

18 March 2026

Epoch Markers

RATS WG @ IETF 125 Shenzhen

Updates since IETF 124

- Security Considerations were significantly improved. The need was highlighted by Usama and requested by the document Shepherd (Jeremy), resulting in changes to the Security Consideration sections and throughout the document, including:
 - EM replay & ordering
 - secure channels for conveyance
 - acceptable duration window (cadence)
 - Bell (key) compromise (veracity appraisal is now out of scope)
 - Disambiguation of Epoch Marker as an implementation of the RFC9334 Epoch ID concept.
- Polished IANA Considerations

Recap of Significant Changes

- The Epoch Marker I-D now specifies an initial (and extensible) set of Epoch ID types and not a complete message structure.
- While the `em` CWT Claim is still defined for Epoch Marker types, no specific "outer structure" is introduced by the I-D (and no corresponding specific COSE usage now) anymore – based on WG feedback
 - To demonstrate how an Epoch Marker with the `tagged-epoch-id` type `cbor-time` can be used as a CBOR-based TimeStampToken (similar to RFC3161), Figure 5 in Appendix A now illustrates an example how that is accomplished
 - Question to the WG: Is a dedicated "protocol I-D" required as a complement for specific challenge-response Epoch Marker ("TST") retrieval or is that clear enough?

Review Status

- Thanks to Jeremy (Shepherd), Jun, Ionut (now a co-editor), and Carl for the extensive review feedback
- Thanks to Michael, Mike, and Diego for implementation feedback
- Jeremy recommended to request secdir and maybe IoTDir review in October 2025 (is this still the plan?)
- Jeremy recommended to *"record whether COSE review was completed and whether any COSE/CWT registrations (headers/claims) are needed"* (is this still the plan?)

"Open" Issues & Next Steps

- COSE Liaison Outcome #59
 - "Record whether COSE review was completed and whether any COSE/CWT registrations (headers/claims) are needed."
- Processing Rules #64
 - "The draft would also benefit from some processing rules, i.e., is it necessary to affirm the hardcoded hash is used, how are nonces processed, how is an epoch bell authorized (TSAs have certs with an ECU, for example), etc.?"
- Next Steps?

18 March 2026

Reference Interaction Model

RATS WG @ IETF 125 Shenzhen

Remaining WGLC Issues since IETF 124

- Addressed Michael's Shepherd review (Thank you Michael!)
- One sub-issues is maybe not sufficiently addressed:
 - "Most of the definitions are reliant on RFC 9334 and are used consistently with the descriptions in that document. A minor editorial point is that the role of Broker is used before it is explained/defined (in Section 7.3.2). As it is capitalized to indicate that it is a formal role, some minor editorial work could be useful to prevent inconsistencies in other documents."
 - Thoughts?

Remaining WGLC Issues since IETF 124

- One sub-issues is not addressed (we think):
 - "A small addition of examples of how to achieve mutual authentication in 9.4.2 would be useful. Other security considerations have suggestions of how implementers might achieve the required property, and that is the only property without a practical way of achieving it."
 - Thoughts?

Remaining WGLC Issues since IETF 124

- One sub-issues is resolved (we think):
 - "Interaction patterns for Evidence vs. Reference Values and Endorsements". Current wording:
 - "While the exact details for conveyance of other Conceptual Messages is out of scope, the models described in this document may be adapted to apply to the conveyance of other Conceptual Messages, such as Endorsements or Attestation Results, or supplemental messages, such as Epoch Markers [[I-D.ietf-rats-epoch-markers](#)] or stand-alone event logs."
 - "The same interaction models may apply to the conveyance of other Conceptual Messages (Endorsements, Reference Values, or Appraisal Policies) with other roles involved. However, that is out of scope for the present document."
 - Thoughts?