

# WoT F2F Dusseldorf

Security sessions agenda

12-13th July 2017

# Overview of sessions

- **Security Use Cases and Scenarios (1.5 hours)**
  - Build a list of important high level security use cases/scenarios
  - Define at least 3 WoT security levels based on it
  - July 12<sup>th</sup> Time: TBD
- **Existing/Proposed Security Architecture (0.5 hours)**
  - Review existing WoT security mechanisms and their purpose
  - Align them with the threat model
  - July 13<sup>th</sup> Time: TBD
- **Privacy (1 hour)**
  - Review WoT publicly accessible privacy-sensitive data
  - Build a list of privacy-sensitive use cases-scenarios
  - July 13<sup>th</sup> Time: TBD

# Security Use Cases and Scenarios

- 1.5 hours slot
- July 12<sup>th</sup> 9am
- Session goals:
  - Build a list of important high level security use cases/scenarios
    - Home user equipment WoT network behind standard firewall?
    - Business office facility WoT network?
    - Factory automation WoT network?
  - Define at least 3 WoT security levels based on it
    - Home?
    - Corporative?
    - Industrial?

# Existing/Proposed Security Mechanisms

- 30 minutes slot
- July 13<sup>th</sup> 9am
- Session goals:
  - Review existing WoT security mechanisms and their purpose
    - TD's optional security parameter
    - Security elements in Scripting API
  - Align them with the threat model
    - What are the threats each mechanism tries to address?

# Privacy

- 1 hour slot
- July 13<sup>th</sup> 9:30am
- Session goals:
  - Review WoT publicly accessible privacy-sensitive data
    - In TD
    - In Scripting API
  - Build a list of privacy-sensitive use cases-scenarios
    - Possibly for the same 3 different security levels:
      - Home, Corporative, Industrial