FIDO Alliance Input to NIST

Consumer Labeling for IoT Devices

October 2021

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to provide input to NIST as it considers how to initiate new labelling programs for IoT Consumer Devices, as called for under Executive Order 14028.

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 Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification and IoT devices.

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.

aetna
amazon
AMERICAN EXPRESS
arm
Bank of America
Daon
egis
FEITIAN
Google
HYPR
IDEMIA
infineon
ING
intel
JUMIO
Lenovo
LINE
LastPass by LogMeIn
mastercard
Microsoft
nok nok
NTT docomo
OneSpan
onfido
PayPal
QUALCOMM
RAON SECURE
RSA
SAMSUNG
Synaptics
THALES
transmit security
TRUSTKEY SOLUTIONS
USAA
VISA
vmware
WELLS FARGO
YAHOO! JAPAN
yubico

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

Earlier this year, FIDO Alliance released its first specification, *FIDO Device Onboard (FDO)*[1] for automatic onboarding of IoT devices. 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.

[1] More details available at https://fidoalliance.org/specifications/download-iot-specifications/ and https://media.fidoalliance.org/wp-content/uploads/2021/04/Introduction-to-FIDO-Device-Onboard-1.pdf

In the next few months, FIDO Alliance will launch a formal certification program to test both the functionality and security of IoT products that claim to implement the FDO standard. While FDO is primarily focused on enterprise and industrial use cases, some of our members have started to share with us plans to also use FDO in consumer devices – as well as their desire to advertise that these devices are FDO-certified as they go to market.

As the FDO certification program prepares to launch, we have four key points to share with NIST:

1. The FDO certification program will be an important labelling program that can support labeling for consumer IoT devices.
2. FIDO Alliance's existing certification programs around authenticators will also be important to consumer IoT labelling efforts, given the important role FIDO authentication will play in enabling consumers to authenticate from other entities in the IoT System (that extend beyond the device, such as smartphones, tablets, PCs), to the systems that control IoT devices in their homes. Indeed, authentication is a key supporting security capability NIST has identified since the inception of NISTIR 8259A (e.g., under the Logical Access to Interface).
3. We understand NIST is seeking comments on what would be an appropriate scope of the concept of 'consumer' in the context of the pilot program. We propose NIST considers the concept of 'consumer' as contemplated by the Consumer Product Safety Commission ("CPSC") (15 U.S.C. §2052(a)(5)(i),(ii)) and focus on household sectors at this stage.
4. As it relates to the concept of IoT 'product', we propose NIST maintains the concept of 'IoT Device' in a manner consistent with Federal Law and NISTIR 8259, 8228,[2] as the default scope at this stage for the baseline requirements criteria (this would also promote consistency with international standards and NISTIR 8259 A and B), while allowing discretion to the IoT Device manufacturer to indicate (in a label or otherwise) an appropriate baseline capability is supported by a different *entity* in the IoT System that extends beyond the device (such as in the case of FDO provided-authentication).[3]

We provide details on the first two of these points below:

1. **The FDO certification program will be an important labelling program for consumer IoT devices.**

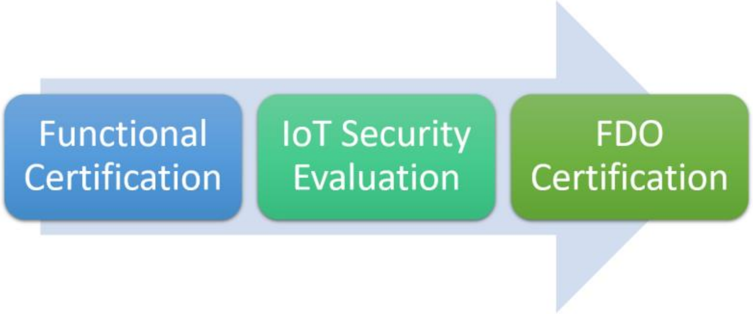
   At its core, FDO enables a "Zero-Touch" onboarding service. To more securely and automatically onboard and provision a device on edge hardware, the device only needs to be drop shipped to the point of installation, connected to the network, and powered up. FDO does the rest. This zero-touch model simplifies the installer's role, reduces costs and eliminates poor security practices, such as shipping default passwords.

   In consumer devices, we are already hearing from FIDO members who intend to use FDO to onboard consumer devices such as thermostats and cameras in the home.

   "FDO Certified" products will have to pass both a functional certification as well as an IoT security evaluation.

[2] In this context NIST should in particular clarify that an IoT Device is a finished product, and is distinguished from conventional IT devices, such as laptops.

[3] Compare to ISO/IEC 27400 (DIS), ISO/IEC 27402 (in draft).



The FDO certification program will look at the following elements (holistically):

- Hardware, typically including microcontrollers, microprocessors, mother board, ICs, physical ports.
- Software including (or not) an embedded OS, its firmware, programs, various applications and most importantly, a FDO application/protocol.
- Sensors which detect and/or measure events in its operational environment and send the information to other components
- Actuators which are output units that execute decisions based on previously processed information
- Security and Privacy evaluation based on defined threat models and security profiles

2. **FIDO Alliance's existing certification programs around authenticators will also be important to consumer IoT labelling efforts, given the important role FIDO authentication will play in enabling consumers to authenticate from other entities in the IoT System such as smartphones, tablets, and PCs, to the systems that control consumer IoT devices in their homes.**

Today the FIDO UAF and FIDO2 authentication standards 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. [4]

FIDO authentication has been embraced by government and industry as the preferred way to deliver high assurance MFA to consumers – most recently in the Office of Management and Budget's Zero Trust Strategy that calls for use of phishing-resistant MFA and calls out the FIDO2 Web Authentication (WebAuthn) standard.[5]

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

- 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.

[4] Note that FID02 is backward compatible with the legacy U2F standard, and U2F is also used in some of these use cases.

[5] https://zerotrust.cyber.gov/federal-zero-trust-strategy/

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.

- More than 850 authentication products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.
- 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.[6]

  Apple has embedded support for FIDO into iOS and MacOS.[7]

  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.[8]

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

FIDO Authenticator Certification Programs

The widespread adoption of FIDO Authentication has been fueled in large part by its robust certification programs that test and confirm that FIDO solutions adhere to FIDO standards.

Note that the FIDO certification program is the largest and most recognized certification program for authentication products in the world. It has been developed over several years by both industry and government (in the U.S., NIST, DoD, NSA, Treasury and GSA are all FIDO Alliance members), ensuring that the certification requirements meet the needs of both the private and public sectors.

In Australia, the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) published guidance on *Implementing Multi-Factor Authentication*[9] that recommended *"For maximum security and effectiveness…use (FIDO) U2F security keys that have been certified to the latest U2F specification version."* The guidance then referenced the FIDO Alliance's website that lists all FIDO Certified products.[10]

[6] 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/

[7] More details on Apple support are at https://fidoalliance.org/expanded-support-for-fido-authentication-in-ios-and-macos/

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

[9] See Implementing Multi-Factor Authentication at https://acsc.gov.au/publications/protect/multi_factor_authentication.htm

[10] See https://fidoalliance.org/certification/fido-certified-products/

ACSC's reference to the FIDO certification program has been helping implementers in Australia by 1) steering them to higher assurance MFA (rather than SMS or OTP) and 2) steering them to a certification program that has certified more than 850 authentication products, demonstrating a mature, competitive, interoperable authentication ecosystem. NIST recognition of the FIDO certification program as one such industry program would have a similar positive effect.

FIDO has also launched a new "Login with FIDO" labelling campaign, with new consumer-facing logos that are designed to allow service providers to easily communicate to consumers about the availability of FIDO login. The two labels are shown below.[11]

fido device unlock

FIDO Device Unlock allows you to use the same technology you use to unlock your device -- like a face scan, fingerprint or PIN -- to log in to websites in a safe and private manner. This may be Windows Hello face, fingerprint or PIN; Mac TouchID; Android Fingerprint; or iOS FaceID or TouchID. All of these operating systems have FIDO built in for safe and private logins.

fido security key

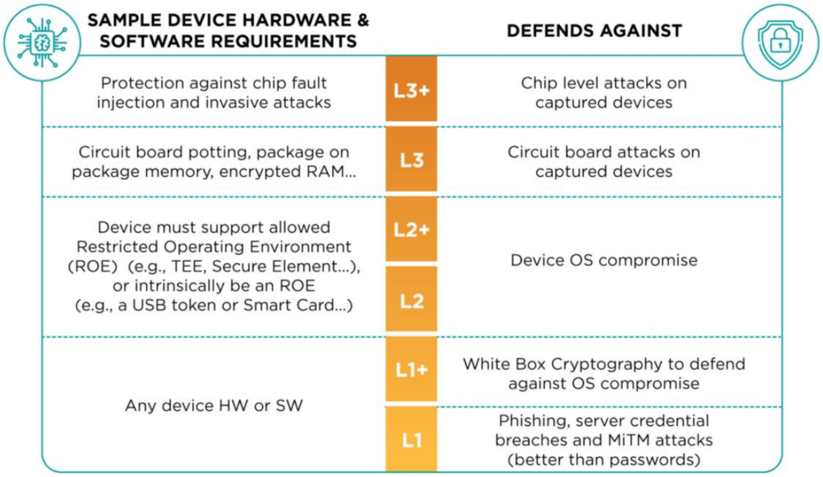
FIDO security keys are small, portable high-security devices that connect to a phone or computer via USB, Bluetooth or NFC. Simply touching this device during sign-in protects accounts from a targeted attack 100% of the time.

In recent years, FIDO Alliance has moved beyond conformance testing to launch new certification programs testing the security of FIDO authenticators, as well as biometric components.

Security Certification Program

FIDO's Certified Authenticator Level program introduces Authenticator Security Requirements to the FIDO Certification Program, looking at how authenticators protect cryptographic key material. This program was launched, in part, to satisfy requests from high assurance communities including government for additional security certifications in FIDO Authenticators.

As detailed below, FIDO has established six different levels of security requirements.[12]



SAMPLE DEVICE HARDWARE & SOFTWARE REQUIREMENTS		DEFENDS AGAINST
Protection against chip fault injection and invasive attacks	L3+	Chip level attacks on captured devices
Circuit board potting, package on package memory, encrypted RAM...	L3	Circuit board attacks on captured devices
Device must support allowed Restricted Operating Environment (ROE) (e.g., TEE, Secure Element...), or intrinsically be an ROE (e.g., a USB token or Smart Card...)	L2+	Device OS compromise
	L2	
Any device HW or SW	L1+	White Box Cryptography to defend against OS compromise
	L1	Phishing, server credential breaches and MiTM attacks (better than passwords)

[11] For additional information, see https://loginwithfido.com/

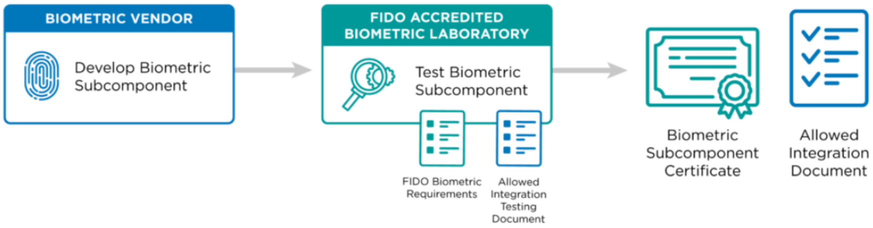
[12] See https://fidoalliance.org/certification/authenticator-certification-levels/ for more details.

Biometric Component Certification Program

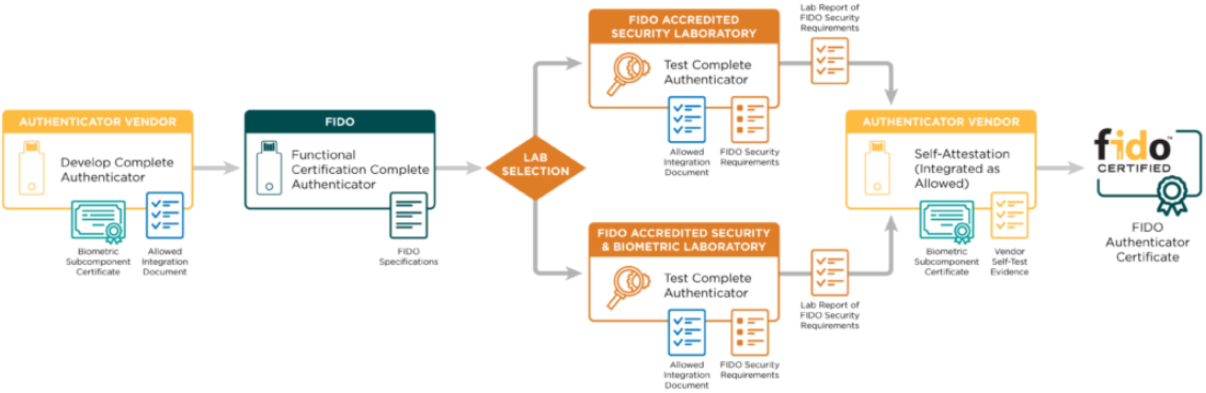
In 2018, FIDO launched a Biometric Component Certification Program, the first independent program to validate biometric technology performance claims that in the past led to concerns over variances in the accuracy and reliability of these solutions.

The program utilizes accredited independent labs to certify that biometric subcomponents meet globally recognized performance standards for biometric recognition performance and Presentation Attack Detection (PAD) and are fit for commercial use. It certifies biometric sensors with a false match rate of 0.0001 or lower (10 times more accurate than current DEA requirements) and was developed in part with input from NIST.[13]

FIDO BIOMETRIC CERTIFICATION TESTING
STEP 1: BIOMETRIC SUBCOMPONENT


BIOMETRIC VENDOR
Develop Biometric Subcomponent
FIDO ACCREDITED BIOMETRIC LABORATORY
Test Biometric Subcomponent
FIDO Biometric Requirements
Allowed Integration Testing Document
Biometric Subcomponent Certificate
Allowed Integration Document

FIDO BIOMETRIC CERTIFICATION TESTING
STEP 2: AUTHENTICATOR


Lab Report of FIDO Security Requirements
FIDO ACCREDITED SECURITY LABORATORY
Test Complete Authenticator
Allowed Integration Document
FIDO Security Requirements
AUTHENTICATOR VENDOR
Develop Complete Authenticator
Biometric Subcomponent Certificate
Allowed Integration Document
FIDO
Functional Certification Complete Authenticator
FIDO Specifications
LAB SELECTION
AUTHENTICATOR VENDOR
Self-Attestation (Integrated as Allowed)
Biometric Subcomponent Certificate
Vendor Self-Test Evidence
fido CERTIFIED
FIDO Authenticator Certificate
FIDO ACCREDITED SECURITY & BIOMETRIC LABORATORY
Test Complete Authenticator
Allowed Integration Document
FIDO Security Requirements
Lab Report of FIDO Security Requirements

In summary, FIDO's existing authentication certification programs have already emerged as an important "consumer label" in the IOT ecosystem today, and the forthcoming FDO certification program will be another valuable contribution to the ecosystem of consumer labels.

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 certification and labelling programs, should NIST staff desire to learn more about how these programs are designed and run.

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

[13] Details at https://fidoalliance.org/certification/biometric-component-certification/