draft-ounsworth-rats-x509-evidence

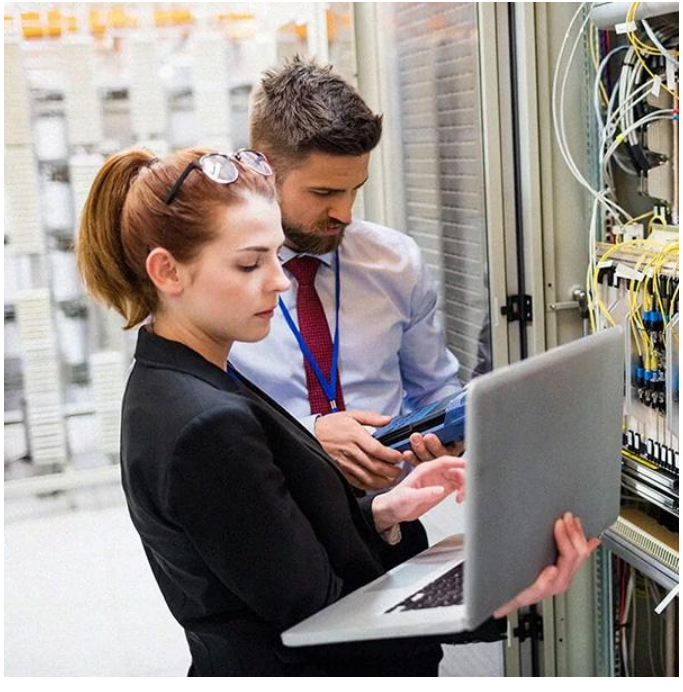
Mike Ounsworth, Hannes Tschofenig

Summary of activity since Prague

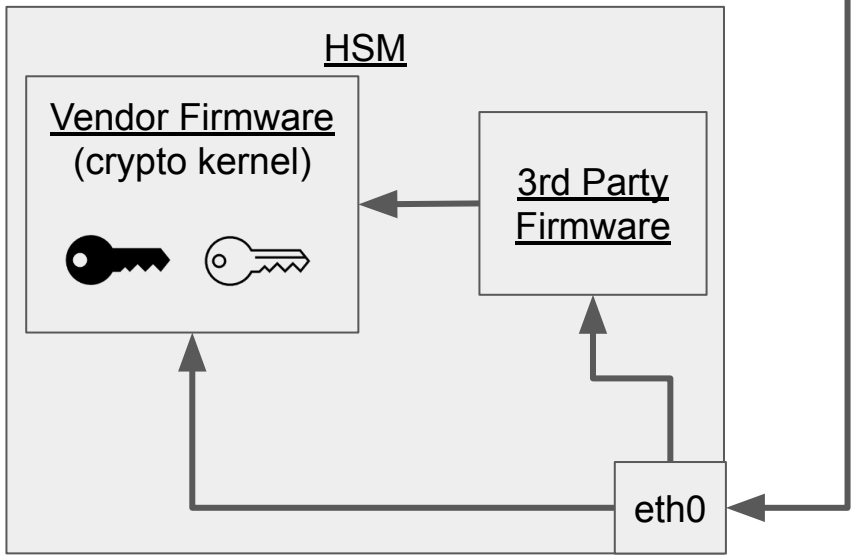
- The design team has continued to meet twice a month (on Mondays, email me for an invite).
  - We continue to have about 10 - 15 attendees each design meeting.
- Main focus has been getting our LAMPS draft-ietf-lamps-csr-attestation to completion.
- Much discussion about the goals and objectives of this work.
- No tangible progress (ie no new draft version)
- All meeting notes are here:
  - https://github.com/lamps-wg/csr-attestation/tree/main/meetingNotes

Scope and purpose

Yes, there exist many evidence formats, but none are generically suitable for “Big HSMs”.



General “Big HSM” device architecture

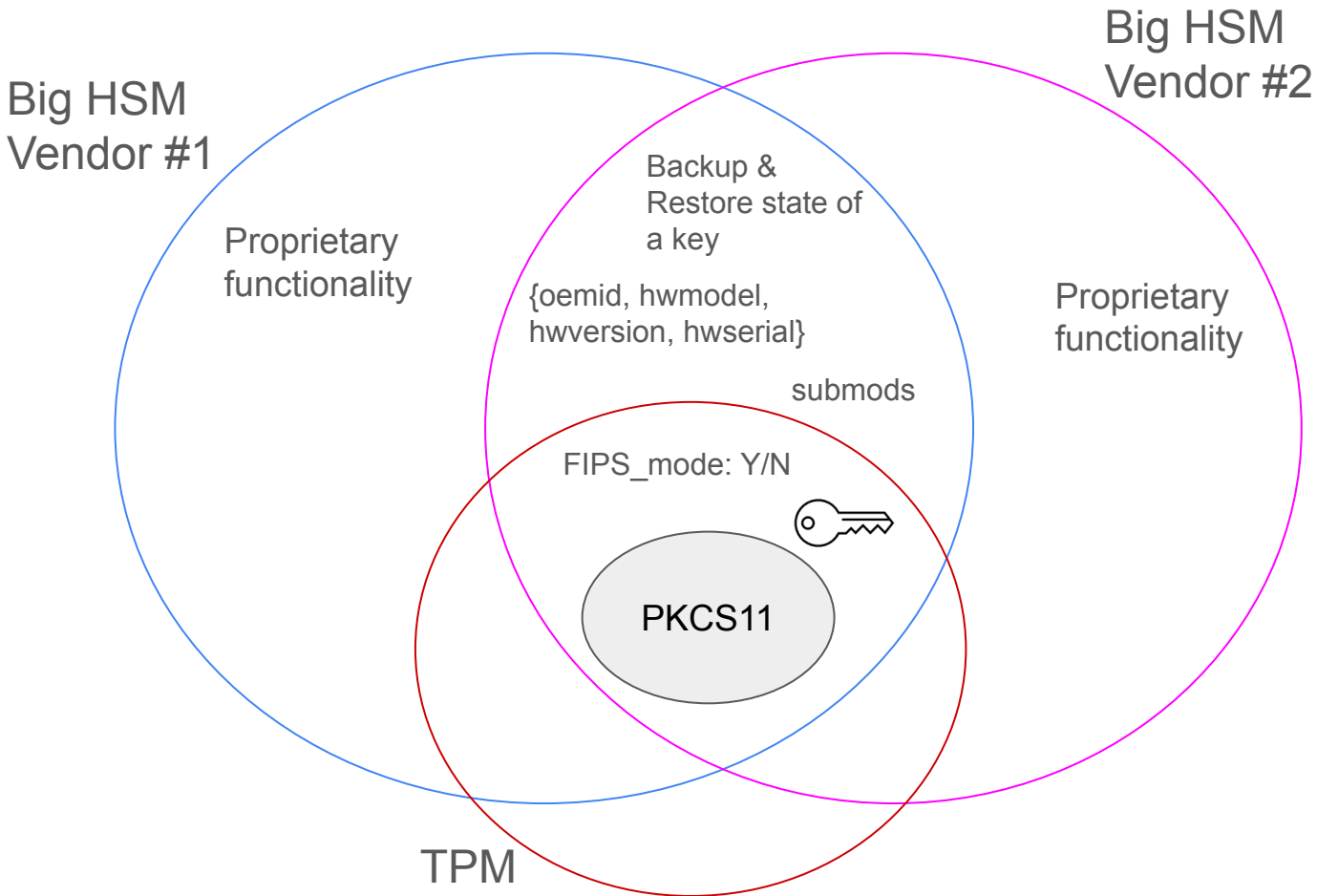


Applications
(ex.: some software using openssl with creds to use the HSM)

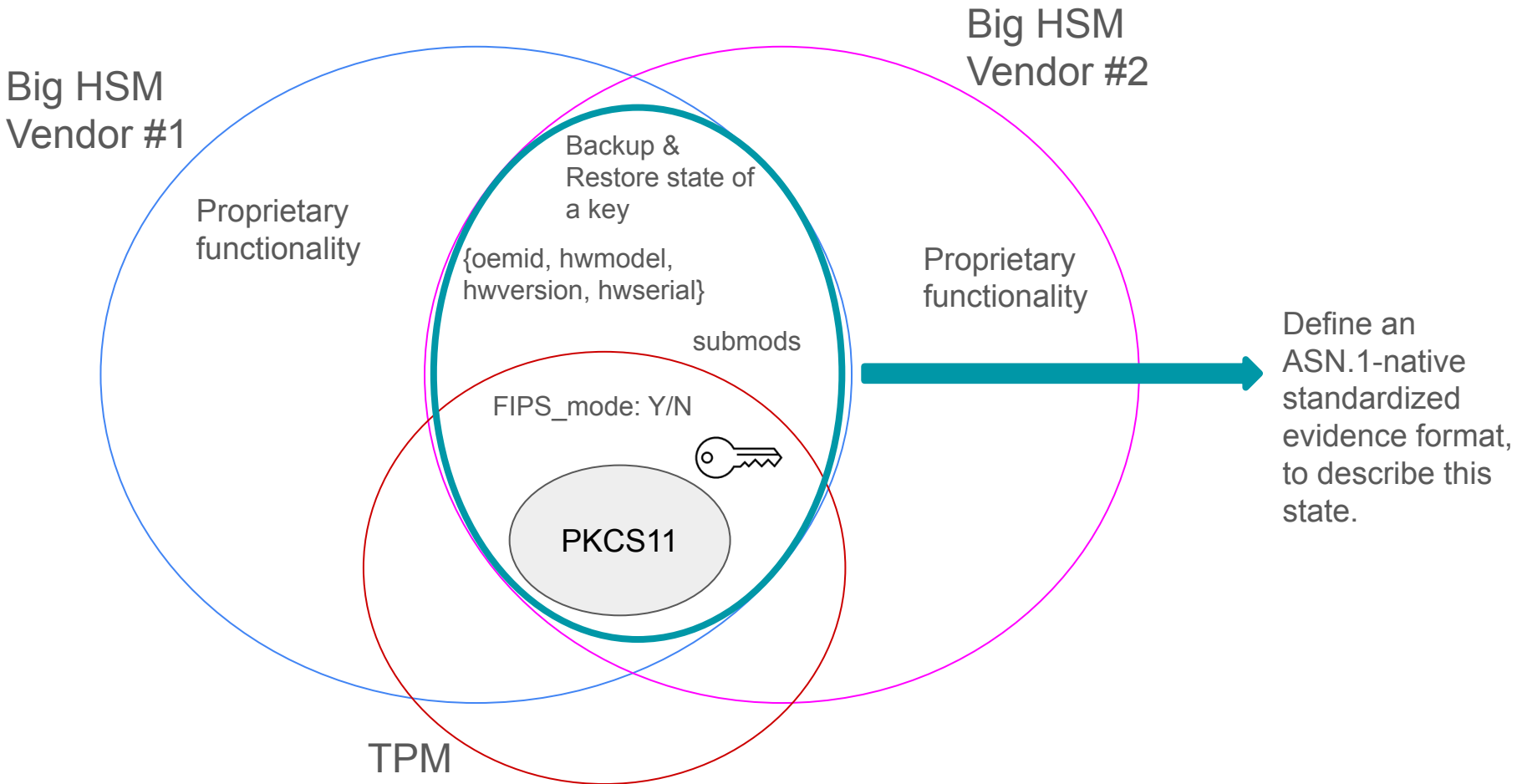
For example maybe this HSM is holding keys to manufacture credit cards; the 3rd party firmware is part of the credit card printing stack to A) harden PKCS#11 around financial sector requirements, and B) format private key material according to financial card specifications.

CSRs for permanent keys within the HSM would be constructed in the software application and sent back into the HSM to be signed.

The rough design goal



The rough design goal



Rough consensus on design goals

- (hot off the press, all DT members may not agree)
- We define a list of claims, all of which are optional (including subject key).
- Format is extensible so that more claims (even proprietary ones) can be added later.
- Hand the empty “form” to the HSM containing the claims you want, and it will fill in the claims with evidence and sign it.
- You can ask for a “Platform Attestation” – ie SubjectKey, and all claims related to it are optional.

- We are making progress on the list of claims. See the running meeting notes:
  - https://github.com/lamps-wg/csr-attestation/blob/main/meetingNotes/2024-03-11.md

Non-consensus on design goals

- Should the wrapper format be X.509 or some custom ASN.1 structure?
  - X.509 idea:
    - When the request is for a Key Attestation, produce a normal X.509 cert; when Platform Attestation, do an Attribute cert. All claims go in X.509v3 extensions.
    - PROs: a common format with good existing tooling.
  - Custom ASN.1 idea:
    - Basically a SEQUENCE OF CLAIM with a signature field.
    - PROs: more flexible; does not carry the baggage of X.509 (DN, SerialNumber, KU, etc); we can design in multiple SubjecKey and signature fields for PQ migration.

Summary

- Trying to get 4 HSM vendors + TCG / TPM to agree on what is “common functionality” has been (un)suprisingly difficult.
- Work is progressing well.
- We almost have the design requirements nailed down.
- Once we have that, the actual format should come together pretty quickly.