IETF RATS
Epoch Markers

https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/05/

IETF 117
July 26th, 2023
San Francisco, USA
Status & Next Steps

● Since Yokohama:
  ○ (partially) addressed Carl’s review
  ○ Dropped “stateless nonces” (i.e., the odd one out)
  ○ More uniform message layout

● Current open issues:
  ○ Still waiting on Informative reference to Concise Evidence
  ○ TODO: Add 'Nonce Handling Consideration' sections for Uni-Directional Remote Attestation and Streaming Remote Attestation in 
  ○ Naming is hard: Maybe we need a better name that says "like a nonce, but used by multiple entities only once"

● Request CfA
Conceptual Messages Wrappers

https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/03/
Status & Next Steps

- An encapsulation for RATS conceptual messages
  - in Background-Check models, it allows RPs to be agnostic about the format of evidence exchanged between Attester and Verifier
- Useful in different contexts
  - Attested TLS (aTLS)
  - TCG DICE
  - (potentially) key attestation formats
- Presented in Yokohama (IETF 116)
- Since Yokohama
  - Addressed Carl’s in-depth review
  - Complete implementation (https://github.com/veraison/cmw)
  - Integrated into the attested TLS prototype and interoperable RA-TLS
- Request CfA