Attesting a TPM in a CSR

IETF 119
16–17 March 2024
Brisbane, Australia

Hackathon Plan

- draft-ietf-lamps-csr-attestation
  - Goal: generate the samples for the I-D appendix (and thus validate the I-D).

1. Generate an Attestation from a TPM using TPM dev tools.
2. Bundle that an ASN.1 structure, and then into a CSR as described in the draft.
3. Get the CSR signed by the TPM
4. Prosper.

What got done

- Implementation experience with:
  - draft-ietf-lamps-csr-attestation

- Hackathon code:
  - https://github.com/mwiseman-byid/csr-attestation-tpm-example

What we learned

- Information sharing between TCG TPM people and IETF X.509 people
  - Fun converting TPM native structures to ASN.1 to embed into a CSR.

Wrap Up

Team members:

Mike Ounsworth, Hannes Tschofenig, Corey Bonnell

First timers @ IETF/Hackathon:

Monty Wiseman