Firmware Encryption

draft-ietf-suit-firmware-encryption

(Russ H., Brendan M., Hannes T.)

Changes since last IETF meeting

- Spec now depends on COSE-HPKE document < draft-tschofenig-cose-hpke-00>
- New content addressing open issues from last IETF meeting, see https://datatracker.ietf.org/meeting/111/materials/slides-111-suit-firmware-encryption-01
- The new content focuses on protecting the encryption info in the envelope and the battery exhaustion problem.

Changes with -02
SUIT Envelope CDDL

```
SUIT_Envelope_Tagged = #6.107(SUIT_Envelope)
SUIT_Envelope = {
  suit-authentication-wrapper => bstr .cbor SUIT_Authentication,
  suit-manifest  => bstr .cbor SUIT_Manifest,
  SUIT_Severable_Manifest_Members,
  suit-protection-wrappers => bstr .cbor {
      *(int/str) => [+ SUIT_Encryption_Info]
  }
  * SUIT_Integrated_Payload,
  * SUIT_Integrated_Dependency,
  * $$SUIT_Envelope_Extensions,
  * (int => bstr)
}
```

Changes with -02
SUIT Manifest CDDL

```
SUIT_Manifest = {
    suit-manifest-version         => 1,
    suit-manifest-sequence-number => uint,
    suit-common                   => bstr .cbor SUIT_Common,
    ? suit-reference-uri          => tstr,
    ? suit-cek-verification       => bstr,
    SUIT_Severable_Members_Choice,
    SUIT_Unseverable_Members,
    * $$SUIT_Manifest_Extensions,
}
```

The suit-cek-verification parameter contains a byte string resulting from the encryption of 8 bytes of 0xA5 using the CEK.

Open Issues

- Released the HPKE code at https://github.com/ARMmbed/mbedtls/pull/5078
- COSE-HPKE code needs to be updated and will be released as well.
- Interop testing missing
- Open issue regarding IV selection for suit-cek-verification calculation

- Please carefully check the draft!