Firmware Encryption with SUIT Manifests

draft-ietf-suit-firmware-encryption
Encrypted Firmware Upgrade

- Both images in flash
- Insufficient RAM to hold entire image
- Exchanged one block at a time
- New image decrypted 1 block at a time
- Old image encrypted 1 block at a time
Constraints

• Update can be interrupted (power loss, etc)
• Need to be restarted when power is restored
• Typically use something like AES-CTR
AEAD vs Update

**AEAD**
- Tag covering whole image
- Must encrypt/decrypt whole image
- Ensures integrity of whole image

**Firmware Update**
- No space for per-block tag
- CTR mode can be done per block
- Rely on signature covering whole image
Needed for SUIT

• COSE to consider allowing unauthenticated encryption
• May have a clause requiring integrity
• Upgrade verifies signature over plaintext before running
• Upgrade may verify signature by decrypting to temporary buffer, to avoid flash wear on invalid image
Next Steps

• Use case of firmware encryption on many hardware devices requires the use of ciphers without integrity protection
• COSE currently requires an AEAD algorithm
• Will ask to register AES-CTR and AES-CBC with an explanation that they should not be used without some other integrity mechanism (like SUIT Manifest signature)
• That Internet-Draft will go through the COSE WG
Other Open Issues
(on https://github.com/suit-wg/suit-firmware-encryption/issues)

• **CEK with a nonce of all zero**

• **Countersignature**

• [hackathon114] SUIT_Encryption_Info may not be associated with a specific firmware image (with PR [here](https://github.com/suit-wg/suit-firmware-encryption/issues))