Updates on draft-wang-ppm-dap-taskprov

IETF 120 – PPM

Goal #1: task binding

- Secure execution of a DAP task requires each party to agree on the task configuration, but there is no mechanism in DAP that enforces this. E.g.:
  - Client doesn't know the `min_batch_size` enforced by the Aggregators
  - Client and Aggregators may disagree on the VDAF config
- This draft specifies a ***report extension*** that, if present, prompts the Aggregator to check that the `task_id == H(task_confdig)` and reject the report if not
  - Specifies an encoding of the task configuration, including DP parameters (currently not used)
  - Binds task parameters to execution: successful execution implies agreement on the parameters

Goal #2: in-band task provisioning

- DAP assumes tasks are provisioned out-of-band
- Specifies a mechanism for advertising new tasks ***in-band***, via an HTTP header
  - Adds ***opt-in*** phase to request handling:
    - Parse task config from HTTP header
    - Check if we've already opted in: if so, then continue; otherwise:
      - Check if the parameters are supported (`min_batch_size` is sufficiently large, VDAF is supported, etc.). If so, then opt in and continue; otherwise, abort the request.
  - Built on top of task binding extension
    - Re-uses task config encoding
    - Task ID is computed from task config

Changes since IETF 118

- Various changes to `TaskConfig` definition (make unrecognized variants decodable)
- Feedback from 118:
  - #54: Make the task provisioning mechanism optional (the extension is now only about task binding)
  - #47: Task provisioning: don't require advertising the task in every upload request
  - #48: Acknowledge risk of the Author fingerprinting the client and discuss limitations of this attack

Ready for adoption?

- Not much more work to do with the draft
- Open issues:
  - Error handling: #29, #34
  - More task parameters: #62
  - More domain separation: #64