# A Firmware Update Architecture for Internet of Things Devices

## draft-ietf-suit-architecture-07

B. Moran, M. Meriac, H. Tschofenig, D. Brown

# Status

- WGLC on -04: https://mailarchive.ietf.org/arch/msg/suit/cu0ZbkISdgImNEdzTC-Wi1y6TEw
- -05 submitted with text about bootloaders: https://mailarchive.ietf.org/arch/msg/suit/crNN-AD-PoxpQyjFAE_4QmUcd4E
- -06 includes text relevant to TEEP based on Montreal IETF meeting: https://mailarchive.ietf.org/arch/msg/suit/cFQOwuPgFIxbNHBcL6FA86tHtVo
- Review by Kathleen: https://mailarchive.ietf.org/arch/msg/suit/utFCnP8MHkrg9-AJC9GRNngViYQ
- -07 update

# -07 Status Update

### 3.3. Use state-of-the-art security mechanisms

End-to-end security between the author and the device is shown in Section 5.

Authentication ensures that the device can cryptographically identify the author(s) creating firmware images and manifests. Authenticated identities may be used as input to the authorization process.

Integrity protection ensures that no third party can modify the manifest or the firmware image.

For confidentiality protection of the firmware image, it must be done in such a way that every intended recipient can decrypt it. The information that is encrypted individually for each device must maintain friendliness to Content Distribution Networks, bulk storage, and broadcast protocols.

A manifest specification must support different cryptographic algorithms and algorithm extensibility. Because of the nature of unchangeable code in ROM for use with bootloaders the use of post-quantum secure signature mechanisms, such as hash-based signatures [I-D.ietf-cose-hash-sig], are attractive because they maintain security in presence of quantum computers.

A mandatory-to-implement set of algorithms has to be defined offering a key length of 112-bit symmetric key or security or more, as outlined in Section 20 of RFC 7925 [RFC7925]. This corresponds to a 233 bit ECC key or a 2048 bit RSA key.

# Next Steps

- Kathleen raised the question whether the document also covers higher-end devices as well.
- Not explicitly the focus of the document but should be covered in the document.
- Is there something we can address more explicitly? What specifically needs to be done in terms of reviews/investigations?