T2TRG/COSE/DID Joint Session

Michael McCool

28 October 2021

W3C Interest Group - Patent Policy

- This is a W3C Web of Things Interest Group meeting.
- Outside guests are permitted, however they have to agree to the W3C IP policies:
  - W3C 2017 Patent Policy
  - Patent Policy FAQ - Q6
- This is a public forum: confidential information should NOT be shared.

Agenda

See: https://github.com/w3c/wot/issues/987

- Signatures and object security (with IETF/COSE)
- Key distribution (with DID)
  - Enabler for local HTTPS and object security
  - Use of DID ids for TDs and in TDDs
  - Selection of appropriate methods
- Discovery
  - Use of DID for introductions; service name
  - Security for directories
  - Use of Core RD
  - Future work on geospatial discovery
- ASDF/TM alignment

Encapsulated JSON Signatures

- Perhaps to be renamed to "Embedded" JSON Signatures
  - Repo: https://github.com/w3c/wot-ejs
- Use case:
  - Signed (Canonicalized) TDs
  - Largish JSON-LD files
  - Want to project from MiM attacks, e.g. changes to URLs, security schemes
  - Need to support chaining
    - Adding annotations in TD Directories, e.g. for update times
    - Remapping URLs in proxies
  - Need partial signing
  - Need signature included in TD
- Capabilities of XML Signatures *seem to be* more appropriate than JWS

DID and Key Distribution

- Major pain point in HTTP-based IoT is TLS on LANs
- Mostly this is a key distribution problem
- Can be solved by using pre-shared keys, but installation of keys a nuisance for the non-expert
- Need browser support for some use cases, e.g. access to home hub dashboard across LAN
- Right now the only general solution for support of TLS that gives interop with browsers is "publicly visible URLs" and HTTPS
  - This means a cloud proxy, STUN/TURN, or other means of ISP firewall
- Is there a better way?

Other ID-Related Issues

- IDs in TDs
  - Are they the ID of the Thing or of the TD?
  - If a TD is remapped, does the ID change?
    - Different language mapping
    - URL mapping when accessed via a proxy
- Anonymous TDs
  - IDs are used a keys in TD Directories
- Privacy
  - If potentially publicly visible, IDs should not contain metadata, i.e. device type
  - Same problem with URLs
  - People do it anyway, even in our examples

DID Topics

- REC Status of DID
  - Concerns about sustainability, etc.
  - Methods that rely on extremely computationally intensive mechanisms should be avoided
- Many methods
  - Which are the best for IoT applications?
  - Need to preserve privacy, etc.
- Technical details
  - Assignment of DID Service name for WoT Things and TD Directories

Geospatial Discovery

- See https://github.com/w3c/wot-testing/issues/167
- Potential new WG Deliverable
  - Extension of WoT Discovery
- Need
  - Ontology for data encoding
  - Support for both static and dynamic data
  - Directory query extension
  - Geospatial introduction mechanisms (i.e. geo-DNS)
  - Coordination with many existing standards orgs in this area

Marked Issues

- https://github.com/w3c/wot-security/labels/T2TRG
- https://github.com/w3c/wot-security-best-practices/labels/T2TRG
- https://github.com/w3c/wot-discovery/labels/T2TRG
- https://github.com/w3c/wot-security/labels/DID
- https://github.com/w3c/wot-security-best-practices/labels/DID
- https://github.com/w3c/wot-discovery/labels/DID