AD Feedback update

• Most issues raised by Roman have been addressed.

• Major changes:
  • Removed guidelines on deferring signature verification (Section 6.2.1)
  • Added internationalization to SUIT_Text

• Remaining issues:
  • Defining mapping from security requirements in RFC9019/9124 to Manifest
Removed: Signature minimization

• Worked by evaluating suit-shared-sequence prior to signature check
  • Required suit-shared-sequence to have no commands with side-effects
• Under each applicability/tampering scenario, the device saves energy

• However...
  • Requires correct implementation of suit-shared-sequence limitations
  • Increases attack surface of the Manifest Processor

• Signature minimization is an implementation detail.
  • An implementer can still do this without explicit guidance: it doesn’t impact interoperability.
Internationalization (1/2)

• (RFC2277) reminds us that "Protocols that transfer text MUST provide for carrying information about the language of that text."
• SUIT_Text did not follow this guidance
• In v24, we have introduced a language-tagged map.
  • We borrowed the content of CBOR’s Tag 38
  • We applied it to a structure instead of text
  • We wrap it
• This is a breaking change.
  • v24 examples do not validate against v24 CDDL
  • Correct examples are in github and will be published with v25
Internationalization (2/2)

v23

SUIT_Text_Map = {
    SUIT_Text_Keys,
    *
    SUIT_Component_Identifier => {
    SUIT_Text_Component_Keys
    }
}

v24

tag38-ltag = text .regexp
"[^a-zA-Z]{1,8}(-[^a-zA-Z0-9]{1,8})*"

SUIT_Text_Map = {
    + tag38-ltag => SUIT_Text_LMap
}

SUIT_Text_LMap = {
    SUIT_Text_Keys,
    * SUIT_Component_Identifier => {
    SUIT_Text_Component_Keys
    }
}
IPR Status

• [https://datatracker.ietf.org/ipr/6008/](https://datatracker.ietf.org/ipr/6008/)
• Patent previously disclosed in #3799 has been abandoned.