Encrypted Payloads in SUIT Manifests

draft-ietf-suit-firmware-encryption-20

Hannes Tschofenig , Russ Housley , Brendan Moran , David Brown , Ken Takayama

SUIT, IETF 120

Status

- Submitted to IESG for Publication, 2024-07-13,
  waiting for AD feedback
- IANA OK
- Depends on draft-ietf-cose-key-thumbprint,
  Waiting for AD Go-Ahead::AD Followup
- Addressed review comments from Deb Cooley in -20.
- Augmented examples with extra comments to offer better explanation.

What do we have?

- Ability to encrypt payloads (firmware, software, configuration data, …) using COSE_Encrypt.
- Key agreement is provided by ephemeral-static (ES) Diffie-Hellman (DH) and AES Key Wrap (AES-KW).
- Instructions for dealing with the encrypted payload provided in SUIT manifest.
- Many working examples based on libcsuit - https://github.com/kentakayama/libcsuit
- Addresses special constraints imposed by use of flash memory on microcontrollers.

Next Steps

- Document will go through IESG and directorate reviews.