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

Plenary, September 2019
Derived Requirements from Use Cases

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Open Solution</td>
</tr>
<tr>
<td>R2</td>
<td>Automatic Onboarding</td>
</tr>
<tr>
<td>R3</td>
<td>Authorization (to onboard) is end-to-end</td>
</tr>
<tr>
<td>R4</td>
<td>Communications Independence</td>
</tr>
<tr>
<td>R5</td>
<td>Late Binding</td>
</tr>
<tr>
<td>R6</td>
<td>Permits Supply Chain Flexibility</td>
</tr>
<tr>
<td>R7</td>
<td>Repurpose / Resale</td>
</tr>
<tr>
<td>R8</td>
<td>Limit Correlation Attacks (Breadcrumbs)</td>
</tr>
<tr>
<td>R9</td>
<td>Deferred Acceptance</td>
</tr>
<tr>
<td>R15</td>
<td>Trusted and Untrusted Installer</td>
</tr>
<tr>
<td>R16</td>
<td>Localized authentication</td>
</tr>
<tr>
<td>R17</td>
<td>Internet, Home, Enterprise &amp; Closed networks</td>
</tr>
<tr>
<td>R18</td>
<td>IOT Owner need not be Network Owner</td>
</tr>
<tr>
<td>R19</td>
<td>Target device range (CPU/RAM/UI/OS etc.)</td>
</tr>
</tbody>
</table>

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:

Issue Tracking:
GitHub

Editors:
- Geoffrey Cooper (Intel)
- Brad Behm (Amazon)
- Ankur Chakrabarty (Google)
- Hanu Kommalapati (Microsoft)
- Giri Mandyam (Qualcomm)
- Hannes Tschofenig (ARM)

Contributors:
- Vitali Bartisch (TrustKey)

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](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 Device Provisioning, Onboarding & Activation

**BENEFITS**

- **Zero touch onboarding** – integrates readily with existing zero touch solutions
- **Fast & more secure** – ~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 1st spec draft

---

1. No product or component can be absolutely secure
FIDO Device Onboard: Late Binding in Supply Chain

Zero Touch without FDO
IoT device software and security customization happens during manufacturing
Result: Complicated build-to-order manufacturing infrastructure, many SKUs, small lot sizes, long lead times, higher cost

Zero Touch with FDO
IoT device software and security customization happens at the end of the supply chain
Benefits: Simplified build-to-plan manufacturing infrastructure, fewer SKUs, large lot sizes, enable stocking distributors, low customization cost
Result: Increased supply chain volume and velocity

Late binding reduces costs & complexity in supply chain – a single device SKU for all customers
Provisioning with FIDO IOT

Single SKU – Multiple Target clouds

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

Device Manufacturer

Device Recipient

Target Cloud (Device Management System) with integrated FIDO IOT Owner

Registration

Load Ownership Voucher at Procurement

Rendezvous service

Late Binding Provisioning

Cloud Managed, IoT data flows

Ownership Voucher

IOT Device power on

Discovery

Registration

Late Binding Provisioning
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?
Requirements to achieve Late Binding

- Manufacturer Credentials only used for onboarding
- Warehousing of Device. Final destination may not be known
- Provisioning of Device. Kind and quantity of credentials varies
- Network Topology. Internet, Intranet, Closed Network

- Security of device identity
- Flexibility of supply chain
- Different clouds use different credentials
- 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
FDO vs SDO

Intel ® Secure Device Onboard (SDO) was submitted to FIDO for consideration

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

SDO/FDO Differences in terminology
- TEE → ROE
- AppID → Multi Application ROE Prefix (MAROEPrefix)

FDO/SDO Syntactic Differences
- CBOR
- COSE - including authenticated encryption
- EAT

FDO/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: FDO IANA Assigned numbers
FIDO Device
Onboard