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

<table>
<thead>
<tr>
<th>LF-Edge (Intel)</th>
<th>Java/C</th>
<th>X86 focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>VinCSS</td>
<td>Go / C</td>
<td>μProc (ESP32)</td>
</tr>
<tr>
<td>RedHat</td>
<td>Rust</td>
<td>Linux focus</td>
</tr>
</tbody>
</table>

• 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/

How FDO works

1. Build and Ship FDO Enabled Devices
   - Device manufacture – supply chain

2. Register Ownership to Target Platform
   - Device power on

3. Register Device to Rendezvous Service
   - Device deployed

4. Devices use FDO to find owner location

5. Devices Authenticated and Provisioned

6. Devices send sensor data to IoT Platform

---

**Device Manufacturer**

1. Single SKU – Multiple Target clouds

2. Load Ownership Voucher at Procurement

---

**Device Recipient**

3. Registration

4. Discovery

5. Late Binding Provisioning

**Target Cloud**

6. Cloud Managed, IoT data flows

---

**Rendezvous service**

---

**Device**
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

Single SKU – Multiple Target clouds

Load Ownership Voucher at Procurement

Rendezvous service

Target Cloud
(Device Management System) with integrated FDO Owner

Registration

Discovery

Late Binding Provisioning

Cloud Managed, IoT data flows

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

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