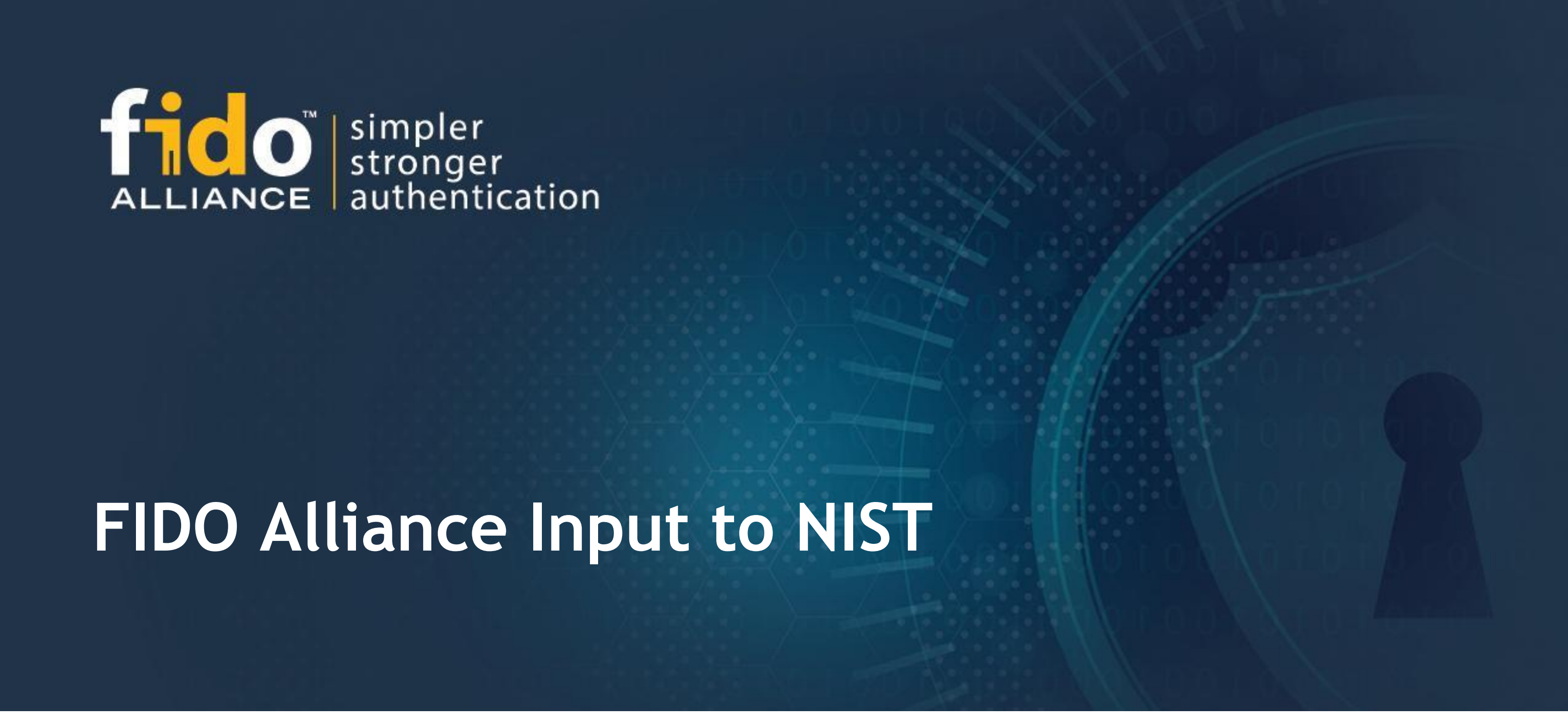

FIDO Alliance Input to NIST

Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management (Draft)

October 2020

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on NIST's draft on Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management. 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.

Over the last year, FIDO has expanded its focus on "authentication of people" to also create new and innovative solutions for "authentication of things." One reason FIDO has focused on this topic is the diversity of our membership: our 40 board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, including most major chipmakers and cloud service providers.

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

The FIDO Alliance IOT Technical Working Group has been working on an application onboarding protocol for a little over a year. This process started in the summer of 2019 with a discussion of use cases, proceeded on to requirements, and is moving towards draft stages. A working draft snapshot of the in-progress FIDO Alliance work is available online at: https://fidoalliance.org/specs/fidoiot/FIDO-IoT-spec-v1.0-wd-20200730.html.

As background, the FIDO working draft has a functional resemblance to Intel Secure Device Onboard (SDO). This is no accident, since the technical working group voted to adopt and modify SDO in December of 2019. Some intended modifications of the spec have yet to be included in the draft, particularly in the area of trusted installer (the NIST paper refers to this as "trusted onboarder"). The existing protocol assumes the installer is untrusted.

Concerning the NIST white paper draft, we have several general comments. The white paper is very detailed and inclusive and has a lot of useful information. We are impressed by the scope and completeness of the effort in general.

Regarding network connectivity, the white paper is somewhat restrictive. IP-based 802.15.4 networks are in common use now, and IP over cellular is in worldwide use. We feel that the bias to WiFi is a shortcoming of this work. Also, if only IP networks are considered, we recommend including this in the title.

Non-IP networks, such as Bluetooth Low Energy, native cellular protocols or LORA have their unique advantages and disadvantages. They are deployed extensively and we feel it is a shortcoming that they are not discussed in the white paper. Some of the discussion in the document is really about shortcomings of WiFi that might be easier to handle in some of these other technologies.

SDO and the FIDO draft are intended for application onboarding, but we feel there is enough overlap that the features might be appropriate for consideration by the NIST. Also, these protocols show that a proxy can be used to enable the installer ("onboarder") to assist with network entry for purposes of running the onboarding protocol; during the onboarding protocol, permanent network credentials can be supplied. We encourage the NIST to evaluate this concept.

We understand that MUD is important for determining network intent. However, the paper seems biased to this particular approach. MUD is treated as synonymous with network intent, where other mechanisms are described generically and related to standards. In fact, SDO and the FIDO Alliance draft both recognize the importance of MUD and make provision for transport of the MUD URL. However, we still feel that a separation of the standard from the technical requirement may yield additional requirements that help to understand ways in which MUD might evolve over time. For example, the MUD acronym includes the manufacturer as the author, but the white paper correctly indicates that later entities interacting with the device during its lifetime may place additional usage requirements on a device (see L1795-1809).

In some cases, the MUD URL is referred to as an authorization mechanism (in particular, in table 8-1). We feel that this is incorrect and encourage a change. Similarly, the MUD server has no conceptual role for determining network attachment, although it may inform the authority for this role based on determination of intent.

The treatment of attestation also has a bias to the DICE effort from the Trusted Computing Group (see section 6.4.8). The IETF RATS Working Group is working on the Entity Attestation Token mechanism, which is used in the FIDO draft. The Entity Attestation Token is more flexible about measurements and device features than DICE. Attestation is important enough that a survey of the various standards would make sense.

Since the FIDO IOT Technical Working Group has a number of chip vendors as members, we also note that the device initialization mechanisms misses an important device initialization technique, where security processor chips (or chips that embed security processors) are initialized in the fab with key materials. This is an important fundamental mechanism for device identification, and it can also dramatically simplify the task of including credentials for device manufacturers. We note that Intel, ARM, Qualcomm and Infineon all have chip-level products that exhibit this identification.

In the FIDO work we have identified a distinction in onboarding algorithms depending on whether there is a trusted or untrusted installer (aka “onboarder”) present. The current FIDO draft, and SDO, are examples of protocols that use an “untrusted installer” model, where no input is permitted from the installer (“onboarder”) person. We have identified this as a requirement, particularly for commercial networks. However, some of our members have identified the advantages to protocol and supply chain when the installer has a significant but limited role.

The white paper identifies the possibility of a trusted onboarder, but does not distinguish between a person who has full access to the device (e.g., “root shell”) and a limited mechanism that still maintains device integrity. We have determined that there is an important set of tradeoffs between convenience and security when the trusted onboarder is able to determine network choice and select the onboarding locus on the IOT platform (sometimes called the “cloud account”), but has no other impact on the process. We encourage this to be examined further for the white paper.

SDO and the FIDO draft use an authentication object called the “ownership voucher.” The white paper makes reference to the Device Information Declaration, which seems to have some overlap. However, the ownership voucher is actually a voucher, which is different from the voucher mechanism in rfc8366. The following table gives some comparison, and we hope it indicates that both trust objects are worthy of NIST investigation.

Ownership Voucher	**RFC8366 Voucher**
Authorization to onboard	Authorization to onboard
Forwards through supply chain	Generated and signed dynamically during onboarding
Contains trust relationship for device onboarding target	Contains 3rd party voucher for device onboarding target
Verifiable in the device using device credentials	Requires external trust to verify
Trust is built up in the supply chain	Trust must be computed instantaneously on demand
Distributed authentication mechanism, incremental work for supply chain entities	Centralized mechanism for target area, global solution would be very expensive. We feel that a very high supply chain overhead is hidden in this mechanism, unless it has only local significance.
Verifiable in a closed network, based on imported credentials	Requires instantaneous access to the specified trust authority (called MASA in RFC8572). Closed networks must be treated as a special case.

The ownership voucher is part of a system of mechanisms within SDO and the FIDO protocol to allow "late binding." This indicates a deferral of the decision to bind the device to specific characteristics of its target environment until it is ready to be introduced to that environment. Many of the inefficiencies of factory initialization are mitigated significantly by late binding.

Another part of the late binding mechanism is the SDO rendezvous mechanism, also used in the FIDO protocol. The purpose of the rendezvous mechanism is to allow the device to find its prospective IOT platform "owner" dynamically. Any pre-configured address within the host is limited to the rendezvous server, and this provides dynamic access to the IOT platform. The rendezvous mechanism includes directions to find the rendezvous service that are flexible enough to allow a closed network to include its own rendezvous server.

In other protocols, network level mechanisms are sometimes used to provide this level of binding. For example, Windows machines use the DNS SRV queries are used to find the local Active Directory server. In the SDO development, it was felt that the owner of the IOT solution is not guaranteed to be the network owner. Relying on the ability to change the network environment would be more difficult for the IOT owner than the ability to deploy an application level service, such as the rendezvous server.

In addition to the above, we have comments specifically on table 6-4 and table 8-1, as requested in the white paper.

Table 6-4 (copied in columns 1-2) with comparisons to SDO/FIDO draft protocols.

Attribute/Capability	**Description**	***SDO/FIDO draft***
security model	whether the mechanism that parties use to gain each other's trust is based on signed vouchers or proof of knowledge	*Signed, forwarded, ownership vouchers and proof of knowledge. Voucher mechanism is different from IETF RFC8366. The ownership voucher has an element of the described device information declaration.*
device identity	information used to identify the device and distinguish it from other devices	*Device key / certificate.*
device authentication	verification that the asserted identity of a device is the device's actual identity	*Sign a nonce with device key.*
device authorization	determination of whether a device should be permitted to connect to the network	*Verify ownership voucher against Owner server's ("IOT Platform's") key. OV is signed to the destination owner.*
secure local credentialing capability	The onboarding solution (as distinct from the device manufacturer) can provision locally significant credentials to the device in a manner that protects them from disclosure, and it is capable of provisioning unique network credentials to each device.	*Late binding mechanism permits arbitrary numbers of credentials to be provisioned.*
maintainable credentials	credentials that expire, can be revoked, and can be renewed relatively easily	*Refresh of credentials is a manual process.* *Ownership voucher does not expire. Device credentials that expire may be interpreted relative to the ownership voucher at owner's discretion.*
device type verification	verification that the device is of the asserted type or from the asserted manufacturer (as	*FIDO protocol uses IETF RATS WG Entity Attestation Token, which may be extended to include this information. However, it is better to*

	opposed to verifying that it has a specific identity)	*send this information in a separate attestation after the connection is encrypted.* *Manufacturer may place arbitrary data about the device in modules accessed via the ServiceInfo negotiation.*
device attestation	proof that some elements of the device (e.g., firmware) have not been tampered with	*See comment of Entity attestation token.*
trust anchors/root of trust	elements that security depends on; if they are compromised, security is undermined	*Requires that credentials in the device are not exposed or modified.* *Requires that private keys in the ownership voucher are not exposed.* *A reset and reprogram of credentials in the device may be foiled using the HMAC secret created during device provisioning.*
trusted onboarder required	Does the onboarding solution require the device onboarder to be trusted, or is this unnecessary because, for example, authorization for the device to access the network can be based on credentials that are bound to the device?	*FIDO intends to pursue a trusted installer / trusted onboarder variant of the protocol. SDO and the current FIDO draft do not have trusted onboarder mechanisms.*
key type	type of keys used (e.g., symmetric, pre-shared, public/private)	*Asymmetric keys for identification; symmetric keys used after key exchange.*
encryption details	the encryption standard used for establishing the secure channel between the device and the network onboarding component, along with those of its attributes and characteristics that impact security, for example, whether it provides forward secrecy	*Signatures and encryption based on the COSE spec (RFC8152)* *Device attestation based on the Entity Attestation Token (IETF RATS WG)* *Server identification using ECDSA and RSA;* *Device identification using X.509; ECDSA; DAA (EPID -- ISO20008/ISO20009)* *Diffie Hellman / ECDH key exchange* *AES variants (encrypt-then-mac and authenticated encryption)*
network selection	determination by the device regarding what network it should join	*No*
network authentication	verification that the asserted identity of a network is the network's actual identity	*No*
network authorization	determination of whether a network should be permitted to onboard (i.e., take control of) a device	*No (other than implicitly via Ownership Voucher)g*

connected device and onboarded device cross-check	verification that the devices operating on the network do not include any devices that were not subjected to the onboarding process	*No*
proof of ownership	the ability to determine what individual or entity owns each device. (Device ownership is relevant because only device owners have the authority to determine onto what networks a device is authorized to be onboarded. Hence the proof of ownership, secure ownership transfer, and “onboard only to authorized networks” characteristics are all related to one another.) An onboarding solution that supports these three characteristics will impose responsibility on some party (e.g., the device manufacturer) to keep the device information declaration updated with accurate ownership and authorized onboarder information.	*Via Device certificate and ownership voucher.*
secure ownership transfer	the ability to convey ownership of a device securely from one individual or entity to another only with the express permission of the device’s current owner. Secure ownership transfer enables proof-of-ownership information to remain accurate even as ownership of a device changes. The secure ownership transfer characteristic goes hand in hand with the proof-of-ownership characteristic and, like the proof-of-ownership characteristic, imposes responsibility on some party to keep the device information declaration up-to-date.	*Without powering on the device, ownership transfer possible by extending the ownership voucher.* *The onboarding protocol (TO2) creates a new ownership voucher, effecting ownership transfer.*
onboard only to authorized networks	the ability to determine to what individuals or entities to which the device owner has granted the authority to onboard the device. If the onboarding solution supports the capability to onboard only to authorized networks, this means that authorized onboarder information is available that the onboarding solution can consult to ensure that a device will permit itself to be onboarded only to a network that has been authorized by the device owner. The “onboard only to authorized networks” characteristic goes hand in hand with the proof-of-ownership and secure ownership transfer characteristics and, like them, it imposes responsibility on some party to keep the device information declaration up-to-date.	*No, other than implicitly via Ownership Voucher*
privacy	ability of the onboarding solution to prevent unauthorized disclosure of personal information during and related to the onboarding process	*All onboarding information is replaced during onboarding except the device key. Ability to create or provision application keys and other*

		credentials during onboarding should prevent correlation attacks. *However, the device certificate may be correlated from one onboarding use to another. If the device certificate is for an EPID device key, this does not identify the device.*
MUD support	The onboarding solution supports conveyance of a device-specific MUD URL to the network. Ideally, this URL should be conveyed in a secure fashion to make it difficult for an attacker to modify it and thereby associate the device with a MUD file that is different from the one intended by the manufacturer. The MUD file URL should also be kept confidential to avoid disclosing information about the device that may inform an attacker regarding its vulnerabilities.	*MUD URL is passed during ServiceInfo as a standard optional component*
evolving communications profile enforcement	The onboarding solution supports a mechanism to enforce an evolving communications profile for the device. A device's purpose changes as it moves through its life cycle, and its communications profile changes accordingly. Enforcement of this evolving communications profile ensures that the device communicates only in the ways that it is expected to communicate during the phase of the onboarding process that it is in at any given time.	*SDO/FIDO supports only device onboard. Both are flexible enough to permit a changing device profile, if this is selected by other management mechanisms.* *SDO/FIDO are both designed to run over any transport mechanism.*
supply-chain security	protection of a device as it moves through all initial phases of its life cycle, e.g., research and development (R&D), manufacturing, integration, rebranding, transport, storage, and shelf life, up to the point at which it is physically obtained by its first post production owner. With respect to onboarding, supply-chain security refers to whether the onboarding solution can integrate with supply-chain management tools. A manufacturer that can monitor a device throughout its supply chain and integrate its supply-chain management tools with a device's onboarding solution should be able to provide strong trust anchors for device onboarding.	*The ownership voucher has security verification mechanisms built into it, that make it easier to securely transit the supply chain. However, protection relies on the security of the private keys of the supply chain entities.*

Table 8-1 with comments in italics

Characteristic	Proposed Set of Recommended Security Capabilities	Recommendations	NISTIR Document Derivation or Other Rationale
security model	Security Model is clearly stated.	The onboarding solution should use voucher mechanisms as a basis of trust, when possible. If the onboarding solution requires that the device or network onboarding component receive information regarding device ownership or a device MUD file, this information should be signed by a trusted third party. *Need to verify vouchers in real time will either be very costly and complicated or limited in scope. Should provide for FIDO mechanism.*	Clarification of the onboarding solution's security model aids in understanding the assumptions on which its assurance depends and helps with managing the vulnerabilities that failure of these assumptions might pose. Reliance on signatures provided by a trusted third party clarifies the onboarding solution's trust anchors.
device identity	The onboarding solution requires that each device have a distinguishing logical identifier and a distinguishing physical identifier.	Preferably, the device identity should be immutable. If it is mutable, then security protections that rely on this identity are weak. As a specific example, using a device interface MAC address as the device's identity is not advised, because even though the MAC address is hard-coded on the network interface card and cannot be changed, this MAC address is mutable in the sense that it is possible to spoof the MAC address and make other devices on the network believe that it is different than it actually is. In addition, device use of MAC randomization to avoid tracking is becoming a common practice, so MAC addresses should never be depended on as identities. *Requirement and example do not match -- requirement is for immutable identity; example is a spoofable identity. Mutable identity is also listed as desirable elsewhere. We can see this both ways. Typically, immutable identity is best, but there are privacy implications, unless specific technologies or measures are brought to bear.*	NISTIR 8259A: core baseline device identification capability, with our additional recommendation that the identity be mutable. ETSI EN 303 645: Provision 5.4-2
device authentication	The onboarding solution supports the ability to verify that the asserted identity of each device is the	The bootstrapping key (e.g., a private key or other secret known only to the device) should use standardized, vetted, and current cryptographic algorithms. The bootstrapping key should be stored on the device in such	NISTIR 8259A: core baseline data protection capability. ETSI EN 303 645: Provisions 5.5-4 and 5.5-5

	device's actual identity.	a way that it is protected from unauthorized access and modification, such as in a cryptographic module.	
device authorization	no capability currently recommended	The onboarding solution should support device authorization through integration with an authorization service (esp. for enterprise solutions)	Consumer networks will not typically have their own authorization service, but they may receive authorization service support from their service provider. Requiring a local authorization service for consumer networks may be too stringent. When supported, device authorization enables more granulated access controls to be enforced for connected devices.
secure local credentialing capability	The onboarding solution supports provisioning local credentials to the device during onboarding in a manner that protects the credentials from disclosure.	The onboarding credentials that the device uses to connect to the network should be unique to the device. These credentials should be protected from unauthorized access and modification both while in transit to and while stored on the device. Authorized entities can delete these credentials from the device. *It is desirable for the device to be provisioned with new "local" or "device local" credentials, to avoid attacks or attack reconnaissance based on knowledge of factory provisioned keys.*	NISTIR 8259A: core baseline device configuration and data protection capabilities. ETSI EN 303 645: Provisions 5.1, 5.1- 1, 5.5-1, and 5.12-1
maintainable credentials	The onboarding solution supports updating a device's onboarding credentials in a secure manner.	Deletion of the device's current onboarding credentials by an authorized entity and then re onboarding the device, thereby provisioning it with new replacement credentials, is an acceptable solution.	NISTIR 8259A: core baseline device configuration and data protection capabilities. ETSI EN 303 645: Provision 5.11-1
device type verification	no capability currently recommended	The process of authenticating the device's identity using the distinguishing logical and physical identifiers (per Row 3 of this table) implicitly provides device type verification.	

device attestation	no capability currently recommended	Integration of device attestation capabilities with the onboarding solution ensures that IoT devices that perform secure boot processes have verified the authenticity and integrity of their chip, firmware, application, and/or software before onboarding.	ETSI EN 303 645: Provisions 5.7-1 and 5.7-2
trust anchors/root of trust	The onboarding solution clearly and explicitly identifies all its trust anchors.	Understanding the onboarding solutions trust anchors helps in the support of vulnerability management.	
trusted onboarder required	no capability currently recommended	It is acceptable if the onboarding solution requires a trusted individual to initiate the bootstrapping process (i.e., to initiate the introduction of the network bootstrapping credentials to the device or the device bootstrapping credentials to the network). *Better definition and narrowing of recommended trusted onboarder (FIDO: trusted installer) behavior is desirable. The existing definition is very broad, and implies that the trusted installer may have arbitrary knowledge and control of the device. Existing solutions can be effective without such a permissive policy.*	
key type	The onboarding solution supports public/private key pairs for the device bootstrapping and network bootstrapping keys.	Symmetric-key-based options are also permitted.	Use of public key cryptography enables the device and the network onboarding component to authenticate to each other and then set up a secure channel. ETSI EN 303 645: Provision 5.5-1
encryption details	It must be possible for an authorized entity to configure the cryptography used in the onboarding process, when applicable, such as choosing a key length. It must also be possible for an authorized entity to render the onboarding	The onboarding solution should be designed with the expectation that the IoT device has the ability to use accepted cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised. Although it should be possible to delete the device's onboarding credentials	NISTIR 8259A: core baseline data protection capability The ability to delete the device's onboarding credentials while relying on its bootstrapping credentials to remain constant supports the capabilities to update and maintain device credentials and to re-onboard the device to different networks. ETSI EN 303 645: Provisions 5.5-1, 5.5-2, 5.5-3, and 5.4- 1

	credentials inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data).	from the device, it should not be possible to delete the device's bootstrapping credentials.	
network selection	The onboarding solution provides the identifier of the network to which the device should connect as part of the onboarding credentials that are provisioned to the device during onboarding.	NISTIR 8259A: core baseline device configuration Capability If multiple local networks are in range, this capability informs the device to what network it should connect. *A network proxy type mechanism that attaches a device to the network can bypass this problem until onboarding is completed. The proxy acts as a trust bridge and allows the device access to the correct network without requiring explicit interaction with the device. During onboarding, the device can be informed of its intended network. The proxy mechanism has the advantage that multiple devices can be onboarded to a given network without requiring that any of them be manually configured.*	
network authentication	The onboarding solution supports the ability to verify that the asserted identity of the network is the network's actual identity.	The onboarding solution may rely upon a trusted individual who is performing the onboarding to determine that the network to which the device is being onboarded is the intended network. If network authentication is automated, it should be performed based on the network's bootstrapping credentials (e.g., an X.509 certificate), which include a public key. The corresponding private key (the bootstrapping key) should be accessible to the network onboarding component and stored so that it is protected from unauthorized access and modification. *Please consider the SDO/FIDO ownership voucher mechanism, which also performs this function.*	NISTIR 8259A: core baseline data protection capability

network authorization	no capability currently recommended	The onboarding solution may include mechanisms such as proof of ownership and “onboard only to authorized networks” that enable the device to verify that a network that is trying to onboard it is authorized to take control of the device. By default, once a device connects to the network, the network will have access to all the device’s capabilities. However, the onboarding solution may include specific application-layer bootstrapping information in the device’s onboarding credentials to specify what controllers, cloud, and application services the device should trust, which in turn would influence what device capabilities get activated. *Please consider the SDO/FIDO ownership voucher mechanism, which also performs this function.*	Given that IoT devices are assumed to be single purpose, it seems safe to assume that the network should have access to all the IoT device’s capabilities once the device connects to the network and enables its application(s).

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.

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