FDO (FIDO Device Onboard) Getting Started Guide

Document Number: 749823 – 1.0

October 2022
FDO Overview
Making Device Provisioning “Plug & Play”

**Legacy Manual Onboarding Approach**

Manual configuration = >20 minutes per device

Slow, insecure, expensive

**IoT Needs “Plug and Play” Model Similar to USB**

Add a printer with USB = ~1 minute per device

Fast, downloaded appropriate drivers, works with different hardware
Fast, Scalable Device Provisioning, Onboarding & Activation

**BENEFITS**

- Zero touch onboarding – integrates readily with existing zero touch solutions
- Can greatly lower onboarding costs
- Fast & more secure\(^1\) – ~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 FDO project up and running, code now on GitHub
- Provision your choice of OS on bare metal COTS Hardware
Provisioning with FDO

1. Build and Ship FDO Enabled Devices
2. Register Ownership Voucher at Procurement
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

Single SKU for Multiple Target clouds

Device Manufacturer

Device Recipient

Target Cloud (Device Management System) with integrated FDO Owner

Late Binding Provisioning

Cloud Managed, IoT data flows

Ownership Voucher

Device

IOT Device

Load Ownership Voucher at Procurement

Registration

Discovery

Load Ownership Voucher at Procurement

Enabled Devices

Device Power on

Device deployed
Hi, I am 123. Where is my management service?

Here is my RoT, Device GUID=123

I manage GUID 123. I’m available at this IP: 11.11.11.11

Here is my Ownership Voucher, I am the Owner for GUID 123

Try 11.11.11.11

Hi, I am 123. Where is my management service?
FDO Software Components
Onboarding with FIDO Device Onboard

1. **Manufacturer**
   - Manufacturer provisions device credentials via DI protocol, creates ownership voucher.

2. **System Integrator/ VAR**
   - Distributer sells device to next owner.

3. **Owner**
   - Owner registers device with Rendezvous Service via TO0 protocol.

4. **Rendezvous Service**
   - Device is installed and powered up; device contacts RV Service via TO1 protocol to obtain URI to Owners DMS.

5. **Device**
   - Device contacts Owner Service via TO2 protocol to obtain configuration information.

**Intel Client-FIDO**
- DI, T1 & T2 protocol support for Intel DAL-enable platforms.

**Client SDK-FIDO**
- DI, T1 & T2 protocol support for Intel non-DAL & TPM platforms and ARM processors. Portable to other architectures.

**Open-Source SW Component**

**Onboarding Process**

**Protocol Stages**

**Out-of-band B2B process**

**Key**
- Open-Source SW Component
- Intel SW Component
- Business Entity
- Onboarding Process
- Protocol Stages
FDO Manufacturer Toolkit Interactions

**Device**

- **FDO Database**
  - **DI Protocol**
  - **Store Key**
  - **Assign voucher (device) to customer**
  - **Extend voucher for device**
  - **Extended voucher**

**Business Systems**

- **Receive order**
- **Receive customer FDO public key**
- **Extended voucher and device to customer**

**Customer / Supply Chain**

- **Seq 1**
- **Seq 2**
- **Seq 3**
FDO Reseller Toolkit Interactions

1. **Device Supplier**
   - Reseller FDO public key(s)

2. **Seq 2**
   - Device order
   - Vouchers
   - Store Vouchers

3. **Seq 3**
   - Store Public Key

4. **Seq 4**
   - Assign device (voucher) to customer
   - Extend voucher
   - Extended voucher

---

**FDO Database**

- Device order
- Vouchers
- Store Vouchers
- Store Public Key
- Assign device (voucher) to customer
- Extend voucher
- Extended voucher

**Business Systems**

- Device order
- Extend voucher
- Extended voucher and device

**Customer or Supply Chain**

- Receive customer FDO public key
- Device order
Manufacturer Requirements
FDO Enabled Device Requirements

- FDO requires Device Initialization (DI) to run on each device at some point during or post manufacturing but before final shipment to customer.

- To run DI, the device must be powered up (and unboxed). (Note: DI is not a requirement if the manufacturer has other means to embed device credentials, then this could be utilized instead of DI).

- There must be some value for correlating the physical device to the Ownership Voucher (OV). This value should be on the device and any packaging it is shipped in. Typically, this is the device serial number and barcodes are used for conveying this value.

- Ownership Vouchers associated with the devices must be delivered to the customer (typically, this is via some B2B electronic transfer).
FDO Tools for Manufacturer Use

- The core tool for running a DI server for devices is the PRI-FIDOIOT Manufacturer Tool.

- On the device, you have the option of running the Client-Intel or Client-SDK.

- There is also the option of running the PRI-FIDOIOT All-In-One (AIO) tool. This encapsulates the PRI Manufacturer Tool along with the Rendezvous and Owner servers. Providing all these servers together allows an easy means to perform end-to-end testing/validation of the protocol on a device. Something which is recommended to be done periodically to ensure that the production devices performs properly.
Verification of FDO can be done by configuring AIO and running DI on the Device followed running TO1 and TO2. A sample payload can also be configured to be downloaded during TO2.

After verification, the configuration can be modified or a separate instance running PRI Manufacturer only can be used to run DI only. After DI is run, a target OS configured to run TO protocol on boot up can be installed. Or depending on the customer, they may install such an OS. In either case, FDO credentials are embedded in secure persistent memory from the DI process and can then be used by the FDO Agent to run the TO protocol.

**Note:** This is End to End Verification
Supply Chain Use Cases
• Depending on the manufacturer and supply chain, several different scenarios to support FDO are possible:

• Scenario 1: Direct to customer from manufacturer. End customer order devices directly from manufacturer, and then devices and OVVs are delivered to customers.

• Scenario 2: Post manufacture. SI (or equivalent) orders (FDO compatible) devices from one-to-many manufacturers, performs DI and then ships to end customers.

• Scenario 3: Manufacturer and distributor supported. Manufacturer offers FDO option and when selected, performs DI on device as part of manufacturing and then delivers devices and vouchers to distributor, who then extends the OV to the customer.

• Scenario 4: Full FDO support throughout supply chain.

• Other scenarios ...
FDO Supply Chain
Scenario 1: Directly to customer from manufacturer

Device Manufacturer (ODM, OEM)

PRI Manufacturer

DI Protocol

FDO Client

Customer A
Device Install

Customer B
Device Install
FDO Supply Chain
Scenario 2: Post manufacture

Device Manufacturer → FDO compatible device

PRI Manufacturer → DI Protocol → FDO Client → unbox

SI (or equivalent) → OV

Customer A → Device Install

Customer B → Device Install
FDO Supply Chain
Scenario 3: Manufacturer and distributor supported
Scenario 4: Support throughout supply chain

- Device Manufacturer (ODM, OEM, SI)
- Distributor / Reseller
- Online Retailer

Customer

- FDO Client
- PRI Manufacturer
- PRI Reseller
- PRI Reseller

Intel supplied tool

Device Install
Important Links
FDO RESOURCES

1. FIDO Specification
   Introduction
   https://fidoalliance.org/intro-to-fido-device-onboard/

2. Developer Docs and SDKs (LF Edge)
   https://www.lfedge.org/projects/securedeviceonboard/

3. Key Field Collateral
   Resource & Documentation Centre

4. Intel specific Developer Docs and SDKs
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2022</td>
<td>1.0</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Legal Disclaimer

- This presentation is not meant to be exhaustive and is provided AS IS, for convenience and information only and is not to be relied upon for any purpose, other than educational. The presentation is intended only to provide the general insights, opinions, and/or internally developed guidelines and procedures of Intel Corporation (Intel). The information in this presentation may need to be adapted to your specific situation or work environment.

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.

- This material may relate to the creation of end products used in safety-critical applications designed to comply with functional safety standards or requirements (“Safety-Critical Applications”) or any application in which failure of the Intel product could result, directly or indirectly, in personal injury or death. It is your sole responsibility to design, manage and assure system-level safeguards to anticipate, monitor and control system failures, and you are solely responsible for all applicable regulatory standards and safety-related requirements concerning your use of any material related to Safety Critical Applications.

- You further agree that some of the material maybe be pre-production in nature and that all material is provided "as is" without any express or implied warranty of any kind.

- The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

- Intel technologies may require enabled hardware, software or service activation.

- No product or component can be absolutely secure.

- The code names presented in this document are only for use by Intel to identify products, technologies, or services in development, that have not been made commercially available to the public, i.e., announced, launched or shipped. They are not "commercial" names for products or services and are not intended to function as trademarks.

- © Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.