

# Encrypted Payloads in SUIT Manifests

[draft-ietf-suit-firmware-encryption](#)

Hannes, Russ, Brendan, David, Ken

# Status

- Detailed update posted to the list:  
<https://mailarchive.ietf.org/arch/msg/suit/Dfm38nCTbvJWrJld2KuloU3gvQI/>
- Good news: the document is close to completion!
- Reference implementation available with  
<https://github.com/kentakayama/libcsuit>
- Document depends on
  - SUIT manifest
  - SUIT trust domains

# What's left to-do?

- A few review comments still have to be addressed:
  - <https://github.com/suit-wg/suit-firmware-encryption/issues>
- MCR suggested to better structure the options for the deployment options.
- Feedback on “Firmware Updates on IoT Devices with Flash Memory”  
Section
  - Position Independent Code (MCR & Christian)
  - Is section informative or normative? Should it be in the appendix? Does not “age” well? (MCR, Christian, Ruud)
  - Hardware-based on-the-fly decryption (Ruud)