RATS Endorsements

draft-dthaler-rats-endorsements-02

Dave Thaler
Verifier inputs

- **EAT**
  - Current state (layer N)
  - Current state (layer 2)
  - Current state (layer 1)
  - Current state (layer 0)

- **CORIM**
  - Reference states (layer N)
  - Reference state (layer 2)
  - Reference state (layer 1)
  - Reference state (layer 0)

- **Appraisal Policy**

- **Comparison Rules**

- **Evidence**

- **Endorsement**

- **Reference Values**
Conditionally endorsed values

• Based on feedback from Thomas Fossati
• Some claims in endorsements might be conditional
• Only applies if actual state matches some expected values
  • Not for immutable values like hardware serial number
• Different from verifier’s appraisal policy since:
  a) not about trustworthiness
  b) under control of endorser not verifier owner
• If “matching” policy is a different format than in Appraisal Policy, verifier may need multiple matching policy format parsers
Endorsing Identity

• Based on feedback from Thomas Fossati
• “Identity” related claims (e.g., verification keys) might be endorsed
• Syntactically, just like any other claim
• Some implementations might treat them differently
  • E.g., first verify Attester’s identity before spending effort on appraising other claims
• Generalization:
  • Appraisal Policy for Evidence might have multiple steps
Multiple Endorsements

Endorsements

- App endorser
  - App claimset
- OS endorser
  - OS claimset
- Firmware endorser
  - Firmware claimset
- Hardware endorser
  - Hardware claimset

Evidence

- App claimset
- OS claimset
- Firmware claimset
- Hardware claimset
New feedback from Muhammad Usama Sardar

- Technical (done):
  - Wanted discussion of endorsing identity and conditionally endorsed values

- Editorial (not yet done):
  - Inconsistent capitalization: “references values” vs “Reference Values”
  - Clarify “group of claims” vs “set of claims”
  - “set of claims” might only have one claim

- Questions about mapping of SGX to claims:
  - Details are for an SGX profile
  - Goal is just to make sure the document is generically applicable
Next steps

• Adopt as WG document?