draft-irtf-cfrg-eddsa-00

Status

- -00 submitted
  - Copy of draft-josefsson-eddsa-ed25519
  - Generalized EdDSA description added from http://ed25519.cr.yp.to/eddsa-20150704.pdf
  - Adds Ed448 and Ed448ph
  - Refers to cfrg-curves draft for curve details

Status

- Ed25519 and Ed25519ph appear done (i.e., no outstanding open issues or suggestions)
  need test vectors for Ed25519ph

- Hash choice for Ed448 pending
- Some review/editorial work needed
  - Sync with cfrg-curves
  - Review security considerations

Ed448 hash options

- Plenty onlist discussion
- Several people voiced support for aligning Ed448 with SHA3
- Can we pick SHAKE256 for KDF and SHA3-512 for prehash and move on?
  - Some support for SHAKE256 as prehash but SHAKE256 is defined as a XOF not hash
- If no agreement here, suggested process forward:
  - Have one week of call for Ed448 hash proposals
  - Have one week of poll for each alternative