IETF Hackathon
Firmware Encryption (SUIT/TEEP)

IETF 110
March 1-5, 2021

Hannes Tschofenig
Hackathon Plan

- SUIT manifest and TEEP protocol specifications offer encryption of firmware/software.
  - draft-ietf-suit-manifest and draft-ietf-teep-protocol
  - They point to COSE.
- No examples are given.
What got done

- COSE_Encrypt using AES key wrap.
- Implementation based on:
  - PSA Crypto API,
  - QCBOR, and
  - Mbed TLS
- Investigated integration into Mcuboot.
- To publish the code I am planning to add it to a SUIT library, such as libcsuit
- Examples are available now.
What I learned

• More details in SUIT manifest spec are needed.

• Use of COSE needs to be profiled to avoid interoperability problems and large code size.

• SUIT implementations use different combinations of crypto libraries and CBOR parsers. Generic COSE encryption handling is difficult to accomplish.

• Virtual hackathons are challenging: Timezone differences - busy schedule – distraction.
Wrap Up

Team member:

Thanks to
- Russ Housley (COSE),
- Ken Takayama (libcsuit),
- Brendan Moran (COSE),
- David Brown (Mcuboot),
- Fabio Utzig (Mcuboot)