Draft-ietf-suit-multiple-trust-domains-01

Ietf 115 London

Summary

- Includes features needed in SUIT for multiple trust domains
  - Manifest signing key delegation
  - TEEP
  - Mutually distrustful signers

Summary of Features

- CWT Delegations for signing key delegation
- Unlink Command (remove a component reference)
- Uninstall Command Sequence (remove a manifest)
- Dependencies (install a manifest signed by another key)

Updates since v00

- Dependencies are no longer indexed separately from components
  - This has several implications
    - Need to handle digests of dependency manifests differently from raw components
      - Currently requires implementation-specific test.
      - A better solution is likely a separate command
    - Need test for component being dependency manifest
      - Only needed for batch processing in manifest (component index = True/array)
    - Process-dependency needs to check if it’s processing a manifest
      - Maybe not; it could just fail
- Uninstall command sequence
  - How to remove a manifest and the components/dependencies it defines.

Open Issues

- Security Considerations still needs to be done
- Component ID for root manifest?
- Condition-image requires two different behaviors
- Any others?

Component ID for root manifest

- Where should a dependent manifest be stored?
  - Single-image device: this is clear
  - Single system configuration device: this is clear
  - System with multiple independent manifests: not clear
- Dependent manifests could be given a component ID.
- How would a dependency's self-declared component ID interact with the dependent's component list?
  - Dependent's component list overrides declared component IDs
  - Designated element of dependent's component list is concatenated with dependency's self-declared component ID

Component ID for root manifest Proposal

- Self-declared component ID is optional
  - Primarily for use by systems with multiple independent ”root” manifests
- Dependent overrides self-declared component ID of dependencies
  - Simplest behavior for ”fetch” operations.