

FDO Discussion

4-28-2022

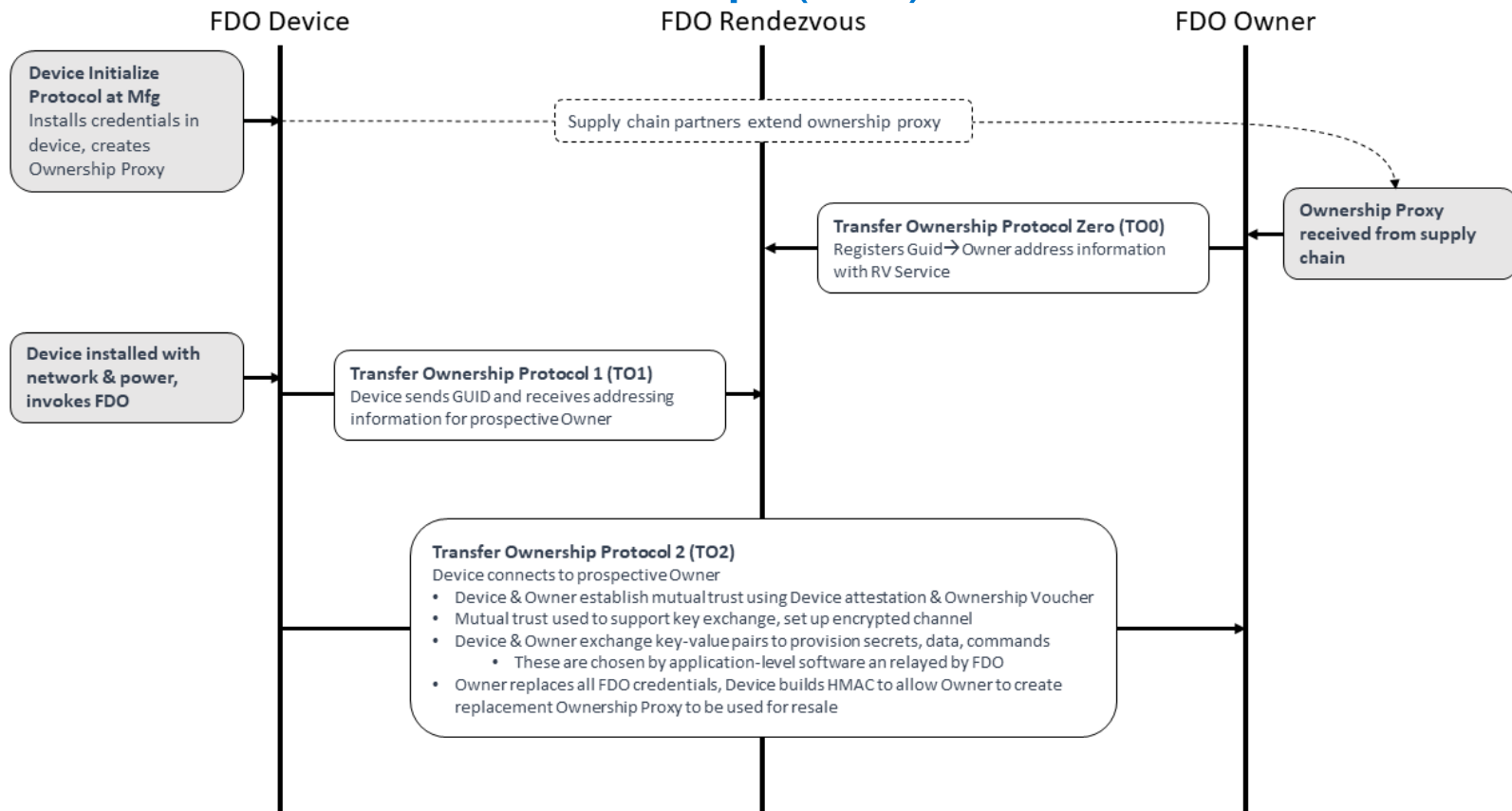
FIDO Device Onboarding (FDO)

- Device onboarding = Transfer of ownership = installing secrets and configuration data
- FDO provides “late binding” when the device is powered on at end user site
- Supports closed network with local Rendezvous Server
- During manufacturing, a FIDO Device configured with:
 - Restricted Operating Environment (ROE)
 - FIDO Device Onboard application running in ROE with device credentials
 - Rendezvous information for current owner of the device (i.e. manufacturer)
 - Ownership Voucher
 - (Optional) HWROT MCU for monolithic system image or TPM

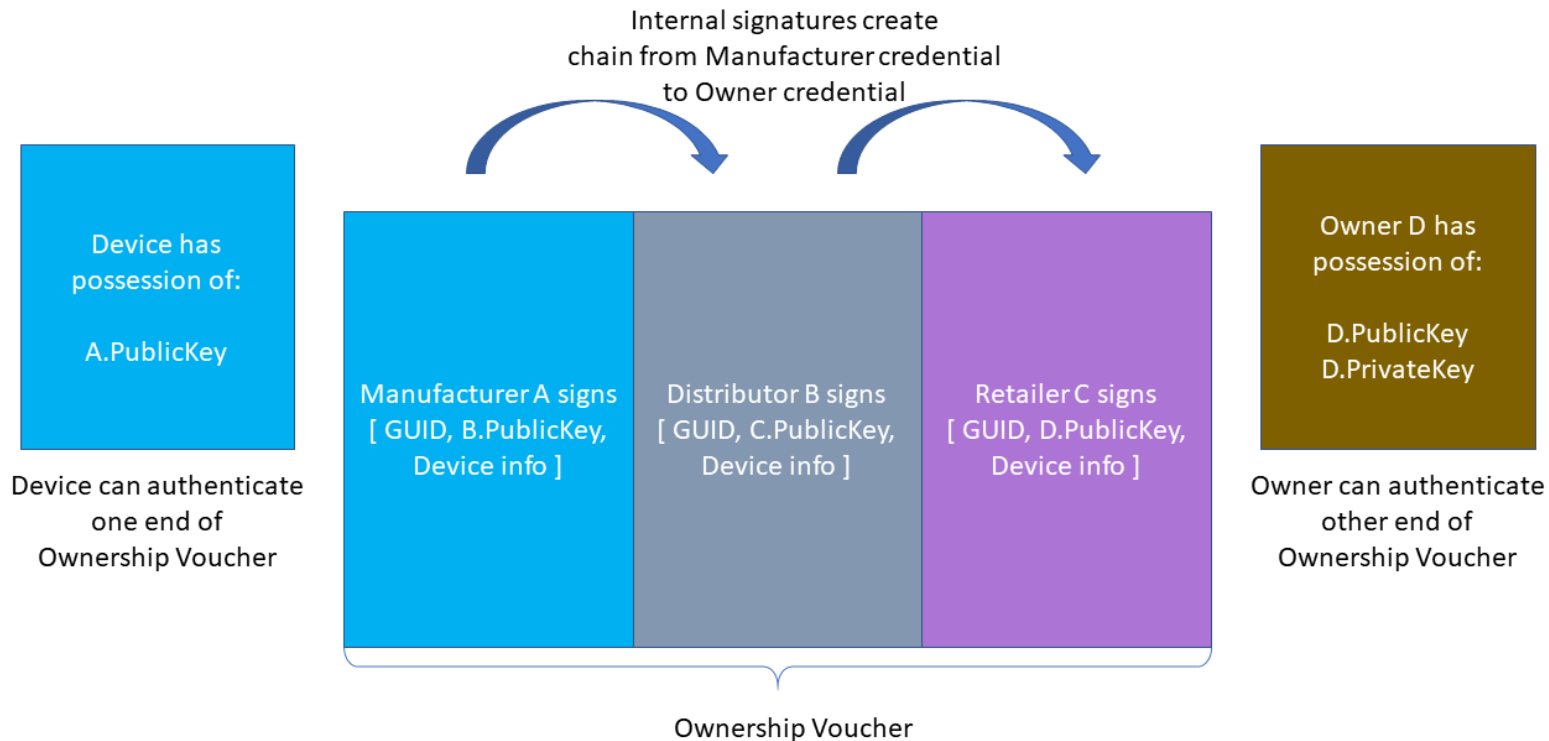
Issues with FDO

- Since UEFI is not a supported ROS it presumes the DPU has a supported ROS installed with FDO support prior to onboarding. Meaning another ZTP step is required before FDO or could drive separate solution SKUs for same DPU HW.
- Additional burden on DPU vendor or OEM to install FDO support at manufacturing including provisioning initial ownership and supplying ownership voucher with purchase.
- The manufacturing process would need to include service stock/spares that are shipped outside of a server.

FDO Transfer of Ownership (TO)

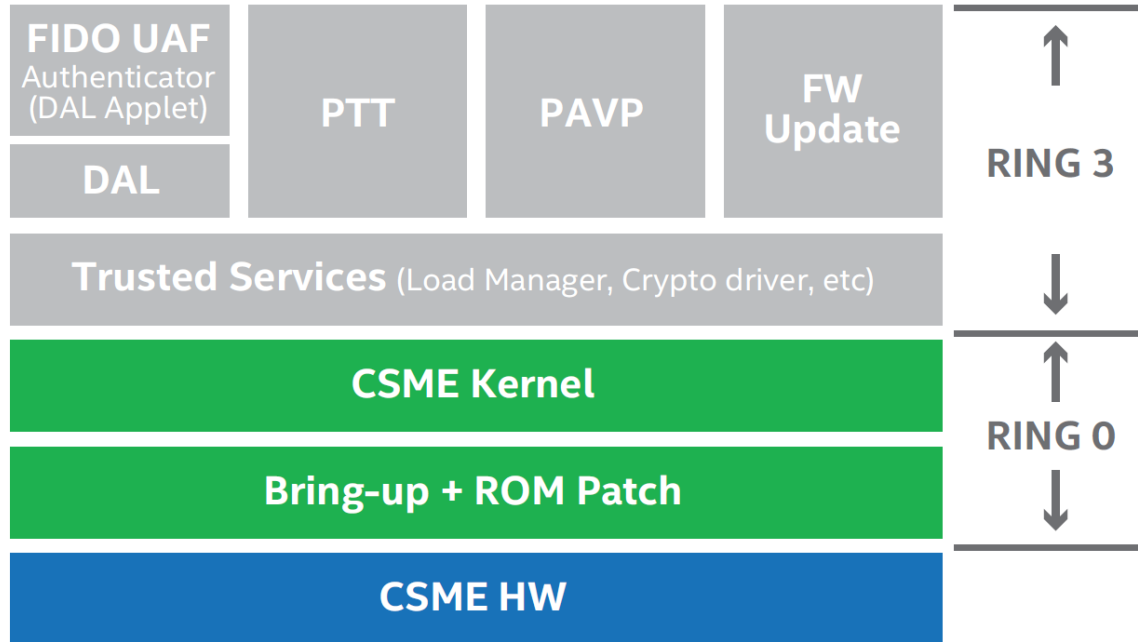


FDO Ownership Voucher

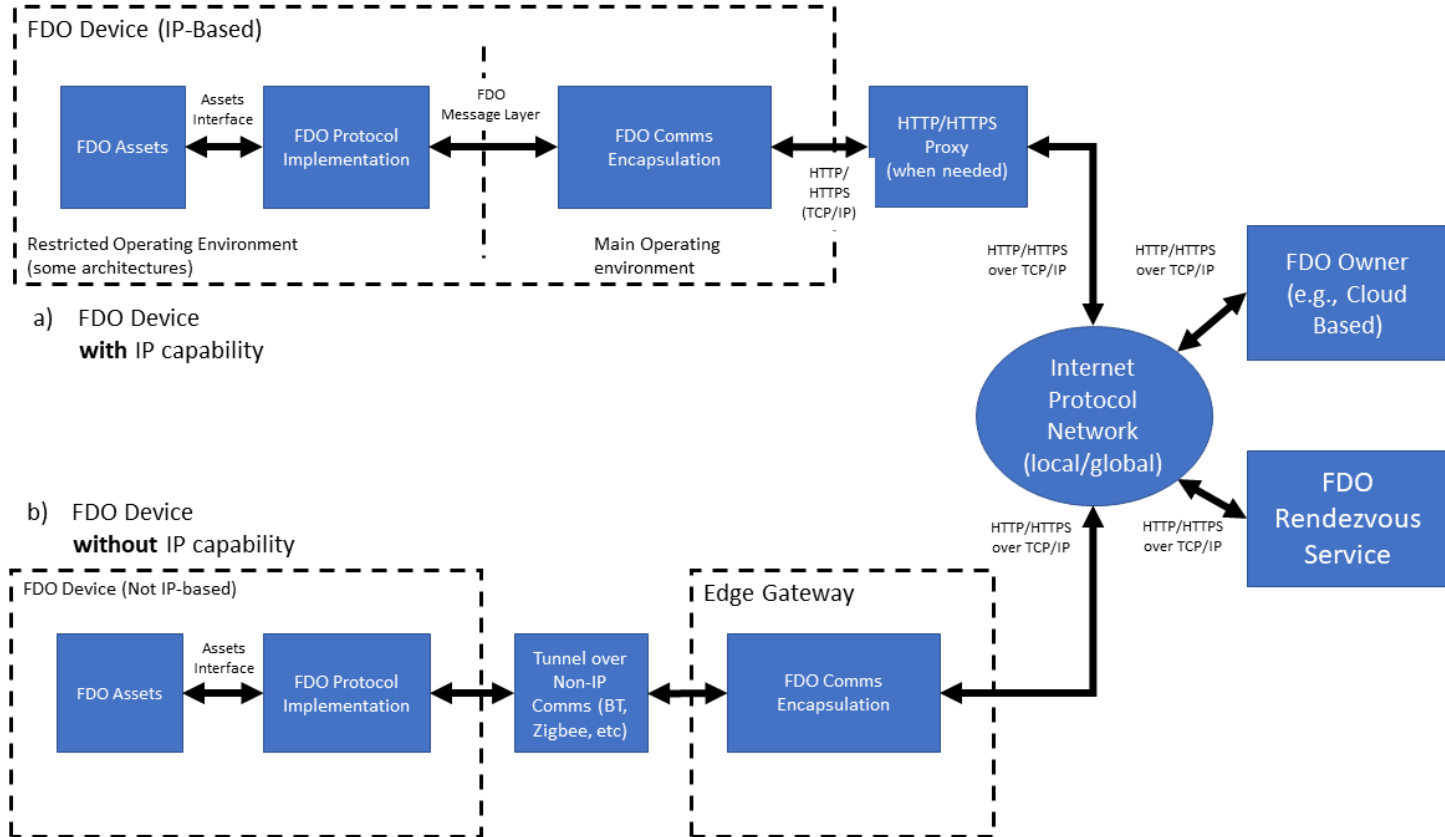


Backup

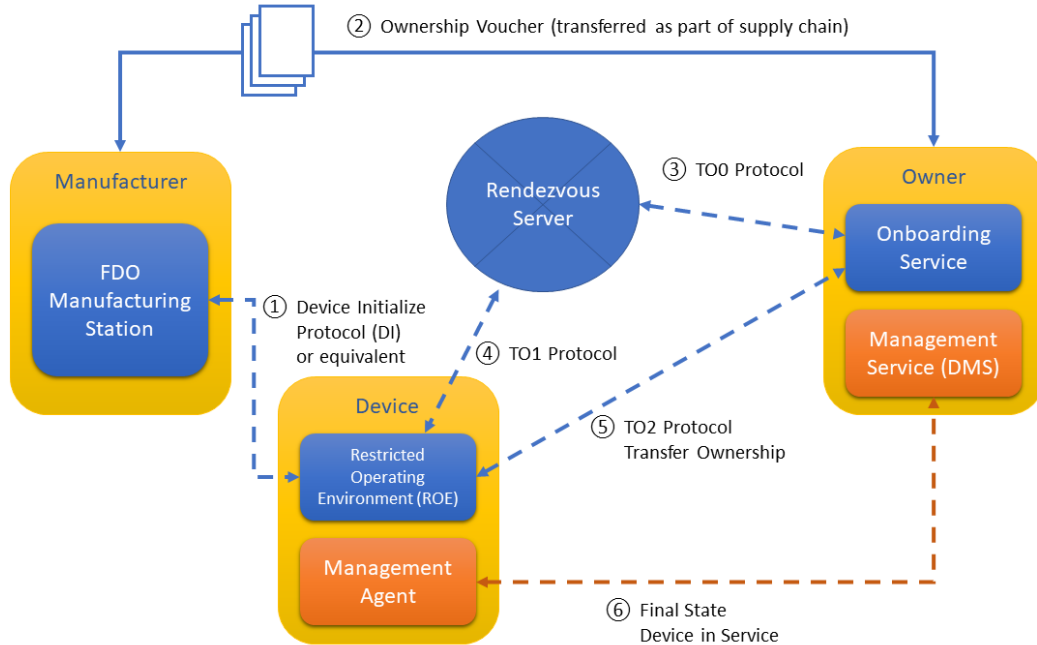
FIDO Stack



FDO transport



FIDO Device Onboarding



Reference

- FDO Device Onboard Spec - <https://fidoalliance.org/specs/FDO/>
- FIDO Support on Intel Platforms - <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/hardware-for-strong-authentication-white-paper.pdf>

DELLTechnologies