

FIDO Alliance Input to Ministry of Economy, Trade and Industry (METI)

IoT Product Security Conformity Assessment Scheme Policy Draft

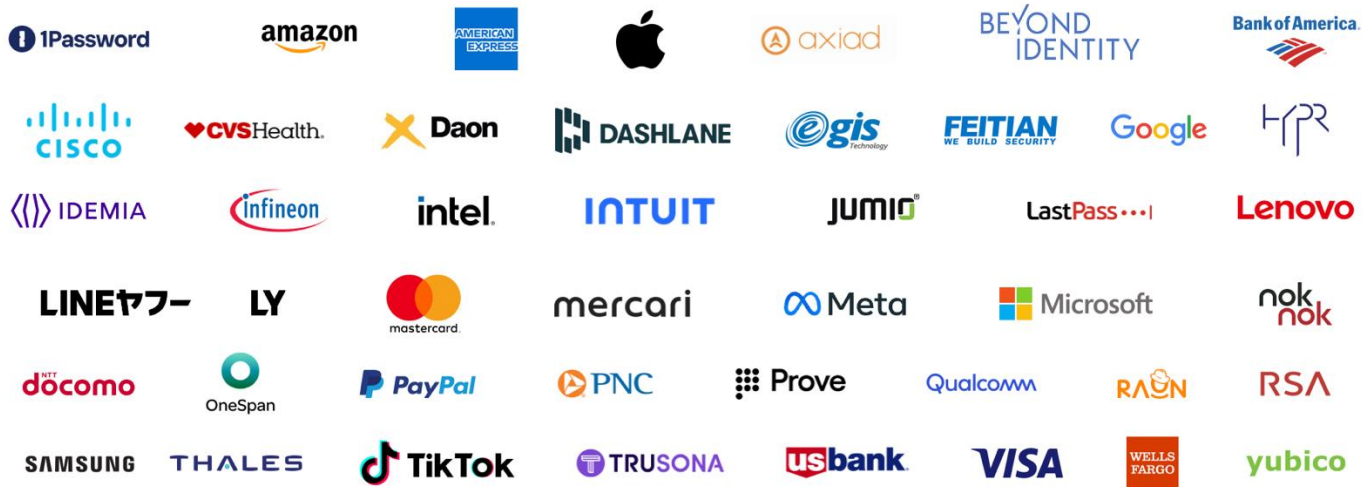
April 2024



The Fast Identity Online (FIDO) Alliance appreciates the opportunity to submit comments on the *IoT Product Security Conformity Assessment Scheme Policy Draft* published by METI.

As background, the FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for robust authentication and secure device onboarding.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance’s leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology.



The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eleven years that have followed – has helped to transform the authentication market.

Today, the FIDO standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy authentication tools.

In 2019, the FIDO Alliance broadened its focus on authentication of people to also look at authentication of things. FIDO Alliance formed a working group that has focused on addressing the challenge of how to “onboard” enterprise, edge or IoT devices to a cloud, network or management platform. The resulting standard, known as FIDO Device Onboard (or FDO), eliminates reliance on passwords, thereby providing a much higher level of security – as well as greater operational efficiency. The FDO specification was written by technology leaders including Intel, Amazon, Google, Microsoft, Qualcomm and ARM and was released in December 2020. An update (Ver 1.1) was released in December 2021.¹ More details on how FDO works are provided later in this document.

More notable with regard to METI’s draft IoT Product Security Conformity Assessment Scheme Policy, FIDO Alliance launched a certification program for FDO products in 2023.

¹ See <https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.1-20211214/FIDO-device-onboard-spec-v1.1-rd-20211214.pdf>

The **FIDO Device Onboard (FDO) Certification Program** is a product certification program intended to certify edge and IoT device implementations of FIDO. These *connected devices* are components defined in the FDO specification, certification requirements, and policy documentation.²

FDO Certification is intended to certify, evaluate, and validate functional and security characteristics, or functional-only characteristics, depending on the component, enabling edge node and IoT device vendors to prove that their solutions adhere to the security and interoperability requirements of the FDO specifications and requirements. Achieving certification allows vendors to demonstrate their products are high quality and at low risk of cyber-threats, while deploying companies can ensure devices will interoperate seamlessly and securely within IoT and distributed computing infrastructures.

An FDO system consists of three major components; (1) The Device that is to be onboarded (an edge or IoT device), (2) An Owner, which is the server or cloud that will manage the Device and (3) a Rendezvous Server, which re-directs the Device to its target Owner during the onboarding process.

Assessment of the functional characteristics is achieved by successfully completing Functional Certification, and similarly, security characteristics are assessed by successfully completing Security Certification.

Certifiable Implementations of FDO include:

1. **Devices:** are manufactured devices enabled with FIDO and ready for provisioning, also known as ‘End Products,’ like PCs, gateways, security cameras, etc. [Subsequent reference and naming might also include “FDO-Enabled Devices”, having the same meaning as “Devices”.]
2. **Device Onboarding (DO) Services:** a component of the device Management Service and connected device platform, rather than a separate network service, constructed to perform FIDO Device Onboard protocols on behalf of the Owner.
3. **Rendezvous Servers (RV):** a server configured to connect and register a Device implementing FIDO with an Owner.

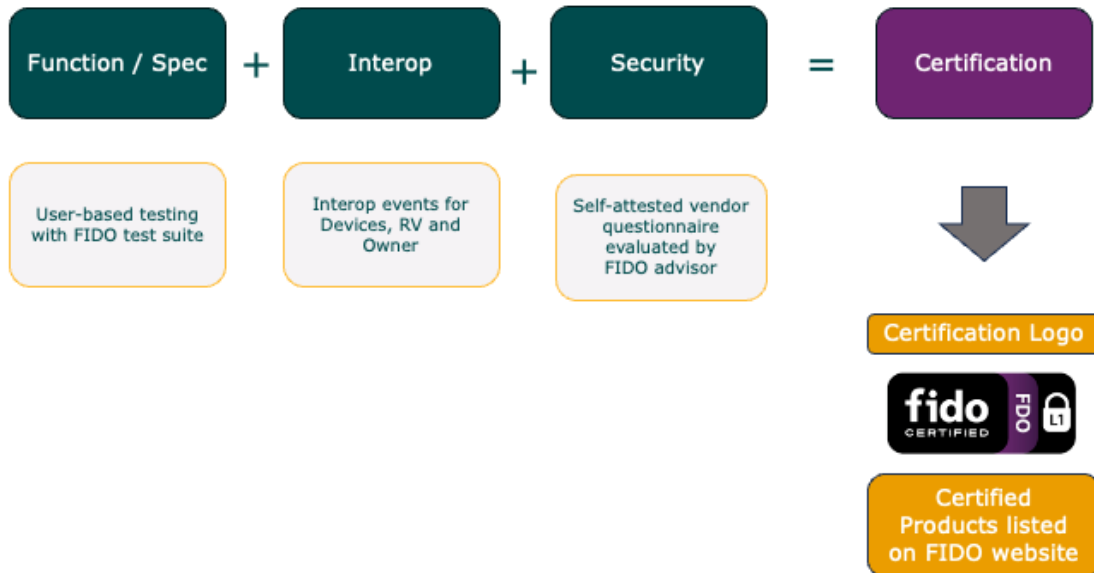
Functional Certification is required for all certifiable implementations: Device Onboarding (DO) Services, Devices, and Rendezvous Servers (RV). Security Certification is required for Device Onboarding Services and Devices meeting the FDO Security and Privacy requirements.

As METI considers ways to establish a security conformity assessment system for IOT products, there are two ways where we believe the FDO Certification program may be useful:

1. METI may be able to leverage some of the work FIDO Alliance has done to test and certify FDO products as METI crafts its own conformance assessment scheme for IOT products
2. METI could choose to recognize FDO Certification as one way that companies in Japan can demonstrate their conformance with METI requirements. This approach would allow METI to leverage an existing, global certification program rather than create its own.

² A more complete briefing on the FDO Certification program can be found at <https://fidoalliance.org/fido-device-onboard/>

The FIDO Certification Flow



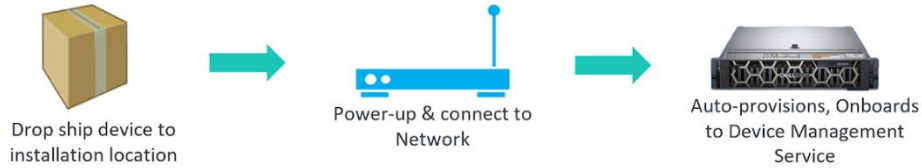
About FIDO Device Onboard (FDO)

FDO is an automated, secure, onboarding system that can be applied to a wide variety of applications. It differs from more consumer centric solutions (such as Matter), in that it assumes that the installer of the equipment is untrusted (i.e. the installer is trusted to have physical access to a location but not to any secure credentials).

Additionally, FDO provides late binding, which means that any FDO enabled device can be onboarded to any platform i.e. devices do not need to be manufactured or configured for a specific customer. This reduces manufacturing and inventory costs.

FDO meets and exceeds the Zero Trust concept in that it authenticates both the device and the server/owner at the time of onboarding.

FDO: Fast, Scalable Device Provisioning, Onboarding & Activation



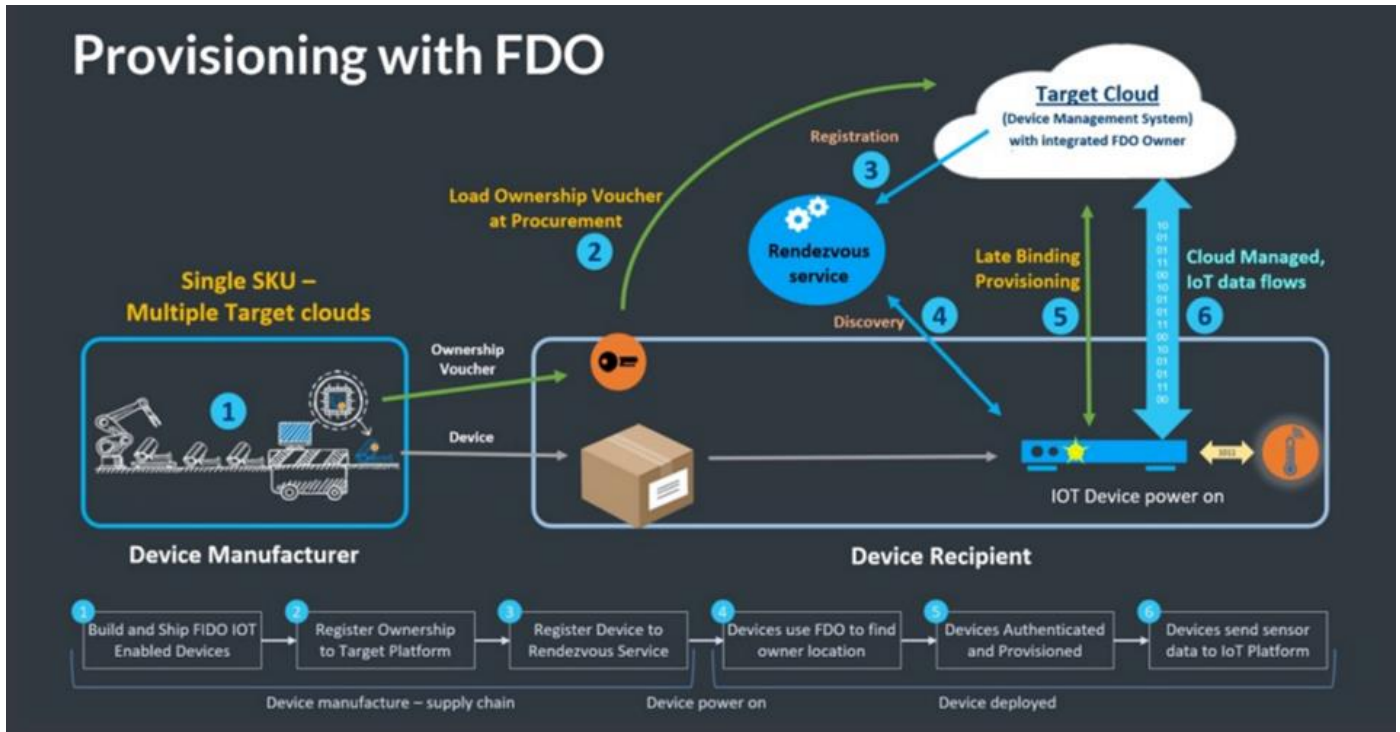
Benefits¹

- Zero touch onboarding – integrates readily with existing zero touch solutions
- Fast & more secure¹ – ~1 minute
- Hardware flexibility – any hardware (ARM MCU to Intel® Xeon®)
- Any cloud – internet, intranet & closed network (“on premises”)
- Late binding - of device to cloud greatly reduces number of SKUs vs. other zero touch offerings
- Implemented – 5 Independent implementations, various programming languages:
 - LF-Edge (Intel), RedHat, VinCSS, Feitan, FIDO test suite
- Certification suite available

3 1. No product or component can be absolutely secure
© FIDO Alliance 2023

CONFIDENTIAL

How FIDO Device Onboard (FDO) works



The following steps are aligned with the numbers in the figure:

1. At the manufacturing stage of the device (or later if preferred), the FDO software client is installed on the device. A trusted key (sometimes called an IDevID or LDevID) is also created inside the device to uniquely identify it. This key may be built into the silicon processor (or associated Trusted Platform Module, know as TPM) or protected within the file system. Other FDO credentials are also placed in the device. A digital proof of ownership, known as the Ownership Voucher (represented as the orange/black key shape in the figure) is created outside the device. This self-protected digital document can be transmitted as a text file. The Ownership Voucher allows the owner of the device to identify themselves during the onboarding process.
2. The device passes its way through the supply chain (for example, from distributor to VAR). 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 Domain Name System (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 uses the Rendezvous Server (RV) to find its target cloud/platform. On-premise and cloud-based RVs can be programmed into the device.
5. Based on the information provided by the RV, the device contacts the cloud/platform. The device uses its trusted key 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, the device and owner perform a cryptographic trick called a key exchange to create a secured, encrypted tunnel between them.

- The cloud/platform can now download credentials and software agents over this encrypted tunnel (or whatever else is needed for correct device operation and management). FDO allows any kind of credential to be downloaded, so that solution owners do not have to change their existing solution when they adopt FDO.

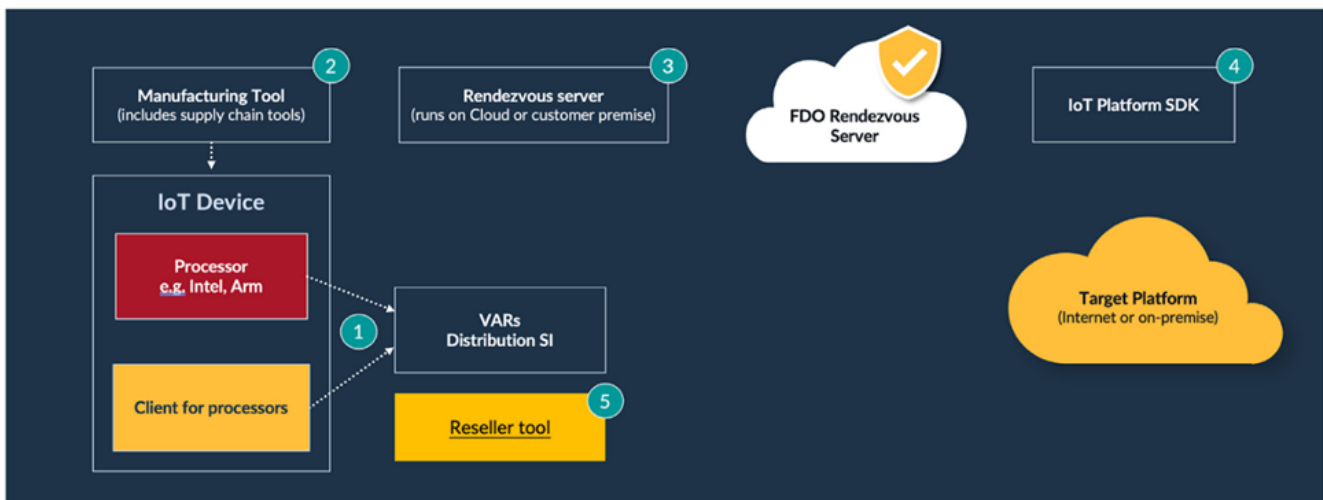
Finally, having finished the FDO process, the device contacts its management platform, which is the platform that manages it for the rest of its lifecycle. FDO then lies dormant, although it can be re-awakened if needed, such as if the device is sold or repurposed.

1. FDO software

Multiple software implementations of the FDO specification have been developed. These include the open-source version developed under the FDO project at Linux Foundation Edge.

<https://www.lfedge.org/projects/fidodeviceonboard/>

This software implementation of FDO consists of several functional elements, which are highlighted in the following generic FDO tool diagram.



The numbered steps in the diagram are described in further detail as follows:

- The FDO client is placed on the device.
- The Manufacturing Tool installs the device credentials and creates the Ownership Voucher.
- The Rendezvous Server can be run in the cloud or on-premise.
- The FDO Platform Software Development Kit (SDK) is integrated into the target cloud or on-premise platform.
- A Reseller tool can be used by the supply chain ecosystem to extend the Ownership Voucher's cryptographic key.
- Additionally, tools provide initial network access for the device (not shown).

Companies have a range of options when implementing the FDO software. They can develop the software themselves directly from the specification, use one of the commercially available implementations of FDO (for example, Red Hat), or they can use the Linux Foundation Edge implementation (described above).

The FDO software within the Linux Foundation Edge has been developed and contributed by Intel, one of the authors of the FDO specification. The code is a mixture of C and Java (depending on which part of the FDO system is being implemented). It offers client software for both Intel and other processors including Arm.

2. Market adoption of FIDO Device Onboard (FDO)



The following are public examples of how a range of end users and technology providers in the industrial, edge, retail, energy and other sectors have adopted FDO.

ExxonMobil

ExxonMobil has adopted FDO as part of its new OPAF based process automation solution.

ExxonMobil


- ExxonMobil is a leader in the move to standards-based, open, secure, interoperable process control solutions (OPAF)
- ExxonMobil and Yokogawa successfully used FDO in their Texas testbed.
- They expect to start running a field trial in the next year at an ExxonMobil Manufacturing facility in Baton Rouge, LA
- ExxonMobil's integrator, Yokogawa, has integrated FDO to automate device installation.
- ExxonMobil's collaborators for the field trial include various IT and OT suppliers



9 | © FIDO Alliance 2023

CONFIDENTIAL

Source: Yokogawa

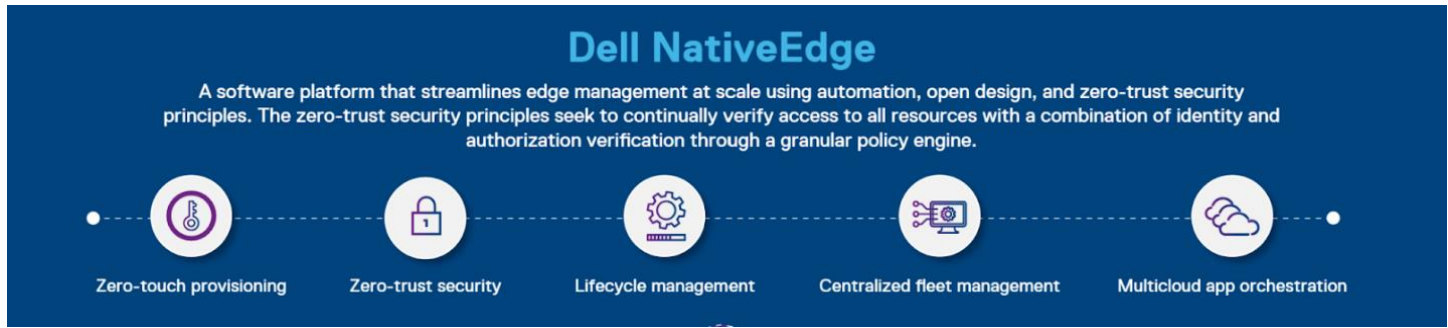


ExxonMobil has used FDO as a part of their overall solution that allows devices to be automatically onboarded and provisioned. The following video from ExxonMobil's David Hedge illustrates this process.

https://www.linkedin.com/posts/dave-hedge_coolstuff-industrialautomation-itotconvergence-activity-7122572917627920384-xlKz?utm_source=share&utm_medium=member_desktop

Dell NativeEdge Solution

The NativeEdge operations software platform enables organizations to securely deploy and manage infrastructure at the edge. NativeEdge supports a wide range of NativeEdge-enabled Devices. It uses zero-trust principles, combined with a holistic factory integration approach and application orchestration, to create a secure edge environment. It can start small with a single device and scale out as needed, and it can be deployed centrally or globally, regardless of network connectivity challenges, absence of technical staff, or facility environment.



With NativeEdge, anyone can easily set up a NativeEdge-enabled Device by simply plugging in a network cable, powering on the device, and stepping away. By leveraging the FIDO Alliance's open standard, FIDO Device Onboard Specification 1.1, Dell assures a streamlined installation process that is as easy as possible.

<https://infohub.delltechnologies.com/p/dell-nativeedge-speeds-edge-deployments-with-fido-device-onboard-fdo/>

Red Hat

Red Hat is the world's leading* provider of enterprise open-source solutions, including high-performing Linux, cloud, container, and Kubernetes technologies.

*Worldwide Operating Systems and Subsystems Market Shares, 2018; released November 2019

"Red Hat Enterprise Linux is the world's leading enterprise Linux platform and the operating system of choice for many organizations deploying IoT and edge compute applications, spanning use cases such as industrial automation, medical, retail and other segments. By collaborating with the FIDO Alliance to implement FIDO specifications for Red Hat Enterprise Linux, we can help customers more easily and quickly onboard and provision their devices to support greater interoperability and enhanced security measures at the edge," said Kelly Switt, senior director, Edge and AI Business Development, Red Hat.

The operating system for enterprise edge

Red Hat FIDO Device Onboard (FDO)

Securing and simplifying device enrollment

Technology Preview

- Solves the problem of “late binding” devices to a management platform or to load other instruction/ secrets
- Cryptographically identifies the system identity and ownership before enrolling and passing configuration and other secrets
- Enables non-technical users to power-on the system and walk away

Available in Red Hat Enterprise Linux 9.0 and 8.6

10

We greatly appreciate METI’s consideration of our comments. We look forward to further discussion with METI on FDO and the FDO Certification program, and would welcome the opportunity to answer any questions or collaborate on approaches as METI considers the best path forward on IOT Product Security Conformity Assessment.

For further information, please contact Atsuhiko Tsuchiya, our APAC Senior Market Development Manager, at tsuchiya@fidoalliance.org or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.