draft-ounsworth-rats-x509-evidence

Mike Ounsworth, Hannes Tschofenig

RATS 118

Background

Who:

- This draft is a product of the “PKIX Attestation” design team that has been operating out of LAMPS since April 2023, which is a group of HSM manufacturers and public CAs.
- This design team already produced draft-ietf-lamps-csr-attestation.

What:

- Under recent CA/B Forum Code Signing BRs, certificate subscribers need to prove to their CA that private keys are stored in a FIPS / CC HSM.
- There is currently no automated way to do this.
- 💡 Perfect use for RATS!
- None of the existing evidence formats are suitable, so we are defining a new one.
- We think (?) that RATS is the right home for this work.

Technical Content

- Selection of EAT claims, but encoded as ASN.1 X.509 extensions (i.e. X.509 is the evidence format).
- Plus some HSM-specific ones:
  - “fips_conf”: FIPS Conformance: evidence that the device performed the correct start-up self-tests, has the correct config, etc, to match its FIPS certification.
  - “cc_conf”: Common Criteria Conformance: ditto for CC.
  - Some we need to add:
    - “non-exportable”, “backup-able”, “card-control”, “dual-control”, any other private key storage properties that are generalizable across HSM vendors.

      (SPOILER: ask 5 HSM vendors to define “non-exportable” and you will get 5 different definitions; design team meetings can be slow moving.)

Next Steps

- This is a -00 version but it shows the direction.
- Will sync with other organizations (e.g. TCG DICE)
- Good time to **adopt** the draft and to have a **RATS/LAMPS collaboration**.
- Anyone interested to join the design team?

Open Issues

- Refinement of HSM-specific claims: FIPS, CC, other common private key storage properties.
- All claims in a single extension, or each their own extension?
- Which claims are optional or required?
- Do we need to define attestation results for use in X.509 certs?
- Running code…