Since Ballot 204…

- A few CAs have had incidents for using third party services
  - At least one CA has explained that the use of such a service was within scope, thus compliant
    - This is in alignment with Peter Bowen’s email about the CA taking responsibility for the process

A few observations and questions

- The original motivation for the prohibition on DTP was to prohibit making external entities responsible for DCV
- Some external services (which ones?) are compliant to use if the use of such services are under audit scope
- There is quite a bit of uncertainty on where the line is
  - Do contracts need to be in place between the CA and the service provider?
  - What services are compliant to use, and which ones are not?
  - What concrete security benefit does establishing the line achieve?