draft-ietf-suit-manifest
Technical changes

• Add Private Enterprise Number as a vendor ID
• Separate digest from COSE_Sign/COSE_MAC
• Add CBOR tags for
  • SUIT_Envelope
  • SUIT_Manifest
• Add index lists
• SUIT Reports removed
Private Enterprise Number Vendor ID

• Supported by draft-ietf-cbor-tags-oid-03:
  • tags a byte string as the X.690 encoding of a relative object identifier
  • understood to be relative to "1.3.6.1.4.1" (PEN OID)

CDDL:

SUIT_Parameters //=(
  suit-parameter-vendor-identifier => (RFC4122_UUID / cbor-pen)
)
cbor-pen = #6.112(bstr)
PEN Vendor ID–Class ID implications

V09 said:
The RECOMMENDED method to create a class ID is:
Class ID = UUID5(Vendor ID, Class-Specific-Information)
Vendor ID must be a UUID here.
This doesn’t work if Vendor ID is a PEN.

V10:
Class ID = UUID5(
    UUID5(NAMESPACE_CBOR_PEN, CBOR_PEN),
    Class-Specific-Information
)
NAMESPACE_CBOR_PEN

Uses the OID Namespace as a starting point, then uses the CBOR OID encoding for the IANA PEN OID (1.3.6.1.4.1):

D8  DE  # tag(111)
    45  # bytes(5)
        2B 06 01 04 01  # X.690 Clause 8.19

#  1.3 6 1 4 1 show component encoding

Computing a type 5 UUID from these produces:

NAMESPACE_CBOR_PEN = UUID5(NAMESPACE_OID, h'D8F452B06010401')
NAMESPACE_CBOR_PEN = 08cfcc43-47d9-5696-85b1-9c738465760e
Remove SUIT_Digest from COSE payload

• Originally placed there for supporting PQC algorithms
  • If multiple MAC/signature structures are present, duplicate digest
  • Only need to duplicate MAC/signature structures if:
    • COSE_Sign1/COSE_MAC0
    • COSE_Sign/COSE_MAC parameters are incompatible
• Enforces that each manifest can only have one canonical digest
  • Simplifies dependency handling
    • No confusion between SHA256 dependency + SHA384 dependency that are the same manifest
    • Prevents two recipients with non-overlapping digest support from receiving identical manifests

• Item 0 in signature list is SUIT_Digest. All subsequent elements are COSE authentication structures
Add CBOR tags

• #6.48: SUIT_Envelope
• #6.480: SUIT_Manifest

• SUIT_Envelope is typically ~300 bytes with ECDSA signature
  • 3-byte tag is probably acceptable.
Index Lists

- Allows simple looping over specific components
- Extension of original index = True semantics

\text{IndexArg} /= \text{uint}
\text{IndexArg} /= \text{bool}
\text{IndexArg} /= [+\text{uint}]

- Set-component-index = [3,7,9] now possible.
- Special cases clarified: try-each, run sequence
  - Whole command is iterated over with each index set in turn
  - Try-Each, Run Sequence are invoked once for each element
SUIT_Report removed

- SUIT_Report somewhat orthogonal to SUIT_Manifest
- Factored into its own draft
Editorial changes

• Thanks to Dave for the review!
• Substantial changes across the whole draft
• Examples have removed hex-printed “bstr .cbor” elements
  • Now shows “bstr .cbor (<decoded cbor>)” instead of hex-printing