Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers

Leveraging FIDO Alliance cybersecurity standards in support of IR8259

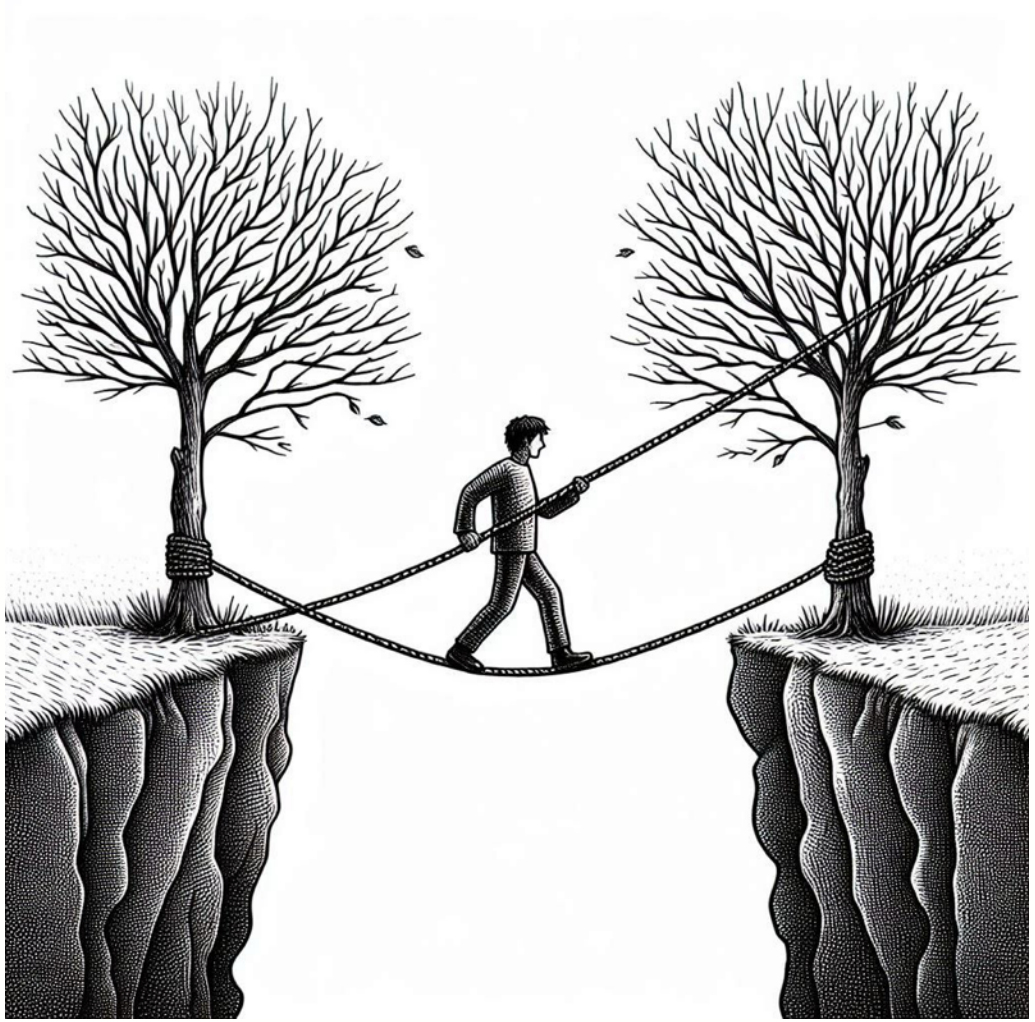
Brad Goodman
bradley.goodman@dell.com
LinkedIn: brad-goodman-nh

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

Secure Machine to Machine Communication

Asymmetric Crypto	Key Establishment
Symmetric Crypto	Secure Data Transmission
PKI	Identity and Certificate Management
TLS	Secure Communication Protocol

Enrollment



Which matters more, the strength of the rope or the strength of the trees?

Strong trees ➔ Onboarding/Enrollment

Strong rope ➔ Secure communication

R8259A - IoT Device Cybersecurity Capability Core Baseline

Device Identification	Device Configuration	Data Protection	Logical Access to Interfaces	Software Update	Cybersecurity State Awareness
The IoT device can be uniquely identified logically and physically.	The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.	The IoT device can protect the data it stores and transmits from unauthorized access and modification.	The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.	The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

IT in Datacenter

IT Personnel are…

- ✓ Trusted
- ✓ Authorized
- ✓ Knowledgeable
- ✓ Equipped (Tools)
- ✓ Secured (Environment, Network)
- ✓ Hands-On

Outside Datacenter

Our predications of **TRUST** don't necessarily hold up outside the datacenter

Operational (OT) Personnel are…

- ✗ Trusted
- ✗ Authorized
- ✗ Knowledgeable
- ✗ Equipped (Tools)
- ✗ Secured (Environment, Network)
- ✓ Hands-On

PROBLEM:

How do we set-up and configure equipment outside datacenter, by people who may not be knowledgeable or trusted in a manner that is both **SECURE** and **AUTOMATED**?

Solve

- Enrollment
- Setup
- Configuration

Constraints

- No IT
- Hands-On OT
  Automated

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.

What is a passkey?

Passkey

/’pas, kē/ noun

Passkeys are a password replacement based on FIDO protocols that provide faster, easier, more secure sign-ins to online services.

A passkey may be synced across a secure cloud so that it’s readily available on all of a user’s devices, or it can be bound to a dedicated device such as a FIDO security key.

4x simpler

Passkeys are 4x simpler to use since they don’t need to be remembered or typed. You just use your fingerprint, face scan, or screen lock to sign in across all your devices and platforms.

Source: Google

FIDO Device Onboarding (FDO)

Method for Secure, Zero-Touch Device Onboarding

Zero-Touch

Does not require any user to perform any operation

Automatic, Plug-and-Play

Secure

- Mutually Attested & Probably between Device and Control Plane
- Define “Ownership”
- Not predicated by user access

Late Binding

Establishment of WHO a device is to onboard to determined AFTER leaving factory

Authors of the FDO specification

The FDO spec was written by technology leaders:

amazon

arm

Google

intel

Microsoft

Qualcomm

DELL

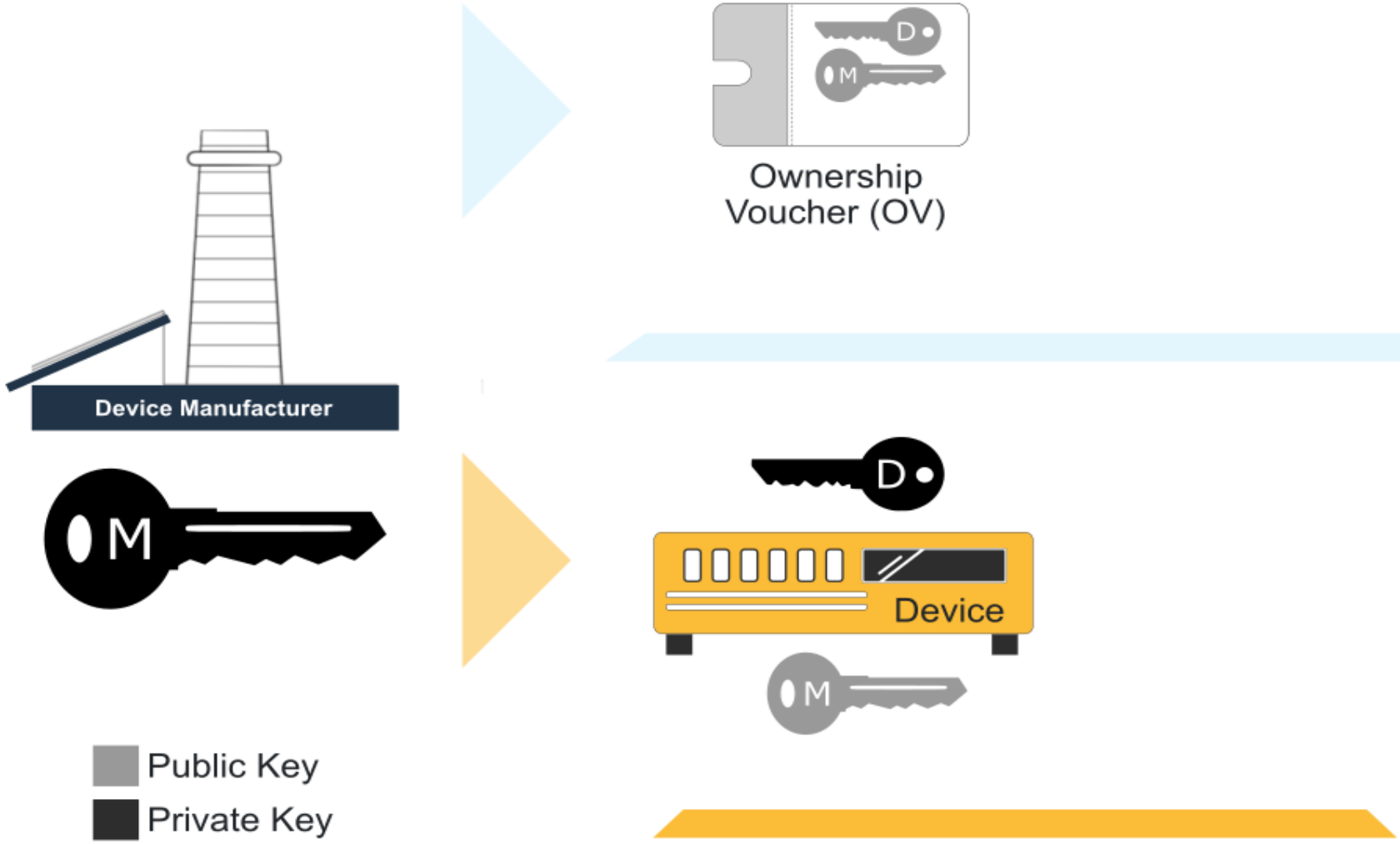
Link to FDO 1.1 specification

1. Device Initialization

DEVICE has its own unique attestation **KEY**

Device leaves factory knowing **KEY** of who **MANUFACTURERD**

OWNERSHIP VOUCHER created – indicates **DEVICE** created by **MANUFACTURER**

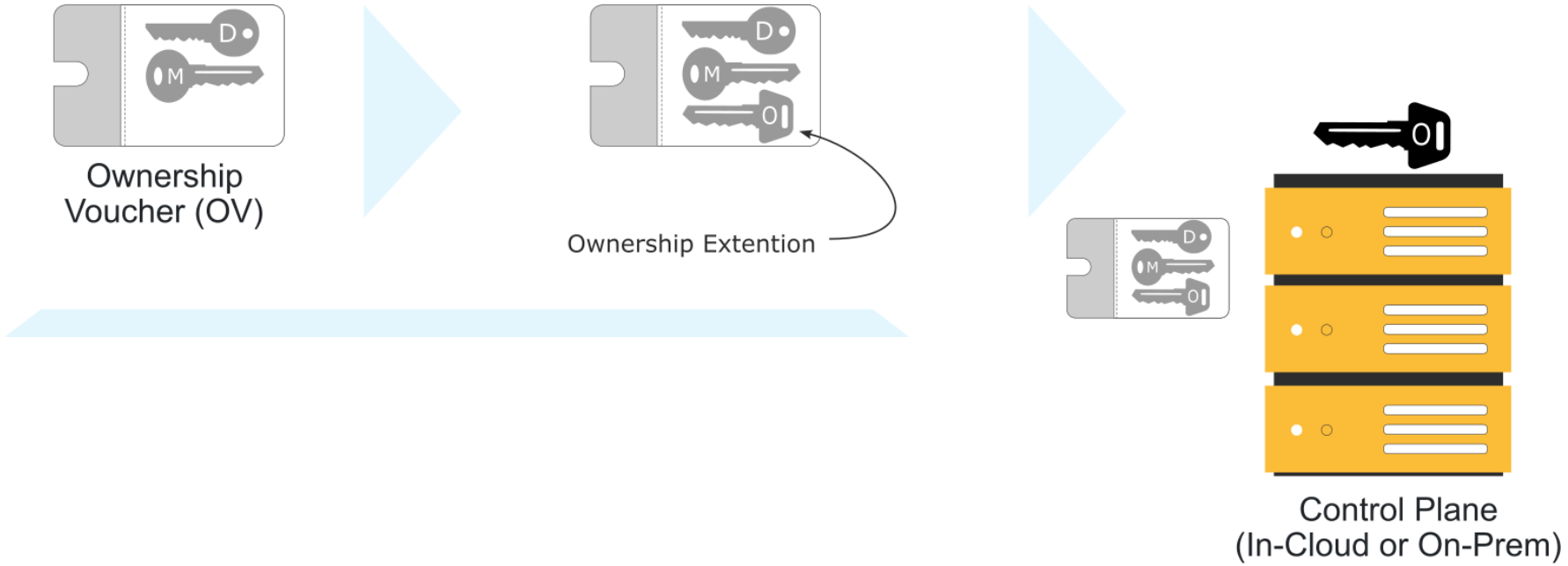


2. Purchase or Resale

DEVICE has been sold to new **OWNER**

Manufacture **EXTENDS** voucher – **SIGNING** amendment which states new **OWNER**

Ownership Voucher delivered to Owner's new Control Plane (or **ONBOARDING SERVICE**)



3. Onboarding

DEVICE contact owner's **ONBOARDING SERVICE**

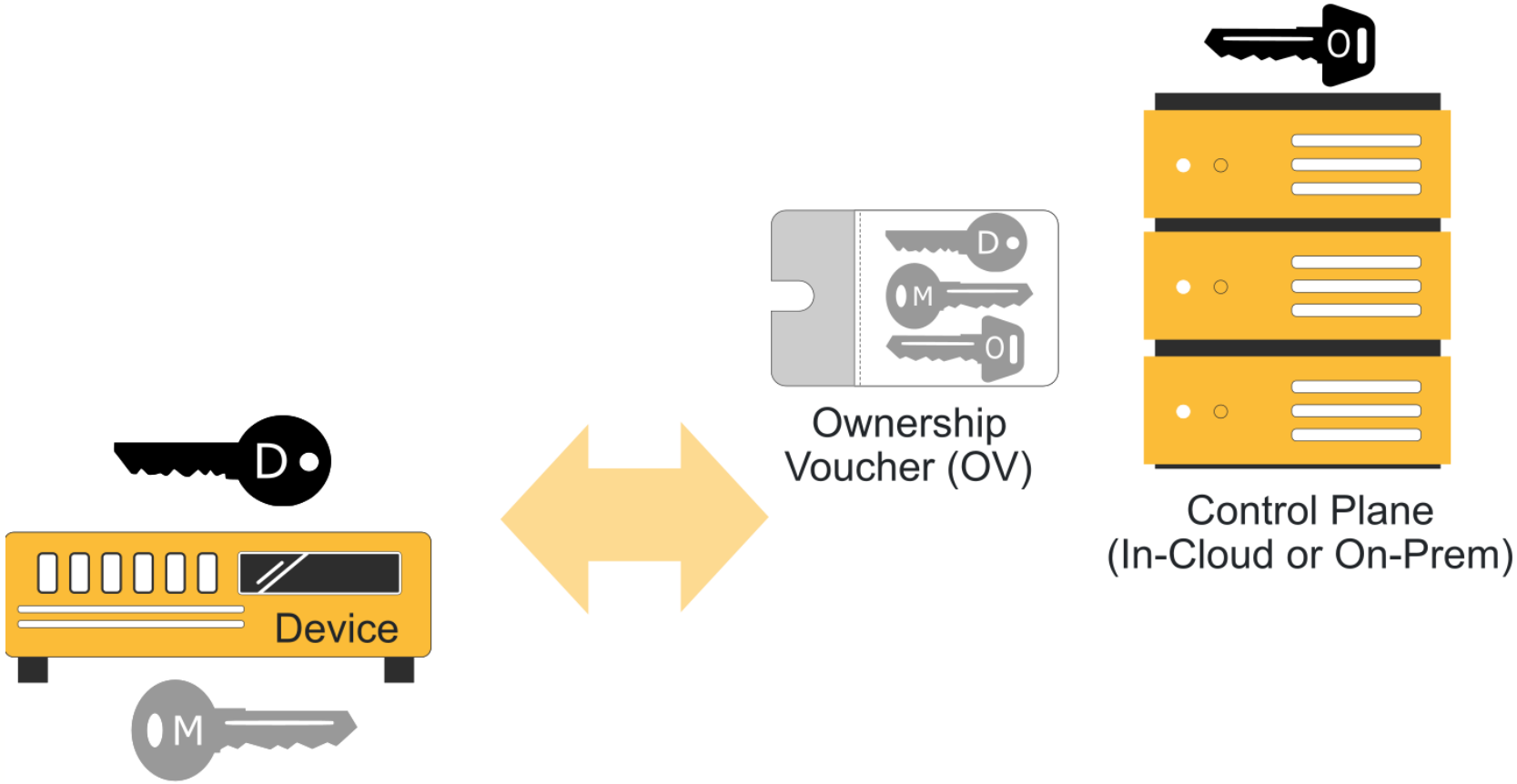
Owner presents Voucher to Device

Device verifies that:

- Voucher was signed by SAME Manufacturer stored in Device
- Voucher references Device Key
- Manufacturer extended ownership to new Owner
- Device is talking to control plane that has Owner key

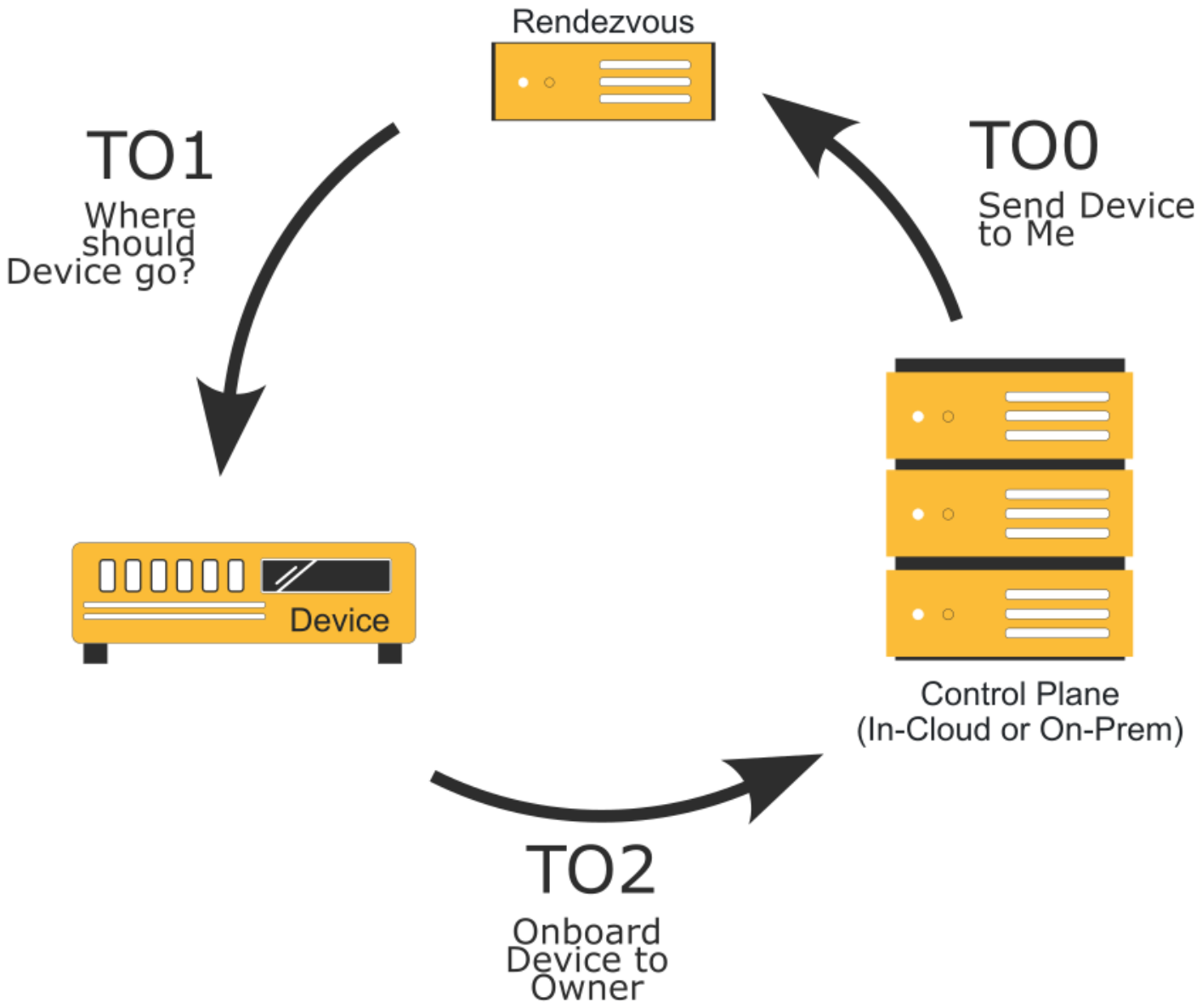
Onboarding Service verifies that:

- Device it is talking to has Device key in Ownership Voucher



After MUTUAL ATTESTATION – Device and Control Plane trust each other.

FDO allows credentials exchange and configuration through encrypted tunnel, after which onboarding is COMPLETE, and Application may run in steady-state via established configuration and credentials.

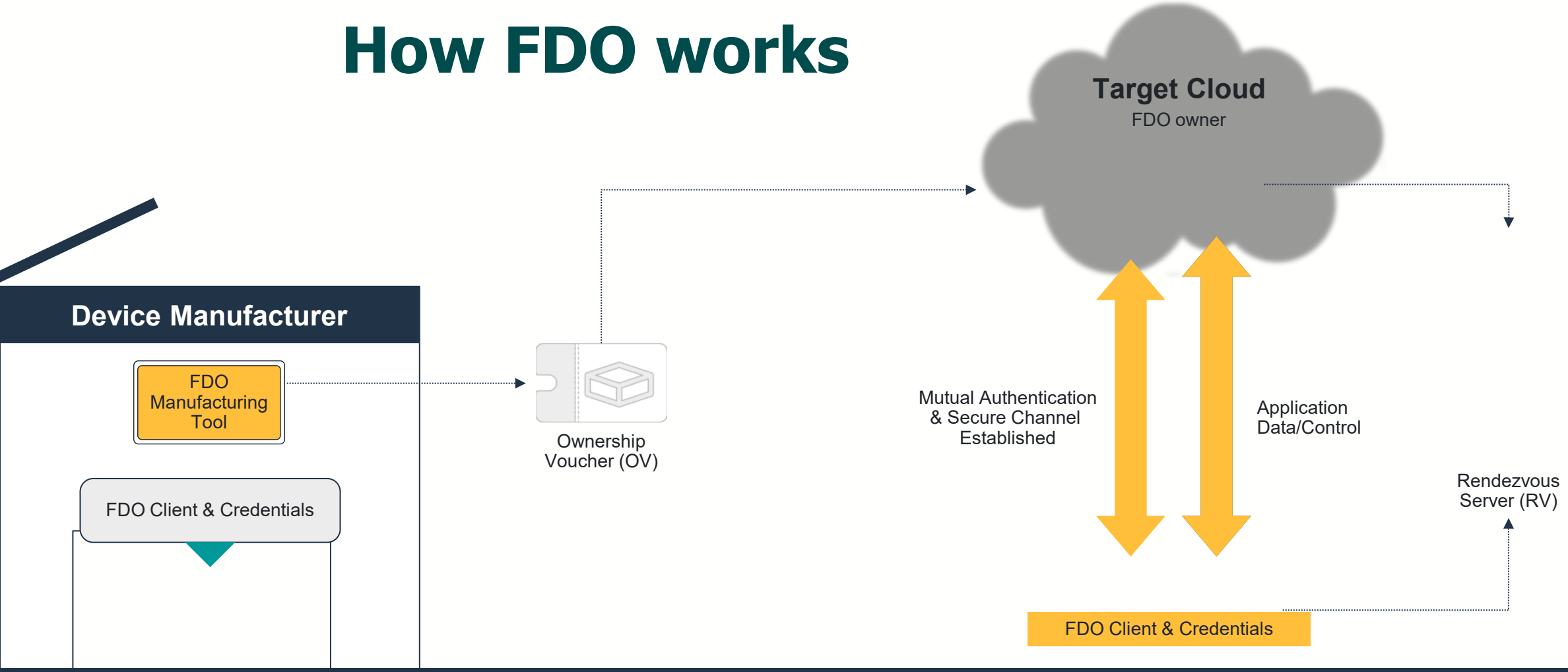


Rendezvous

How **DEVICE** gets introduced to **ONBOARDING SERVICE**

The “Three Fundamental Protocols” of FDO

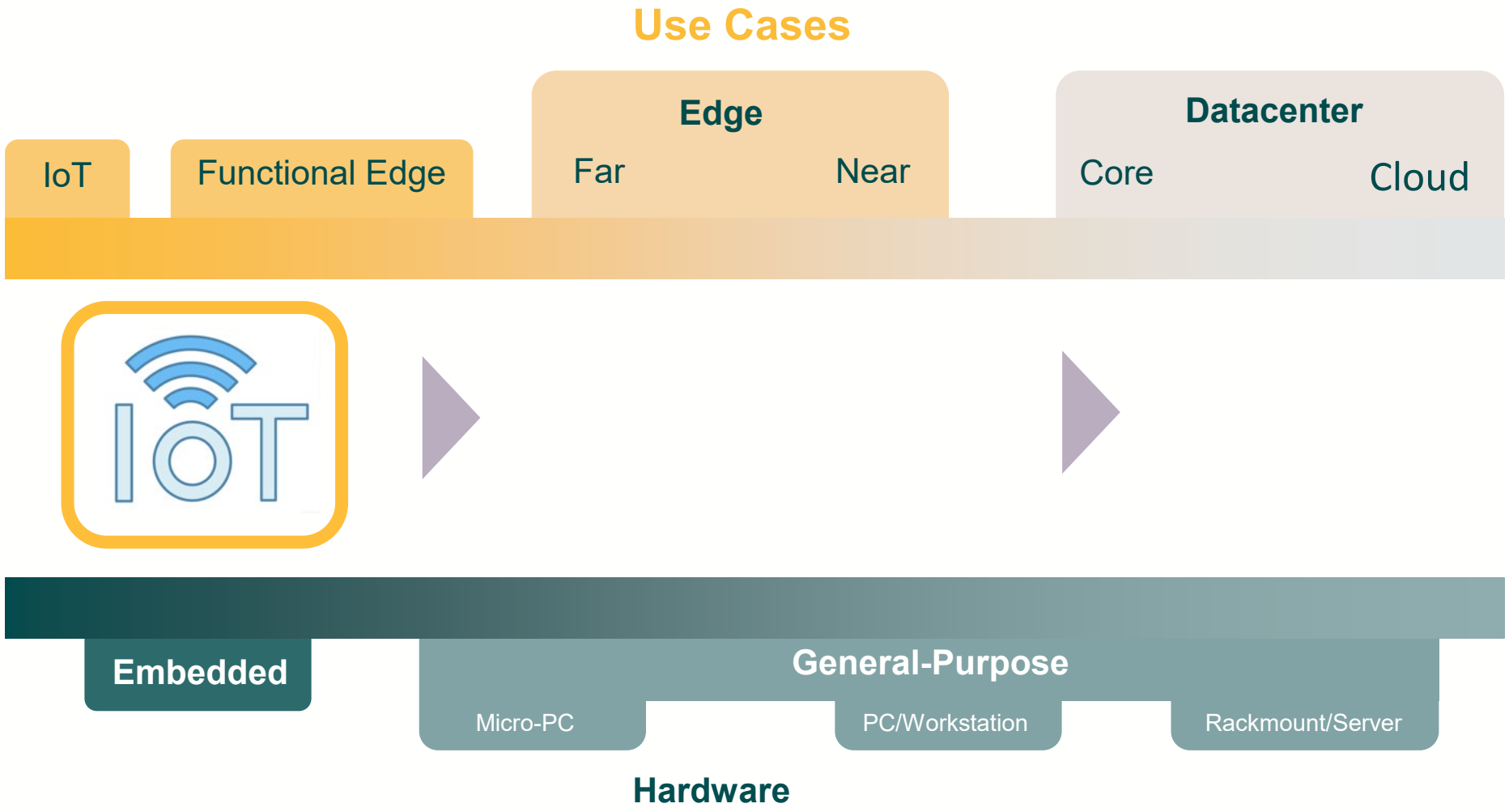
How FDO works



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

Scope

Designed to work across spectrum of use cases, and hardware types



Toolbox

Device Identification	Device Configuration	Data Protection	Logical Access to Interfaces	Software Update	Cybersecurity State Awareness
The IoT device can be uniquely identified logically and physically.	The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.	The IoT device can protect the data it stores and transmits from unauthorized access and modification.	The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.	The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.
X.509 Certificates → Subject Name → Public keys Harder to prove: • DNS name • IP address	Signed code Signed config Safe key storage: • TPM • Hardware specific	Encrypted storage Encrypted RAM TLS data comms • Identified • Encrypted	Boot identity Local identity Local authorization	Signed updates Verified on device	TEE can help Verify: • identity • configuration • code • data

Logical Identifiers

FDO Device Identification done via **DEVICE ATTESTATION KEY** (DAK)

Public Key-based mechanisms reduce spoofing, fishing

Other example of such include IDevID (TCG Standard)

Table 1: The Devi

Device Cybersecurity Capability	Common Eleme
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifie 2. A unique physical identif external or internal locati device authorized entitie Note: the physical and logic may represent the same va do not have to.

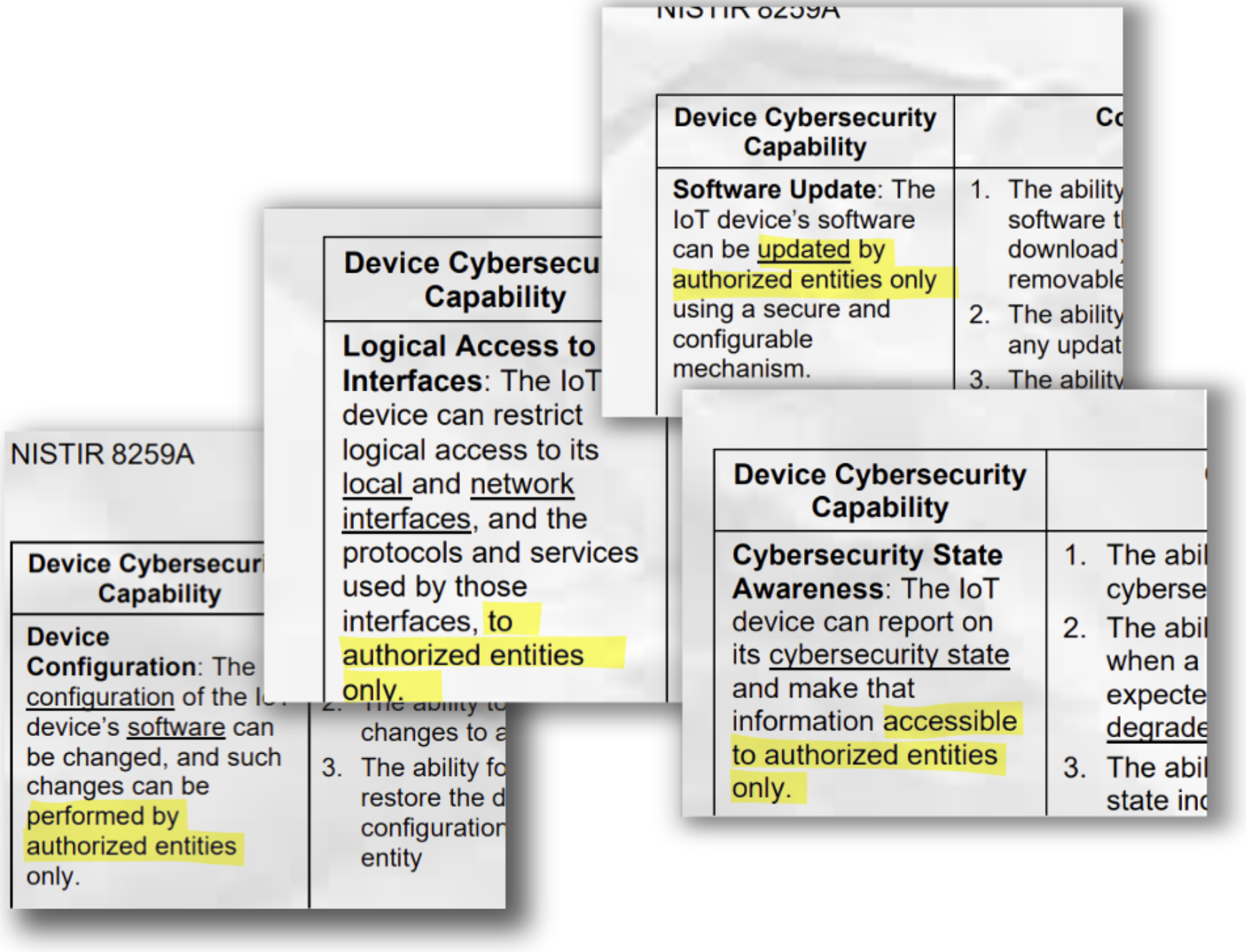
Authorized Entities

FDO provides a rigid and provable mechanism to establish “Ownership”

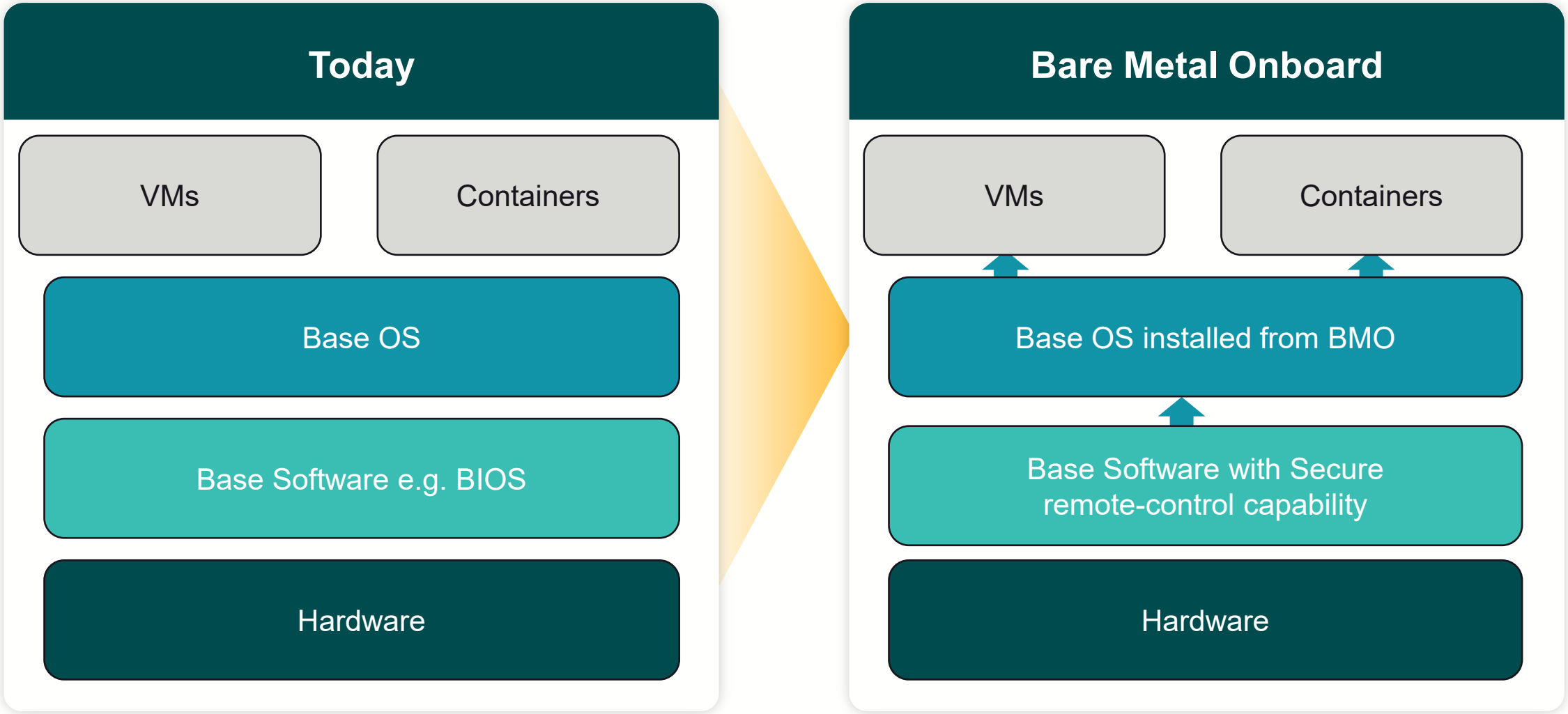
This establishes a Root of Trust from which further notions of “Authority” and “Authorization” can stem

Any direct or physical user access can be established through this mechanism

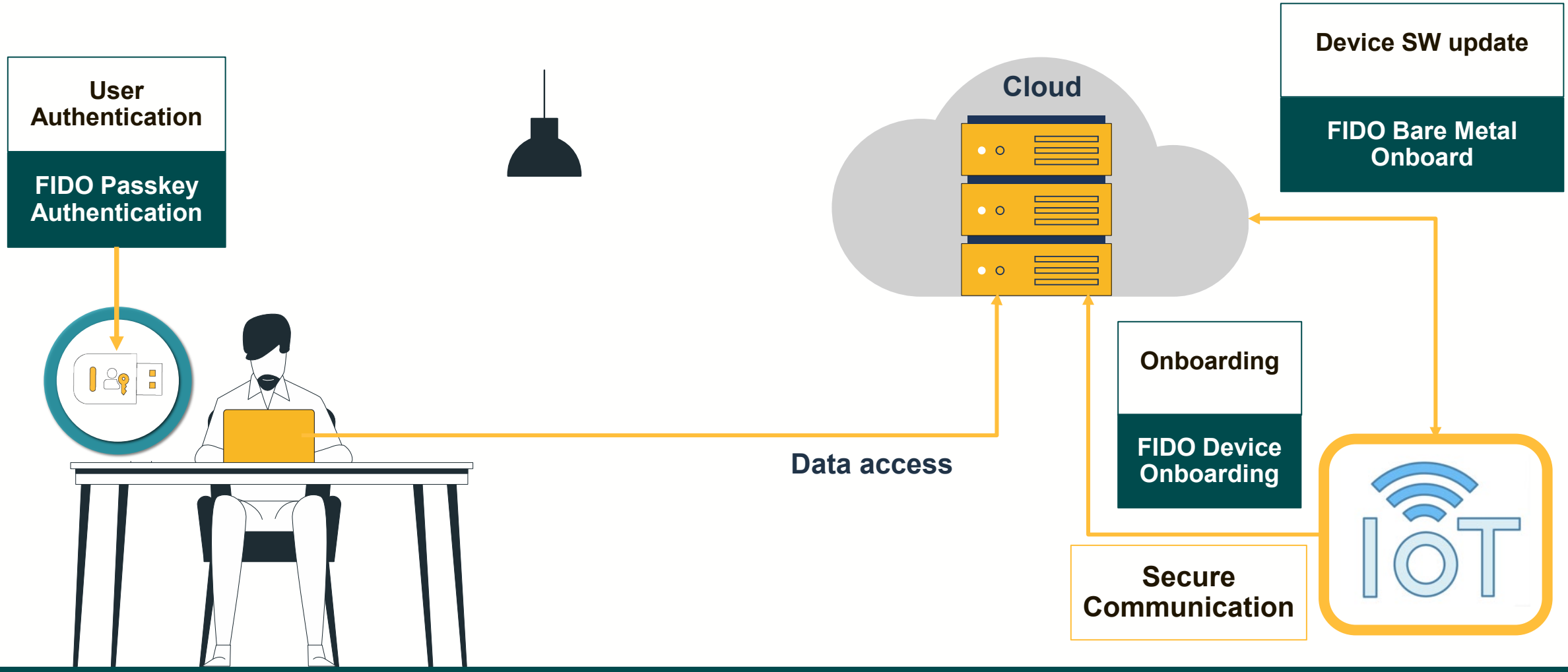
Ongoing work like FDO Owner-signed payloads or Dell EstateKey leverage as such.



Bare Metal Onboard



FIDO Alliance Solutions



Questions?