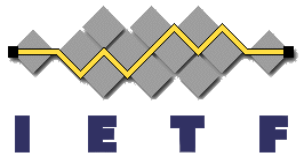
Barreto-Lynn-Scott Elliptic Curve Key Representations for JOSE and COSE



draft-looker-cose-bls-key-representations

Tobias Looker & Mike Jones

IETF 113, Vienna

March 21, 2022

Context

- Barreto-Lynn-Scott (BLS) elliptic curves belong to the pairing-friendly curves branch of cryptography.
- Related work is under way at the CFRG (https://www.ietf.org/archive/id/draft-irtf-cfrg-pairing-friendly-curves-10.html).
- In reference to pairing friendly curves, the BLS family is regarded by many as the most secure and efficient curves available for pairing-based operations.
- This draft registers identifiers for BLS-based cryptographic keys in both JWK and COSE_Key formats.

Why

- There are numerous applications for pairing-based cryptography, however the most relevant and recent work includes:
  - BLS Signatures (https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-bls-signature-04) - Aggregate signature scheme used by several prominent DLT distributed ledger technology projects.
  - BBS Signatures (https://identity.foundation/bbs-signature/draft-bbs-signatures.html) - A zero knowledge proof enabled signature scheme capable of selective disclosure and un-linkable presentations.
- Standardizing the key representations for the BLS curves will help to support these initiatives.
- Ongoing work with JSON Web Proof (JWP) will provide the basis for JOSE-based expression of signature schemes like BBS signatures, meaning a way to express the keys in a manner consistent with JOSE (e.g., via JWK) becomes valuable.

Next Steps

- The authors request working group review of the document.
- Following addressing working group review comments, we plan to request working group adoption.