Introduction to Pairing Friendly Curves Representation in JOSE and COSE Draft

Kyle Den Hartog (MATTR)

https://datatracker.ietf.org/doc/draft-denhartog-pairing-curves-jose-cose/

Why did we author this?

- Currently working in the Decentralized Identity space where my company (MATTR) has authored a method to sign Verifiable Credentials (or any arbitrary message) with BBS+ signatures
- We'd like to be able to represent the curve of our choice (BLS12-381) in JWK/CWK format inside of DID Documents
- We see benefits to pairing friendly curves and signature formats that rely on this elliptic curve property quite useful in the future for things like threshold signatures and attribute-based credential signatures

What's in the draft currently?

- Currently this draft builds upon draft-irtf-cfrg-pairing-friendly-curves-09[1]
- Includes all curves defined in 4.2 (128-bit security) and 4.3 (256-bit security)
  - Bn256G1 and Bn256G2 in JOSE and COSE representations (prohibited)
  - Bn462G1 and Bn462G2 in JOSE and COSE representations (optional)
  - Bls12381G1 and Bls12381G2 in JOSE and COSE representations (optional)
  - Bls48581G1 and Bls48581G2 in JOSE and COSE representations (optional)

Points to be considered

- What's the most pragmatic way to encode these keys? Need to remain aligned to JWK/CWK formatting.
  - Need to further consider impact for alignment with other use cases where these curves are already in use
- Should a signature format be co-registered to make use of the key formats within the JOSE/COSE suites right away?
- How should subgroups (G1/G2) be represented?
  - Would it be better to use the "crv" parameter or some other method?
- What would be the best path forward for this draft to get these registered in the JOSE/COSE IANA registries?
- Should Bn256G1 and Bn256G2 be registered but prohibited status?

Questions?

- Places I watch for discussion on the topic
  - This meeting (time permitting)
  - COSE WG Mailing list
  - Issues in github repo: https://github.com/mattrglobal/bls12381-jwk-draft
  - My email: kyle.denhartog@mattr.global