Attestation within TLS

Hannes Tschofenig
Problem Statement

• A challenge in IoT is the secure enrolment of edge/endpoint devices with a cloud service.

• The cloud service needs to know that the connecting device is:
  • Genuine
  • Booted to a known-good configuration
  • Running the correct, up-to-date software stack
  • Authorised to connect to the service

• After connection is allowed, there needs to be a secure (encrypted) communication channel established between the device and the cloud.
Idea: Integrate Attestation into TLS
Resources

• Initial draft available at https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-00

• Proof-of-Concept in development. Uses Mbed TLS (TLS 1.3), Parsec and Veraison:
  • Mbed TLS: https://github.com/Mbed-TLS/mbedtls
  • Parsec: https://parsec.community/
  • Veraison: https://github.com/veraison