Attested Certificate Signing Request (CSR)

IETF 118
4–5 November 2023
Prague, Czech Republic

Hackathon Plan

- Prototyping “attested” CSRs (IETF LAMPS Group)
  - draft-tschofenig-lamps-nonce-cmp-est
  - draft-ietf-lamps-csr-attestation-02
- Integrate functionality into existing implementation.
- Wanted full PoC with three parties: TPM-based attester, Certification Authority and Attestation Verifier

What got done

- Switched implementations several times. Integration into TPM more difficult than expected.
- Settled with Go-based EST implementation and Veraison verifier.
- Discovered challenges with the freshness mechanism designed for EST. Drafts will have to be updated.

What we learned

- Feedback to the working group available and new issues filed at https://github.com/hannestschofenig/tschofenig-ids/issues/69
- Building a complete PoC in a 1.5 days hackathon is challenging.
- Had fun despite constant interruptions.

Wrap Up

Team members:

* Thomas Fossati
* Ionut Mihalcea
* Hannes Tschofenig