PROJECT DESCRIPTION

TRUSTED INTERNET OF THINGS (IOT) DEVICE NETWORK-LAYER ONBOARDING AND LIFECYCLE MANAGEMENT

Enhancing Internet Protocol-Based IoT Device and Network Security

Paul Watrobski
Murugiah Souppaya

Information Technology Laboratory
National Institute of Standards and Technology

Susan Symington
Parisa Grayeli
Joshua Klosterman
Blaine Mulugeta

The MITRE Corporation

William C. Barker

Dakota Consulting

May 2021

iot-onboarding@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

Network-layer onboarding of an Internet of Things (IoT) device is the provisioning of network credentials to that device. The current lack of trusted IoT device onboarding processes leaves many networks vulnerable to having unauthorized devices connect to them. It also leaves devices vulnerable to being taken over by networks that are not authorized to onboard them. This NCCoE project will focus on approaches to trusted network-layer onboarding of IoT devices and lifecycle management of the devices. The NCCoE will build a trusted network-layer onboarding solution example using commercially available technology that will address a set of cybersecurity challenges aligned to the NIST Cybersecurity Framework. This project will result in a freely available NIST Cybersecurity Practice Guide.

ACKNOWLEDGMENT

This project description was developed from the presentations and discussions that occurred at the NCCoE-hosted Virtual Workshop on Trusted IoT Device Network-Layer Onboarding and Lifecycle Management. NCCoE thanks Karen Scarfone for contributing to the development of this project description and Geoffrey Cooper, Michael Fagan, Dan Harkins, and Russ Housley for their input.

KEYWORDS

application-layer onboarding; attestation; bootstrapping; device lifecycle management; hardware root of trust; Internet of Things (IoT); network-layer onboarding; network security; network segmentation

DISCLAIMER

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Purpose

Network-layer onboarding of an Internet of Things (IoT) device is the provisioning of network credentials to that device. Network credentials are needed so that only authorized devices can connect to and use an organization's networks. (Note that the network credential is different from the unique authoritative credential that the manufacturer is expected to install on the device in the form of an Initial Device Identifier [IDevID] or keypair. The unique authoritative credential is sometimes referred to as the device's *birth identity* or *birth certificate* and it is independent of context, whereas the network credential is locally significant.) In the past, established approaches to network-layer onboarding for IoT devices have had some challenges:

- Using the same pre-shared network credential for every device is the simplest approach, but it does not identify each device, nor does it give devices a way to verify they are connecting to the correct network.
- Manually provisioning a unique network credential for each device often makes the onboarding process complex, resource intensive, error prone, and insecure.
- Having manufacturers assign a unique network credential to each device during the manufacturing process is expensive and inefficient.

A different approach to network-layer onboarding—one that enables scalable provisioning of unique network credentials to devices when they are deployed rather than when they are manufactured—is needed. The desired process, called *trusted network-layer onboarding*, is an automated approach with these characteristics:

- provides each device with unique network credentials,
- provides the device and the network an opportunity to mutually authenticate,
- is performed over an encrypted channel (to protect credential confidentiality),
- does not provide anyone with access to the credentials, and
- can be performed repeatedly throughout the device lifecycle.

Trusted network-layer onboarding provides assurance that a network is not put at risk as new IoT devices are added to it, and it also safeguards IoT devices from being taken over by unauthorized networks. These safeguards are especially important when onboarding safety-critical devices, whose compromise could pose public safety threats.

This document defines a National Cybersecurity Center of Excellence (NCCoE) project, for which we are seeking feedback. The project focuses on trusted network-layer onboarding of IoT devices and lifecycle management of the devices. The project's objective is to define best practices for performing trusted network-layer onboarding, which will aid in the implementation and use of trusted onboarding solutions for IoT devices at scale. This project seeks to define and demonstrate onboarding solutions that can be broadly adopted for use by many industry sectors.

This project will result in products such as a publicly available National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide Special Publication (SP) 1800, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge. Additional artifacts such as blogs, papers, demonstration videos, and infographics will be developed to supplement the SP 1800.

Scope

The project encompasses trusted network-layer onboarding of IoT devices deployed across different internet protocol-based environments using wired, Wi-Fi, and broadband networking technologies. The project addresses onboarding of Internet Protocol (IP) based devices in the initial phase and will consider using technologies such as Zigbee or Bluetooth in future phases. The scope also includes additional security capabilities that can be integrated with and enhanced by the onboarding mechanism to protect the device and the network to which it connects throughout the device's lifecycle. Enterprise, consumer, and industrial use cases are all considered to be in scope at this time.

Assumptions/Challenges

As with any other device, an IoT device needs appropriate credentials in order to connect to a network securely. To take full advantage of economies of scale, manufacturers seek to make devices as identical as possible for all customers. This desire implies an onboarding solution that defers the provisioning of a device's network and other locally significant credentials from the time of manufacture to the time of deployment. The unique authoritative credentials that a manufacturer installs on each device (i.e., the device's *birth identity or birth certificate*) should be targeted to enable and simplify the network-layer onboarding process for its intended users, while keeping the device manufacturing process efficient. Note that the unique authoritative credentials that the manufacturer installs can include a unique identity and a secret, and can range from simple raw public and private keys to X.509 certificates that are signed by a trusted authority.

Some mechanisms that are currently used to perform onboarding for IoT devices tend to be inefficient or insecure. Some networks allow all devices to use the same pre-shared password, which means that whether or not a device is granted access to the network has nothing to do with the individual identity of the device or even the device's type. Because many IoT devices lack a functional user interface, some current mechanisms use Wi-Fi as the interface to the device and insecurely provision network credentials over an open network. Furthermore, although networks can falsely identify themselves, the device is not typically provided with a way to verify that the network to which it is connecting is actually the intended network.

Other networks use a more robust security model that requires each device to have its own distinct network credential to connect. However, provisioning such a network credential manually often means that the onboarding process is complex, resource intensive, and possibly error prone. If the process requires individuals to have access to the device's network credentials, such access makes those credentials more vulnerable to being disclosed to unauthorized parties. Building a device's network and other locally significant credentials into the device at the point of manufacture [1] would effectively require the manufacturer to customize devices on a per-customer, build-to-order basis, which is complex, inefficient, and expensive [2]. Instead, scalable, secure, network-layer onboarding solutions rely on devices being equipped with unique authoritative credentials (e.g., unique identity, private key, possibly a certificate) by the manufacturer and leverage these unique authoritative credentials at the time of deployment to perform trusted network-layer onboarding of the devices [3], [4], [5].

This NCCoE project description builds on the document-based research presented in the NIST Draft Cybersecurity White Paper: Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management [6]. That paper describes key concepts and characteristics for a trusted network-layer onboarding solution in addition to other capabilities

like device attestation, device intent, and asset management. The trusted network-layer onboarding characteristics that we will try to demonstrate in this project are discussed later in the "Desired Capabilities" section.

2 SCENARIOS

The scenarios we are considering for the project all depend on trusted network-layer onboarding. They describe different stages of the onboarding mechanism and include demonstrations of additional protections that can be integrated with onboarding to protect the IoT device throughout its lifecycle.

Scenario 1: Trusted network-layer onboarding

This scenario involves trusted network-layer onboarding of an authorized IoT device directly to an authorized network, as performed after the device has booted up and is placed in onboarding mode. In this scenario, after the identities of the device and the network are authenticated, a network onboarding component—a logical component authorized to onboard devices on behalf of the network—provisions unique network credentials to the device over a secure channel. The device then uses these credentials to connect to the network. Note that this scenario could also require the device to perform other preparatory tasks such as to retrieve the most recent firmware and update as part of the initial boot process.

Scenario 2: Validation of device authenticity and integrity

This scenario involves performing attestation, supply chain management (e.g., hardware, firmware, and software component inventory), configuration monitoring, or other asset-management-related operations on an IoT device to validate its authenticity and integrity. These operations may be performed as part of a trusted boot process or at some other point before permitting the device to be onboarded to the network. In some instances, the device may be able to get the most recent firmware update as part of the initial boot process [5]. After the device connects to the network, attestation may be performed intermittently to establish renewed trust between the device and application servers or other components with which it interacts.

Scenario 3: Trusted application-layer onboarding

This scenario involves trusted application-layer onboarding that is performed automatically on an IoT device after it connects to a network [7]. As a result, this scenario can be thought of as a series of steps that would be performed as an extension of scenario 1. For example, the device could automatically download the latest version of its application from a trusted application service that is hosted on the local network or in the cloud, or the device could contact a trusted lifecycle management service to check for available updates or patches. Application-layer onboarding could also include device health posture attestation designed to enforce that the device meets a specific security baseline.

Scenario 4: Re-onboarding a wiped device

This scenario involves re-onboarding an IoT device to a network after wiping it clean of any stored data so that it can be re-credentialed and re-used.

Scenario 5: Onboarding with device intent enforcement

This scenario involves onboarding an IoT device to a network, augmented with a mechanism for device intent enforcement (for example, Manufacturer Usage Description [MUD] [8]). This mechanism could include a number of features, such as:

- secure communication of device intent data from the device to the network,
- assignment of the IoT device to a separate subnetwork,
- ongoing support for device intent enforcement after the device connects to the network, and
- use of a locally-defined device intent policy that overrides the original device intent policy provided by the device manufacturer (or other entity).

3 High-Level Architecture

Notional Logical Architecture

Figure 1 depicts a notional logical architecture that includes a trusted network-layer onboarding solution and several possible optional components. The layers in Figure 1 create a dependency chain of protections that can be traced upward, both in terms of the order in which the protections are invoked and the support that each protection provides to those depicted above it.

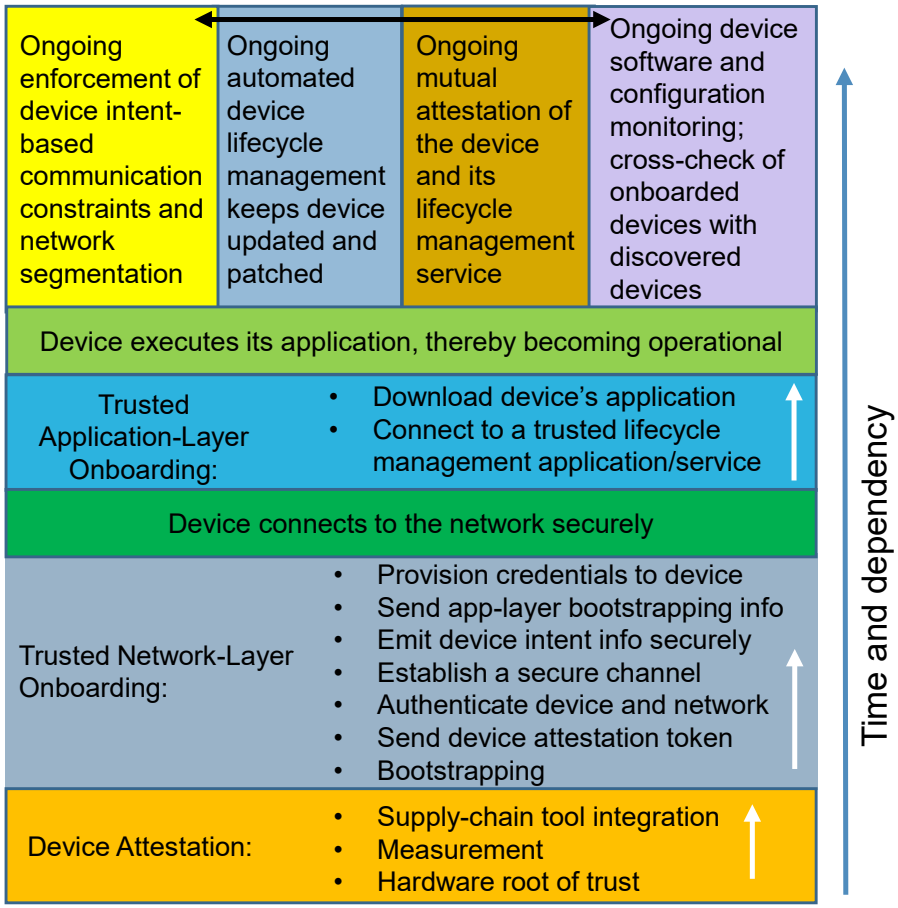

Figure 1: Dependency Chain of Protection Mechanisms

Various degrees of platform trust may be achieved through a secure boot process, which starts with a hardware root of trust that provides secure storage for the device's private key. More assurance can be provided by using cryptographic measurement to generate verifiable evidence attesting to the integrity of each successive running piece of the device's hardware, firmware, operating system, and other software before passing control to it. When integrated with trusted network-layer onboarding, these additional security capabilities reinforce each other to enhance protection of both the device itself and the network to which it connects.

The trusted network-layer onboarding portion of Figure 1 includes evaluation of the device's attestation token, device and network authentication, secure conveyance of device intent and application-layer bootstrapping information, and provisioning of the device's credentials over a secure channel. When the device obtains a unique credential with which to access the network, the network is given knowledge of this device, e.g., what it is authorized to do. Once the device has completed network-layer onboarding, it can use its newly provisioned credentials to connect to the network securely.

After the device has connected to the network, if application-layer onboarding information was present in the device's bootstrapping credentials and if application-layer onboarding is supported, this application-layer onboarding information is used to automatically establish a secure connection between the device and a trusted lifecycle management service. The service downloads the latest version of the intended application to the device. Next, the device executes the application and becomes operational on the network.

While the device is operational, a number of processes can be performed on an ongoing basis to ensure continued security throughout the device's lifecycle. Examples include, but are not limited to, the following. Additional capabilities, such as device profiling, device behavior analysis, device health posture attestation, and others are also possible:

- If device intent is supported, the traffic filters that were specified by the device intent information are enforced to ensure that communications to and from the device are restricted to only those that are required. Local network policy can also be applied in addition to the device intent-specified policy.
- The device can be assigned to a particular network segment, for example based on level of trust, device type, or attestation token evaluation. The device can be dynamically reassigned to another segment, such as quarantining the device if its trustworthiness comes into question.
- The device's firmware, software, and configuration are updated and patched as needed to address vulnerabilities.
- The device and its trusted lifecycle management service perform ongoing mutual attestation to ensure each other's trustworthiness.
- If the trusted network-layer onboarding solution and the organization's asset management system are integrated, the asset management system can periodically cross-check its discovered devices with the onboarded IoT devices to ensure there are no discrepancies. The asset management system can also assess and remediate the devices' software and configurations to identify known vulnerabilities.

Notional High-Level Solution Architecture

Figure 2 depicts a notional high-level architecture for a trusted network-layer onboarding solution. The means of access to the network could be wired and/or wireless. The architecture

has five component types: IoT devices to be onboarded; a network onboarding component; an authorization service; a supply chain integration service; and an access point, router, or switch providing local network connectivity for the IoT devices. Figure 2 does not include other components that would be needed to provide additional protections throughout the device lifecycle, such as attestation, device intent, application-layer onboarding, and others listed above, but it does show how the information required to support these protections could be securely conveyed to the network during the network-layer onboarding process.

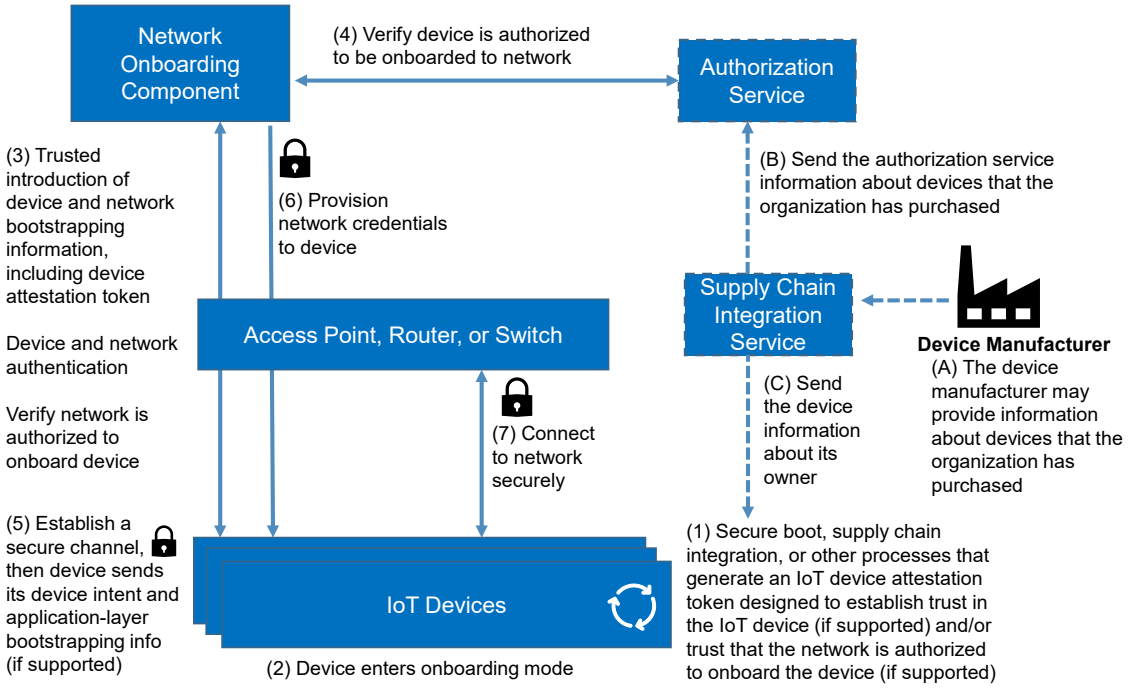

Figure 2: Notional High-Level Architecture

The following summarizes possible steps in trusted network-layer onboarding based on the Figure 2 architecture. The numbered and lettered items correspond to the numbers and letters in the figure. A, B and C are an optional series of steps that may precede or occur as part of the onboarding process.

A. The device manufacturer may send information about devices that the organization has purchased to an on-premises or cloud-based supply chain integration service.

B. The supply chain integration service may provide device information to the authorization service to help it determine whether devices that are attempting to onboard to the network are authorized to do so.

C. The supply chain integration service may provide the device with information about its owner to help the device determine whether the network that is attempting to onboard it is authorized to do so.

1. This is an optional step for devices and onboarding solutions that support attestation. The IoT device generates or receives an attestation token that makes claims about the device posture (e.g., device ID, manufacturer, model, installed software, versions, boot

state, measurements, integrity checks of running hardware and firmware/software). This step might involve integration with supply-chain management tools that can provide assurance that devices are authentic, that their hardware, firmware, and software has not been tampered with or altered, or that they are owned by a specific entity.

2. The IoT device to be onboarded is placed in onboarding mode, i.e., it is put into a state such that it is actively listening for and able to send onboarding protocol messages.
3. Bootstrapping is performed to provide a trusted introduction of device information to the network onboarding component and network information to the device. In some onboarding solutions, a person may be required to perform some aspects of this trusted introduction of bootstrapping information and this introduction may be performed out of band, but other onboarding solutions may support zero-touch, in-band introduction of bootstrapping information. The distribution of device information from the manufacturer to both the authorization service and the device via the supply chain integration service, as shown in optional steps A, B, and C of Figure 2, may help facilitate such a zero-touch introduction of information. Using the device and network bootstrapping credentials that were provided via the trusted introduction, the network onboarding component authenticates the identity of the IoT device and the IoT device authenticates the identity of the network. The device also verifies that the network is authorized to onboard it. The device sends the device attestation token that it had generated in step 1 (if any) to the network onboarding component.
4. The network onboarding component consults the network's authorization service to verify that the device is authorized to be onboarded to the network.
5. A secure channel is established between the network onboarding component and the device. If supported, the device uses the secure channel to send device intent and application-layer bootstrapping information to the network.
6. The network onboarding component uses the secure channel to send the device its network credentials.
7. The device uses its newly provisioned credentials to securely connect to the network.

Component List

The project's high-level architecture is expected to include the following components:

- **IoT devices**: Each device must be able to participate in trusted network-layer onboarding and to securely store private keys, credentials, and other information. Each device may have other capabilities that enable its use with additional solution components, such as the examples listed below.
- **Network onboarding component**: The network onboarding component is a logical component on the network that runs the network-layer onboarding protocol. It is authorized to interact with IoT devices on behalf of the network and use the network-layer onboarding protocol to onboard devices to the network.
- **Authorization service**: The authorization service must be able to determine which IoT devices are authorized to be onboarded to the network and maintain a record of which devices have been onboarded.
- **Supply chain integration service:** The supply chain integration service receives information about devices that the organization has purchased and provides this

information to the authorization service to help the authorization service determine which devices are authorized to be onboarded to the network.

- **Access point, router, or switch**: The access point, router, or switch must be able to provide network access for all traffic to and from the IoT devices.

In addition, the architecture may contain several types of additional components, none of which are depicted in Figure 2. The following is a list of some of the types of additional components that could potentially be included. This list is not intended to be prescriptive or comprehensive:

- **Device intent management**: This could include device intent managers, information servers, and components applying device intent policy.
- **Attestation service**: An attestation service could receive attestation tokens from IoT devices, evaluate them, and generate results that it returns to the network onboarding component to enable that component to decide whether or not the devices are trustworthy enough to be onboarded. The attestation service could also receive attestation tokens from IoT devices and any other connected components on an ongoing basis to help determine their continued trustworthiness.
- **Controller, application server, or cloud service**: This remote service could securely download one or more applications to the device during application-layer onboarding.
- **Lifecycle management service**: This service could perform ongoing, automated lifecycle management of the device, such as applying firmware, software, and configuration updates to manage the overall security posture of the device throughout its lifecycle.
- **Asset management**: This service could integrate with the onboarding system to enable cross-checking the list of devices that have been securely onboarded with the inventory of connected devices. It could also monitor the software and configuration of onboarded IoT devices for known vulnerabilities.

Desired Capabilities

The following are desired capabilities for a trusted network-layer onboarding solution. They are drawn from the list and definitions in [6]. Note that this list does not include additional capabilities beyond the trusted network-layer onboarding solution itself, such as application-layer onboarding and ongoing device lifecycle management protections. See the “Logical Architecture” section of this document for more information on these capabilities.

Device Identity Management, Authentication, and Access Control:

- Each IoT device has unique, distinguishing logical and physical identifiers that map uniquely to the device. Ideally, these identifiers should be privacy-preserving.
- The solution verifies that the asserted identity of each device is the device’s actual identity.
- The solution integrates with an authorization mechanism that determines whether each device should be permitted to connect to the network.
- The solution securely provisions locally significant and unique credentials to the device.
- The solution updates/replaces the device’s network credentials in a secure manner.

Network Identity Management, Authentication, and Access Control:

- The solution provides the identifier of the network to which the device should connect as part of the network credentials that it provisions.

- The solution verifies that the network's asserted identity is its actual identity.
- The solution enables the device to verify that the network is authorized to take control of the device before the device allows itself to be onboarded.

Data Protection:

- The solution uses standardized encryption, cryptographic hashing, and digital signature validation algorithms.
- The solution can be reused on a device to replace the device's current credentials. Before doing so, sensitive information that has been stored on the device since the completion of the manufacturing process may be deleted.
- Any artifacts that the onboarding solution uses to support proof-of-ownership, secure ownership transfer, or other mechanisms used to establish authorization to onboard are protected from unauthorized disclosure while in transit and at rest.

4 Relevant Standards and Guidance

The following standards, papers, and other documents served as guidance for the proposed project:

- G. Cooper et al. (editors), *FIDO Device Onboard Specification*, Proposed Standard, March 23, 2021. https://fidoalliance.org/specs/FDO/fido-device-onboard-v1.0-ps-20210323/fido-device-onboard-v1.0-ps-20210323.pdf
- European Telecommunications Standards Institute (ETSI), *Cyber Security for Consumer Internet of Things: Baseline Requirements*, ETSI EN 303 645, V2.1.1 (2020-06), June 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- M. Fagan, K.N. Megas, K. Scarfone, and M. Smith, *IoT Device Cybersecurity Capability Core Baseline,* National Institute of Standards and Technology, NISTIR 8259A, May 2020. https://doi.org/10.6028/NIST.IR.8259A
- G. Mandyam, L. Lundblade, M. Ballesteros, and J. O'Donoghue, *The Entity Attestation Token (EAT)*, IETF Remote Attestation Procedures Working Group, March 2021. Available: https://tools.ietf.org/html/draft-ietf-rats-eat-09
- M. Pritikin, M. Richardson, T.T.E. Eckert, M.H. Behringer, and K.W. Watsen, *Bootstrapping Remote Secure Key Infrastructures (BRSKI)*, Nov. 2020. https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
- K. Watsen, I. Farrer, and M. Abrahamsson, *Secure Zero Touch Provisioning (SZTP)*, IETF RFC 8572, April 2019. Available: https://datatracker.ietf.org/doc/rfc8572
- Wi-Fi Alliance, *Wi-Fi Easy Connect™ Specification Version 2.0*, 2020. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Easy_Connect_Specification_v2.0.pdf

APPENDIX A REFERENCES

[1] Intel Corporation, *Intel Secure Device Onboard*, Intel Corporation Product Brief, 2019. Available: https://www.intel.com/content/dam/www/public/us/en/documents/idz/iot/briefs/sdo-product-brief.pdf

[2] Kaiser Associates, Inc., *IoT Onboarding: A Device Manufacturer's Perspective*, 2017. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/kaiser-associates-iot-onboarding-for-device-manufacturers-whitepaper.pdf

[3] Wi-Fi Alliance, *Wi-Fi Easy Connect™ Specification Version 2.0*,2020. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Easy_Connect_Specification_v2.0.pdf

[4] M. Pritikin, M. Richardson, T.T.E. Eckert, M.H. Behringer, and K.W. Watsen, *Bootstrapping Remote Secure Key Infrastructures (BRSKI)*, Nov. 2020. Available: https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/

[5] K. Watsen, I. Farrer, and M. Abrahamsson, *Secure Zero Touch Provisioning (SZTP)*, IETF RFC 8572, April 2019. Available: https://datatracker.ietf.org/doc/rfc8572

[6] S. Symington, W. Polk, and M. Souppaya, *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management (Draft)*, National Institute of Standards and Technology (NIST) Draft Cybersecurity White Paper, Gaithersburg, MD, Sept. 2020, 88 pp. https://doi.org/10.6028/NIST.CSWP.09082020-draft

[7] G. Cooper et al. (editors), *FIDO Device Onboard Specification*, Proposed Standard, March 23, 2021. https://fidoalliance.org/specs/FDO/fido-device-onboard-v1.0-ps-20210323/fido-device-onboard-v1.0-ps-20210323.pdf

[8] E. Lear, R. Droms, and D. Romascanu, *Manufacturer Usage Description Specification,* IETF Request for Comments (RFC) 8520, March 2019. Available: https://tools.ietf.org/html/rfc8520