FIDO Device Onboard: A specification for automated, secure IoT provisioning technology

Improves IoT security and reduces costs with automated onboarding

In the world of IoT, the first thing referenced is often the size of the market opportunity. Numbers in billions are often presented in terms of volume of units. IDC expects the IoT market to maintain a double-digit annual growth rate and surpass the $1 trillion mark in 2022. Talked about less is what it will take for the opportunity of IoT to be realized. At the heart of this are costs and complexities of 'onboarding' IoT devices in industrial, enterprise or consumer applications.

IoT device onboarding involves the installation of the physical device and the setup of credentials so that it can securely communicate with its target cloud or platform. Today this onboarding process is usually done manually by a technician – a process that is slow, expensive, and insecure. Industry sources have said that it is not uncommon for the cost of installation and setup to exceed the cost of the device itself.

Although multiple companies have worked to automate the onboarding process, there wasn't a widely accepted industry standard. Also, many proprietary solutions that do exist require that the end customer be known at the time of the device manufacture so that the device can be pre-configured. This creates friction and cost in the supply chain.

The FIDO Alliance stepped up in the summer of 2019 to address this industry challenge. With its broad membership of leading cloud service providers, semiconductor companies and security companies, the Alliance is well positioned to bring together those that create and supply the technologies in the IoT ecosystem. The FIDO Alliance formed its IoT Technical Working Group (IoT TWG) with these stakeholders to define a new standard for automated, secure IoT onboarding.

Less than 2 years after the working group formed, the FIDO Alliance is now releasing to the industry the FIDO Device Onboarding (FDO) specification.

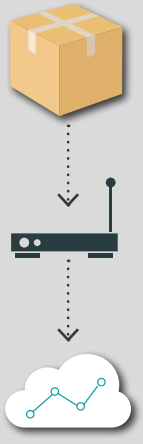
Creating a Standard for IoT

The FIDO Alliance IoT TWG began its work by creating a list of target use cases to address. They then examined current industry solutions to see if any could be readily adapted to meet these use cases. Intel offered its Secure Device Onboarding (SDO) technology to the working group and this was accepted as the foundation for the new specification. The technical editors of the working group (which included representatives from Arm, Amazon Web Services, Microsoft, Google, Intel, Infineon and Qualcomm) identified where gaps existed and how these could best be closed. The fruits of this work are represented in the FDO specification.

Benefits of FDO

FDO Provides these benefits:[1]

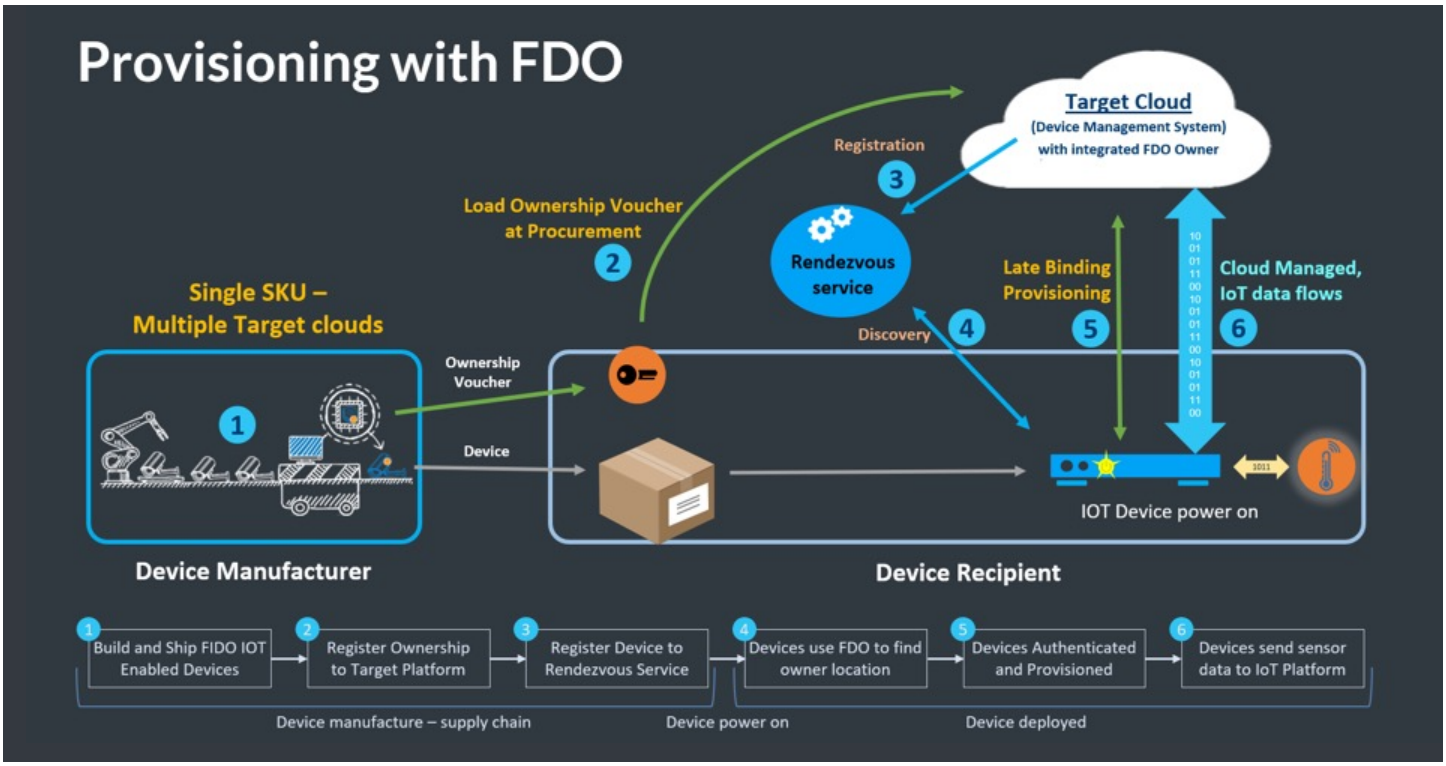
- Zero touch onboarding – integrates readily with existing zero touch solutions
- Fast & more secure[1] – ~1 minute
- Hardware flexibility – any hardware – from ARM MCU to Intel® Xeon® processors
- Any cloud – internet & on-premise
- Late binding of device to cloud greatly reduces number of SKUs vs. other zero touch offerings
- Open specification
- Industry standard via FIDO Alliance
- Specification developed by leading Cloud Service Providers, Semiconductor companies and security companies.



Note 1: No product or component can be absolutely secure

How Does FDO Work?

The figure below illustrates how FDO works.

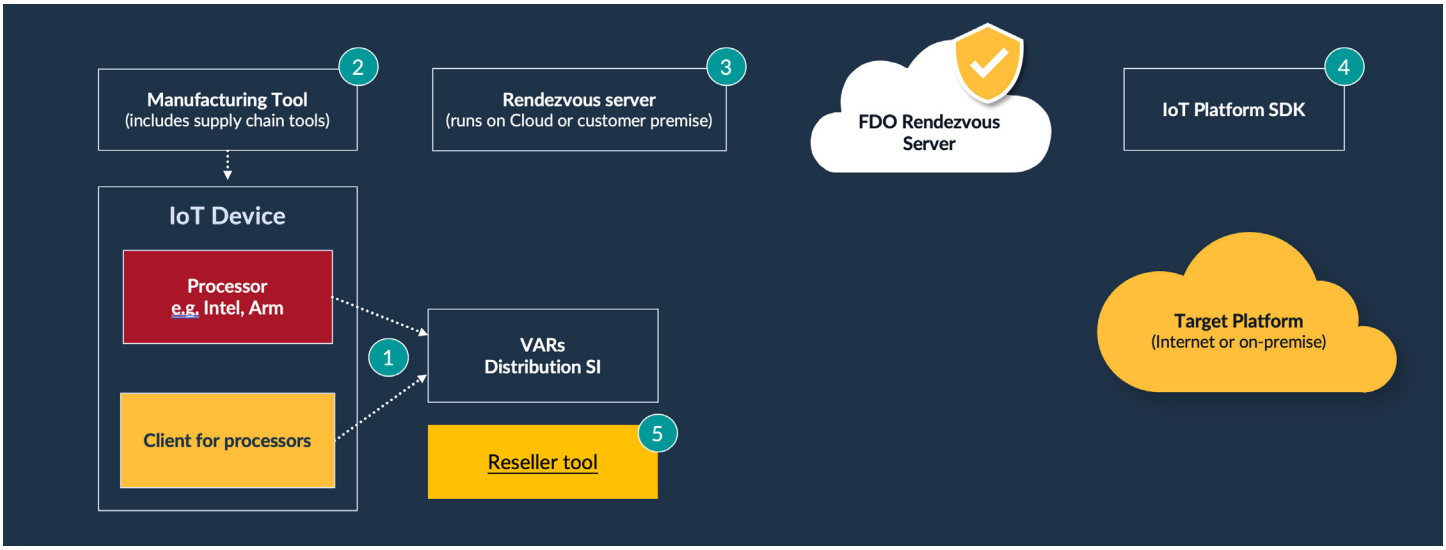


1. At the manufacturing stage of the IoT Device (or if preferred, at a later time), the FDO software client is installed on the device. A Root of Trust key (RoT) is also created inside the device to uniquely identify it. This RoT can take the form of cryptographic keys built into the silicon processor (or associated TPM) at the time of manufacture or alternatively can be placed in the file system. Other FDO credentials are also placed inside the device together with web addresses that will be needed later in the process.

   Lastly, a digital proof of ownership (known as the Ownership Voucher and represented as the orange/black key in the figure) is created outside the device. This self-protected digital document (can be transmitted as a text file) allows the owner of the Device to identify themselves later in the onboarding process. Changes to the target cloud for this device can be registered by changing the Ownership Voucher, without unboxing the device.
2. The IoT device passes its way through the supply chain (e.g. from distributor to VAR, etc. The Ownership Voucher file follows a parallel path.
3. Once the target cloud or platform is selected by the Device owner, the Ownership Voucher is sent to that cloud/platform. In turn, the Ownership Voucher is registered with the Rendezvous Server (RV). The RV acts in a comparable way to a DNS service.
4. When the time for device onboarding comes, the device is connected to the network and powered on. After the device boots up, it 'calls' the Rendezvous Server (RV) that was programmed into it in Step 1. The device identifies itself to the RV and in turn the RV matches the device to its target cloud/platform. The web address for the target cloud/platform is provided to the device. Multiple RV's can be programmed into the device, including both on-prem and cloud.
5. Based on the information provided by the RV in the prior stage, the device contacts the cloud/platform. The Device uses its Root of Trust to uniquely identify itself to the cloud/platform and in return the cloud/platform identifies itself as the device owner using the Ownership Voucher. Next, these mutual attestations allow a secured, encrypted tunnel to be created between the device and the cloud/platform.
6. The cloud/platform can now download over the encrypted tunnel whatever credentials or software agents are needed for correct device operation and management. FDO allows the credentials to vary so that IoT solutions owners do not have to change their solution when they adopt FDO. This step completes the FDO process. The device contacts its management platform, which will manage it for the rest of its lifecycle. FDO lies dormant, although it can be re-awakened in the event of a transfer of ownership of the device e.g. its sale.

FDO software components

The major software functions within FDO are shown in the diagram below.



1. The FDO Client placed on the IoT Device
2. The Manufacturing tools that installs the Device credentials and creates the Ownership Voucher
3. The Rendezvous server (which can be run in the cloud or on-premise)
4. The FDO Platform SDK that is integrated into the target cloud or on-premise platform
5. A Reseller tool that can be used by the supply chain ecosystem to extend the Ownership Voucher's cryptographic key
6. Additionally, tools for provide initial network access for the Device (not shown)

Applications of FDO

FDO has been developed to address a wide range of IoT applications in the world of industrial and enterprise. Moving forward it is expected to be extended to support consumer/home applications.

"The demand for automatic onboarding, traceability and updating of assets is growing, and manufacturers are challenged to rapidly identify and replace defective devices before they disrupt operations," said Riky Comini, Senior Director of Industrial Automation, Molex. "Integrating FDO into our IAS4.0 platform will prove invaluable in informing our roadmap for the future of industrial automation and Molex's broad portfolio of industry-leading connectivity solutions."

"The Open Horizon project wanted a simple solution to zero-touch provisioning that would have wide support from hardware manufacturers, maximum flexibility, and a staged approach. The FDO specification from the FIDO Alliance certainly meets those requirements. After implementing and shipping support in Open Horizon, we're pleased with the results and with the feedback we've received from those using it in the field," said, Joe Pearson, Technology Strategist, IBM Cloud and Technical Steering Committee Chair, Open Horizon project. "We're looking forward to implementing FDO in our Smart Agriculture SIG's use cases, and in the Open Retail Reference Architecture."

"This is a major milestone that aims to solve one of today's critical challenges with deploying IoT systems. The new FDO standard will help reduce cost, save time and improve security, all helping the IoT industry to expand rapidly," said Christine Boles, Vice President, Internet of Things Group and General Manager, Industrial Solutions Division at Intel. "Implementation of the FDO standard will enable businesses to truly take advantage of the full IoT opportunity by replacing the current manual onboarding process with an automated, highly secure industry solution."

Accelerating FDO market adoption with Open Source software

Having an industry onboarding specification with FIDO is a major step forward. However, mass deployment will require multiple companies in the supply chain (device manufacturers, semiconductor companies, cloud service providers, etc.) to create and deploy FDO compliant software and associated tools. To jump start this, the FIDO Alliance has made early versions of the FDO specification available publicly so that software development could take place within the Open Source community. Linux Foundation Edge (LF-Edge), a software community focused on building an Open Source Framework for the Edge, represents an ideal landing place for this effort. Intel offered its SDO software to the Linux Foundation – Edge and a project was officially kicked off in summer 2020. More details can be found at https://www.lfedge.org/projects/securedeviceonboard.

The software team working within LF-Edge expect to have an alpha code implementation of FDO in Spring 2021 and a released version by Summer 2021.

Getting involved

Whether you are an end customer, OEM, ODM, cloud provider or silicon player, FDO can bring value to you and your customers.

To learn more, reach out to the FIDO Alliance (info@fidoalliance.org) or the Linux Foundation Edge Secure Device Onboard project (sdo-info@lfedge.org).