fido™ ALLIANCE | simpler stronger authentication

FIDO Alliance Solving The IOT Onboarding Challenge

April 2022

Richard Kerslake and Team Intel

Fast, Scalable Device Provisioning, Onboarding & Activation

Drop ship device to installation location

Power-up & connect to Network

Auto-provisions, Onboards to Device Management Service

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 FDO project up and running, code now on GitHub
- Provision your choice of OS on bare metal COTS Hardware

1. No product or component can be absolutely secure

2

FIDO Device Onboarding Terms

FIDO device onboarding is a flexible software solution that simplifies and automates the process of **onboarding** IoT devices.

- **Onboarding** is the process by which a device establishes a trusted connection with a service or a platform
- The device is onboarded to “something.” That “something” can be an orchestration cluster, device management system or an OS provisioning system

The Onboarding Challenge

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

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

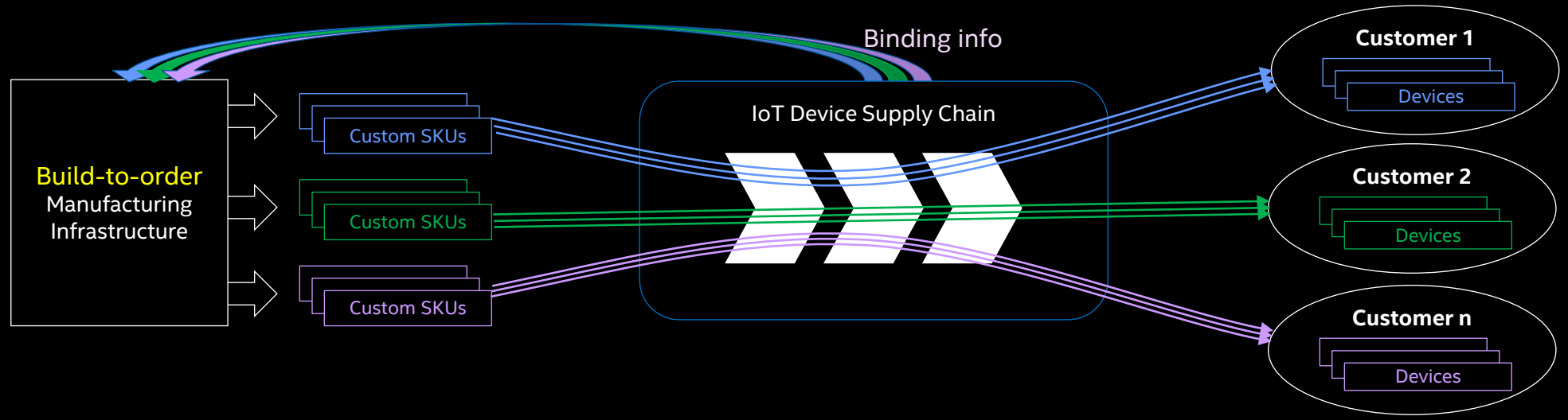
IBM TARGET Microsoft docomo mastercard verizon

intuit NHS CVS Health ebay

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

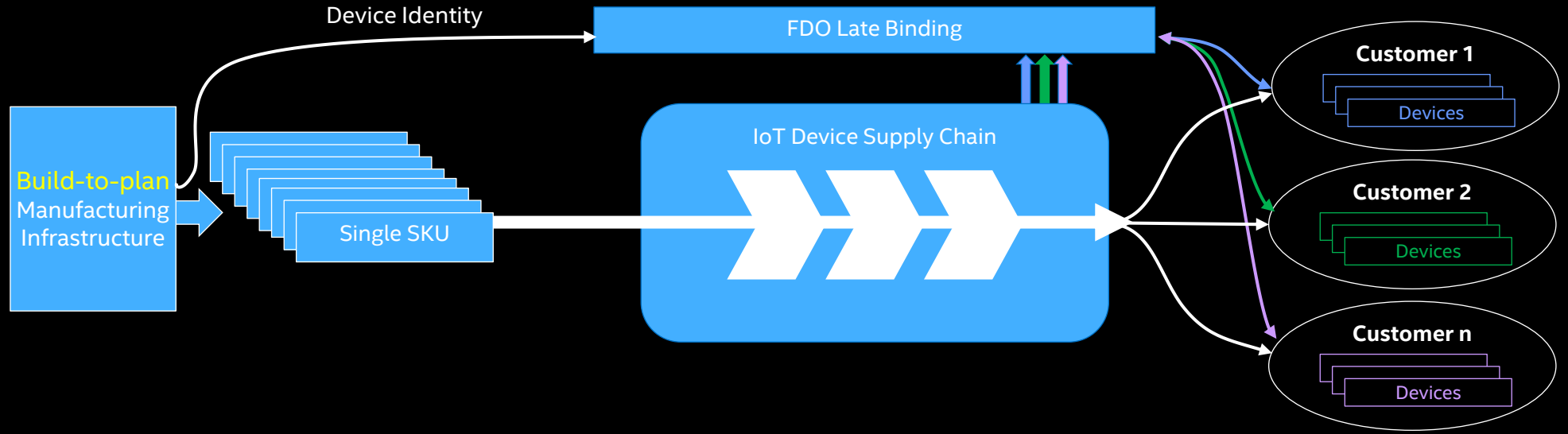


Zero Touch with FDO
IoT device software and security customization happens at the end of the supply chain

Benefits:

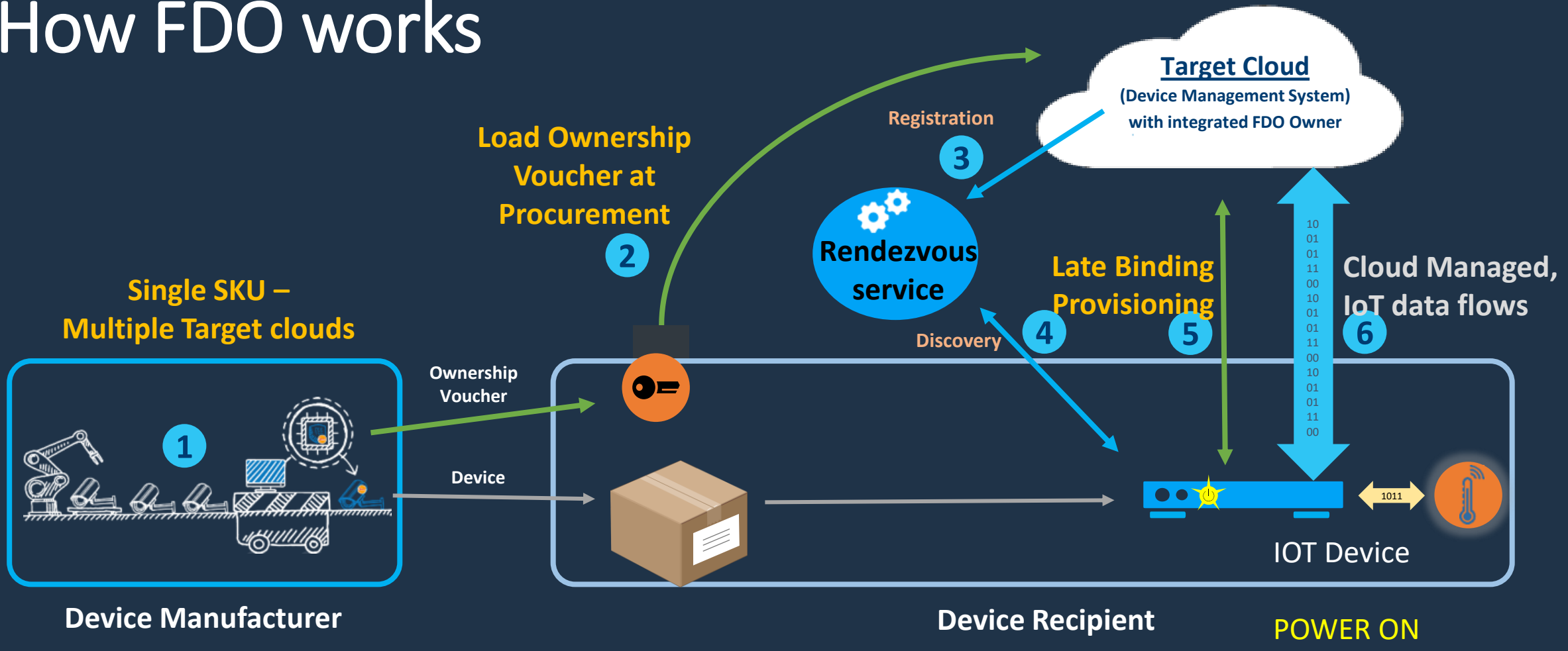
Simplified build-to-plan manufacturing infrastructure, fewer SKUs, large lot sizes, enable stocking distributors, low customization cost

Result: *Increased supply chain volume and velocity*



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

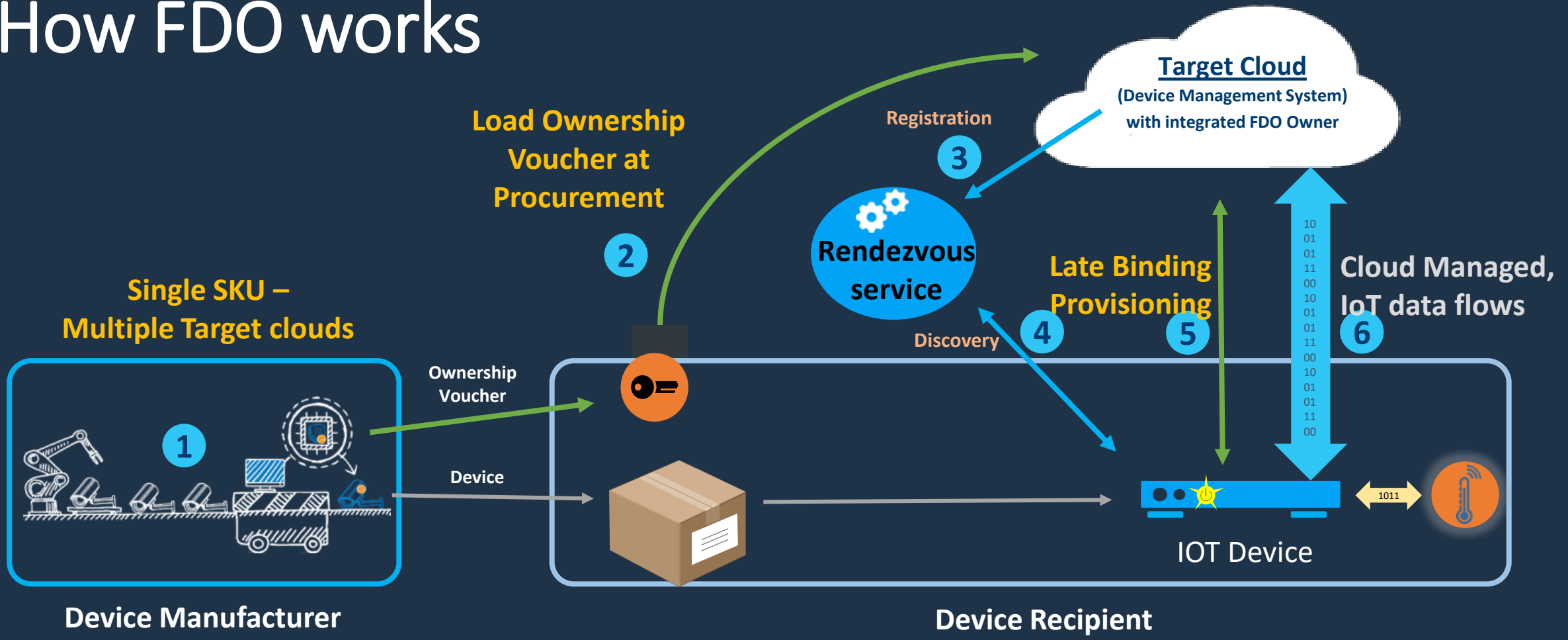
How FDO works



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

Device manufacture – supply chain | Device power on | Device deployed

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

Device manufacture – supply chain | Device power on | Device deployed

FDO – Major Software Components

Rendezvous Server
(Internet or on-premise)

Management
Platform
(Internet or on-premise)

Manufacturing Tool
(includes supply chain tools) 2

Rendezvous server
(runs on Cloud or customer premise) 3

IOT Device

Processor
e.g. Intel, Arm

Client for Arm, Intel, other processors and TPM 1

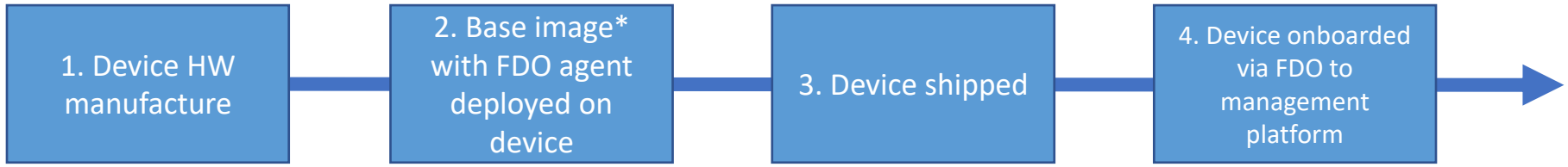
VARs
Distribution SI

Reseller tool 5

FDO Owner
(IoT Platform SDK) 4

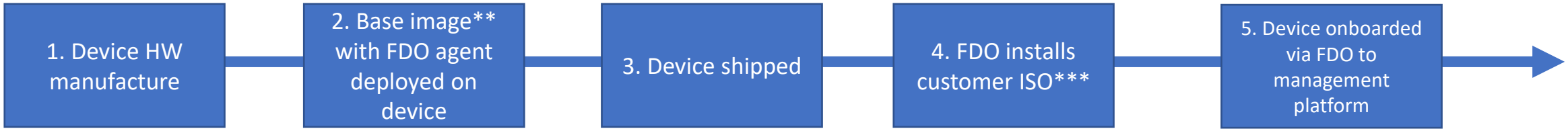
FDO Deployment models

A. Baseline FDO deployment model



* Base image is full customer ISO i.e. Linux + Customer application + FDO Agent

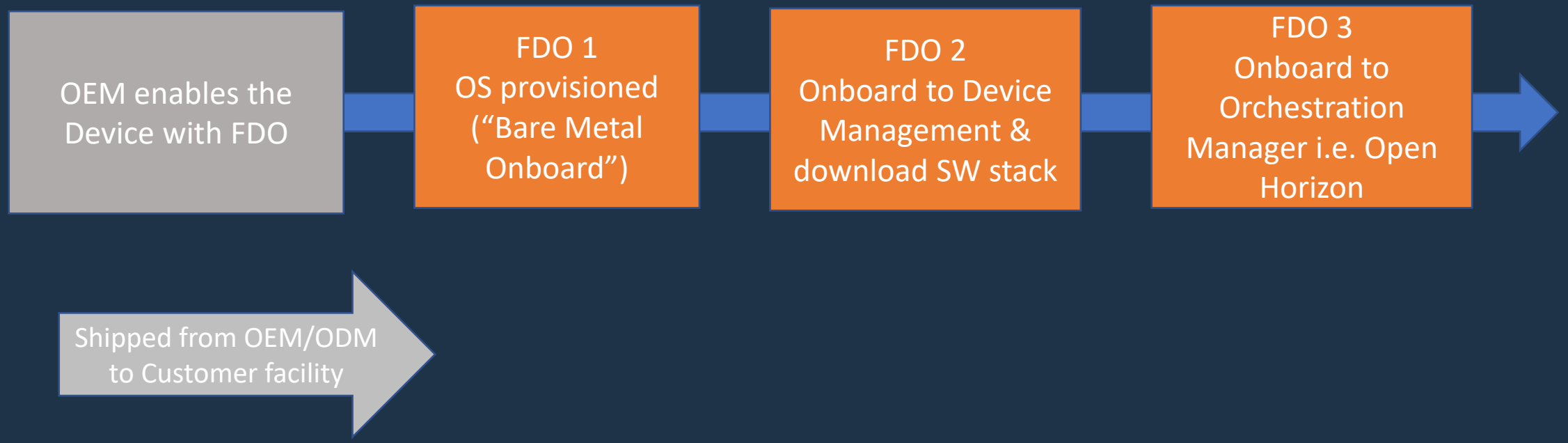
B. FDO with BareMetal deployment model



** Base image is Minimal OS + FDO Agent. Runs from RAM on boot up.
ESP used to create Minimal OS

*** Base image in Stage 2 is the same regardless of the final customer ISO chosen

Intel Multistage FDO Onboarding concept for Customer



FDO – Major Software Components

CATEGORY	DESCRIPTION
FDO Client-Intel & other CPU 1	Client-Intel, Client-SDK • Software that runs on devices to perform FDO protocols (DI, TO) • Available for both Intel and non-Intel devices
FDO Manufacturer Toolkit 2	Manufacturer (used by OEM/ODM or any entity that performs DI) • FDO Device Initialization (DI) • Ownership Voucher Generation • Public Key import and storage • Extension of Ownership Vouchers
FDO Reseller Toolkit 5	Reseller (used by distributors, VARs and resellers) • Extension of Ownership Voucher • Ownership voucher import and storage • Public Key import and storage
FDO Rendezvous Service 3	The FDO Rendezvous service receives Ownership Voucher registration requests from the FDO Owner (TO0). The FDO Rendezvous Service verifies the necessary credentials from the FDO Device and provides necessary information to the FDO Device (TO1) to connect to the FDO Owner (TO2) . • The FDO Rendezvous service is packaged as a Docker container and can be deployed on cloud or on-premises including closed networks • The Rendezvous Service also provides the option to allow and deny requests based on the owner, manufacturer and reseller public keys and based on the GUID used in the Device Ownership Voucher header.
FDO Owner 4	FDO Owner Onboarding Service is used by the final owner in the chain to provision the device and control is across a network using a Manager. • After the protocols are completed, the Owner Onboarding Service transfers control of the device to the Owner's Management Service (DMS). • The FDO Rendezvous service receives Ownership Voucher registration requests from the FDO Owner Onboarding Service (TO0). The FDO Rendezvous Service verifies the necessary credentials from the FDO Device and provides necessary information to the FDO Device (TO1) to connect to the FDO Owner (TO2) . The Owner (TO2) has received Ownership Voucher and transfer of ownership is complete. • All the device credentials are then replaced with the owner's credentials except for Device attestation key. • The FDO Owner is packaged as a Docker container.

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

fido™ ALLIANCE | simpler stronger authentication

Questions