Canonical and signed TDs

Michael.Lagally@oracle.com

24.3.2021

Summary of arch-call discussions discussions on canonical TDs in architecture calls (Nov/Dec 2021)

https://github.com/w3c/wot-profile/issues/55

See also corresponding proof /ld-proof issues in other TFs:

https://github.com/w3c/wot-thing-description/issues/940

https://github.com/w3c/wot-security/issues/166

Canonical TD

A canonical form of a TD is an external representation in a well defined invariant format.

This presentation focuses on JSON, however same requirements also for CBOR, and other representation formats.

It can be used for identity checks of two TDs, cryptographic operations, …

A canonical form enables to check for identity by simple comparisons of strings or byte arrays.

Canonical TD proposal

There’s a canonical JSON serialisation that lays the groundwork.

JSON Canonicalization Scheme (JCS)

- https://tools.ietf.org/html/rfc8785

Additional rules / clarification needed on:

- default values
- Prefixes
- Array ordering
- Structural ordering, e.g. “declare before use” (@type annotation)

Arch call on 10.12.:

We prefer shortness of a TD over verbosity:

- default values MUST not be included in the canonical form of a TD
- prefixes: use the compact form

Signed TDs

- A TD where the authenticity can be validated.

Basic approach:

Calculate a cryptographic hash on a canonical TD and sign it with a trusted signing mechanism

JSON Web Signature (JWS)

https://tools.ietf.org/html/rfc7515

Defines two formats:

- JSON serialisation
- Compact serialisation

Signed TDs

- We have to select a specific signing mechanism / algorithm, may need to update to a new version when an algorithm gets broken. There needs to be an extension of the TD data model to support https://tools.ietf.org/html/rfc7515.
- As a strawman we agree to use JWE with a selected set of algorithms (t.b.d: select algorithms that have not been compromised yet and can be done on resource constrained devices)
- See: https://datatracker.ietf.org/wg/jose/documents/
- Review the algorithm choices done by CBOR (COSE) https://tools.ietf.org/html/rfc8152

Some open issues

- Self contained TDs only?
- Handling of thing models?