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.

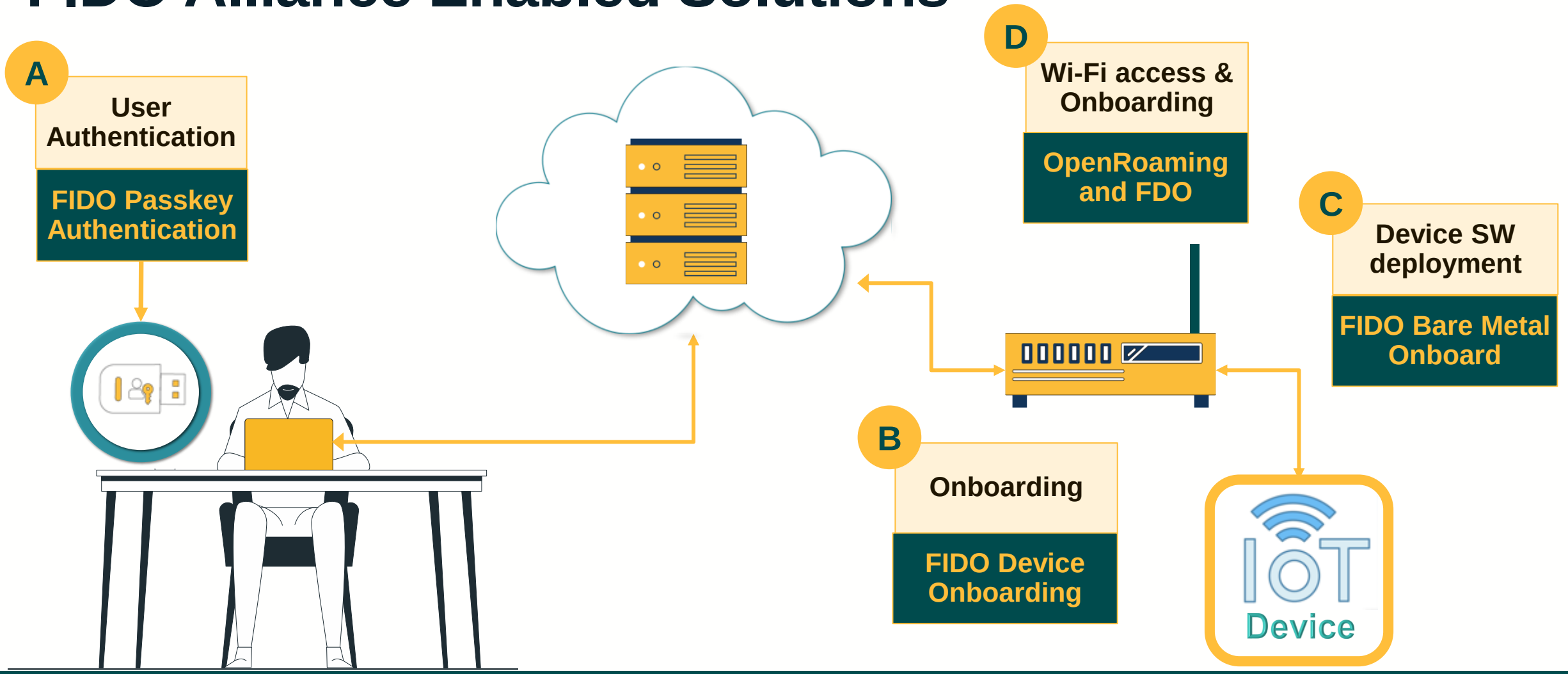
We have 350+ members from around the world.

amazon Google Microsoft

DELL Apple CISCO

We created passkeys.

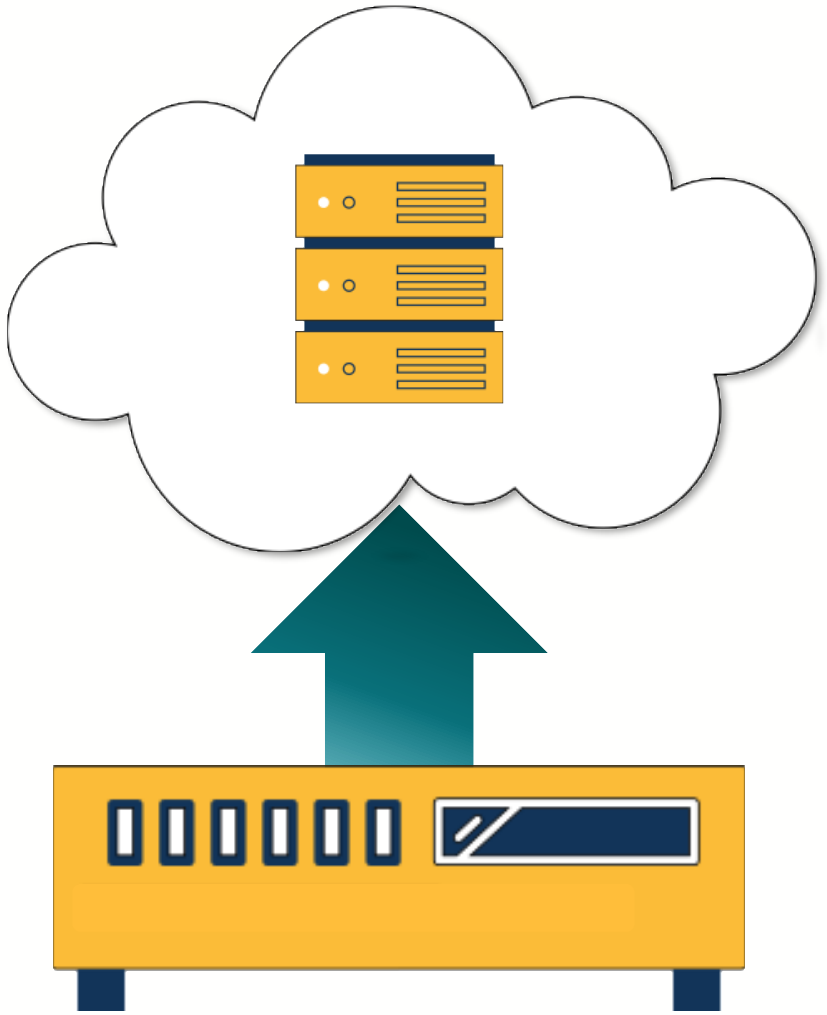
FIDO Alliance Enabled Solutions



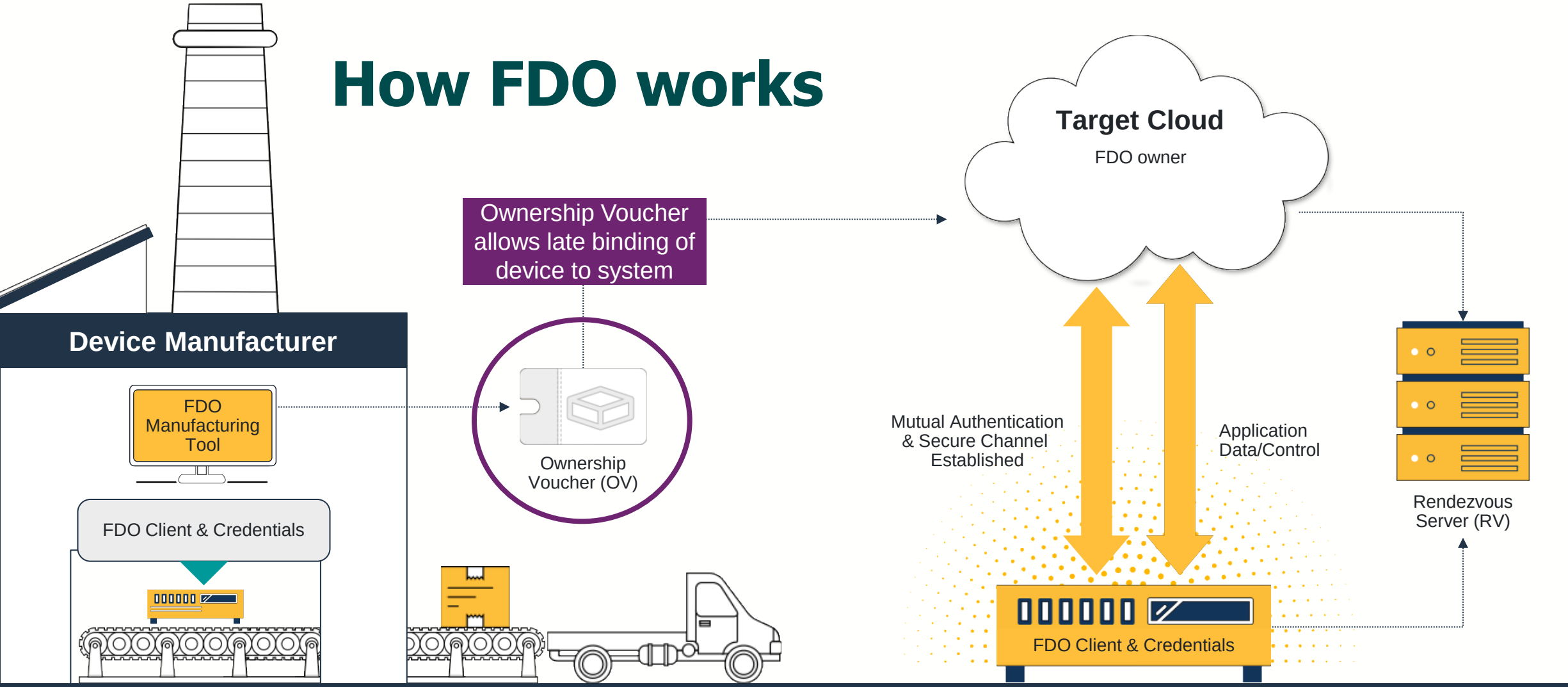
FIDO Device Onboard (FDO)

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

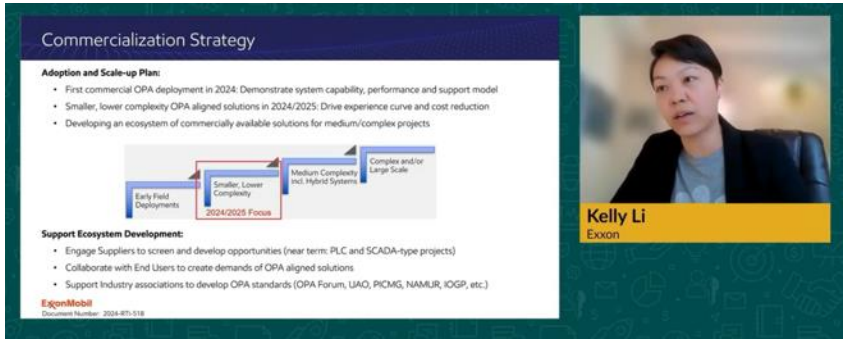
Microsoft

Dell

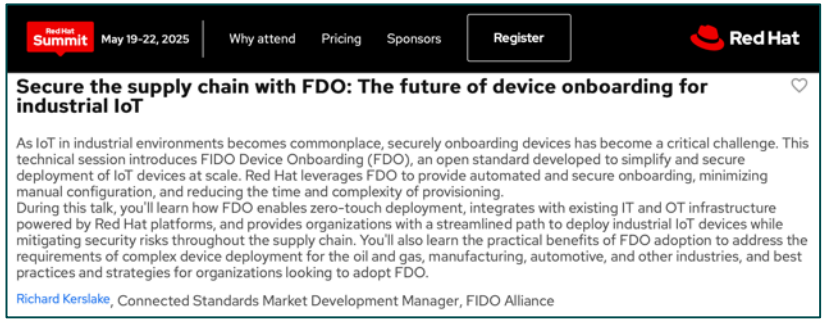
ASRock

Wireless Broadband Alliance

ExxonMobil

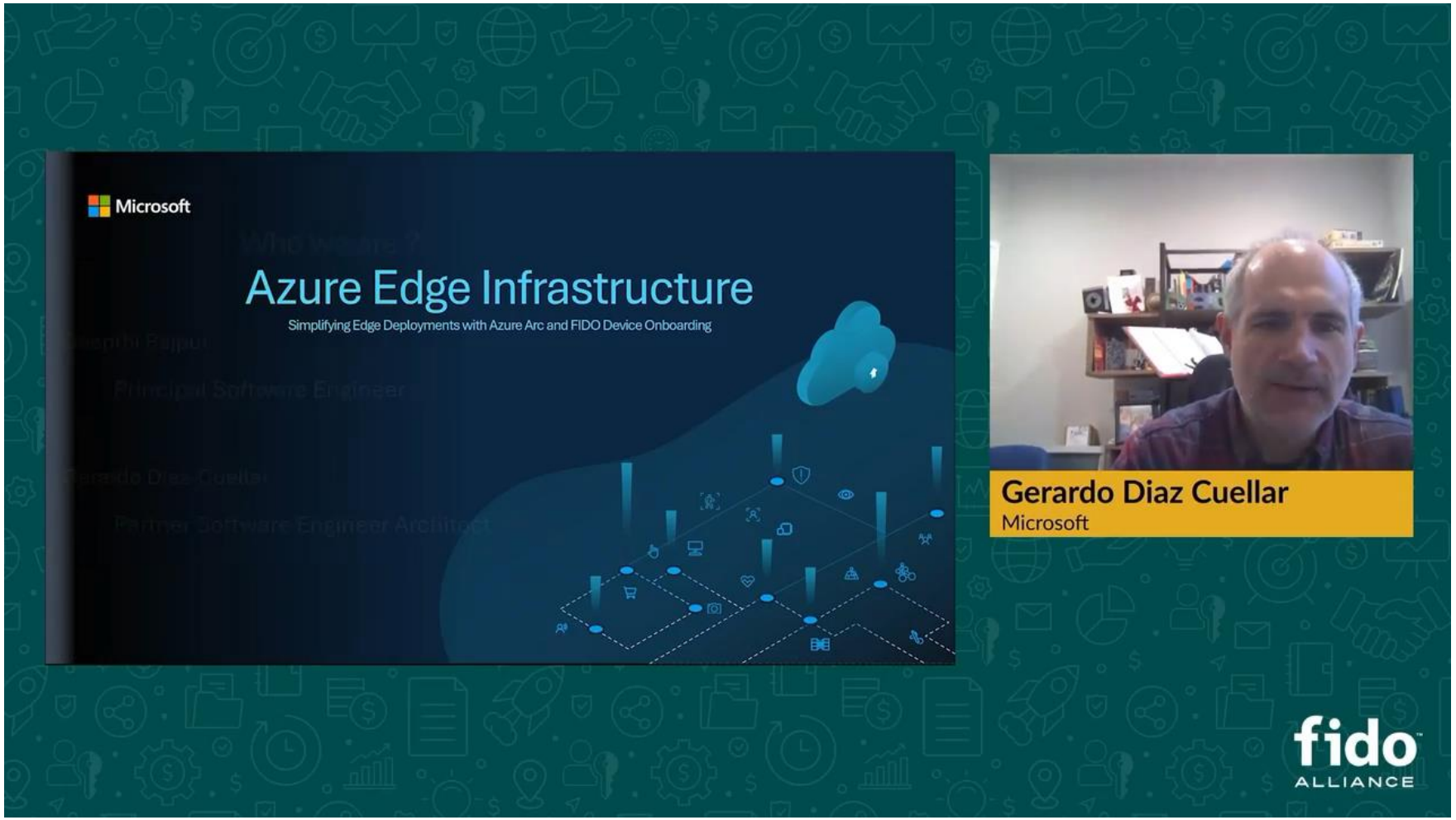


Red Hat



Microsoft present Azure Edge at Ignite

Link to all Workshop videos



Note: Videos have been edited for brevity

Moving forward – FIDO Bare Metal Onboard (BMO)

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

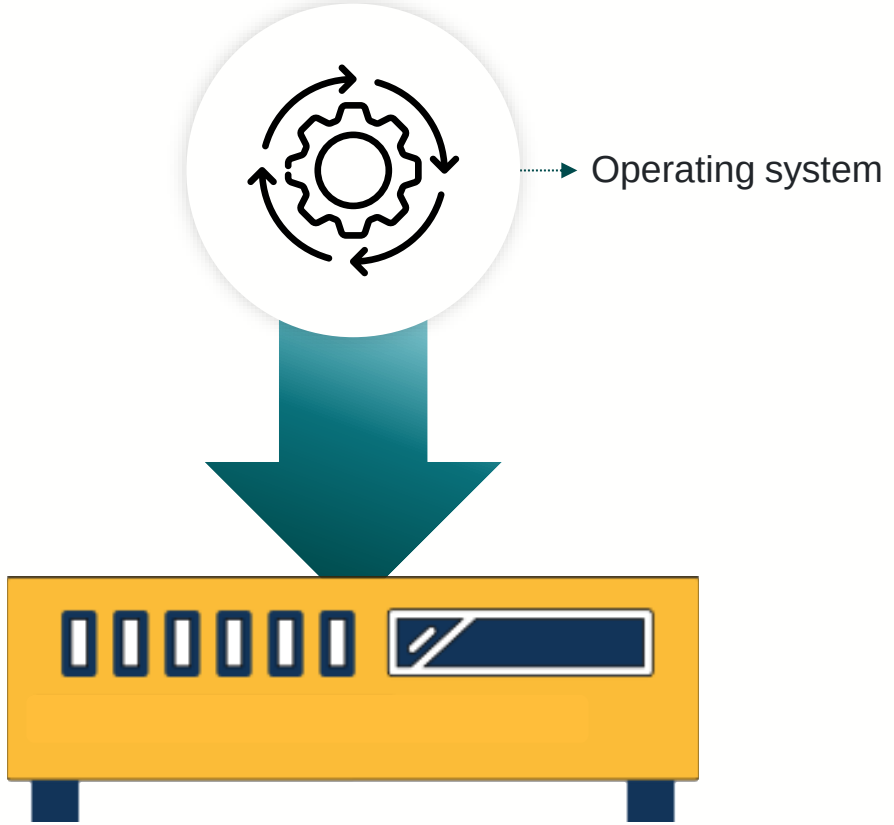
Before Onboarding takes place

- 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

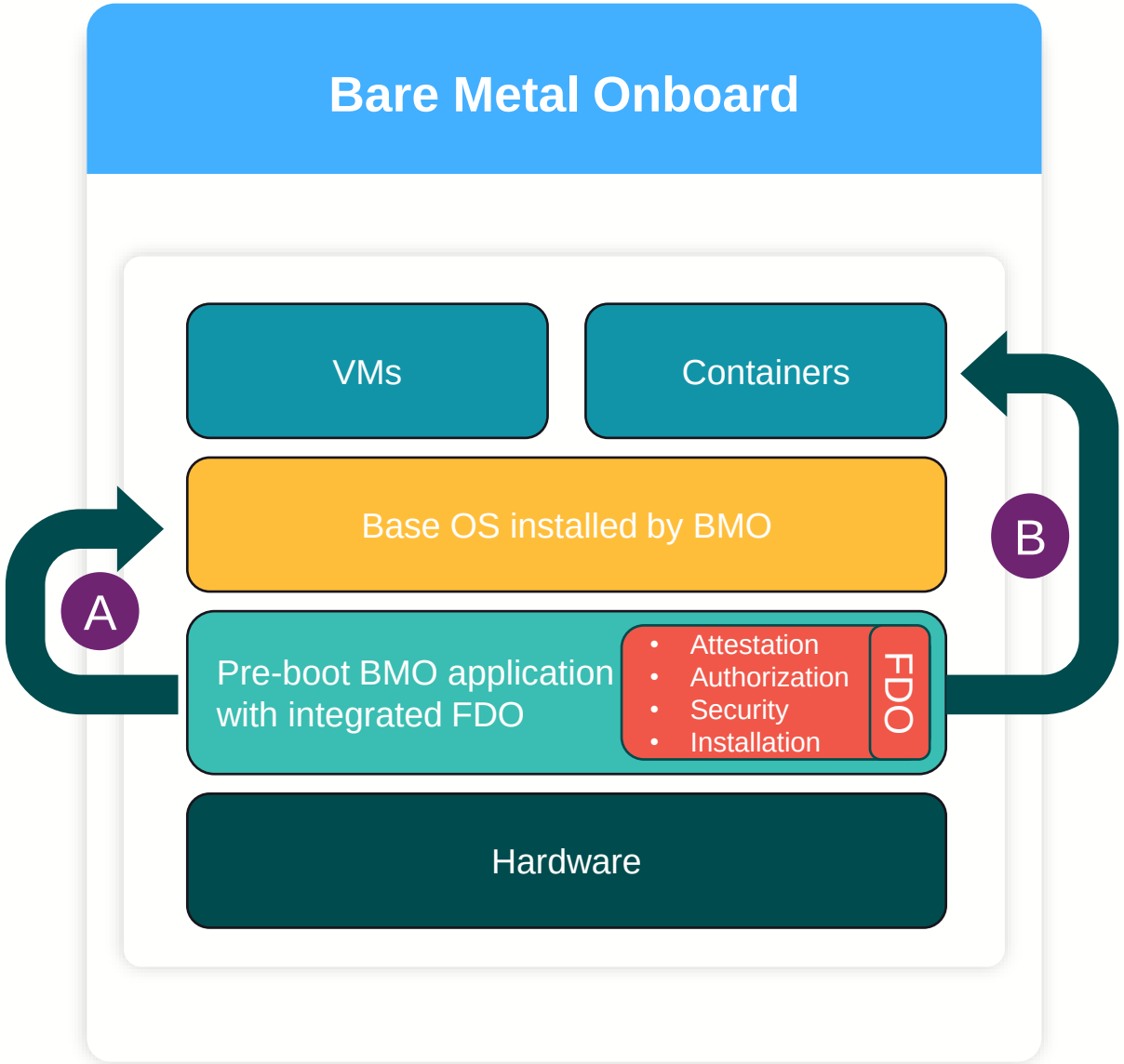
A novel approach in which the base OS is delivered to the device after it has been installed in its target location, eliminating the need for OS installation prior to deployment.

B

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

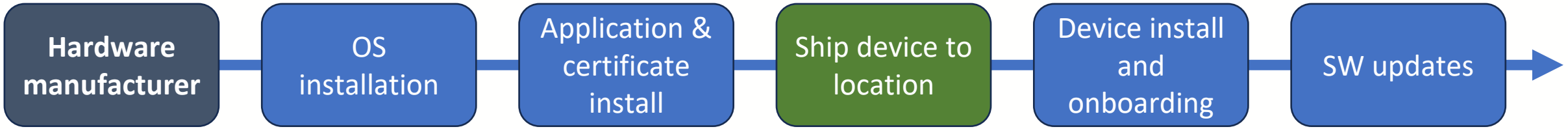
- Certificates
- Applications
- Containers
- Virtual machines.

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

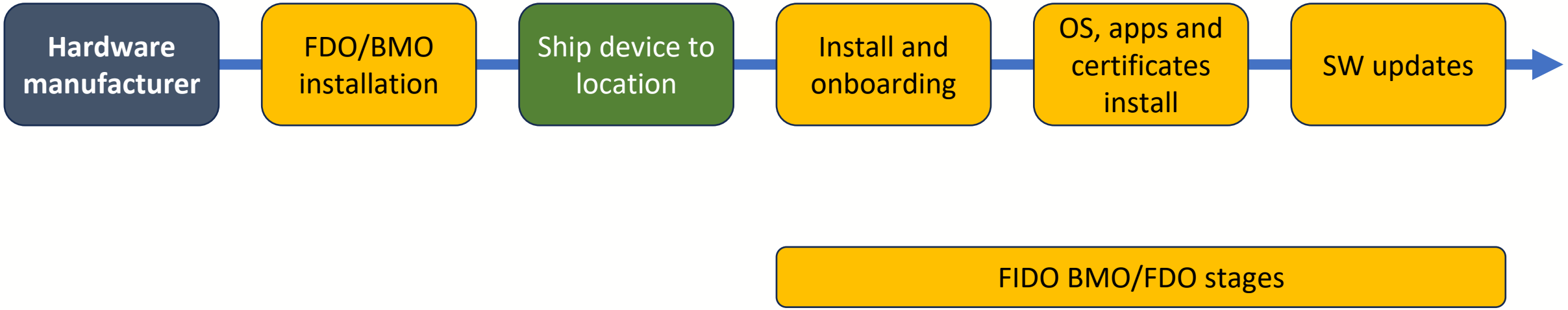


Conventional Vs BMO/FDO Device Flow

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.
5. **Recovery Mechanism**: Restore to a secure baseline in emergencies. — **BARE METAL ONBOARD**

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