

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)

An Update on Provenance

|(ə)n ˌɛpˈdɑːt ən ˈprɒvən(ə)ns|

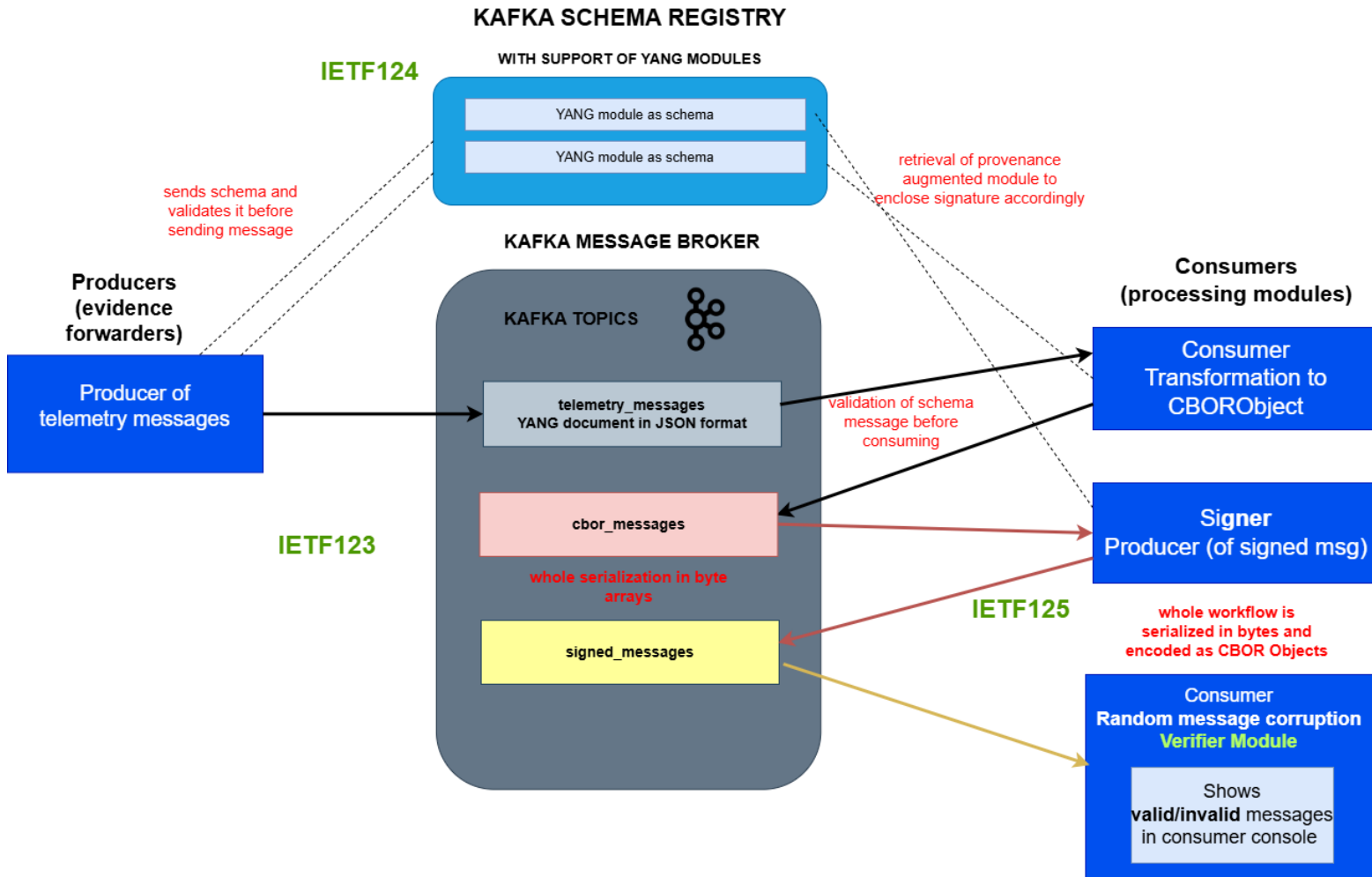
- Corrected JSON examples
 - Inclusion of the signature at the end of the document → easier approach for i) code development ii) implementation for data streaming processes
- Most important update: CBOR
 - Added proposed *.sid* file for ietf-yang-provenance YANG module
 - Added examples for all enclosing methods
 - Using CBOR diagnostic notation (partially similar to JSON)
 - Using SIDs
 - Evolution aligned with the reference implementation

Aligning with the Reference Implementation

- Adapted the whole workflow to byte[] and CBOR Object formatted data
- Canonicalization using a library which adopts RFC8949 (CBOR) with deterministic encoding
- CBOR implementation also supports YANG schema-based signature processing
- Readable representation in CBOR diagnostic notation

```
Key: key1
CBOR bytes size: 290
Decoded Original CBOR:
{"ietf-interfaces:interfaces": [{"interface": [{"name": "eth0", "type": "iana-if-type:ethernetCsmacd",
"if-index": 1, "statistics": {"discontinuity-time": "2014-07-29T13:43:12Z"}, "oper-status": "up",
"admin-status": "up"}]}, {"provenance-signature":
h'D28451A301260363786D6C04676563322E6B6579A0F658401242F4F162115E9AE59E978E0E66E4740F89585B9676A3D9489D370AC6F97
8BE7F4B139E31A62C21D3DDF1EFCE5CE870B0D2D7BAEFF1C07DE6D17B4F41889AE'}]}
Tampered CBOR applied!
CBOR to verify:
{"ietf-interfaces:interfaces": {"tampered": true, "interface": [{"name": "eth0", "type":
"iana-if-type:ethernetCsmacd", "if-index": 1, "statistics": {"discontinuity-time": "2014-07-29T13:43:12Z"},
"oper-status": "up", "admin-status": "up"}]}, {"provenance-signature":
h'D28451A301260363786D6C04676563322E6B6579A0F658401242F4F162115E9AE59E978E0E66E4740F89585B9676A3D9489D370AC6F97
8BE7F4B139E31A62C21D3DDF1EFCE5CE870B0D2D7BAEFF1C07DE6D17B4F41889AE'}]}
Signature valid? false
SIGNATURE STATUS: INVALID
Offset: 3
-----
Key: key1
CBOR bytes size: 290
Decoded Original CBOR:
{"ietf-interfaces:interfaces": [{"interface": [{"name": "eth0", "type": "iana-if-type:ethernetCsmacd",
"if-index": 1, "statistics": {"discontinuity-time": "2014-07-29T13:43:12Z"}, "oper-status": "up",
"admin-status": "up"}]}, {"provenance-signature":
h'D28451A301260363786D6C04676563322E6B6579A0F65840407E4D4CBFA1ED0C908C428B265592CD7043346F6B328858B9BC73DD97779
0C20CE9C1C7284097131276F3438589994939C6AFB0D65248EFB1DF64CD99D99A9F'}]}
Using original CBOR (no tampering)
CBOR to verify:
{"ietf-interfaces:interfaces": {"interface": [{"name": "eth0", "type": "iana-if-type:ethernetCsmacd",
"if-index": 1, "statistics": {"discontinuity-time": "2014-07-29T13:43:12Z"}, "oper-status": "up",
"admin-status": "up"}]}, {"provenance-signature":
h'D28451A301260363786D6C04676563322E6B6579A0F65840407E4D4CBFA1ED0C908C428B265592CD7043346F6B328858B9BC73DD97779
0C20CE9C1C7284097131276F3438589994939C6AFB0D65248EFB1DF64CD99D99A9F'}]}
Signature valid? true
SIGNATURE STATUS: VALID
Offset: 4
```

Hackathon



Following IETF 123 and IETF 124, we continued working on the same demo, showcasing:

1. End-to-end workflow in a Kafka message broker: data ingestion, serialization, formatting, and Signer/Verifier modules
2. YANG schema validation prior to data processing
3. Workflow operating on byte serialization and CBOR object management (binary only, no JSON)

What Comes Next

- Time for a deep YANG and security review (draft will not evolve new YANG modules)
 - Involving the YANG Doctors and the SEC Area
 - How do we request this?
- Improve the trust model
 - Address multiple signatories → Explore COSE multi-sign (now signing with COSE_Sign1)
 - As already requested
- Align with other related proposals
 - Addressing provenance, trust, metadata... → security policies, green framework draft datasheets and metric, notification envelope draft, telemetry-data
 - And keeping the pace with YANG Push → tested with Kafka with YANG Schema registry
 - Experiment and validate within these application scenarios
- Evolve the RI as the draft evolves
 - As an essential validation and demonstration tool → mainly refining methods and integrate multi-signing