fido ALLIANCE simpler stronger authentication

FIDO Device Onboard (FDO) Update to IETF IOTOPS

2023-11-09
Geoffrey Cooper, Intel Corporation
Co-Chair FIDO IOT Technical Working Group

2023/11 – FDO news at a glance

- Implementors “gone public”
  - Dell Edge
  - IBM OpenHorizon
  - Exxon (blogged)

- Independent Implementations

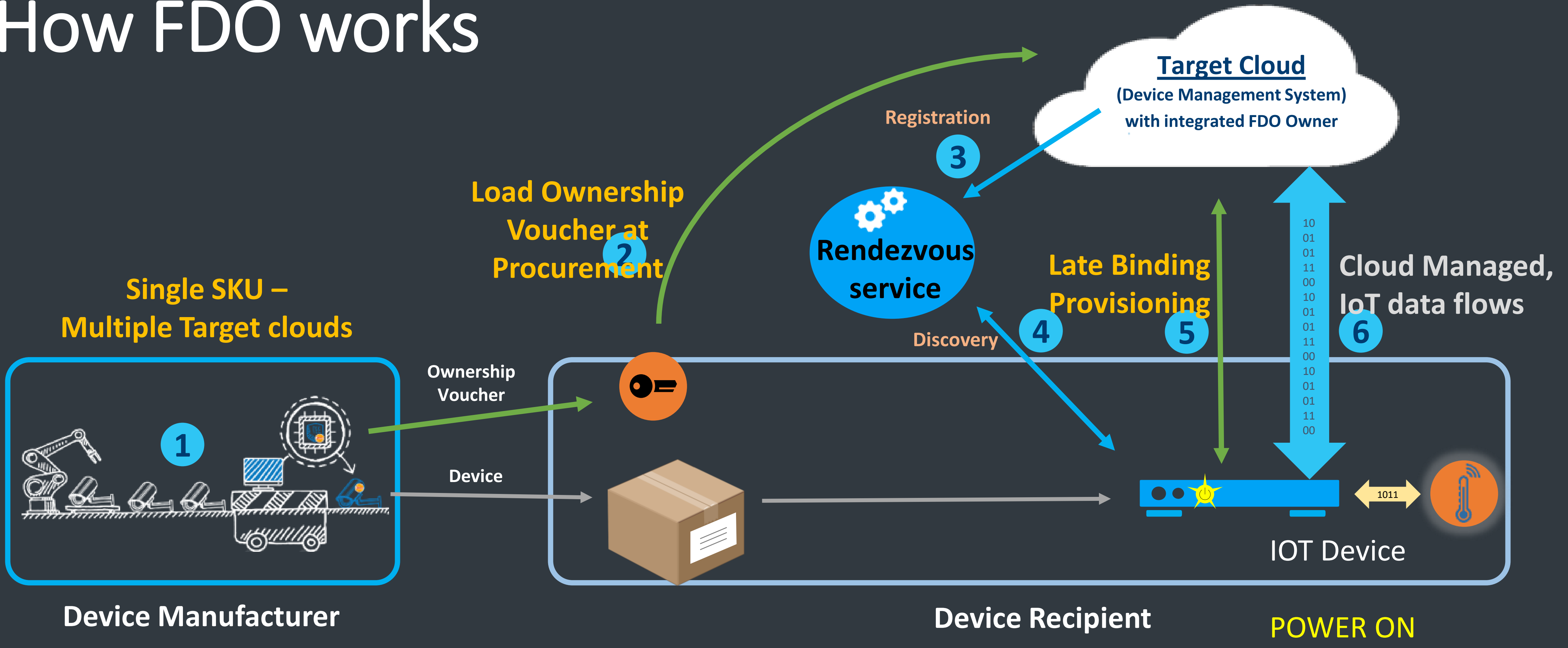
LF-Edge (Intel)	Java/C	X86 focus
VinCSS	Go / C	µProc (ESP32)
RedHat	Rust	Linux focus

- FDO 1.1 specification held steady to help implementors
  - 6 app notes published (1 pending)
  - FDO TPM spec (more later)
  - https://fidoalliance.org/specifications/download-iot-specifications/

- FIDO Alliance FDO Certification
  - FIDO conformance testing kickoff
  - Certification of implementations started (low security levels so far)
  - https://fidoalliance.org/fido-device-onboard/

https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-PS-v1.1-20220419/FIDO-Device-Onboard-PS-v1.1-20220419.html

How FDO works



Target Cloud

(Device Management System)

with integrated FDO Owner

Registration 3

Rendezvous service

Load Ownership Voucher at Procurement 2

Single SKU – Multiple Target clouds

Late Binding Provisioning 5

Discovery 4

Cloud Managed, IoT data flows 6

1

Ownership Voucher

Device

IOT Device

Device Manufacturer

Device Recipient

POWER ON

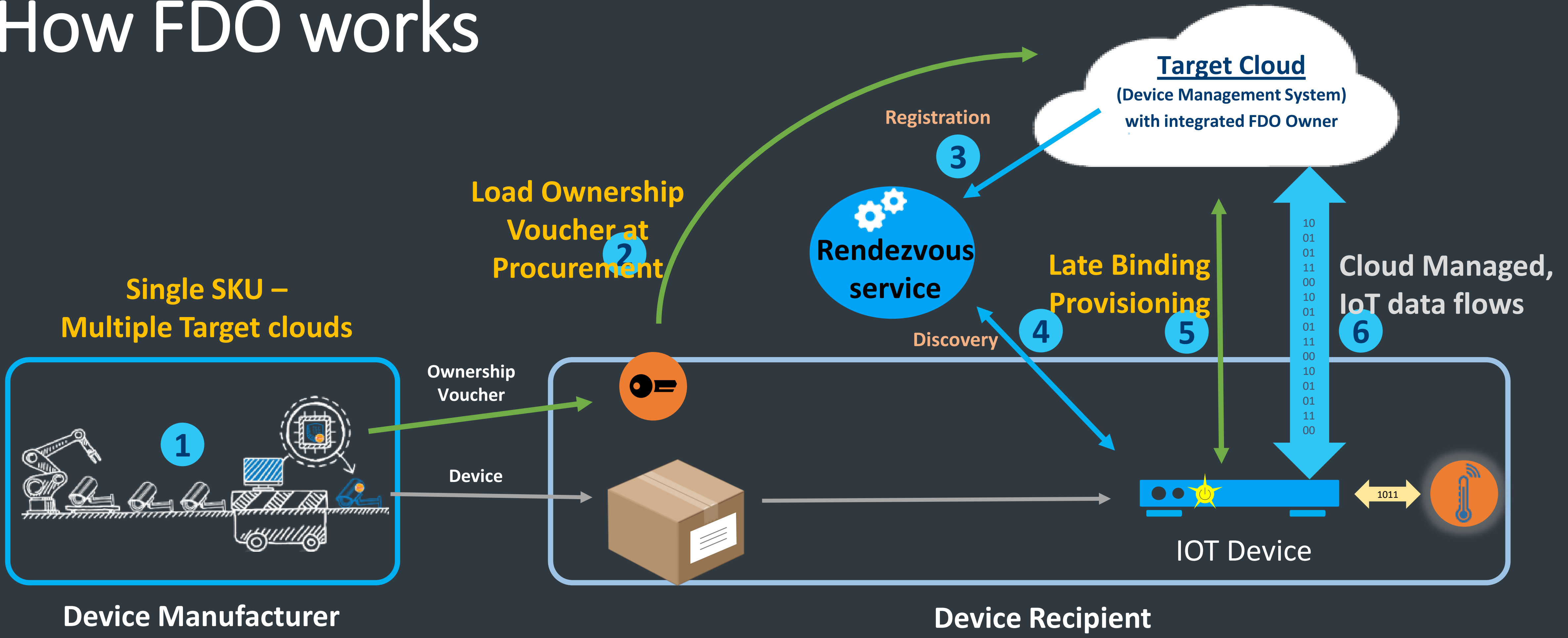
1 Build and Ship FDO Enabled Devices → 2 Register Ownership to Target Platform → 3 Register Device to Rendezvous Service → 4 Devices use FDO to find owner location → 5 Devices Authenticated and Provisioned → 6 Devices send sensor data to IoT Platform

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

How FDO is the same and different from IETF onboarding protocols (BRSKI, SZTP)

Feature	Mechanism	How same	How different
IETF foundations	Transport, Encoding	TCP (TLS)	CBOR, COSE, EAT
Discovery of server	Network discovery. Rendezvous Server.	Escape to use network discovery (RV Bypass)	Application server required, no change to or reliance on network.
Authorization via Supply Chain	Ownership Voucher	One voucher per device	Signed incrementally to each owner, permits routing in supply chain.
Mutual Authentication	Digital Signature	Device Certificate	Server authorized via Ownership Voucher
Encryption	TLS-like	KEX + Encrypted Messages	Implemented in FDO, not in TLS
Onboarding	ServiceInfo Modules	Usually download files, like everyone else	Sub-protocols with base functions for onboarding. Can be extended for custom non-shell applications.
Non-IETF protocols	Stream & Network independence	Runs over TCP most of the time	Can run over non-IP streams (with RV bypass)

FDO in TPM Specification – Review Draft

- Review Draft 10/2023 (to be posted shortly to FIDO Alliance web site)
- Standard for Storing FDO credentials in the TPM
  - You do NOT HAVE TO store FDO credentials in the TPM (e.g., if there isn't one!)
- When you DO have a TPM, features:
  - TPM's with credentials in the chip
  - Discovery of credentials (e.g., Linux startup)
  - Determine if FDO has run already (or needs to be run)
  - Use credentials to run FDO, of course!
  - Update credentials to run FDO again
  - Lock access to credentials until reboot
- Basic Security model:
  - System configuration must allow FDO to examine TPM for credentials before system normal startup. Could be BIOS or OS startup scripting.
  - FDO runs, or does not run
  - FDO locks credentials in TPM until next boot

https://fidoalliance.org/specifications/download-iot-specifications/

FDO in TPM Specification (2)

- Credentials are separated by security status
  - Keys/Secrets
  - Active flag (whether to run FDO or not)
  - Other FDO parameters
  - Ownership Voucher (optional, used to help TPM chip vendor initialize FDO on behalf of the eventual OS that will run it)
- Classes of credentials are assigned to known addresses in the TPM
- Security configuration for each is specified in the spec

Please read and review!

Thanks for your time