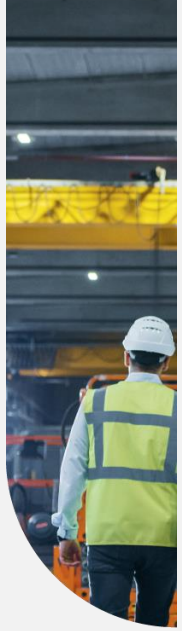


FORTINET

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021

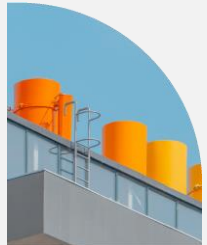
FIDO Device Onboard – a new industry standard that addresses the insecurity and cost of installing IOT devices.

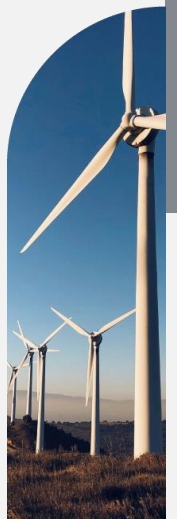
Richard Kerslake

Industrial Controls and Robotics | Intel

fido alliance

intel





How long does it take to manually onboard[1] 10,000 Gateways, Devices, Sensors?

Answer:

Over 2-man years[2]

1. Assumes out-of-box to securely streaming data to an IoT Platform
2. Kaiser Associates Research and Analysis, IoT study, August 2017

The Onboarding Challenge

- Manual installation requires trusted and skilled staff
- Manual installation adds cost and time to IOT deployments, impacting program ROI
- Wide variety of IOT devices – hardware and Operating Systems
- Most devices headless (i.e. don’t have displays)
- Different connectivity – wired / wireless

Onboarding solutions today

Onboarding solutions exist today, but don’t fully meet the needs of the industry

- **Manual onboarding**
  - Slow
  - Insecure
  - Expensive

- **Proprietary ‘zero touch’**
  - Linked to one cloud/platform
  - Only one silicon provider
  - Require programming of target platform/cloud/user at manufacture

The FIDO Alliance brings together the world's leading technology companies to develop and promote the adoption of a standardized, simpler, and more secure online experience that installs trust and confidence in a digital world.

Backed by global tech leaders

+ Sponsor members

+ Associate members

+ Liaison members

Track record of successful collaboration

- 3 Sets of Specs Released

fido™ UAF fido™ U2F fido2

- Growing Platform Support




- Increasing Market Adoption

IBM TARGET Microsoft docomo mastercard verizon

intuit NHS CVSHealth ebay

FIDO Alliance IOT Tech WG

FIDO IOT Charter: *"The IoT TWG has been established to develop use cases, …,* ***automated onboarding, and binding of applications and/or users to IoT devices****, …"*

First F2F meeting: July 2019
45 IoT Use Cases Presented

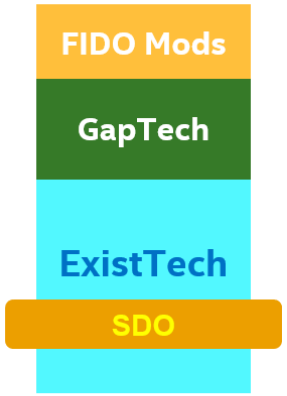
Attendees: 4 CSP's / 6 Chip companies

Google	Arm	Lenovo
Microsoft	Intel	NXP
RSA	AWS	eWBM
Qualcomm	Infineon	Device Authority
Alibaba	Phoenix Technologies	

Plenary, September 2019
Derived Requirements from Use Cases

R1	Open Solution
R2	Automatic Onboarding
R3	Authorization (to onboard) is end-to-end
R4	Communications Independence
R5	Late Binding
R6	Permits Supply Chain Flexibility
R7	Repurpose / Resale
R8	Limit Correlation Attacks (Breadcrumbs)
R9	Deferred Acceptance
R15	Trusted and Untrusted Installer
R16	Localized authentication
R17	Internet, Home, Enterprise & Closed networks
R18	IOT Owner need not be Network Owner
R19	Target device range (CPU/RAM/UI/OS etc.)

F2F meeting: Dec 2019
SDO moved to working draft



FIDO IOT TWG: March 2021
FDO 1.0 PS (FIDO standard level)

FIDO Device Onboard Specification

Proposed Standard, March 23, 2021

This version:
https://fidoalliance.org/specs/FDO/fido-device-onboard-v1.0-ps-20210323

Issue Tracking:
GitHub

Editors:
Geoffrey Cooper (Intel)
Brad Behm (Amazon)
Ankur Chakraborty (Google)
Hanu Kommalapati (Microsoft)
Giri Mandyam (Qualcomm)
Hannes Tschofenig (ARM)

Contributors:
Witali Bartsch (TrustKey)

https://fidoalliance.org/specifications/download-iot-specifications/

Fast, Scalable Device Provisioning, Onboarding & Activation

Drop ship device to installation location

Power-up & connect to Network

Auto-provisions, Onboards to Cloud

BENEFITS[1]

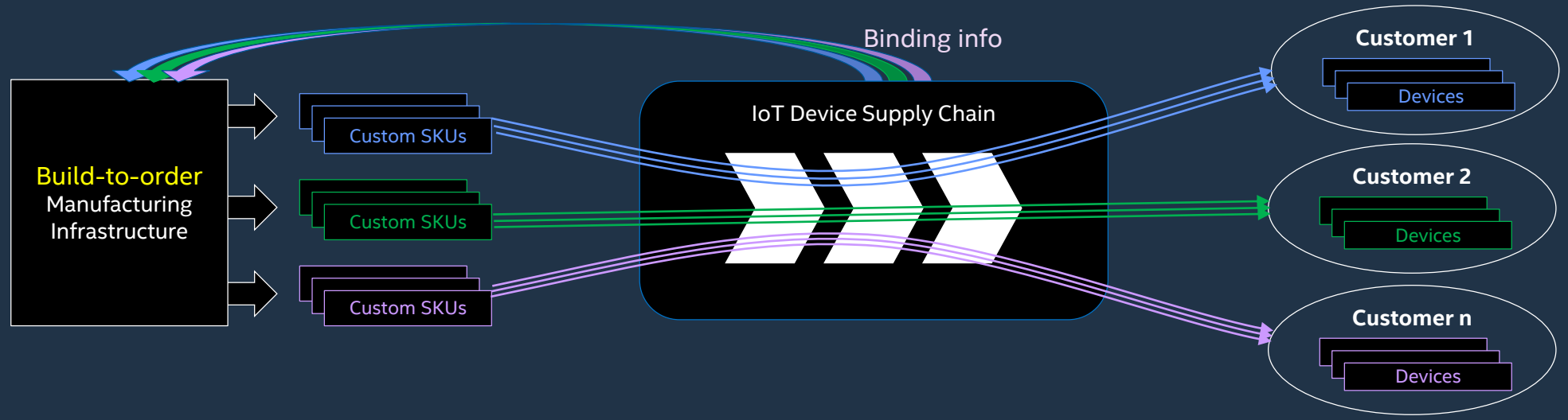
- Zero touch onboarding – integrates readily with existing zero touch solutions
- Fast & more secure[1] – ~1 minute
- Hardware flexibility – any hardware (from ARM MCU to Intel® Xeon® processors)
- Any cloud – internet & on-premise
- Late binding - of device to cloud greatly reduces number of SKUs vs. other zero touch offerings
- Open - LF-Edge SDO project up and running. FDO 1.0 code now on GitHub

1. No product or component can be absolutely secure

FIDO Device Onboard: Late Binding in Supply Chain

Zero Touch without FDO
IoT device software and security customization happens during manufacturing

Result:
Complicated build-to-order manufacturing infrastructure, many SKUs, small lot sizes, long lead times, higher cost

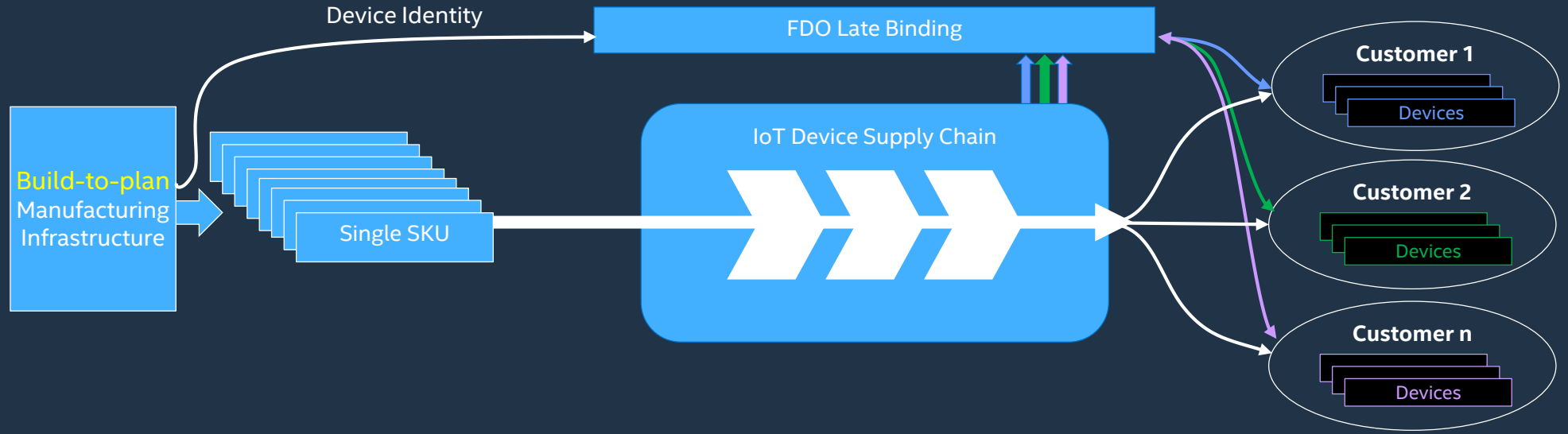


Zero Touch with FDO
IoT device software and security customization happens at the end of the supply chain

Benefits:

Simplified build-to-plan manufacturing infrastructure, fewer SKUs, large lot sizes, enable stocking distributors, low customization cost

Result: *Increased supply chain volume and velocity*

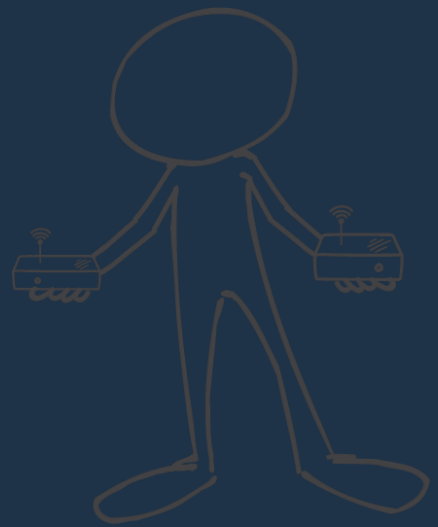


Late binding reduces costs & complexity in supply chain – a single device SKU for all customers

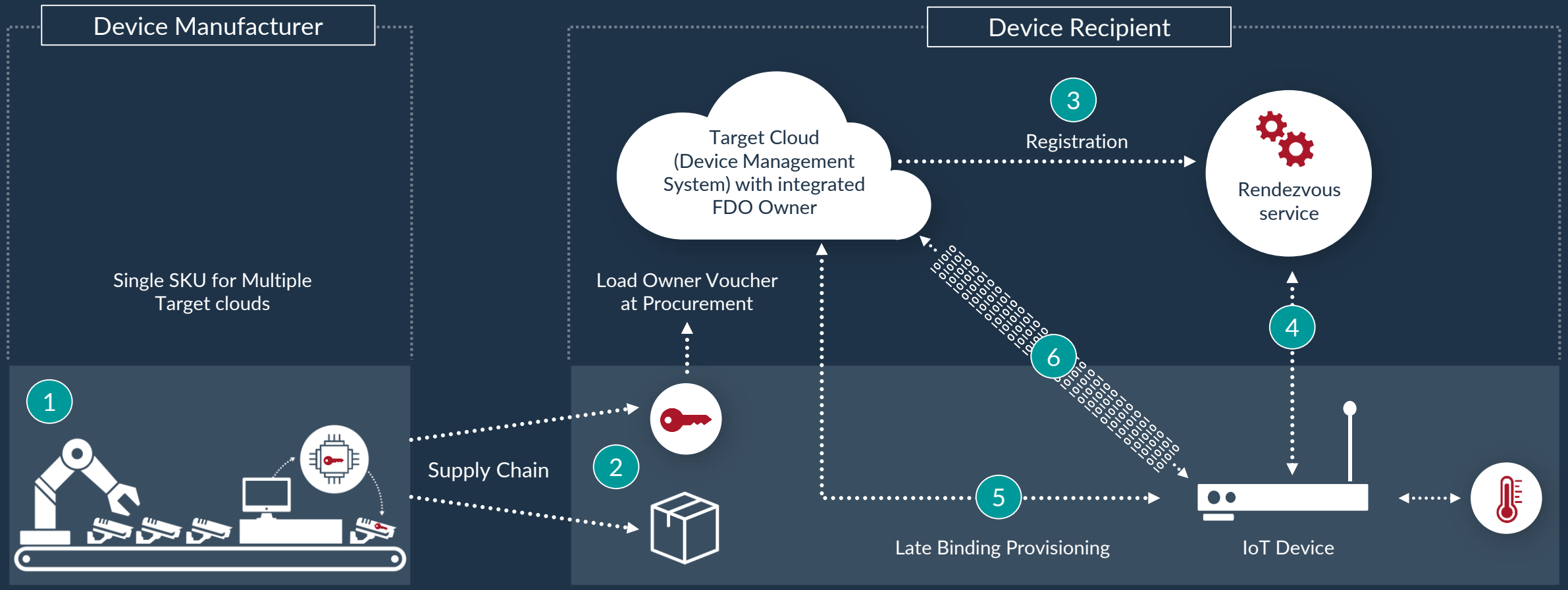
Aligning FIDO IOT to Use Case and Ecosystem

Use cases where FIDO IOT delivers maximum value

- Industrial and Enterprise devices:
  Gateways, servers, sensors, actuators, control systems, medical, etc.
- Multi-ecosystem applications and services:
  not tied to specific cloud/platform framework
- Distributor sales:
  deliver from stock, specify binding info after sale to customer
- Device resale / redeploy:
  reset to factory conditions repeat onboarding process with new credentials

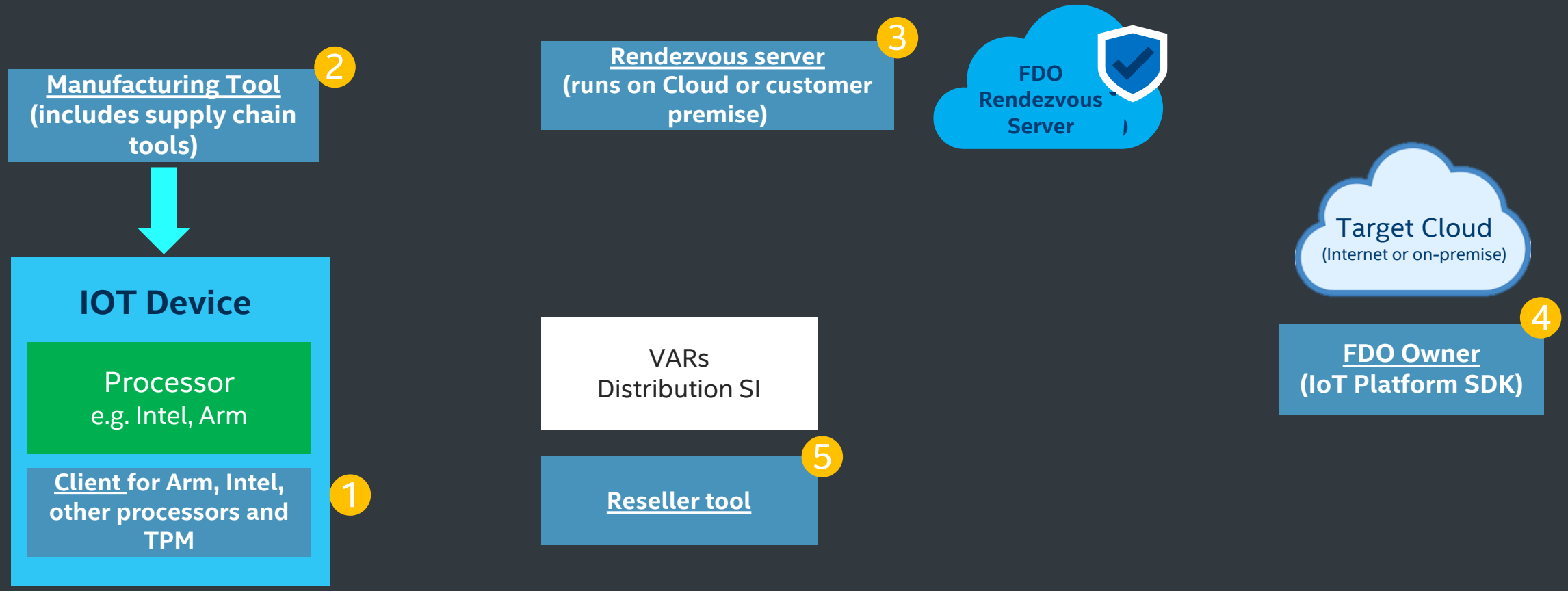


How FDO Works

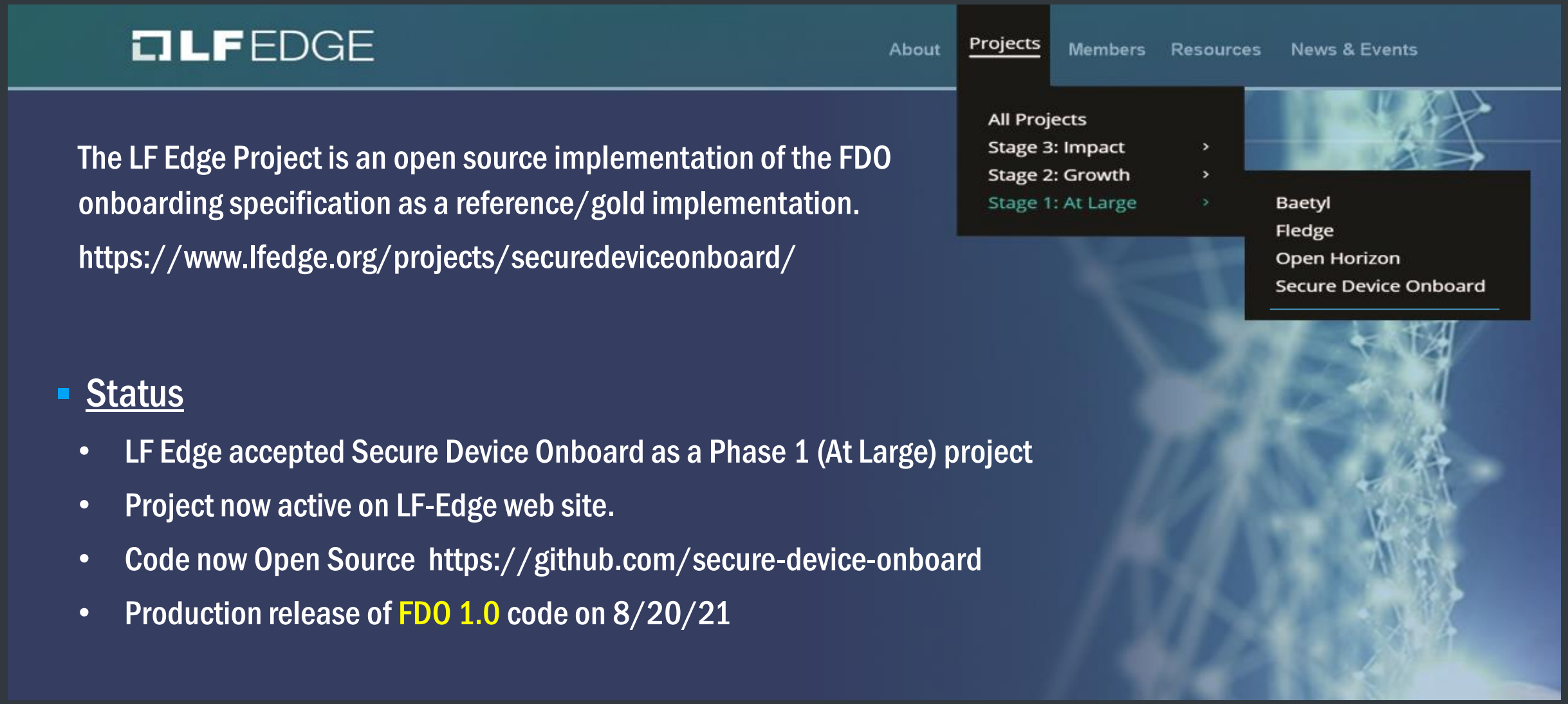


1. Build and Ship FDO Enabled Devices
2. Register Ownership to Target Platform
3. Register Device to Rendezvous Service
4. Devices use FDO to find owner location
5. Devices Authenticated and Provisioned
6. Devices send sensor data to IoT Platform

FDO – Major Software Components



FDO/SDO: LF-Edge project & Open Source



The LF Edge Project is an open source implementation of the FDO onboarding specification as a reference/gold implementation.

https://www.lfedge.org/projects/securedeviceonboard/

- **Status**
  - LF Edge accepted Secure Device Onboard as a Phase 1 (At Large) project
  - Project now active on LF-Edge web site.
  - Code now Open Source https://github.com/secure-device-onboard
  - Production release of FDO 1.0 code on 8/20/21

Certification and Security

- FIDO has an established security certification program for existing FIDO authenticator specifications (UAF, U2F, FIDO 2.0/Webauthn)
  - Levels that correspond to achievable security assurance
    - **L1** – Based on vendor questionnaire
      - SW authenticators, e.g. from an app store
    - **L2** – Design documentation submitted by vendor and assessed by 3rd-party certification lab
      - Authenticators developed in a trusted SW environment
    - **L3** – Sample device submitted to 3rd-party lab for verification of design and additional penetration testing
      - Authenticators instantiated in a secure element

Using FDO and Intel Bare Metal Onboard option for “SKU in Place” imaging

Bare metal device
(HW Only)

Imaging Station
(Light Linux + FDO Agent)

Download image
(SW image, OS, VM etc.)

FDO setup kit

Ship for imaging

Ship to point of installation

FDO imaging

IOT device

Bare metal device

Image device with FDO + Linux (OEM or SI, any location)

Onboard device and download customers target SW image

Goals for 2021

- Drive industry adoption by building broad industry support across End users, OEMs, ODMs, silicon partners, etc.

- Launch FDO certification programs later this year.
  - Functional certification/interop testing
  - Security certification testing

- Continue work on v.next based on implementation feedback and to address additional requirements

OPERATIONAL TECHNOLOGY
SYMPOSIUM 2021

Q&A

Thank you.

Richard Kerslake

OPERATIONAL TECHNOLOGY SYMPOSIUM 2021