FIDO Alliance Input to NIST

Draft Guidance for Federal Agencies and IoT Device Manufacturers

February 2021

© 2020 FIDO Alliance. All rights reserved.

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on NIST's Draft Guidance for Federal Agencies and IoT Device Manufacturers.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

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, 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 eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

As we detail in this document, FIDO's members decided in 2019 to expand its focus beyond passwordless authentication of people to also focus on specifications that enable passwordless authentication of things. FIDO Alliance launched a new IOT Technical Working Group (IoT TWG) charged with developing use cases, target architectures and specifications covering:

- IoT device attestation/authentication profiles to enable interoperability between service providers and IoT devices
- Automated onboarding, and binding of applications and/or users to IoT devices
- IoT device authentication and provisioning via smart routers and IoT hubs

NIST's call for comments comes at a timely moment, as the Alliance is about to finalize and release its first specification, *FIDO Device Onboard (FDO)* for automatic onboarding of IoT devices. As we detail in the pages that follow, FDO is an important new specification developed with significant input from leading chipmakers and cloud providers, with a simple goal: Secure, passwordless onboarding of any device to any cloud.

The full review draft of the FDO Specification is at https://fidoalliance.org/specs/FDO/FIDO-Device-Onboard-RD-v1.0-20201202.html.

© 2020 FIDO Alliance. All rights reserved.

While FDO is currently in review draft, it is scheduled to be finalized and released in the next two months. FDO addresses a number of sub-capabilities called out in the draft of NISTIR 8259D (Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government). FIDO Alliance requests that FDO be cited as an informative reference in this document.

Additionally, the FIDO UAF and FIDO2 specifications used for human authentication are already being used today to securely manage authentication of individuals to systems that manage IOT devices. As we detail below, UAF and FIDO2 should also be included in the informative references.

Below we provide more detail on each of these comments:

1. **The FIDO Device Onboard (FDO) specification addresses several key sub-capabilities in NISTIR 8259D.**

   FDO is a device onboarding scheme from the FIDO Alliance, sometimes called "device provisioning."

   Device onboarding is the process of installing secrets and configuration data into a device so that the device is able to connect and interact securely with an IoT platform. The IoT platform is used by the device owner to manage the device by: patching security vulnerabilities; installing or updating software; retrieving sensor data; by interacting with actuators; etc. FDO is an automatic onboarding mechanism, meaning that it is invoked autonomously and performs only limited, specific, interactions with its environment to complete.

   A unique feature of FDO is the ability for the device owner to select the IoT platform at a late stage in the device life cycle. The secrets or configuration data may also be created or chosen at this late stage. This feature is called "late binding".

   Various events may trigger device onboarding to take place, but the most common case is when a device is first "unboxed" and installed. The device connects to a prospective IOT platform over a communications medium, with the intent to establish mutual trust and enter an onboarding dialog.

   As it relates to NISTIR 8259D, FDO provides a specification to address a critical initial step: the automated "turn on" of IOT devices.

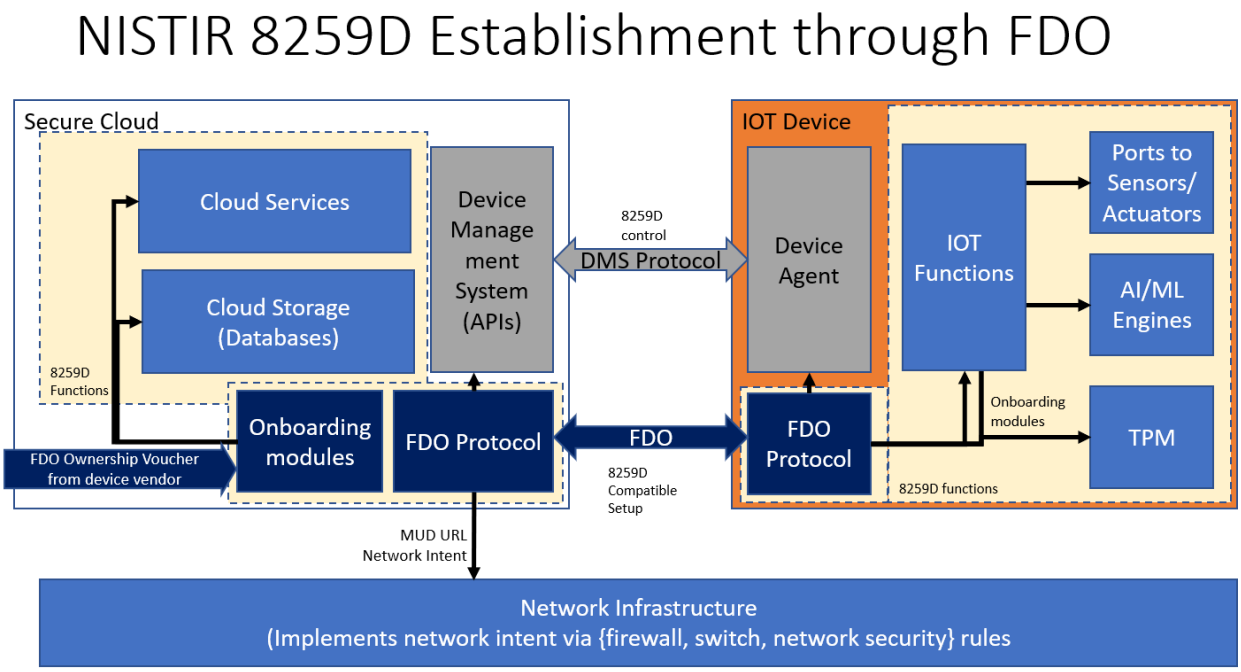
   While 8259D deals primarily with ongoing device operation – as opposed to the initial onboarding of devices – the FDO specification provides a foundational capability that enables many of the key sub-capabilities called out in 8259D for ongoing device operation to be delivered.

   Even if 8259D capabilities are provided within an IOT device, they must be enabled – and FDO will allow them to be enabled. For example:

   - Key pairs must be created and public keys associated with certificates that provide appropriate trust levels
   - The device management service and the device agent must be cryptographically mated and connected via networking
   - Software must be downloaded or updated to handle locally connected hardware or AI subsystems to perform required functions
   - Data protection must be turned on and enabled from secured secrets. Secrets can originate from local hardware key stores or via the DMS connection to remote Hardware Security Modules.

© 2020 FIDO Alliance. All rights reserved.

The graphic below details how FDO enables a number of critical 8259D capabilities to be established.



FDO is itself created using 8259D mechanisms. A FDO key is provisioned in the device, and trust is provided via a device certificate from the manufacturer. A digital document, called an Ownership Voucher, is used to identify the onboarding entity to the device. A key exchange is used to create an integrity protected and encrypted channel. Onboarding modules in the cloud communicate with onboarding modules configured into the device. This exchange allows the device' 8259D mechanisms to be securely enabled and mated with their cloud counterparts. For example, modules can access hardware functions or enable AI/ML engines. A device agent, enabled by FDO, can be provisioned with keys to access a Device Management System in the cloud, allowing remote control for normal device operation.

FDO has the ability to download scripts and small software packages, but it can also be mated with and enable a device Software Over the Air (SOTA) feature to download additional software packages. For example, Linux systems may provide a SOTA mechanism based on RPM or DEB, using Linux' mechanism to download these packages from Internet repositories and verify them using distributed keys (FDO may also distribute the verification keys).

Since FDO overlaps 8259D functionality and provides a module extension mechanism, it is also possible to extend FDO in a given environment to share 8259D functions for multiple implementations. The FDO specification does not mandate this behavior, but this is an opportunity provided by the protocol.

FDO's ability to provide strong device authentication and provisioning of local credentials without requiring manual user intervention is unparalleled in the industry and essential for meeting the requirements of control IA-3 (Device Identification and Authentication) as described in NIST SP 800-53, especially for the Moderate and High baselines defined in that document.

© 2020 FIDO Alliance. All rights reserved.

As such, it is important for 8259D to include a reference to FDO in its informative references and to explain how 8259D links with the controls and baselines in NIST SP 800-53 and NIST SP 800-53B.

As the chart below details, there are numerous sub-capabilities where FDO provides foundational elements.

FDO and 8259D

Key abilities	During FDO	Affected by FDO
Device Identity (1) Identifier Mgt Support & (2) Actions; (3) hardware keys	Authentication via Device identifier configured by manufacturer (e.g., root of trust key).	Additional keys and/or certificate trust can be set up. Hardware keys may be accessed via FDO modules.
Device Configuration (2) Change device software / configuration; configure crypto; Invoke remote (software) update	FDO software pre-configured on device. FDO cryptographically creates secure channel to send commands to device	FDO configures and enables installed software; FDO can access local SOTA capability to add/update local software (e.g., WGET or RPM); software can be verified using credentials downloaded via FDO. Device agent configured with credentials to match DMS policy.
Data protection (1) Identifier management, (2) Actions based on device identity	FDO secure channel encrypts and verifies data sent to/from device during FDO	FDO modules can access cryptography hardware and software modules to enable data protection mechanisms with keys in local hardware key stores (e.g., FIDO authentication key / TPM secrets)

The table below details specific 8259D sub-capabilities where FDO should be listed as an informative reference to address some or all of the key abilities listed in Table 1 of 8259D. Note that some sub-capabilities from the draft are not listed as they are not relevant here. Likewise, where FDO only addresses some key abilities, those abilities have been highlighted in yellow.

Sub-Capability	**Key Abilities**	**Possible SP 800-53 Rev. 5 Controls Supported**	**Relationship to FDO. References are to sections of FDO RD01** **Note: FDO is an onboarding protocol only, and does not maintain continuous operation after initial onboarding, thus several sections do not apply to FDO operation**
Device Identity			
1. Identifier Management Support	• Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device)	• IA-4, Identifier Management	2.3.1; 3.3.6 Device identifier is required; verified using Entity Attestation Token. Linked to the device, not a person.
2. Actions Based on Device Identity	• Ability to monitor specific actions based on the IoT device identity • Ability to identify software loaded on the IoT device based on IoT device identity	• AU-3, Content of Audit Records • CM-8, System Component Inventory	3.8.2 DevMod module provides recommendation on device information passed to IOT platform. Module extension mechanism (3.8.3) permits other information.
3. Physical Identifiers	• Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access	• MP-4 Media Storage • PE-22 Component Marking	Not mandated. Module extension mechanism (3.8.3) may apply
Device Configuration			

© 2020 FIDO Alliance. All rights reserved.

2. Device Configuration Control	• Ability to change the device's software configuration settings • Ability for authorized entities to restore the device to a secure configuration defined by an authorized entity • Configuration settings for use with the Device Configuration capability including, but not limited to: o Ability for authorized entities to configure the cryptography use itself, such as choosing a key length o Ability to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations o Ability to enable or disable notification when an update is available and specify who or what is to be notified	• CM-2, Baseline Configuration • CM-3, Configuration Change Control • CM-6, Configuration Settings	Changing device' software, access to remote update: an intended capability, provided via module extension mechanism (3.8.3) Onboarding parameters are reset during TO2.SetupDevice (5.5.7) Cryptography configuration is configured by device manufacturer and set during the device initialization process, perhaps using the DI protocol (5.2)
Data Protection			
1. Cryptographic Capabilities & Support	• Ability to execute cryptographic mechanisms of appropriate strength and performance • Ability to verify digital signatures • Ability to run hashing algorithms • Ability to compute and compare hashes	• SC-13, Cryptographic Protection	All these capabilities are mandated within FDO, such as (3.5; 3.3.2, 3.3.5, 3.3.6, 3.4, 5.3.3, 5.4.3, 5.5.3, 5.5.6, 5.5.7)
2. Cryptographic Key Management	• Ability to change keys securely • Ability to generate key pairs • Ability to store encryption keys securely	• SC-12, Cryptographic Key Establishment and Management	2.3.1 Initial device keying is required, but outside the protocol scope. The device's identification of the remote relying party is adjusting in TO2.SetupDevice (5.5.7) Secure storage of encryption keys is needed, but outside protocol scope.
Logical Access to Interfaces			
1. Authentication Support	• Ability for the IoT device to require authentication prior to connecting to the device • Ability for the IoT device to support a second, or	• IA-2, Identification and Authentication • IA-6, Authenticator Feedback	IOT platform must authenticate to device (2.3.1; 5.5.3) Only one authentication mechanism is provided. EPID (Enhanced Privacy ID) provides ability for device to mask authentication information (2.3.1)

© 2020 FIDO Alliance. All rights reserved.

	more, authentication method(s) through an out-of-band path such as: Temporary passwords or other one-use credentials; Third-party credential checks; Biometrics; Text messages; Hard Tokens; etc. • Ability for the IoT device to hide or mask authentication information during the authentication process		
2. Authentication Configuration	• Ability to set the time period for how long the device will remain locked after an established configurable limit of unsuccessful login attempts has been met • Ability to disable or lock access to the device after an established number of unsuccessful login attempts • Ability to display and/or report the previous date and time of the last successful login following successful login authentication		N/A (protocol is intended to run before device login is enabled)
4. Authorization Support	• Ability to identify authorized users and processes • Ability to differentiate between authorized and unauthorized users (physical and remote)	• IA-2, Identification and Authentication	Device and Owner entities perform mutual authentication (2.3), but the normal meaning of this entry is N/A
5. Authentication & Identity Management	• Ability to establish access to the IoT device to perform organizationally-defined user actions without identification or authentication	• AC-14, Permitted Actions Without Identification or Authentication	FDO does not directly support authentication for access after onboarding, but it is the secure connection FDO enables between device and cloud at onboarding that makes this later authentication possible.
7. Interface Control	• Ability to establish requirements for remote access to the IoT device and/or IoT device interface including: o Usage restrictions o Configuration requirements o Connection requirements	• AC-17 Remote Access • CM-7, Least Functionality • AC-3, Access Enforcement • AC-18, Wireless Access	Initial configuration of these items, as appropriate to a given IOT device, is an intended capability, provided via module extension mechanism (3.8.3); however this use is optional

© 2020 FIDO Alliance. All rights reserved.

	o Manufacturer established requirement" • Ability to restrict use of IoT device components (e.g., ports, functions, microphones, video) • Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device • Ability to restrict updating actions to authorized entities • Ability to restrict access to the cybersecurity state indicator to authorized entities • Ability to restrict use of IoT device services • Ability to enforce the established local and remote access requirements • Ability to support wireless technologies needed by the organization (e.g., Microwave, Packet radio (UHF/VHF), Bluetooth, Manufacturer defined) • Ability to establish and configure IoT device settings for wireless technologies including wireless authentication protocols (e.g., EAP/TLS, PEAP)		
Software Update			
1. Update Application Support	• Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means • If software updates are delivered and applied automatically: o Ability to verify and authenticate any update before installing it o Ability to enable or disable updating	• SI-2, Flaw Remediation	An intended capability, provided via module extension mechanism (3.8.3). See example in 3.8.3.6 that explains how device updates might be transmitted.
Cybersecurity State Awareness			

© 2020 FIDO Alliance. All rights reserved.

1. Access to Event Information	• Ability to access information about the IoT device's cybersecurity state and other necessary data • Ability to preserve system state information	• SI-4, System Monitoring • AU-12, Audit Record Generation	Module extension mechanism (3.8.3) provides back channel which may apply here.
Device Security			
1. Secure Execution	• Ability to execute code in confined virtual environments • Ability to separate IoT device processes into separate execution domains	• SC-39, Process Isolation	Protocols are designed to run in Restricted Operating Environment (ROE), which is consistent with this set of device capabilities. The nature of a particular ROE selected is left up to the implementor (1.4, 2.3)
3. Secure Resource Usage	• Ability to manage memory address space assigned to processes • Ability to enforce access to memory space through the kernel • Ability to prevent a process from accessing memory space of another process • Ability to enforce configured disk quotas • Ability to utilize file compression technologies (e.g., to provide denial of service protection)	• SC-39, Process Isolation • SC-5, Denial of Service Protection	Module extension mechanism (3.8.3) may apply
4. Secure Device Operation	• Ability to define various operational states • Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services) in accordance with organizationally-defined policies	• CP-10, System Recovery and Reconstitution • SC-24, Fail in Known State11 • CM-7, Least Functionality • CP-12, Safe Mode	Module extension mechanism (3.8.3) may apply for initial system operation. Organizationally defined policies are not likely to be in place before FDO operates, but might be configured as through module extension.

2. UAF and FIDO2 should also be included in the informative references.

Today the FIDO standards UAF and FIDO2 are being used across cloud, banking, payments, fintech, health care, government, enterprises, and e-commerce to deliver authentication that is both more secure and also easier to use. Increasingly, these standards are being used to control the authentication of people to systems controlling IOT devices.

FIDO authentication has been embraced by government and industry as the preferred way to deliver high assurance MFA to consumers.

As we detail below, FIDO provides an ideal way to securely manage logical access of human users to systems used to manage IOT devices.

© 2020 FIDO Alliance. All rights reserved.

Specifically, FIDO UAF and FIDO2 standards should be referenced as a way to support the "Authentication Support" sub-capability of the "Logical Access to Interfaces" listed in Table 1 of 8259D.

- UAF and FIDO2 can enable secure authentication of people to systems controlling IOT devices.
- UAF enables secure authentication via an on-device biometric or PIN match, combined with an asymmetric public-private key pair; FIDO2 enables secure authentication via the same approach, or alternatively, via a stand-alone Security Key that connects to a computing device via USB or NFC.

FIDO Alliance's work to standardize the use of on-device biometric matching coupled with authentication certificates using public key cryptography has transformed the identity and authentication market, creating a standards-based alternative to legacy authentication tools such as central-match biometric systems, one-time passwords (OTPs) and traditional PKI.

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy and usability.

FIDO is a global standard supported by every major platform

Over the last five years, the FIDO Alliance has delivered a comprehensive framework of open industry standards for multi-factor authentication (MFA) that addressed key security and usability shortcomings in previous MFA tools, and that provide practitioners with new options for crafting digital identity solutions.

FIDO standards have delivered improvements in online authentication by means of open, interoperable technical specifications that leverage proven public key cryptography and on-device match of biometrics for stronger security and device-based user verification for better usability. The impact of FIDO standards, and formal certification testing to those standards, is notable:

- Firms including Google, Microsoft, PayPal, Apple, Amazon, Verizon, Facebook, ING Bank, Bank of America, USAA, Aetna, Intuit, Cigna, eBay, Dropbox, Salesforce and their peers around the world have deployed authentication solutions based on the FIDO standards .
- Governments around the world that are either using FIDO today for citizen identity or have announced plans to modernize citizen identity systems around a FIDO-centric architecture include Korea, Thailand, Taiwan, the United Kingdom, and the United States. In the U.S., the Login.gov service has adopted FIDO authentication to protect accounts used to access a variety of citizen-facing services. And CISA has advised election officials to adopt FIDO security keys.[1]
- The W3C has finalized a formal new Web Authentication standard (WebAuthn)[2] that is part of the FIDO2 standards. This standard enables FIDO functionality to be embedded in major browsers (i.e., Chrome, Edge, Firefox, Safari) – meaning that FIDO-standard MFA can be deployed for any web application without any significant burden on the part of an implementer. As of January 2021, over 86% of browsers in use have built-in support for FIDO through support of WebAuthn.
- The ITU has formally adopted the FIDO specifications as standards, through ITU X.1277 (FIDO Universal Authentication Framework) and ITU X.1288 (FIDO Client to Authenticator Protocol (CTAP)/Universal 2-factor Framework)
- More than 750 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.

[1] See https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Actions_to_Counter_Email-Based_Attacks_on_Election-Related_S508C.pdf

[2] See https://www.w3.org/TR/webauthn/

© 2020 FIDO Alliance. All rights reserved.

- Core device platforms have also become FIDO Certified, leading to smartphones and laptops where FIDO Authentication is built in natively into browsers and platforms – meaning that neither implementers nor their customers need to buy a separate technology to enable MFA.

  For example, Microsoft has embedded FIDO at the OS level in Windows 10, where it provides the basis for the Windows Hello passwordless login solution.[3]

  And, Google has embedded support for FIDO in at both the OS level (Android) and the browser (Chrome) – all devices running Android 7 and above (more than 1 billion in total across the globe) are now FIDO Certified to serve as authenticators.[4]

  All told, we estimate that well over 4 billion devices on market today have built-in support for FIDO Authentication.

We greatly appreciate NIST's consideration of our comments. We look forward to further discussion with NIST on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this response. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should NIST staff desire to learn more about how FIDO authentication works.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.

[3] More details on the Microsoft announcement are at https://www.microsoft.com/en-us/microsoft-365/blog/2018/11/20/sign-in-to-your-microsoft-account-without-a-password-using-windows-hello-or-a-security-key/

[4] More details on the Google announcement are at https://threatpost.com/google-ditches-passwords-in-latest-android-devices/142164/

© 2020 FIDO Alliance. All rights reserved.