Looking back to IETF122

Selected WG work or BOFs at or around IETF122
that might be of interest to T2TRG security work

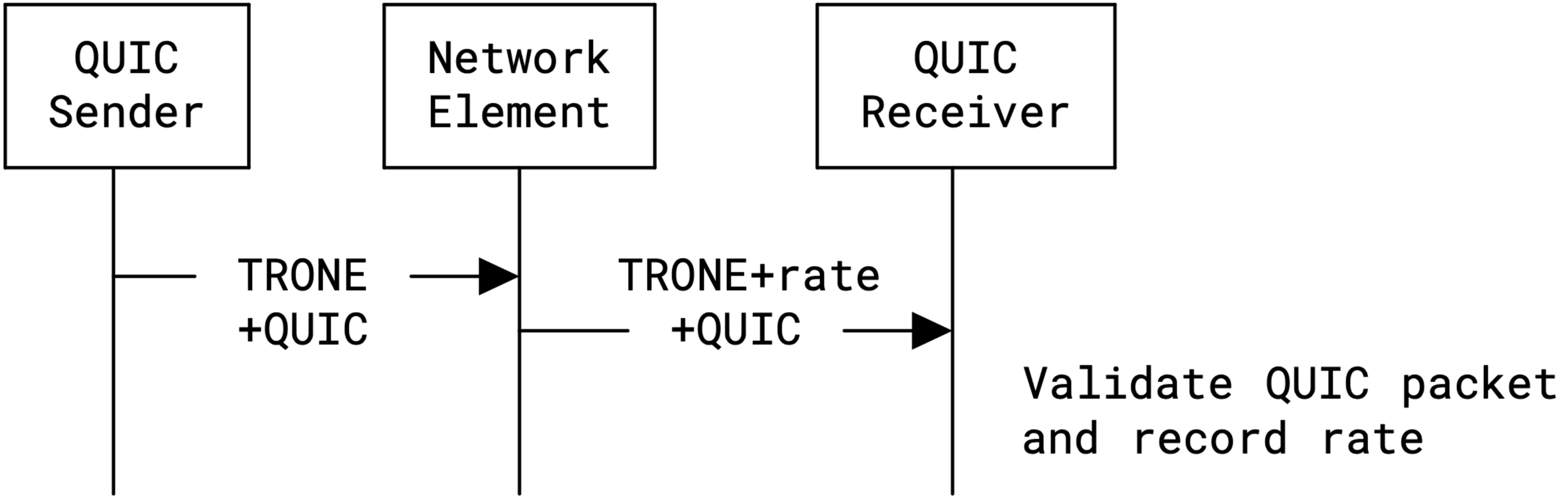
Perspective: Players, Objectives, Beliefs

SCONE: TRONE protocol

(Transparent Rate Optimization for Network Endpoints)
Players: QUIC Endpoints, Network Elements
Objective: Endpoints can ask network about rate limiting
Beliefs: Authenticated information from path to endpoint

- Source endpoint coalesces (unprotected) TRONE packet with QUIC packet(s)
- Receiving endpoint authenticates QUIC packets as from source
- Network Elements can patch rate limiting information into TRONE packet
  - must have been on-path, or it wouldn't have had the QUIC packet(s)

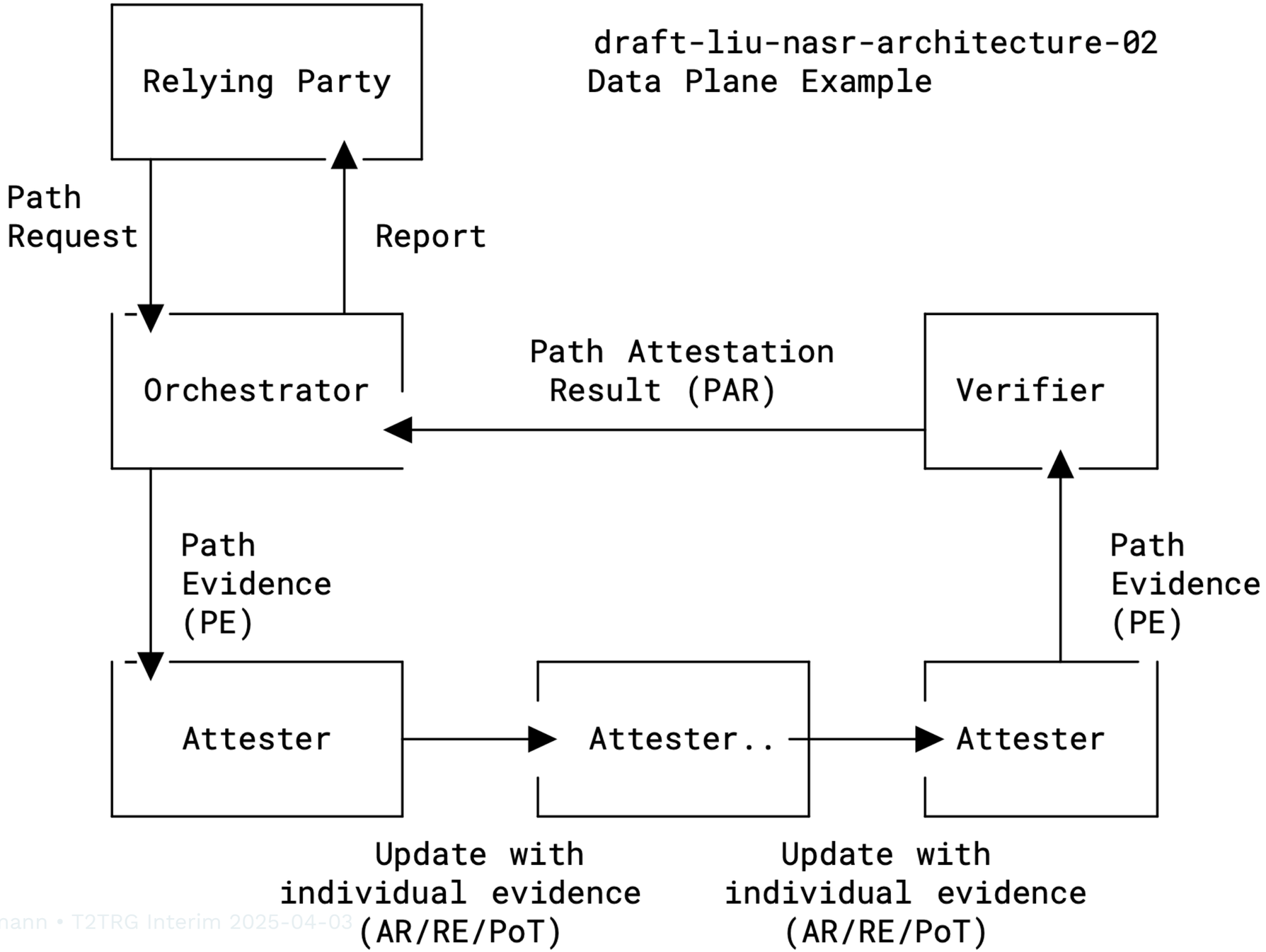
draft-thoji-scone-trone-protocol-00



NASR BOF

(Network Attestation for Secured foRwarding)
Players: Relying Party, Network Elements (Attesters), ++
Objective: Ensure that packets take "secure" path
Beliefs: Authenticated, attested status of routers

— Network Elements supply path evidence

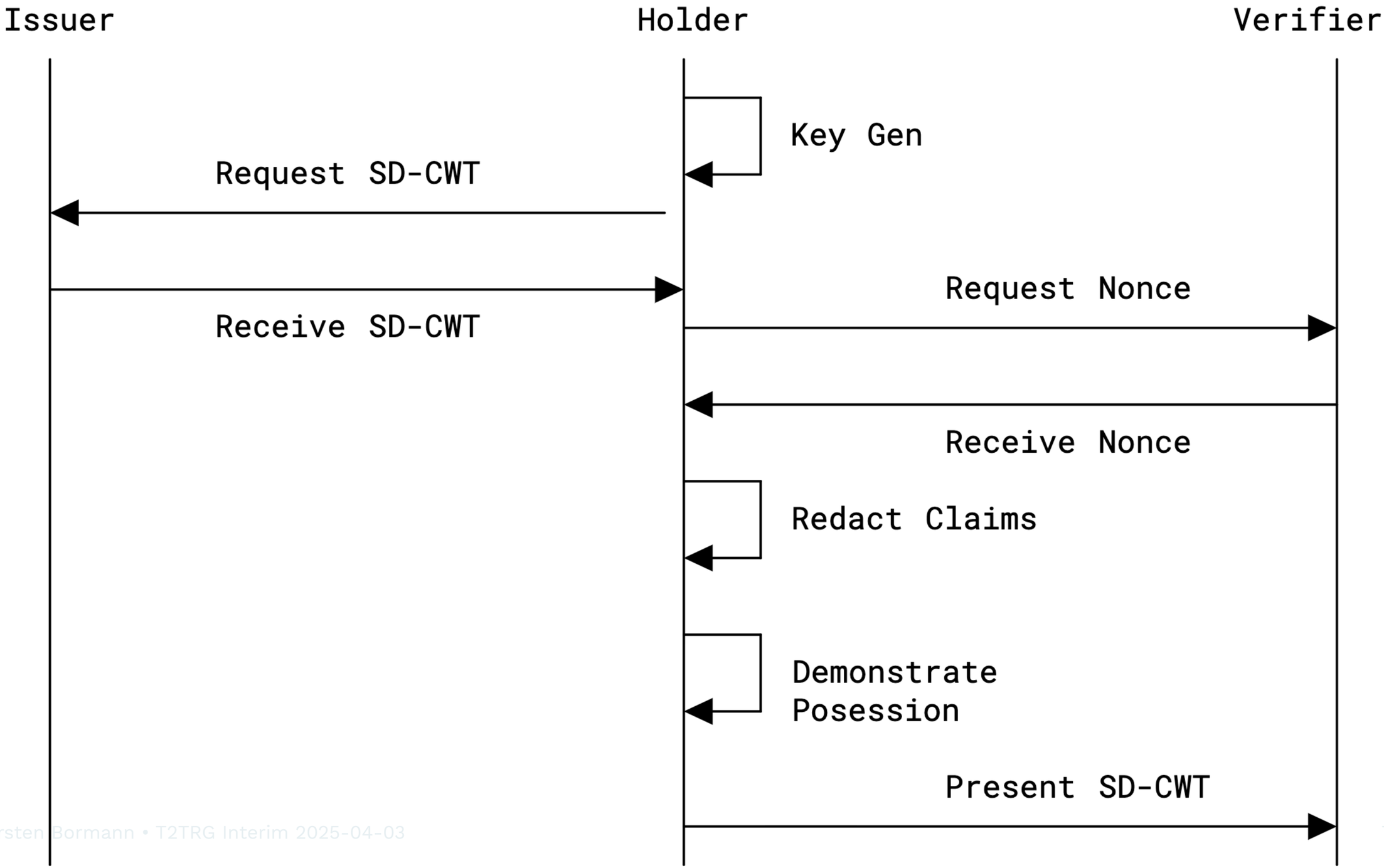

draft-liu-nasr-architecture-02
Data Plane Example
Relying Party
Path
Request
Report
Orchestrator
Path Attestation
Result (PAR)
Verifier
Path
Evidence
(PE)
Path
Evidence
(PE)
Attester
Attester..
Attester
Update with
individual evidence
(AR/RE/PoT)
Update with
individual evidence
(AR/RE/PoT)

Selective Disclosure x

Variants: SD-JWT (OAuth WG), SD-CWT (SPICE)
Based on three kinds of players:

— Issuer: signs JWT or CWT (claims), provides to holder
— Holder (Subject, Presenter): can present claims to RP
— "Verifier" (Relying Party): can verify by issuer signature

Objective: Let Holder be selective which claims it discloses


Issuer
Holder
Verifier
Key Gen
Request SD-CWT
Request Nonce
Receive SD-CWT
Receive Nonce
Redact Claims
Demonstrate
Posession
Present SD-CWT

Beliefs (JWT/CWT three-legged model):

— Holder prepares/asks for claims set,
provides a public holder confirmation key

— Issuer signs (endorses) claims set into SD-JWT/SD-CWT
binding it to Holder's confirmation key
(➔ enabling Proof of Possession)

— Verifier gives significance to ("trusts") issuer statements,
but possibly doesn't know Holder

— Holder can now build SD-KBT to authenticate to Verifier
- binding its confirmation key
- enabling use of claims set as identity

Enabling Redacting by Holder (data minimization):

- Holder can redact individual claims in signed JWT/CWT
  - Presenting only a subset of claims to Verifier
  - Verifier can still verify the Issuer's signature: redacted claims contain enough info to check

Issue:
Linkability of (possibly differently redacted) information

(Partial mitigation: single use + batch issuance of signed SD-JWT/SD-CWT from Issuer)

SCITT: Supply Chain Integrity, Transparency, and Trust

- Issuers make signed statements
- Subject (of statement): can be Entity/User/Device or an Artifact
- Clients (may be the issuers): register these with:
- Transparency Service puts these registrations into append-only log,
  - Implements Registration Policy
  - Issues Receipts
- Auditors: examine Transparency Service
- ...

Objective: Create transparency for signed statement
Beliefs: Signed Statements can be attributed to an issuer

draft-ietf-scitt-architecture-11