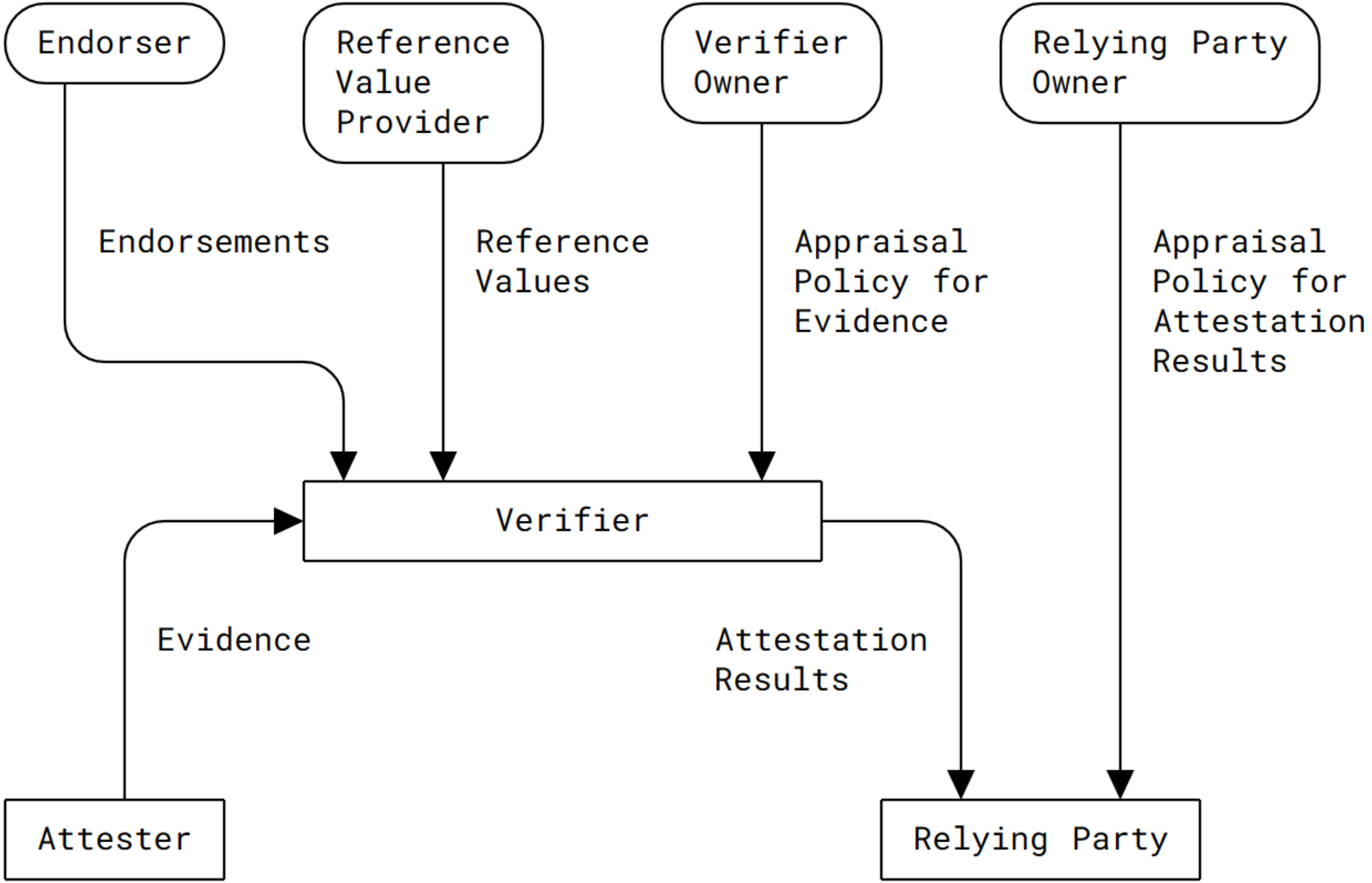
RATS Endorsements

draft-dthaler-rats-endorsements-00

Dave Thaler


Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
Endorsements
Reference Values
Appraisal Policy for Evidence
Appraisal Policy for Attestation Results
Verifier
Evidence
Attestation Results
Attester
Relying Party

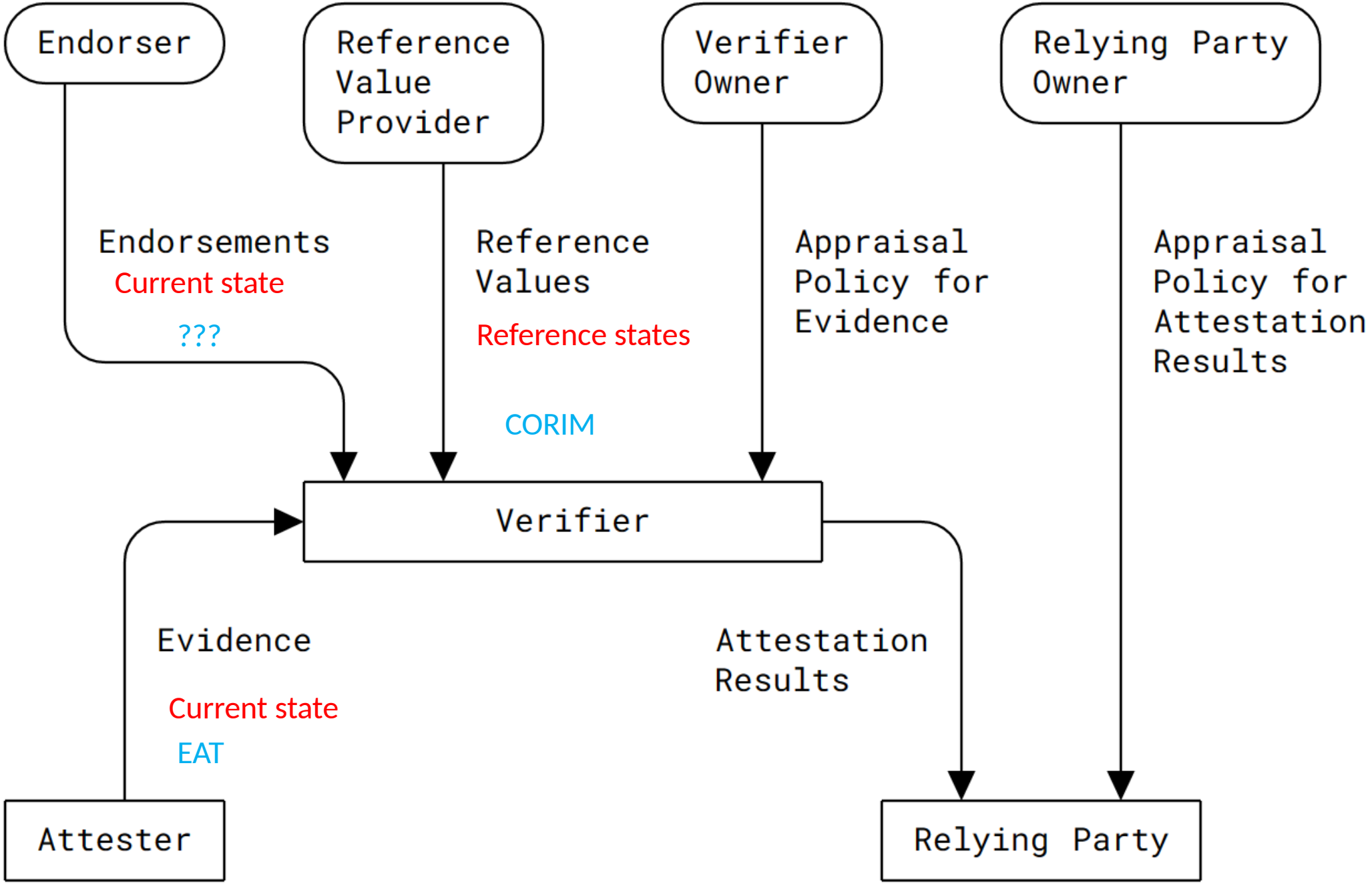
Conceptual messages

- **Appraisal Policy for Evidence:** A set of rules that a Verifier uses to evaluate the validity of information about an Attester.
  - *How* to compare information about current state against information about desired (or “valid”) states
- **Reference Values:** A set of values against which values of Claims can be compared as part of applying an Appraisal Policy for Evidence. Reference Values are sometimes referred to in other documents as "known-good values", "golden measurements", or "nominal values". These terms typically assume comparison for equality, whereas here, Reference Values might be more general and be used in any sort of comparison.
- **Evidence:** A set of Claims generated by an Attester to be appraised by a Verifier. Evidence may include configuration data, measurements, telemetry, or inferences.
- **Endorsement:** A secure statement that an Endorser vouches for the integrity of an Attester's various capabilities, such as Claims collection and Evidence signing.

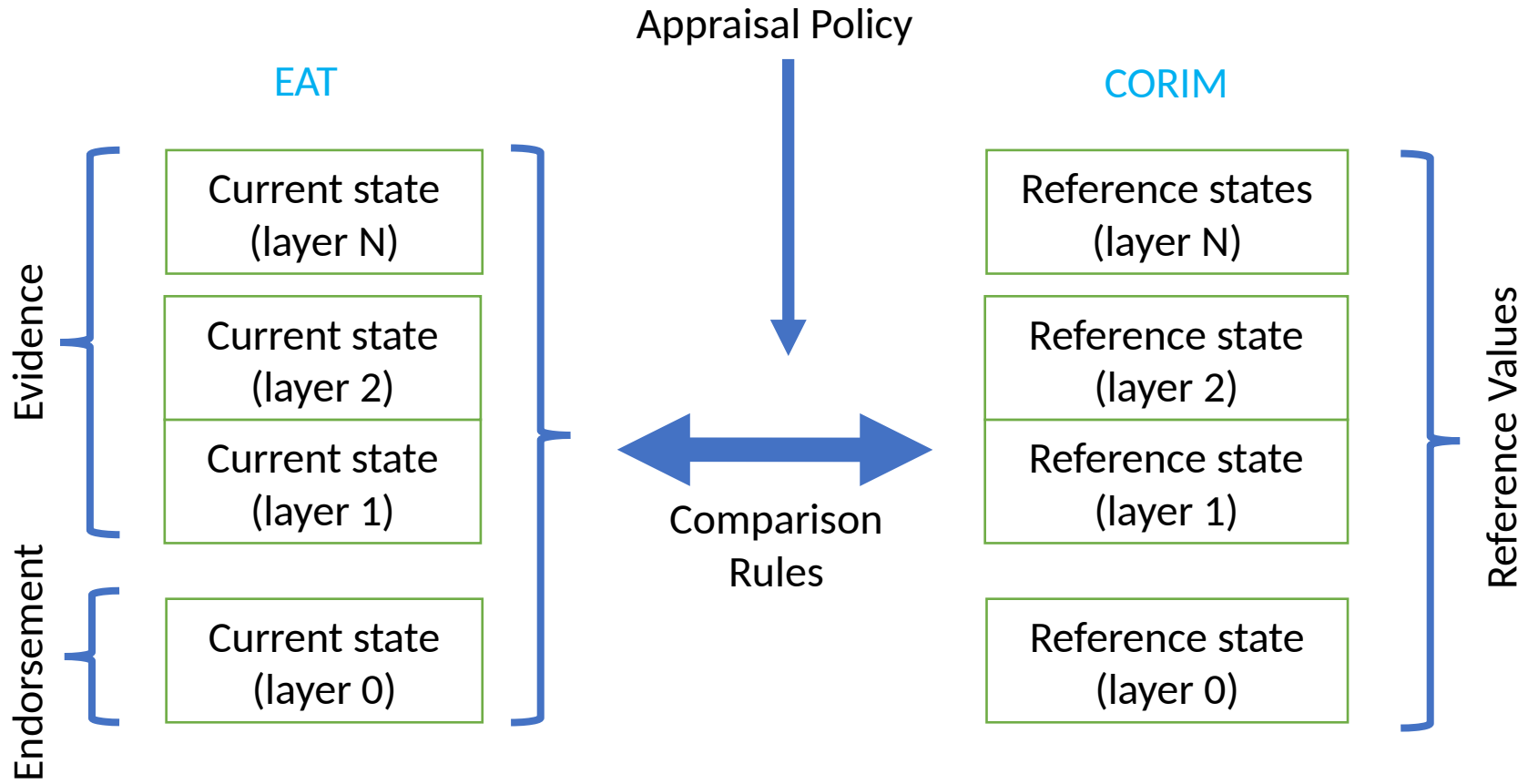
Current state vs desired state

- Current state of something is a specific value
  - Conceptually: “name = value” pairs
- Reference values used in desired state can have many values, e.g.:
  - Allow list: “name in [value1, value2, value3, …]”
  - Block list: “name not in [value1, value2, value3, …]”
  - Upper & lower bounds on a range: “value1 <= name <= value2”

- Thus, encoding current state vs reference states have semantic differences


Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner
Endorsements
Current state
???
Reference Values
Reference states
CORIM
Appraisal Policy for Evidence
Appraisal Policy for Attestation Results
Verifier
Evidence
Current state
EAT
Attestation Results
Attester
Relying Party

Verifier inputs



“Complexity is the enemy of security”

- Using one common format for current state (Evidence + Endorsements) simplifies comparison
  - Simplicity reduces risk of security flaws
  - E.g., general claim defined for claimsets allows use in both Evidence and Endorsements, for all layers
- EAT for Evidence EAT for Endorsements
- Vendor-proprietary Evidence Vendor-proprietary Endorsements
- CORIM for Evidence CORIM for Endorsements
- EAT for Evidence <≠> CORIM for Endorsements

Constrained node Relying Party

- To trust the Verifier, it may need to have a minimal internal Verifier just capable of a boolean decision on the regular Verifier
- Minimal internal Verifier may not need dynamic Reference Values, just hard coded in image
  - Hence no need for Reference Value parser for such a case
- Same might be true for Endorsements, or Endorsements might be sent with the Evidence
- If sent with Evidence, need Endorsement parser but have parser for Evidence format

Summary

- Anything with multiple values of the same thing is “Reference Values”
- “Endorsement” is current state
  - Each claim has a single value
- Security risk lessened when Evidence format == Endorsement format