Applying COSE Signatures for YANG Data Provenance

draft-ietf-opsawg-yang-provenance

D. López, A. Pastor, A. Méndez (*Telefónica)*

A. Huang Feng (*INSA-Lyon*)

H. Birkholz (*Fraunhofer SIT*)

IETF#124, Montreal, November 2025

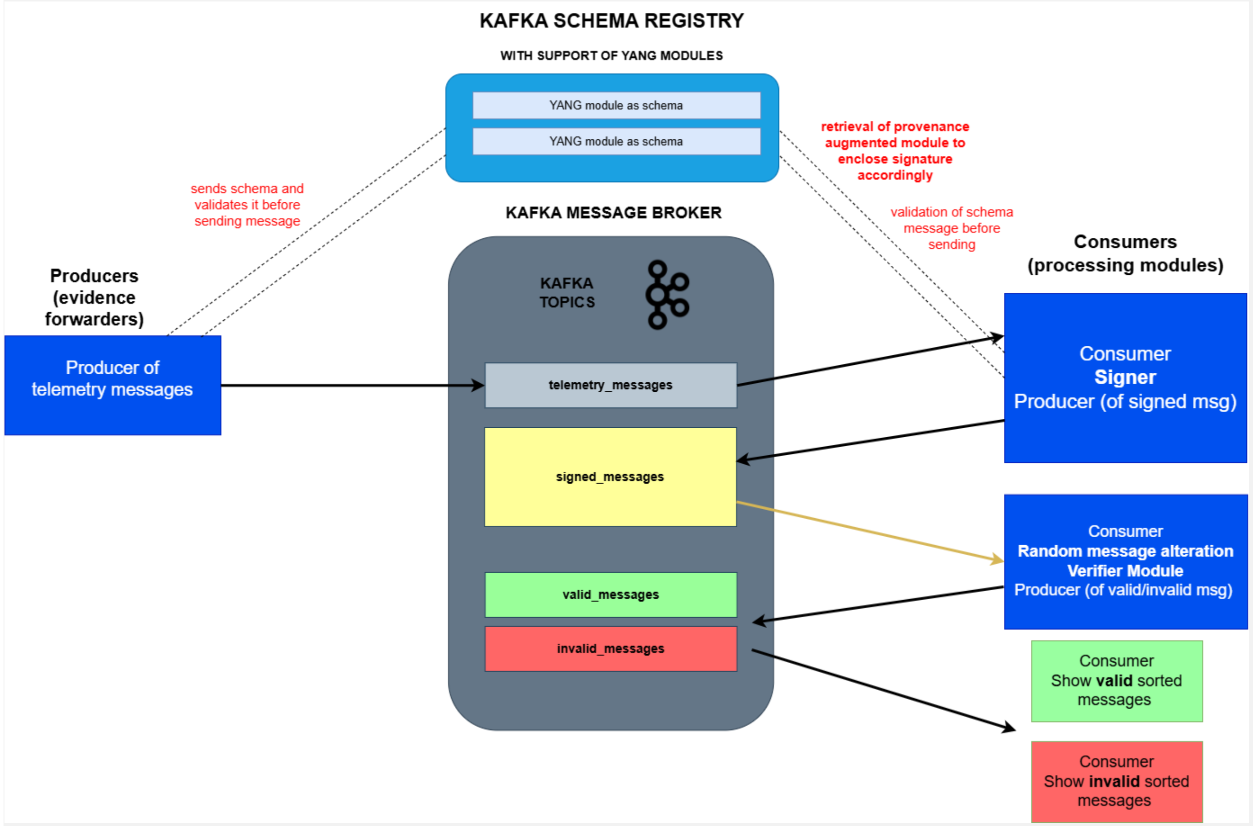
An Update on Prov·e·nance |(ə)n ˌəpˈdāt än ˈprävən(ə)ns|

- Mature YANG definition
  - Focus on YANG modules defined in the draft
  - Clarify procedures and enhance examples
  - Evolution aligned with the reference implementation
- Main changes
  - All YANG modules refined
  - Enhanced description and procedure for the first enclosing method
    - Use of a dedicated leaf in any YANG module, based on augmentation
    - The procedure now properly describes how to augment any valid module with a leaf holding provenance signatures
  - Updated examples

Aligning with the Reference Implementation

- Enhanced logic for processing signatures in EM1
- The process now
  - Accepts the YANG module containing the signature augment
    - Or any module importing the *provenance-signature* type defined in the draft
  - Automatically retrieves
    - The leaf name for the signature
    - The module name (JSON) or namespace (XML)
  - Generates the new signed element or verifies it based on these values
- Usable in any YANG processing pipeline
- And applicable to EM2 (YANG Push) and EM3 (Instance Metadata)

Reference Implementation (@Hackathon)



- Evolved reference implementation
  - Full schema-based signature processing
- Keeping the two flavors
  - Microservices, integrable with any YANG source or consumer
  - Integrated within a Kafka message broker
  - This demonstrator most focused on Kafka and YANG Push

What Comes Next

- Time for a deep YANG and security review
  - Involving the YANG Doctors and the SEC Area
- Improve the trust model
  - Address multiple signatories
  - As already requested
- Address CBOR
- Align with other related proposals
  - Addressing provenance, trust, metadata…
  - And keeping the pace with YANG Push
  - Experiment and validate within these application scenarios
- Evolve the RI as the draft evolves
  - As an essential validation and demonstration tool