



# Onboarding

Virtual F2F March 2020

Michael McCool: Intel Principal Engineer / W3C WoT WG Co-chair

# Requirements Gathering

- What are the inputs and outputs of the process?
- What are the different states in the lifecycle?
- What are the provisioning "levels"
  - What keys and access rights need to be set?
  - When does registration with directory services happen?
  - Is registration with a directory service required?
- What is the scope of WoT for onboarding?
  - Is it handled "externally" and assumed that keys are already provisioned?
  - Do we target "automatic onboarding"?

# Provisioning vs. Registration

- Provisioning
  - Generate unique identity for a device
  - Assign keys and access rights to a device
- Registration
  - Enter device in a registry so it can be discovered non-locally or when offline
  - E.g. registration with a directory service
  - Typically will need an identity and access rights to do this

# Discussion

- Onboarding is about establishing trust
  - Key provisioning only one part
    - Establish identity (support authentication)
    - Assign access rights (support authorization)
  - Who does what?
    - Who assigns access rights?
    - Who is the user? Is there a separate administrator?
    - Relate to “stakeholders/roles” terminology in use case definitions
  - Processes
    - Specific approaches/technologies (“onboarding tool”) vs. abstract framework (“oauth2”)
  - WoT support needed
    - Security metadata in TD – requirements
    - Keywords to describe onboarding process used?
    - References to public keys, eg via keys? Need signed TDs to do this securely.
    - Look at DID – align stakeholder terminology
    - How to handles changes in operational state, eg reboots? Look at existing ecosystems...

# Concerns

- How to deploy
  - What features should be supported in reference implementation, eg. node-wot
- Need recommended best practices for
  - Onboarding
  - Access controls
    - Including support for roles/scopes
  - Authentication