Distributed Aggregation Protocol WGLC updates

Tim Geoghegan - PPM interim

December 1, 2025

Recent activity in DAP

- September 16: PPM chairs issue WGLC for DAP
- September 22: HTTPDIR provides review of DAP
- DAP editors make 8 PRs addressing 15 issues
- Highlights:
  - VDAF "preparation" becomes "verification" (matching VDAF change)
  - Consolidate media types into a single `application/ppm-dap;message=whatever`
    - Only wire breaking change
  - Various editorial improvements
- Thanks to Darrel Miller and Martin Thomson for thoughtful reviews!

VDAF changes

- VDAF is pretty much done
- Headline news in draft-irtf-cfrg-vdaf-17: Armando Faz's Rhizomes paper
- Significant performance improvement
- Presentations from CFRG @ IETF 124:
  - VDAF update (Chris Patton)
  - Rhizomes (Armando Faz)

What's left?

- 3 open issues
- Update references to other documents
- IANA registry chores
- VDAF is also pretty much done
  - Hopefully RGLC
  - Potentially going for another round of crypto panel review

Working Group Last Call

- WGLC announced September 16
- Was meant to end October 7
- What do we do now?