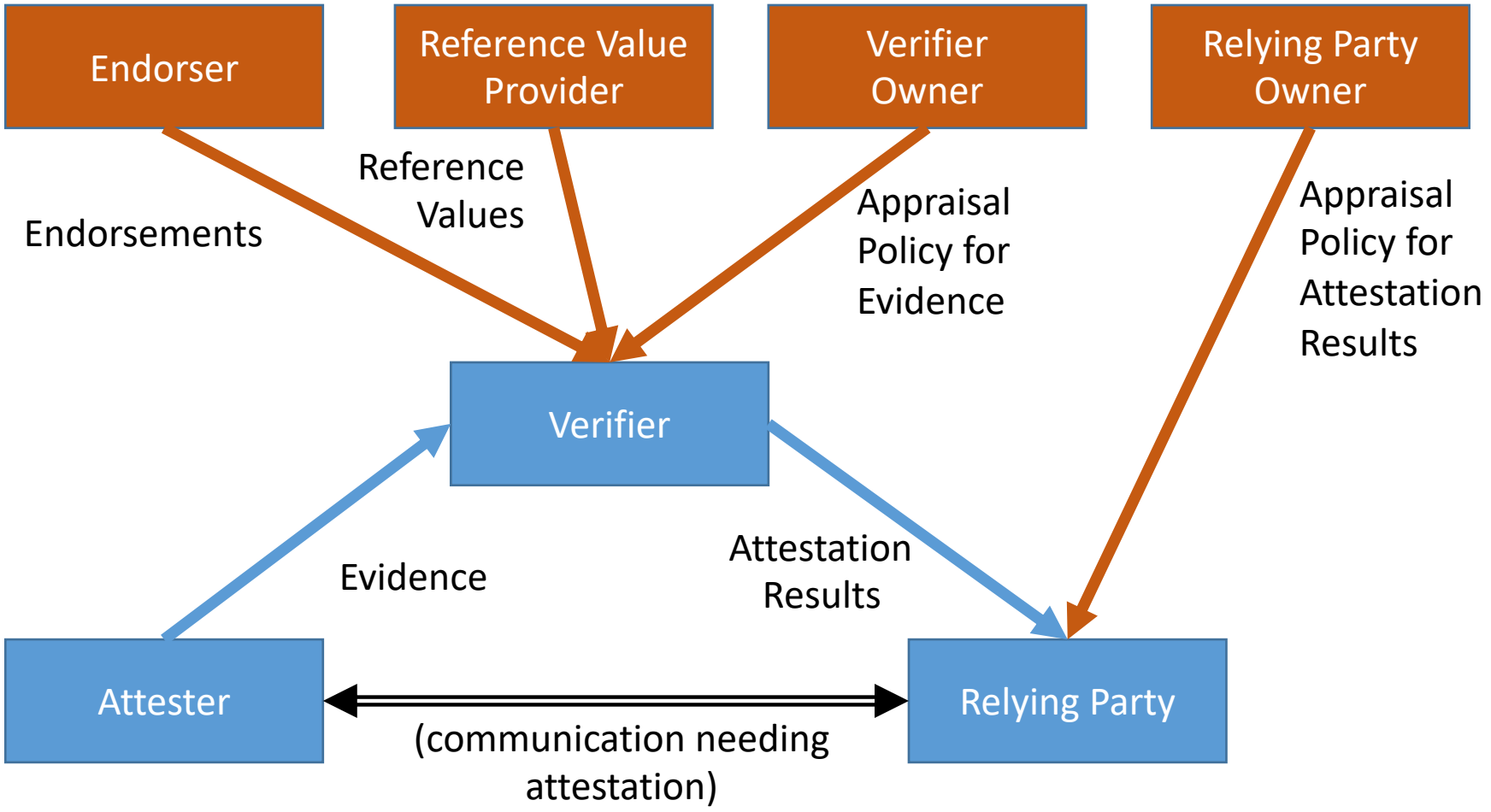
IETF Remote Attestation Architecture Overview

Dave Thaler (as co-editor)

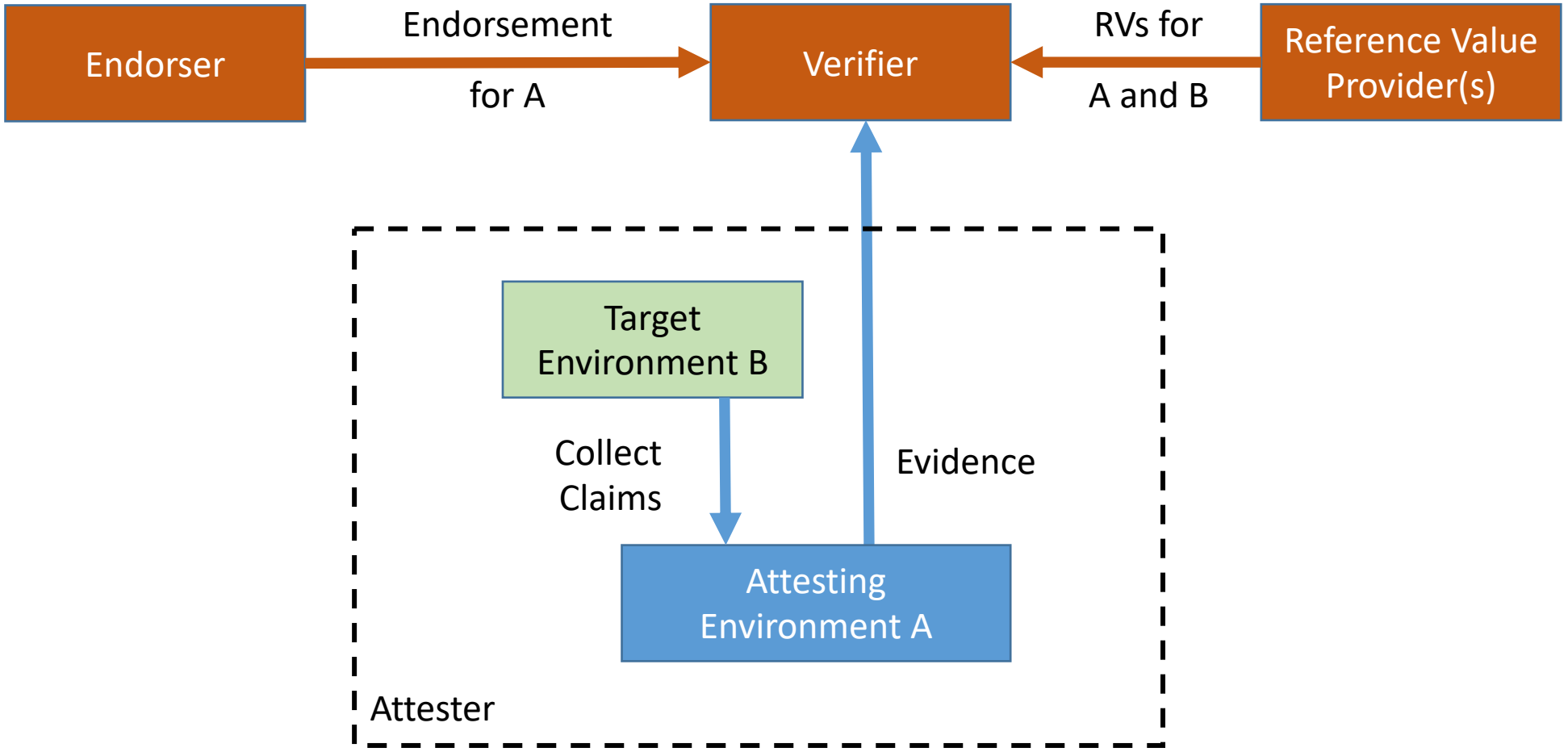
Remote ATtestation procedureS (RATS) WG

- Chartered to do architecture and standardize data formats
  - But not protocols or code
- Common participants between TAC / RATS:
  - Dave Thaler, Thomas Fossati, Eric Voit, …
- RATS arch doc and CCC deep dive whitepaper reference each other
- WG documents: https://tools.ietf.org/wg/rats/

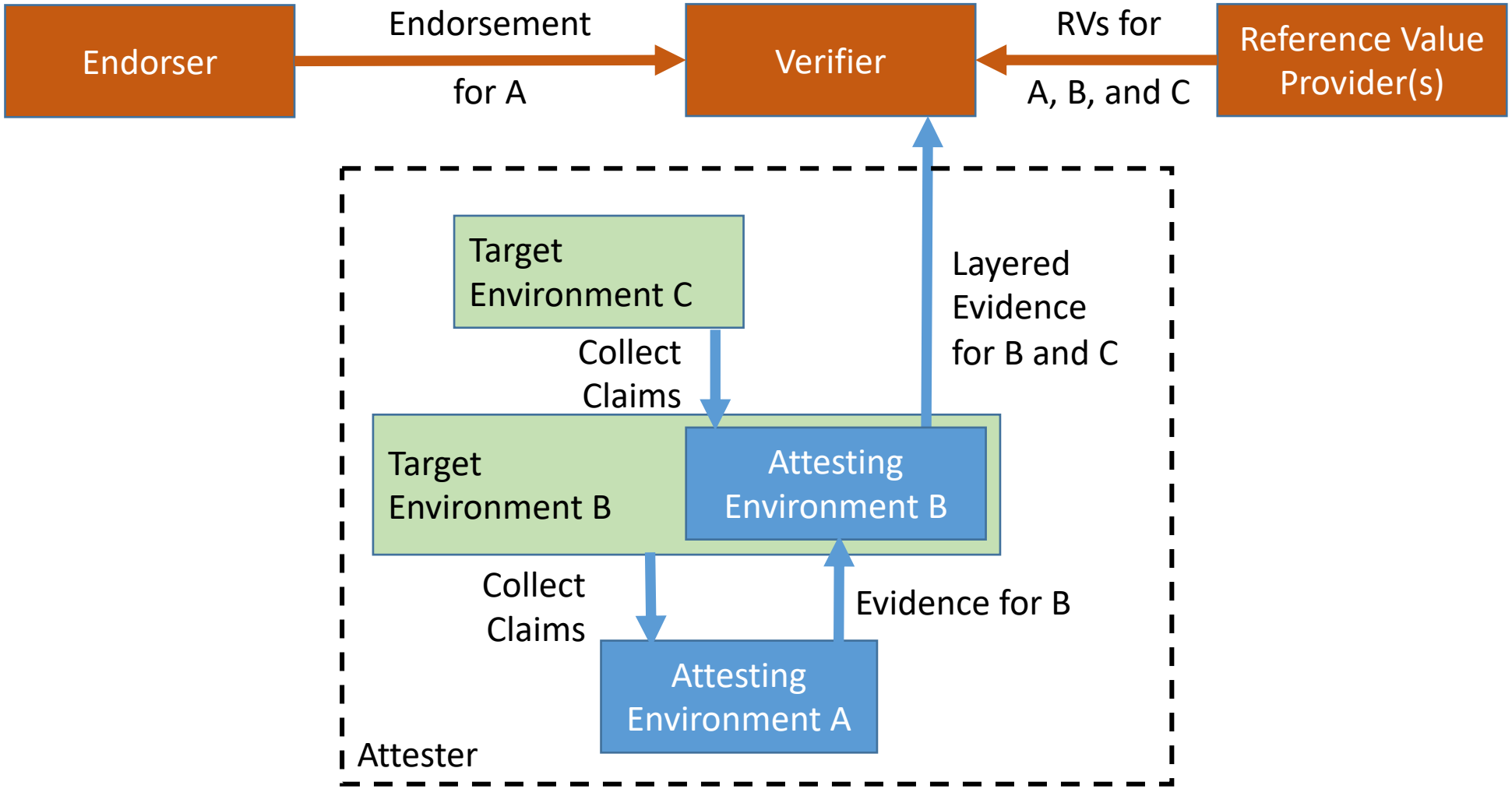
RATS Architecture: Conceptual Data Flow



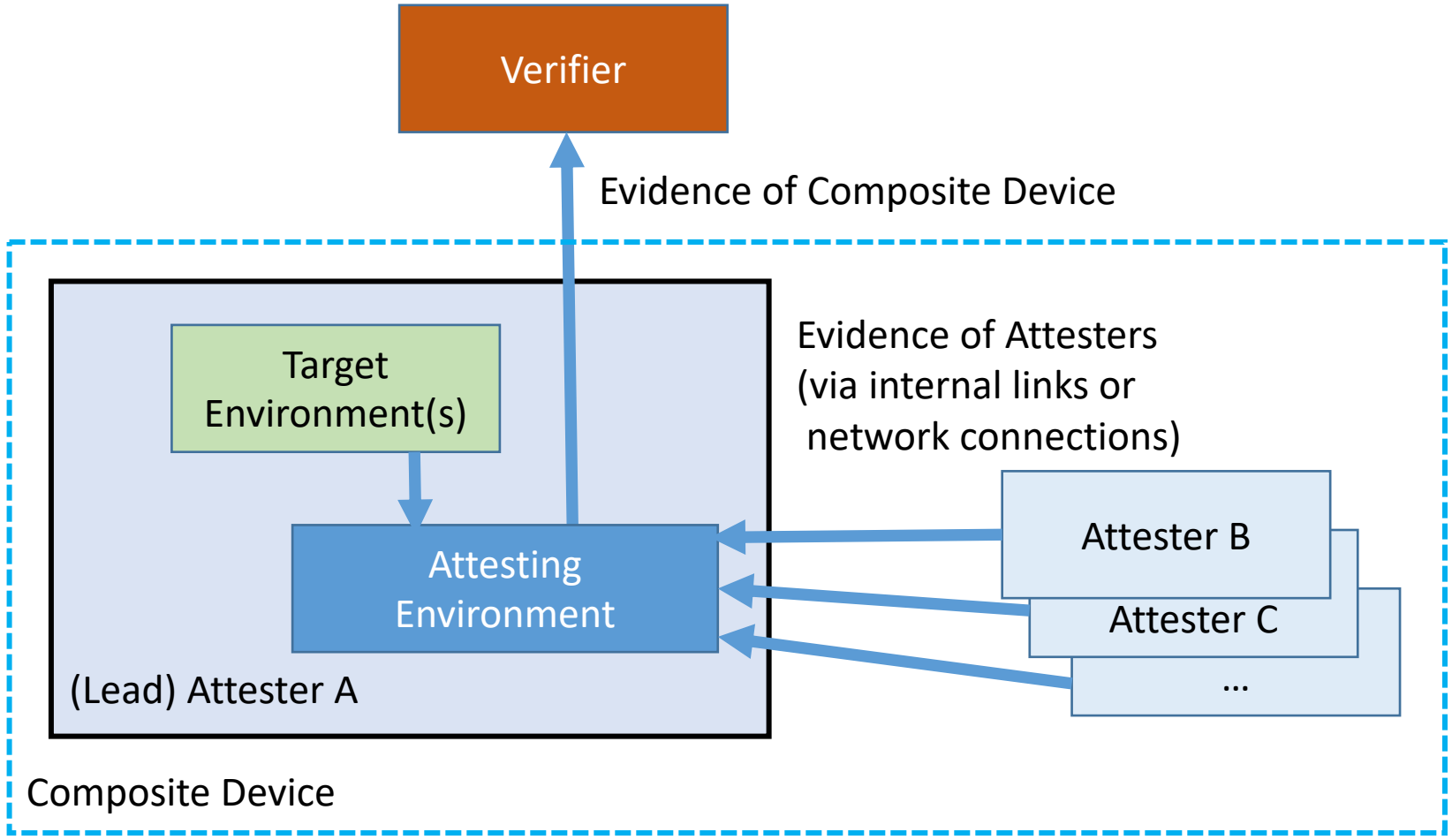
Two types of environment in attester…



In general these can be chained…

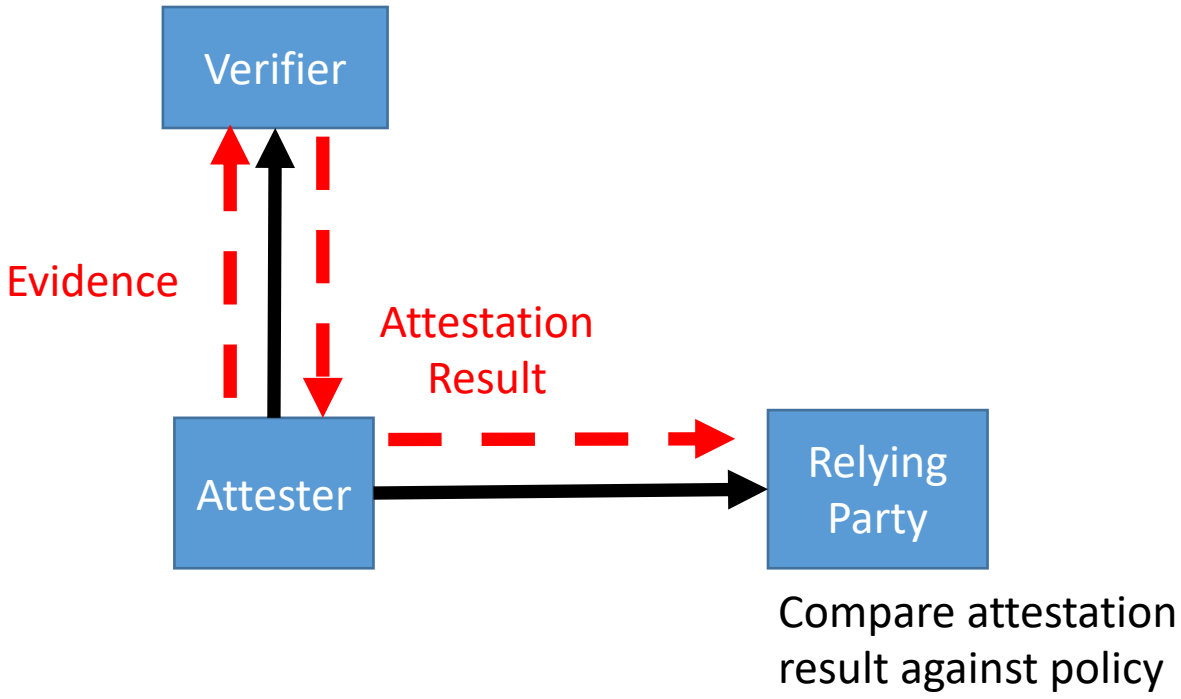


Might even have more complex devices…

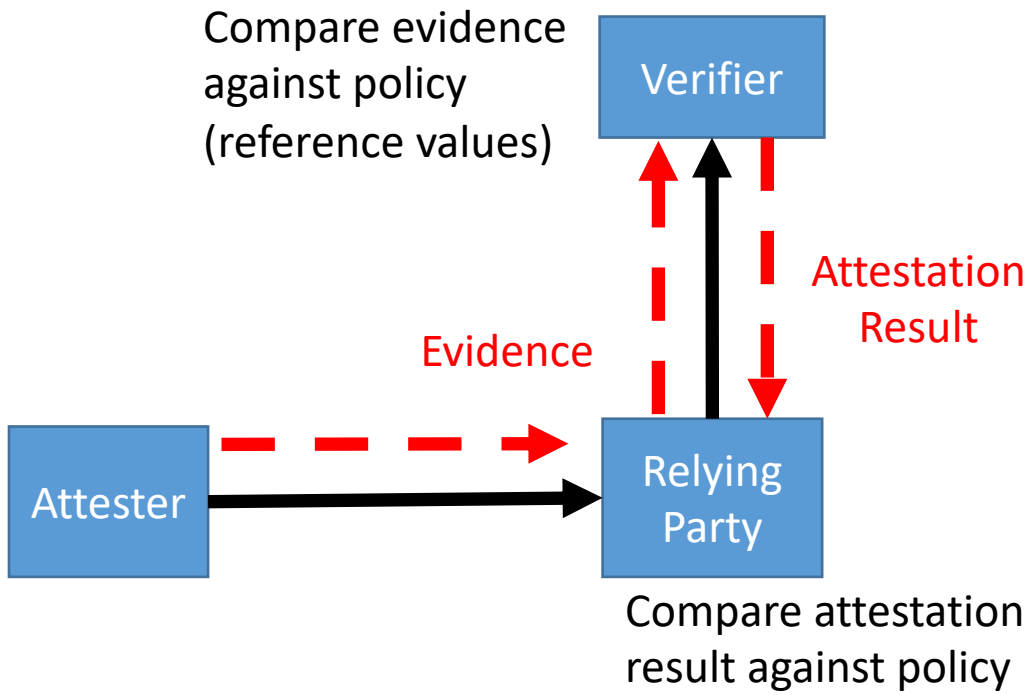


Mapping conceptual data flow to protocols…

"Passport" model:

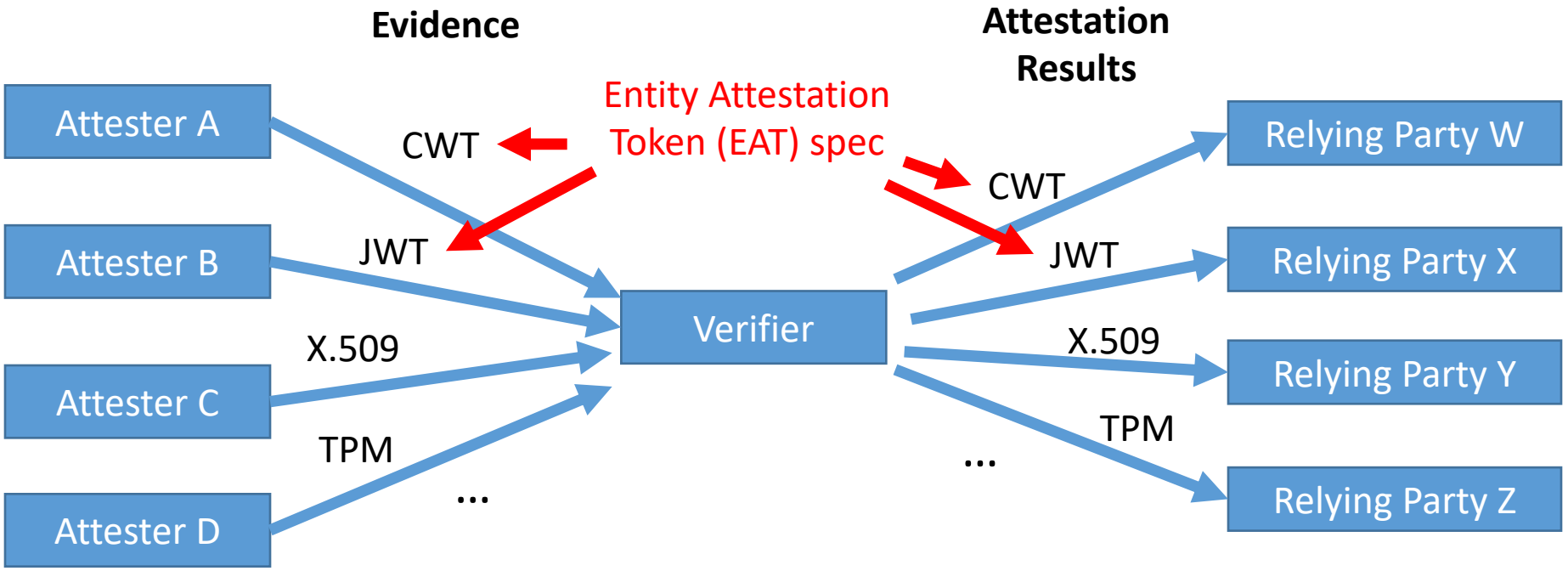


"Background check" model:



Relationship among formats

- Evidence, Attestation Results, and Endorsements can all have different claims formats
- There can be multiple formats possible for each one, including existing standard or proprietary formats, e.g.:



Freshness & replay protection

- Verifier cares about:
  - Was Evidence recently signed by Attester, not an old replay?
  - Are values of claims recent, not obsolete values in recent evidence?
- Relying Party cares about:
  - Was Attestation Result is recently signed by Verifier, not an old replay?
  - Are values of any claims recent, not obsolete values in recent results?
- How “recent” is up to the appraisal policy
- Details are up to the protocol, but there are three common ways…

Method 1: Timestamps

- Put timestamps in claims in Evidence and Attestation Results
- Requires roughly synchronized clocks
  - Requires a trusted source of time, internal or external
  - Requires secure time sync protocol (e.g., ntpsec inside TEE)
- Also adds claims about the signer's time sync mechanism
- No additional messages or state at attestation time

Method 2: Nonces

- Receiver supplies nonce that sender must include in signed Evidence or Attestation Results
- No dependency on time sync or clocks at senders
- Receivers have to keep state to remember each nonce supplied until it’s used
- Receivers need a clock to “expire” nonces, but need not be synced
- Only addresses freshness of Evidence / Attestation Results, not freshness of claim values

Method 3: Epoch handles

- Some “handle distributor” periodically sends out epoch handles to sender(s) and receiver(s)
- Senders use latest epoch handle in all messages in place of nonce
- Receivers check if received handle is in most recent set (e.g., of size 2)
- Receiver state is constant, compared to nonces
- Only handle distributor requires a reliable clock
- “Recency” policy limited to a multiple of handle distribution period

Questions?