

IETF 123 Madrid - 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 March 2025

- Formerly known as “Key Attestation”
 - 3 or 4 versions of this draft have been floating with different titles
 - Lining up language and definitions with RFC 9334
- Separated Information Model from Data Model
 - Stabilized Data Model (ASN.1)
- Introduced the role of “Presenter”
 - Initiates the operation of generating PKIX evidence at HSM
 - Specifies information to be claimed by HSM
 - Transfers evidence to Verifier
- Added a section on “Attestation Request”
 - Optional format for requesting PKIX evidence

Current Work

- We are continuing bi-weekly meetings inviting those who are interested
- Address GitHub issues
- Complete a functional implementation
 - A sister implementation already exists
- Reach WG LC (by IETF 124 Montreal)

Information Model

- To-Be-Signed Section is composed of “Entities”
 - Proposed types: Platform, Key, Transaction
 - Extensible (type by OID)
- Entities have a collection of “Attributes”
 - Attribute associate type to a value
 - Large number of attribute types are proposed (defined by OIDs)
 - Nature of value is defined by type of attribute:
 - Integer, bytes, string, bool, time, oid, null

Questions

- Evidence is made up of claims
 - Should the concept of “attribute” be renamed “claim” to line up with EAT?
 - Language collision between HSM / PKCS#11 / PKIX / RATS
 - Is “evidence” the correct term here?
- “Attestation Request” produces PKIX Evidence
 - Provided by Presenter to HSM; HSM produces evidence
 - Should it be renamed “Evidence Request”?
 - Large HSMs with multi-tenant support require authentication of Presenter.
- “Evidence vs Trusted Self-Assertions”
 - HSMs are generally endorsed by a manufacturer or other parties
 - Henk Birkholz and Michael Richardson are exploring this question
 - PKIX Evidence format is a flat structure and assumes that Attesting and Target Environments are the same. Matches better the HSM industry with third party validation laboratories. It does not match cleanly the nested evidence offered in other RATS specification (DICE, ROTs).

References

Datatracker:

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

GitHub:

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