*

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

draft-ietf-cose-bls-key-representations

Tobias Looker & Mike Jones

IETF 115, London
November 8, 2022

What Does It Do?

- Defines and registers required parameters with IANA for cryptographic key representation of the Barreto-Lynn-Scott Elliptic curve family in both COSE_Key and JWK

Why Do It?

- Multiple new algorithms emerging that make use of this curve
  - BLS signatures, CFRG draft
  - The BBS signature scheme, CFRG draft – newly adopted

Status

- Simple draft primarily registering parameters
- Adopted by working group in July 2022
- Published -01 recently, which added JWK based examples
- COSE_Key examples pending