fido™ ALLIANCE | simpler stronger authentication

# FIDO IoT and RATS/EAT

Giri Mandyam, FIDO IoT Working Group Chair

# Overview

- The Fast Identity Online (FIDO) Alliance is a standards/certification body focused on passwordless authentication
  - Several standards enabling user authentication (incl. biometrics)
  - Security and functional certification programs
- Recent standards effort on IoT secure onboarding
- First specification released in August 2020
  - https://fidoalliance.org/specs/fidoiot/FIDO-IoT-spec-v1.0-wd-20200730.html

# What Does Onboarding Entail?

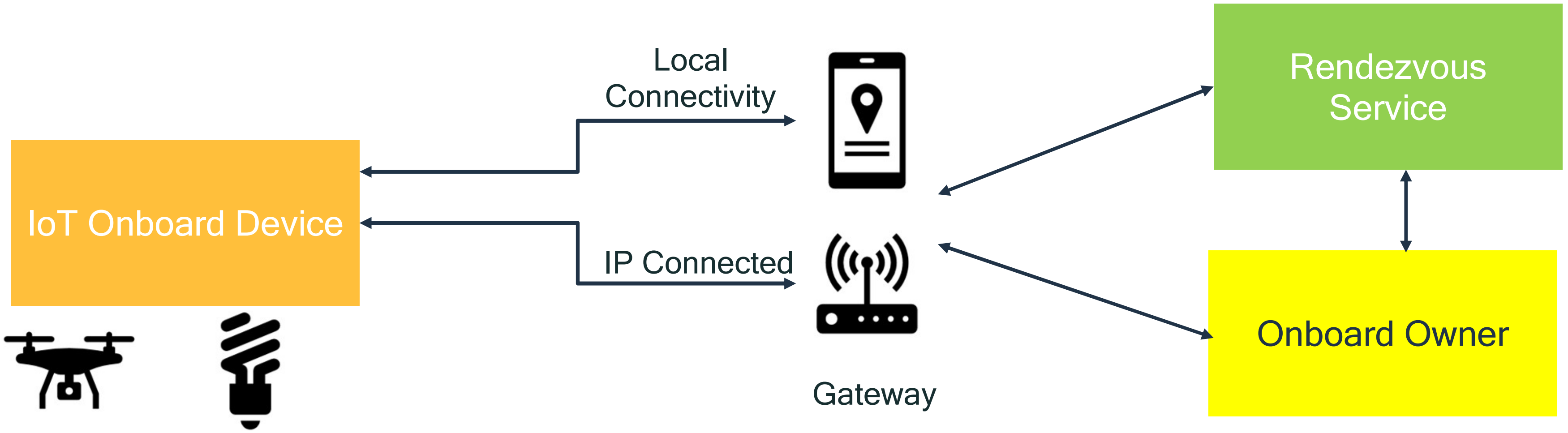
- 3 primary steps
  - ①OEM completes manufacturing of device and ships
  - ②End user purchases device, installs it, and powers it up for first time
  - ③End user establishes ownership relationship with device
- “Zero-touch” onboarding is a goal for most manufacturers
  - User powers up device for the first time – is able to establish ownership with minimal intervention
- Common approaches could entail
  - ①Installing an app on a personal device (tablet, smartphone)
  - ②App connects to cloud – user authenticates to onboarding service
  - ③App connects to IoT device
  - ④Ownership established via cloud service

# Attestation in Onboarding

## What is attestation?

- Describes the process by which software executing on a device provides an assertion to a relying party about the integrity of its platform
  - *Relying party* is any service provider that consumes the attestation produced by a device, usually as part of some transaction
  - In the case of IoT device onboarding, both the Rendezvous Server and Device Owner can be Relying Parties
- The attestation can be based on several criteria, including
  - An assessment of the operating system kernel
  - Enumeration of 3rd-party applications installed on device
  - Suspicious events such as protected memory access
- Attestation data is formed by combining indications of such payload into a compact data structure that can be sent to a relying party
  - Attestation data is used to form an attestation statement, which is the actual message sent to the relying party
  - Attestation statement should be cryptographically-verifiable (signed and/or encrypted)

# FIDO IoT System Architecture



# Protocols

- Device Initialization (DI)
  - Provisioning IoT device with security-related information during manufacture
- Transfer Ownership Protocol 0 (TO0)
  - Device Owner seeds information in the Rendezvous Server about the IoT device to be onboarded (unique ID, i.e. GUID) and owner's IP address
  - ***Attestable***
- TO1
  - Device contacts and identifies itself to rendezvous server
    - Upon first power up after manufacture or after a factory reset
  - ***Attestable***
- TO2
  - Device contacts owner.  Owner takes over device management.
  - ***Attestable***

# EAT Dependencies

- T01 and T02 leverage EAT
- Minimum required claims
  - Nonce
  - UEID
- FIDO intends to complete standard and launch interop/certification program
- What is the issue?
  - EAT standard is not complete
  - EAT-proposed claims are not registered
  - FIDO cannot complete standard and launch interop/certification program using CWT private space
    - See https://www.iana.org/assignments/cwt/cwt.xhtml
    - Certification must be done on finished product
      - Vendors will prefer to productize with registered claims, not private space

# Request

- EAT spec not ready for Last Call as of IETF 109
- FIDO requests accelerating that IETF register a minimal subset of the claims outlined in the current EAT draft with IANA
  - Register claims prior to RFC publication
- Determine minimum set of claims and complete registration no later than IETF 110