



LIS25-200K3

Introducing the FIDO Device Onboard (FDO) specification

Richard Kerslake – FIDO Alliance



What is the FIDO Alliance?



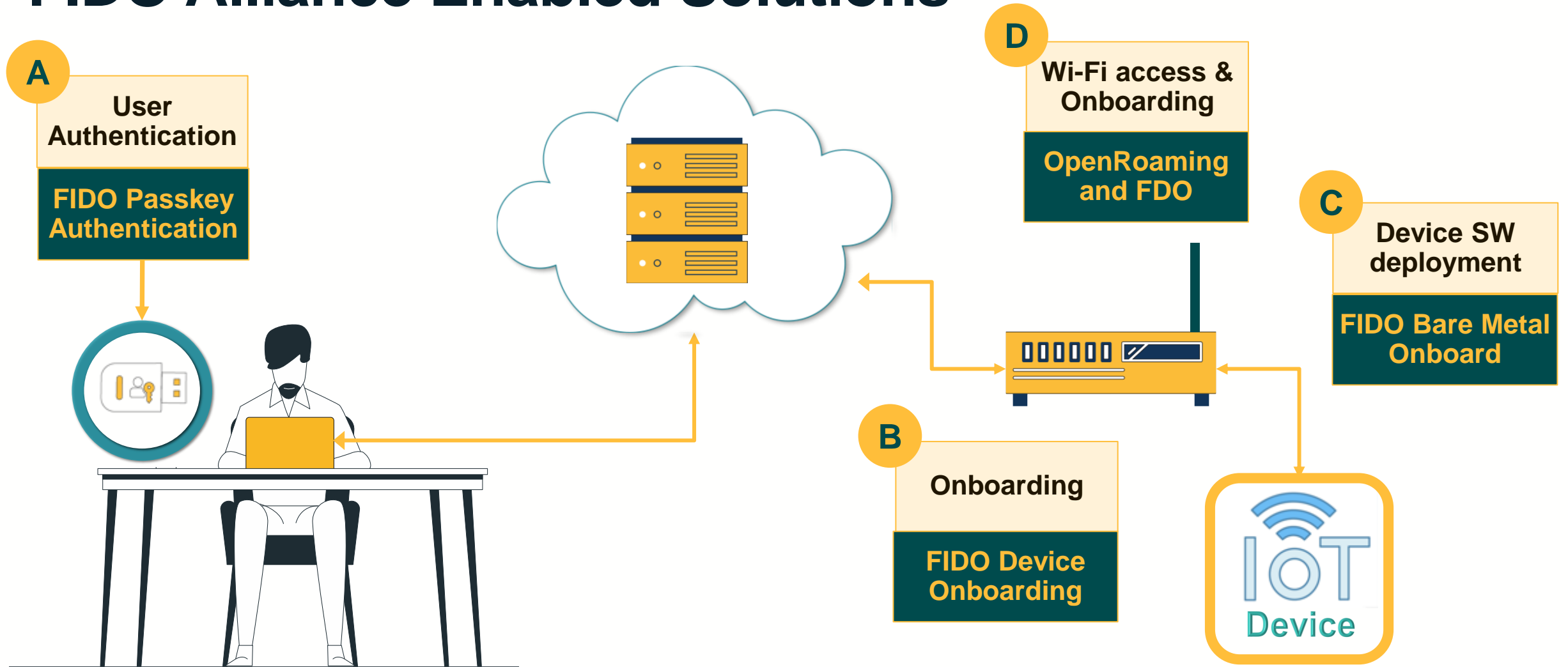
The FIDO Alliance is an open industry association with a focused mission: **reduce the world's reliance on passwords.**

We have 350+ members from around the world.



We created passkeys.

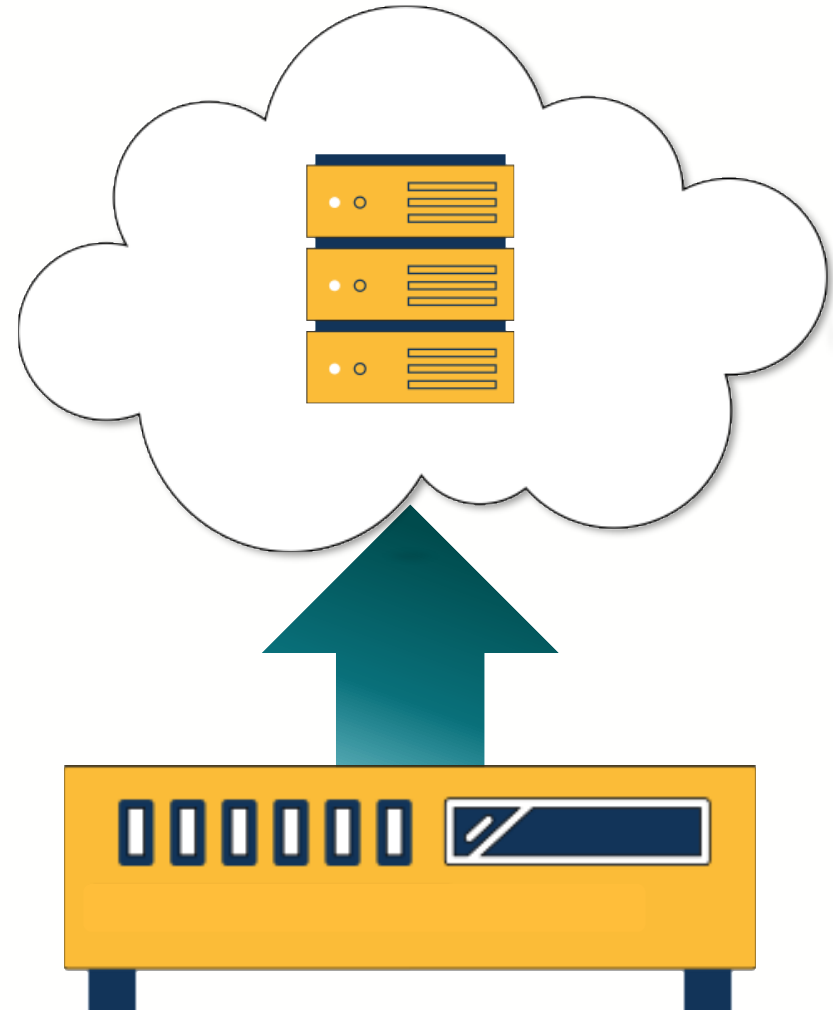
FIDO Alliance Enabled Solutions



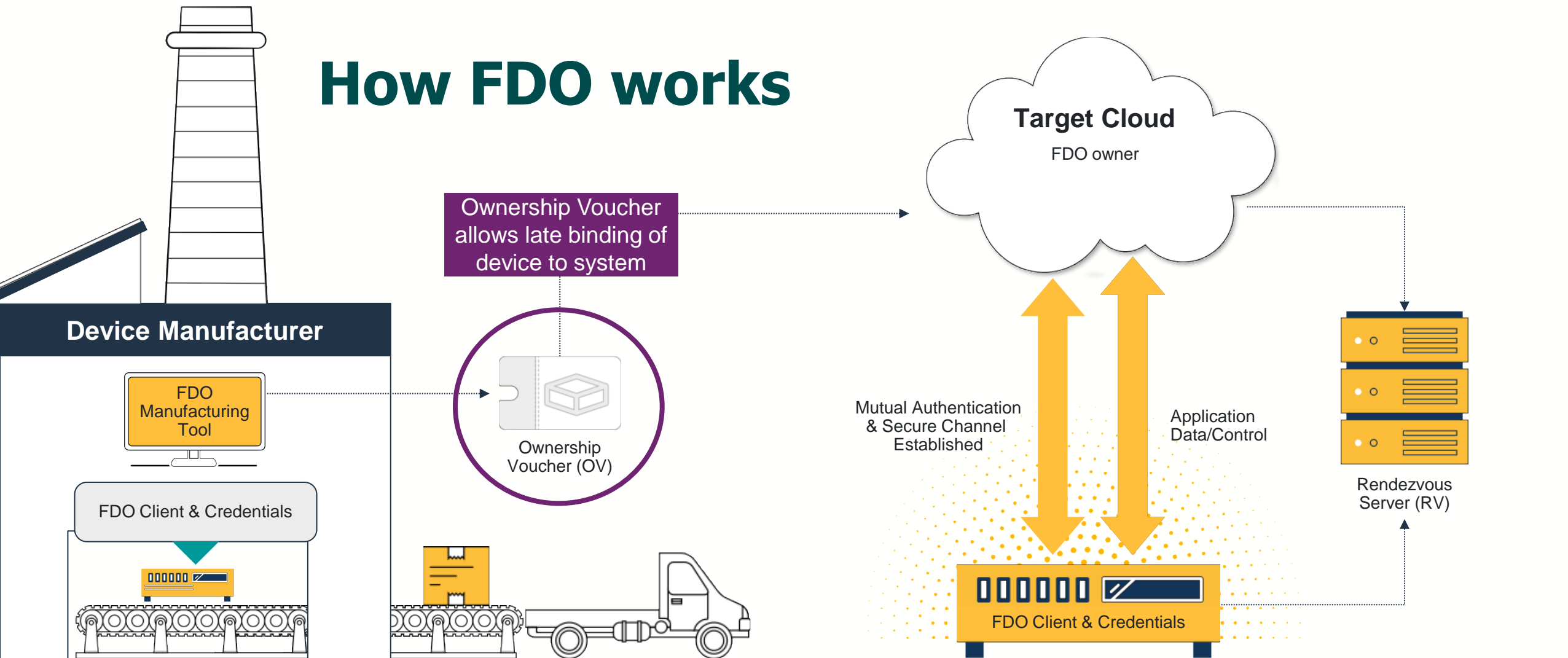
FIDO Device Onboard (FDO)

What problem does FIDO Device Onboard (FDO) solve?

- When a device is being installed in a facility, it must be “onboarded” to its management platform (on-premise or cloud).
- FDO provides secure “plug and play” onboarding for almost any device/network.



How FDO works



- 1 FDO agent & FDO credentials placed in device
Ownership Voucher (OV) created
- 2 Device in box shipped to installation location
- 3 Load Ownership Voucher (OV) to Cloud
- 4 Register OV with Rendezvous Server
- 5 Device given network connectivity and powers up
- 6 Device contacts RV and is re-directed to Cloud
- 7 Mutual authentication takes place
Secure channel is established
Onboarding takes place using FSIM's
- 8 Cloud Managed, Device data flows

FDO ServiceInfo Modules (FSIMs) are subprotocols within the FDO protocol to define secure and flexible configuration of credentials and data during device onboarding


- FDO creates secured attested tunnel and runs FSIM's over it.
- Owner (server) uses FSIM's to credential the device for the target application.
- FSIM examples: command execution, file upload/download, and PKI provisioning using a certificate signing request (CSR).

FSIMs


Standard FSIMs can be augmented with custom application-specific FSIMs

FDO Ecosystem moment

Microsoft



Azure Edge Infrastructure
Resilient Edge Deployment with Azure Arc and FIDO Device Onboarding



Gerardo Diaz Cuellar
Microsoft

Azure Local
Enabled by Azure Arc

Dell



The edge
where data is acted on near its point of creation to generate immediate, essential value



Jenna Tartaglino
Consultant Product Manager - Edge, Dell EMC

Authenticate Virtual Summit:
Securing the Edge and Connected Devices with FDO
Dec. 14, 2023

Securing the Edge with FDO

ASRock

FIDO-enabled IPC Solutions in Industrial Applications



Process Automation
Factory Automation
Water Agency
Smart Factory Patrolling
Charging Station

FIDO-enabled Industrial PC Solutions
IEP-7020E Series
IEP-5010G Series


Wireless Broadband Alliance

ExxonMobil

Commercialization Strategy

Adoption and Scale-up Plan:


- First commercial OPA deployment in 2024: Demonstrate system capability, performance and support model
- Smaller, lower complexity OPA aligned solutions in 2024/2025: Drive experience curve and cost reduction
- Developing an ecosystem of commercially available solutions for medium/complex projects



Support Ecosystem Development:

- Engage Suppliers to screen and develop opportunities (near term: PLC and SCADA-type projects)
- Collaborate with End Users to create demands of OPA aligned solutions
- Support Industry associations to develop OPA standards (OPA Forum, UAO, PICMG, NAMUR, IOGP, etc.)

ExxonMobil
Document Number: 2024-071-518



Kelly Li
Exxon

Red Hat

Red Hat Summit May 19-22, 2025

Why attend Pricing Sponsors Register

Red Hat

Secure the supply chain with FDO: The future of device onboarding for industrial IoT

As IoT in industrial environments becomes commonplace, securely onboarding devices has become a critical challenge. This technical session introduces FIDO Device Onboarding (FDO), an open standard developed to simplify and secure deployment of IoT devices at scale. Red Hat leverages FDO to provide automated and secure onboarding, minimizing manual configuration, and reducing the time and complexity of provisioning. During this talk, you'll learn how FDO enables zero-touch deployment, integrates with existing IT and OT infrastructure powered by Red Hat platforms, and provides organizations with a streamlined path to deploy industrial IoT devices while mitigating security risks throughout the supply chain. You'll also learn the practical benefits of FDO adoption to address the requirements of complex device deployment for the oil and gas, manufacturing, automotive, and other industries, and best practices and strategies for organizations looking to adopt FDO.

Richard Kerslake, Connected Standards Market Development Manager, FIDO Alliance



Wireless Broadband Alliance



OpenRoaming for IoT
FIDO Device Onboard Framework

Source: Wireless Broadband Alliance
Artifact: OpenRoaming for IoT & FIDO Device Onboard Design
Issue Date: November 2024
Version: 1.1.0
Status: Public

Microsoft present Azure Edge at Ignite



[Link to all Workshop videos](#)

The screenshot shows a presentation slide for Microsoft Azure Edge Infrastructure. The slide has a dark blue background with a light blue cloud icon and a network diagram at the bottom. The text on the slide includes the Microsoft logo, the title "Azure Edge Infrastructure", the subtitle "Simplifying Edge Deployments with Azure Arc and FIDO Device Onboarding", and the names of the presenters: "Gerardo Diaz Cuellar" and "Principal Software Engineer Architect". A video inset in the top right corner shows Gerardo Diaz Cuellar, a man with grey hair wearing a red shirt, speaking. Below the video inset is a yellow banner with the text "Gerardo Diaz Cuellar" and "Microsoft". The FIDO Alliance logo is in the bottom right corner of the slide.

Microsoft

Who were?

Azure Edge Infrastructure

Simplifying Edge Deployments with Azure Arc and FIDO Device Onboarding

Gerardo Diaz Cuellar

Principal Software Engineer Architect

Gerardo Diaz Cuellar

Microsoft

fido
ALLIANCE

Moving forward – FIDO Bare Metal Onboard (BMO)

Please note that this section reflects the current thoughts of the FIDO Working Group but is not POR

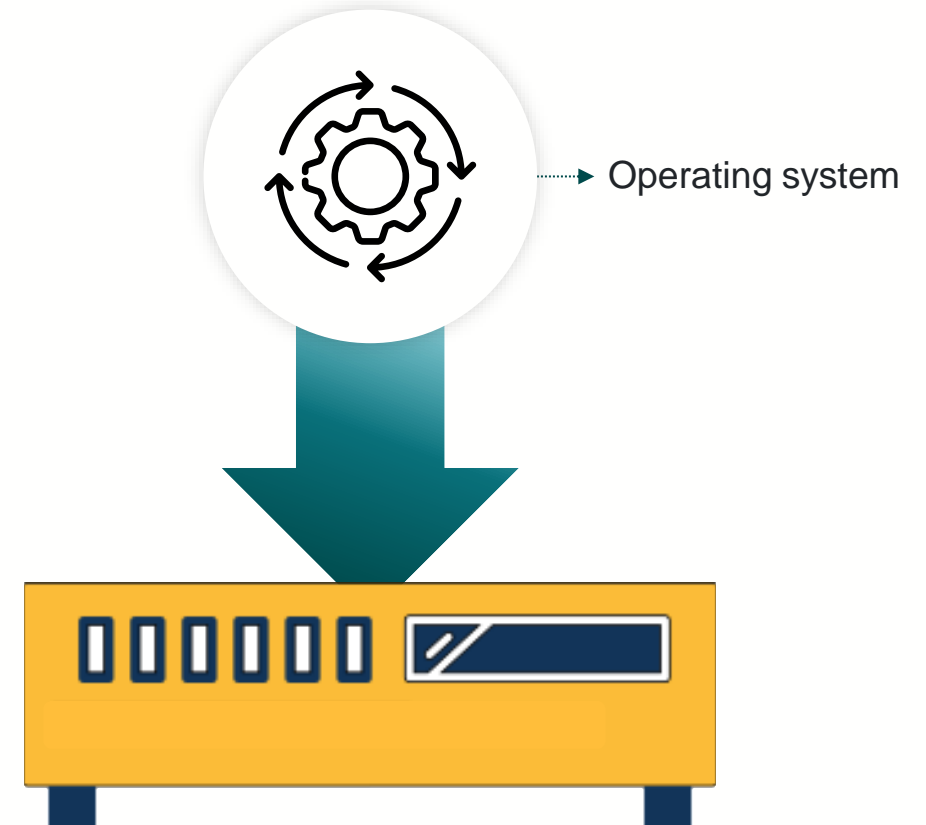
Before Onboarding takes place

- Before Onboarding, the OS (and potentially applications) are installed
 - This can be done directly after manufacture or manually at a staging point

Impact

- Effort/time/cost associated with manually installing the OS/apps.
- Multiple device SKUs needed if OS installed at device manufacture
- If SW issues occur at a late date, a technician is needed on-site to re-install SW and bring up device

The need: A secure ability to remotely control the device before OS boots



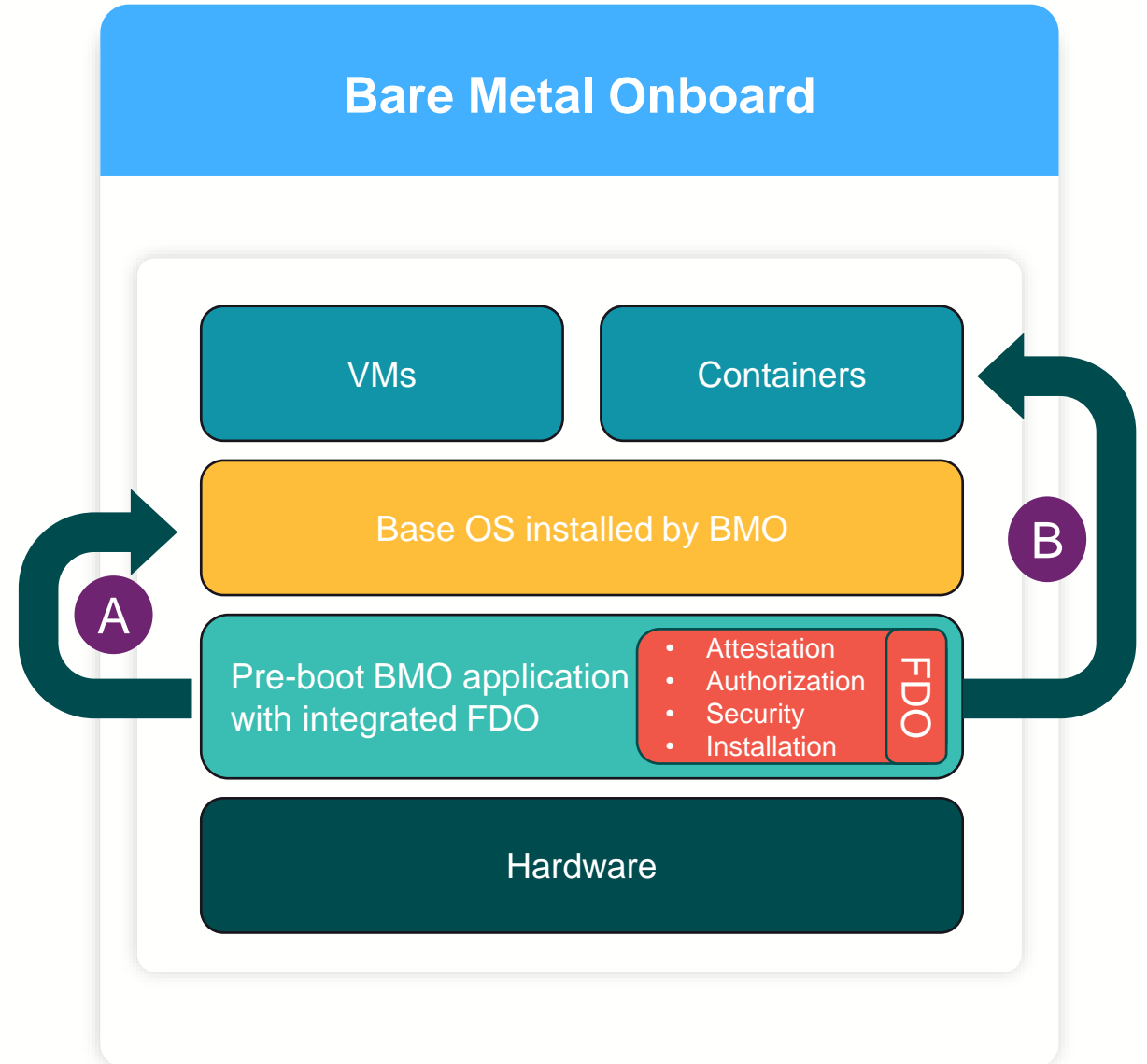
FIDO Bare Metal Onboard (BMO)

A A novel approach in which the base OS is delivered to the device after it has been installed in its target location, eliminating the need for OS installation prior to deployment.

B Additionally, FDO can be run after BMO to deliver credentials and other software components e.g.

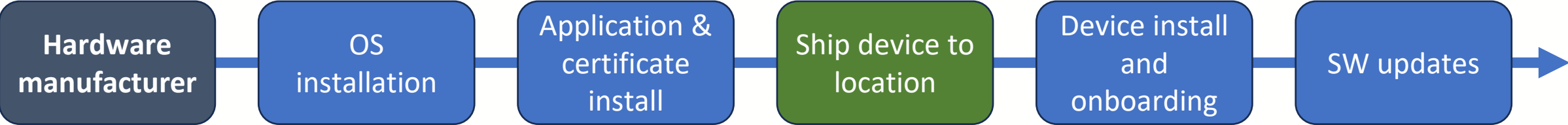
- Certificates
- Applications
- Containers
- Virtual machines.

FIDO BMO can be used to bring device back to a Known Good State

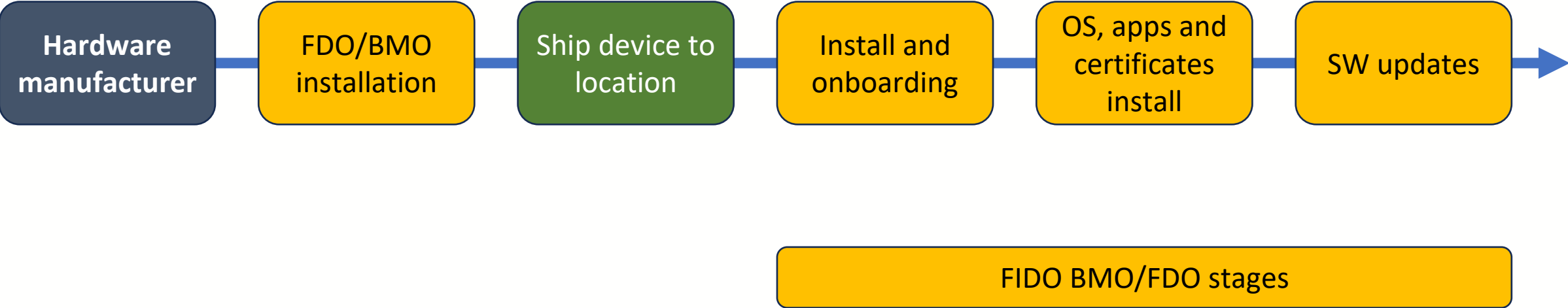


Conventional Vs BMO/FDO Device Flow

Conventional device flow



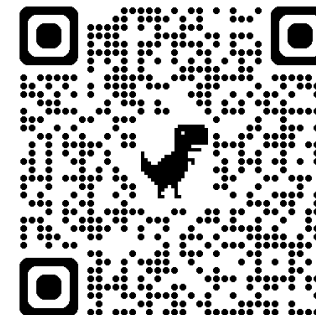
Device flow with FIDO BMO/FDO



Wi-Fi OpenRoaming with Onboarding

OpenRoaming for IoT – FIDO Device Onboarding Framework

- The **Wireless Broadband Alliance** (WBA) and the FIDO Alliance have joined forces to integrate **FIDO Device Onboard** (FDO) and WBA OpenRoaming™ technologies.
- This collaboration aims to create a seamless and secure onboarding process for Internet of Things (IoT) Wi-Fi devices.
 - Zero-touch, secure onboarding
 - OpenRoaming and FDO integration
 - Alternative network environments
 - Supply chain security



IoT/Edge Challenges

From a cybersecurity viewpoint, IoT/Edge products must provide:

1. **Secure Communication:** Enable encrypted, reliable data transmission.

2. **Private Data Access:** Safeguard sensitive IoT data for users.

PASSKEYS

3. **Management Connectivity:** Provide secure onboarding to on-site or cloud platforms.

FIDO DEVICE ONBOARD

4. **Robust & Upgradable Software:** Ensure resilience, updates, and cybersecurity.

BARE METAL ONBOARD

5. **Recovery Mechanism:** Restore to a secure baseline in emergencies.

FDO Workshop Sessions today – 14:00 to 17:00

Workshop Introduction: Comprehensive overview of FIDO Device Onboarding (FDO) and FIDO Bare Metal Onboard (BMO), with hands-on code review, use cases, credential storage and more.

1. FDO overview
2. Provisioning in FDO: By Whom & How?
3. Innovative Onboarding: Exploring Bare Metal and Early Onboarding in FDO
4. FDO Credential Storage: Best Practices and Alternatives
5. FDO Codebase: A Practical Guide for Developers
6. FDO Clients
7. Data Center Server Onboarding: Is FDO a Superior Alternative?
8. Summary of workshop and call to action

Brad Goodman

FIDO DO Working Group Chair
Principle Engineer
International Product Engineering
Distinguished Member of Technical Staff
Edge Computing Architect
Dell

Geof Cooper

FIDO Alliance
Co-inventor of FDO

Thank you