draft-moran-suit-trust-domains-00

IETF112 online

Brendan Moran

Summary

- Export of metadata from draft-ietf-suit-manifest
- Contains:
    - Delegation Chains
    - Dependencies
        - Integrated dependencies
    - Multiple SUIT processors
    - Unlink directive

TEEP Dependency

- TEEP depends on this draft for:
  - Dependencies
  - Unlink
- Contributors welcome!

Delegation Chains

- List of:
  - Lists of:
    - CBOR Web Tokens with Proof of Possession claim
- Manifest Processor starts at first CWT in each list
  - Should be authenticated by a trust anchor
  - Should provide authentication information for next CWT
  - If subject is unknown, verify signature
  - If subject is known, skip ahead
- Each CWT authenticates next CWT
- Last CWT in each list provides the public key to verify a manifest signature

Dependencies

- Originally a fundamental component of SUIT

- Heavily influenced the design of SUIT

- Allows multiple authorities to coordinate releases of independently signed manifests

- The Process Dependency directive enables a dependent to specify when to handle a dependency's commands at a per-sequence granularity

- Required to support encrypted manifests

Integrated Dependencies

- A dependency is placed in the SUIT envelope.
- Typical use is likely to be for encrypted manifests
- Integrated Dependencies are referenced by tstr, the same as any other integrated payload

Multiple SUIT processors

- Used for multiple, mutually distrustful processors in a single device
- E.g. radio module with firmware in IoT device
- Dependency prefix is used to identify the subordinate processor
- Dependency manifest is passed to the subordinate processor along with any parameters for components matching the dependency prefix
- Status information is returned (e.g. SUIT Report)

Unlink directive

- Explicitly state that a manifest no longer depends on a specific component
    - Used in TEEP to delete TAs

Open Issues

- No running code for:
  - Delegation
  - Multiple Manifest Processors
  - Integrated Dependencies

- Is the use of CWTs correct?

- Contributors welcome!