CRYPTO4A

IETF 124 Montréal - RATS WG

Jean-Pierre Fiset

(Mike Ounsworth, Hannes Tschofenig, Monty Wiseman, Henk Birkholz, Ned Smith)

PKIX Evidence for Remote Attestation of HSMs

https://datatracker.ietf.org/doc/draft-ietf-rats-pkix-key-attestation/

Update since July 2025

- Removed the concept of “Root of Trust”
  - It was confusing and did not add value to the specification.
  - Whether the Attesting and Target Environments are the same is irrelevant.
- Aligned attribute definitions with EAT and PKCS11
  - In some cases, the definitions were re-used.
  - For key purpose, OIDs are assigned to attributes.
- General care and maintenance
  - 11 opened issues; 31 closed issues
- We are continuing bi-weekly meetings inviting those who are interested

CRYPTO4A

Contributions to RATS - Presenter

This draft introduces the role of Presenter

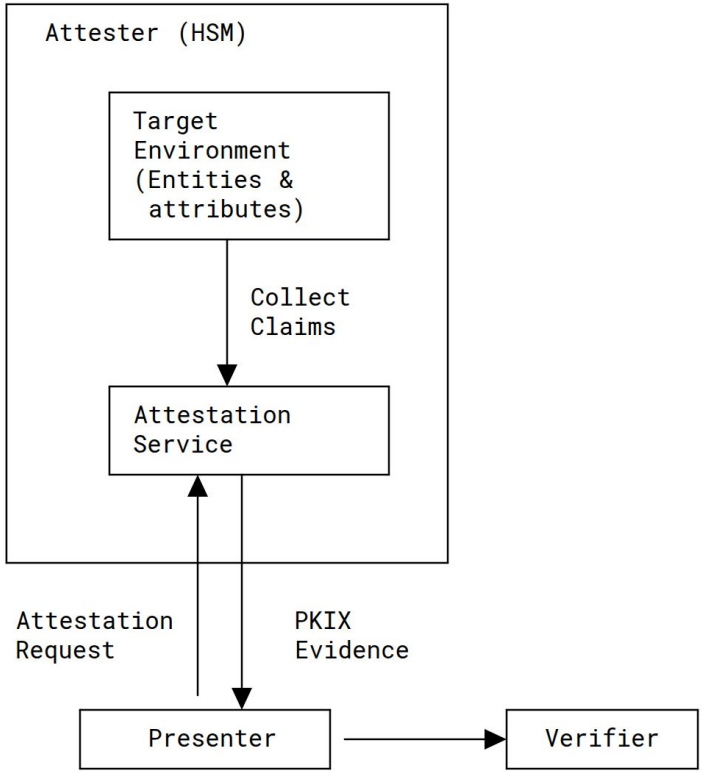
“Role that facilitates communication between the Attester and the Verifier. The Presenter initiates the operation of generating evidence at the Attester and passes the generated evidence to the Verifier. In the case of HSMs, the Presenter is responsible of selecting the claims that are part of the generated evidence.”

Examples of presenters:

- TLS library collecting Key Attestation from the local TPM or PKCS#11 HSM about the certificate private key.
- VPN client or security agent or MDM collecting secure boot attestation from the local hardware.

CRYPTO4A

Presenter



CRYPTO4A

Contributions to RATS - Large Target Environment

- Since HSMs have a large addressable space, it is not desired to provide the complete state as evidence.
  - Some exposures might have confidentiality implications
- The selecting of the portions to be measured is left to the Presenter.
  - Portions are referred to as entities - looking for a better word
  - Entities are associated with attributes - roughly the EAT claims/measurements
  - Keys and platform are entities.
  - Responsibilities associated with Presenter
- The division of the target environment is necessary:
  - Prevents collisions between similar claims of different portions
  - It helps comprehension of the provided evidence.
  - Requires “attestation request”

CRYPTO4A

Upcoming Work

- Add support for User Modules (usermods)
  - Look into EAT and other specifications
- Complete Extended Key Usage for X.509 (dependency)
  - draft-jpfiset-lamps-attestationkey-eku
- Complete a functional implementation
  - A sister implementation already exists
  - Mike Ounsworth is developing a similar work in RUST
- Reach WG LC (by IETF 125 Shenzhen)

Requesting Support from WG

- Is the structure sound?
  - Evidence -> entities -> attributes
  - Very generic terms, are they the correct ones?
  - Considering renaming “entity” to “subject”
- Review of Presenter Role
  - Does it align with other efforts with the WG

References

Datatracker:

https://datatracker.ietf.org/doc/draft-ietf-rats-pkix-key-attestation/

GitHub:

https://github.com/ietf-rats-wg/key-attestation