RATS Endorsements

draft-ietf-rats-endorsements-03

Dave Thaler

Henk Birkholz

Thomas Fossati

WGLC discussion

On Sept. 24, Ned (as chair) posted:

> The following drafts were proposed for WGLC at IETF 120:

> * draft-ietf-rats-endorsements<https://datatracker.ietf.org/doc/draft-ietf-rats-endorsements/>

> [...]

>

> The RATS chairs typically allow 2-weeks for list review / comment.

>

> Is there any more discussion on these drafts regarding WGLC?

Carl Wallace and Kathleen Moriarty responded with comments, though Carl did say
"I reviewed draft-ietf-rats-endorsements in support of WGLC.
In general, the draft is fine and could probably progress as-is"

Security Considerations - Kathleen

- “I am also wondering if there are additional security considerations on the layers, differing sources for policies mentioned in the draft, and formats for developers or implementers.”

OLD:

6. Endorsement Format Considerations
   - 6.1. Security Considerations
   - 6.2. Scalability Considerations
7. IANA Considerations

NEW:

6. Endorsement Format Considerations
   - 6.1. Security Considerations for Formats
   - 6.2. Scalability Considerations for Formats
7. Security Considerations
8. IANA Considerations

Trust and bindings – Carl (1)

- “I think it may benefit from a bit **more discussion on how trust is established in endorsements and how the binding from endorsements to target environment is established**. There is no mention of either **in the security considerations section**. RFC 9334 defines endorsements as being a “secure statement”, so piggybacking off that definition to **reference some (abstract) state that must be present in the verifier** to verify the endorsement may suffice.”

Existing Section 4 (Endorsing Verification Keys) does have text on binding:

> the Verifier typically is provisioned with a trusted root CA certificate such that an Endorsement from an Endorser includes the Attester's verification key material in the form of a certificate that chains up to that trusted root. Such a certificate might be stored in the Verifier, or might be resolved on demand via some protocol, or might be passed to the Verifier along with the Evidence to verify, depending on the protocol.

Security Considerations – Carl/Kathleen

7. Security Considerations

Section 8.4 of [RFC9334] discusses how a Verifier stores one or more trust anchors in its trust anchor store. The Verifier's trust in an Endorser is expressed via storing a trust anchor for the Endorser. The binding from an Endorsement to a given Target Environment is done as discussed in Section 4 of this document.

[RFC9334] (especially Section 3.2 and Section 12) also discusses security considerations around the attestation of layers, and around sources of appraisal policies. Section 4 of this document covers additional considerations in these areas, and Section 6.1 covers additional considerations around Endorsement formats.

Timeliness – Carl (1)

- "Commenting on the need (or lack of need) for timeliness of endorsements may be worthwhile as well. There is discussion of actual state relative to points in time but not how endorsements fit on the timeline."

PR proposes adding new section to address:

5. Timeliness

Specific protocol documents are also responsible for documenting how Timeliness of the Endorsement itself (e.g., using a certificate lifetime) is provided.

Section 8.1 of [RFC9334] discusses timeliness of claims in Evidence. When additional static claims are provided in Endorsements, no additional steps are needed for timeliness of those claims since they are static rather than dynamically varying by time. Once timeliness of Evidence is verified, any matching conditionally endorsed values can be applied.

If Endorsements ever carry dynamic claims in the future (e.g., whether any vulnerabilities in the version of firmware are currently known), then the same timeliness considerations as for claims in Evidence would apply, and would be the responsibility of specific protocol documents. See Section 10 of [RFC9334] and Appendix A of [RFC9334] for further discussion.

Nit – Carl (2)

- Carl:
  - One nit, section 5 states the following:
    - “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 (e.g., claims from a Target Environment might include a **secure identifier** of what Endorser can provide additional claims about it), or some combination of the two.”
  - Given the evidence has not yet been verified, referring to the identifier as a “secure identifier” is probably not appropriate.

- Fix: s/secure identifier/identifier/

Next step

- Merge PRs and submit -04
- WGLC status?