

# 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*)

# News on Provenance | nōōz än 'prävən(ə)ns |

- Draft adopted
  - Two versions since adoption ([draft-ietf-opsawg-yang-provenance-01](#))
  - Most changes related to comments received in the adoption call
  - And experience with the reference implementation
- Main changes
  - Discussion on application scenarios
  - Clarification on the processing of provenance signatures
  - Explicit mention to augmentation in the explicit leaf enclosing method
  - Update of the YANG Push Notification enclosing method
  - YANG modules completed, including IANA considerations
  - Updated security considerations, with focus on the trust fabric
  - Examples in the appendix aligned with the above changes

# Introductory and Basic Issues

- Three application scenarios discussed in the introduction
  - Telemetry and monitoring data
  - Device configuration integrity
  - Network-wide service orchestration
- Explicitly associate the provenance-signature type with the processing of provenance signatures (that is...)
  - Both for generation and validation
- Describe processing rules
  - Both for generation and validation

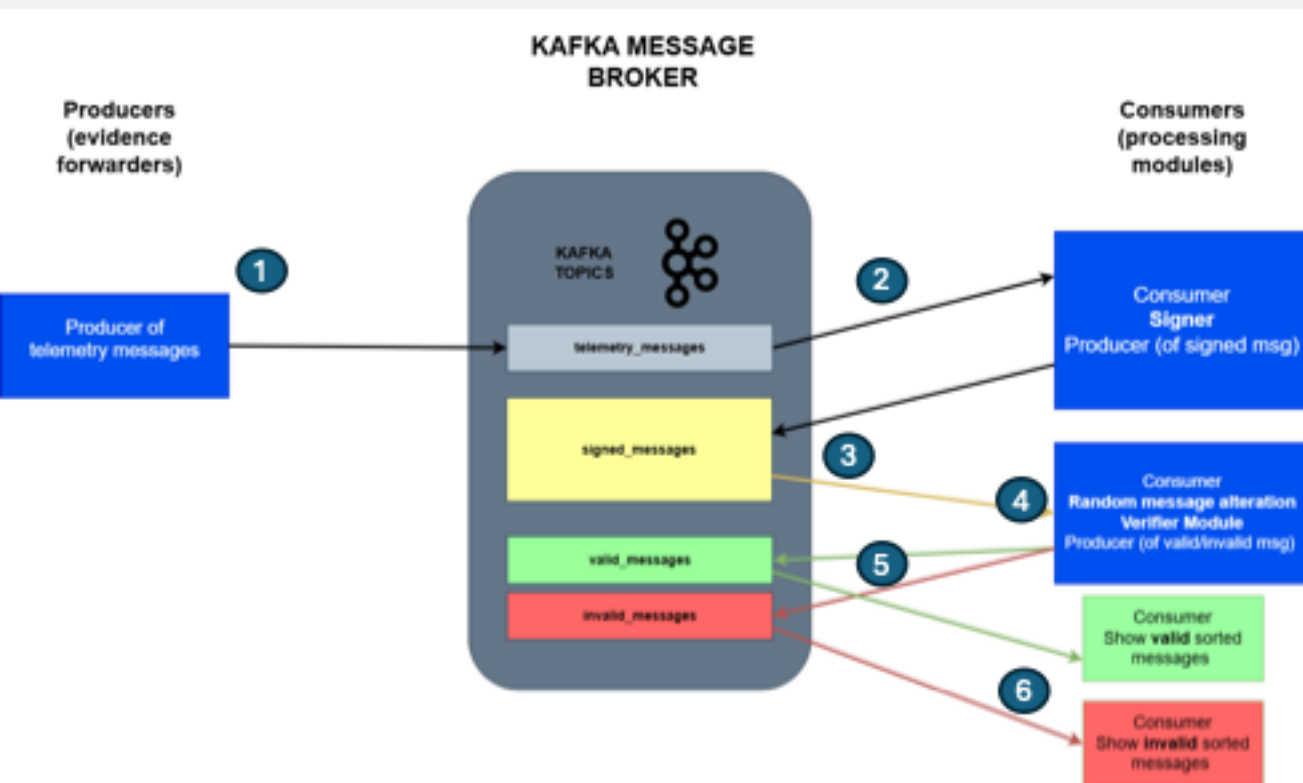
# YANG Updates

- Augmentation now explicitly mentioned for EM1
  - The one associated to a specific leaf
- EM2 (YANG Push Notification) updated
  - Following the updated schema
  - Extension of the notification envelope
  - YANG module updated accordingly
- Definition of the YANG module for EM3 (instance data)
- Update namespace for EM4 (annotations)

# (IANA and Security) Considerations

- Trust issues as part of the security considerations
  - Not in the scope of the draft
  - But certainly relevant
- Sample deployment patterns
  - Private keys at controller entities
  - Per device private keys
  - Multi-signatory issues
- IANA considerations aligned with YANG modules

# Reference Implementation (@Hackathon)



- Enhanced reference implementation
  - Aligned with the WG-adopted draft
- In two flavors
  - Microservices, integrable with any YANG source or consumer
  - Integrated within a Kafka message broker
- Aiming at convergence with current efforts on YANG Push

# What Comes Next

- Get ready for a YANG review
  - All definitions now available
  - Consistency check
- Evolve the RI addressing Kafka and YANG Push
  - Converge with current efforts
  - Foster wider adoption
- Improve the trust model
  - Address multiple signatories
  - Complete recommendations by means of the RI
- Experiment and validate all referenced application scenarios