Security

Michael McCool

2020 June 22

Outline

- Recent related work
  - Lifecycle
  - Use cases
- Signing TDs
  - Avoiding man-in-the-middle attacks
  - Implications for TD updates
- DIDs
  - See also discussion of DIDs in Discovery session
- OAuth2
  - Use cases and flows
- E2E Security

Related Work

- Lifecycle
  - Definition of states and credential management requirements
- Architecture
  - Alignment of stakeholder and terminology definitions
- Use Cases
  - Description of security and privacy considerations for select use cases, e.g. retail
  - To do: *All* use cases have security and privacy considerations...

Signing TDs

- Modification/spoofing of TDs is a potential security risk
  - Might enable man-in-the-middle attacks; need integrity protection
  - For example, a malicious directory service might modify URLs in the TDs it returns to redirect a Consumer to a fake Thing (acting as a proxy on the actual Thing) in order to harvest credentials (e.g. passwords)
- Mitigations:
  - Self-signing IDs (eg. DIDs including hash of TD contents)
  - Proof sections (e.g. using Linked Data Proofs)
- Implications:
  - Updating TDs is more expensive
  - IDs might change if TDs are updated
  - A lot easier to manage if TDs are "mostly static"

Decentralized IDs

Previously reviewed; see DID Working Draft

- WoT seems to fall under the "service endpoint" DID use case

Key applications:

1. Use of DIDs as IDs for TDS
   - Can include hash to confirm associated content of TDs
   - Provides stable URL for TD
2. Can be resolved to DID Document
   - Can include typed links which can be used for discovery (Introduction phase)
   - Might point directly at TDs or at directories (various Exploration services)
3. Key Distribution
   - Possible use to distribute public keys w/ referenceable URLs

OAuth2

- Proposal to re-introduce additional OAuth2 flows to TDs
  - Delegating to an external service to obtain and validate credentials makes sense in IoT context
  - Use of scopes for roles is useful – user set can change without having to update devices
  - OAuth2 depends on the use of (bearer) tokens
  - However, bearer tokens alone do not provide information on how to obtain authorization (token servers)
- Concern raised that some flows may not make sense for IoT devices
  - Issue about interpretation of some flows as requiring a "user agent"
  - Need to define use cases for all flows
  - May need to consider additional experimental flows, e.g. "device"

End-to-End Security

- New text in WoT Security and Privacy Guidelines around E2E Security
- Summary: this concept depends on the definition of "ends"
- Different "ends" lead to different definitions

Other Key Open Issues

- Review Conexxus Security and Privacy Model
  - Ensure we are aligned
- Review Lifecycle model and diagram
- Add Security and Privacy Consideration to all Use Cases
  - And ultimately, to derived Requirements