draft-ietf-suit-trust-domains-04

IETF117
July 2023

Summary

- No functional modification from v02 in IETF116

- Added SUIT Manifest examples
- Sophisticating document based on Reviews
- Going to add use case section

- In WGLC

3 Manifest Examples (1/3)

1. Key Delegation Chain
   - The Author delegates an entity to sign a Manifest
   - for those Devices who trust only Author's public key
   - by generating CWT with entity's public key signed by Author

```
/ NOTE: Signed by Author and wrapped in CWT /
{
  / cnf / 8: {
    / NOTE: public key of delegated authority /
    / COSE_Key / 1: {
      / kty / 1: 2 / EC2 /,
      / crv / -1: 1 / P-256 /,
      / x / -2:
h'0E908AA8F066DB1F084E0C3652C63952BD99F2A5BDB22F9E01367AAD03ABA68B',
      / y / -3:
h'77DA1BD8AC4F0CB490BA210648BF79AB164D49AD3551D71D314B2749EE42D29A'
    }
  }
```

3 Manifest Examples (2/3)

2. Process Dependency
   - A dependent Manifest refers dependency Manifest
   - identifying with the digest of dependency
   - As an example, this example depends on delegation Manifest

```
/ directive-set-component-index / 12, 1 / dependency manifest /,
/ directive-override-parameters / 20, {
  / parameter-image-digest / 3: << [
    / digest-algorithm-id: / -16 / SHA256 /,
    / digest-bytes: /
      h'6EA128D7BB19B86F77C4227F2A29F22026A41958ACC45CC0A35BA388B13E2F51'
  ] >>
},
/ condition-dependency-integrity / 7, 15,
/ directive-process-dependency / 11, 0,
```

3 Manifest Examples (3/3)

3. Integrated Dependency

- Composite two Manifest into one Manifest

```
  / NOTE: Example 0 /
  "#dependent.suit":

h'D86BA301589E8181589AD28443A10126A0584FA108A101A401022001215820 0E

908AA8F066DB1F084E0C3652C63952BD99F2A5BDB22F9E01367AAD03ABA68B22

582077DA1BD8AC4F0CB490BA210648BF79AB164D49AD3551D71D314B2749EE42

D29A5840FB2D5ACF66B9C8573CE92E13BFB8D113F798715CC10B5A0010B11925

C155E7245A64E131073B87AC50CAC71650A21315B82D06CA2298CD1A95519AAE

4C4B5315025874835824822F58206EA128D7BB19B86F77C4227F2A29F22026A4

1958ACC45CC0A35BA388B13E2F51584AD28443A10126A0F6584099F949043701
```

Fixed A Lot

- Fixed inconsistent terminology
  - #6, #7, #9, #11, #12, #13, #14
  - Thanks to Dave's review comments
- Fixed CDDL
  - #4, #10
- Fixed IANA Consideration
  - #8, #16

Going to add Use Case section

- Hannes raised this Issue
  - “I believe the document is missing text in the introduction to explain the use cases better. Interestingly, there is use case text in Section 6. I would move the three example use cases to the intro.”
- Brendan and I will do this soon

In WG Last Call

Reviews are welcome!