

Encrypted Payloads in SUIT Manifests

draft-ietf-suit-firmware-encryption

H. Tschofenig, R. Housley, B. Moran, D. Brown, K.
Takayama

Version -22 & -23

- Addressing review feedback after the Dublin IETF meeting.
- Changes:
 - Lots of wording improvements throughout the draft
 - Merged Sections 4 „Encryption Extensions“ and Section 5 „Extended Directives“ into „Excryption Extensions“.
 - Annotated examples with line numbers for better readability
 - Used coaps URIs in the examples
 - Alignment with CDDL diagnostic notation
 - Added extra security considerations to highlight padding oracle vulnerabilities.
 - Added further references
- See [diff](#) for the full details.

Next Steps

- [Github](#) repo shows two open issues:
 - [Fixed IV value zero for AES-CBC and AES-CTR #38](#)
 - [\[Review by Kris\] The reason why using CBC is safe is not clear #82](#)
 - Two PRs available, which
 - remove any text about AES-CBC since it is not part of the [SUITE MTI](#) draft, and
 - Update the text to take the IV value communicated via COSE header into account.
 - PRs:
 - [Removing AES-CBC from the description #83](#)
 - [IV Value #84](#)
 - **Ready to merge these PRs and to submit a new draft.**
- Objections?**