draft-ietf-pquip-hybrid-signature-spectrums

N. Bindel, B. Hale, D. Connolly, F. Driscoll

Reminder: Context and Timeline

- Draft covers design and security trade-offs among hybrid signature approaches.
  - May 2024 – Draft adopted by working group
  - October 2024 – WGLC -> Lots of helpful comments
  - January 2025 – WGLC completed
  - March-May 2025 – AD review -> Lots more helpful comments
  - June 2025 – Final version of draft updated
  - July 2025 – IETF and no further comments?

v06 -> v07 (following IESG review)

- Added clarification of relationship between artifacts and non-separability.
- Added information about the importance of configuration (“policy”).
- Generalising the need-for-approval spectrum (blackbox options)
- Simplifying some sections to avoid confusion e.g., removing references to SUF-CMA and different types of backwards compatibility.
- Lots of tidying up!

Let’s ship it!

- Addressed all comments at IESG review of v06. Published v07.
- No comments on return to WG.