



simpler  
stronger  
authentication

# FIDO Device Onboard (FDO)

Geoffrey Cooper  
FIDO IoT Technical Working Group  
Principal Engineer, Intel Corporation  
February 2021

# 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: Dec 2020  
FIDO Device Onboard Review Draft released

## FIDO Device Onboard Specification



Review Draft, December 02, 2020

**This version:**

<https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.0-20201202.html>

**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)

# FDO/SDO: LF-Edge project & Open Source



About

Projects

Members

Resources

News & Events

All Projects

Stage 3: Impact >

Stage 2: Growth >

Stage 1: At Large >

Baetyl

Fledge

Open Horizon

Secure Device Onboard

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

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

## ■ Status

- Open Source code at: <https://github.com/secure-device-onboard>
- **Now migrating development from SDO to FDO**
  - Protocol testing release of **FDO RD01**
  - Production release of **FDO 1.0** projected for 2H21 (subject to finalization of FDO 1.0 spec)

# Fast, Scalable & Secure<sup>1</sup> X

## Device Provisioning, Onboarding & Activation

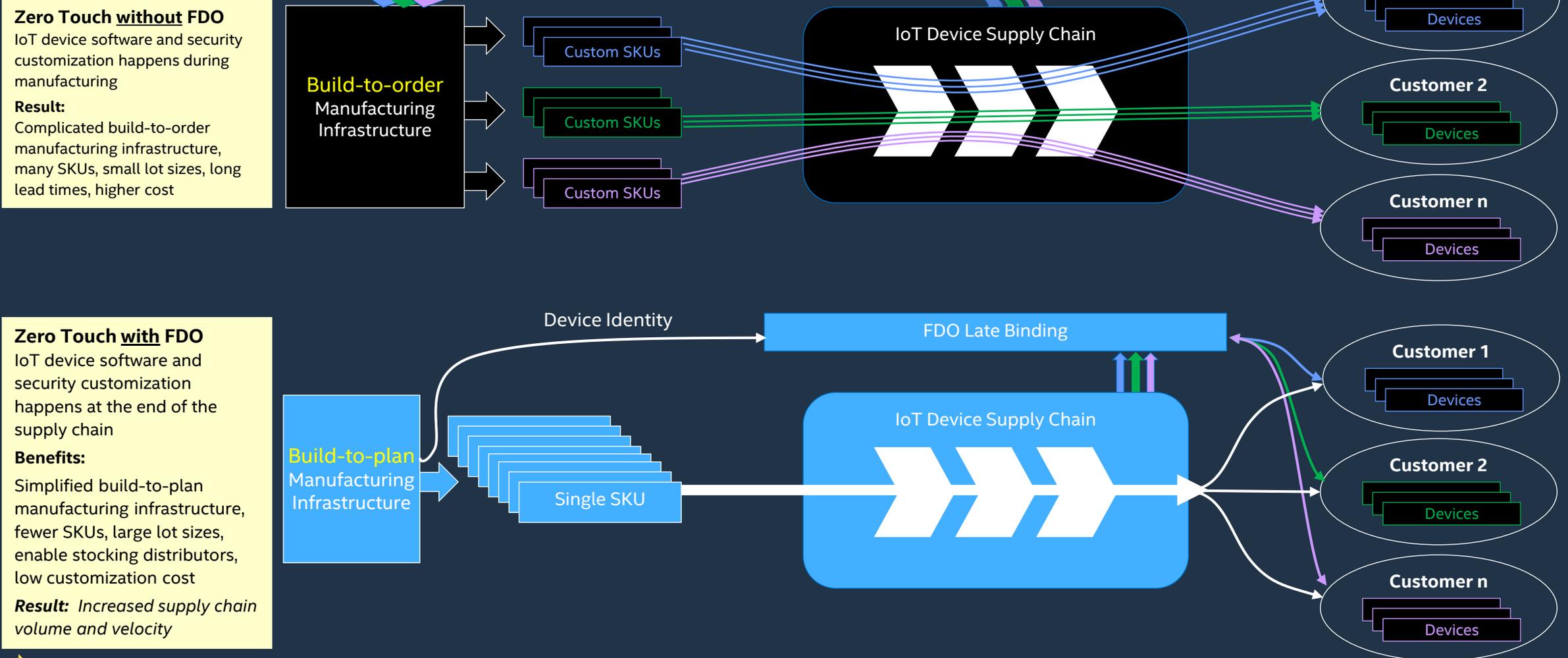


### BENEFITS<sup>1</sup>

- Zero touch onboarding – integrates readily with existing zero touch solutions
- Fast & more secure<sup>1</sup> – ~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, code now on GitHub
- Industry standard - FIDO Alliance has released 1<sup>st</sup> spec draft

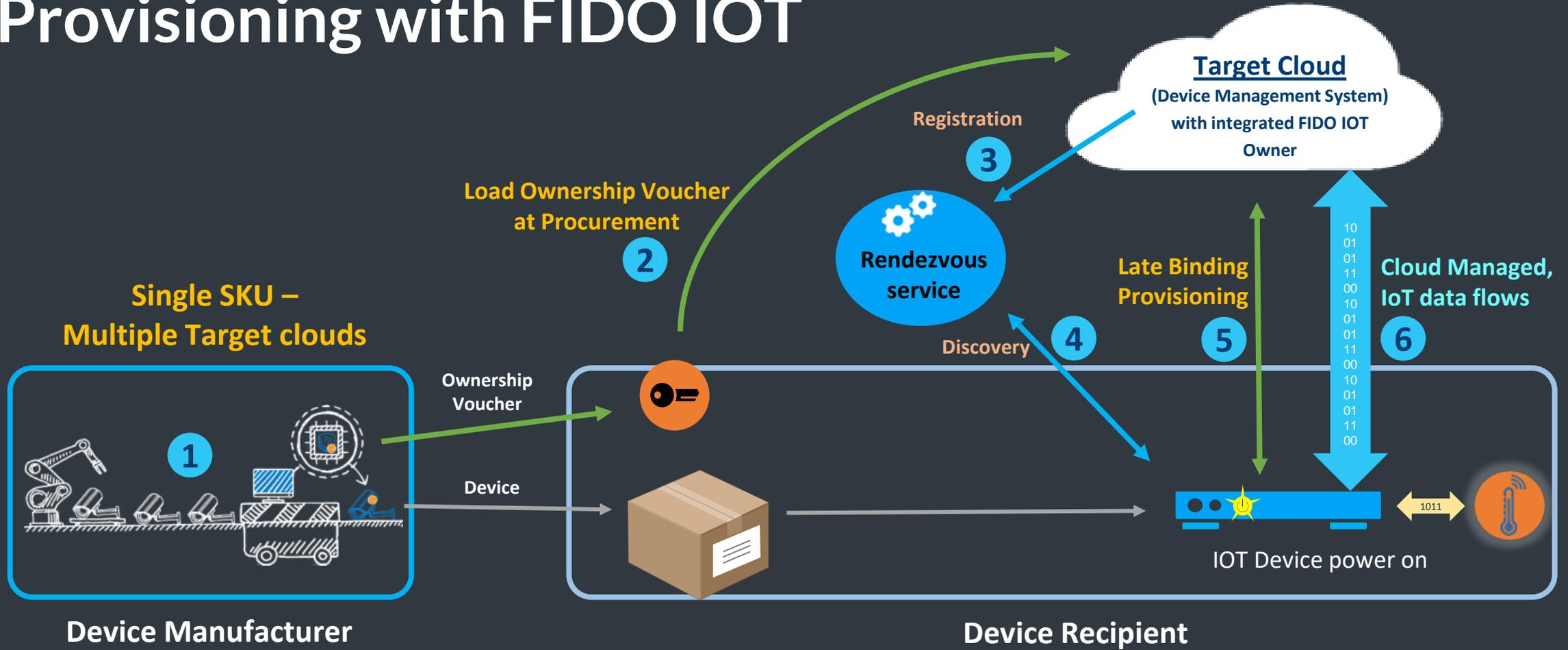
1. No product or component can be absolutely secure

# FIDO Device Onboard: Late Binding in Supply Chain



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

# Provisioning with FIDO IOT



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

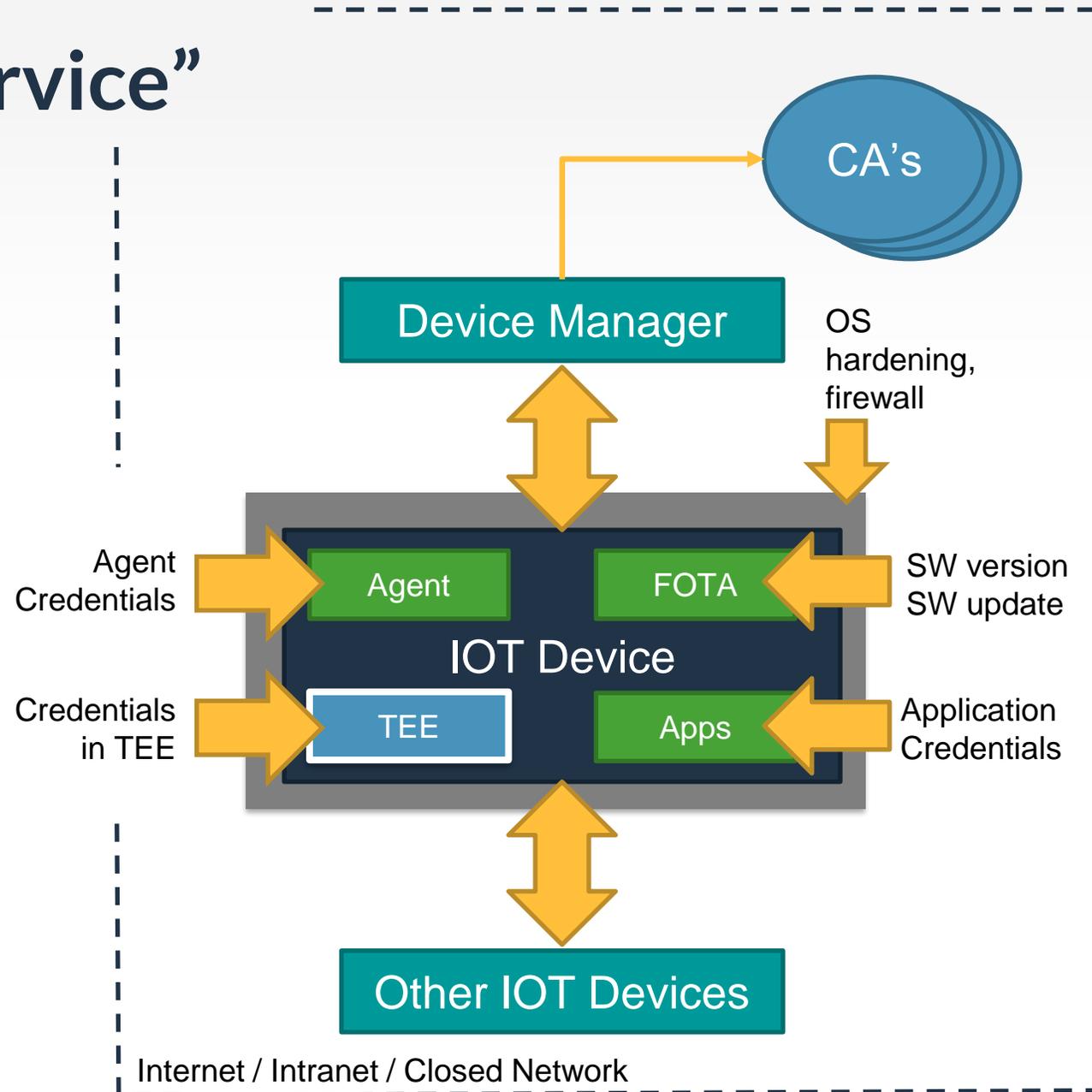
# FDO: Out of Box → “in Service”

## FDO Download:

- Initialization/Hardening Scripts including Agent
- Crypto and other Credentials
- Trust for local keys (CSR/Cert, multiple CA's)
- Data files / programs (small, agent is most likely)

## Use FDO to set up:

- Agents
- Software update (existing FOTA)
- Connection to other IOT devices
- FDO “Owner” to IOT devices
- Keys in TEE (e.g., using CSR)
- Devices in closed networks



# Questions?



**fido**<sup>™</sup>  
ALLIANCE



# Requirements to achieve Late Binding

Manufacturer  
Credentials only  
used for  
onboarding

Security of device identity

Warehousing of  
Device.  
Final destination  
may not be known

Flexibility of supply chain

Provisioning of  
Device.  
Kind and quantity  
of credentials  
varies

Different clouds use  
different credentials

Network  
Topology.  
Internet,  
Intranet,  
Closed Network

Different destinations have  
different networks

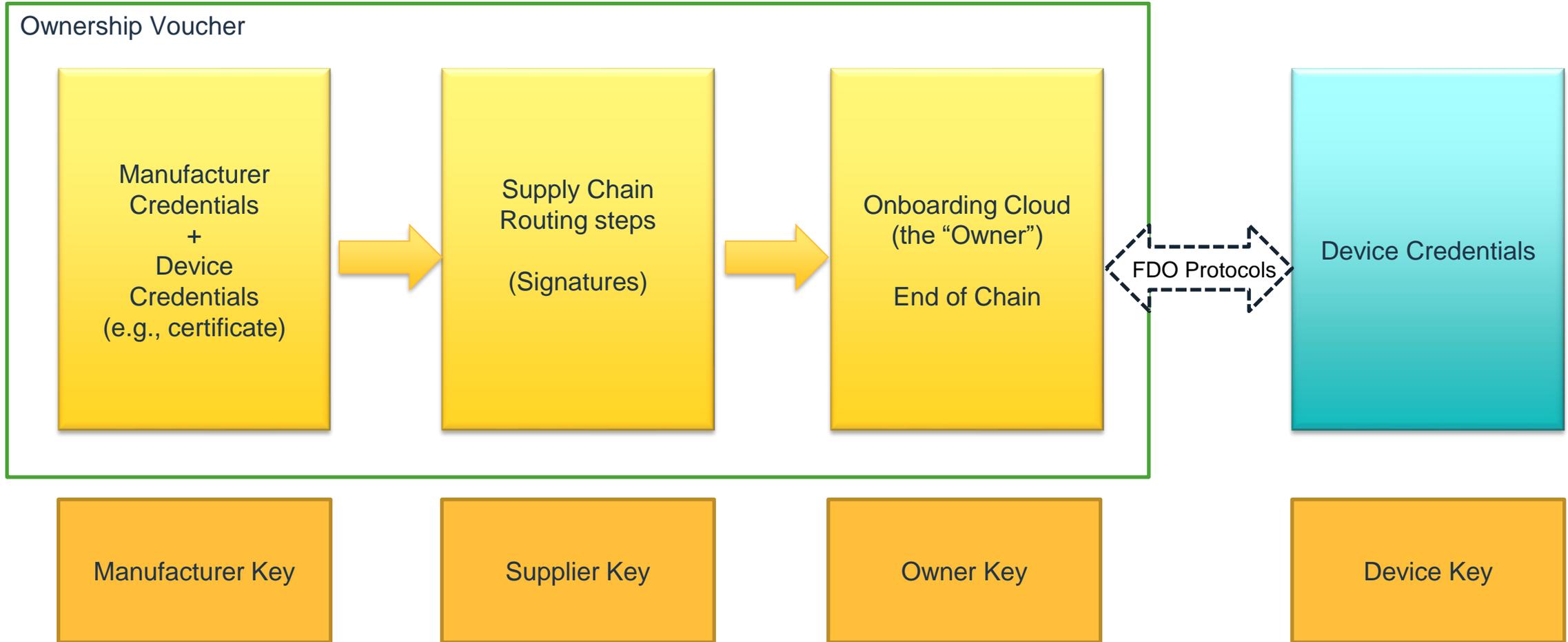
Ownership Voucher  
Data Structure for Late Binding

Separate authentication from Service / Info.  
Flexibility of provisioning for Late Binding



# FDO Ownership Voucher

The Ownership Voucher is a digital textual message. It is cryptographically mated to the Device factory credentials, so that it allows the IOT Device to distinguish the late-bound Owner, even if both are in a closed network



# Aligning FDO to Use Case and Ecosystem



## Good fit

- **Mass produced devices:** thermometers, sensors, actuators, controls, lighting, medical, edge servers, etc.
- **Multi-ecosystem applications and services:** not tied to specific cloud 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



## Poor fit

- **Custom build-to-order devices:** manufactured for specific customer
- **Single-ecosystem devices:** manufactured for specific service
- **Extremely constrained platforms:** thresholds TBD
- **Deployments with no or inadequate connectivity:** specific use-cases TBD



# FIDO vs SDO

Intel<sup>®</sup> Secure Device Onboard (SDO) was submitted to FIDO for consideration

- FIDO is based on SDO, functionally very similar.
- FIDO plans to add “trusted installer” functionality – not available in FIDO 1.0.
- FIDO WD02 released 7/30/2020
- FIDO RD01 published 12/02/202 (normative feature freeze)

SDO/FIDO Differences in terminology

- TEE → ROE
- AppID → Multi Application ROE Prefix (MAROEPrefix)

FIDO/SDO Syntactic Differences

- CBOR
- COSE - including authenticated encryption
- EAT

FIDO/SDO Functional differences

- Crypto profile (one)
- ServiceInfo is one CBOR type
- Multi rounds of ServiceInfo
- Message order, names changed to put all authentication first.
- More crypto (COSE), better KDF
- Rendezvous bypass added
- TBD: FIDO IANA Assigned numbers

# FIDO Device Onboard



**fido**<sup>™</sup>  
ALLIANCE