RATS WG
Epoch-Markers

Henk Birkholz <henk.birkholz@ietf.contact>

IETF120 Vancouver, 23rd July

https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/
Henk Birkholz, Thomas Fossati, Wei Pan, Carsten Bormann
Purpose (recap of some examples)

https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/

- A specification to realize the Epoch ID illustrated in RFC 9334
  - Examples applications include:
    - Recentness and freshness proofs
    - "Multi-Party-Nonce" that is not only used once and or not used in a challenge-response interactions only
- Well-defined content structures, for example:
  - RFC3161 payload TimeStampToken
  - COSE-signed CBOR time-tag (RFC-to-be 9581)
WG Adoption Call

https://datatracker.ietf.org/doc/minutes-118-rats-202311080830/
https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/

• **IETF 118**
  o Nancy: "to help Henk reach out to COSE for review and assessment to adopt at COSE."
  o Chairs: Offered "to reach out to COSE chairs to facilitate determination of which WG this belongs in."

• **Between IETF 119 & 120** the editors reached out to COSE:
  o There is no desire to do it in COSE
  o Can we adopt now?