

# RATS Endorsements

draft-dthaler-rats-endorsements-03

**Dave Thaler**

Henk Birkholz

Thomas Fossati

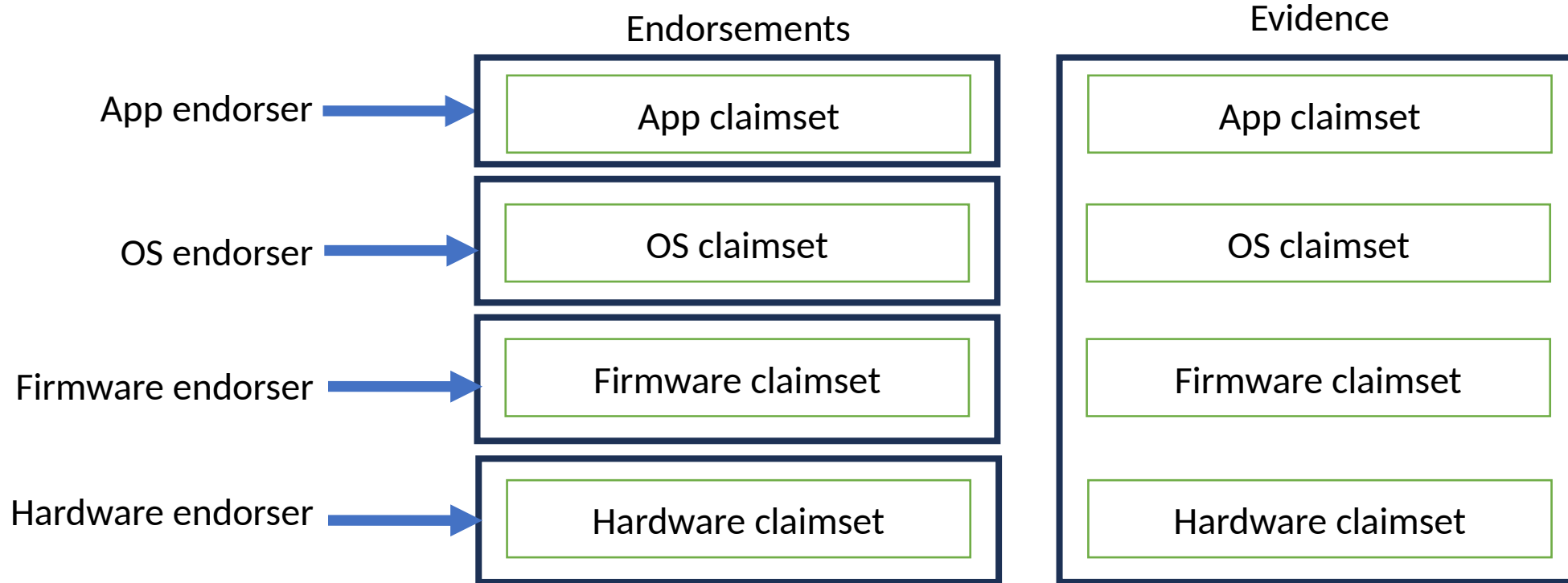
# Changes prior to IETF 117, discussed last time

- Added discussion of conditionally endorsed values
- Added discussion of endorsing “identity”
  - Laurence wanted additions (or name changes) to this section
  - Henk (and Laurence?) volunteered to contribute text
- Goal is an Informational document
  - Logically an extension of RATS Architecture [RFC9334]
- Any Proposed Standard work goes in more specific documents
  - E.g., corim, attestationsets, etc.

# Changes since IETF 117

- Added Henk and Thomas as co-authors
- Added acknowledgments for Thomas H., Laurence, Kathleen
- Updated term capitalization to match RATS Architecture
  - “Reference Values”, “Attester”, “Verifier”, etc.
- Clarified text around claimsets, per feedback from Muhammad Usama Sardar
- Used “Target Environment” instead of “component” for consistency with other specs

# Multiple Endorsements



# Added text per IETF 117

- “When Target Environments from different vendors each have their own Endorser, it is important that a Verifier be able to distinguish **which Endorser is allowed to provide an Endorsement about which Target Environment**. For example, the OS Endorser might be trusted to provide additional claims about the OS, but not about the hardware. Thus it is not as simple as saying that a Verifier has a trusted set of Endorsers.
- The binding between Target Environment and Endorser might be part of the Appraisal Policy for Evidence, or might be specified as part of the Evidence itself, or some combination of the two.
- An Endorsement format specification should explain how this concern is addressed.”

# IETF 117 minutes: Endorsing “Identity”

- Laurence: I want to talk about attestation keys and identity in relation to this draft. This is an architecture draft, so it will impact design of all sorts of future things. An important point is the **key material to verify the evidence**. It **deserves a lengthy discussion** in the draft. Don't call it "identity" because to most people "identity" does not mean "key material". I do not support adoption of the draft unless you **frame up that attestation key material is different from identity**.
  - Henk and Laurence (?) volunteer to contributing text.
- Henk: The one place that "identity" makes sense is "**device identity**" -- **everything else** can be hard to identify, so we should not call it "identity".
- Still need text contributions, but **should not hold up WG adoption**

# Next steps

- Request adopting as WG document
- Welcome text contributions/co-authors, esp. around key material